aws

Panduan Pengguna

Amazon Virtual Private Cloud



Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Virtual Private Cloud: Panduan Pengguna

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu Amazon VPC? ... 1
Fitur ... 1
Mulai menggunakan Amazon VPC ... 3
Bekerja dengan Amazon VPC ... 3
Harga untuk Amazon VPC ... 3
Cara Amazon VPC Berfungsi ... 6
VPC dan subnet ... 7
VPC default dan nondefault ... 7
Tabel rute ... 8
Mengakses internet ... 8
Mengakses jaringan perusahaan atau rumah ... 9
Connect VPC dan jaringan ... 10
AWS jaringan global pribadi ... 10
Merencanakan VPC Anda ... 11
Mendaftar untuk Akun AWS ... 11
Mendaftar untuk Akun AWS ... 11
Memverifikasi izin ... 11
Tentukan rentang alamat IP Anda ... 11
Pilih Zona Ketersediaan Anda ... 12
Rencanakan konektivitas internet Anda ... 12
Buat VPC Anda ... 13
Men-deploy aplikasi Anda ... 13
Penentuan alamat IP ... 15
Alamat IPv4 privat ... 16
Alamat IPv4 publik ... 16
Alamat IPv6 ... 18
Alamat IPv6 publik ... 19
Alamat IPv6 pribadi ... 19
Gunakan Alamat IP Anda sendiri ... 21
Gunakan Manajer Alamat IP Amazon VPC ... 22
Blok VPC CIDR ... 22
Blok IPv4 VPC CIDR ... 22
Mengelola blok CIDR IPv4 untuk VPC ... 23
Pembatasan pengaitan blok CIDR IPv4 ... 26

Blok IPv6 VPC CIDR 28
Blok subnet CIDR 29
Ukuran subnet untuk IPv4 30
Ukuran subnet untuk IPv6 30
Bandingkan IPv4 dan IPv6 31
Daftar prefiks terkelola 33
Konsep dan aturan daftar prefiks 33
Identity and access management untuk daftar prefiks 35
Customer-managed daftar awalan 36
AWS Daftar prefiks yang dikelola 46
Pengoptimalan AWS manajemen infrastruktur dengan daftar awalan 48
AWS Rentang alamat IP 51
Unduh 52
Kontrol keluar 52
Umpan geolokasi 53
Temukan rentang alamat 53
Sintaksis 59
Berlangganan notifikasi 65
Dukungan IPv6 untuk VPC Anda 67
Menambahkan dukungan IPv6 untuk VPC Anda 67
Contoh VPC tumpukan ganda 72
Dukungan IPv6 pada AWS 74
Layanan yang mendukung IPv6 74
Dukungan IPv6 tambahan 88
Pelajari selengkapnya 89
Virtual private cloud 90
Dasar-dasar VPC 91
Rentang alamat IP VPC 91
Diagram VPC 91
Sumber daya VPC 92
Opsi konfigurasi VPC 93
VPC default 95
Komponen VPC default 95
Subnet default 98
Bekerja dengan VPC default dan subnet default 99
Buat VPC 103

Buat VPC plus sumber daya VPC lainnya 103
Buat VPC saja 105
Buat VPC menggunakan AWS CLI 107
Visualisasikan sumber daya di VPC Anda 112
Tambah atau hapus blok CIDR 113
Set opsi DHCP 116
Apa itu DHCP? 116
Konsep set opsi DHCP 117
Bekerja dengan set opsi DHCP 121
Atribut DNS 125
Memahami Amazon DNS 126
Lihat nama host DNS untuk instans EC2 Anda 131
Melihat dan memperbarui atribut DNS untuk VPC Anda 132
Penggunaan Alamat Jaringan 133
Melebihi Kuota NAU 134
Bagaimana NAU dihitung 134
Contoh NAU 135
Bagikan subnet VPC 137
Prasyarat subnet bersama 138
Bekerja dengan subnet bersama 138
Penagihan dan pengukuran untuk pemilik dan peserta 141
Tanggung jawab dan izin untuk pemilik dan peserta 142
AWS sumber daya dan subnet VPC bersama 145
Memperluas VPC ke Zona lain 146
Subnets di AWS Zona Lokal 147
Subnets di AWS Wavelength 152
Subnets di AWS Outposts 155
Hapus VPC Anda 156
Hapus menggunakan konsol 157
Hapus menggunakan CLI 158
Hasilkan IaC dari tindakan konsol 159
Subnet 161
Dasar-Dasar Subnet 161
Rentang alamat IP subnet 161
Jenis subnet 162
Diagram subnet 163

Perutean subnet 163
Pengaturan subnet 163
Keamanan subnet 164
Membuat subnet 165
Menambahkan atau menghapus blok IPv6 CIDR dari subnet Anda 167
Ubah atribut pengalamatan IP subnet Anda 167
Reservasi CIDR subnet 169
Bekerja dengan reservasi CIDR subnet menggunakan konsol 170
Bekerja dengan reservasi CIDR subnet menggunakan AWS CLI 170
Tabel rute 171
Konsep tabel rute 172
Tabel rute subnet 174
Tabel rute gateway 181
Prioritas rute 184
Opsi perutean contoh 186
Buat tabel rute dan rute 202
Kelola tabel rute subnet 204
Ganti tabel rute utama 208
Mengaitkan tabel rute dengan gateway 209
Mengganti atau memulihkan target untuk rute lokal 209
Perutean lanjutan 211
Memecahkan masalah keterjangkauan 258
Wisaya perutean Middlebox 258
Prasyarat wizard perutean Middlebox 259
Arahkan lalu lintas VPC ke alat keamanan 259
Pertimbangan wizard perutean Middlebox 262
Skenario Middlebox 262
Hapus subnet 272
Hubungkan VPC Anda 274
Gateway internet 275
Dasar-dasar gateway internet 276
Membuat gateway internet baru 279
Menghapus gateway internet 281
Egress-only gerbang internet 282
Egress-only dasar-dasar gateway internet 283
Tambahkan akses internet khusus egress ke subnet 284

Perangkat NAT 287
Gateway NAT 288
Instans NAT 342
Bandingkan perangkat NAT 354
Alamat IP elastis 357
Konsep dan aturan alamat IP Elastis 358
Mulai gunakan alamat IP Elastic 360
AWS Gerbang Transit 369
AWS Virtual Private Network 370
Koneksi peering VPC 372
Memantau 373
Log Alur VPC 374
Dasar-dasar log alur 375
Catatan log alur 378
Contoh catatan log alur 395
Batasan log alur 406
Harga 410
Bekerja dengan log alur 411
Publikasikan ke CloudWatch Log 414
Terbitkan ke Amazon S3 422
Publikasikan ke Amazon Data Firehose 431
Kueri menggunakan Athena 439
Identitas dan manajemen akses di Log Aliran VPC 444
Pemecahan Masalah 452
CloudWatch metrik 456
Metrik dan dimensi NAU 457
Mengaktifkan atau menonaktifkan pemantauan NAU 460
Contoh CloudWatch alarm NAU 460
Laporan penagihan dan penggunaan 461
Manajemen alamat IP 462
Titik akhir VPC 463
Transit gateway 463
Analisis jaringan 464
Mirroring lalu lintas 464
Kisi VPC 465
Sumber daya lintas akun/wilayah 465

Jelaskan jaringan VPC Anda 466
Lokasi geografis 467
Subnet 468
Konektivitas Jaringan 470
Kontrol keamanan 475
Manajemen lalu lintas 477
Sumber daya terkait 479
Keamanan 481
Perlindungan data 482
Privasi lalu lintas antarjaringan 483
Menerapkan enkripsi VPC saat transit 484
Mode Kontrol Enkripsi 484
Memantau status Enkripsi Arus Lalu Lintas 485
Pengecualian Kontrol Enkripsi VPC 486
Alur kerja implementasi 487
Status Kontrol Enkripsi VPC 487
AWS dukungan layanan dan kompatibilitas 488
Harga 3
AWS CLI referensi perintah 493
Sumber daya tambahan 494
Manajemen identitas dan akses 494
Audiens 495
Mengautentikasi menggunakan identitas 495
Mengelola akses menggunakan kebijakan 496
Bagaimana cara Amazon VPC bekerja sama dengan IAM 498
Contoh kebijakan 503
Pemecahan Masalah 516
AWS kebijakan yang dikelola 518
Menggunakan peran tertaut layanan 522
Keamanan infrastruktur 527
Isolasi jaringan 527
Mengendalikan lalu lintas jaringan 528
Membandingkan grup keamanan dan ACL jaringan 529
Grup keamanan 530
Dasar-dasar grup keamanan 532
Contoh grup keamanan 533

Aturan grup keamanan ... 534
Grup keamanan default ... 540
Membuat grup keamanan ... 542
Mengonfigurasi aturan grup keamanan ... 544
Menghapus grup keamanan ... 546
Mengaitkan grup keamanan dengan beberapa VPC ... 547
Bagikan grup keamanan dengan AWS Organizations ... 550
ACL jaringan ... 556
Dasar-dasar ACL jaringan ... 557
Aturan ACL Jaringan ... 559
ACL jaringan default ... 560
ACL jaringan kustom ... 562
Path MTU Discovery ... 568
Buat ACL jaringan ... 568
Kelola asosiasi ACL jaringan ... 572
Menghapus ACL jaringan ... 575
Contoh: Kontrol akses ke instans dalam subnet ... 576
Ketahanan ... 579
Validasi kepatuhan ... 580
Blokir akses publik ke VPC dan subnet ... 581
Dasar-dasar VPC BPA ... 582
Menilai dampak VPC BPA dan memantau VPC BPA ... 588
Contoh lanjutan ... 593
Praktik terbaik ... 647
Gunakan dengan layanan lain ... 649
AWS PrivateLink ... 650
AWS Network Firewall ... 651
Route 53 Resolver DNS Firewall ... 653
Reachability Analyzer ... 654
Contoh ... 655
Lingkungan uji ... 656
Ikhtisar ... 656
1. Buat VPC ... 658
2. Men-deploy aplikasi Anda ... 659
3. Uji konfigurasi Anda ... 660
4. Bersihkan ... 660

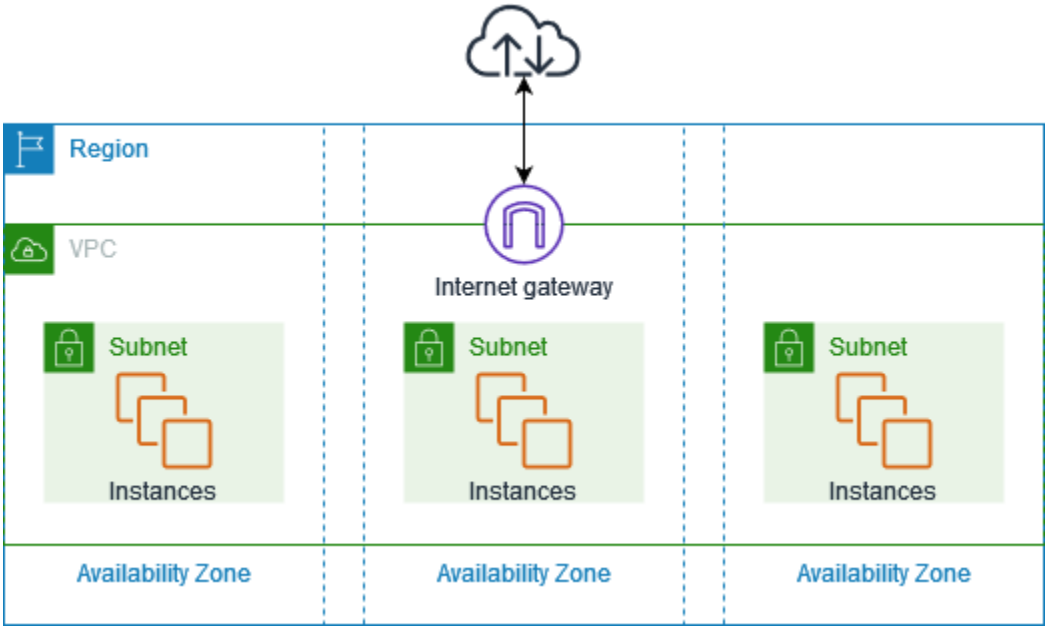
Server web dan database ... 660
Ikhtisar ... 661
1. Buat VPC ... 665
2. Men-deploy aplikasi Anda ... 666
3. Uji konfigurasi Anda ... 666
4. Bersihkan ... 667
Server pribadi ... 667
Gambaran umum ... 667
1. Buat VPC ... 670
2. Men-deploy aplikasi Anda ... 671
3. Uji konfigurasi Anda ... 671
4. Bersihkan ... 672
Tutorial ... 673
Memulai dengan Amazon VPC menggunakan AWS CLI ... 673
Prasyarat ... 674
Buat VPC ... 674
Buat subnet ... 675
Konfigurasikan konektivitas internet ... 677
Buat Gateway NAT ... 678
Konfigurasikan pengaturan subnet ... 679
Buat grup keamanan ... 680
Verifikasi konfigurasi VPC Anda ... 681
Menyebarkan contoh EC2 ... 682
Pemecahan masalah ... 225
Pembersihan sumber daya ... 685
Pergi ke produksi ... 686
Langkah selanjutnya ... 687
Buat VPC dengan subnet pribadi dan gateway NAT menggunakan AWS CLI ... 687
Prasyarat ... 674
Buat VPC dan subnet ... 689
Buat dan konfigurasikan konektivitas internet ... 691
Buat gateway NAT ... 693
Buat titik akhir VPC untuk Amazon S3 ... 694
Konfigurasikan grup keamanan ... 695
Buat template peluncuran untuk EC2 instance ... 696
Buat penyeimbang beban dan grup target ... 698

Membuat grup Auto Scaling 699
Uji konfigurasi Anda 700
Pembersihan sumber daya 685
Langkah berikutnya 687
Kuota 703
VPC dan subnet 703
DNS 704
Alamat IP elastis 704
Gateway 704
Customer-managed daftar awalan 705
ACL jaringan 707
Antarmuka jaringan 707
Tabel rute 708
Server rute 709
Grup keamanan 711
Berbagi subnet VPC 712
Penggunaan Alamat Jaringan 713
Amazon EC2 API throttling 713
Sumber daya kuota tambahan 713
Riwayat dokumen 715
..... dccxxvii

Apa itu Amazon VPC?

Dengan Amazon Virtual Private Cloud (Amazon VPC), Anda dapat meluncurkan AWS sumber daya di jaringan virtual yang terisolasi secara logis yang telah Anda tentukan. Jaringan virtual ini sangat mirip dengan jaringan konvensional yang akan Anda operasikan di pusat data Anda sendiri dengan manfaatnya, yaitu menggunakan infrastruktur AWS yang dapat diskalakan.

Diagram berikut menunjukkan contoh VPC. VPC memiliki satu subnet di setiap Availability Zone di Region, EC2 instance di setiap subnet, dan gateway internet untuk memungkinkan komunikasi antara sumber daya di VPC Anda dan internet.



Untuk informasi selengkapnya, lihat Amazon Virtual Private Cloud (Amazon VPC).

Fitur

Fitur-fitur berikut membantu Anda mengonfigurasi VPC untuk menyediakan konektivitas yang dibutuhkan aplikasi Anda:

Awan pribadi virtual (VPC)

VPC adalah jaringan virtual yang sangat mirip dengan jaringan tradisional yang akan Anda operasikan di pusat data Anda sendiri. Setelah Anda membuat VPC, Anda dapat menambahkan subnet.

Subnet

Sebuah subnet adalah rentang alamat IP di VPC Anda. Subnet harus berada di Availability Zone tunggal. Setelah menambahkan subnet, Anda dapat menyebarkan AWS sumber daya di VPC Anda.

Penentuan alamat IP

Anda dapat menetapkan alamat IP, baik IPv4 dan IPv6, ke subnet VPCs dan Anda. Anda juga dapat membawa IPv4 alamat publik dan alamat IPv6 GUA ke AWS dan mengalokasikannya ke sumber daya di VPC Anda, EC2 seperti instance, gateway NAT, dan Network Load Balancer.

Perutean

Gunakan tabel rute untuk menentukan ke mana lalu lintas jaringan dari subnet atau gateway Anda diarahkan.

Gateway dan titik akhir

Gateway menghubungkan VPC Anda ke jaringan lain. Misalnya, gunakan gateway internet untuk menghubungkan VPC Anda ke internet. Gunakan titik akhir VPC untuk terhubung Layanan AWS secara pribadi, tanpa menggunakan gateway internet atau perangkat NAT.

Koneksi mengintip

Gunakan koneksi peering VPC untuk merutekan lalu lintas antara sumber daya menjadi dua. VPCs

Pencerminan Lalu lintas

Salin lalu lintas jaringan dari antarmuka jaringan dan kirimkan ke peralatan keamanan dan pemantauan untuk inspeksi paket mendalam.

Transit gateway

Gunakan gateway transit, yang bertindak sebagai hub pusat, untuk merutekan lalu lintas antara Anda VPCs, koneksi VPN, dan Direct Connect koneksi.

Log Alur VPC

Flow log menangkap informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di VPC Anda.

Koneksi VPN

Hubungkan VPCs ke jaringan lokal menggunakan AWS Virtual Private Network (Site-to-Site VPN).

Mulai menggunakan Amazon VPC

Anda Akun AWS menyertakan VPC default di masing-masing. Wilayah AWS Default Anda VPCs dikonfigurasi sedemikian rupa sehingga Anda dapat segera mulai meluncurkan dan menghubungkan ke EC2 instance. Untuk informasi selengkapnya, lihat Merencanakan VPC Anda.

Anda dapat memilih untuk membuat tambahan VPCs dengan subnet, alamat IP, gateway dan routing yang Anda butuhkan. Untuk informasi selengkapnya, lihat the section called “Buat VPC”.

Bekerja dengan Amazon VPC

Anda dapat membuat dan mengelola Anda VPCs menggunakan salah satu antarmuka berikut:

- Konsol Manajemen AWS— Menyediakan antarmuka web yang dapat Anda gunakan untuk mengakses Anda VPCs.
- AWS Command Line Interface (AWS CLI) - Menyediakan perintah untuk serangkaian AWS layanan yang luas, termasuk Amazon VPC, dan didukung di Windows, Mac, dan Linux. Untuk informasi selengkapnya, lihat AWS Command Line Interface.
- AWS SDKsMenyediakan bahasa khusus APIs dan menangani banyak detail koneksi, seperti menghitung tanda tangan, menangani percobaan ulang permintaan, dan penanganan kesalahan. Untuk informasi selengkapnya, lihat AWS SDKs.
- Kueri API — Menyediakan tindakan API tingkat rendah yang Anda hubungi menggunakan permintaan HTTPS. Menggunakan API Kueri merupakan cara paling langsung untuk mengakses Amazon VPC, tetapi mengharuskan aplikasi Anda menangani detail tingkat rendah seperti membuat hash untuk menandatangani permintaan, dan penanganan kesalahan. Untuk informasi selengkapnya, lihat tindakan Amazon VPC di Referensi Amazon EC2 API.

Harga untuk Amazon VPC

Tidak ada biaya tambahan untuk menggunakan VPC. Namun, ada biaya untuk beberapa komponen VPC, seperti gateway NAT, Manajer Alamat IP, pencerminan lalu lintas, Reachability Analyzer, dan Network Access Analyzer. Untuk informasi lebih lanjut, lihat Harga Amazon VPC.

Hampir semua sumber daya yang Anda luncurkan di virtual private cloud (VPC) memberi Anda alamat IP untuk konektivitas. Sebagian besar sumber daya di VPC Anda menggunakan alamat pribadi IPv4 . Sumber daya yang membutuhkan akses langsung ke internet melalui IPv4, bagaimanapun, menggunakan IPv4 alamat publik.

Amazon VPC memungkinkan Anda meluncurkan layanan terkelola, seperti Elastic Load Balancing, Amazon RDS, dan Amazon EMR, tanpa menyiapkan VPC terlebih dahulu. Ini dilakukan dengan menggunakan VPC default di akun Anda jika Anda memilikinya. Setiap IPv4 alamat publik yang disediakan ke akun Anda oleh layanan terkelola akan dikenakan biaya. Biaya ini akan dikaitkan dengan layanan Amazon VPC di Anda. AWS Cost and Usage Report

Harga untuk IPv4 alamat publik

IPv4 Alamat publik adalah IPv4 alamat yang dapat dirutekan dari internet. IPv4 Alamat publik diperlukan agar sumber daya dapat dijangkau secara langsung dari internet melalui. IPv4

Jika Anda adalah pelanggan Tingkat AWS Gratis yang sudah ada atau baru, Anda mendapatkan 750 jam penggunaan IPv4 alamat publik dengan EC2 layanan tanpa biaya. Jika Anda tidak menggunakan EC2 layanan di Tingkat AWS Gratis, IPv4 alamat publik akan dikenakan biaya. Untuk informasi harga tertentu, lihat tab IPv4 Alamat publik di Harga Amazon VPC.

IPv4 Alamat pribadi (RFC 1918) tidak dikenakan biaya. Untuk informasi selengkapnya tentang cara IPv4 alamat publik dikenakan biaya untuk dibagikan VPCs, lihat Penagihan dan pengukuran untuk pemilik dan peserta.

IPv4 Alamat publik memiliki jenis berikut:

- Alamat IP elastis (EIPs): IPv4 Alamat publik statis yang disediakan oleh Amazon yang dapat Anda kaitkan dengan EC2 instance, elastic network interface, atau AWS sumber daya.
- EC2 IPv4 alamat publik: IPv4 Alamat publik yang ditetapkan ke EC2 instans oleh Amazon (jika EC2 instance diluncurkan ke subnet default atau jika instance diluncurkan ke subnet yang telah dikonfigurasi untuk menetapkan alamat publik IPv4 secara otomatis).
- BYOIPv4 alamat: IPv4 Alamat publik dalam rentang IPv4 alamat yang Anda bawa AWS menggunakan Bring your own IP address (BYOIP).
- Alamat yang dikelola layanan: IPv4 IPv4 Alamat publik secara otomatis disediakan pada AWS sumber daya dan dikelola oleh layanan. AWS Misalnya, IPv4 alamat publik di Amazon ECS, Amazon RDS, atau Amazon. WorkSpaces

Daftar berikut menunjukkan AWS layanan paling umum yang dapat menggunakan IPv4 alamat publik.

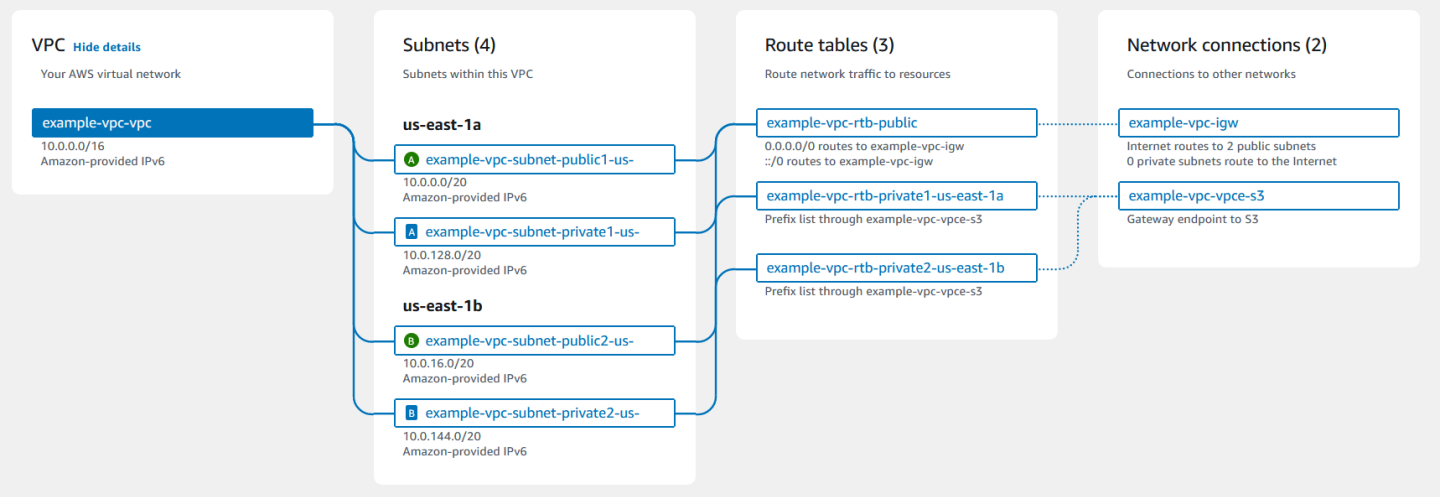
- WorkSpaces Aplikasi Amazon
- AWS Client VPN

- AWS Database Migration Service
- Amazon EC2
- Amazon Elastic Container Service
- Amazon EKS
- Amazon EMR
- GameLift Peladen Amazon
- AWS Global Accelerator
- AWS Mainframe Modernization
- Amazon Managed Streaming untuk Apache Kafka
- Amazon MQ
- Amazon RDS
- Amazon Redshift
- AWS Site-to-Site VPN
- Gerbang NAT VPC Amazon
- Amazon WorkSpaces
- Penyeimbang Beban Elastis

Cara Amazon VPC Berfungsi

Dengan Amazon Virtual Private Cloud (Amazon VPC), Anda dapat meluncurkan AWS sumber daya dalam jaringan virtual yang terisolasi secara logis yang telah Anda tentukan. Jaringan virtual ini sangat mirip dengan jaringan konvensional yang akan Anda operasikan di pusat data Anda sendiri dengan manfaatnya, yaitu menggunakan infrastruktur AWS yang dapat diskalakan.

Berikut ini adalah representasi visual dari VPC dan sumber dayanya dari panel Pr atinjau yang ditampilkan saat Anda membuat VPC menggunakan. Konsol Manajemen AWS Untuk VPC yang ada, Anda dapat mengakses visualisasi ini pada tab peta sumber daya. Contoh ini menunjukkan sumber daya yang awalnya dipilih pada halaman Buat VPC saat Anda memilih untuk membuat VPC ditambah sumber daya jaringan lainnya. VPC ini dikonfigurasi dengan IPv4 CIDR dan Amazon-provided IPv6 CIDR, subnet di dua Zona Ketersediaan, tiga tabel rute, gateway internet, dan titik akhir gateway. Karena kami telah memilih gateway internet, visualisasi menunjukkan bahwa lalu lintas dari subnet publik dialihkan ke internet karena tabel rute yang sesuai mengirimkan lalu lintas ke gateway internet.



Konsep

- VPC dan subnet
- VPC default dan nondefault
- Tabel rute
- Mengakses internet
- Mengakses jaringan perusahaan atau rumah
- Connect VPC dan jaringan

- AWS jaringan global pribadi

VPC dan subnet

Sebuah virtual private cloud (VPC) adalah jaringan sebuah virtual yang didedikasikan untuk akun AWS Anda. Secara logis terisolasi dari jaringan virtual lain di AWS Cloud. Anda dapat menentukan rentang alamat IP untuk VPC, menambahkan subnet, menambahkan gateway, dan mengaitkan grup keamanan.

Sebuah subnet adalah rentang alamat IP di VPC Anda. Anda meluncurkan AWS sumber daya, seperti instans Amazon EC2, ke subnet Anda. Anda dapat menghubungkan subnet ke internet, VPC lain, dan pusat data Anda sendiri, dan merutekan lalu lintas ke dan dari subnet Anda menggunakan tabel rute.

Pelajari selengkapnya

- Penentuan alamat IP
- Virtual private cloud
- Subnet

VPC default dan nondefault

Jika akun Anda dibuat setelah 4 Desember 2013, itu dilengkapi dengan VPC default di setiap Wilayah. VPC default dikonfigurasi dan siap untuk Anda gunakan. Misalnya, ia memiliki subnet default di setiap Zona Ketersediaan di Wilayah, gateway internet terlampir, rute di tabel rute utama yang mengirimkan semua lalu lintas ke gateway internet, dan pengaturan DNS yang secara otomatis menetapkan nama host DNS publik ke instans dengan alamat IP publik dan mengaktifkan resolusi DNS melalui server Amazon-provided DNS (lihatAtribut DNS untuk VPC Anda). Oleh karena itu, instance EC2 yang diluncurkan di subnet default secara otomatis memiliki akses ke internet. Jika Anda memiliki VPC default di Wilayah dan Anda tidak menentukan subnet saat meluncurkan instance EC2 ke Wilayah tersebut, kami memilih salah satu subnet default dan meluncurkan instance ke subnet tersebut.

Anda dapat juga membuat VPC Anda sendiri dan mengonfigurasinya sesuai kebutuhan. Hal ini dikenal sebagai VPC nondefault. Subnet yang Anda buat di VPC nondefault dan subnet tambahan yang Anda buat di VPC default Anda disebut subnet nondefault.

Pelajari selengkapnya

- the section called “VPC default”
- the section called “Buat VPC”

Tabel rute

Tabel rute berisi seperangkat aturan, yang disebut rute, yang digunakan untuk menentukan ke mana lalu lintas jaringan dari VPC Anda diarahkan. Anda dapat secara eksplisit mengaitkan subnet dengan tabel rute tertentu. Jika tidak, subnet secara implisit dikaitkan dengan tabel rute utama.

Setiap rute dalam tabel rute menentukan rentang alamat IP ke mana lalu lintas Anda ingin arahkan (tujuan) dan gateway, antarmuka jaringan, atau koneksi yang Anda gunakan untuk mengirim lalu lintas (target).

Pelajari selengkapnya

- Konfigurasikan tabel rute

Mengakses internet

Anda mengendalikan bagaimana instans yang Anda luncurkan ke sumber daya akses VPC di luar VPC.

VPC default mencakup gateway internet, dan setiap subnet default adalah subnet publik. Setiap instans yang Anda luncurkan ke subnet default memiliki alamat IPv4 privat dan alamat IPv4 publik. Instans ini dapat berkomunikasi dengan internet melalui gateway internet. Gateway internet memungkinkan instans Anda terhubung ke internet melalui jaringan edge Amazon EC2.

Secara default, setiap instans yang Anda luncurkan ke subnet nondefault memiliki alamat IPv4 privat, tetapi tidak memiliki alamat IPv4 publik, kecuali jika Anda secara khusus menetapkan satu alamat saat meluncurkannya, atau jika Anda mengubah atribut alamat IP publik subnet. Instans ini dapat berkomunikasi antara satu sama lain, tetapi tidak dapat mengakses internet.

Anda dapat mengaktifkan akses internet untuk sebuah instans yang diluncurkan ke subnet nondefault dengan melampirkan gateway internet untuk VPC nya (jika VPC bukan VPC default) dan mengaitkan alamat P Elastis dengan instans.

Atau, untuk memungkinkan sebuah instans di VPC Anda untuk memulai koneksi keluar ke internet tetapi mencegah koneksi masuk yang tidak diminta dari internet, Anda dapat menggunakan perangkat network address translation (NAT). NAT memetakan beberapa alamat IPv4 privat ke alamat IPv4 publik tunggal. Anda dapat mengkonfigurasi perangkat NAT dengan alamat IP Elastis dan menghubungkannya ke internet melalui gateway internet. Hal ini memungkinkan sebuah instans dalam subnet privat untuk terhubung ke internet melalui perangkat NAT, merutekan lalu lintas dari instans ke gateway internet dan setiap jawaban ke instans.

Jika Anda mengaitkan blok CIDR IPv6 dengan VPC Anda dan menetapkan alamat IPv6 ke instans Anda, instans dapat terhubung ke internet melalui IPv6 melalui gateway internet. Sebagai alternatif, instans dapat memulai koneksi keluar ke internet melalui IPv6 menggunakan gateway internet egress-only. Lalu lintas IPv6 terpisah dari lalu lintas IPv4; tabel rute Anda harus menyertakan rute terpisah untuk lalu lintas IPv6.

Pelajari selengkapnya

- Aktifkan akses internet untuk VPC menggunakan gateway internet
- Aktifkan lalu lintas IPv6 keluar menggunakan gateway internet khusus keluar
- Sambungkan ke internet atau jaringan lain menggunakan perangkat NAT

Mengakses jaringan perusahaan atau rumah

Anda dapat secara opsional menghubungkan VPC Anda ke pusat data perusahaan Anda sendiri menggunakan AWS Site-to-Site VPN koneksi IPsec, menjadikan AWS Cloud sebagai ekstensi dari pusat data Anda.

Koneksi Site-to-Site VPN terdiri dari dua terowongan VPN antara gateway pribadi virtual atau gateway transit di AWS samping, dan perangkat gateway pelanggan yang terletak di pusat data Anda. Perangkat gateway pelanggan adalah perangkat fisik atau perangkat lunak yang Anda konfigurasikan di sisi koneksi Site-to-Site VPN Anda.

Pelajari selengkapnya

- AWS Site-to-Site VPN Panduan Pengguna
- Gerbang Transit Amazon VPC

Connect VPC dan jaringan

Anda dapat membuat Koneksi peering VPC antara dua VPC yang memungkinkan Anda merutekan lalu lintas antara kedua VPC secara privat. Instans pada salah satu VPC dapat berkomunikasi satu sama lain seolah-olah kedua VPC ada di jaringan yang sama.

Anda juga dapat membuat transit gateway dan menggunakannya untuk menghubungkan VPC dan jaringan on-premise Anda. Gateway transit bertindak sebagai router virtual regional untuk lalu lintas yang mengalir di antara lampirannya, yang dapat mencakup VPC, koneksi VPN, Direct Connect gateway, dan koneksi peering gateway transit.

Pelajari selengkapnya

- Panduan Peering Amazon VPC
- Gerbang Transit Amazon VPC

AWS jaringan global pribadi

AWS menyediakan jaringan global pribadi berkinerja tinggi dan latensi rendah yang menghadirkan lingkungan komputasi awan yang aman untuk mendukung kebutuhan jaringan Anda. AWS Wilayah terhubung ke beberapa Penyedia Layanan Internet (ISP) serta tulang punggung jaringan global privat, yang memberikan peningkatan performa jaringan untuk lalu lintas lintas Wilayah yang dikirim oleh pelanggan.

Paket yang berasal dari AWS jaringan dengan tujuan di jaringan tetap berada di AWS jaringan AWS global, kecuali lalu lintas ke atau dari Wilayah AWS China dan Wilayah Cloud Berdaulat AWS Eropa. Ini benar apakah tujuannya adalah alamat IP pribadi atau alamat IP publik. Misalnya, jika instance EC2 di dua VPC berkomunikasi menggunakan alamat IP publik, lalu lintas tetap berada di jaringan global pribadi. Tujuan dapat berada di Zona Ketersediaan yang sama, Zona Ketersediaan yang berbeda di Wilayah yang sama, atau Wilayah yang berbeda.

Kehilangan paket jaringan dapat disebabkan oleh sejumlah faktor, termasuk tabrakan aliran jaringan, kesalahan tingkat yang lebih rendah (Lapisan 2), dan kegagalan jaringan lainnya. Kami merekayasa dan mengoperasikan jaringan kami untuk meminimalkan kehilangan paket. Kami mengukur tingkat kerugian paket (PLR) di seluruh tulang punggung global yang menghubungkan Wilayah. AWS Kami mengoperasikan jaringan tulang punggung kami untuk menargetkan p99 dari PLR per jam kurang dari 0,0001%.

Merencanakan VPC Anda

Selesaikan tugas-tugas berikut untuk mempersiapkan membuat dan menghubungkan VPC Anda. Setelah selesai, Anda akan siap untuk menerapkan aplikasi Anda AWS.

Tugas

- Mendaftar untuk Akun AWS
- Memverifikasi izin
- Tentukan rentang alamat IP Anda
- Pilih Zona Ketersediaan Anda
- Rencanakan konektivitas internet Anda
- Buat VPC Anda
- Men-deploy aplikasi Anda

Mendaftar untuk Akun AWS

Mendaftar untuk Akun AWS

Untuk memulainya AWS, Anda membutuhkan Akun AWS. Untuk informasi tentang membuat Akun AWS, lihat Mem ulai dengan an Akun AWS di Panduan AWS Account Management Referensi.

Memverifikasi izin

Sebelum Anda dapat menggunakan Amazon VPC, Anda harus memiliki izin yang diperlukan. Untuk informasi selengkapnya, lihat Identity and access management untuk Amazon VPC dan Contoh kebijakan Amazon VPC.

Tentukan rentang alamat IP Anda

Sumber daya di VPC Anda berkomunikasi satu sama lain dan dengan sumber daya melalui internet menggunakan alamat IP. Saat Anda membuat VPC dan subnet, Anda dapat memilih rentang alamat IP mereka. Saat Anda menyebarkan sumber daya di subnet, seperti instans EC2, sumber daya tersebut menerima alamat IP dari rentang alamat IP subnet. Untuk informasi selengkapnya, lihat Penentuan alamat IP.

Saat Anda memilih ukuran untuk VPC Anda, pertimbangkan berapa banyak alamat IP yang Anda perlukan di seluruh Akun AWS dan VPC Anda. Pastikan bahwa rentang alamat IP untuk VPC Anda tidak tumpang tindih dengan rentang alamat IP untuk jaringan Anda sendiri. Jika Anda memerlukan konektivitas antara beberapa VPC, Anda harus memastikan bahwa mereka tidak memiliki alamat IP yang tumpang tindih.

IP Address Manager (IPAM) memudahkan untuk merencanakan, melacak, dan memantau alamat IP untuk aplikasi Anda. Untuk informasi selengkapnya, lihat Panduan Manajer Alamat IP.

Pilih Zona Ketersediaan Anda

Wil AWS ayah adalah lokasi fisik tempat kami mengelompokkan pusat data, yang dikenal sebagai Zona Ketersediaan. Setiap Zona Ketersediaan memiliki daya, pendinginan, dan keamanan fisik independen, dengan daya redundan, jaringan, dan konektivitas. Zona Ketersediaan di suatu Wilayah secara fisik dipisahkan oleh jarak yang berarti, dan saling berhubungan melalui jaringan bandwidth tinggi, latensi rendah. Anda dapat merancang aplikasi Anda untuk berjalan di beberapa Availability Zone untuk mencapai toleransi kesalahan yang lebih besar.

Lingkungan produksi

Untuk lingkungan produksi, sebaiknya pilih setidaknya dua Zona Ketersediaan dan menyebarkan AWS sumber daya secara merata di setiap Zona Ketersediaan aktif.

Lingkungan pengembangan atau pengujian

Untuk lingkungan pengembangan atau pengujian, Anda dapat memilih untuk menghemat uang dengan menerapkan sumber daya Anda hanya di satu Zona Ketersediaan.

Rencanakan konektivitas internet Anda

Rencanakan untuk membagi setiap VPC menjadi subnet berdasarkan persyaratan konektivitas Anda. Contoh:

- Jika Anda memiliki server web yang akan menerima lalu lintas dari klien di internet, buat subnet untuk server ini di setiap Zona Ketersediaan.
- Jika Anda juga memiliki server yang hanya akan menerima lalu lintas dari server lain di VPC, buat subnet terpisah untuk server ini di setiap Zona Ketersediaan.
- Jika Anda memiliki server yang akan menerima lalu lintas hanya melalui koneksi VPN ke jaringan Anda, buat subnet terpisah untuk server ini di setiap Zona Ketersediaan.

Jika aplikasi Anda akan menerima lalu lintas dari internet, VPC harus memiliki gateway internet. Melampirkan gateway internet ke VPC tidak secara otomatis membuat instans Anda dapat diakses dari internet. Selain melampirkan gateway internet, Anda harus memperbarui tabel rute subnet dengan rute ke gateway internet. Anda juga harus memastikan bahwa instance memiliki alamat IP publik dan grup keamanan terkait yang memungkinkan lalu lintas dari internet melalui port dan protokol tertentu yang diperlukan oleh aplikasi Anda.

Atau, daftarkan instans Anda dengan penyeimbang beban yang menghadap ke internet. Penyeimbang beban menerima lalu lintas dari klien dan mendistribusikannya di seluruh instans terdaftar di satu atau beberapa Zona Ketersediaan. Untuk informasi selengkapnya, lihat Elastic Load Balancing. Untuk mengizinkan instans di subnet pribadi mengakses internet (misalnya, untuk mengunduh pembaruan) tanpa mengizinkan koneksi masuk yang tidak diminta dari internet, tambahkan gateway NAT publik di setiap Zona Ketersediaan aktif dan perbarui tabel rute untuk mengirim lalu lintas internet ke gateway NAT. Untuk informasi selengkapnya, lihat the section called “Mengakses internet dari subnet privat”.

Buat VPC Anda

Setelah Anda menentukan jumlah VPC dan subnet yang Anda butuhkan, blok CIDR apa yang akan ditetapkan ke VPC dan subnet Anda, dan cara menghubungkan VPC Anda ke internet, Anda siap untuk membuat VPC Anda. Jika Anda membuat VPC menggunakan Konsol Manajemen AWS dan menyertakan subnet publik dalam konfigurasi Anda, kami membuat tabel rute untuk subnet dan menambahkan rute yang diperlukan untuk akses langsung ke internet. Untuk informasi selengkapnya, lihat the section called “Buat VPC”.

Men-deploy aplikasi Anda

Setelah membuat VPC, Anda dapat menerapkan aplikasi Anda.

Lingkungan produksi

Untuk lingkungan produksi, Anda dapat menggunakan salah satu layanan berikut untuk menyebarkan server di beberapa Zona Ketersediaan, untuk mengonfigurasi penskalaan sehingga Anda mempertahankan jumlah minimum server yang diperlukan oleh aplikasi Anda, dan untuk mendaftarkan server Anda dengan penyeimbang beban untuk mendistribusikan lalu lintas secara merata di seluruh server Anda.

- Amazon EC2 Auto Scaling

- Armada EC2
- Amazon Elastic Container Service (Amazon ECS)

Lingkungan pengembangan atau pengujian

Untuk lingkungan pengembangan atau pengujian, Anda dapat memilih untuk meluncurkan satu instans EC2. Untuk informasi selengkapnya, lihat Mem ulai dengan Amazon EC2 di Panduan Pengguna Amazon EC2.

Pengalamatan IP untuk VPC dan subnet Anda

Penentuan alamat IP memungkinkan sumber daya dalam VPC Anda berkomunikasi satu sama lain, dan dengan sumber daya melalui internet.

Notasi Classless Inter-Domain Routing (CIDR) adalah cara untuk mewakili alamat IP dan masker jaringannya. Format alamat ini adalah sebagai berikut:

- Alamat IPv4 individu adalah 32 bit, dengan 4 kelompok hingga 3 digit desimal, 0-255. Misalnya, 10.0.1.0.
- Blok IPv4 CIDR memiliki alamat IPv4 diikuti oleh garis miring dan angka dari 0 hingga 32. Misalnya, 10.0.0. 0/16 mewakili 65.536 alamat IPv4 dari 10.0.0.0 hingga 10.0.255.255.
- Alamat IPv6 individu adalah 128 bit, dengan 8 segmen dari 4 digit heksadesimal. Misalnya, 2001:0 db 8:85 a 3:0000:0000:8 a2e: 0370:7334. Tidak perlu memasukkan nol terdepan dalam segmen. Anda juga dapat mengganti segmen all-zero berturut-turut dengan titik dua (::) satu kali dalam sebuah alamat. Oleh karena itu, alamat contoh dapat dikompresi sebagai 2001:db 8:85 a3: :8a2e: 370:7334.
- Blok IPv6 CIDR memiliki alamat IPv6 yang diakhiri dengan segmen all-zero, dengan segmen all-zero diganti dengan titik dua, diikuti oleh garis miring dan angka dari 0 hingga 128. Misalnya, 2001:db 8:1234:1 a00: :/56 mewakili 2^72 alamat IPv6 dari 2001:db 8:1234:1 a 00:0000:0000:0000:0000 hingga 2001:db 8:1234:1 aff:ffff:ffff:ffff:ffff:ffff: ffff.

Untuk informasi lebih lanjut, lihat Apa itu CIDR?

Daftar Isi

- Alamat IPv4 privat
- Alamat IPv4 publik
- Alamat IPv6
- Gunakan Alamat IP Anda sendiri
- Gunakan Manajer Alamat IP Amazon VPC
- Blok VPC CIDR
- Blok subnet CIDR
- Bandingkan IPv4 dan IPv6
- Mengkonsolidasikan dan mengelola blok CIDR jaringan dengan daftar awalan terkelola

- AWS Rentang alamat IP
- Dukungan IPv6 untuk VPC Anda
- AWS Layanan yang mendukung IPv6

Alamat IPv4 privat

Alamat IPv4 privat (juga disebut sebagai Alamat IP privat dalam topik ini) tidak dapat dijangkau melalui internet, dan dapat digunakan untuk komunikasi antar instans di VPC Anda. Saat Anda meluncurkan instance ke VPC, alamat IP pribadi utama dari rentang alamat IPv4 subnet ditetapkan ke antarmuka jaringan utama (misalnya, eth0) instans. Setiap instans juga diberikan nama host DNS privat (internal) yang berubah ke alamat IP privat instans. Nama host dapat terdiri dari dua jenis: berbasis sumber daya atau. IP-based Untuk informasi selengkapnya, lihat penamaan instans EC2. Jika Anda tidak menentukan alamat IP privat primer, kami akan memilih alamat IP yang tersedia di rentang subnet untuk Anda. Untuk informasi selengkapnya tentang antarmuka jaringan, lihat Antarmuka Jaringan Elastis di Panduan Pengguna Amazon EC2.

Anda dapat menetapkan alamat IP privat tambahan, yang dikenal sebagai alamat IP privat sekunder, untuk contoh yang berjalan di VPC. Tidak seperti alamat IP privat primer, Anda dapat menetapkan ulang alamat IP Privat sekunder dari satu jaringan ke jaringan lainnya. Alamat IP privat tetap terkait dengan antarmuka jaringan saat instans dihentikan dan dimulai, dan dilepas saat instans dihentikan. Untuk informasi selengkapnya tentang alamat IP primer dan sekunder, lihat Beberapa Alamat IP di Panduan Pengguna Amazon EC2.

Kami merujuk ke alamat IP privat sebagai alamat IP yang berada dalam rentang CIDR IPv4 VPC. Sebagian besar rentang alamat IP VPC jatuh dalam rentang alamat IP privat (yang tidak dapat dirutekan secara publik) yang ditentukan di RFC 1918; namun, Anda dapat menggunakan blok CIDR publik untuk VPC Anda. Terlepas dari rentang alamat IP VPC Anda, kami tidak mendukung akses langsung ke internet dari blok CIDR VPC Anda, termasuk blok CIDR yang dapat dirutekan secara publik. Anda harus mengatur akses internet melalui gateway; misalnya, gateway internet, gateway pribadi virtual, AWS Site-to-Site VPN koneksi, atau Direct Connect.

Kami tidak pernah mengiklankan rentang alamat IPv4 dari subnet ke internet.

Alamat IPv4 publik

Semua subnet memiliki atribut yang menentukan apakah antarmuka jaringan yang dibuat di subnet secara otomatis menerima alamat IPv4 publik (juga disebut sebagai alamat IP publik dalam topik ini).

Oleh karena itu, saat Anda meluncurkan instance ke subnet yang mengaktifkan atribut ini, alamat IP publik ditetapkan ke antarmuka jaringan utama yang dibuat untuk instance tersebut. Alamat IP publik dipetakan ke alamat IP privat primer melalui terjemahan alamat jaringan (NAT).

> **Note**
>
> AWS biaya untuk semua alamat IPv4 publik, termasuk alamat IPv4 publik yang terkait dengan instans yang sedang berjalan dan alamat IP Elastic. Untuk informasi selengkapnya, lihat tab Alamat IPv4 Publik di halaman harga Amazon VPC.

Anda dapat mengontrol apakah instans Anda menerima alamat IP publik dengan melakukan tindakan berikut:

- Memodifikasi atribut pengalamatan IP publik dari subnet Anda. Untuk informasi selengkapnya, lihat Ubah atribut pengalamatan IP subnet Anda.
- Mengaktifkan atau menonaktifkan fitur pengalamatan IP publik selama peluncuran instans, yang menggantikan atribut pengalamatan IP publik subnet.
- Anda dapat membatalkan penetapan alamat IP publik dari instance setelah diluncurkan dengan mengelola alamat IP yang terkait dengan antarmuka jaringan. Untuk informasi selengkapnya, lihat Mengelola alamat IP di Panduan Pengguna Amazon EC2.

Alamat IP publik ditetapkan dari kolam alamat IP publik Amazon, dan tidak dikaitkan dengan akun Anda. Ketika alamat IP publik tidak dikaitkan dengan instans Anda, alamat IP tersebut dilepas kembali ke kolam, dan tidak lagi tersedia untuk Anda gunakan. Dalam kasus tertentu, kami merilis alamat IP publik dari instans Anda, atau menetapkannya ke yang baru. Untuk informasi selengkapnya, lihat Alamat IP Pu blik di Panduan Pengguna Amazon EC2.

Jika Anda memerlukan alamat IP publik yang persisten yang dialokasikan ke akun Anda dan yang dapat ditetapkan ke dan dilepaskan dari instans sesuai kebutuhan, gunakan alamat IP Elastis. Untuk informasi selengkapnya, lihat Mengaitkan alamat IP Elastic dengan sumber daya di VPC Anda.

Jika VPC Anda diaktifkan untuk mendukung nama host DNS, setiap instans yang menerima alamat IP publik atau alamat IP Elastis juga diberikan nama host DNS publik. Kami mengubah nama host DNS publik menjadi alamat IP publik instans di luar jaringan instans, dan untuk alamat IP privat instans dari dalam jaringan instans. Untuk informasi selengkapnya, lihat Atribut DNS untuk VPC Anda.

Jika Anda menggunakan Amazon VPC IP Address Manager (IPAM), Anda bisa mendapatkan blok alamat IPv4 publik yang berdekatan dari AWS dan menggunakannya untuk mengalokasikan alamat IP Elastic berurutan ke sumber daya. AWS Menggunakan blok alamat IPv4 yang berdekatan dapat secara signifikan mengurangi overhead manajemen untuk daftar kontrol akses keamanan dan menyederhanakan alokasi dan pelacakan alamat IP untuk penskalaan perusahaan. AWS Untuk informasi selengkapnya, lihat Meng alokasikan alamat IP Elastis berurutan dari kumpulan IPAM di Panduan Pengguna IPAM Amazon VPC.

Alamat IPv6

Ketika internet terus berkembang, begitu pula kebutuhan akan alamat IP. Format yang paling umum untuk alamat IP adalah IPv4. Format baru untuk alamat IP adalah IPv6, yang menyediakan ruang alamat yang lebih besar daripada IPv4. IPv6 menyelesaikan masalah kehabisan alamat IPv4 dan memungkinkan Anda untuk menghubungkan lebih banyak perangkat ke internet. Transisi berlangsung bertahap, tetapi seiring bertambahnya adopsi IPv6, Anda dapat menyederhanakan jaringan Anda dan memanfaatkan kemampuan canggih IPv6 untuk konektivitas, kinerja, dan keamanan yang lebih baik.

Banyak AWS layanan, seperti Amazon EC2, Amazon S3, dan Amazon CloudFront, menawarkan dual-stack (IPv4 dan IPv6) atau IPv6-only dukungan, memungkinkan sumber daya ditetapkan alamat IPv6 dan diakses melalui protokol IPv6. Ini menyederhanakan konfigurasi jaringan dan manajemen untuk pelanggan yang mengadopsi IPv6.

Layanan lain menawarkan dual-stack dan IPv6-only dukungan terbatas atau sebagian.

Untuk informasi selengkapnya tentang layanan yang mendukung IPv6, lihatAWS Layanan yang mendukung IPv6.

Perhatikan bahwa beberapa alamat IPv6 dicadangkan oleh Gugus Tugas Rekayasa Internet. Untuk informasi selengkapnya tentang rentang alamat IPv6 yang dicadangkan, lihat Registri Alamat IPv6 I ANA dan Special-Purpose RFC4291.

> **Note**
>
> Pengalamatan IPv6 publik dan pribadi tersedia di AWS. AWS mendefinisikan alamat IP publik sebagai yang diiklankan di internet dari AWS, sementara alamat IP pribadi tidak dan tidak dapat diiklankan di internet dari AWS.

Daftar Isi

- Alamat IPv6 publik
- Alamat IPv6 pribadi

Alamat IPv6 publik

Amazon-provided Alamat IPv6 selalu diiklankan di internet. Mereka unik secara global, dan karenanya dapat dijangkau melalui internet. Anda dapat mengontrol apakah sumber daya seperti instans EC2 dapat dijangkau menggunakan alamat IPv6-nya dengan mengontrol routing untuk subnet Anda, atau dengan menggunakan grup keamanan dan ACL jaringan.

Berikut adalah beberapa cara yang dapat Anda persiapkan untuk menggunakan alamat IPv6 publik untuk beban kerja Anda:

- Buat IPAM dengan Amazon VPC IP Address Manager dan sediakan rentang alamat IPv6 Amazon-owned publik ke kumpulan alamat IPAM. Untuk informasi selengkapnya, lihat Membuat kumpulan IPv6 di Panduan Pengguna IPAM Amazon VPC.
- Jika Anda memiliki IPAM dan Anda memiliki rentang alamat IPv6 publik, bawa beberapa atau semua rentang alamat IPv6 publik ke IPAM dan sediakan rentang alamat IPv6 publik ke kumpulan alamat IPAM. Untuk informasi selengkapnya, lihat Tutorial: Membawa alamat IP Anda ke IPAM di Panduan Pengguna IPAM Amazon VPC.
- Jika Anda tidak memiliki IPAM tetapi Anda memiliki rentang alamat IPv6 publik, bawa beberapa atau semua rentang alamat IPv6 publik ke. AWS Untuk informasi selengkapnya, lihat Membawa alamat IP Anda sendiri (BYOIP) ke Amazon EC2 di Panduan Pengguna Amazon EC2.

Ketika Anda siap untuk menggunakan alamat IPv6 publik, Anda dapat menetapkan alamat IPv6 publik ke instans (lihat alamat IPv6 di Panduan Pengguna Amazon EC2), Anda dapat mengalokasikan blok IPv6 CIDR publik ke VPC Anda (lihatTambahkan atau hapus blok CIDR dari VPC Anda) dan mengaitkan blok IPv6 CIDR dengan subnet Anda (lihat). Ubah atribut pengalamatan IP subnet Anda

Alamat IPv6 pribadi

Alamat IPv6 pribadi adalah alamat IPv6 yang tidak diiklankan dan tidak dapat diiklankan di Internet dari. AWS

Anda dapat menggunakan alamat IPv6 pribadi jika Anda ingin jaringan pribadi Anda mendukung IPv6 dan Anda tidak memiliki niat untuk merutekan lalu lintas dari alamat ini ke Internet. Jika Anda ingin terhubung ke internet dari sumber daya yang memiliki alamat IPv6 pribadi, Anda bisa, tetapi Anda harus merutekan lalu lintas melalui sumber daya di subnet lain dengan alamat IPv6 publik untuk melakukannya.

Ada dua jenis alamat IPv6 pribadi:

- Rentang ULA IPv6: Alamat IPv6 seperti yang didefinisikan dalam RFC4193. Rentang alamat ini selalu dimulai dengan “fc” atau “fd”, yang membuatnya mudah diidentifikasi. Ruang ULA IPv6 yang valid adalah apa pun di bawah fd00: :/8 yang tidak tumpang tindih dengan rentang cadangan Amazon fd00: :/16.
- Rentang GUA IPv6: Alamat IPv6 seperti yang didefinisikan dalam RFC3587. Opsi untuk menggunakan rentang GUA IPv6 sebagai alamat IPv6 pribadi dinonaktifkan secara default dan harus diaktifkan sebelum Anda dapat menggunakannya. Untuk informasi selengkapnya, lihat Meng aktifkan penyediaan CIDR GUA IPv6 pribadi di Panduan Pengguna IPAM Amazon VPC.

Perhatikan hal-hal berikut:

- Alamat IPv6 pribadi hanya tersedia melalui Amazon VPC IP Address Manager (IPAM). IPAM menemukan sumber daya dengan alamat IPv6 ULA dan GUA dan memantau kumpulan untuk tumpang tindih IPv6 ULA dan ruang alamat GUA.
- Saat Anda menggunakan rentang GUA IPv6 pribadi, kami mengharuskan Anda menggunakan rentang GUA IPv6 milik Anda.
- Alamat IPv6 pribadi tidak dan tidak dapat diiklankan di internet oleh AWS. AWS tidak mengizinkan keluar langsung ke internet publik dari rentang IPv6 pribadi bahkan jika ada gateway internet atau gateway internet hanya keluar di VPC. Alamat IPv6 pribadi secara otomatis dihapus di tepi gateway internet memastikan bahwa alamat tersebut tidak dirutekan secara publik.
- AWS menyimpan 4 alamat IPv6 pribadi subnet pertama dan yang terakhir.
- Rentang yang valid untuk ULA IPv6 pribadi adalah /9 hingga/60 dimulai dengan fd80: :/9.
- Jika Anda memiliki rentang GUA IPv6 pribadi yang dialokasikan ke VPC, Anda tidak dapat menggunakan ruang GUA IPv6 publik yang tumpang tindih dengan ruang GUA IPv6 pribadi di VPC yang sama.
- Komunikasi antara sumber daya dengan IPv6 ULA pribadi dan rentang alamat GUA didukung (seperti melalui Direct Connect, VPC peering, gateway transit, atau koneksi VPN).

- Anda dapat menggunakan alamat IPv6 pribadi dengan IPv6-only dan subnet VPC dual-stack, penyeimbang beban elastis, dan titik akhir. AWS Global Accelerator
- Tidak ada biaya untuk alamat IPv6 pribadi.

Berikut adalah beberapa cara yang dapat Anda persiapkan untuk menggunakan alamat IPv6 pribadi untuk beban kerja Anda:

- Buat IPAM dengan Amazon VPC IP Address Manager dan sediakan rent ang ULA IPv6 pribadi ke kumpulan alamat IPAM. Untuk informasi selengkapnya, lihat Membuat kumpulan IPv6 di Panduan Pengguna IPAM Amazon VPC.
- Buat IPAM dengan Amazon VPC IP Address Manager dan sediakan rentang GUA IPv6 pribadi ke kumpulan alamat IPAM. Opsi untuk menggunakan rentang GUA IPv6 sebagai alamat IPv6 pribadi dinonaktifkan secara default dan harus diaktifkan pada IPAM Anda sebelum Anda dapat menggunakannya. Untuk informasi selengkapnya, lihat Meng aktifkan penyediaan CIDR GUA IPv6 pribadi di Panduan Pengguna IPAM Amazon VPC.

Ketika Anda siap untuk menggunakan alamat IPv6 pribadi, Anda dapat mengalokasikan blok CIDR IPv6 pribadi dari kumpulan IPAM ke VPC Anda (lihatTambahkan atau hapus blok CIDR dari VPC Anda) dan mengaitkan blok IPv6 CIDR dengan subnet Anda (lihat). Ubah atribut pengalamatan IP subnet Anda

Gunakan Alamat IP Anda sendiri

Anda dapat membawa sebagian atau seluruh rentang alamat IPv4 publik Anda sendiri atau rentang alamat IPv6 ke akun Anda AWS . Anda tetap memiliki baris alamat sendiri, tetapi AWS mengiklankannya di internet secara default. Setelah Anda membawa rentang alamat ke AWS, itu muncul di akun Anda sebagai kumpulan alamat. Anda dapat membuat alamat IP Elastis dari kumpulan alamat IPv4 Anda, dan Anda dapat mengaitkan blok CIDR IPv6 dari kumpulan alamat IPv6 Anda dengan VPC.

Untuk informasi selengkapnya, lihat Membawa alamat IP Anda sendiri (BYOIP) di Panduan Pengguna Amazon EC2.

Gunakan Manajer Alamat IP Amazon VPC

Amazon VPC IP Address Manager (IPAM) adalah fitur VPC yang memudahkan Anda merencanakan, melacak, dan memantau alamat IP untuk beban kerja Anda. AWS Anda dapat menggunakan IPAM untuk mengalokasikan CIDR alamat IP ke VPC menggunakan aturan bisnis tertentu.

Untuk informasi selengkapnya, lihat Apa itu IPAM? dalam Panduan Pengguna Amazon VPC IPAM.

Blok VPC CIDR

Alamat IP untuk cloud pribadi virtual Anda (VPC) diwakili menggunakan notasi Classless Inter-Domain Routing (CIDR). VPC harus memiliki blok IPv4 CIDR terkait. Anda dapat secara opsional mengaitkan blok IPv4 CIDR tambahan dan satu atau lebih blok IPv6 CIDR. Untuk informasi selengkapnya, lihat Pengalamatan IP untuk VPC dan subnet Anda.

Daftar Isi

- Blok IPv4 VPC CIDR
- Mengelola blok CIDR IPv4 untuk VPC
- Pembatasan pengaitan blok CIDR IPv4
- Blok IPv6 VPC CIDR

Blok IPv4 VPC CIDR

Saat Anda membuat VPC, Anda harus menentukan blok CIDR IPv4 untuk VPC. Ukuran blok yang diizinkan adalah antara netmask /16 (alamat IP 65,536) dan netmask /28 (alamat IP 16). Setelah Anda membuat VPC, Anda dapat mengaitkan blok CIDR IPv4 tambahan dengan VPC. Untuk informasi selengkapnya, lihat Tambahkan atau hapus blok CIDR dari VPC Anda.

Saat Anda membuat VPC, sebaiknya tentukan blok CIDR dari rentang alamat IPv4 pribadi seperti yang ditentukan dalam RFC 1918.

Rentang RFC 1918	Contoh Blok CIDR
10.0.0.0 - 10.255.255.255 (awalan) 10/8	10.0.0. 0/16
172.16.0.0 - 172.31.255.255 (172. 16/12 awalan)	172.31.0. 0/16

Rentang RFC 1918	Contoh Blok CIDR
192.168.0.0 - 192.168.255.255 (192. 168/16 awalan)	192.168.0. 0/20

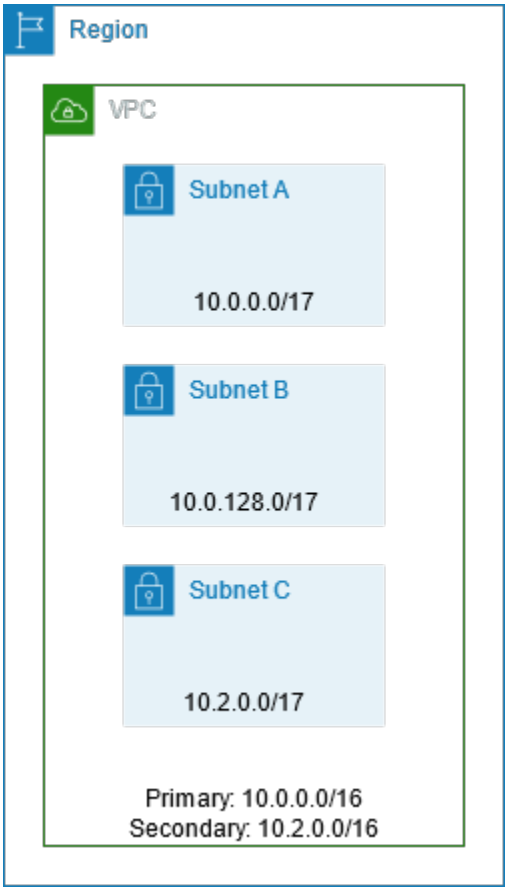
Pertimbangan-pertimbangan

- Anda tidak dapat menentukan blok CIDR berikut untuk VPC Anda:
  - 0.0.0. 0/8
  - 127.0.0. 0/8 (rentang alamat loopback host internal)
  - 169.254.0. 0/16 (rentang alamat link-lokal)
  - 224.0.0. 0/4 (rentang alamat multicast)
- Saat Anda membuat VPC untuk digunakan dengan AWS layanan, periksa dokumentasi layanan untuk memverifikasi apakah ada persyaratan khusus untuk konfigurasinya.
- Beberapa AWS layanan menggunakan kisaran `172.17.0.0/16` CIDR. Layanan dapat mengalami konflik alamat IP jika rentang alamat IP sudah digunakan di jaringan Anda. Misalnya, AWS Cloud9 dan penggunaan SageMaker AI Amazon`172.17.0.0/16`. Untuk menghindari konflik, jangan gunakan rentang ini saat membuat VPC Anda. Untuk informasi selengkapnya, lihat Tidak dapat terhubung ke lingkungan EC2 karena alamat IP VPC digunakan oleh Docker di Panduan Pengguna. AWS Cloud9
- Anda dapat membuat VPC dengan blok CIDR yang dapat dirutekan secara publik yang berada di luar rentang alamat IPv4 prvat yang ditentukan dalam RFC 1918. Namun, untuk tujuan dokumentasi ini, kami menyebut alamat IP pribadi sebagai alamat IPv4 yang berada dalam kisaran CIDR VPC Anda.
- Jika Anda membuat VPC menggunakan alat baris perintah atau Amazon EC2 API, blok CIDR secara otomatis dimodifikasi ke bentuk kanoniknya. Misalnya, jika Anda menentukan 100.68.0. 18/18 untuk blok CIDR, kami membuat blok CIDR 100.68.0. 0/18.

Mengelola blok CIDR IPv4 untuk VPC

Anda dapat mengaitkan blok CIDR IPv4 sekunder dengan VPC Anda. Ketika Anda mengaitkan blok CIDR dengan VPC Anda, rute secara otomatis ditambahkan ke tabel rute VPC Anda untuk mengaktifkan perutean di dalam VPC (tujuannya adalah blok CIDR dan target adalah `local`).

Dalam contoh berikut, VPC memiliki blok CIDR primer dan sekunder. Blok CIDR untuk Subnet A dan Subnet B berasal dari blok VPC CIDR utama. Blok CIDR untuk Subnet C berasal dari blok VPC CIDR sekunder.



Tabel rute berikut menunjukkan rute lokal untuk VPC.

Tujuan	Target
10.0.0. 0/16	Lokal:
10.2.0. 0/16	Lokal:

Untuk menambahkan blok CIDR ke VPC Anda, aturan berikut berlaku:

- Ukuran blok yang diperbolehkan adalah antara netmask `/28` dan netmask `/16`.
- Blok CIDR tidak boleh tumpang tindih dengan blok CIDR yang ada yang sudah dikaitkan dengan VPC.

- Ada pembatasan pada rentang alamat IPv4 yang dapat Anda gunakan. Untuk informasi selengkapnya, lihat Pembatasan pengaitan blok CIDR IPv4.
- Anda tidak dapat menambah atau mengurangi ukuran blok CIDR yang ada.
- Anda memiliki kuota pada jumlah blok CIDR yang dapat Anda kaitkan dengan VPC dan pada jumlah rute yang dapat Anda tambahkan ke tabel rute. Anda tidak dapat mengaitkan blok CIDR jika hal ini membuat Anda melebihi kuota Anda. Untuk informasi selengkapnya, lihat Kuota Amazon VPC.
- Blok CIDR tidak boleh sama besar atau lebih besar dari kisaran CIDR tujuan di sebuah rute di salah satu tabel rute VPC. Sebagai contoh, dalam sebuah VPC dimana blok CIDR utama adalah `10.2.0.0/16`, Anda memiliki rute yang ada dalam tabel rute dengan tujuan `10.0.0.0/24` ke virtual private gateway. Anda ingin mengaitkan blok CIDR sekunder di rentang `10.0.0.0/16`. Karena rute yang ada, Anda tidak dapat mengaitkan blok CIDR `10.0.0.0/24` atau yang lebih besar. Namun, Anda dapat mengaitkan blok CIDR sekunder `10.0.0.0/25` atau yang lebih kecil.
- Aturan berikut berlaku saat Anda menambahkan blok CIDR IPv4 ke VPC yang merupakan bagian dari koneksi peering VPC:
  - Jika koneksi peering VPC `active`, Anda dapat menambahkan blok CIDR ke VPC asalkan blok-blok tersebut tidak tumpang tindih dengan blok CIDR dari VPC rekan.
  - Jika koneksi peering VPC adalah `pending-acceptance`, pemilik peminta VPC tidak dapat menambahkan blok CIDR ke VPC, terlepas apakah blok tumpang tindih dengan blok CIDR dari VPC penerima. Baik pemilik VPC penerima harus menerima koneksi peering, atau pemilik VPC peminta harus menghapus permintaan koneksi peering VPC, menambahkan blok CIDR, dan kemudian meminta koneksi peering VPC.
  - Jika koneksi peering VPC adalah `pending-acceptance`, pemilik VPC penerimsa dapat menambahkan blok CIDR ke VPC. Jika blok CIDR sekunder tumpang tindih dengan blok CIDR dari VPC peminta, permintaan koneksi peering VPC mengintip menjadi gagal dan tidak dapat diterima.
- Jika Anda menggunakan Direct Connect untuk terhubung ke beberapa VPC melalui gateway Direct Connect, VPC yang terkait dengan gateway Direct Connect tidak boleh memiliki blok CIDR yang tumpang tindih. Jika Anda menambahkan blok CIDR ke VPC yang dikaitkan dengan gateway Direct Connect, pastikan bahwa blok CIDR yang baru tidak tumpang tindih dengan blok CIDR yang sudah ada dari VPC manapun yang dikaitkan lainnya. Untuk informasi selengkapnya, lihat Gateway Direct Connect di Panduan Pengguna Direct Connect .
- Bila Anda menambahkan atau menghapus blok CIDR, blok bisa saja berstatus: `associating` | `associated` | `disassociating` | `disassociated` | `failing` | `failed`. Blok CIDR siap digunakan saat berada dalam status `associated`.

Anda dapat memutus pengaitan blok CIDR yang Anda telah dikaitkan dengan VPC Anda; namun, Anda tidak dapat memutus pengaitan blok CIDR yang VPC-nya Anda buat di awal (blok CIDR utama). Untuk melihat CIDR utama untuk VPC Anda di konsol Amazon VPC, pilih VPC Anda, pilih kotak centang untuk VPC Anda, dan pilih tab CIDRs. Untuk melihat CIDR utama menggunakan AWS CLI, gunakan perintah describe-vpcs sebagai berikut. CIDR utama dikembalikan di tingkat atas. `CidrBlock element`

```
aws ec2 describe-vpcs --vpc-id vpc-1a2b3c4d --query Vpcs[*].CidrBlock --output text
```

Berikut ini adalah output contoh.

```
10.0.0.0/16
```

Pembatasan pengaitan blok CIDR IPv4

Tabel berikut memberikan ikhtisar asosiasi blok VPC CIDR yang diizinkan dan dibatasi untuk blok VPC CIDR yang ada. Alasan pembatasan adalah bahwa beberapa AWS layanan menggunakan fitur cross-VPC dan lintas akun yang memerlukan blok CIDR yang tidak bertentangan di sisi layanan. AWS

Rentang alamat IPv4 yang ada	Asosiasi terbatas	Asosiasi yang diizinkan
10.0.0. 0/8	Blok CIDR dari rentang RFC 1918* lainnya (172.16.0. 0/12 dan 192.168.0. 0/16). Jika salah satu blok CIDR yang terkait dengan VPC berasal dari 10.0.0. 0/15 rentang (10.0.0.0 hingga 10.1.255.255), Anda tidak dapat menambahkan blok CIDR dari 10.0.0. 0/16 rentang (10.0.0.0 hingga 10.0.255.255). Blok CIDR dari 198.19.0. 0/16 jangkauan.	Blok CIDR lainnya dari 10.0.0. 0/8 kisaran antara netmask /16 dan netmask /28 yang tidak dibatasi. Setiap blok CIDR IPv4 yang dapat dirutekan secara publik (non-RFC 1918) antara netmask /16 dan netmask /28 atau blok CIDR antara netmask /16 dan netmask /28 dari 100.64.0. 0/10 jangkauan.

Rentang alamat IPv4 yang ada	Asosiasi terbatas	Asosiasi yang diizinkan
169.254.0. 0/16	Blok CIDR dari blok “link local” dicadangkan seperti yang dijelaskan dalam RFC 5735 dan tidak dapat ditetapkan ke VPC.	
172.16.0. 0/12	Blok CIDR dari rentang RFC 1918* lainnya (10.0.0. 0/8 dan 192.168.0. 0/16). Blok CIDR dari 172.31.0. 0/16 jangkauan. Blok CIDR dari 198.19.0. 0/16 jangkauan.	Blok CIDR lainnya dari 172.16.0. 0/12 kisaran antara netmask /16 dan netmask /28 yang tidak dibatasi. Setiap blok CIDR IPv4 yang dapat dirutekan secara publik (non-RFC 1918) antara netmask /16 dan netmask /28 atau blok CIDR antara netmask /16 dan netmask /28 dari 100.64.0. 0/10 jangkauan.
192.168.0. 0/16	Blok CIDR dari rentang RFC 1918* lainnya (10.0.0. 0/8 dan 172.16.0. 0/12). Blok CIDR dari 198.19.0. 0/16 jangkauan.	Blok CIDR lainnya dari 192.168.0. 0/16 berkisar antara netmask /16 dan netmask /28. Setiap blok CIDR IPv4 yang dapat dirutekan secara publik (non-RFC 1918) antara netmask /16 dan/28 netmask atau blok CIDR dari 100.64.0. 0/10 berkisar antara netmask /16 dan netmask /28.
198.19.0. 0/16	Blok CIDR dari RFC 1918 rentang*.	Setiap blok CIDR IPv4 yang dapat dirutekan secara publik (non-RFC 1918) antara netmask /16 dan/28 netmask atau blok CIDR dari 100.64.0. 0/10 berkisar antara netmask /16 dan netmask /28.

Rentang alamat IPv4 yang ada	Asosiasi terbatas	Asosiasi yang diizinkan
Blok CIDR yang dapat dirutekan secara publik (non-RFC 1918), atau blok CIDR dari 100.64.0. 0/10jangkauan	Blok CIDR dari RFC 1918 rentang*. Blok CIDR dari 198.19.0. 0/16 jangkauan.	Blok CIDR IPv4 lainnya yang dapat dirutekan publik (non-RFC 1918) antara netmask /16 dan netmask /28 atau blok CIDR antara netmask /16 dan netmask /28 dari 100.64.0. 0/10 jangkauan. Anda juga dapat mengaitkan CIDR di salah satu rentang RFC 1918, tetapi untuk melakukan ini Anda harus menambahkan CIDR itu terlebih dahulu ketika Anda membuat VPC dan kemudian menambahkan CIDR non-RFC 1918.

* Rentang RFC 1918 adalah rentang alamat IPv4 pribadi yang ditentukan dalam RFC 1918.

Blok IPv6 VPC CIDR

Anda dapat mengaitkan satu blok CIDR IPv6 saat membuat VPC baru atau Anda dapat mengaitkan hingga lima blok IPv6 CIDR dari `/44` ke dalam penambahan. `/60` `/4` Anda dapat meminta blok CIDR IPv6 dari kumpulan alamat IPv6 Amazon. Untuk informasi selengkapnya, lihat Tambahkan atau hapus blok CIDR dari VPC Anda.

Jika Anda telah mengaitkan blok IPv6 CIDR dengan VPC Anda, Anda dapat mengaitkan blok IPv6 CIDR dengan subnet yang ada di VPC Anda atau saat Anda membuat subnet baru. Untuk informasi selengkapnya, lihat the section called “Ukuran subnet untuk IPv6”.

Misalnya, Anda membuat VPC dan menentukan bahwa Anda ingin mengaitkan blok Amazon-provided IPv6 CIDR dengan VPC. Amazon menetapkan blok CIDR IPv6 berikut ini untuk VPC Anda: `2001:db8:1234:1a00::/56`. Anda tidak dapat memilih rentang alamat IP tersebut oleh Anda sendiri. Anda dapat membuat sebuah subnet dan mengaitkan blok CIDR IPv6 dari kisaran ini; misalnya, `2001:db8:1234:1a00::/64`.

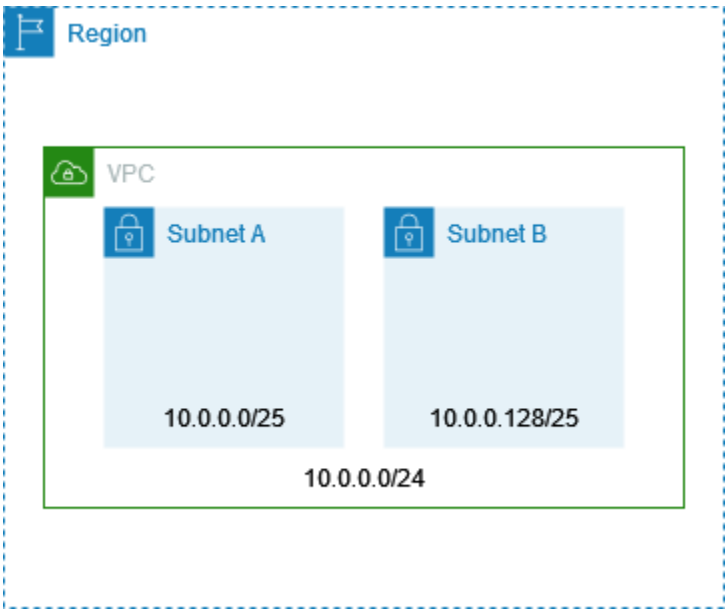
Anda dapat memisahkan blok IPv6 CIDR dari VPC. Setelah Anda memutus pengaitan blok CIDR IPv6 dari sebuah VPC, Anda tidak dapat mengharapkan untuk menerima CIDR yang sama jika Anda mengaitkan blok CIDR IPv6 dengan VPC Anda lagi nanti.

Blok subnet CIDR

Alamat IP untuk subnet Anda diwakili menggunakan notasi Classless Inter-Domain Routing (CIDR). Blok CIDR dari subnet dapat sama dengan blok CIDR untuk VPC (untuk membuat subnet tunggal di VPC), atau subset blok CIDR untuk VPC (untuk membuat beberapa subnet di VPC).

Jika Anda membuat lebih dari satu subnet dalam sebuah VPC, blok-blok CIDR pada subnet-subnet tidak akan tumpang tindih.

Sebagai contoh, jika anda membuat VPC dengan blok CIDR `10.0.0.0/24`, block tersebut men-support 256 alamat IP. Anda dapat memecahkan blok CIDR ini menjadi dua subnet, masing-masing mendukung 128 alamat IP. Satu subnet menggunakan blok CIDR `10.0.0.0/25` (untuk alamat `10.0.0.0` - `10.0.0.127`) dan yang lain menggunakan blok CIDR `10.0.0.128/25` (untuk alamat `10.0.0.128` - `10.0.0.255`).



Ada alat yang tersedia di internet untuk membantu Anda menghitung dan membuat blok CIDR subnet IPv4 dan IPv6. Anda dapat menemukan alat yang sesuai dengan kebutuhan Anda dengan mencari istilah-istilah seperti 'kalkulator subnet' atau 'kalkulator CIDR'. Grup rekayasa jaringan Anda juga dapat membantu Anda menentukan blok CIDR IPv4 dan IPv6 untuk ditentukan untuk subnet Anda.

Ukuran subnet untuk IPv4

Ukuran blok IPv4 CIDR yang diizinkan untuk subnet adalah antara netmask dan /28 netmask. /16 Empat alamat IP pertama dan alamat IP terakhir di setiap blok CIDR subnet tidak tersedia untuk Anda gunakan, dan mereka tidak dapat ditetapkan ke sumber daya, seperti instance EC2. Sebagai contoh, dalam sebuah subnet dengan blok CIDR 10.0.0.0/24, lima alamat IP berikut dicadangkan:

- 10.0.0.0: Alamat jaringan.
- 10.0.0.1: Dicadangkan oleh AWS untuk router VPC.
- 10.0.0.2: Dicadangkan oleh. AWS Alamat IP server DNS adalah basis rentang jaringan VPC plus dua. Untuk VPC dengan beberapa blok CIDR, alamat IP server DNS terletak di CIDR utama. Kami juga mencadangkan basis setiap rentang subnet ditambah dua untuk semua blok CIDR di VPC. Untuk informasi selengkapnya, lihat Server Amazon DNS.
- 10.0.0.3: Dicadangkan AWS untuk penggunaan di masa mendatang.
- 10.0.0.255: Alamat siaran jaringan. Kami tidak men-support siaran di VPC, oleh karena itu kami mencadangkan alamat ini.

Jika Anda membuat subnet menggunakan alat baris perintah atau Amazon EC2 API, blok CIDR secara otomatis dimodifikasi ke bentuk kanonisnya. Misalnya, jika Anda menentukan 100.68.0. 18/18 untuk blok CIDR, kami membuat blok CIDR 100.68.0. 0/18.

Jika Anda membawa rentang alamat IPv4 untuk AWS menggunakan BYOIP, Anda dapat menggunakan semua alamat IP dalam rentang, termasuk alamat pertama (alamat jaringan) dan alamat terakhir (alamat siaran).

Ukuran subnet untuk IPv6

Jika Anda telah mengaitkan blok CIDR IPv6 dengan VPC Anda, Anda dapat mengaitkan blok CIDR IPv6 dengan subnet yang ada di VPC Anda, atau saat Anda membuat subnet baru. Kemungkinan panjang netmask IPv6 berada di antara /44 dan /64 secara bertahap. /4

Ada alat yang tersedia di internet untuk membantu Anda menghitung dan membuat blok CIDR subnet IPv6. Anda dapat menemukan alat yang sesuai dengan kebutuhan Anda dengan mencari istilah seperti 'kalkulator subnet IPv6' atau 'kalkulator IPv6 CIDR'. Grup rekayasa jaringan Anda juga dapat membantu Anda menentukan blok CIDR IPv6 untuk menspesifikasi subnet Anda.

Empat alamat IPv6 pertama dan alamat IPv6 terakhir di setiap blok CIDR subnet tidak tersedia untuk Anda gunakan, dan mereka tidak dapat ditetapkan ke instance EC2. Sebagai contoh, dalam sebuah subnet dengan blok CIDR `2001:db8:1234:1a00/64`, lima alamat IP berikut dicadangkan:

- `2001:db8:1234:1a00::`
- `2001:db8:1234:1a00::1`: Dicadangkan oleh AWS untuk router VPC.
- `2001:db8:1234:1a00::2`
- `2001:db8:1234:1a00::3`
- `2001:db8:1234:1a00:ffff:ffff:ffff:ffff`

Selain alamat IP yang disediakan oleh AWS router VPC dalam contoh di atas, alamat IPv6 berikut dicadangkan untuk router VPC default:

- Alamat IPv6 link-local dalam rentang FE80: :/10 yang dihasilkan menggunakan. EUI-64 Untuk informasi selengkapnya tentang alamat link-local, lihat Link-local alamat.
- Alamat IPv6 link-lokal. `FE80:ec2::1`

Jika Anda perlu berkomunikasi dengan router VPC melalui IPv6, Anda dapat mengonfigurasi aplikasi Anda untuk berkomunikasi dengan alamat mana pun yang paling sesuai dengan kebutuhan Anda.

Bandingkan IPv4 dan IPv6

Tabel berikut merangkum perbedaan antara IPv4 dan IPv6 di Amazon EC2 dan Amazon VPC.

Untuk daftar AWS layanan yang mendukung konfigurasi dual-stack (IPv4 and IPv6) dan konfigurasi IPv6 -only, lihat. Layanan yang mendukung IPv6

Karakteristik	IPv4	IPv6
Ukuran VPC	Hingga 5 CIDRs dari /16 hingga /28. Kuota ini dapat disesuaikan.	Hingga 5 CIDRs dari/44 hingga/60 dengan kelipatan /4. Kuota ini dapat disesuaikan.
Ukuran subnet	Dari /16 hingga /28.	Dari /44 hingga/64 dengan kelipatan /4.

Karakteristik	IPv4	IPv6
Pemilihan alamat	Anda dapat memilih blok IPv4 CIDR untuk VPC Anda atau Anda dapat mengalokasikan blok CIDR dari Amazon VPC IP Address Manager (IPAM). Untuk informasi lebih lanjut, lihat Apa itu IPAM? di Panduan Pengguna Amazon VPC IPAM.	Anda dapat membawa blok IPv6 CIDR Anda sendiri AWS untuk VPC Anda, memilih blok CIDR yang IPv6 disediakan Amazon, atau Anda dapat mengalokasikan blok CIDR dari Amazon VPC IP Address Manager (IPAM). Untuk informasi lebih lanjut, lihat Apa itu IPAM? di Panduan Pengguna Amazon VPC IPAM.
Akses internet	Membutuhkan gateway internet.	Membutuhkan gateway internet. Mendukung komunikasi outbound-only menggunakan gateway internet khusus egres.
Alamat IP elastis	Didukung. Memberikan EC2 contoh IPv4 alamat publik statis permanen.	Tidak didukung. EIPs menjaga IPv4 alamat publik dari sebuah instance statis pada instance restart. IPv6 alamat statis secara default.
Gateway NAT	Didukung. Contoh di subnet pribadi dapat terhubung ke internet menggunakan gateway NAT publik atau ke sumber daya lain VPCs menggunakan gateway NAT pribadi.	Didukung. Anda dapat menggunak an gateway NAT NAT64 untuk mengaktifkan instance di subnet IPv6 -only untuk berkomunikasi dengan sumber daya IPv4 -only di dalam VPCs, di antara, di jaringan lokal VPCs, atau melalui internet.
Nama DNS	Instans menerima nama DNS berbasis IPBN atau RBN yang disediakan Amazon. Nama DNS menyelesaikan catatan DNS yang dipilih untuk instance.	Instance menerima nama DNS berbasis IPBN atau RBN yang disediakan Amazon. Nama DNS menyelesaikan catatan DNS yang dipilih untuk instance.

Mengkonsolidasikan dan mengelola blok CIDR jaringan dengan daftar awalan terkelola

Daftar awalan terkelola adalah sekumpulan satu atau lebih blok CIDR. Anda dapat menggunakan daftar prefiks untuk memudahkan pengkonfigurasian dan pemeliharaan grup keamanan dan tabel rute Anda. Anda dapat membuat daftar prefiks dari alamat penyuratan IP yang sering Anda gunakan, dan menyebutkannya mereka sebagai satu set dalam aturan dan rute grup keamanan bukannya menyebutkannya secara individual. Sebagai contoh, Anda dapat mengkonsolidasikan aturan grup keamanan dengan blok CIDR yang berbeda tetapi port dan protokol yang sama ke aturan tunggal yang menggunakan daftar prefiks. Jika Anda menskalakan jaringan Anda dan harus mengizinkan lalu lintas dari blok CIDR lain, Anda dapat memperbarui daftar prefiks yang relevan dan semua grup keamanan yang menggunakan daftar prefiks harus diperbarui. Anda juga dapat menggunakan daftar awalan terkelola dengan AWS akun lain menggunakan Resource Access Manager (RAM).

Ada dua tipe daftar prefiks:

- Customer-managed daftar awalan — Kumpulan rentang alamat IP yang Anda tentukan dan kelola. Anda dapat membagikan daftar awalan Anda dengan AWS akun lain, memungkinkan akun tersebut untuk mereferensikan daftar awalan di sumber daya mereka sendiri.
- AWS-daftar awalan yang dikelola — Kumpulan rentang alamat IP untuk AWS layanan. Anda tidak dapat membuat, memodifikasi, berbagi, atau menghapus daftar prefiks yang dikelola AWS.

Daftar Isi

- Konsep dan aturan daftar prefiks
- Identity and access management untuk daftar prefiks
- Customer-managed daftar awalan
- AWS Daftar prefiks yang dikelola
- Pengoptimalan AWS manajemen infrastruktur dengan daftar awalan

Konsep dan aturan daftar prefiks

Sebuah daftar prefiks terdiri dari entri. Setiap entri terdiri dari suatu blok CIDR dan, secara opsional, deskripsi untuk blok CIDR tersebut.

Customer-managed daftar awalan

Aturan berikut berlaku untuk daftar prefiks yang dikelola konsumen:

- Daftar prefiks mendukung satu jenis pengalamatan IP saja (IPv4 atau IPv6). Anda tidak dapat menggabungkan blok CIDR IPv4 dan IPv6 dalam satu daftar prefiks.
- Daftar prefiks hanya berlaku untuk Wilayah tempat Anda membuatnya.
- Ketika Anda membuat daftar prefiks, Anda harus menentukan jumlah maksimum entri yang dapat didukung oleh daftar prefiks tersebut.
- Ketika Anda menyebutkan daftar prefiks di suatu sumber daya, jumlah maksimum entri untuk daftar prefiks tersebut dihitung berdasarkan kuota untuk jumlah entri untuk sumber daya tersebut. Sebagai contoh, jika Anda membuat daftar prefiks dengan maksimum 20 entri dan Anda sebutkan daftar prefiks tersebut dalam aturan grup keamanan, ini dianggap sebagai 20 aturan grup keamanan.
- Ketika Anda menyebutkan daftar prefiks dalam tabel rute, maka aturan rute prioritas akan berlaku. Untuk informasi selengkapnya, lihat Prioritas rute untuk daftar prefiks.
- Anda dapat memodifikasi daftar awalan. Saat Anda menambahkan atau menghapus entri, kami membuat versi baru dari daftar awalan. Sumber daya yang mereferensikan awalan selalu menggunakan versi saat ini (terbaru). Anda dapat memulihkan entri dari versi sebelumnya dari daftar awalan, yang juga membuat versi baru.
- Ada kuota yang terkait dengan daftar prefiks. Untuk informasi selengkapnya, lihat Customer-managed daftar awalan.
- Customer-managed Daftar awalan tersedia di semua Wil AWS ayah komersial (termasuk GovCloud (AS) dan Wilayah China).

AWS Daftar prefiks yang dikelola

Aturan berikut berlaku untuk daftar aw AWS alan yang dikelola:

- Anda tidak dapat membuat, memodifikasi, berbagi, atau menghapus daftar aw AWS alan yang dikelola.
- Daftar AWS awalan yang dikelola berbeda memiliki bobot yang berbeda saat Anda menggunakannya. Untuk informasi selengkapnya, lihat AWS-bobot daftar awalan yang dikelola.
- Anda tidak dapat melihat nomor versi daftar awalan AWS yang dikelola.

Identity and access management untuk daftar prefiks

Secara default, pengguna tidak memiliki izin untuk membuat, melihat, memodifikasi, atau menghapus daftar awalan. Anda dapat membuat kebijakan IAM dan melampirkannya ke peran yang memungkinkan pengguna bekerja dengan daftar awalan.

Untuk melihat daftar tindakan Amazon VPC serta kunci sumber daya dan kondisi yang dapat Anda gunakan dalam kebijakan IAM, lihat Tindakan, sumber daya, dan kunci kondisi untuk Amazon EC2 di Referensi Otorisasi Layanan.

Contoh kebijakan berikut memungkinkan pengguna untuk melihat dan bekerja hanya dengan daftar prefiks `pl-123456abcde123456`. Pengguna tidak dapat membuat atau menghapus daftar prefiks.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:GetManagedPrefixListAssociations",
                "ec2:GetManagedPrefixListEntries",
                "ec2:ModifyManagedPrefixList",
                "ec2:RestoreManagedPrefixListVersion"
            ],
            "Resource": "arn:aws:ec2:us-east-1:123456789012:prefix-
list/pl-123456abcde123456"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeManagedPrefixLists",
            "Resource": "*"
        }
    ]
}
```

Untuk informasi selengkapnya tentang bekerja dengan IAM di Amazon VPC, lihat Identity and access management untuk Amazon VPC.

Customer-managed daftar awalan

Customer-managed Daftar awalan memungkinkan Anda untuk menentukan dan memelihara rangkaian rentang alamat IP Anda sendiri, yang dikenal sebagai awalan, di dalamnya AWS. Alih-alih hardcoding alamat IP ini ke berbagai sumber daya Anda, Anda dapat membuat daftar awalan terpusat dan mereferensikannya di mana pun diperlukan. Ini tidak hanya menyederhanakan pengelolaan alamat IP Anda tetapi juga meningkatkan konsistensi dan kegunaan kembali di seluruh AWS lanskap Anda.

Salah satu fitur menonjol dari daftar awalan yang dikelola pelanggan adalah kemampuan untuk membagikannya dengan akun lain. AWS Dengan memberikan akses ke daftar awalan Anda, Anda dapat mengaktifkan tim atau organisasi lain untuk menggunakan rentang alamat IP yang Anda tentukan di sumber daya mereka sendiri. Pendekatan kolaboratif ini menumbuhkan pengalaman cloud yang lebih kohesif dan efisien, di mana manajemen alamat IP dibagikan dan disinkronkan.

Pada bagian berikut, kami akan menyelami lebih dalam aspek praktis bekerja dengan daftar awalan yang dikelola pelanggan, termasuk panduan langkah demi langkah untuk membuat, mengelola, dan berbagi rentang alamat IP Anda.

> **Note**
>
> Anda dapat mengotomatiskan pengelolaan daftar awalan menggunakan Amazon VPC IPAM untuk menyinkronkan CIDR secara otomatis berdasarkan aturan yang Anda tetapkan. Ini menghilangkan pembaruan manual saat infrastruktur Anda berubah. Untuk informasi selengkapnya, lihat Men gotomatiskan pembaruan daftar awalan dengan IPAM di Panduan Pengguna IPAM Amazon VPC.

Tugas

- Bekerja dengan daftar prefiks yang dikelola konsumen

Bekerja dengan daftar prefiks yang dikelola konsumen

Bagian ini menjelaskan cara bekerja dengan daftar awalan yang dikelola pelanggan.

Daftar Isi

- Membuat daftar prefiks
- Lihat daftar prefiks

- Melihat entri untuk daftar prefiks
- Melihat asosiasi (referensi) untuk daftar prefiks Anda
- Ubah daftar awalan
- Mengubah ukuran daftar awalan
- Memulihkan versi sebelumnya dari daftar prefiks
- Menghapus daftar prefiks
- Bagikan daftar awalan yang dikelola pelanggan

Membuat daftar prefiks

Ketika Anda membuat daftar prefiks, Anda harus menentukan jumlah maksimum entri yang dapat didukung oleh daftar prefiks tersebut.

Batasan

Anda tidak dapat menambahkan suatu daftar prefiks ke aturan grup keamanan jika jumlah aturan ditambah entri maks untuk daftar prefiks melebihi kuota aturan per grup keamanan untuk akun Anda.

Untuk membuat daftar prefiks menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Daftar Prefiks yang Dikelola.
3. Pilih Buat daftar prefiks.
4. Untuk Nama daftar prefiks, masukkan nama untuk daftar prefiks.
5. Untuk Entri maksimum, masukkan jumlah maksimum entri untuk daftar prefiks.
6. Untuk Keluarga alamat, pilih apakah daftar prefiks mendukung entri IPv4 atau IPv6.
7. Untuk Entri daftar prefiks, pilih Tambahkan entri baru, dan masukkan blok CIDR dan deskripsi untuk entri tersebut. Ulangi langkah ini untuk setiap entri.
8. (Opsional) Untuk Tag, tambahkan tag ke daftar prefiks untuk membantu Anda untuk mengidentifikasinya nanti.
9. Pilih Buat daftar prefiks.

Untuk membuat daftar awalan menggunakan AWS CLI

Gunakan perintah create-managed-prefix-list.

Lihat daftar prefiks

Anda dapat melihat daftar awalan, daftar awalan yang dibagikan dengan Anda, dan daftar awalan yang AWS dikelola.

Untuk melihat daftar prefiks menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Daftar Prefiks yang Dikelola.
3. Kol om ID Pemilik menunjukkan ID AWS akun pemilik daftar awalan. Untuk daftar awalan yang AWS dikelola -managed, ID Pemilik adalah AWS.

Untuk melihat daftar awalan menggunakan AWS CLI

Gunakan perintah describe-managed-prefix-lists.

Melihat entri untuk daftar prefiks

Anda dapat melihat entri untuk daftar awalan Anda, daftar awalan yang dibagikan dengan Anda, dan daftar awalan yang AWS dikelola.

Untuk melihat entri untuk daftar prefiks menggunakan konsol ini

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Daftar Prefiks yang Dikelola.
3. Pilih kotak centang untuk daftar awalan.
4. Di panel bawah, pilih Entri untuk melihat entri untuk daftar prefiks.

Untuk melihat entri untuk daftar awalan menggunakan AWS CLI

Gunakan perintah get-managed-prefix-list-entries.

Melihat asosiasi (referensi) untuk daftar prefiks Anda

Anda dapat melihat ID dan pemilik sumber daya yang terkait dengan daftar prefiks Anda. Sumber daya yang terkait adalah sumber daya yang menyebutkan daftar prefiks Anda dalam entri atau aturan mereka.

Batasan

Anda tidak dapat melihat sumber daya terkait untuk daftar awalan yang AWS dikelola -.

Untuk melihat asosiasi daftar prefiks menggunakan konsol ini

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Daftar Prefiks yang Dikelola.
3. Pilih kotak centang untuk daftar awalan.
4. Di panel bawah, pilih Asosiasi untuk melihat sumber daya yang menyebutkan daftar prefiks.

Untuk melihat asosiasi daftar awalan menggunakan AWS CLI

Gunakan perintah get-managed-prefix-list-associations.

Ubah daftar awalan

Anda dapat mengubah nama daftar prefiks Anda, dan Anda dapat menambahkan atau menghapus entri. Untuk mengubah jumlah maksimum entri, lihatMengubah ukuran daftar awalan.

Memperbarui entri daftar awalan membuat versi baru dari daftar awalan. Memperbarui nama atau jumlah maksimum entri untuk daftar awalan tidak membuat versi baru dari daftar awalan.

Pertimbangan-pertimbangan

- Anda tidak dapat mengubah daftar awalan yang AWS dikelola.
- Saat Anda meningkatkan jumlah maksimum entri dalam daftar awalan, ukuran maksimum yang ditingkatkan diterapkan pada kuota entri untuk sumber daya yang mereferensikan daftar awalan. Jika salah satu sumber daya ini tidak dapat mendukung peningkatan ukuran maksimum, operasi modifikasi gagal dan ukuran maksimum sebelumnya dipulihkan.

Untuk mengubah daftar prefiks menggunakan konsol ini

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Daftar Prefiks yang Dikelola.
3. Pilih kotak centang untuk daftar awalan, dan pilih Tindakan , Ubah daftar awalan.
4. Untuk Nama daftar prefiks, masukkan nama baru untuk daftar prefiks.
5. Jika daftar awalan terkelola telah dikonfigurasi sebagai target resolver daftar awalan IPAM, Anda akan melihat opsi sinkronisasi resolver daftar awalan IPAM.

Pilih apakah akan mengaktifkan atau menonaktifkan sinkronisasi dengan resolver daftar awalan IPAM. Saat diaktifkan, daftar awalan CIDR diperbarui secara otomatis berdasarkan aturan pemilihan CIDR resolver terkait. Saat dinonaktifkan, daftar awalan CIDR tidak diperbarui secara otomatis. Untuk informasi selengkapnya tentang fitur ini, lihat Men gotomatiskan pembaruan daftar awalan dengan IPAM di Panduan Pengguna Amazon VPC IPAM.

6. Untuk Entri daftar prefiks, pilih Hapus untuk menghapus entri yang ada. Untuk menambahkan entri baru, pilih Tambahkan entri baru dan masukkan blok CIDR dan deskripsi untuk entri tersebut.
7. Pilih Simpan daftar prefiks.

Untuk memodifikasi daftar awalan menggunakan AWS CLI

Gunakan perintah modify-managed-prefix-list.

Mengubah ukuran daftar awalan

Anda dapat mengubah ukuran daftar awalan dan mengubah jumlah maksimum entri untuk daftar awalan hingga 1000. Untuk informasi selengkapnya tentang kuota daftar awalan yang dikelola pelanggan, lihat. Customer-managed daftar awalan

Untuk mengubah ukuran daftar awalan menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Daftar Prefiks yang Dikelola.
3. Pilih kotak centang untuk daftar awalan, dan pilih Tindakan, Ubah ukuran daftar awalan.
4. Untuk entri maks baru, masukkan nilai.
5. Pilih Ubah Ukuran.

Untuk mengubah ukuran daftar awalan menggunakan AWS CLI

Gunakan perintah modify-managed-prefix-list.

Memulihkan versi sebelumnya dari daftar prefiks

Anda dapat memulihkan entri dari versi sebelumnya dari daftar awalan Anda. Ini membuat versi baru dari daftar awalan.

Jika Anda mengurangi ukuran daftar awalan, Anda harus memastikan bahwa daftar awalan cukup besar untuk berisi entri dari versi sebelumnya.

Untuk memulihkan versi sebelumnya dari daftar prefiks menggunakan konsol ini

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Daftar Prefiks yang Dikelola.
3. Pilih kotak centang untuk daftar awalan, dan pilih Tindakan, Puli hkan daftar awalan.
4. Untuk Pilih versi daftar awalan, pilih versi sebelumnya. Entri untuk versi yang dipilih ditampilkan dalam entri daftar Awalan.
5. Pilih Pulihkan daftar prefiks.

Untuk mengembalikan versi sebelumnya dari daftar awalan menggunakan AWS CLI

Gunakan perintah restore-managed-prefix-list-version.

Menghapus daftar prefiks

Untuk menghapus daftar prefiks, Anda harus terlebih dulu menghapus referensi untuk itu dalam sumber daya Anda (seperti dalam tabel rute Anda). Jika Anda telah membagikan daftar prefiks menggunakan AWS RAM, setiap referensi dalam sumber daya yang dimiliki konsumen harus dihapus terlebih dahulu.

Batasan

Anda tidak dapat menghapus daftar awalan AWS-managed.

Untuk menghapus prefiks menggunakan konsol ini

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Daftar Prefiks yang Dikelola.
3. Pilih daftar prefiks, dan pilih Tindakan, Hapus daftar prefiks.
4. Di kotak dialog konfirmasi, masukkan `delete`, dan Hapus..

Untuk menghapus daftar awalan menggunakan AWS CLI

Gunakan perintah delete-managed-prefix-list.

Bagikan daftar awalan yang dikelola pelanggan

Dengan AWS Resource Access Manager (AWS RAM), pemilik daftar awalan yang dikelola pelanggan dapat berbagi daftar awalan dengan yang berikut:

- AWS Akun tertentu di dalam atau di luar organisasinya di AWS Organizations
- Sebuah unit organisasi di dalam organisasinya di AWS Organizations
- Seluruh organisasi di AWS Organizations

Konsumen dengan siapa daftar awalan telah dibagikan dapat melihat daftar awalan dan entrinya, dan mereka dapat mereferensikan daftar awalan di AWS sumber daya mereka.

Untuk informasi selengkap AWS RAM nya, lihat Panduan AWS RAM Pengguna. Untuk informasi selengkapnya tentang kuota, lihat Kuota layanan di Panduan AWS RAM Pengguna.

> **Important**
>
> Tidak ada biaya tambahan untuk membagikan daftar prefiks.

Daftar Isi

- Izin daftar prefiks bersama
- Bekerja dengan daftar prefiks bersama

Izin daftar prefiks bersama

Izin untuk pemilik

Pemilik bertanggung jawab untuk mengelola daftar prefiks bersama dan entrinnya. Pemilik dapat melihat ID AWS sumber daya yang mereferensikan daftar awalan. Namun, mereka tidak dapat menambah atau menghapus referensi ke daftar awalan di AWS sumber daya yang dimiliki oleh konsumen.

Pemilik tidak dapat menghapus daftar prefiks jika daftar prefiks tersebut direferensikan dalam sumber daya yang dimiliki oleh konsumen.

Izin untuk konsumen

Konsumen dapat melihat entri dalam daftar awalan bersama, dan mereka dapat mereferensikan daftar awalan bersama di AWS sumber daya mereka. Namun, konsumen tidak dapat mengubah, memulihkan, atau menghapus daftar prefiks bersama.

Bekerja dengan daftar prefiks bersama

AWS daftar awalan menyediakan cara mudah untuk mengelola dan mereferensikan rentang alamat IP yang digunakan oleh berbagai AWS layanan. Selain daftar awalan yang AWS dikelola, Anda juga dapat membuat dan membagikan daftar awalan yang dikelola pelanggan Anda sendiri dengan akun lain. AWS

Berbagi daftar awalan dapat sangat berguna bagi organisasi dengan persyaratan jaringan yang kompleks atau yang perlu mengoordinasikan penggunaan alamat IP di beberapa AWS beban kerja. Dengan membagikan daftar awalan, Anda dapat memastikan manajemen alamat IP yang konsisten dan menyederhanakan konfigurasi jaringan untuk kolaborator Anda.

Bagian ini menjelaskan dan cara berbagi daftar awalan dan cara mengidentifikasi dan menggunakan daftar awalan yang telah dibagikan dengan akun Anda.

Daftar Isi

- Bagikan daftar prefiks
- Membatalkan pembagian daftar prefiks bersama
- Mengidentifikasi daftar prefiks bersama
- Mengidentifikasi referensi ke daftar prefiks bersama

Bagikan daftar prefiks

Untuk membagikan daftar prefiks, Anda harus menambahkannya ke pembagian sumber daya. Jika Anda tidak memiliki pembagian sumber daya, Anda harus terlebih dahulu membuatnya dengan menggunakan Konsol AWS RAM.

Jika Anda adalah bagian dari organisasi di AWS Organizations, dan berbagi dalam organisasi Anda diaktifkan, konsumen di organisasi Anda secara otomatis diberikan akses ke daftar awalan bersama. Jika tidak, konsumen menerima undangan untuk mengikuti pembagian sumber daya dan diberikan akses ke daftar prefiks bersama setelah menerima undangan tersebut.

Anda dapat membuat pembagian sumber daya dan membagikan daftar prefiks yang Anda miliki menggunakan konsol AWS RAM , atau AWS CLI.

> **Important**
>
> - Untuk membagikan daftar awalan, Anda harus memilikinya. Anda tidak dapat membagikan daftar prefiks yang telah dibagikan dengan Anda. Anda tidak dapat membagikan daftar awalan yang AWS dikelola.
> - Untuk membagikan daftar prefiks dengan organisasi atau unit organisasi Anda di AWS Organizations, Anda harus mengaktifkan pembagian dengan AWS Organizations. Untuk informasi lebih lanjut, lihat Aktifkan pembagian dengan AWS Organizations dalam Panduan Pengguna AWS RAM .

Untuk membuat berbagi sumber daya dan berbagi daftar awalan menggunakan AWS RAM konsol

Ikuti langkah-langkah di Buat pembagian sumber daya di Panduan Pengguna AWS RAM . Untuk Pilih jenis sumber daya, pilih Daftar Prefiks, lalu pilih kotak centang untuk daftar prefiks Anda.

Untuk menambahkan daftar awalan ke berbagi sumber daya yang ada menggunakan AWS RAM konsol

Untuk menambahkan prefiks terkelola yang Anda miliki ke pembagian sumber daya yang ada, ikuti langkah-langkah dalam Memperbarui pembagian sumber daya di Panduan Pengguna AWS RAM . Untuk Memilih jenis sumber daya pilih Daftar Prefiks, lalu pilih kotak centang untuk daftar prefiks Anda.

Untuk membagikan daftar awalan yang Anda miliki menggunakan AWS CLI

Gunakan perintah berikut untuk membuat dan memperbarui pembagian sumber daya:

- buat-berbagi sumber daya
- berbagi sumber daya asosiasi
- perbaruan-sumber daya-berbagi

Membatalkan pembagian daftar prefiks bersama

Ketika Anda membatalkan pembagian daftar prefiks, konsumen tidak dapat lagi melihat daftar prefiks atau entri di akun mereka, dan mereka tidak dapat menyebutkan daftar prefiks di sumber daya mereka. Jika daftar prefiks sudah direferensikan dalam sumber daya konsumen, referensi tersebut

terus berfungsi seperti biasa, dan Anda dapat melanjutkan melihat referensi tersebut. Jika Anda memperbarui daftar prefiks ke versi baru, referensi akan menggunakan versi terbaru tersebut.

Untuk membatalkan berbagi daftar awalan bersama yang Anda miliki, Anda harus menghapusnya dari berbagi sumber daya menggunakan AWS RAM.

Untuk membatalkan berbagi daftar awalan bersama yang Anda miliki menggunakan AWS RAM konsol

Lihat Memperbarui Pembagian Sumber Daya di Panduan Pengguna.AWS RAM

Untuk membatalkan berbagi daftar awalan bersama yang Anda miliki menggunakan AWS CLI

Gunakan perintah disassociate-resource-share.

Mengidentifikasi daftar prefiks bersama

Pemilik dan konsumen dapat mengidentifikasi daftar prefiks bersama menggunakan konsol Amazon VPC dan AWS CLI.

Untuk mengidentifikasi daftar prefiks bersama menggunakan konsol Amazon VPC

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Daftar Prefiks yang Dikelola.
3. Halaman menampilkan daftar prefiks yang Anda miliki dan daftar prefiks yang dibagikan dengan Anda. Kolom ID pemilik menunjukkan ID akun AWS dari pemilik daftar prefiks.
4. Untuk melihat informasi pembagian sumber daya untuk daftar prefiks, pilih daftar prefiks dan pilih Pembagian di panel bawah.

Untuk mengidentifikasi daftar awalan bersama menggunakan AWS CLI

Gunakan perintah describe-managed-prefix-lists. Perintah mengembalikan daftar awalan yang Anda miliki dan daftar awalan yang dibagikan dengan Anda. `OwnerId`menunjukkan ID AWS akun pemilik daftar awalan.

Mengidentifikasi referensi ke daftar prefiks bersama

Pemilik dapat mengidentifikasi sumber daya milik konsumen yang mereferensikan daftar awalan bersama.

Untuk mengidentifikasi referensi ke daftar prefiks bersama menggunakan konsol Amazon VPC

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Daftar Prefiks yang Dikelola.
3. Pilih daftar prefiks dan pilih Asosiasi di panel bawah.
4. ID sumber daya yang menyebutkan daftar prefiks tercantum dalam kolom ID Sumber Daya. Pemilik sumber daya tercantum dalam kolom Pemilik sumber daya.

Untuk mengidentifikasi referensi ke daftar awalan bersama menggunakan AWS CLI

Gunakan perintah get-managed-prefix-list-associations.

AWS Daftar prefiks yang dikelola

AWS Daftar awalan yang dikelola adalah kumpulan rentang alamat IP untuk AWS layanan. Daftar awalan ini dikelola oleh Amazon Web Services dan menyediakan cara untuk mereferensikan alamat IP yang digunakan oleh berbagai AWS penawaran. Ini bisa sangat berguna saat mengonfigurasi grup keamanan atau kontrol tingkat jaringan lainnya dalam VPC.

Daftar awalan mencakup berbagai AWS layanan, termasuk S3 dan DynamoDB, dan banyak lainnya. Dengan menggunakan daftar awalan terkelola, Anda dapat memastikan bahwa konfigurasi jaringan Anda mutakhir dan memperhitungkan alamat IP yang digunakan oleh AWS layanan yang Anda andalkan dengan benar. Ini dapat membantu menyederhanakan tugas jaringan dan mengurangi overhead administratif untuk memelihara daftar alamat IP secara manual.

Selain manfaat praktis, menggunakan daftar awalan terkelola juga selaras dengan praktik terbaik AWS keamanan. Dengan mengandalkan informasi alamat IP otoritatif yang disediakan oleh AWS, Anda dapat meminimalkan risiko kesalahan konfigurasi atau masalah konektivitas yang tidak terduga. Hal ini bisa sangat penting untuk aplikasi atau beban kerja kritis dengan persyaratan kepatuhan yang ketat.

Daftar Isi

- Available AWS Daftar prefiks yang dikelola
- AWS-bobot daftar awalan yang dikelola
- Gunakan AWS-daftar awalan yang dikelola

Available AWS Daftar prefiks yang dikelola

Layanan berikut menyediakan daftar aw AWS alan yang dikelola.

Layanan AWS	Nama daftar awalan	Bobot
Amazon CloudFront	com.amazonaws.global.cloudfront.origin-facing (IPv4)	55
	com.amazonaws.global.ipv6.cloudfront.origin-facing (IPv6)	
Amazon DynamoDB	com.amazonaws. *region*.dynamodb	1
Hubungkan Instans Amazon EC2	com.amazonaws. *region*.ec2-instance-connect	2
	com.amazonaws. *region*.ipv6.ec2-instance-connect	2
AWS Ground Station	com.amazonaws.global.stasiun bumi	5
Rute Amazon 53	com.amazonaws. *region*.ipv6.route53-pemeriksaan kesehatan	25
	com.amazonaws. *region*.route53-pemeriksaan kesehatan	25
Amazon S3	com.amazonaws. *region*.s3	1
Amazon S3 Express Satu Zona	com.amazonaws. *region*.s3express	6
AWS Secrets Manager	com.amazonaws. *region*.secretsmanager-dikelola-rahasia-eksternal	20
Amazon VPC Lattice	com.amazonaws. *region*.vpc-latex	10
	com.amazonaws. *region*.ipv6.vpc-latex	10

Untuk melihat AWS-daftar awalan yang dikelola menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Daftar Prefiks yang Dikelola.
3. Di bidang pencarian, tambahkan ID Pemilik: AWS filter.

Untuk melihat AWS-daftar awalan yang dikelola menggunakan AWS CLI

Gunakan perintah describe-managed-pre fix-lists sebagai berikut.

```
aws ec2 describe-managed-prefix-lists --filters Name=owner-id,Values=AWS
```

AWS-bobot daftar awalan yang dikelola

Berat daftar aw AWS alan yang dikelola mengacu pada jumlah entri yang diambil dalam sumber daya.

Misalnya, bobot daftar awalan yang CloudFront dikelola Amazon adalah 55. Berikut ini adalah bagaimana hal ini memengaruhi kuota Amazon VPC Anda:

- Grup keamanan — Kuota default adalah 60 aturan, menyisakan ruang untuk hanya 5 aturan tambahan dalam grup keamanan. Anda dapat meminta kenaikan kuota untuk kuota ini.
- Tabel rute — Kuota default adalah 50 rute, jadi Anda harus meminta peningkatan kuota sebelum Anda dapat menambahkan daftar awalan ke tabel rute.

Gunakan AWS-daftar awalan yang dikelola

AWS Daftar awalan yang dikelola dibuat dan dikelola oleh AWS dan dapat digunakan oleh siapa saja yang memiliki AWS akun. Anda tidak dapat membuat, memodifikasi, berbagi, atau menghapus daftar aw AWS alan yang dikelola.

Seperti daftar awalan yang dikelola pelanggan, Anda dapat menggunakan daftar aw AWS alan yang dikelola dengan AWS sumber daya seperti grup keamanan dan tabel rute. Untuk informasi selengkapnya, lihat Pengoptimalan AWS manajemen infrastruktur dengan daftar awalan.

Pengoptimalan AWS manajemen infrastruktur dengan daftar awalan

Anda dapat mereferensikan daftar awalan di AWS sumber daya berikut.

Sumber daya

- Grup keamanan VPC
- Tabel rute subnet
- Tabel rute transit gateway
- AWS Network Firewall kelompok aturan
- Kontrol akses jaringan Grafana yang Dikelola Amazon
- AWS Outposts rak gateway lokal

Grup keamanan VPC

Anda dapat menentukan daftar prefiks sebagai sumber untuk aturan ke dalam, atau sebagai tujuan untuk aturan keluar. Untuk informasi selengkapnya, lihat Grup keamanan.

> **Important**
>
> Anda tidak dapat mengubah aturan yang ada untuk menggunakan daftar awalan. Anda harus membuat aturan baru untuk menggunakan daftar awalan.

Untuk menyebutkan daftar prefiks dalam aturan grup keamanan menggunakan konsol ini

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Grup Keamanan.
3. Pilih grup keamanan yang akan diperbarui.
4. Pilih Tindakan, Mengedit aturan ke dalam atau Tindakan, Mengedit aturan keluar.
5. Pilih Tambahkan aturan. Untuk Jenis, pilih jenis lalu lintas. Untuk Sumber (aturan masuk) atau Tujuan (aturan keluar), pilih Kustom. Kemudian, di bidang berikutnya, di bawah Daftar A walan, pilih ID daftar awalan.
6. Pilih Simpan aturan.

Untuk mereferensikan daftar awalan dalam aturan grup keamanan menggunakan AWS CLI

Gunakan perintah authorize-security-group-ingress dan authorize-security-group-egress. Untuk parameter `--ip-permissions`, tentukan ID dari daftar prefiks menggunakan `PrefixListIds`.

Tabel rute subnet

Anda dapat menentukan daftar prefiks sebagai tujuan untuk entri tabel rute. Anda tidak dapat menyebutkan daftar prefiks dalam tabel rute gateway. Untuk informasi lebih lanjut tentang tabel rute, lihat Konfigurasikan tabel rute.

Untuk menyebutkan daftar prefiks dalam tabel rute menggunakan konsol ini

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Tabel rute, dan pilih tabel rute.
3. Pilih Tindakan, Sunting rute.
4. Untuk menambahkan rute, pilih Tambahkan rute.
5. Untuk Tujuan masukkan ID dari daftar prefiks.
6. Untuk Target, pilih target.
7. Pilih Simpan perubahan.

Untuk mereferensikan daftar awalan dalam tabel rute menggunakan AWS CLI

Gunakan perintah create-route (AWS CLI). Gunakan parameter `--destination-prefix-list-id` untuk menentukan ID dari daftar prefiks.

Tabel rute transit gateway

Anda dapat menentukan daftar prefiks sebagai tujuan untuk rute. Untuk informasi selengkapnya, lihat Referensi daftar prefiks di Transit Gateway Amazon VPC.

AWS Network Firewall kelompok aturan

Grup AWS Network Firewall aturan adalah seperangkat kriteria yang dapat digunakan kembali untuk memeriksa dan menangani lalu lintas jaringan. Jika Anda membuat grup aturan Suricata-compatible stateful di AWS Network Firewall, Anda dapat mereferensikan daftar awalan dari grup aturan. Untuk informasi selengkapnya, lihat Referensi daftar awalan Amazon VPC dan Membuat grup aturan stateful di Panduan Peng AWS Network Firewall embang.

Kontrol akses jaringan Grafana yang Dikelola Amazon

Anda dapat menentukan satu atau beberapa daftar awalan sebagai aturan masuk untuk permintaan ke ruang kerja Grafana yang Dikelola Amazon. Untuk informasi selengkapnya tentang kontrol akses

jaringan ruang kerja Grafana, termasuk cara mereferensikan daftar awalan, lihat Mengelola akses jaringan di Panduan Pengguna Amazon Managed Grafana.

AWS Outposts rak gateway lokal

Setiap AWS Outposts rak menyediakan gateway lokal yang memungkinkan Anda menghubungkan sumber daya Outpost dengan jaringan lokal Anda. Anda dapat mengelompokkan CIDR yang sering Anda gunakan dalam daftar awalan dan mereferensikan daftar ini sebagai target rute di tabel rute gateway lokal Anda. Untuk informasi selengkapnya, lihat Mengel ola rute tabel rute gateway lokal di Panduan AWS Outposts Pengguna untuk rak.

AWS Rentang alamat IP

AWS menerbitkan rentang alamat IP saat ini dalam format JSON. Dengan informasi ini, Anda dapat mengidentifikasi lalu lintas dari AWS. Anda juga dapat menggunakan informasi ini untuk mengizinkan atau menolak lalu lintas ke atau dari beberapa Layanan AWS.

Pertimbangan-pertimbangan

- Kami menerbitkan rentang alamat IP untuk layanan yang biasa digunakan pelanggan untuk melakukan pemfilteran keluar. Kami tidak mempublikasikan rentang alamat IP untuk semua layanan.
- Layanan menggunakan rentang alamat IP mereka untuk berkomunikasi dengan layanan lain atau untuk berkomunikasi dengan jaringan pelanggan.
- Rentang alamat IP yang Anda bawa AWS melalui bring your own IP address (BYOIP) tidak termasuk dalam file. `.json` Untuk informasi selengkapnya, lihat Mengiklankan rentang alamat Anda melalui AWS Panduan Pengguna Amazon EC2.

Beberapa layanan menerbitkan rentang alamat mereka menggunakan daftar awalan AWS yang dikelola -managed. Untuk informasi selengkapnya, lihat the section called “Available AWS Daftar prefiks yang dikelola”.

Daftar Isi

- Unduh file JSON
- Kontrol keluar
- Umpan geolokasi

- Temukan rentang alamat IP untuk Layanan AWS
- Sintaks untuk AWS Kisaran alamat IP JSON
- AWS Pemberitahuan rentang alamat IP

Unduh file JSON

Untuk melihat rentang alamat saat ini, unduh ip-ranges.json ip-ranges.json ip-ranges.json ip-ranges.json Untuk menjaga riwayat, simpan versi berturut-turut dari file JSON di komputer Anda sendiri. Untuk menentukan apakah ada perubahan sejak terakhir kali Anda menyimpan file, periksa waktu penerbitan di file saat ini dan bandingkan dengan waktu penerbitan di file terakhir yang Anda simpan.

Berikut ini adalah contoh curl perintah yang menyimpan file JSON ke direktori saat ini.

```
curl -O https://ip-ranges.amazonaws.com/ip-ranges.json
```

Jika mengakses file ini secara terprogram, Anda bertanggung jawab untuk memastikan bahwa aplikasi mengunduh file hanya setelah berhasil memverifikasi sertifikat TLS yang disajikan oleh server.

Untuk menerima pemberitahuan pembaruan pada file JSON, lihatAWS Pemberitahuan rentang alamat IP.

Kontrol keluar

Untuk mengizinkan sumber daya yang Anda buat dengan satu AWS layanan hanya mengakses AWS layanan lain, Anda dapat menggunakan informasi rentang alamat IP di file ip-ranges.json untuk melakukan pemfilteran keluar. Pastikan aturan grup keamanan mengizinkan lalu lintas keluar ke blok CIDR dalam daftar AMAZON. Ada ku ota untuk kelompok keamanan. Bergantung pada jumlah rentang alamat IP di setiap Wilayah, Anda mungkin memerlukan beberapa grup keamanan per Wilayah.

> **Note**
>
> Beberapa AWS layanan dibangun di atas EC2 dan menggunakan ruang alamat IP EC2. Jika Anda memblokir lalu lintas ke ruang alamat IP EC2, Anda juga memblokir lalu lintas ke layanan non-EC2 ini.

Umpan geolokasi

Rentang alamat IP di dalam `ip-ranges.json` adalah oleh Wilayah AWS. Namun, Zona Lokal tidak berada di lokasi fisik yang sama dengan Wilayah induknya. Data geolokasi yang dipublikasikan di geo-ip-feed.csv akun untuk Zona Lokal. Data mengikuti RFC 8 805.

Temukan rentang alamat IP untuk Layanan AWS

File JSON rentang alamat AWS IP yang disediakan oleh AWS dapat menjadi sumber daya yang berharga untuk menemukan alamat IP dari berbagai AWS layanan dan menggunakan informasi itu untuk meningkatkan keamanan jaringan dan kontrol akses Anda. Dengan mengurai data terperinci yang terkandung dalam file JSON ini, Anda dapat secara tepat mengidentifikasi rentang alamat IP yang terkait dengan wilayah tertentu Layanan AWS .

Misalnya, Anda dapat menggunakan rentang alamat IP untuk mengonfigurasi kebijakan keamanan jaringan yang kuat, menyiapkan aturan firewall granular untuk mengizinkan atau menolak akses ke AWS sumber daya tertentu. Informasi ini juga dapat berguna untuk berbagai AWS Network Firewall tugas. Tingkat kontrol ini sangat penting untuk melindungi aplikasi dan data Anda, memastikan bahwa hanya lalu lintas resmi yang dapat mencapai yang diperlukan Layanan AWS. Selain itu, memiliki kecerdasan IP ini dapat membantu Anda memastikan aplikasi Anda dikonfigurasi dengan benar untuk berkomunikasi dengan AWS titik akhir yang tepat, meningkatkan keandalan dan kinerja secara keseluruhan.

Selain aturan firewall, `ip-ranges.json` file juga dapat dimanfaatkan untuk mengkonfigurasi pemfilteran keluar yang canggih pada infrastruktur jaringan Anda. Dengan memahami rentang alamat IP tujuan untuk yang berbeda Layanan AWS, Anda dapat mengatur kebijakan routing atau menggunakan solusi keamanan jaringan lanjutan seperti mengizinkan atau memblokir lalu lintas keluar secara selektif berdasarkan tujuan yang dituju. Kontrol keluar ini sangat penting untuk mengurangi risiko kebocoran data dan akses yang tidak sah.

Penting untuk dicatat bahwa `ip-ranges.json` file diperbarui secara berkala, jadi menjaga salinan lokal terbaru sangat penting untuk memastikan Anda memiliki informasi yang paling akurat dan terkini. Dengan terus menggunakan konten file ini, Anda dapat mengelola akses jaringan dan keamanan secara efisien untuk aplikasi AWS berbasis Anda, memperkuat postur keamanan cloud Anda secara keseluruhan.

Contoh berikut dapat membantu Anda memfilter rentang alamat AWS IP sesuai dengan apa yang Anda cari. Di Linux, Anda dapat mengunduh dan menggunakan alat jq untuk mengurai

salinan lokal file JSON. Ini AWS Tools for Windows PowerShell termasuk cmdlet, Get-AWSPublicIpAddressRange, yang dapat Anda gunakan untuk mengurai file JSON ini. Untuk informasi selengkapnya, lihat blog berikut: Men anyakan Rentang Alamat IP Publik untuk AWS.

Untuk mendapatkan file JSON, lihatthe section called “Unduh”. Untuk informasi selengkapnya tentang sintaks file JSON, lihatthe section called “Sintaksis”.

Contoh

- Dapatkan tanggal pembuatan file
- Dapatkan alamat IP untuk Wilayah tertentu
- Dapatkan semua alamat IPv4
- Dapatkan semua alamat IPv4 untuk layanan tertentu
- Dapatkan semua alamat IPv4 untuk layanan tertentu di Wilayah tertentu
- Dapatkan semua alamat IPv6
- Dapatkan semua alamat IPv6 untuk layanan tertentu
- Dapatkan semua alamat IP untuk grup perbatasan tertentu

Dapatkan tanggal pembuatan file

Contoh berikut mendapatkan tanggal pembuatan`ip-ranges.json`.

jq

```
$ jq .createDate < ip-ranges.json

"2024-08-01-17-22-15"
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -OutputPublicationDate

Thursday, August 1, 2024 9:22:35 PM
```

Dapatkan alamat IP untuk Wilayah tertentu

Contoh berikut memfilter file JSON untuk alamat IP untuk Wilayah yang ditentukan.

jq

```
$ jq '.prefixes[] | select(.region=="us-east-1")' < ip-ranges.json

{
  "ip_prefix": "23.20.0.0/14",
  "region": "us-east-1",
  "network_border_group": "us-east-1",
  "service": "AMAZON"
},
{
  "ip_prefix": "50.16.0.0/15",
  "region": "us-east-1",
  "network_border_group": "us-east-1",
  "service": "AMAZON"
},
{
  "ip_prefix": "50.19.0.0/16",
  "region": "us-east-1",
  "network_border_group": "us-east-1",
  "service": "AMAZON"
},
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -Region us-east-1

IpPrefix        Region      NetworkBorderGroup         Service
--------        ------       -------                   -------
23.20.0.0/14    us-east-1    us-east-1                 AMAZON
50.16.0.0/15    us-east-1    us-east-1                 AMAZON
50.19.0.0/16    us-east-1    us-east-1                 AMAZON
...
```

Dapatkan semua alamat IPv4

Contoh berikut menyaring file JSON untuk alamat IPv4.

jq

```
$ jq -r '.prefixes | .[].ip_prefix' < ip-ranges.json
```

```
23.20.0.0/14
27.0.0.0/22
43.250.192.0/24
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange | where {$_.IpAddressFormat -eq "Ipv4"} | select
 IpPrefix

IpPrefix
--------
23.20.0.0/14
27.0.0.0/22
43.250.192.0/24
...
```

Dapatkan semua alamat IPv4 untuk layanan tertentu

Contoh berikut memfilter file JSON untuk alamat IPv4 untuk layanan yang ditentukan.

jq

```
$ jq -r '.prefixes[] | select(.service=="GLOBALACCELERATOR") | .ip_prefix' < ip-
ranges.json

13.248.117.0/24
15.197.34.0/23
15.197.36.0/22
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -ServiceKey GLOBALACCELERATOR | where
 {$_.IpAddressFormat -eq "Ipv4"} | select IpPrefix

IpPrefix
--------
13.248.117.0/24
15.197.34.0/23
15.197.36.0/22
```

```
...
```

Dapatkan semua alamat IPv4 untuk layanan tertentu di Wilayah tertentu

Contoh berikut memfilter file JSON untuk alamat IPv4 untuk layanan yang ditentukan di Wilayah yang ditentukan.

jq

```
$ jq -r '.prefixes[] | select(.region=="us-east-1") |
 select(.service=="GLOBALACCELERATOR") | .ip_prefix' < ip-ranges.json

13.248.124.0/24
99.82.166.0/24
99.82.171.0/24
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -Region us-east-1 -ServiceKey GLOBALACCELERATOR
 | where {$_.IpAddressFormat -eq "Ipv4"} | select IpPrefix

IpPrefix
--------
13.248.117.0/24
99.82.166.0/24
99.82.171.0/24
...
```

Dapatkan semua alamat IPv6

Contoh berikut menyaring file JSON untuk alamat IPv6.

jq

```
$ jq -r '.ipv6_prefixes | .[].ipv6_prefix' < ip-ranges.json

2a05:d07c:2000::/40
2a05:d000:8000::/40
2406:dafe:2000::/40
```

```
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange | where {$_.IpAddressFormat -eq "Ipv6"} | select
 IpPrefix

IpPrefix
--------
2a05:d07c:2000::/40
2a05:d000:8000::/40
2406:dafe:2000::/40
...
```

Dapatkan semua alamat IPv6 untuk layanan tertentu

Contoh berikut menyaring file JSON untuk alamat IPv6 untuk layanan yang ditentukan.

jq

```
$ jq -r '.ipv6_prefixes[] | select(.service=="GLOBALACCELERATOR") | .ipv6_prefix' <
 ip-ranges.json

2600:1f01:4874::/47
2600:1f01:4802::/47
2600:1f01:4860::/47
2600:9000:a800::/40
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -ServiceKey GLOBALACCELERATOR | where
 {$_.IpAddressFormat -eq "Ipv6"} | select IpPrefix

IpPrefix
--------
2600:1f01:4874::/47
2600:1f01:4802::/47
2600:1f01:4860::/47
2600:9000:a800::/40
...
```

Dapatkan semua alamat IP untuk grup perbatasan tertentu

Contoh berikut memfilter file JSON untuk semua alamat IP untuk grup perbatasan yang ditentukan.

jq

```
$ jq -r '.prefixes[] | select(.network_border_group=="us-west-2-lax-1")
 | .ip_prefix' < ip-ranges.json
70.224.192.0/18
52.95.230.0/24
15.253.0.0/16
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange | where {$_.NetworkBorderGroup -eq "us-west-2-
lax-1"} | select IpPrefix

IpPrefix
--------
70.224.192.0/18
52.95.230.0/24
15.253.0.0/16
...
```

Sintaks untuk AWS Kisaran alamat IP JSON

AWS menerbitkan rentang alamat IP saat ini dalam format JSON. Untuk mendapatkan file JSON, lihatthe section called “Unduh”. Sintaks file JSON adalah sebagai berikut.

```
{
  "syncToken": "0123456789",
  "createDate": "yyyy-mm-dd-hh-mm-ss",
  "prefixes": [
    {
      "ip_prefix": "cidr",
      "region": "region",
      "network_border_group": "network_border_group",
      "service": "subset"
    }
  ],
```

```
  "ipv6_prefixes": [
    {
      "ipv6_prefix": "cidr",
      "region": "region",
      "network_border_group": "network_border_group",
      "service": "subset"
    }
  ]
}
```

syncToken

Waktu penerbitan, dalam format waktu jangka waktu Unix.

Tipe: String

Contoh: `"syncToken": "1416435608"`

createDate

Tanggal dan waktu publikasi, dalam YY-MM-DD-hh-mm-ss format UTC.

Tipe: String

Contoh: `"createDate": "2014-11-19-23-29-02"`

prefiks

Prefiks IP untuk rentang alamat IPv4.

Jenis: Array

ipv6_prefixes

Prefiks IP untuk rentang alamat IPv6.

Jenis: Array

ip_prefix

Rentang alamat IPv4 publik, dalam notasi CIDR. Perhatikan bahwa AWS mungkin mengiklankan awalan dalam rentang yang lebih spesifik. Misalnya, awalan 96.127.0. 0/17 dalam file dapat diiklankan sebagai 96.127.0. 0/21, 96.127,8. 0/21, 96.127.32. 0/19, dan 96.127.64. 0/18.

Tipe: String

Contoh: `"ip_prefix": "198.51.100.2/24"`

ipv6_prefix

Rentang alamat IPv6 publik, dalam notasi CIDR. Perhatikan bahwa AWS mungkin mengiklankan awalan dalam rentang yang lebih spesifik.

Tipe: String

Contoh: `"ipv6_prefix": "2001:db8:1234::/64"`

network_border_group

Nama grup perbatasan jaringan, yang merupakan kumpulan unik Zona Ketersediaan atau Zona Lokal tempat mengiklan AWS kan alamat IP, atau`GLOBAL`. Lalu lintas untuk `GLOBAL` layanan dapat ditarik ke atau berasal dari beberapa (hingga semua) Zona Ketersediaan atau Zona Lokal tempat mengik AWS lankan alamat IP.

Tipe: String

Contoh: `"network_border_group": "us-west-2-lax-1"`

region

Wil AWS ayah atau`GLOBAL`. Lalu lintas untuk `GLOBAL` layanan dapat ditarik ke atau berasal dari beberapa (hingga semua) Wil AWS ayah.

Tipe: String

Nilai yang valid: `af-south-1` `ap-east-1` `ap-east-2` | `ap-northeast-1` | `ap-northeast-2` `ap-northeast-3` | `ap-south-1` | `ap-south-2` | `ap-southeast-1` | `ap-southeast-2` | `ap-southeast-3` `ap-southeast-4` | `ap-southeast-5` | `ap-southeast-6` | `ap-southeast-7` | `ca-central-1` `ca-west-1` | `cn-north-1` | `cn-northwest-1` | `eu-central-1` | `eu-central-2` | `eu-north-1` `eu-south-1` | `eu-south-2` | `eu-west-1` | `eu-west-2` | `eu-west-3` | `il-central-1` `mx-central-1` | `me-central-1` | `me-south-1` | `sa-east-1` | `us-east-1` | `us-east-2` `us-gov-east-1` | `us-gov-west-1` | `us-west-1` | `us-west-2`| `GLOBAL`

Contoh: `"region": "us-east-1"`

layanan

Subset rentang alamat IP. Alamat yang tercantum untuk `API_GATEWAY` hanya jalan keluar. Tentukan `AMAZON` untuk mendapatkan semua rentang alamat IP (artinya setiap subset juga ada di dalam subset `AMAZON`). Namun, beberapa rentang alamat IP hanya ada di subset `AMAZON` (artinya rentang tersebut tidak juga tersedia di subset lain).

Tipe: String

Nilai yang valid: AMAZON AMAZON_APPFLOW AMAZON_CONNECT | API_GATEWAY | AURORA_DSQL CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRONT | CLOUDFRONT_ORIGIN_FACING | CODEBUILD DYNAMODB | EBS | EC2 | EC2_INSTANCE_CONNECT | GLOBALACCELERATOR IVS_LOW_LATENCY | IVS_REALTIME | KINESIS_VIDEO_STREAMS | MEDIA_PACKAGE_V2 | ROUTE53 | ROUTE53_HEALTHCHECKS ROUTE53_HEALTHCHECKS_PUBLISHING | ROUTE53_RESOLVER | S3 | WORKSPACES_GATEWAYS

Contoh: `"service": "AMAZON"`

Rentang tumpang tindih

Rentang alamat IP yang dikembalikan oleh kode layanan apa pun juga dikembalikan oleh kode AMAZON layanan. Misalnya, semua rentang alamat IP yang dikembalikan oleh kode S3 layanan juga dikembalikan oleh kode AMAZON layanan.

Ketika layanan A menggunakan sumber daya dari layanan B, ada rentang alamat IP yang dikembalikan oleh kode layanan untuk layanan A dan layanan B. Namun, rentang alamat IP ini digunakan secara eksklusif oleh layanan A, dan tidak dapat digunakan oleh layanan B. Misalnya, Amazon S3 menggunakan sumber daya dari Amazon EC2, jadi ada rentang alamat IP yang dikembalikan oleh kode EC2 layanan S3 dan kode layanan. Namun rentang alamat IP ini digunakan secara eksklusif oleh Amazon S3. Oleh karena itu, kode S3 layanan mengembalikan semua rentang alamat IP yang digunakan secara eksklusif oleh Amazon S3. Untuk mengidentifikasi rentang alamat IP yang digunakan secara eksklusif oleh Amazon EC2, temukan rentang alamat IP yang dikembalikan oleh kode EC2 layanan tetapi bukan kode S3 layanan.

Pelajari selengkapnya

Bagian ini menyediakan tautan ke informasi tambahan untuk kode layanan yang berbeda.

- AMAZON_APPFLOW— Rentang alamat IP
- AMAZON_CONNECT— Siapkan jaringan Anda
- CHIME_MEETINGS— Meng konfigurasi untuk media dan pensinyalan
- CLOUDFRONT— Lokasi dan rentang alamat IP server CloudFront tepi
- DYNAMODB— Rentang alamat IP
- EC2— Alamat IPV4 Pu blik

- `EC2_INSTANCE_CONNECT`— Pras yarat Koneksi Instance EC2
- `GLOBALACCELERATOR`— Rentang lokasi dan alamat IP server tepi Global Accelerator
- `ROUTE53`— Rentang alamat IP server Amazon Route 53
- `ROUTE53_HEALTHCHECKS`— Rentang alamat IP server Amazon Route 53
- `ROUTE53_HEALTHCHECKS_PUBLISHING`— Rentang alamat IP server Amazon Route 53
- `WORKSPACES_GATEWAYS`— Server gateway PCoIP

Catatan rilis

Tabel berikut menjelaskan pembaruan sintaks`ip-ranges.json`. Kami juga menambahkan kode Wilayah baru dengan setiap peluncuran Wilayah.

Deskripsi	Tanggal rilis
Menambahkan kode layanan `IVS_LOW_LATENCY` .	Juli 29, 2025
Menambahkan kode layanan `AURORA_DSQL` .	Mei 21, 2025
Menambahkan kode layanan `IVS_REALTIME` .	Juni 11, 2024
Menambahkan kode layanan `MEDIA_PACKAGE_V2` .	9 Mei 2023
Menambahkan kode layanan `CLOUDFRONT_ORIGIN_FACING` .	Oktober 12, 2021
Menambahkan kode layanan `ROUTE53_RESOLVER` .	24 Juni 2021
Menambahkan kode layanan `EBS`.	12 Mei 2021
Menambahkan kode layanan `KINESIS_VIDEO_STREAMS` .	19 November 2020
Menambahkan kode layanan `CHIME_MEETINGS` dan `CHIME_VOICECONNECTOR` .	19 Juni 2020

Deskripsi	Tanggal rilis
Menambahkan kode layanan `AMAZON_APPFLOW` .	9 Juni 2020
Menambahkan dukungan untuk grup perbatasan jaringan.	7 April 2020
Menambahkan kode layanan `WORKSPACES_GATEWAYS` .	30 Maret 2020
Menambahkan kode layanan `ROUTE53_HEALTHCHECK_PUBLISHING` .	30 Januari 2020
Menambahkan kode layanan `API_GATEWAY` .	26 September 2019
Menambahkan kode layanan `EC2_INSTANCE_CONNECT` .	26 Juni 2019
Menambahkan kode layanan `DYNAMODB`.	25 April 2019
Menambahkan kode layanan `GLOBALACCELERATOR` .	20 Desember 2018
Menambahkan kode layanan `AMAZON_CONNECT` .	20 Juni 2018
Menambahkan kode layanan `CLOUD9`.	20 Juni 2018
Menambahkan kode layanan `CODEBUILD` .	19 April 2018
Menambahkan kode layanan `S3`.	28 Februari 2017
Menambahkan dukungan untuk rentang alamat IPv6.	22 Agustus 2016
Rilis awal	19 November 2014

AWS Pemberitahuan rentang alamat IP

AWS menerbitkan rentang alamat IP saat ini dalam format JSON. Setiap kali ada perubahan pada rentang alamat AWS IP, kami mengirim pemberitahuan ke pelanggan topik Amazon SNS bernama`AmazonIpSpaceChanged`. Untuk informasi selengkapnya tentang sintaks file JSON, lihatthe section called “Sintaksis”.

Payload notifikasi berisi informasi dalam format berikut.

```
{
  "create-time":"yyyy-mm-ddThh:mm:ss+00:00",
  "synctoken":"0123456789",
  "md5":"6a45316e8bc9463c9e926d5d37836d33",
  "url":"https://ip-ranges.amazonaws.com/ip-ranges.json"
}
```

create-time

Tanggal dan waktu pembuatan.

Notifikasi dapat dikirim tidak berurutan. Oleh karena itu, sebaiknya periksa stempel waktu untuk memastikan urutan yang benar.

synctoken

Waktu penerbitan, dalam format waktu jangka waktu Unix.

md5

Nilai hash kriptografis file `ip-ranges.json`. Anda dapat menggunakan nilai ini untuk memeriksa apakah file yang diunduh rusak.

url

Lokasi file `ip-ranges.json`. Untuk informasi selengkapnya, lihat the section called “Unduh”.

Anda dapat berlangganan untuk menerima pemberitahuan sebagai berikut.

Untuk berlangganan AWS Pemberitahuan rentang alamat IP

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home.
2. Di bilah navigasi, ubah Wilayah menjadi AS Timur (Virginia Utara), jika perlu. Anda harus memilih Wilayah ini karena notifikasi SNS tempat Anda berlangganan dibuat di Wilayah ini.

3. Di panel navigasi, pilih Langganan.
4. Pilih Buat langganan.
5. Di kotak dialog Create subscription (Buat langganan), lakukan hal berikut:
   a. Untuk Topic ARN (ARN Topik), salin Amazon Resource Name (ARN) berikut:

      ```
      arn:aws:sns:us-east-1:806199016981:AmazonIpSpaceChanged
      ```

   b. Untuk Protocol (Protokol), pilih protokol yang akan digunakan (misalnya, `Email`).
   c. Untuk Endpoint (Titik akhir), ketik titik akhir untuk menerima notifikasi (misalnya, alamat email Anda).
   d. Pilih Buat langganan.
6. Anda akan dihubungi di titik akhir yang Anda tentukan dan diminta untuk mengonfirmasi langganan Anda. Misalnya, jika Anda menentukan alamat email, Anda akan menerima pesan email dengan baris subjek `AWS Notification - Subscription Confirmation`. Ikuti petunjuk untuk mengonfirmasi langganan Anda.

Notifikasi tergantung pada ketersediaan titik akhir. Oleh karena itu, Anda mungkin ingin memeriksa file JSON secara berkala untuk memastikan bahwa Anda memiliki rentang terbaru. Untuk informasi selengkapnya tentang keandalan Amazon SNS, lihat https://aws.amazon.com/sns/faqs/#Reliability.

Jika Anda tidak ingin lagi menerima notifikasi ini, gunakan prosedur berikut untuk berhenti berlangganan.

Untuk berhenti berlangganan dari AWS Pemberitahuan rentang alamat IP

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home.
2. Di panel navigasi, pilih Langganan.
3. Pilih kotak centang untuk langganan.
4. Pilih Actions (Tindakan), Delete Subscriptions (Hapus Langganan).
5. Saat diminta konfirmasi, pilih Delete (Hapus).

Untuk informasi selengkapnya tentang Amazon SNS, lihat Panduan Developer Amazon Simple Notification Service.

Dukungan IPv6 untuk VPC Anda

Jika Anda memiliki VPC yang sudah ada yang hanya mendukung IPv4, dan sumber daya di subnet yang dikonfigurasi untuk menggunakan IPv4 saja, Anda dapat menambahkan dukungan IPv6 untuk VPC dan sumber daya Anda. VPC Anda dapat beroperasi dalam mode dual-stack — sumber daya Anda dapat berkomunikasi melalui IPv4, atau IPv6, atau keduanya. Komunikasi IPv4 dan IPv6 terpisah satu sama lain.

Anda tidak dapat menonaktifkan dukungan IPv4 untuk VPC dan subnet; ini adalah sistem pengalamatan IP default untuk Amazon VPC dan Amazon EC2.

Pertimbangan-pertimbangan

- Tidak ada jalur migrasi dari IPv4-only subnet ke IPv6-only subnet.
- Contoh ini mengasumsikan bahwa Anda memiliki VPC yang ada dengan subnet publik dan pribadi. Untuk informasi tentang membuat VPC baru untuk digunakan dengan IPv6, lihat. the section called “Buat VPC”
- Sebelum Anda mulai menggunakan IPv6, pastikan Anda telah membaca fitur pengalamatan IPv6 untuk Amazon VPC:. Bandingkan IPv4 dan IPv6

Daftar Isi

- Menambahkan dukungan IPv6 untuk VPC Anda
- Contoh konfigurasi VPC dual-stack

Menambahkan dukungan IPv6 untuk VPC Anda

Tabel berikut memberikan gambaran umum tentang proses untuk mengaktifkan IPv6 untuk VPC Anda.

Daftar Isi

- Langkah 1: Tautkan blok CIDR IPv6 dengan VPC dan subnet Anda
- Langkah 2: Perbarui tabel rute VPC Anda
- Langkah 3: Perbarui aturan grup keamanan Anda
- Langkah 4: Tetapkan alamat IPv6 ke instans Anda

Langkah	Catatan
Langkah 1: Tautkan blok CIDR IPv6 dengan VPC dan subnet Anda	Kaitkan blok Amazon-provided atau BYOIP IPv6 CIDR dengan VPC Anda dan dengan subnet Anda.
Langkah 2: Perbarui tabel rute VPC Anda	Memperbarui tabel rute Anda untuk rute lalu lintas IPv6 Anda. Untuk subnet publik, buat rute yang rute merutekan semua lalu lintas IPv6 dari subnet ke gateway internet. Untuk subnet privat, buat rute yang merutekan semua lalu lintas IPv6 yang terikat internet dari subnet ke gateway internet hanya keluar.
Langkah 3: Perbarui aturan grup keamanan Anda	Memperbarui aturan grup keamanan Anda untuk menyertakan aturan untuk alamat IPv6. Hal ini memungkinkan lalu lintas IPv6 mengalir ke dan dari instans Anda. Jika Anda telah membuat aturan ACL jaringan kustom untuk mengontrol aliran lalu lintas ke dan dari subnet Anda, Anda harus menyertakan aturan untuk lalu lintas IPv6.
Langkah 4: Tetapkan alamat IPv6 ke instans Anda	Anda menetapkan alamat IPv6 ke instans Anda dari rentang alamat IPv6 subnet Anda.

Langkah 1: Tautkan blok CIDR IPv6 dengan VPC dan subnet Anda

Anda dapat mengaitkan blok CIDR IPv6 dengan VPC Anda, dan kemudian mengaitkan blok CIDR `/64` dari rentang itu dengan masing-masing subnet.

Untuk mengaitkan Blok CIDR IPv6 dengan VPC

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih VPC Anda.
3. Pilih VPC Anda.
4. Pilih T ind akan, Edit CIDRs dan kemudian pilih Tambahkan IPv6 CIDR baru.

5. Pilih salah satu opsi berikut, lalu pilih Pilih CIDR:

   - Amazon-provided Blok IPv6 CIDR — Gunakan blok IPv6 CIDR dari kumpulan alamat IPv6 Amazon. Untuk Grup Perbatasan Jaringan, pilih grup yang mengiklan AWS kan alamat IP.
   - IPAM-allocated Blok IPv6 CIDR — Gunakan blok IPv6 CIDR dari kumpulan IPAM. https://docs.aws.amazon.com/vpc/latest/ipam/how-it-works-ipam.html Pilih kolam IPAM dan blok IPv6 CIDR.
   - IPv6 CIDR milik saya — Gunakan blok IPv6 CIDR dari kumpulan alamat IPv6 Anda (BYOIP). https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-byoip.html Pilih kumpulan alamat IPv6 dan blok IPv6 CIDR.

6. Pilih Tutup.

Untuk mengaitkan Blok CIDR IPv6 dengan subnet

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Pengguna.
3. Pilih subnet.
4. Pilih T ind akan, Edit IPv6 CIDR dan kemudian pilih Tambahkan IPv6 CIDR.
5. Edit blok CIDR sesuai kebutuhan (misalnya, ganti`00`).
6. Pilih Simpan.
7. Ulangi prosedur ini untuk subnet lain di VPC Anda.

Untuk informasi selengkapnya, lihat Blok IPv6 VPC CIDR.

Langkah 2: Perbarui tabel rute VPC Anda

Saat Anda mengaitkan blok IPv6 CIDR dengan VPC Anda, kami secara otomatis menambahkan rute lokal ke setiap tabel rute untuk VPC untuk mengizinkan lalu lintas IPv6 dalam VPC.

Anda harus memperbarui tabel rute untuk subnet publik Anda untuk mengaktifkan instance (seperti server web) untuk menggunakan gateway internet untuk lalu lintas IPv6. Anda juga harus memperbarui tabel rute untuk subnet pribadi Anda untuk mengaktifkan instans (seperti instance database) untuk menggunakan gateway internet khusus keluar untuk lalu lintas IPv6, karena gateway NAT tidak mendukung IPv6.

Untuk memperbarui tabel rute untuk subnet publik

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Pengguna. Pilih subnet publik. Pada tab Tabel rute, pilih ID tabel rute untuk membuka halaman detail untuk tabel rute.
3. Pilih tabel rute. Di tab Rute, pilih Edit rute.
4. Pilih Tambahkan rute. Pilih `::/0` tujuan. Pilih ID gateway internet untuk Target.
5. Pilih Simpan perubahan.

Untuk memperbarui tabel rute untuk subnet pribadi

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih gateway Egress-only internet. Pilih Buat gateway internet hanya keluar. Pilih VPC Anda dari VPC, lalu pilih Buat gateway internet hanya keluar.

   Untuk informasi selengkapnya, lihat Aktifkan lalu lintas IPv6 keluar menggunakan gateway internet khusus keluar.
3. Di panel navigasi, pilih Pengguna. Pilih subnet pribadi. Pada tab Tabel rute, pilih ID tabel rute untuk membuka halaman detail untuk tabel rute.
4. Pilih tabel rute. Di tab Rute, pilih Edit rute.
5. Pilih Tambahkan rute. Pilih `::/0` tujuan. Pilih ID gateway internet khusus keluar untuk Target.
6. Pilih Simpan perubahan.

> **Note**
>
> Tabel rute tidak dapat memiliki tujuan yang sama (:: /0) yang menunjuk ke gateway internet dan gateway internet khusus keluar secara bersamaan. Jika Anda menerima pesan kesalahan yang menyatakan “Ada rute ipv6 yang ada dengan hop berikutnya sebagai Gerbang internet” saat mengonfigurasi gateway internet khusus keluar, Anda harus terlebih dahulu menghapus rute IPv6 yang ada ke gateway internet sebelum menambahkan rute ke gateway internet khusus keluar.

Untuk informasi selengkapnya, lihat Opsi perutean contoh.

Langkah 3: Perbarui aturan grup keamanan Anda

Untuk mengaktifkan instans Anda untuk mengirim dan menerima lalu lintas melalui IPv6, Anda harus memperbarui aturan grup keamanan untuk menyertakan aturan untuk alamat IPv6. Misalnya, dalam contoh di atas, Anda dapat memperbarui server web grup keamanan (`sg-11aa22bb11aa22bb1`) untuk menambahkan aturan yang mengizinkan akses HTTP, HTTPS, dan SSH masuk dari alamat IPv6. Anda tidak perlu membuat perubahan apa pun pada aturan masuk untuk grup keamanan database Anda; aturan yang memungkinkan semua komunikasi dari `sg-11aa22bb11aa22bb1` mencakup komunikasi IPv6.

Untuk memperbarui aturan grup keamanan masuk

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Grup keamanan dan pilih grup keamanan server web Anda.
3. Di tab Aturan masuk, pilih Edit aturan masuk.
4. Untuk setiap aturan yang memungkinkan lalu lintas IPv4, pilih Tambahkan aturan dan konfigurasikan aturan untuk mengizinkan lalu lintas IPv6 yang sesuai. Misalnya, untuk menambahkan aturan yang memungkinkan semua lalu lintas HTTP melalui IPv6, pilih HTTP untuk Jenis dan `::/0` Sumber.
5. Setelah selesai menambahkan aturan, pilih S impan aturan.

Memperbarui aturan grup keamanan keluar

Saat Anda mengaitkan blok IPv6 CIDR dengan VPC Anda, kami secara otomatis menambahkan aturan keluar ke grup keamanan untuk VPC yang memungkinkan semua lalu lintas IPv6. Namun, jika Anda mengubah aturan keluar asal untuk grup keamanan Anda, aturan ini tidak secara otomatis ditambahkan, dan Anda harus menambahkan aturan keluar setara untuk lalu lintas IPv6.

Memperbarui aturan ACL jaringan Anda

Ketika Anda mengaitkan blok IPv6 CIDR dengan VPC, kami secara otomatis menambahkan aturan ke ACL jaringan default untuk mengizinkan lalu lintas IPv6. Namun, jika Anda mengubah ACL jaringan default atau jika Anda telah membuat ACL jaringan khusus, Anda harus menambahkan aturan untuk lalu lintas IPv6 secara manual. Untuk informasi selengkapnya, lihat Menambahkan dan menghapus aturan.

Langkah 4: Tetapkan alamat IPv6 ke instans Anda

Semua tipe instans generasi saat ini yang mendukung IPv6. Jika jenis instans Anda tidak mendukung IPv6, Anda harus mengubah ukuran instance ke jenis instans yang didukung sebelum Anda dapat menetapkan alamat IPv6. Proses yang akan Anda gunakan tergantung pada apakah jenis instance baru yang Anda pilih kompatibel dengan jenis instans saat ini. Untuk informasi selengkapnya, lihat Meng ubah jenis instans di Panduan Pengguna Amazon EC2. Jika Anda harus meluncurkan instance dari AMI baru untuk mendukung IPv6, Anda dapat menetapkan alamat IPv6 ke instance Anda selama peluncuran.

Setelah Anda memverifikasi apakah tipe instans Anda mendukung IPv6, Anda dapat menetapkan alamat IPv6 ke instans Anda menggunakan konsol Amazon EC2. Alamat IPv6 ditetapkan ke antarmuka jaringan utama (misalnya, eth0) untuk instance. Untuk informasi selengkapnya, lihat Men etapkan alamat IPv6 ke instance di Panduan Pengguna Amazon EC2.

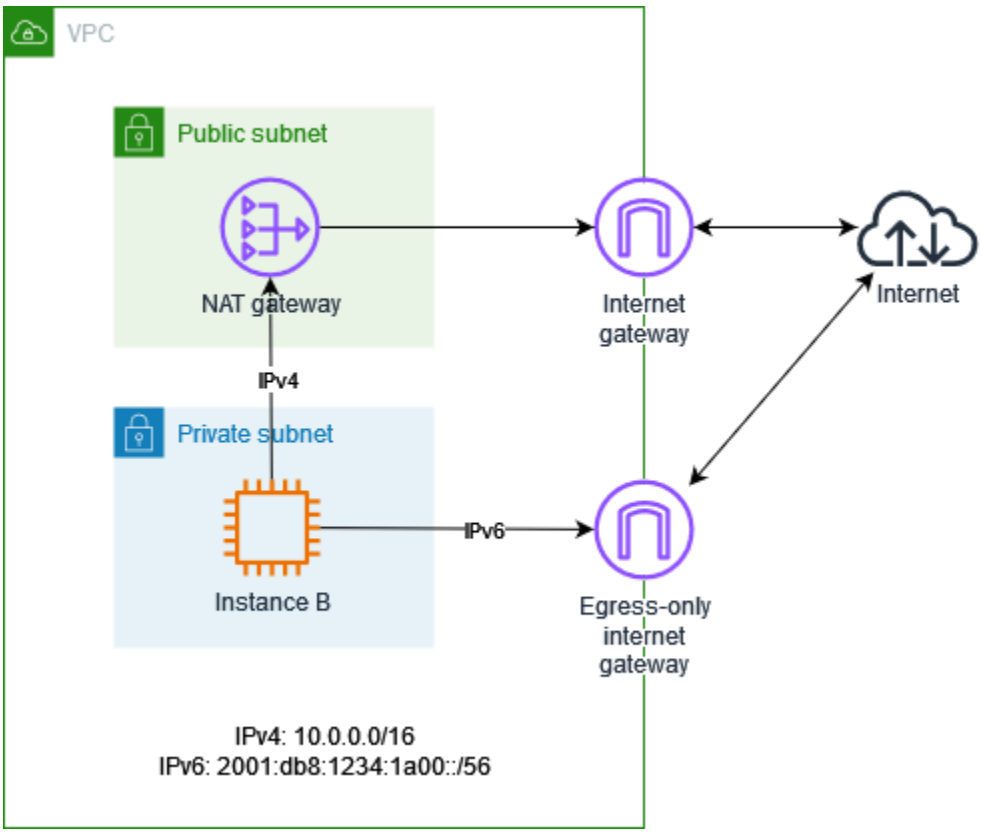
Anda dapat terhubung ke instans Windows menggunakan alamat IPv6-nya. Untuk informasi selengkapnya, lihat Menghubun gkan ke instans Linux menggunakan klien SSH di Panduan Pengguna Amazon EC2.

Jika Anda meluncurkan instans menggunakan AMI untuk versi sistem operasi saat ini, instans Anda dikonfigurasi untuk IPv6. Jika Anda tidak dapat melakukan ping ke alamat IPv6 dari instans Anda, lihat dokumentasi untuk sistem operasi Anda untuk mengonfigurasi IPv6.

Contoh konfigurasi VPC dual-stack

Dengan konfigurasi dual-stack, Anda dapat menggunakan alamat IPv4 dan IPv6 untuk komunikasi antara sumber daya di VPC Anda dan sumber daya melalui internet.

Diagram berikut merupakan arsitektur VPC Anda. VPC Anda memiliki subnet publik dan subnet pribadi. VPC dan subnet memiliki blok IPv4 CIDR dan blok IPv6 CIDR. Ada instance EC2 di subnet pribadi yang memiliki alamat IPv4 dan alamat IPv6. Instans dapat mengirim lalu lintas IPv4 keluar ke internet menggunakan gateway NAT dan lalu lintas IPv6 keluar ke internet menggunakan gateway internet khusus keluar.



Tabel rute untuk subnet publik

Berikut ini adalah tabel rute untuk subnet publik. Dua entri pertama adalah rute lokal. Entri ketiga mengirimkan semua lalu lintas IPv4 ke gateway internet. Perhatikan bahwa entri keempat diperlukan hanya jika Anda berencana untuk meluncurkan instans EC2 dengan alamat IPv6 di subnet publik.

Tujuan	Target
VPC IPv4 CIDR	lokal
VPC IPv6 CIDR	lokal
0.0.0. 0/0	*internet-gateway-id*
::/0	*internet-gateway-id*

Tabel rute untuk subnet pribadi

Berikut ini adalah tabel rute untuk subnet pribadi. Dua entri pertama adalah rute lokal. Entri ketiga mengirimkan semua lalu lintas IPv4 ke gateway NAT. Entri terakhir mengirimkan semua lalu lintas IPv6 ke gateway internet khusus keluar.

Tujuan	Target
VPC IPv4 CIDR	lokal
VPC IPv6 CIDR	lokal
0.0.0. 0/0	*nat-gateway-id*
::/0	*egress-only-gateway-id*

AWS Layanan yang mendukung IPv6

Komputer dan perangkat pintar menggunakan alamat IP untuk berkomunikasi satu sama lain melalui internet dan jaringan lainnya. Karena internet terus tumbuh, begitu juga kebutuhan akan alamat IP. Format yang paling umum untuk alamat IP adalah IPv4. Format baru untuk alamat IP adalah IPv6, yang menyediakan ruang alamat yang lebih besar daripada IPv4.

Layanan AWS dukungan untuk IPv6 mencakup dukungan untuk konfigurasi tumpukan ganda (IPv4 dan IPv6) atau konfigurasi hanya IPv6. Misalnya, virtual private cloud (VPC) adalah bagian yang terisolasi secara logis AWS Cloud di mana Anda dapat meluncurkan AWS sumber daya. Dalam VPC, Anda dapat membuat subnet yang hanya IPv4, dual stack, atau IPv6 saja.

Layanan AWS mendukung akses melalui titik akhir publik. Beberapa Layanan AWS juga mendukung akses menggunakan titik akhir pribadi yang didukung oleh AWS PrivateLink. Layanan AWS dapat mendukung IPv6 melalui titik akhir pribadi mereka bahkan jika mereka tidak mendukung IPv6 melalui titik akhir publik mereka. Titik akhir yang mendukung IPv6 dapat merespons kueri DNS dengan catatan AAAA.

Layanan yang mendukung IPv6

Tabel berikut mencantumkan Layanan AWS yang menyediakan dukungan tumpukan ganda, hanya dukungan IPv6, dan titik akhir yang mendukung IPv6. Kami akan memperbarui tabel ini saat kami merilis dukungan tambahan untuk IPv6. Untuk spesifik tentang bagaimana layanan mendukung IPv6, lihat dokumentasi untuk layanan tersebut.

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Titik akhir publik mendukung IPv6	Titik akhir pribadi mendukung IPv6 [1]
AWS Amplify	Ya	Tidak	Ya	
Amazon API Gateway	Ya	Tidak	Ya	Ya
AWS App Mesh	Ya	Ya	Ya	Tidak
AWS App Runner	Ya	Tidak	Ya	Ya
AWS AppConfig	Ya	Tidak	Ya	Ya
Penskalaan Otomatis Aplikasi	Tidak	Tidak	Ya	Ya
AWS Application Discovery Service	Ya	Tidak	Ya	Ya
Pengontrol Pemulihan Aplikasi (ARC)	Ya	Tidak	Ya	
WorkSpaces Aplikasi Amazon	Ya	Tidak	Tidak	Tidak
AWS AppSync [2]	Sebagian	Tidak	Sebagian	Ya
Amazon Athena	Ya	Tidak	Ya	Ya
AWS Audit Manager	Tidak	Tidak	Ya	Ya
Amazon Aurora	Ya	Tidak	Ya	Tidak
Amazon Aurora DSQL	Tidak	Tidak	Ya	Ya
AWS Auto Scaling	Tidak	Tidak	Ya	Ya

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Titik akhir publik mendukung IPv6	Titik akhir pribadi mendukung IPv6 1
AWS B2B Pertukaran Data	Ya	Tidak	Ya	Ya
AWS Backup	Ya	Tidak	Ya	Ya
AWS Batch	Ya	Tidak	Ya	Ya
Amazon Bedrock	Tidak	Tidak	Ya	Ya
AWS Manajemen Penagihan dan Biaya Ekspor Data	Ya	Tidak	Ya	Ya
AWS Manajemen Penagihan dan Biaya Kalkulator Harga	Ya	Tidak	Ya	Ya
AWS Billing Conductor	Ya	Tidak	Ya	Ya
AWS Budgets	Ya	Tidak	Ya	
Amazon Braket	Ya	Ya	Ya	Ya
AWS Certificate Manager	Ya	Tidak	Ya	Tidak
Amazon Chime SDK	Ya	Tidak	Ya	
Amazon Comprehend	Ya	Ya	Ya	Ya
AWS Clean Rooms	Ya	Ya	Ya	Ya
AWS Clean Rooms ML	Ya	Ya	Ya	Ya
AWS Cloud9	Ya	Tidak	Ya	

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Titik akhir publik mendukung IPv6	Titik akhir pribadi mendukung IPv6 1
AWS Cloud Control API	Ya	Tidak	Ya	Ya
CloudFormation	Tidak	Tidak	Ya	Ya
Amazon CloudFront	Ya	Ya	Ya	
AWS CloudHSM	Ya	Tidak	Ya	Ya
AWS CloudTrail	Ya	Tidak	Ya	Ya
Amazon CloudWatch	Ya	Ya	Ya	Ya
Wawasan CloudWatch Aplikasi Amazon	Tidak	Tidak	Ya	Ya
Monitor CloudWatch Internet Amazon	Tidak	Tidak	Ya	Ya
CloudWatch Log Amazon	Ya	Ya	Ya	Ya
Manajer Akses CloudWatch Observabilitas Amazon	Ya	Ya	Ya	
Amazon CloudWatch Synthetics	Ya	Tidak	Ya	Ya
AWS Cloud Map	Ya	Ya	Ya	Ya
AWS Awan WAN	Ya	Tidak	Ya	Tidak
AWS CodeArtifact	Ya	Tidak	Ya	Ya

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Titik akhir publik mendukung IPv6	Titik akhir pribadi mendukung IPv6 1
Connect Profil Pelanggan Pelanggan	Ya	Tidak	Ya	Ya
AWS CodeBuild	Tidak	Tidak	Ya	Ya
AWS CodeCommit	Tidak	Tidak	Ya	Ya
AWS CodeDeploy	Tidak	Tidak	Ya	Ya
AWS Compute Optimizer	Tidak	Tidak	Ya	Ya
Amazon Comprehend Medical	Tidak	Tidak	Ya	Ya
Amazon CodeGuru Profiler	Ya	Tidak	Ya	Ya
Amazon Cognito	Ya	Tidak	Ya	
AWS Config	Tidak	Tidak	Ya	Ya
AWS Control Tower	Tidak	Tidak	Ya	Ya
AWS Cost Explorer	Ya	Tidak	Ya	Ya
Hub Optimisasi Biaya AWS	Ya	Tidak	Ya	Ya
AWS Data Exchange	Tidak	Tidak	Ya	Ya
Amazon Data Firehose	Tidak	Tidak	Ya	Ya
Amazon Data Lifecycle Manager	Ya	Tidak	Ya	Ya

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Titik akhir publik mendukung IPv6	Titik akhir pribadi mendukung IPv6 1
AWS Database Migration Service	Ya	Tidak	Tidak	Ya
AWS DataSync	Ya	Ya	Ya	Ya
Amazon DataZone	Tidak	Tidak	Ya	Ya
AWS Deadline Cloud	Ya	Tidak	Ya	Ya
Amazon Detective	Ya	Ya	Ya	
Direct Connect	Ya	Ya	Tidak	Ya
Directory Service	Tidak	Tidak	Ya	Ya
API langsung Amazon EBS	Ya	Tidak	Ya	Ya
Amazon EC2	Ya	Ya	Ya	Tidak
EC2 Image Builder	Ya	Ya	Ya	Ya
Amazon ECR	Ya	Tidak	Ya	Tidak
Amazon ECS	Ya	Ya	Ya	Ya
Amazon EFS	Ya	Ya	Ya	Ya
Amazon EKS	Sebagian	Sebagian	Ya	Ya
Amazon EMR	Tidak	Tidak	Ya	Ya
AWS Elastic Beanstalk	Ya	Tidak	Ya	Ya
AWS Elastic Disaster Recovery	Tidak	Tidak	Ya	Ya

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Titik akhir publik mendukung IPv6	Titik akhir pribadi mendukung IPv6 [1]
Elastic Load Balancing	Sebagian	Sebagian	Ya	Tidak
Amazon ElastiCache	Ya	Ya	Tidak	Ya
AWS Elemental MediaConvert	Tidak	Tidak	Ya	Ya
AWS Elemental MediaConnect	Ya	Ya	Ya	Sebagian
AWS Pesan Pengguna Akhir Sosial	Ya	Tidak	Ya	Tidak
Resolusi Entitas AWS	Ya	Tidak	Ya	Ya
Amazon EventBridge	Tidak	Tidak	Ya	Ya
AWS Fargate	Ya	Tidak	Ya	Ya
Amazon FSx	Tidak	Tidak	Ya	Ya
GameLift Aliran Amazon	Ya	Tidak	Ya	Ya
AWS Global Accelerator	Ya	Tidak	Ya	
AWS Glue	Ya	Tidak	Tidak	Ya
AWS Glue DataBrew	Tidak	Tidak	Ya	Ya
Grafana Dikelola Amazon [3]	Ya	Tidak	Ya	Ya
AWS Ground Station [4]	Ya	Tidak	Ya	Ya
Amazon GuardDuty	Tidak	Tidak	Ya	Ya
AWS HealthImaging	Tidak	Tidak	Ya	Ya

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Titik akhir publik mendukung IPv6	Titik akhir pribadi mendukung IPv6 1
AWS HealthLake	Tidak	Tidak	Ya	Ya
AWS HealthOmics	Tidak	Tidak	Ya	Ya
AWS Identity and Access Management (IAM)	Ya	Ya	Ya	Tidak
AWS Penganalisis Akses IAM	Ya	Tidak	Ya	Ya
AWS IAM Identity Center	Ya	Tidak	Ya	
AWS Peran IAM Di Mana Saja	Tidak	Tidak	Ya	Ya
Amazon Inspector	Ya	Ya	Ya	Ya
Layanan Video Interaktif Amazon (IVS) 5	Ya	Tidak	Ya	Ya
AWS IoT Core	Ya	Tidak	Ya	Ya
AWS IoT Device Defender	Ya	Tidak	Ya	Tidak
AWS IoT Device Management	Ya	Tidak	Ya	Tidak
AWS IoT FleetWise	Ya	Tidak	Ya	Ya
AWS IoT Greengrass	Ya	Tidak	Ya	Tidak
AWS IoT SiteWise	Ya	Tidak	Ya	Ya

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Titik akhir publik mendukung IPv6	Titik akhir pribadi mendukung IPv6 1
AWS IoT TwinMaker	Ya	Tidak	Ya	Ya
AWS IoT Wireless	Ya	Tidak	Ya	Ya
Amazon Kendra	Tidak	Tidak	Ya	Tidak
AWS Key Management Service	Ya	Sebagian	Ya	Ya
Amazon Keyspaces	Ya	Ya	Ya	Ya
Amazon Keyspaces CDC streams	Ya	Ya	Ya	Ya
Amazon Kinesis Data Streams	Ya	Tidak	Ya	Ya
AWS Lake Formation	Tidak	Tidak	Tidak	Ya
AWS Lambda	Ya	Tidak	Ya	Ya
AWS Launch Wizard	Tidak	Tidak	Ya	Ya
AWS License Manager	Tidak	Tidak	Ya	Ya
Amazon Lightsail	Ya	Ya	Ya	Ya
Amazon Location Service	Tidak	Tidak	Ya	Ya
Amazon MQ	Tidak	Tidak	Ya	Ya
Amazon MWAA	Tidak	Tidak	Ya	Ya
Amazon Macie	Ya	Tidak	Ya	Ya

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Titik akhir publik mendukung IPv6	Titik akhir pribadi mendukung IPv6 1
AWS Mainframe Modernization	Ya	Tidak	Ya	Ya
Amazon Managed Grafana	Tidak	Tidak	Ya	Ya
Amazon Managed Service for Prometheus	Ya	Tidak	Ya	Ya
Orkestrator AWS Migration Hub	Tidak	Tidak	Ya	Ya
AWS Network Firewall	Ya	Ya	Tidak	Ya
AWS Network Manager	Ya	Tidak	Ya	Tidak
OpenSearch Layanan Amazon	Ya	Tidak	Ya	
AWS Organizations	Ya	Tidak	Ya	Ya
AWS Outposts	Tidak	Tidak	Ya	Ya
Amazon Personalize	Ya	Tidak	Ya	Ya
Amazon Pinpoint	Ya	Tidak	Ya	Ya
Amazon Polly	Ya	Tidak	Ya	Ya
Daftar Harga AWS	Tidak	Tidak	Ya	Tidak
AWS Private Certificate Authority	Ya	Tidak	Ya	Ya

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Titik akhir publik mendukung IPv6	Titik akhir pribadi mendukung IPv6 1
AWS Private CA Konektor untuk Active Directory	Ya	Tidak	Ya	Ya
AWS Private CA Konektor untuk SCEP	Ya	Tidak	Ya	Ya
AWS PrivateLink	Ya	Ya	Ya	
Amazon Q Bisnis	Tidak	Tidak	Ya	Tidak
Amazon RDS	Ya	Tidak	Ya	Tidak
API Amazon RDS Data	Tidak	Tidak	Ya	Ya
Wawasan Performa Amazon RDS	Tidak	Tidak	Ya	Ya
Amazon Redshift	Ya	Tidak	Ya	
Amazon Rekognition	Tidak	Tidak	Ya	Ya
Tempat Sampah Daur Ulang	Ya	Tidak	Ya	Ya
AWS re:Post Privat	Ya	Tidak	Ya	Ya
AWS Resource Access Manager	Ya	Tidak	Ya	Ya
Penjelajah Sumber Daya AWS	Ya	Tidak	Ya	Tidak
AWS Resource Groups	Ya	Ya	Ya	Ya

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Titik akhir publik mendukung IPv6	Titik akhir pribadi mendukung IPv6 1
AWS Resource Groups Tagging API	Ya	Ya	Ya	Ya
Amazon Route 53	Ya	Ya	Ya	Ya
Amazon S3	Ya	Tidak	Ya	Tidak
Amazon S3 on Outposts	Tidak	Tidak	Ya	Tidak
Amazon SageMaker	Tidak	Tidak	Ya	Ya
AWS Secrets Manager	Ya	Tidak	Ya	Ya
AWS Security Hub	Tidak	Tidak	Ya	Ya
Amazon Security Lake	Ya	Tidak	Ya	Ya
AWS Security Token Service	Ya	Tidak	Ya	Ya
AWS Service Catalog	Tidak	Tidak	Ya	Ya
AWS Shield	Ya	Ya	Tidak	Ya
Layanan Email Sederhana Amazon	Ya	Tidak	Ya	Ya
Layanan Notifikasi Sederhana Amazon	Ya	Tidak	Ya	Ya
Amazon Simple Queue Service	Ya	Tidak	Ya	Ya
Layanan Alur Kerja Sederhana Amazon	Ya	Tidak	Ya	Ya

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Titik akhir publik mendukung IPv6	Titik akhir pribadi mendukung IPv6 [1]
AWS Site-to-Site VPN	Ya	Tidak	Ya	Tidak
AWS Snow Family	Tidak	Tidak	Ya	
AWS Step Functions	Ya	Tidak	Ya	Ya
AWS Storage Gateway	Ya	Ya	Ya	Ya
AWS Systems Manager	Tidak	Tidak	Ya	Ya
Manajer Insiden AWS Systems Manager	Tidak	Tidak	Ya	Ya
AWS Systems Manager untuk SAP	Tidak	Tidak	Ya	Ya
Amazon Textract	Tidak	Tidak	Ya	Ya
Amazon Timestream	Tidak	Tidak	Ya	Ya
Amazon Transcribe	Ya	Ya	Ya	Ya
AWS Transfer Family [6]	Ya	Tidak	Ya	Ya
AWS Transit Gateway	Ya	Tidak	Ya	Tidak
Amazon Translate	Ya	Ya	Ya	Ya
AWS Trusted Advisor	Tidak	Tidak	Ya	Ya
Notifikasi Pengguna AWS	Tidak	Tidak	Ya	Ya
Izin Terverifikasi Amazon	Ya	Tidak	Ya	Ya

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Titik akhir publik mendukung IPv6	Titik akhir pribadi mendukung IPv6 [1]
VMware Cloud aktif AWS	Tidak	Tidak	Ya	Ya
Amazon VPC	Ya	Ya	Ya	Tidak
Kisi VPC Amazon	Tidak	Tidak	Ya	Ya
AWS WAF	Ya	Ya	Tidak	
AWS WAFV2	Tidak	Tidak	Ya	Ya
AWS Well-Architected Tool	Tidak	Tidak	Ya	Ya
Amazon WorkMail	Tidak	Tidak	Ya	Ya
Amazon WorkSpaces	Ya	Tidak	Ya	Ya
AWS X-Ray	Ya	Tidak	Ya	Ya

[1] Sel kosong menunjukkan bahwa layanan tidak terintegrasi dengan AWS PrivateLink.

[2] Entri ini mewakili dukungan IPv6 untuk operasi konfigurasi AWS AppSync GraphLQL dan Event API, melalui SDK API.AWS AppSync IPv6 tidak didukung untuk koneksi klien ke GraphQL AWS AppSync dan Event API yang dikelola pelanggan.

[3] Entri ini mewakili dukungan IPv6 untuk operasi manajemen ruang kerja Grafana, seperti memperbarui ruang kerja dan izin ruang kerja. Tidak ada dukungan IPv6 untuk operasi ruang kerja Grafana umum, seperti membuat dan mengedit dasbor atau menanyakan sumber data.

[4] Entri ini mewakili dukungan IPv6 untuk operasi pesawat AWS Ground Station kontrol, seperti memanggil API.AWS Ground Station IPv6 tidak didukung oleh bidang AWS Ground Station data, jadi pastikan sumber daya yang Anda kirimkan data (seperti instans Amazon EC2) dapat diakses melalui IPv4.

[5] Entri ini mewakili dukungan IPv6 untuk operasi pesawat kontrol Amazon IVS, seperti memanggil titik akhir IVS.

[6] Untuk detail lebih lanjut tentang dukungan IPv6 di AWS Transfer Family, kunjungi batasan IPv6.

Dukungan IPv6 tambahan

Hitung

- Amazon EC2 mendukung peluncuran instans berdasarkan Sistem Nitro ke dalam subnet. IPv6-only
- Amazon EC2 menyediakan titik akhir IPv6 untuk Layanan Metadata Instans (IMDS) dan Layanan Sinkronisasi Waktu Amazon.

Pengembangan Game

- Amazon GameLift Streams mendukung streaming melalui IPv6 pada runtime Microsoft Windows Server 2022 Base.

Jaringan dan Pengiriman Konten

- Amazon VPC mendukung pembuatan IPv6-only subnet.
- Amazon VPC membantu sumber daya IPv6 berkomunikasi dengan AWS sumber daya IPv4 dengan mendukung DNS64 di subnet dan NAT64 di gateway NAT Anda.

Keamanan, Identitas, dan Kepatuhan

- Amazon Detective mendukung alamat IPv6 dalam temuan terkait jaringan dan profil entitas.
- AWS Identity and Access Management (IAM) mendukung alamat IPv6 dalam kebijakan berbasis identitas IAM.
- Amazon Macie mendukung alamat IPv6 dalam informasi identitas pribadi (PII).
- Amazon Security Lake mendukung alamat IPv6 di semua operasi pada sumber log dan pelanggan.

Pengelolaan dan Tata Kelola

- AWS CloudTrail catatan termasuk sumber informasi IPv6.
- AWS CLI v2 mendukung pengunduhan melalui koneksi IPv6 untuk IPv6-only klien.

Pelajari selengkapnya

- IPv6 di AWS
- Dual Stack dan Arsitektur Referensi VPC IPv6-only Amazon (PDF)

Mengonfigurasikan cloud privat virtual

Amazon Virtual Private Cloud (VPC) adalah blok bangunan mendasar, memungkinkan Anda untuk menyediakan jaringan virtual yang terisolasi secara logis di dalam cloud. AWS Dengan membuat VPC Anda sendiri, Anda mendapatkan kontrol penuh atas lingkungan jaringan, termasuk kemampuan untuk menentukan rentang alamat IP, subnet, tabel perutean, dan opsi konektivitas.

AWS Akun Anda berisi VPC default untuk setiap AWS Wilayah. VPC default ini hadir pra-konfigurasi dengan pengaturan yang menjadikannya opsi yang nyaman untuk meluncurkan sumber daya dengan cepat. Namun, VPC default mungkin tidak selalu selaras dengan kebutuhan jaringan jangka panjang Anda. Di sinilah membuat VPC tambahan bisa menguntungkan.

Membuat VPC tambahan menawarkan beberapa keuntungan dibandingkan mengandalkan VPC default yang disediakan dengan setiap akun baru. AWS Dengan VPC yang dikelola sendiri, Anda dapat merancang topologi jaringan agar sesuai dengan kebutuhan spesifik Anda, baik itu menerapkan aplikasi multi-tier, menghubungkan ke sumber daya lokal, atau memisahkan beban kerja berdasarkan departemen atau unit bisnis.

Selain itu, membuat beberapa VPC dapat memungkinkan keamanan dan isolasi yang lebih besar antara berbagai aplikasi atau unit bisnis Anda. Setiap VPC bertindak sebagai jaringan virtual terpisah, memungkinkan Anda menerapkan kebijakan keamanan, kontrol akses, dan konfigurasi perutean yang berbeda yang disesuaikan dengan setiap lingkungan.

Pada akhirnya, keputusan untuk menggunakan VPC default atau membuat satu (atau lebih) VPC kustom harus didasarkan pada persyaratan aplikasi spesifik Anda, kebutuhan keamanan, dan tujuan skalabilitas jangka panjang. Menginvestasikan waktu untuk merancang infrastruktur VPC Anda dengan cermat dapat membayar dividen dalam bentuk fondasi jaringan cloud yang kuat, aman, dan mudah beradaptasi.

Daftar Isi

- Dasar-dasar VPC
- Opsi konfigurasi VPC
- VPC default
- Buat VPC
- Visualisasikan sumber daya di VPC Anda
- Tambahkan atau hapus blok CIDR dari VPC Anda

- Opsi DHCP ditetapkan di Amazon VPC
- Atribut DNS untuk VPC Anda
- Penggunaan Alamat Jaringan untuk VPC Anda
- Bagikan subnet VPC Anda dengan akun lain
- Memperluas VPC ke Zona Lokal, Zona Panjang Gelombang, atau Pos Terdepan
- Hapus VPC Anda
- Hasilkan infrastruktur sebagai kode dari tindakan konsol VPC Anda dengan Console-to-Code

Dasar-dasar VPC

VPC mencakup semua Availability Zone di suatu Wilayah. Setelah membuat VPC, Anda dapat menambahkan satu atau beberapa subnet di setiap Availability Zone. Untuk informasi selengkapnya, lihat Subnet.

Daftar Isi

- Rentang alamat IP VPC
- Diagram VPC
- Sumber daya VPC

Rentang alamat IP VPC

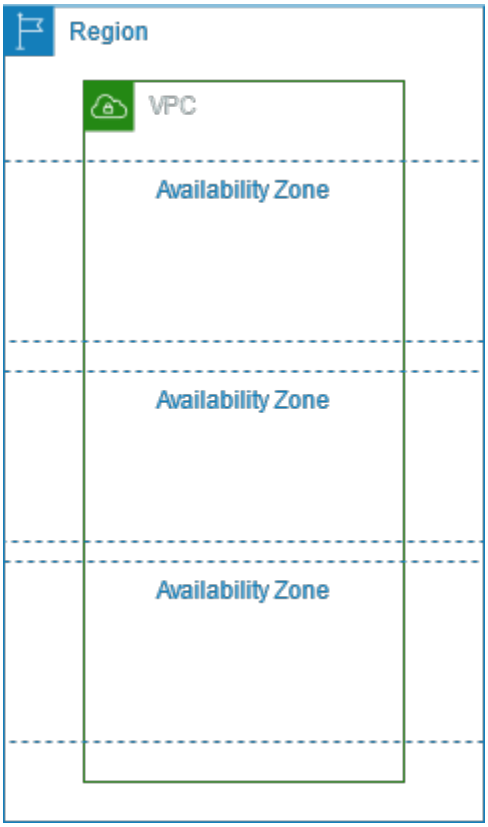
Saat Anda membuat VPC, Anda menentukan alamat IP-nya sebagai berikut:

- Hanya IPv4 - VPC memiliki blok CIDR IPv4 tetapi tidak memiliki blok CIDR IPv6.
- Dual stack — VPC memiliki blok IPv4 CIDR dan blok IPv6 CIDR.

Untuk informasi selengkapnya, lihat Pengalamatan IP untuk VPC dan subnet Anda.

Diagram VPC

Diagram berikut menunjukkan VPC tanpa sumber daya VPC tambahan. Misalnya konfigurasi VPC, lihat. Contoh



Sumber daya VPC

Setiap VPC secara otomatis dilengkapi dengan sumber daya berikut:

- Set opsi DHCP default
- ACL jaringan default
- Grup keamanan default
- Tabel rute utama

Anda dapat membuat sumber daya berikut untuk VPC Anda:

- ACL Jaringan
- Tabel rute khusus
- Grup keamanan
- Gerbang internet
- Gateway NAT

Opsi konfigurasi VPC

Anda dapat menentukan opsi konfigurasi berikut saat membuat VPC.

Zona Ketersediaan

Pusat data diskrit dengan daya redundan, jaringan, dan konektivitas di suatu Wilayah. AWS Anda dapat menggunakan beberapa AZ untuk mengoperasikan aplikasi produksi dan database yang lebih tersedia, toleran terhadap kesalahan, dan skalabel daripada yang mungkin dilakukan dari satu pusat data. Jika Anda mempartisi aplikasi yang berjalan di subnet di seluruh AZ, Anda lebih terisolasi dan terlindungi dari masalah seperti pemadaman listrik, sambaran petir, tornado, dan gempa bumi.

Blok CIDR

Anda harus menentukan rentang alamat IP untuk VPC dan subnet Anda. Untuk informasi selengkapnya, lihat Pengalamatan IP untuk VPC dan subnet Anda.

Opsi DNS

Jika Anda memerlukan nama host DNS IPv4 publik untuk instans EC2 yang diluncurkan ke subnet Anda, Anda harus mengaktifkan kedua opsi DNS. Untuk informasi selengkapnya, lihat Atribut DNS untuk VPC Anda.

- Aktifkan nama host DNS: Instans EC2 yang diluncurkan di VPC menerima nama host DNS publik yang sesuai dengan alamat IPv4 publiknya.
- Aktifkan resolusi DNS: Resolusi DNS untuk nama host DNS pribadi disediakan untuk VPC oleh server DNS Amazon, yang disebut Resolver Route 53.

gateway internet

Menghubungkan VPC Anda ke Internet. Contoh di subnet publik dapat mengakses internet karena tabel rute subnet berisi rute yang mengirimkan lalu lintas menuju internet ke gateway internet. Jika server tidak perlu dijangkau langsung dari internet, Anda tidak boleh menyebarkannya ke subnet publik. Untuk informasi lebih lanjut, lihat gateway Internet.

Nama

Nama yang Anda tentukan untuk VPC dan sumber daya VPC lainnya digunakan untuk membuat tag Nama. Jika Anda menggunakan fitur pembuatan otomatis tag nama di konsol, nilai tag memiliki format *name* -*resource*.

Gateway NAT

Mengaktifkan instance di subnet pribadi untuk mengirim lalu lintas keluar ke internet, tetapi mencegah sumber daya di internet terhubung ke instance. Dalam produksi, kami menyarankan Anda menerapkan gateway NAT di setiap AZ aktif. Untuk informasi selengkapnya, silakan lihat Gateway NAT.

Tabel rute

Berisi seperangkat aturan, yang disebut rute, yang menentukan ke mana lalu lintas jaringan dari subnet atau gateway Anda diarahkan. Untuk informasi selengkapnya, lihat Tabel rute.

Subnet

Rentang alamat IP dalam VPC Anda. Anda dapat meluncurkan AWS sumber daya, seperti instans EC2, ke subnet Anda. Setiap subnet berada sepenuhnya dalam satu Availability Zone. Dengan meluncurkan instans di setidaknya dua Availability Zone, Anda dapat melindungi aplikasi Anda dari kegagalan satu Availability Zone.

Subnet publik memiliki rute langsung ke gateway internet. Sumber daya dalam subnet publik dapat mengakses internet publik. Subnet pribadi tidak memiliki rute langsung ke gateway internet. Sumber daya dalam subnet pribadi memerlukan komponen lain, seperti perangkat NAT, untuk mengakses internet publik.

Untuk informasi selengkapnya, lihat Subnet.

Penghunian

Opsi ini menentukan apakah instans EC2 yang Anda luncurkan ke VPC akan berjalan pada perangkat keras yang dibagikan dengan perangkat keras lain Akun AWS atau pada perangkat keras yang didedikasikan untuk penggunaan Anda saja. Jika Anda memilih penyewaan VPC yang *`Default`* akan menjadi, instans EC2 yang diluncurkan ke VPC ini akan menggunakan atribut penyewaan yang ditentukan saat Anda meluncurkan instance -- Untuk informasi selengkapnya, lihat Meluncurkan instance menggunakan parameter yang ditentukan dalam Panduan Pengguna Amazon EC2. Jika Anda memilih penyewaan VPC, instans akan selalu berjalan sebagai Instans Khusus pada perangkat keras yang didedikasikan untuk Anda gunakan. `Dedicated` Jika Anda menggunakan AWS Outposts, Outpost Anda memerlukan konektivitas pribadi; Anda harus menggunakan tenancy. `Default`

VPC default

Saat Anda mulai menggunakan Amazon VPC, Anda memiliki VPC default di setiap AWS Wilayah. VPC default dilengkapi dengan subnet publik di setiap Zona Ketersediaan, gateway internet, dan pengaturan untuk mengaktifkan resolusi DNS. Oleh karena itu, Anda dapat segera mulai meluncurkan instans Amazon EC2 ke VPC default. Anda juga dapat menggunakan layanan seperti Elastic Load Balancing, Amazon RDS, dan Amazon EMR di VPC default Anda.

VPC default cocok untuk memulai dengan cepat dan untuk meluncurkan instans publik seperti blog atau situs web sederhana. Anda dapat mengubah komponen VPC default Anda sesuai kebutuhan.

Anda dapat menambahkan subnet ke VPC default Anda. Untuk informasi selengkapnya, lihat the section called “Membuat subnet”.

Daftar Isi

- Komponen VPC default
- Subnet default
- Bekerja dengan VPC default dan subnet default

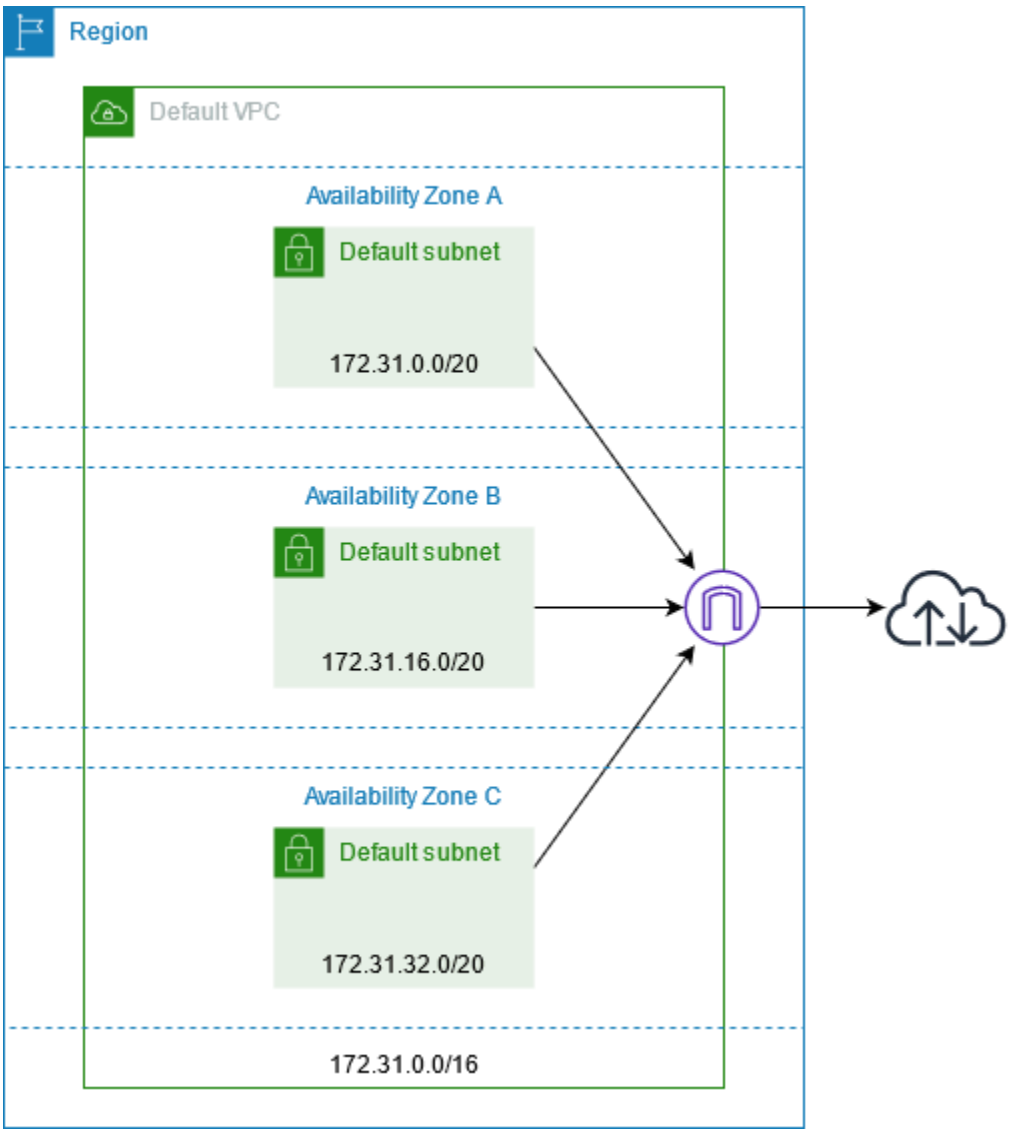
Komponen VPC default

Ketika kita membuat VPC default, kita melakukan hal berikut untuk menyiapkannya untuk Anda:

- Membuat VPC dengan ukuran blok CIDR IPv4 `/16` (`172.31.0.0/16`). Tindakan ini menyediakan 65.536 alamat IPv4 privat.
- Membuat subnet default ukuran `/20` di setiap Availability Zone. Tindakan ini menyediakan hingga 4.096 alamat per subnet, beberapa di antaranya disimpan untuk kami gunakan.
- Membuat gateway internet dan menghubungkannya ke VPC default Anda.
- Menambahkan rute ke tabel rute utama yang mengarahkan semua lalu lintas (`0.0.0.0/0`) ke gateway internet.
- Membuat grup keamanan default dan mengaitkannya dengan VPC default Anda.
- Membuat daftar kontrol akses (ACL) jaringan default dan mengaitkannya dengan VPC default Anda.
- Kaitkan opsi DHCP default yang ditetapkan untuk AWS akun Anda dengan VPC default Anda.

> **Note**
>
> - Amazon membuat sumber daya di atas atas nama Anda. Kebijakan IAM tidak berlaku untuk tindakan ini karena Anda tidak melakukan tindakan ini. Misalnya, jika Anda memiliki kebijakan IAM yang menolak kemampuan untuk menelepon CreateInternetGateway, dan kemudian Anda memang CreateDefaultVpc gil, gateway internet di VPC default masih dibuat. Untuk mencegah Amazon membuat gateway internet, Anda harus menolak CreateDefaultVpc dan CreateInternetGateway.
> - Untuk memblokir semua lalu lintas ke dan dari gateway internet di akun Anda, lihatBlokir akses publik ke VPC dan subnet.

Gambar berikut menggambarkan komponen kunci yang kita siapkan untuk VPC default.



Tabel berikut menunjukkan rute di tabel rute utama untuk VPC default.

Tujuan	Target
172.31.0. 0/16	lokal
0.0.0. 0/0	*internet_gateway_id*

Anda dapat menggunakan VPC default sebagaimana Anda akan menggunakan VPC lain:

- Menambahkan subnet nondefault tambahan.
- Mengubah tabel rute utama.

- Menambahkan tabel rute tambahan.
- Mengaitkan grup keamanan tambahan.
- Memperbarui aturan grup keamanan default.
- Tambahkan AWS Site-to-Site VPN koneksi.
- Menambahkan lebih banyak blok CIDR IPv4.
- Mengakses VPC di Wilayah terpencil dengan menggunakan gateway Direct Connect. Untuk informasi tentang opsi gateway Direct Connect, lihat Gateway Direct Connect di Panduan Pengguna AWS Direct Connect .

Anda dapat menggunakan subnet default sebagaimana Anda menggunakan subnet lainnya; menambahkan tabel rute kustom dan mengatur ACL jaringan. Anda juga dapat menentukan subnet default tertentu ketika Anda meluncurkan instans EC2.

Atau, Anda dapat memilih mengaitkan blok CIDR IPv6 dengan VPC default Anda.

Subnet default

Secara default, suatu subnet default adalah subnet publik, karena tabel rute utama mengirimkan lalu lintas subnet yang ditujukan untuk internet ke gateway internet. Anda dapat membuat subnet default menjadi subnet pribadi dengan menghapus rute dari tujuan 0.0.0. 0/0 ke gateway internet. Namun, jika Anda melakukan ini, tidak ada instans EC2 berjalan di subnet tersebut yang dapat mengakses internet.

Instans yang Anda luncurkan ke subnet default menerima alamat IPv4 publik dan alamat IPv4 privat, dan nama host DNS publik dan privat. Instans yang Anda luncurkan ke subnet nondefault di VPC default tidak menerima alamat IPv4 publik atau nama host DNS. Anda dapat mengubah perilaku pengalamatan IP publik default subnet Anda. Untuk informasi selengkapnya, lihat Ubah atribut pengalamatan IP subnet Anda.

Dari waktu ke waktu, AWS dapat menambahkan Zona Ketersediaan baru ke Wilayah. Sebagian besar kami secara otomatis membuat subnet default baru di Availability Zone ini untuk VPC default Anda dalam beberapa hari. Namun, jika Anda membuat perubahan pada VPC default Anda, kami tidak akan menambahkan subnet default baru. Jika Anda ingin subnet default untuk Availability Zone baru, Anda dapat membuat subnet default sendiri. Untuk informasi selengkapnya, lihat Membuat subnet default.

Bekerja dengan VPC default dan subnet default

Bagian ini menjelaskan cara bekerja dengan VPC default dan subnet default.

Daftar Isi

- Menampilkan VPC default dan subnet default
- Membuat VPC default
- Membuat subnet default
- Menampilkan subnet default dan VPC default

Menampilkan VPC default dan subnet default

Anda dapat menampilkan VPC dan subnet default Anda menggunakan konsol Amazon VPC atau baris perintah.

Untuk melihat VPC dan subnet default Anda menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih VPC Anda.
3. Di kolom VPC Default, cari nilai Ya. Perhatikan ID dari VPC default.
4. Di panel navigasi, pilih Pengguna.
5. Di bilah pencarian, ketik ID dari VPC default. Subnet yang dikembalikan adalah subnet di VPC default Anda.
6. Untuk memverifikasi subnet mana yang merupakan subnet default, cari nilai Ya dalam kolom Subnet Default.

Untuk mendeskripsikan VPC default Anda menggunakan baris perintah

- Gunakan describe-vpcs (AWS CLI)
- Gunakan Get-EC2Vpc (AWS Tools for Windows PowerShell)

Gunakan perintah-perintah tersebut dengan filter `isDefault` dan tetapkan nilai filter ke `true`.

Untuk mendeskripsikan subnet default Anda menggunakan baris perintah

- Gunakan describe-subnets (AWS CLI)

- Gunakan Get-EC2Subnet (AWS Tools for Windows PowerShell)

Gunakan perintah-perintah tersebut dengan filter `vpc-id` dan tetapkan nilai filter ke ID VPC default. Dalam output, bidang `DefaultForAz` diatur ke `true` untuk subnet default.

Membuat VPC default

Jika Anda menghapus VPC default, Anda dapat membuat yang baru. Anda tidak dapat memulihkan VPC default sebelumnya yang Anda hapus, dan Anda tidak dapat menandai VPC nondefault yang ada sebagai VPC default.

Bila Anda membuat VPC default, itu dibuat dengan komponen standar VPC default, termasuk subnet default di setiap Availability Zone. Anda tidak dapat menentukan komponen Anda sendiri. Subnet blok CIDR VPC default baru Anda mungkin tidak memetakan Availability Zone yang sama sebagaimana VPC default Anda sebelumnya. Sebagai contoh, jika subnet dengan blok CIDR `172.31.0.0/20` telah dibuat di `us-east-2a` di VPC default sebelumnya, mungkin dibuat di `us-east-2b` di VPC default baru Anda.

Jika Anda sudah memiliki VPC default di Wilayah, Anda tidak dapat membuat yang lain.

Untuk membuat VPC default menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih VPC Anda.
3. Pilih Tindakan, Buat VPC Default.
4. Pilih Buat. Tutup layar konfirmasi.

Untuk membuat VPC default menggunakan baris perintah

Anda dapat menggunakan perintah create-defaul AWS CLI t-vpc. Perintah ini tidak memiliki parameter input.

```
aws ec2 create-default-vpc
```

Berikut ini adalah contoh output.

```
{
    "Vpc": {
```

```
        "VpcId": "vpc-3f139646",
        "InstanceTenancy": "default",
        "Tags": [],
        "Ipv6CidrBlockAssociationSet": [],
        "State": "pending",
        "DhcpOptionsId": "dopt-61079b07",
        "CidrBlock": "172.31.0.0/16",
        "IsDefault": true
    }
}
```

Atau, Anda dapat menggunakan PowerShell perintah New-EC2DefaultVpc Alat untuk Windows atau tindakan CreateDefaultVpc Amazon EC2 API.

Membuat subnet default

> **Note**
>
> Anda tidak dapat membuat subnet default menggunakan Konsol Manajemen AWS.

Anda dapat membuat subnet default di Availability Zone yang tidak memiliki subnet default. Misalnya, Anda mungkin ingin membuat subnet default jika Anda telah menghapus subnet default, atau jika AWS telah menambahkan Zona Ketersediaan baru dan tidak secara otomatis membuat subnet default untuk zona tersebut di VPC default Anda.

Jika Anda membuat subnet default, subnet default tersebut dibuat dengan ukuran blok CIDR IPv4 `/20` di ruang bersebelahan yang tersedia berikutnya di VPC default Anda. Aturan-aturan berikut berlaku:

- Anda tidak dapat menentukan blok CIDR sendiri.
- Anda tidak dapat memulihkan subnet default yang telah dihapus sebelumnya.
- Anda hanya dapat memiliki satu subnet default per Availability Zone.
- Anda tidak dapat membuat subnet default di VPC nondefault.

Jika tidak ada cukup ruang alamat di VPC default Anda untuk membuat Blok CIDR ukuran `/20`, permintaan gagal. Jika Anda memerlukan lebih banyak ruang alamat, Anda dapat tambahkan blok CIDR IPv4 ke VPC Anda.

Jika Anda telah mengaitkan blok CIDR IPv6 dengan VPC default Anda, subnet default baru tidak akan secara otomatis menerima blok CIDR IPv6. Sebaliknya, Anda dapat mengaitkan blok CIDR IPv6 dengan subnet default setelah Anda membuatnya. Untuk informasi selengkapnya, lihat Menambahkan atau menghapus blok IPv6 CIDR dari subnet Anda.

Untuk membuat subnet default menggunakan AWS CLI

Gunakan AWS CLI perintah create-default-subnet dan tentukan Zona Ketersediaan tempat untuk membuat subnet.

```
aws ec2 create-default-subnet --availability-zone us-east-2a
```

Berikut ini adalah output contoh.

```
{
    "Subnet": {
        "AvailabilityZone": "us-east-2a",
        "Tags": [],
        "AvailableIpAddressCount": 4091,
        "DefaultForAz": true,
        "Ipv6CidrBlockAssociationSet": [],
        "VpcId": "vpc-1a2b3c4d",
        "State": "available",
        "MapPublicIpOnLaunch": true,
        "SubnetId": "subnet-1122aabb",
        "CidrBlock": "172.31.32.0/20",
        "AssignIpv6AddressOnCreation": false
    }
}
```

Untuk informasi selengkapnya tentang pengaturan AWS CLI, lihat Panduan AWS Command Line Interface Pengguna.

Atau, Anda dapat menggunakan PowerShell perintah New-EC2DefaultSubnet Alat untuk Windows atau tindakan CreateDefaultSubnet Amazon EC2 API.

Menampilkan subnet default dan VPC default

Anda dapat menghapus subnet default atau VPC default sebagaimana Anda menghapus subnet atau VPC lainnya. Namun, jika Anda menghapus subnet default atau VPC default, Anda harus secara eksplisit menentukan subnet di salah satu VPC Anda saat meluncurkan instance. Jika Anda tidak

memiliki VPC lain, Anda harus membuat VPC dengan subnet di setidaknya satu Zona Ketersediaan. Untuk informasi selengkapnya, lihat Buat VPC.

Jika Anda menghapus VPC default, Anda dapat membuat yang baru. Untuk informasi selengkapnya, lihat Membuat VPC default.

Jika Anda menghapus subnet default, Anda dapat membuat yang baru. Untuk informasi selengkapnya, lihat Membuat subnet default. Untuk memastikan bahwa subnet default baru Anda berperilaku seperti yang diharapkan, ubah subnet atribut untuk menetapkan alamat IP publik untuk instans yang diluncurkan di subnet tersebut. Untuk informasi selengkapnya, lihat Ubah atribut pengalamatan IP subnet Anda. Anda hanya dapat memiliki satu subnet default per Availability Zone. Anda tidak dapat membuat subnet default di VPC nondefault.

Buat VPC

Gunakan prosedur berikut untuk membuat virtual private cloud (VPC). VPC harus memiliki sumber daya tambahan, seperti subnet, tabel rute, dan gateway, sebelum Anda dapat membuat sumber daya AWS di VPC.

Daftar Isi

- Buat VPC plus sumber daya VPC lainnya
- Buat VPC saja
- Buat VPC menggunakan AWS CLI

Untuk informasi tentang memodifikasi VPC, lihat. the section called “Tambah atau hapus blok CIDR”

Buat VPC plus sumber daya VPC lainnya

Gunakan prosedur berikut untuk membuat VPC ditambah sumber daya VPC tambahan yang Anda perlukan untuk menjalankan aplikasi Anda, seperti subnet, tabel rute, gateway internet, dan gateway NAT. Misalnya konfigurasi VPC, lihat. Contoh

Untuk membuat VPC, subnet, dan sumber daya VPC lainnya menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di dasbor VPC, pilih Buat VPC.
3. Agar Sumber Daya dapat dibuat, pilih VPC dan lainnya.

4. Biarkan pembuatan otomatis tag Nama dipilih untuk membuat tag Nama untuk sumber daya VPC atau hapus untuk menyediakan tag Nama Anda sendiri untuk sumber daya VPC.
5. Untuk blok IPv4 CIDR, masukkan rentang IPv4 alamat untuk VPC. VPC harus memiliki rentang IPv4 alamat.
6. (Opsional) Untuk mendukung IPv6 lalu lintas, pilih blok IPv6 CIDR, blok CIDR yang disediakan Amazon IPv6 .
7. Pilih opsi Sewa. Opsi ini menentukan apakah EC2 instance yang Anda luncurkan ke VPC akan berjalan pada perangkat keras yang dibagikan dengan perangkat keras lain Akun AWS atau pada perangkat keras yang didedikasikan untuk penggunaan Anda saja. Jika Anda memilih penyewaan VPC yang `Default` akan menjadi EC2 , instance yang diluncurkan ke VPC ini akan menggunakan atribut penyewaan yang ditentukan saat Anda meluncurkan instance. Untuk informasi selengkapnya, lihat Meluncurkan instance menggunakan parameter yang ditentukan di Panduan EC2 Pengguna Amazon. Jika Anda memilih penyewaan VPC, instans akan selalu berjalan sebagai Instans Khusus pada perangkat keras yang didedikasikan untuk Anda gunakan. `Dedicated` Jika Anda menggunakan AWS Outposts, Outpost Anda memerlukan konektivitas pribadi; Anda harus menggunakan tenancy. `Default`
8. Untuk Jumlah Availability Zones (AZs), sebaiknya Anda menyediakan subnet di setidaknya dua Availability Zone untuk lingkungan produksi. Untuk memilih subnet Anda, perluas Kustomisasi AZs. AZs Jika tidak, biarkan AWS memilihnya untuk Anda.
9. Untuk mengkonfigurasi subnet Anda, pilih nilai untuk Jumlah subnet publik dan Jumlah subnet pribadi. Untuk memilih rentang alamat IP untuk subnet Anda, perluas Sesuaikan subnet blok CIDR. Jika tidak, biarkan AWS memilihnya untuk Anda.
10. (Opsional) Jika sumber daya dalam subnet pribadi memerlukan akses ke internet publik melalui IPv4, untuk gateway NAT, pilih jumlah AZs di mana untuk membuat gateway NAT. Dalam produksi, kami menyarankan Anda menerapkan gateway NAT di setiap AZ dengan sumber daya yang memerlukan akses ke internet publik. Perhatikan bahwa ada biaya yang terkait dengan gateway NAT. Untuk informasi selengkapnya, lihat Harga untuk NAT gateway.
11. (Opsional) Jika sumber daya di subnet pribadi memerlukan akses ke internet publik melalui IPv6, untuk gateway internet Egress saja, pilih Ya.
12. (Opsional) Jika Anda perlu mengakses Amazon S3 langsung dari VPC Anda, pilih titik akhir VPC, S3 Gateway. Ini menciptakan titik akhir VPC gateway untuk Amazon S3. Untuk informasi selengkapnya, lihat titik akhir Gateway di AWS PrivateLink Panduan.
13. (Opsional) Untuk opsi DNS, kedua opsi untuk resolusi nama domain diaktifkan secara default. Jika default tidak memenuhi kebutuhan Anda, Anda dapat menonaktifkan opsi ini.

14. (Opsional) Untuk menambahkan tag ke VPC Anda, perluas Tag tambahan, pilih Tambahkan tag baru, dan masukkan kunci tag dan nilai tag.
15. Di panel Pratinjau, Anda dapat memvisualisasikan hubungan antara sumber daya VPC yang telah dikonfigurasi. Garis padat mewakili hubungan antar sumber daya. Garis putus-putus mewakili lalu lintas jaringan ke gateway NAT, gateway internet, dan titik akhir gateway. Setelah Anda membuat VPC, Anda dapat memvisualisasikan sumber daya di VPC Anda dalam format ini kapan saja menggunakan tab Peta sumber daya. Untuk informasi selengkapnya, lihat Visualisasikan sumber daya di VPC Anda.
16. Setelah selesai mengonfigurasi VPC Anda, pilih Buat VPC.

Buat VPC saja

Gunakan prosedur berikut untuk membuat VPC tanpa sumber daya VPC tambahan menggunakan konsol VPC Amazon.

Untuk membuat VPC tanpa sumber daya VPC tambahan menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di dasbor VPC, pilih Buat VPC.
3. Agar Sumber Daya dapat dibuat, pilih VPC saja.
4. (Opsional) Untuk tag Nama, masukkan nama untuk VPC Anda. Melakukan hal itu akan menciptakan tag dengan kunci `Name` dan nilai yang Anda tentukan.
5. Untuk blok IPv4 CIDR, lakukan salah satu hal berikut:
   - Pilih input manual IPv4 CIDR dan masukkan rentang IPv4 alamat untuk VPC Anda.
   - Pilih blok IPv4 CIDR yang dialokasikan IPAM, pilih kumpulan alamat Amazon VPC IP Address Manager (IPAM) dan netmask. IPv4 Ukuran blok CIDR dibatasi oleh aturan alokasi pada kolam IPAM. IPAM adalah fitur VPC yang memudahkan Anda merencanakan, melacak, dan memantau alamat IP untuk AWS beban kerja Anda. Untuk informasi selengkapnya, lihat Panduan Pengguna Amazon VPC IPAM.

     Jika Anda menggunakan IPAM untuk mengelola alamat IP Anda, kami sarankan Anda memilih opsi ini. Jika tidak, blok CIDR yang Anda tentukan untuk VPC Anda mungkin tumpang tindih dengan alokasi CIDR IPAM.
6. (Opsional) Untuk membuat VPC tumpukan ganda, tentukan rentang IPv6 alamat untuk VPC Anda. Untuk blok IPv6 CIDR, lakukan salah satu hal berikut:

- Pilih blok IPv6 CIDR yang dialokasikan IPAM jika Anda menggunakan Amazon VPC IP Address Manager dan Anda ingin menyediakan CIDR dari kolam IPAM. IPv6 Jika Anda menggunakan blok IPv6 CIDR yang dialokasikan IPAM untuk menyediakan VPCs, Anda mendapatkan manfaat yang berdekatan IPv6 CIDRs untuk pembuatan VPC. IPv6 CIDRs Dialokasikan secara bersebelahan adalah yang dialokasikan secara CIDRs berurutan. CIDRs Mereka memungkinkan Anda untuk menyederhanakan aturan keamanan dan jaringan Anda; IPv6 CIDRs dapat digabungkan dalam satu entri di seluruh jaringan dan konstruksi keamanan seperti daftar kontrol akses, tabel rute, grup keamanan, dan firewall.

  Anda memiliki dua opsi untuk menyediakan rentang alamat IP ke VPC di bawah blok CIDR:

  - Panjang Netmask: Pilih opsi ini untuk memilih panjang netmask untuk CIDR. Lakukan salah satu tindakan berikut:
    - Jika ada panjang netmask default yang dipilih untuk kolam IPAM, Anda dapat memilih panjang netmask default ke IPAM untuk menggunakan panjang netmask default yang ditetapkan untuk kolam IPAM oleh administrator IPAM. Untuk informasi selengkapnya tentang aturan alokasi panjang netmask default opsional, lihat Membuat IPv6 kumpulan Regional di Panduan Pengguna Amazon VPC IPAM.
    - Jika tidak ada panjang netmask default yang dipilih untuk kolam IPAM, pilih panjang netmask yang lebih spesifik daripada panjang netmask CIDR kolam IPAM. Misalnya, jika CIDR kolam IPAM adalah /50, Anda dapat memilih panjang netmask antara/52 hingga /60 untuk VPC. Kemungkinan panjang netmask adalah antara /44 dan /60 dengan kelipatan /4.
  - Pilih CIDR: Pilih opsi ini untuk memasukkan IPv6 alamat secara manual. Anda hanya dapat memilih panjang netmask yang lebih spesifik daripada panjang netmask dari CIDR kolam IPAM. Misalnya, jika CIDR kolam IPAM adalah /50, Anda dapat memilih panjang netmask antara/52 hingga /60 untuk VPC. Kemungkinan panjang IPv6 netmask adalah antara /44 dan /60 dengan kelipatan /4.
- Pilih blok IPv6 CIDR yang disediakan Amazon untuk meminta blok IPv6 CIDR dari kumpulan alamat Amazon. IPv6 Untuk Network Border Group, pilih grup tempat AWS mengiklankan alamat IP. Amazon menyediakan ukuran blok IPv6 CIDR tetap /56.
- Pilih IPv6 CIDR yang dimiliki oleh saya untuk menyediakan IPv6 CIDR yang telah Anda bawa. AWS Untuk informasi selengkapnya tentang membawa rentang alamat IP Anda sendiri AWS, lihat Membawa alamat IP Anda sendiri (BYOIP) di EC2 Panduan Pengguna Amazon. Anda dapat menyediakan rentang alamat IP untuk VPC menggunakan opsi berikut untuk blok CIDR:
  - Tidak ada preferensi: Pilih opsi ini untuk menggunakan panjang netmask /56.

- Pilih CIDR: Pilih opsi ini untuk memasukkan IPv6 alamat secara manual dan pilih panjang netmask yang lebih spesifik daripada ukuran BYOIP CIDR. Misalnya, jika CIDR kumpulan BYOIP adalah /50, Anda dapat memilih panjang netmask antara /52 hingga /60 untuk VPC. Kemungkinan panjang IPv6 netmask adalah antara /44 dan /60 dengan kelipatan /4.

7. (Opsional) Pilih opsi Sewa. Opsi ini menentukan apakah EC2 instance yang Anda luncurkan ke VPC akan berjalan pada perangkat keras yang dibagikan dengan perangkat keras lain Akun AWS atau pada perangkat keras yang didedikasikan untuk penggunaan Anda saja. Jika Anda memilih penyewaan VPC yang akan *`Default`* menjadi EC2 , instance yang diluncurkan ke VPC ini akan menggunakan atribut penyewaan yang ditentukan saat Anda meluncurkan instance -- Untuk informasi selengkapnya, lihat Meluncurkan instance menggunakan parameter yang ditentukan di Panduan Pengguna Amazon. EC2 Jika Anda memilih penyewaan VPC, instans akan selalu berjalan sebagai Instans Khusus pada perangkat keras yang didedikasikan untuk Anda gunakan. `Dedicated` Jika Anda menggunakan AWS Outposts, Outpost Anda memerlukan konektivitas pribadi; Anda harus menggunakan tenancy. `Default`
8. (Opsional) Untuk menambahkan tag ke VPC Anda, pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.
9. Pilih Buat VPC.
10. Setelah membuat VPC, Anda dapat menambahkan subnet. Untuk informasi selengkapnya, lihat Membuat subnet.

Buat VPC menggunakan AWS CLI

Prosedur berikut berisi contoh AWS CLI perintah untuk membuat VPC ditambah sumber daya VPC tambahan yang diperlukan untuk menjalankan aplikasi. Jika Anda menjalankan semua perintah dalam prosedur ini, Anda akan membuat VPC, subnet publik, subnet pribadi, tabel rute untuk setiap subnet, gateway internet, gateway internet khusus egres, dan gateway NAT publik. Jika Anda tidak membutuhkan semua sumber daya ini, Anda hanya dapat menggunakan contoh perintah yang Anda butuhkan.

Prasyarat

Sebelum Anda mulai, instal dan konfigurasikan file AWS CLI. Ketika Anda mengkonfigurasi AWS CLI, Anda akan diminta untuk AWS kredensialnya. Contoh dalam prosedur ini mengasumsikan bahwa Anda juga mengonfigurasi Wilayah default. Jika tidak, tambahkan `--region` opsi ke setiap perintah. Untuk informasi selengkapnya, lihat Menginstal atau memperbarui AWS CLI dan Mengonfigurasi. AWS CLI

Penandaan

Anda dapat menambahkan tag ke sumber daya setelah Anda membuatnya dengan menggunakan perintah create-tags. Atau, Anda dapat menambahkan `--tag-specification` opsi ke perintah penciptaan untuk sumber daya sebagai berikut.

```
--tag-specifications ResourceType=vpc,Tags=[{Key=Name,Value=my-project}]
```

Untuk membuat VPC plus sumber daya VPC dengan menggunakan AWS CLI

1. Gunakan perintah create-vpc berikut untuk membuat VPC dengan blok CIDR yang ditentukan. IPv4

   ```
   aws ec2 create-vpc --cidr-block 10.0.0.0/24 --query Vpc.VpcId --output text
   ```

   Atau, untuk membuat VPC tumpukan ganda, tambahkan `--amazon-provided-ipv6-cidr-block` opsi untuk menambahkan blok IPv6 CIDR yang disediakan Amazon, seperti yang ditunjukkan pada contoh berikut.

   ```
   aws ec2 create-vpc --cidr-block 10.0.0.0/24 --amazon-provided-ipv6-cidr-block --
   query Vpc.VpcId --output text
   ```

   Perintah ini mengembalikan ID VPC baru. Berikut ini contohnya.

   ```
   vpc-1a2b3c4d5e6f1a2b3
   ```

2. [Dual stack VPC] Dapatkan blok IPv6 CIDR yang terkait dengan VPC Anda dengan menggunakan perintah deskripsi-vpcs berikut.

   ```
   aws ec2 describe-vpcs --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
    Vpcs[].Ipv6CidrBlockAssociationSet[].Ipv6CidrBlock --output text
   ```

   Berikut ini adalah output contoh.

   ```
   2600:1f13:cfe:3600::/56
   ```

3. Buat satu atau lebih subnet, tergantung pada kasus penggunaan Anda. Dalam produksi, kami menyarankan Anda meluncurkan sumber daya di setidaknya dua Availability Zone. Gunakan salah satu perintah berikut untuk membuat setiap subnet.

- IPv4-Only subnet — Untuk membuat subnet dengan blok IPv4 CIDR tertentu, gunakan perintah create-subnet berikut.

```
aws ec2 create-subnet --vpc-id vpc-1a2b3c4d5e6f1a2b3 --cidr-block 10.0.1.0/20
 --availability-zone us-east-2a --query Subnet.SubnetId --output text
```

- Subnet tumpukan ganda - Jika Anda membuat VPC tumpukan ganda, Anda dapat menggunakan `--ipv6-cidr-block` opsi untuk membuat subnet tumpukan ganda, seperti yang ditunjukkan pada perintah berikut.

```
aws ec2 create-subnet --vpc-id vpc-1a2b3c4d5e6f1a2b3 --cidr-block 10.0.1.0/20
 --ipv6-cidr-block 2600:1f13:cfe:3600::/64 --availability-zone us-east-2a --
query Subnet.SubnetId --output text
```

- IPv6-Only subnet - Jika Anda membuat VPC tumpukan ganda, Anda dapat menggunakan `--ipv6-native` opsi untuk membuat subnet IPv6 -only, seperti yang ditunjukkan pada perintah berikut.

```
aws ec2 create-subnet --vpc-id vpc-1a2b3c4d5e6f1a2b3 --ipv6-native --ipv6-
cidr-block 2600:1f13:cfe:3600::/64 --availability-zone us-east-2a --query
 Subnet.SubnetId --output text
```

Perintah ini mengembalikan ID subnet baru. Berikut ini contohnya.

```
subnet-1a2b3c4d5e6f1a2b3
```

4. Jika Anda memerlukan subnet publik untuk server web Anda, atau untuk gateway NAT, lakukan hal berikut:

   a. Buat gateway internet dengan menggunakan create-internet-gatewayperintah berikut. Perintah mengembalikan ID gateway internet baru.

```
aws ec2 create-internet-gateway --query InternetGateway.InternetGatewayId --
output text
```

   b. Lampirkan gateway internet ke VPC Anda dengan menggunakan perintah berikut attach-internet-gateway. Gunakan ID gateway internet yang dikembalikan dari langkah sebelumnya.

```
aws ec2 attach-internet-gateway --vpc-id vpc-1a2b3c4d5e6f1a2b3 --internet-
gateway-id igw-id
```

c. Buat tabel rute kustom untuk subnet publik Anda dengan menggunakan create-route-tableperintah berikut. Perintah mengembalikan ID dari tabel rute baru.

```
aws ec2 create-route-table --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
 RouteTable.RouteTableId --output text
```

d. Buat rute dalam tabel rute yang mengirimkan semua IPv4 lalu lintas ke gateway internet dengan menggunakan perintah create-route berikut. Gunakan ID tabel rute untuk subnet publik.

```
aws ec2 create-route --route-table-id rtb-id-public --destination-cidr-block
 0.0.0.0/0 --gateway-id igw-id
```

e. Kaitkan tabel rute dengan subnet publik dengan menggunakan associate-route-tableperintah berikut. Gunakan ID tabel rute untuk subnet publik dan ID subnet publik.

```
aws ec2 associate-route-table --route-table-id rtb-id-public --subnet-
id subnet-id-public-subnet
```

5. [IPv6] Anda dapat menambahkan gateway internet khusus egres sehingga instance di subnet pribadi dapat mengakses internet melalui IPv6 (misalnya, untuk mendapatkan pembaruan perangkat lunak), tetapi host di internet tidak dapat mengakses instance Anda.

a. Buat gateway internet khusus egress dengan menggunakan perintah -gateway berikutcreate-egress-only-internet. Perintah mengembalikan ID gateway internet baru.

```
aws ec2 create-egress-only-internet-gateway --vpc-id vpc-1a2b3c4d5e6f1a2b3 --
query EgressOnlyInternetGateway.EgressOnlyInternetGatewayId --output text
```

b. Buat tabel rute khusus untuk subnet pribadi Anda dengan menggunakan create-route-tableperintah berikut. Perintah mengembalikan ID dari tabel rute baru.

```
aws ec2 create-route-table --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
 RouteTable.RouteTableId --output text
```

c. Buat rute di tabel rute untuk subnet pribadi yang mengirimkan semua IPv6 lalu lintas ke gateway internet khusus egres dengan menggunakan perintah create-route berikut. Gunakan ID tabel rute yang dikembalikan pada langkah sebelumnya.

```
aws ec2 create-route --route-table-id rtb-id-private --destination-cidr-
block ::/0 --egress-only-internet-gateway eigw-id
```

d. Kaitkan tabel rute dengan subnet pribadi dengan menggunakan associate-route-tableperintah berikut.

```
aws ec2 associate-route-table --route-table-id rtb-id-private --subnet-
id subnet-id-private-subnet
```

6. Jika Anda memerlukan gateway NAT untuk sumber daya Anda di subnet pribadi, lakukan hal berikut:

a. Buat alamat IP elastis untuk gateway NAT dengan menggunakan perintah allocate-address berikut.

```
aws ec2 allocate-address --domain vpc --query AllocationId --output text
```

b. Buat gateway NAT di subnet publik dengan menggunakan perintah berikut create-nat-gateway. Gunakan ID alokasi yang dikembalikan dari langkah sebelumnya.

```
aws ec2 create-nat-gateway --subnet-id subnet-id-public-subnet --allocation-
id eipalloc-id
```

c. (Opsional) Jika Anda sudah membuat tabel rute untuk subnet pribadi di langkah 5, lewati langkah ini. Jika tidak, gunakan create-route-tableperintah berikut untuk membuat tabel rute untuk subnet pribadi Anda. Perintah mengembalikan ID dari tabel rute baru.

```
aws ec2 create-route-table --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
 RouteTable.RouteTableId --output text
```

d. Buat rute dalam tabel rute untuk subnet pribadi yang mengirimkan semua IPv4 lalu lintas ke gateway NAT dengan menggunakan perintah create-route berikut. Gunakan ID tabel rute untuk subnet pribadi, yang Anda buat baik di langkah ini atau di langkah 5.

```
aws ec2 create-route --route-table-id rtb-id-private --destination-cidr-
block 0.0.0.0/0 --gateway-id nat-id
```

e. (Opsional) Jika Anda sudah mengaitkan tabel rute dengan subnet pribadi di langkah 5, lewati langkah ini. Jika tidak, gunakan associate-route-tableperintah berikut untuk mengaitkan tabel rute dengan subnet pribadi. Gunakan ID tabel rute untuk subnet pribadi, yang Anda buat baik di langkah ini atau di langkah 5.

```
aws ec2 associate-route-table --route-table-id rtb-id-private --subnet-
id subnet-id-private-subnet
```

Visualisasikan sumber daya di VPC Anda

Bagian ini menjelaskan bagaimana Anda dapat melihat representasi visual dari sumber daya di VPC Anda menggunakan tab Peta sumber daya. Sumber daya berikut terlihat di peta sumber daya:

- VPC
- Subnet
  - Availability Zone diwakili dengan huruf.
  - Subnet publik berwarna hijau.
  - Subnet pribadi berwarna biru.
- Tabel rute
- Gateway internet
- Gateway internet khusus egress
- Gateway NAT
- Titik akhir Gateway (Amazon S3 dan Amazon DynamoDB)

Peta sumber daya menunjukkan hubungan antara sumber daya di dalam VPC dan bagaimana lalu lintas mengalir dari subnet ke gateway NAT, gateway internet, dan titik akhir gateway.

Anda dapat menggunakan peta sumber daya untuk memahami arsitektur VPC, melihat berapa banyak subnet yang ada di dalamnya, subnet mana yang terkait dengan tabel rute mana, dan tabel rute mana yang memiliki rute ke gateway NAT, gateway internet, dan titik akhir gateway.

Anda juga dapat menggunakan peta sumber daya untuk menemukan konfigurasi yang tidak diinginkan atau salah, seperti subnet pribadi yang terputus dari gateway NAT atau subnet pribadi

dengan rute langsung ke gateway internet. Anda dapat memilih sumber daya dalam peta sumber daya, seperti tabel rute, dan mengedit konfigurasi untuk sumber daya tersebut.

Untuk memvisualisasikan sumber daya di VPC Anda

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih VPCs.
3. Pilih VPC.
4. Pilih tab Peta sumber daya untuk menampilkan visualisasi sumber daya.
5. Pilih Tampilkan detail untuk melihat detail selain sumber daya IDs dan zona yang ditampilkan secara default.
   - VPC: Rentang IPv4 dan IPv6 CIDR yang ditetapkan ke VPC.
   - Subnet: Rentang IPv4 dan IPv6 CIDR yang ditetapkan untuk setiap subnet.
   - Tabel rute: Asosiasi subnet, dan jumlah rute dalam tabel rute.
   - Koneksi jaringan: Detail yang terkait dengan setiap jenis koneksi:
     - Jika ada subnet publik di VPC, ada sumber daya gateway internet dengan jumlah rute dan sumber dan subnet tujuan untuk lalu lintas menggunakan gateway internet.
     - Jika ada gateway internet khusus egress-only, ada sumber daya gateway internet khusus egres dengan jumlah rute dan subnet sumber dan tujuan untuk lalu lintas menggunakan gateway internet khusus egres.
     - Jika ada gateway NAT, ada sumber daya gateway NAT dengan jumlah antarmuka jaringan dan alamat IP Elastis untuk gateway NAT.
     - Jika ada titik akhir gateway, ada sumber daya titik akhir gateway dengan nama AWS layanan (Amazon S3 atau Amazon DynamoDB) yang dapat Anda sambungkan menggunakan titik akhir.
6. Arahkan kursor ke sumber daya untuk melihat hubungan antara sumber daya. Garis padat mewakili hubungan antar sumber daya. Garis putus-putus mewakili lalu lintas jaringan ke koneksi jaringan.

Tambahkan atau hapus blok CIDR dari VPC Anda

Bagian ini menjelaskan cara menambah atau menghapus IPv4 dan IPv6 CIDR blok dari VPC.

Important

- VPC Anda dapat memiliki hingga lima IPv4 dan lima blok IPv6 CIDR secara default, tetapi batas ini dapat disesuaikan. Untuk informasi selengkapnya, lihat Kuota Amazon VPC. Untuk informasi tentang pembatasan blok CIDR untuk VPC, lihat. Blok VPC CIDR
- Jika VPC Anda memiliki lebih dari satu blok IPv4 CIDR yang terkait dengannya, Anda dapat menghapus blok IPv4 CIDR dari VPC. Anda tidak dapat menghapus blok IPv4 CIDR utama. Anda harus menghapus seluruh blok CIDR; Anda tidak dapat menghapus subset dari blok CIDR atau rentang gabungan blok CIDR. Anda harus terlebih dahulu menghapus semua subnet di blok CIDR.
- Jika Anda tidak lagi menginginkan IPv6 dukungan di VPC Anda, tetapi Anda ingin terus menggunakan VPC Anda untuk membuat dan berkomunikasi dengan IPv4 sumber daya, Anda dapat menghapus blok CIDR. IPv6
- Untuk menghapus blok IPv6 CIDR, Anda harus terlebih dahulu membatalkan penetapan IPv6 alamat apa pun yang ditetapkan ke instans apa pun di subnet Anda.
- Menghapus blok IPv6 CIDR tidak secara otomatis menghapus aturan grup keamanan, aturan ACL jaringan, atau rute tabel rute yang telah Anda konfigurasikan untuk IPv6 jaringan. Anda harus secara manual mengubah atau menghapus aturan-aturan atau rute-rute ini.

Untuk menambah atau menghapus blok CIDR dari VPC menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Your VPCs.
3. Pilih VPC, lalu pilih Tindakan, Edit. CIDRs
4. Untuk menghapus CIDR, pilih Hapus di sebelah CIDR.
5. Untuk menambahkan CIDR, pilih Tambahkan CIDR baru atau Tambahkan IPv4 CIDR baru IPv6.
6. Untuk menambahkan CIDR untuk blok IPv4 CIDR, lakukan salah satu hal berikut:
   - Pilih input manual IPv4 CIDR dan masukkan blok IPv4 CIDR.
   - Pilih CIDR yang dialokasikan IPAM dan pilih IPv4 CIDR dari kolam IPAM. IPv4
   - Pilih Simpan.
7. Untuk menambahkan CIDR untuk blok IPv6 CIDR, lakukan hal berikut:

- Pilih blok IPv6 CIDR yang dialokasikan IPAM jika Anda menggunakan Amazon VPC IP Address Manager dan Anda ingin menyediakan CIDR dari kolam IPAM. IPv6 Anda memiliki dua opsi untuk menyediakan rentang alamat IP ke VPC di bawah blok CIDR:
  - Panjang Netmask: Pilih opsi ini untuk memilih panjang netmask untuk CIDR. Lakukan salah satu tindakan berikut:
    - Jika ada panjang netmask default yang dipilih untuk kolam IPAM, Anda dapat memilih panjang netmask default ke IPAM untuk menggunakan panjang netmask default yang ditetapkan untuk kolam IPAM oleh administrator IPAM. Untuk informasi selengkapnya tentang aturan alokasi panjang netmask default opsional, lihat Membuat IPv6 kumpulan Regional di Panduan Pengguna Amazon VPC IPAM.
    - Jika tidak ada panjang netmask default yang dipilih untuk kolam IPAM, pilih panjang netmask yang lebih spesifik daripada panjang netmask CIDR kolam IPAM. Misalnya, jika CIDR kolam IPAM adalah /50, Anda dapat memilih panjang netmask antara/52 hingga /60 untuk VPC. Kemungkinan panjang netmask adalah antara /44 dan /60 dengan kelipatan /4.
  - Pilih CIDR: Pilih opsi ini untuk memasukkan IPv6 alamat secara manual. Anda hanya dapat memilih panjang netmask yang lebih spesifik daripada panjang netmask dari CIDR kolam IPAM. Misalnya, jika CIDR kolam IPAM adalah /50, Anda dapat memilih panjang netmask antara/52 hingga /60 untuk VPC. Kemungkinan panjang IPv6 netmask adalah antara /44 dan /60 dengan kelipatan /4.
- Pilih blok IPv6 CIDR yang disediakan Amazon untuk meminta blok IPv6 CIDR dari kumpulan alamat Amazon. IPv6 Untuk Network Border Group, pilih grup tempat AWS mengiklankan alamat IP. Amazon menyediakan ukuran blok IPv6 CIDR tetap /56.
- Pilih IPv6 CIDR yang dimiliki oleh saya untuk menyediakan IPv6 CIDR yang telah Anda bawa. AWS Untuk informasi selengkapnya, lihat Membawa alamat IP Anda sendiri (BYOIP) ke Amazon EC2 di EC2 Panduan Pengguna Amazon. Anda memiliki dua opsi untuk menyediakan rentang alamat IP ke VPC di bawah blok CIDR:
  - Tidak ada preferensi: Pilih opsi ini untuk menggunakan panjang netmask /56.
  - Pilih CIDR: Pilih opsi ini untuk memasukkan IPv6 alamat secara manual dan pilih panjang netmask yang lebih spesifik daripada ukuran BYOIP CIDR. Misalnya, jika CIDR kumpulan BYOIP adalah /50, Anda dapat memilih panjang netmask antara /52 hingga /60 untuk VPC. Kemungkinan panjang IPv6 netmask adalah antara /44 dan /60 dengan kelipatan /4.
  - Pilih Pilih CIDR setelah selesai.

8. Pilih Tutup.

9. Jika Anda telah menambahkan blok CIDR ke VPC Anda, Anda dapat membuat subnet yang menggunakan blok CIDR baru. Untuk informasi selengkapnya, lihat Membuat subnet.

Untuk mengaitkan atau memisahkan blok CIDR dari VPC menggunakan AWS CLI

Gunakan associate-vpc-cidr-blockdan disassociate-vpc-cidr-blockperintah.

Opsi DHCP ditetapkan di Amazon VPC

Perangkat jaringan di VPC Anda menggunakan Dynamic Host Configuration Protocol (DHCP). Anda dapat menggunakan set opsi DHCP untuk mengontrol aspek-aspek berikut dari konfigurasi jaringan di jaringan virtual Anda:

- Server DNS, nama domain, atau server Network Time Protocol (NTP) yang digunakan oleh perangkat di VPC Anda.
- Apakah resolusi DNS diaktifkan di VPC Anda.

Daftar Isi

- Apa itu DHCP?
- Konsep set opsi DHCP
- Bekerja dengan set opsi DHCP

Apa itu DHCP?

Setiap perangkat pada jaringan TCP/IP memerlukan alamat IP untuk berkomunikasi melalui jaringan. Di masa lalu, alamat IP harus ditetapkan ke setiap perangkat di jaringan Anda secara manual. Saat ini, alamat IP ditetapkan secara dinamis oleh server DHCP menggunakan Dynamic Host Configuration Protocol (DHCP).

Aplikasi yang berjalan pada EC2 instance dapat berkomunikasi dengan server Amazon DHCP sesuai kebutuhan untuk mengambil sewa alamat IP mereka atau informasi konfigurasi jaringan lainnya (seperti alamat IP server DNS Amazon atau alamat IP router di VPC Anda).

Anda dapat menentukan konfigurasi jaringan yang disediakan oleh server Amazon DHCP dengan menggunakan set opsi DHCP.

Jika Anda memiliki konfigurasi VPC yang mengharuskan aplikasi Anda membuat permintaan langsung ke server Amazon IPv6 DHCP, perhatikan hal berikut:

- Sebuah EC2 instance dalam subnet dual-stack hanya dapat mengambil IPv6 alamatnya dari server DHCP. IPv6 Itu tidak dapat mengambil konfigurasi jaringan tambahan dari server IPv6 DHCP, seperti nama server DNS atau nama domain.
- Sebuah EC2 instance dalam subnet IPv6 -only dapat mengambil IPv6 alamatnya dari server IPv6 DHCP dan dapat mengambil informasi konfigurasi jaringan tambahan, seperti nama server DNS dan nama domain.
- Untuk EC2 contoh di subnet IPv6 -only, Server IPv4 DHCP akan mengembalikan 169.254.169.253 sebagai server nama jika "AmazonProvidedDNS" secara eksplisit disebutkan dalam set opsi DHCP. Jika "AmazonProvidedDNS" hilang dari set opsi, Server IPv4 DHCP tidak akan mengembalikan alamat apakah server IPv4 nama lain disebutkan dalam set opsi atau tidak.

Server Amazon DHCP juga dapat menyediakan keseluruhan IPv4 atau IPv6 awalan ke antarmuka jaringan di VPC Anda menggunakan delegasi awalan (lihat Menetapkan awalan ke antarmuka jaringan EC2 Amazon di Panduan Pengguna Amazon). EC2 IPv4 delegasi awalan tidak disediakan dalam tanggapan DHCP. IPv4 awalan yang ditetapkan ke antarmuka dapat diambil menggunakan IMDS (lihat Kategori metadata instans di Panduan Pengguna Amazon). EC2

Konsep set opsi DHCP

Kumpulan opsi DHCP adalah sekelompok pengaturan jaringan yang digunakan oleh sumber daya di VPC Anda, seperti instans EC2, untuk berkomunikasi melalui jaringan virtual Anda.

Setiap Wilayah memiliki set opsi DHCP default. Setiap VPC menggunakan set opsi DHCP default untuk Wilayah-nya kecuali Anda membuat dan mengaitkan set opsi DHCP kustom dengan VPC atau mengonfigurasi VPC tanpa set opsi DHCP.

Jika VPC Anda tidak memiliki set opsi DHCP yang dikonfigurasi:

- Untuk inst ans EC2 yang dibangun pada Sistem Nitro, konfigur AWS asikan `169.254.169.253` sebagai server nama domain default.
- Untuk inst ans EC2 yang dibangun di Xen, tidak ada server nama domain yang dikonfigurasi dan, karena instans di VPC tidak memiliki akses ke server DNS, mereka tidak dapat mengakses internet.

Anda dapat mengaitkan set opsi DHCP dengan beberapa VPC, tetapi setiap VPC hanya dapat memiliki satu set opsi DHCP terkait.

Jika Anda menghapus VPC, set opsi DHCP yang terkait dengan VPC dipisahkan dari VPC.

Daftar Isi

- Set opsi DHCP default
- Set opsi DHCP kustom

Set opsi DHCP default

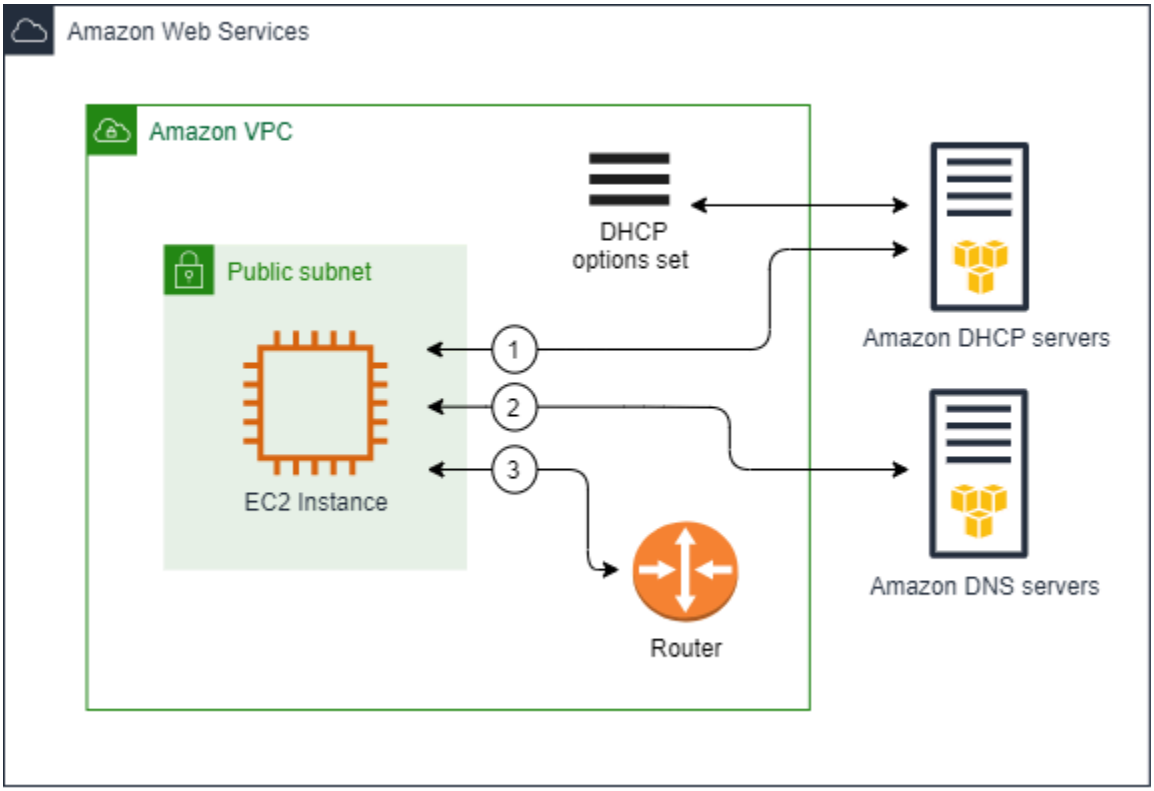
Set opsi DHCP default berisi pengaturan berikut:

- Server nama domain: Server DNS yang digunakan antarmuka jaringan Anda untuk resolusi nama domain. Untuk set opsi DHCP default, ini selalu`AmazonProvidedDNS`. Untuk informasi selengkapnya, lihat Server Amazon DNS.
- Nama domain: Nama domain yang harus digunakan klien saat menyelesaikan nama host menggunakan Domain Name System (DNS). Untuk informasi selengkapnya tentang nama domain yang digunakan untuk instans EC2, lihat nama host instans Amazon EC2.
- Waktu Sewa Pilihan IPv6: Seberapa sering instance yang berjalan dengan IPv6 yang ditetapkan untuk itu melewati pembaruan sewa DHCPv6. Waktu sewa default adalah 140 detik. Perpanjangan sewa biasanya terjadi ketika setengah dari waktu sewa telah berlalu.

Saat Anda menggunakan set opsi DHCP default, pengaturan berikut tidak digunakan, tetapi ada default untuk instans EC2:

- Server NTP: Secara default, instans EC2 menggunakan Layanan Sinkronisasi Waktu Amazon untuk mengambil waktu.
- Server nama NetBIOS: Untuk instans EC2 yang menjalankan Windows, nama komputer NetBIOS adalah nama ramah yang ditetapkan untuk instance untuk mengidentifikasinya di jaringan. Server nama NetBIOS menyimpan daftar pemetaan antara nama komputer NetBIOS dan alamat jaringan untuk jaringan yang menggunakan NetBIOS sebagai layanan penamaan mereka.
- Jenis node NetBIOS: Untuk instans EC2 yang menjalankan Windows, ini adalah metode yang digunakan instans untuk menyelesaikan nama NetBIOS ke alamat IP.

Saat Anda menggunakan set opsi default, server Amazon DHCP menggunakan pengaturan jaringan di set opsi default. Saat Anda meluncurkan instance di VPC Anda, mereka melakukan hal berikut, seperti yang ditunjukkan pada diagram: (1) berinteraksi dengan server DHCP, (2) berinteraksi dengan server DNS Amazon, dan (3) terhubung ke perangkat lain di jaringan melalui router untuk VPC Anda. Instans dapat berinteraksi dengan server DHCP Amazon kapan saja untuk mendapatkan sewa alamat IP dan pengaturan jaringan tambahan.



Set opsi DHCP kustom

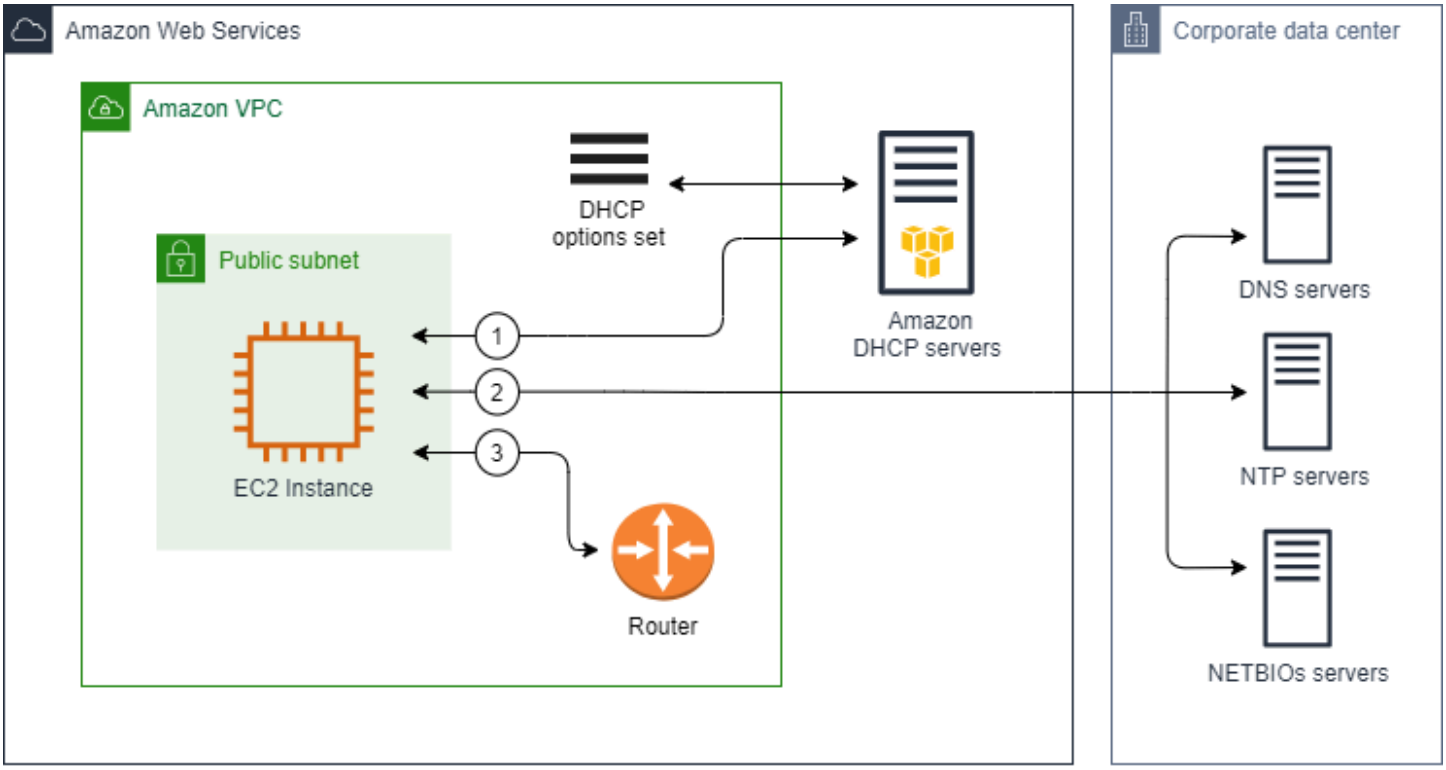
Anda dapat membuat set opsi DHCP kustom dengan pengaturan berikut, dan kemudian mengaitkannya dengan VPC:

- Server nama domain: Server DNS yang digunakan antarmuka jaringan Anda untuk resolusi nama domain.
- Nama domain: Nama domain yang digunakan klien saat menyelesaikan nama host menggunakan Sistem Nama Domain (DNS).
- Server NTP: Server NTP yang menyediakan waktu untuk instance.
- Server nama NetBIOS: Untuk instans EC2 yang menjalankan Windows, nama komputer NetBIOS adalah nama ramah yang ditetapkan untuk instance untuk mengidentifikasinya di jaringan. Server

nama NetBIOS memelihara daftar pemetaan antara nama komputer NetBIOS dan alamat jaringan untuk jaringan yang menggunakan NetBIOS sebagai layanan penamaan mereka.

- Jenis node NetBIOS: Untuk instans EC2 yang menjalankan Windows, metode yang digunakan instans untuk menyelesaikan nama NetBIOS ke alamat IP.
- Waktu Sewa Pilihan IPv6 (opsional): Nilai (dalam detik, menit, jam, atau tahun) untuk seberapa sering instance yang berjalan dengan IPv6 yang ditetapkan untuk itu melewati perpanjangan sewa DHCPv6. Nilai yang dapat diterima adalah antara 140 dan 4294967295 detik (sekitar 138 tahun). Jika tidak ada nilai yang dimasukkan, waktu sewa default adalah 140 detik. Jika Anda menggunakan pengalamatan jangka panjang untuk instans EC2, Anda dapat meningkatkan waktu sewa dan menghindari permintaan perpanjangan sewa yang sering. Perpanjangan sewa biasanya terjadi ketika setengah dari waktu sewa telah berlalu.

Saat Anda menggunakan kumpulan opsi khusus, instance yang diluncurkan ke VPC Anda melakukan hal berikut, seperti yang ditunjukkan pada diagram: (1) menggunakan pengaturan jaringan di set opsi DHCP kustom, (2) berinteraksi dengan server DNS, NTP, dan NetBIOS yang ditentukan dalam set opsi DHCP kustom, dan (3) sambungkan ke perangkat lain di jaringan melalui router untuk VPC Anda.



Tugas terkait

- Buat set opsi DHCP
- Ubah set opsi yang terkait dengan VPC

Bekerja dengan set opsi DHCP

Gunakan prosedur berikut untuk melihat dan bekerja dengan set opsi DHCP. Untuk informasi selengkapnya tentang cara kerja set opsi DHCP, lihatthe section called “Konsep set opsi DHCP”.

Tugas

- Buat set opsi DHCP
- Ubah set opsi yang terkait dengan VPC
- Hapus set opsi DHCP

Buat set opsi DHCP

Set opsi DHCP kustom memungkinkan Anda untuk menyesuaikan VPC Anda dengan server DNS Anda sendiri, nama domain, dan banyak lagi. Anda dapat membuat set opsi DHCP tambahan sebanyak yang Anda inginkan. Namun, Anda hanya dapat mengaitkan VPC dengan satu opsi DHCP yang ditetapkan pada satu waktu.

> **Note**
>
> Setelah Anda membuat set opsi DHCP, Anda tidak dapat memodifikasinya. Untuk memperbarui opsi DHCP untuk VPC Anda, Anda harus membuat set opsi DHCP baru dan kemudian mengaitkannya dengan VPC Anda.

Untuk membuat set opsi DHCP menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih set opsi DHCP.
3. Pilih Buat set opsi DHCP.
4. Untuk pengaturan Tag, secara opsional masukkan nama untuk set opsi DHCP. Jika Anda memasukkan nilai, secara otomatis membuat tag Nama untuk set opsi DHCP.

5. Untuk opsi DHCP, berikan pengaturan konfigurasi yang Anda butuhkan.

   - Nama domain (opsional): Masukkan nama domain yang harus digunakan klien saat menyelesaikan nama host menggunakan DNS. Jika Anda tidak menggunakan AmazonProvided DNS, server nama domain kustom Anda harus menyelesaikan nama host yang sesuai. Jika Anda menggunakan zona host pribadi Amazon Route 53, Anda dapat menggunakan AmazonProvided DNS. Untuk informasi selengkapnya, lihat Atribut DNS untuk VPC Anda.

     > **Note**
     >
     > Hanya gunakan nama domain yang Anda kontrol sepenuhnya.

     Beberapa sistem operasi Linux menerima beberapa nama domain yang dipisahkan oleh spasi. Namun, Windows dan sistem operasi Linux lainnya memperlakukan nilai sebagai domain tunggal, yang menghasilkan perilaku yang tidak terduga. Jika set opsi DHCP Anda dikaitkan dengan VPC yang memiliki instance yang menjalankan sistem operasi yang memperlakukan nilai sebagai domain tunggal, tentukan hanya satu nama domain.

   - Server nama domain (opsional): Masukkan server DNS yang akan digunakan untuk menyelesaikan alamat IP host dari nama host.

     Anda dapat memasukkan salah satu **`AmazonProvidedDNS`** atau server nama domain khusus. Menggunakan keduanya dapat menghasilkan perilaku tak terduga. Anda dapat memasukkan alamat IP hingga empat server nama IPv4 domain (atau hingga tiga server nama IPv4 domain dan**`AmazonProvidedDNS`**) dan empat server nama IPv6 domain yang dipisahkan dengan koma. Meskipun Anda dapat menentukan hingga delapan server nama domain, beberapa sistem operasi mungkin memberlakukan batas bawah. Untuk informasi selengkapnya tentang AmazonProvidedDNS dan server DNS Amazon, lihat. Server Amazon DNS

     > **Important**
     >
     > Jika VPC Anda memiliki gateway internet, pastikan untuk menentukan server DNS Anda sendiri atau server DNS Amazon (AmazonProvidedDNS) untuk nilai server nama Domain. Jika tidak, instance di VPC tidak akan memiliki akses ke DNS, yang menonaktifkan akses internet.

- Server NTP (opsional): Masukkan alamat IP hingga delapan server Network Time Protocol (NTP) (empat IPv4 alamat dan empat alamat). IPv6

  Server NTP menyediakan waktu untuk jaringan Anda. Anda dapat menentukan Layanan Sinkronisasi Waktu Amazon di IPv4 alamat `169.254.169.123` atau IPv6 alamat`fd00:ec2::123`. Instans berkomunikasi dengan Layanan Sinkronisasi Waktu Amazon secara default. Perhatikan bahwa IPv6 alamat hanya dapat diakses pada EC2 instans yang dibangun pada Sistem Nitro.

  Untuk informasi selengkapnya tentang opsi server NTP, lihat RFC 2132. Untuk informasi selengkapnya tentang Layanan Sinkronisasi Waktu Amazon, lihat Mengatur waktu instans Anda di Panduan EC2 Pengguna Amazon.

- Server nama NetBIOS (opsional): Masukkan alamat IP hingga empat server nama NetBIOS.

  Untuk EC2 contoh yang menjalankan OS Windows, nama komputer NetBIOS adalah nama ramah yang ditugaskan ke instance untuk mengidentifikasinya di jaringan. Server nama NetBIOS menyimpan daftar pemetaan antara nama komputer NetBIOS dan alamat jaringan untuk jaringan yang menggunakan NetBIOS sebagai layanan penamaan mereka.

- Jenis node NetBIOS (opsional): Enter**1**,, **24**, atau. **8** Kami menyarankan Anda menentukan **2** (point-to-point atau P-node). Penyiaran dan multicast saat ini tidak di-support. Untuk informasi lebih lanjut tentang jenis node ini, lihat bagian 8.7 dari RFC 2132 dan bagian 10 dari 001. RFC1

  Untuk EC2 contoh yang menjalankan OS Windows, ini adalah metode yang digunakan instance untuk menyelesaikan nama NetBIOS ke alamat IP. Dalam set opsi default, tidak ada nilai untuk jenis node NetBIOS.

- IPv6 Waktu Sewa Pilihan (opsional): Nilai (dalam detik, menit, jam, atau tahun) untuk seberapa sering instance yang berjalan dengan yang IPv6 ditugaskan padanya melewati perpanjangan DHCPv6 sewa. Nilai yang dapat diterima adalah antara 140 dan 2147483647 detik (sekitar 68 tahun). Jika tidak ada nilai yang dimasukkan, waktu sewa default adalah 140 detik. Jika Anda menggunakan pengalamatan jangka panjang untuk EC2 contoh, Anda dapat meningkatkan waktu sewa dan menghindari permintaan perpanjangan sewa yang sering. Perpanjangan sewa biasanya terjadi ketika setengah dari waktu sewa telah berlalu.

6. Tambahkan Tag.
7. Pilih Buat set opsi DHCP. Perhatikan nama atau ID dari set opsi DHCP baru.

8. Untuk mengonfigurasi VPC untuk menggunakan set opsi baru, lihat. Ubah set opsi yang terkait dengan VPC

Untuk membuat opsi DHCP yang ditetapkan untuk VPC Anda menggunakan baris perintah

- create-dhcp-options (AWS CLI)
- New-EC2DhcpOption (AWS Tools for Windows PowerShell)

Ubah set opsi yang terkait dengan VPC

Setelah Anda membuat set opsi DHCP, Anda dapat mengaitkannya dengan satu atau lebih VPCs. Anda hanya dapat mengaitkan satu set opsi DHCP dengan VPC sekaligus. Jika Anda tidak mengaitkan opsi DHCP yang disetel dengan VPC, ini menonaktifkan resolusi nama domain di VPC.

Saat Anda mengaitkan satu set opsi DHCP baru dengan VPC, semua instance yang ada dan semua instance baru yang Anda luncurkan di VPC tersebut menggunakan opsi baru. Anda tidak perlu memulai ulang atau meluncurkan ulang instans Anda. Instans-instans secara otomatis berubah dalam beberapa jam, tergantung pada seberapa sering mereka memperbarui sewa DHCP mereka. Jika Anda lebih suka, Anda dapat secara eksplisit memperbarui sewa menggunakan sistem operasi pada instans.

Untuk mengubah set opsi DHCP yang terkait dengan VPC menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Your VPCs.
3. Pilih kotak centang untuk VPC, lalu pilih Tindakan, Edit pengaturan VPC.
4. Untuk set opsi DHCP, pilih set opsi DHCP baru. Atau, pilih Tidak ada opsi DHCP yang disetel untuk menonaktifkan resolusi nama domain untuk VPC.
5. Pilih Simpan.

Untuk mengubah set opsi DHCP yang terkait dengan VPC menggunakan baris perintah

- associate-dhcp-options (AWS CLI)
- Register-EC2DhcpOption (AWS Tools for Windows PowerShell)

Hapus set opsi DHCP

Bila Anda tidak lagi memerlukan set opsi DHCP, gunakan prosedur berikut untuk menghapusnya. Anda tidak dapat menghapus set opsi DHCP jika sedang digunakan. Untuk setiap VPC yang terkait dengan opsi DHCP yang akan dihapus, Anda harus mengaitkan opsi DHCP yang berbeda yang ditetapkan dengan VPC atau mengonfigurasi VPC agar tidak menggunakan set opsi DHCP. Untuk informasi selengkapnya, lihat the section called “Ubah set opsi yang terkait dengan VPC”.

Untuk menghapus opsi DHCP yang disetel menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih set opsi DHCP.
3. Pilih tombol radio untuk set opsi DHCP, lalu pilih Tindakan, Hapus set opsi DHCP.
4. Ketika diminta untuk konfirmasi, masukkan**`delete`**, dan kemudian pilih Hapus opsi DHCP set.

Untuk menghapus opsi DHCP yang ditetapkan menggunakan baris perintah

- delete-dhcp-options (AWS CLI)
- Remove-EC2DhcpOption (AWS Tools for Windows PowerShell)

Atribut DNS untuk VPC Anda

Sistem Nama Domain(DNS) adalah standar dimana nama yang digunakan di internet diganti menjadi alamat IP yang sesuai. Nama host DNS adalah nama yang secara unik dan tepat untuk komputer; yang terdiri dari nama host dan nama domain. Server DNS mengubah nama host DNS menjadi alamat IP yang sesuai.

Alamat IPv4 publik memungkinkan komunikasi melalui internet, sementara alamat IPv4 pribadi memungkinkan komunikasi dalam jaringan instance. Untuk informasi selengkapnya, lihat Pengalamatan IP untuk VPC dan subnet Anda.

Amazon menyediakan server DNS (Amazon Route 53 Resolver) untuk VPC Anda. Untuk menggunakan server DNS Anda sendiri sebagai gantinya, buat satu set opsi DHCP baru untuk VPC Anda. Untuk informasi selengkapnya, lihat Opsi DHCP ditetapkan di Amazon VPC.

Daftar Isi

- Memahami Amazon DNS

- Lihat nama host DNS untuk instans EC2 Anda
- Melihat dan memperbarui atribut DNS untuk VPC Anda

Memahami Amazon DNS

Sebagai AWS arsitek atau administrator, salah satu komponen jaringan dasar yang akan Anda temui adalah server DNS Amazon, juga dikenal sebagai Route 53 Resolver. Layanan resolver DNS ini terintegrasi secara asli ke setiap Zona Ketersediaan di Wil AWS ayah Anda, memberikan solusi yang andal dan dapat diskalakan untuk resolusi nama domain dalam Virtual Private Cloud (VPC) Anda. Di bagian ini Anda akan belajar tentang alamat IP server DNS Amazon, nama host DNS pribadi yang dapat diselesaikan, dan aturan yang mengatur penggunaannya.

Daftar Isi

- Server Amazon DNS
- Aturan dan pertimbangan
- Nama host DNS untuk instans EC2
- Atribut DNS untuk VPC Anda
- Kuota DNS
- Zona host pribadi

Server Amazon DNS

Route 53 Resolver (juga disebut “server DNS Amazon” atau “AmazonProvidedDNS”) adalah layanan DNS Resolver yang dibangun ke dalam setiap Zona Ketersediaan di suatu AWS Wilayah. Route 53 Resolver terletak di `169.254.169.253` (IPv4), `fd00:ec2::253` (IPv6), dan pada rentang CIDR IPV4 pribadi utama yang disediakan untuk VPC Anda ditambah dua. Misalnya, jika Anda memiliki VPC dengan IPv4 CIDR `10.0.0.0/16` dan IPv6 CIDR`2001:db8::/32`, Anda dapat mencapai Route 53 Resolver di `169.254.169.253` (IPv4), (IPv6), `fd00:ec2::253` atau (IPv4). `10.0.0.2` Sumber daya dalam VPC menggunakan alamat lokal tautan untuk kueri DNS. Kueri ini diangkut ke Route 53 Resolver secara pribadi dan tidak terlihat di jaringan. Dalam IPv6-only subnet, alamat link-lokal IPv4 (169.254.169.253) masih dapat dijangkau selama "AmazonProvidedDNS” adalah server nama dalam set opsi DHCP.

Saat Anda meluncurkan instance ke VPC, kami menyediakan instance dengan nama host DNS pribadi. Kami juga menyediakan nama host DNS publik jika instance dikonfigurasi dengan alamat IPv4 publik dan atribut DNS VPC diaktifkan.

Format nama host DNS pribadi tergantung pada cara Anda mengonfigurasi instance EC2 saat Anda meluncurkannya. Untuk informasi selengkapnya tentang jenis nama host DNS pribadi, lihat jenis nama host instans Amazon EC2 di Panduan Pengguna Amazon EC2.

Server DNS Amazon di VPC Anda digunakan untuk resolve nama domain DNS yang Anda tentukan di zona host pribadi di Route 53. Untuk informasi selengkapnya tentang zona yang di-host pribadi, lihat Bekerja dengan Zona Host Pribadi di Panduan Developer Amazon Route 53.

Aturan dan pertimbangan

Saat menggunakan server DNS Amazon, aturan dan pertimbangan berikut berlaku.

- Anda tidak dapat mem-filter lalu lintas ke atau dari server DNS Amazon menggunakan ACL jaringan atau grup keamanan.
- Layanan yang menggunakan kerangka Hadoop, seperti Amazon EMR, memerlukan instans untuk resolve nama domain mereka sendiri yang sudah sepenuhnya memenuhi syarat (FQDN). Dalam kasus tersebut, resolusi DNS dapat gagal jika opsi `domain-name-servers` diatur ke nilai kustom. Untuk memastikan resolusi DNS yang tepat, pertimbangkan untuk menambahkan forwarder bersyarat pada server DNS Anda untuk meneruskan kueri untuk domain *`region-name`*`.compute.internal` untuk server DNS Amazon. Untuk informasi selengkapnya, lihat Pengaturan sebuah VPC untuk host klaster di Panduan Pengelolaan Amazon EMR.
- Amazon Route 53 Resolver hanya mendukung kueri DNS rekursif.

Nama host DNS untuk instans EC2

Ketika Anda meluncurkan sebuah instance, ia selalu menerima alamat IPv4 pribadi dan nama host DNS pribadi yang sesuai dengan alamat IPv4 pribadinya. Jika instance Anda memiliki alamat IPv4 publik, atribut DNS untuk VPC-nya menentukan apakah instans menerima nama host DNS publik yang sesuai dengan alamat IPv4 publik. Untuk informasi selengkapnya, lihat Atribut DNS untuk VPC Anda.

Dengan server DNS yang disediakan Amazon diaktifkan, nama host DNS diselesaikan sebagai berikut.

Nama DNS IPv4 pribadi

Nama host DNS IPv4 pribadi dari sebuah instance diselesaikan ke alamat IPv4 pribadinya. Anda dapat menggunakan nama host DNS IPv4 pribadi untuk komunikasi antar instance di VPC yang

sama atau di VPC yang terhubung. Untuk informasi selengkapnya, lihat Alamat IPv4 pribadi di Panduan Pengguna Amazon EC2.

Nama DNS IPv4 publik

Nama host DNS IPv4 publik dari sebuah instance diselesaikan ke alamat IPv4 publiknya (di luar jaringan instance) atau alamat IPv4 pribadinya (di dalam jaringan instance). Untuk informasi selengkapnya, lihat Alamat IPv4 Publik di Panduan Pengguna Amazon EC2.

Untuk menyelesaikan nama DNS IPv4 publik ke alamat IPv4 pribadi melalui koneksi peering VPC, Anda harus mengaktifkan resolusi DNS untuk koneksi peering. Untuk informasi selengkapnya, lihat Mengaktifkan resolusi DNS untuk koneksi peering VPC.

Nama DNS sumber daya pribadi

Nama RBN-based DNS yang dapat diselesaikan ke catatan DNS A dan AAAA yang dipilih untuk instance ini. Nama host DNS ini terlihat dalam detail instance untuk instance di dual-stack dan IPv6-only subnet. Untuk informasi selengkapnya tentang RBN, lihat jenis nama host instans EC2 di Panduan Pengguna Amazon EC2.

Atribut DNS untuk VPC Anda

Atribut VPC berikut menentukan dukungan DNS yang disediakan untuk VPC Anda. Jika kedua atribut diaktifkan, instance yang diluncurkan ke VPC menerima nama host DNS publik jika ditetapkan alamat IPv4 publik atau alamat IP Elastic saat pembuatan. Jika Anda mengaktifkan kedua atribut untuk VPC yang sebelumnya tidak mengaktifkan keduanya, instance yang sudah diluncurkan ke VPC tersebut menerima nama host DNS publik jika mereka memiliki alamat IPv4 publik atau alamat IP Elastic.

Untuk memeriksa apakah atribut ini diaktifkan untuk VPC Anda, lihatMelihat dan memperbarui atribut DNS untuk VPC Anda.

Atribut	Deskripsi
`enableDnsHostnames`	Menentukan apakah VPC mendukung penetapan nama host DNS publik ke instans dengan alamat IP publik. Default untuk atribut ini adalah `false` kecuali VPC adalah VPC default. Perhatikan A turan dan pertimbangan untuk atribut ini di bawah ini.

Atribut	Deskripsi
`enableDnsSupport`	Menentukan apakah VPC mendukung resolusi DNS melalui server DNS yang disediakan Amazon. Jika atribut ini`true`, kueri ke server DNS yang disediakan Amazon berhasil. Untuk informasi selengkapnya, lihat Server Amazon DNS. Default untuk atribut ini adalah`true`. Perhatikan A turan dan pertimbangan untuk atribut ini di bawah ini.

Aturan dan pertimbangan

- Jika kedua atribut diatur ke `true`, hal berikut ini terjadi:
  - Instans dengan alamat IP publik menerima nama host DNS publik yang sesuai.
  - Server Resolver Route 53 dapat menyelesaikan nama host DNS Amazon-provided pribadi.
- Jika setidaknya salah satu atribut disetel ke`false`, hal berikut terjadi:
  - Instans dengan alamat IP publik tidak menerima nama host DNS publik yang sesuai.
  - Resolver Route 53 tidak dapat menyelesaikan nama Amazon-provided host DNS pribadi.
  - Instans-instans menerima nama host DNS pribadi kustom jika ada nama domain kustom di kumpulan opsi DHCP. Jika Anda tidak menggunakan server Resolver Route 53, server nama domain kustom Anda harus menyelesaikan nama host yang sesuai.
- Jika Anda menggunakan nama domain DNS kustom yang ditentukan di zona host pribadi di Amazon Route 53, atau menggunakan DNS pribadi dengan antarmuka VPC endpoints (AWS PrivateLink), Anda harus menyetel `enableDnsSupport` atribut `enableDnsHostnames` dan ke. `true`
- Route 53 Resolver dapat menyelesaikan nama host DNS pribadi ke alamat IPv4 pribadi untuk semua ruang alamat, termasuk di mana rentang alamat IPv4 VPC Anda berada di luar rentang alamat IPv4 pribadi yang ditentukan oleh RFC 1918. https://tools.ietf.org/html/rfc1918 Namun, jika Anda membuat VPC sebelum Oktober 2016, Resolver Route 53 tidak menyelesaikan nama host DNS pribadi jika rentang alamat IPv4 VPC Anda berada di luar rentang ini. Untuk mengaktifkan support untuk ini, hubungi Dukungan.

Kuota DNS

Ada batas 1024 paket per detik (PPS) untuk layanan yang menggunakan alamat link-local. Batas ini mencakup agregat permintaan DNS Resolver Route 53, permintaan Instance Metadata Service (IMDS), permintaan Amazon Time Service Network Time Protocol (NTP), dan permintaan Layanan Lisensi Windows (untuk instans berbasis Microsoft Windows). Kuota ini tidak dapat dinaikkan jumlahnya.

Jumlah kueri DNS per detik yang didukung oleh Route 53 Resolver bervariasi berdasarkan jenis kueri, ukuran respons, dan protokol yang digunakan. Untuk informasi selengkapnya dan rekomendasi untuk arsitektur DNS yang dapat diskalakan, lihat Panduan AWS Teknis DNS Hybrid dengan Active Directory.

Jika Anda mencapai kuota, Resolver Route 53 menolak lalu lintas. Beberapa penyebab untuk mencapai kuota mungkin masalah pelambatan DNS, atau kueri metadata instance yang menggunakan antarmuka jaringan Resolver Route 53. Untuk informasi tentang cara memecahkan masalah throttling DNS VPC, lihat Bagaimana saya dapat menentukan apakah kueri DNS saya ke Amazon dengan adanya server DNS gagal disebabkan throttling DNS VOC. Untuk informasi tentang pengambilan metadata instans, lihat Mengambil metadata instans di Panduan Pengguna Amazon EC2.

Zona host pribadi

Untuk mengakses sumber daya di VPC menggunakan nama domain DNS khusus, seperti`example.com`, alih AWS-alih menggunakan alamat IPv4 pribadi atau nama host DNS pribadi yang disediakan, Anda dapat membuat zona host pribadi di Route 53. Zona host pribadi adalah wadah yang menyimpan informasi tentang bagaimana Anda ingin mengarahkan lalu lintas untuk domain dan subdomainnya dalam satu atau lebih VPC tanpa mengekspos sumber daya Anda ke internet. Anda kemudian dapat membuat kumpulan catatan sumber daya Route 53, yang menentukan bagaimana Route 53 menanggapi kueri untuk domain dan subdomain Anda. Misalnya, jika Anda ingin browser meminta example.com diarahkan ke server web di VPC Anda, Anda akan membuat catatan A di zona host pribadi Anda dan menentukan alamat IP atas server web tersebut. Untuk informasi selengkapnya tentang membuat sebuah zona yang di-hosting privat, lihat Bekerja dengan Zona yang di-hosting privat di Panduan Developer Amazon Route 53.

Untuk mengakses sumber daya menggunakan nama domain DNS kustom, Anda harus terhubung ke sebuah instans dalam VPC Anda. Dari instans Anda, Anda dapat menguji bahwa sumber daya Anda di zona host pribadi Anda dapat diakses dari nama DNS kustom dengan menggunakan perintah `ping`; sebagai contoh, `ping mywebserver.example.com`. (Anda harus memastikan bahwa

aturan grup keamanan instans Anda mengizinkan lalu lintas inbound ICMP untuk perintah `ping` untuk bekerja.)

Zona yang dihosting pribadi tidak mendukung hubungan transitif di luar VPC; misalnya, Anda tidak dapat mengakses sumber daya menggunakan nama DNS pribadi kustom mereka dari sisi lain koneksi VPN.

> **Important**
>
> Jika Anda menggunakan nama domain DNS khusus yang ditentukan di zona host pribadi di Amazon Route 53, Anda harus menyetel `enableDnsSupport` atribut `enableDnsHostnames` dan `ketrue`.

Lihat nama host DNS untuk instans EC2 Anda

Anda dapat melihat nama host DNS untuk sebuah instans yang berjalan atau antarmuka jaringan menggunakan konsol Amazon EC2 atau baris perintah. Mengetahui nama host ini penting untuk menghubungkan ke sumber daya Anda.

Kolom DNS Publik (IPv4) dan DNS Pribadi tersedia ketika opsi DNS diaktifkan untuk VPC yang terkait dengan instans. Untuk informasi selengkapnya, lihat the section called “Atribut DNS untuk VPC Anda”.

Instans

Untuk melihat nama host DNS untuk sebuah instans menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Instans.
3. Pilih Instans Anda dari daftar.
4. Di panel rincian, DNS Publik (IPv4) dan DNS Pribadi menampilkan nama host DNS, jika ada.

Untuk melihat nama host DNS untuk sebuah instans menggunakan baris perintah

- describe-instances (AWS CLI)
- Get-EC2Instance (AWS Tools for Windows PowerShell)

Antarmuka jaringan

Untuk melihat nama host DNS pribadi untuk antarmuka jaringan menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Antarmuka Jaringan.
3. Pilih antarmuka jaringan dari daftar.
4. Di panel rincian, kolom DNS Pribadi (IPv4) menampilkan nama host DNS pribadi.

Untuk melihat nama host DNS untuk antarmuka jaringan menggunakan baris perintah

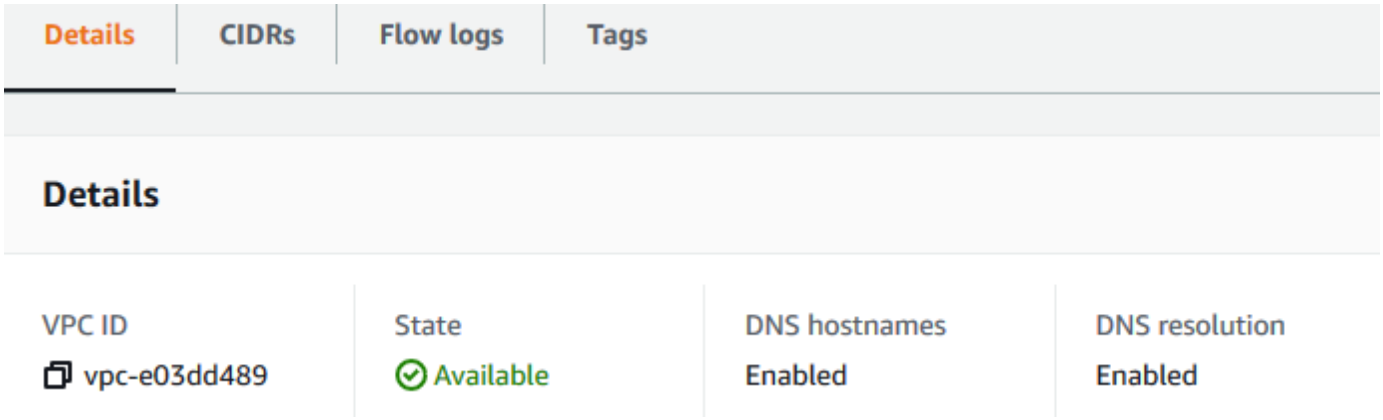
- describe-network-interfaces (AWS CLI)
- Get-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Melihat dan memperbarui atribut DNS untuk VPC Anda

Anda dapat melihat dan memperbarui atribut support DNS untuk VPC Anda menggunakan konsol Amazon VPC. Pengaturan ini mengontrol apakah instans Anda mendapatkan nama host DNS publik dan apakah server DNS Amazon dapat menyelesaikan nama DNS pribadi Anda. Mengkonfigurasi atribut ini dengan benar sangat penting untuk memastikan komunikasi yang lancar dalam VPC Anda.

Untuk menjelaskan dan memperbarui support DNS untuk VPC menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih VPC Anda.
3. Pilih kotak centang untuk VPC.
4. Tinjau informasi di Detail. Dalam contoh ini, nama host DNS dan resolusi DNS diaktifkan.



5. Untuk memperbarui pengaturan ini, pilih Tind akan, lalu pilih Edit pengaturan VPC. Pilih atau hapus Aktifkan pada atribut DNS yang sesuai dan pilih Simpan perubahan.

Untuk mendeskripsikan support DNS untuk VPC menggunakan baris perintah

- describe-vpc-attribute (AWS CLI)
- Get-EC2VpcAttribute (AWS Tools for Windows PowerShell)

Untuk memperbarui support DNS untuk VPC menggunakan baris perintah

- modify-vpc-attribute (AWS CLI)
- Edit-EC2VpcAttribute (AWS Tools for Windows PowerShell)

Penggunaan Alamat Jaringan untuk VPC Anda

Penggunaan Alamat Jaringan (NAU) adalah metrik yang diterapkan ke sumber daya di jaringan virtual Anda untuk membantu Anda merencanakan dan memantau ukuran VPC Anda. Setiap unit NAU berkontribusi pada total yang mewakili ukuran VPC Anda.

Penting untuk memahami jumlah total unit yang membentuk NAU VPC Anda karena kuota VPC berikut membatasi ukuran VPC:

- Penggunaan Alamat Jaringan — Jumlah maksimum unit NAU yang dapat dimiliki oleh satu VPC. Setiap VPC dapat memiliki hingga 64.000 unit NAU secara default. Anda dapat meminta kenaikan kuota hingga 256.000.
- Penggunaan Alamat Jaringan Peered — Jumlah maksimum unit NAU untuk VPC dan semua VPC yang diintip. Jika VPC diintip dengan VPC lain di Wilayah yang sama, gabungan VPC dapat memiliki hingga 128.000 unit NAU secara default. Anda dapat meminta kenaikan kuota hingga 512.000. Kuota ini berlaku untuk peering antar VPC di Wilayah yang sama, termasuk peering antar VPC di akun yang berbeda. AWS VPC yang diintip di berbagai Wilayah tidak berkontribusi pada kuota ini.

Anda dapat menggunakan NAU dengan cara berikut:

- Sebelum Anda membuat jaringan virtual Anda, hitung unit NAU untuk membantu Anda memutuskan apakah Anda harus menyebarkan beban kerja di beberapa VPC.

- Setelah Anda membuat VPC, gunakan Amazon CloudWatch untuk memantau penggunaan VPC NAU sehingga tidak tumbuh melampaui kuota NAU Anda. Kami menyarankan Anda membuat CloudWatch alarm Amazon untuk memantau kuota NAU. Untuk informasi selengkapnya, lihat the section called “CloudWatch metrik”.

Melebihi Kuota NAU

Jika Anda melebihi kuota NAU untuk VPC Anda, panggilan API berikut gagal dengan pengecualian sisi klien:

- `RunInstances`
- `AttachNetworkInterface`
- `AssignPrivateIpAddresses`
- `AssignIpv6Addresses`
- `AcceptVpcPeeringConnection`

Pengecualian spesifik tergantung pada kuota yang Anda melebihi:

- `NetworkAddressUsageLimitExceeded`— VPC melebihi kuota NAU-nya.
- `NetworkAddressUsagePeeredLimitExceeded`— VPC melebihi kuota NAU Peered-VPC.

Kegagalan ini memengaruhi kemampuan Anda untuk meluncurkan instans, melampirkan antarmuka jaringan, menetapkan alamat baru, menerima koneksi peering VPC, dan menskalakan atau mengelola beban kerja di VPC yang terpengaruh. Untuk menghindari gangguan, pantau penggunaan NAU dengan Amazon CloudWatch dan minta kenaikan sebelum Anda mencapai kuota.

Bagaimana NAU dihitung

Jika Anda memahami bagaimana NAU dihitung, ini dapat membantu Anda merencanakan penskalaan VPC Anda.

Tabel berikut menjelaskan sumber daya mana yang membentuk jumlah NAU dalam VPC dan berapa banyak unit NAU yang digunakan setiap sumber daya. Beberapa AWS sumber daya direpresentasikan sebagai unit NAU tunggal dan beberapa sumber daya direpresentasikan sebagai beberapa unit NAU. Anda dapat menggunakan tabel untuk mempelajari bagaimana NAU dihitung.

Sumber daya	Unit NAU
Setiap IPv4 pribadi atau publik dan setiap alamat IPv6 yang ditetapkan ke antarmuka jaringan untuk instance EC2 di VPC	1
Antarmuka jaringan tambahan yang terpasang ke instance EC2	1
Awalan ditetapkan ke antarmuka jaringan	1
Penyeimbang Beban Jaringan untuk AZ	6
Penyeimbang Beban Gateway untuk AZ	6
Titik akhir VPC untuk AZ	6
Lampiran gateway transit	6
Fungsi lambda	6
Gateway NAT	6
Target pemasangan EFS	6
Antarmuka EFA (EFA dengan perangkat ENA) atau antarmuka EFA-only	1
Amazon EKS pod	1

Contoh NAU

Contoh berikut menunjukkan cara menghitung NAU.

Contoh 1 - Dua VPC terhubung menggunakan peering VPC

VPC yang diintip di Wilayah yang sama berkontribusi pada kuota NAU gabungan.

- VPC1
  - 50 Penyeimbang Beban Jaringan dalam 2 subnet di Zona Ketersediaan terpisah - 600 unit NAU
  - 5.000 instance (masing-masing dengan alamat IPv4 dan alamat IPv6) dalam satu subnet dan 5.000 instans (masing-masing dengan alamat IPv4 dan alamat IPv6) di subnet lain - 20.000 unit
  - 100 fungsi Lambda - 600 unit NAU

- VPC 2
  - 50 Penyeimbang Beban Jaringan dalam 2 subnet di Zona Ketersediaan terpisah - 600 unit NAU
  - 5.000 instance (masing-masing dengan alamat IPv4 dan alamat IPv6) dalam satu subnet dan 5.000 instans (masing-masing dengan alamat IPv4 dan alamat IPv6) di subnet lain - 20.000 unit
  - 100 fungsi Lambda - 600 unit NAU
- Jumlah NAU peering total: 42.400 unit
- Kuota PEERING NAU default: 128.000 unit

Contoh 2 - Dua VPC terhubung menggunakan gateway transit

VPC yang terhubung menggunakan gateway transit tidak berkontribusi pada kuota NAU gabungan seperti yang mereka lakukan untuk VPC yang diintip.

- VPC1
  - 50 Penyeimbang Beban Jaringan dalam 2 subnet di Zona Ketersediaan terpisah - 600 unit NAU
  - 5.000 instance (masing-masing dengan alamat IPv4 dan alamat IPv6) dalam satu subnet dan 5.000 instans (masing-masing dengan alamat IPv4 dan alamat IPv6) di subnet lain - 20.000 unit
  - 100 fungsi Lambda - 600 unit NAU
- VPC 2
  - 50 Penyeimbang Beban Jaringan dalam 2 subnet di Zona Ketersediaan terpisah - 600 unit NAU
  - 5.000 instance (masing-masing dengan alamat IPv4 dan alamat IPv6) dalam satu subnet dan 5.000 instans (masing-masing dengan alamat IPv4 dan alamat IPv6) di subnet lain - 20.000 unit
  - 100 fungsi Lambda - 600 unit NAU
- Jumlah NAU total per VPC: 21.200 unit
- Kuota NAU default per VPC: 64.000 unit

Contoh 3 - Dua VPC terhubung menggunakan peering VPC lintas wilayah

VPC yang diintip di berbagai Wilayah tidak berkontribusi pada kuota NAU gabungan. AWS mengevaluasi setiap VPC terhadap kuota NAU per VPC miliknya sendiri, dan sumber daya rekan lintas wilayah tidak diperhitungkan dalam NAU yang diintip oleh VPC. Contoh ini mengasumsikan satu-satunya peering setiap VPC adalah peering lintas wilayah yang ditampilkan (tidak ada rekan intra-wilayah tambahan).

- VPC 1 (Wilayah A)

  - 50 Penyeimbang Beban Jaringan dalam 2 subnet di Zona Ketersediaan terpisah - 600 unit NAU
  - 5.000 instance (masing-masing dengan alamat IPv4 dan alamat IPv6) dalam satu subnet dan 5.000 instans (masing-masing dengan alamat IPv4 dan alamat IPv6) di subnet lain - 20.000 unit
  - 100 fungsi Lambda - 600 unit NAU
- VPC 2 (Wilayah B)
  - 50 Penyeimbang Beban Jaringan dalam 2 subnet di Zona Ketersediaan terpisah - 600 unit NAU
  - 5.000 instance (masing-masing dengan alamat IPv4 dan alamat IPv6) dalam satu subnet dan 5.000 instans (masing-masing dengan alamat IPv4 dan alamat IPv6) di subnet lain - 20.000 unit
  - 100 fungsi Lambda - 600 unit NAU
- Jumlah NAU total per VPC: 21.200 unit
- Kuota NAU default per VPC: 64.000 unit
- Jumlah NAU yang dipeered per VPC: 21.200 unit (hanya sumber daya VPC sendiri yang dihitung; rekan lintas wilayah berkontribusi 0)
- Kuota NAU yang diintip default per VPC: 128.000 unit (rekan lintas wilayah tidak dihitung dalam kuota ini)

Bagikan subnet VPC Anda dengan akun lain

Berbagi subnet VPC memungkinkan beberapa orang Akun AWS untuk membuat sumber daya aplikasi mereka, seperti instans Amazon EC2, database Amazon Relational Database Service (RDS), cluster Amazon Redshift, dan AWS Lambda fungsi, menjadi cloud pribadi virtual (VPC) bersama yang dikelola secara terpusat. Dalam model ini, akun yang memiliki VPC (pemilik) berbagi satu atau lebih subnet dengan akun lain (peserta) milik organisasi yang sama. AWS Organizations Setelah subnet dibagikan, peserta dapat melihat, membuat, mengubah, dan menghapus sumber daya aplikasi mereka di subnet yang dibagikan dengan mereka. Peserta tidak dapat melihat, mengubah, atau menghapus sumber daya milik peserta lain atau pemilik VPC.

Anda dapat berbagi subnet VPC untuk menggunakan routing implisit dalam VPC untuk aplikasi yang memerlukan tingkat interkonektivitas tinggi dan berada dalam batas kepercayaan yang sama. Hal ini mengurangi jumlah VPC yang Anda buat dan kelola, saat menggunakan akun terpisah untuk penagihan dan kontrol akses. Anda dapat menyederhanakan topologi jaringan dengan menghubungkan subnet Amazon VPC bersama menggunakan fitur konektivitas, seperti gateway transit AWS PrivateLink, dan peering VPC. Untuk informasi selengkapnya tentang manfaat berbagi subnet VPC, lihat Berbagi VPC: Pendekatan baru untuk beberapa akun dan manajemen VPC.

Ada kuota yang terkait dengan berbagi subnet VPC. Untuk informasi selengkapnya, lihat Berbagi subnet VPC.

Daftar Isi

- Prasyarat subnet bersama
- Bekerja dengan subnet bersama
- Penagihan dan pengukuran untuk pemilik dan peserta
- Tanggung jawab dan izin untuk pemilik dan peserta
- AWS sumber daya dan subnet VPC bersama

Prasyarat subnet bersama

Bagian ini berisi prasyarat untuk bekerja dengan subnet bersama:

- Akun untuk pemilik dan peserta VPC harus dikelola oleh AWS Organizations.
- Anda harus mengaktifkan berbagi sumber daya di AWS RAM konsol dari akun manajemen untuk organisasi Anda. Untuk informasi selengkapnya, lihat Meng aktifkan berbagi sumber daya AWS Organizations di dalam Panduan AWS RAM Pengguna.
- Anda harus membuat berbagi sumber daya. Anda dapat menentukan subnet yang akan dibagikan saat Anda membuat berbagi sumber daya, atau menambahkan subnet ke berbagi sumber daya nanti menggunakan prosedur di bagian berikutnya. Untuk informasi selengkapnya, lihat Membuat berbagi sumber daya di Panduan AWS RAM Pengguna.

Bekerja dengan subnet bersama

Bagian ini menjelaskan cara bekerja dengan subnet bersama di AWS konsol dan AWS CLI.

Daftar Isi

- Membagikan subnet
- Membatalkan pembagian subnet bersama
- Mengidentifikasi pemilik subnet bersama

Membagikan subnet

Anda dapat berbagi subnet non-default dengan akun lain dalam organisasi Anda sebagai berikut. Selain itu, Anda dapat berbagi grup keamanan di seluruh AWS Organisasi. Untuk informasi selengkapnya, lihat Bagikan grup keamanan dengan AWS Organizations.

Untuk membagikan subnet menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Subnet.
3. Pilih subnet Anda dan pilih Tindakan, Bagikan subnet.
4. Pilih pembagian sumber daya Anda dan pilih Bagikan subnet.

Untuk berbagi subnet menggunakan AWS CLI

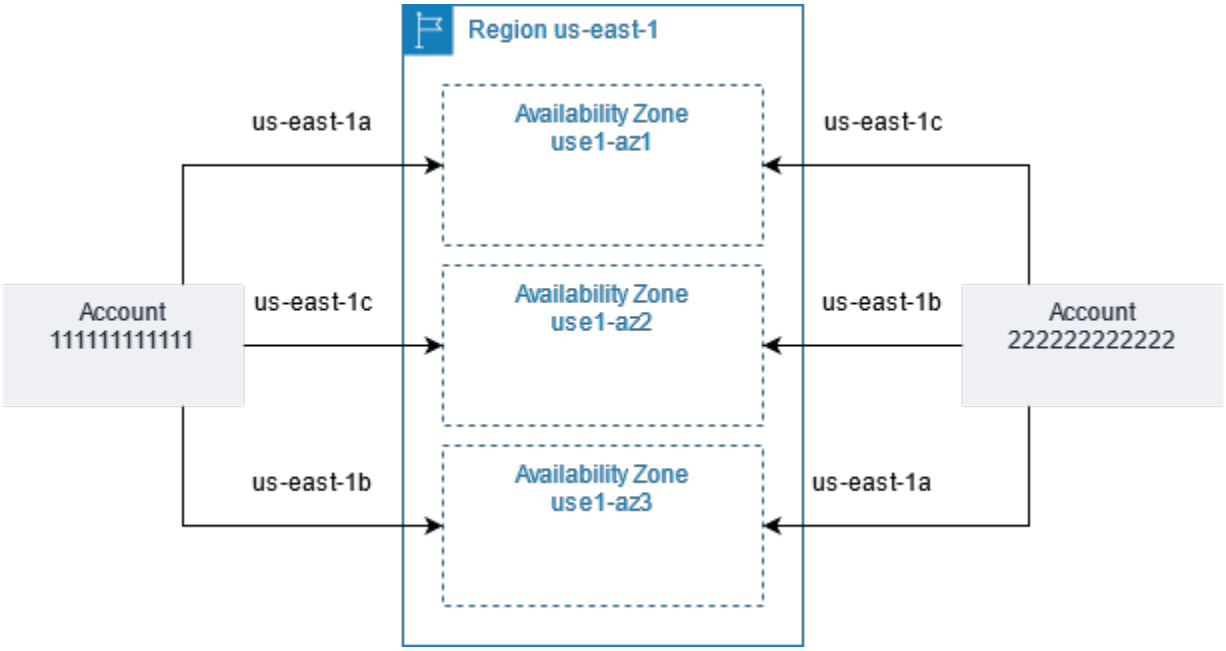
Gunakan perintah create-resource-share dan associate-resource-share.

Memetakan subnet di seluruh Availability Zone

Untuk memastikan bahwa sumber daya didistribusikan di seluruh Availability Zone untuk suatu Wilayah, kami secara independen memetakan Availability Zone untuk nama masing-masing akun. Misalnya, Zona Ketersediaan `us-east-1a` untuk AWS akun Anda mungkin tidak memiliki lokasi yang sama `us-east-1a` dengan AWS akun lain.

Untuk mengoordinasikan Zona Ketersediaan di seluruh akun untuk berbagi VPC, Anda harus menggunakan ID AZ, yang merupakan pengidentifikasi unik dan konsisten untuk Zona Ketersediaan. Misalnya, `use1-az1` ID AZ untuk salah satu Zona Ketersediaan di Wil `us-east-1` ayah. Gunakan ID AZ untuk menentukan lokasi sumber daya dalam satu akun relatif terhadap akun lain. Anda dapat melihat ID AZ untuk setiap subnet di konsol Amazon VPC.

Diagram berikut menggambarkan dua akun dengan pemetaan kode Zona Ketersediaan yang berbeda ke ID AZ.



Membatalkan pembagian subnet bersama

Pemilik dapat membatalkan pembagian subnet bersama dengan para peserta kapan saja. Setelah pemilik membatalkan pembagian subnet bersama, berlaku aturan berikut:

- Sumber daya peserta yang ada terus berjalan di subnet yang tidak dibagikan. AWS layanan terkelola (misalnya, Elastic Load Balancing) yang memiliki automated/managed alur kerja (seperti penskalaan otomatis atau penggantian node) mungkin memerlukan akses berkelanjutan ke subnet bersama untuk beberapa sumber daya.
- Peserta tidak dapat lagi membuat sumber daya baru di subnet yang pembagiannya dibatalkan.
- Peserta dapat mengubah, menjelaskan, dan menghapus sumber daya mereka yang ada di subnet.
- Jika peserta masih memiliki sumber daya di subnet yang pembagiannya dibatalkan, pemilik tidak dapat menghapus subnet bersama atau VPC subnet bersama. Pemilik hanya dapat menghapus subnet atau VPC subnet bersama setelah peserta menghapus semua sumber daya di subnet yang pembagiannya dibatalkan.

Untuk membatalkan pembagian subnet menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Subnet.
3. Pilih subnet Anda dan pilih Tindakan, Batalkan pembagian subnet.

4. Pilih Tindakan, Hentikan pembagian.

Untuk membatalkan berbagi subnet menggunakan AWS CLI

Gunakan perintah disassociate-resource-share.

Mengidentifikasi pemilik subnet bersama

Peserta dapat melihat subnet yang telah dibagikan dengan mereka dengan menggunakan konsol Amazon VPC, atau alat baris perintah.

Untuk mengidentifikasi pemilik subnet menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Subnet. Kolom Pemilik menampilkan pemilik subnet.

Untuk mengidentifikasi pemilik subnet menggunakan AWS CLI

Gunakan perintah describe-subnets and describe-vpcs, yang meliputi ID pemilik di outputnya.

Penagihan dan pengukuran untuk pemilik dan peserta

Bagian ini berisi rincian penagihan dan pengukuran bagi mereka yang memiliki subnet bersama dan bagi mereka yang bekerja dengan subnet bersama:

- Dalam VPC bersama, setiap peserta membayar sumber daya aplikasi mereka termasuk instans Amazon EC2, database Amazon Relational Database Service, cluster Amazon Redshift, dan fungsi. AWS Lambda Peserta juga membayar biaya transfer data yang terkait dengan transfer data Zona Interavailabilitas serta transfer data melalui koneksi peering VPC, lintas gateway internet, dan lintas gateway. AWS Direct Connect
- Pemilik VPC membayar biaya per jam (jika berlaku), biaya pemrosesan data dan transfer data di seluruh gateway NAT, gateway pribadi virtual, gateway transit, dan titik akhir VPC. AWS PrivateLink Selain itu, alamat IPv4 publik yang digunakan dalam VPC bersama ditagih kepada pemilik VPC. Untuk informasi selengkapnya tentang harga alamat IPv4 publik, lihat tab Alamat IPv4 Publik di halaman harga Amazon VPC.
- Transfer data dalam Zona Ketersediaan yang sama (diidentifikasi secara unik menggunakan AZ-ID) gratis terlepas dari kepemilikan akun dari sumber daya komunikasi.

Tanggung jawab dan izin untuk pemilik dan peserta

Bagian ini mencakup rincian tentang tanggung jawab dan izin bagi mereka yang memiliki subnet bersama (pemilik) dan bagi mereka yang menggunakan subnet bersama (peserta).

Sumber daya pemilik

Pemilik bertanggung jawab atas sumber daya VPC yang mereka miliki. Pemilik VPC bertanggung jawab untuk membuat, mengelola, dan menghapus sumber daya yang terkait dengan VPC bersama. Ini termasuk subnet, tabel rute, ACL jaringan, koneksi peering, titik akhir gateway, titik akhir antarmuka, titik akhir Route 53 Resolver, gateway internet, gateway NAT, gateway pribadi virtual, dan lampiran gateway transit.

Sumber daya peserta

Peserta bertanggung jawab atas sumber daya VPC yang mereka miliki. Peserta dapat membuat kumpulan sumber daya VPC terbatas dalam VPC bersama. Misalnya, peserta dapat membuat antarmuka jaringan dan grup keamanan, dan mengaktifkan log aliran VPC untuk antarmuka jaringan yang mereka miliki. Sumber daya VPC yang dibuat peserta dihitung terhadap kuota VPC di akun peserta, bukan akun pemilik. Untuk informasi selengkapnya, lihat Berbagi subnet VPC.

Sumber daya VPC

Tanggung jawab dan izin berikut berlaku untuk sumber daya VPC saat bekerja dengan subnet VPC bersama:

Log alur

- Peserta dapat membuat, menghapus, dan menjelaskan log alur untuk antarmuka jaringan yang mereka miliki di subnet VPC bersama.
- Peserta tidak dapat membuat, menghapus, atau menjelaskan log alur untuk antarmuka jaringan yang tidak mereka miliki di subnet VPC bersama.
- Peserta tidak dapat membuat, menghapus, atau menjelaskan log alur untuk subnet VPC bersama.
- Pemilik VPC dapat membuat, menghapus, dan menjelaskan log alur untuk antarmuka jaringan yang tidak mereka miliki di subnet VPC bersama.
- Pemilik VPC dapat membuat, menghapus, dan menjelaskan log alur untuk subnet VPC bersama.
- Pemilik VPC tidak dapat menjelaskan atau menghapus log alur yang dibuat oleh peserta.

Gerbang internet dan gateway internet khusus keluar

- Peserta tidak dapat membuat, melampirkan, atau menghapus gateway internet dan gateway internet khusus keluar di subnet VPC bersama. Peserta dapat menggambarkan gateway internet dalam subnet VPC bersama. Peserta tidak dapat menggambarkan gateway internet khusus keluar di subnet VPC bersama.

Gateway NAT

- Peserta tidak dapat membuat, menghapus, atau menjelaskan gateway NAT di subnet VPC bersama.

Daftar kontrol akses jaringan (NACL)

- Peserta tidak dapat membuat, menghapus, atau mengganti NACL di subnet VPC bersama. Peserta dapat menjelaskan NACL yang dibuat oleh pemilik VPC di subnet VPC bersama.

Antarmuka jaringan

- Peserta dapat membuat antarmuka jaringan di subnet VPC bersama. Peserta tidak dapat bekerja dengan antarmuka jaringan yang dibuat oleh pemilik VPC di subnet VPC bersama dengan cara lain, seperti melampirkan, melepaskan, atau memodifikasi antarmuka jaringan. Peserta dapat memodifikasi atau menghapus antarmuka jaringan di VPC bersama yang mereka buat. Misalnya, peserta dapat mengaitkan atau memisahkan alamat IP dengan antarmuka jaringan yang mereka buat.
- Pemilik VPC dapat menggambarkan antarmuka jaringan yang dimiliki oleh peserta dalam subnet VPC bersama. Pemilik VPC tidak dapat bekerja dengan antarmuka jaringan yang dimiliki oleh peserta dengan cara lain, seperti melampirkan, melepaskan, atau memodifikasi antarmuka jaringan yang dimiliki oleh peserta dalam subnet VPC bersama.

Tabel rute

- Peserta tidak dapat bekerja dengan tabel rute (misalnya, membuat, menghapus, atau mengaitkan tabel rute) di subnet VPC bersama. Peserta dapat menjelaskan tabel rute dalam subnet VPC bersama.

Grup keamanan

- Peserta dapat bekerja dengan (membuat, menghapus, mendeskripsikan, memodifikasi, atau membuat aturan masuk dan keluar untuk) grup keamanan yang mereka miliki di subnet VPC bersama. Peserta dapat bekerja dengan grup keamanan yang dibuat oleh pemilik VPC jika pemilik VPC berbagi grup keamanan dengan peserta.
- Peserta dapat membuat aturan di grup keamanan yang mereka miliki yang merujuk grup keamanan milik peserta lain atau pemilik VPC sebagai berikut: account- - number/security group-id
- Peserta tidak dapat meluncurkan instans menggunakan grup keamanan default untuk VPC karena itu milik pemilik.
- Peserta tidak dapat meluncurkan instans menggunakan grup keamanan non-default yang dimiliki oleh pemilik VPC atau peserta lain kecuali grup keamanan di bagikan dengan mereka.
- Pemilik VPC dapat menjelaskan grup keamanan yang dibuat oleh peserta dalam subnet VPC bersama. Pemilik VPC tidak dapat bekerja dengan grup keamanan yang dibuat oleh peserta dengan cara lain. Misalnya, pemilik VPC tidak dapat meluncurkan instans menggunakan grup keamanan yang dibuat oleh peserta.

Subnet

- Peserta tidak dapat memodifikasi subnet bersama atau atribut terkaitnya. Hanya pemilik VPC yang bisa. Peserta dapat menggambarkan subnet dalam subnet VPC bersama.
- Pemilik VPC dapat berbagi subnet hanya dengan akun lain atau unit organisasi yang berada di organisasi yang sama dari AWS Organisasi. Pemilik VPC tidak dapat berbagi subnet yang berada di VPC default.

Transit gateway

- Hanya pemilik VPC yang dapat melampirkan gateway transit ke subnet VPC bersama. Peserta tidak bisa.

VPC

- Peserta tidak dapat memodifikasi VPC atau atribut terkait mereka. Hanya pemilik VPC yang bisa. Peserta dapat menggambarkan VPC, sikap mereka, dan set opsi DHCP.
- Tag dan tag VPC untuk sumber daya dalam VPC bersama tidak dibagikan dengan peserta.

- Peserta dapat mengaitkan grup keamanan mereka sendiri dengan VPC bersama. Hal ini memungkinkan peserta untuk menggunakan grup keamanan dengan antarmuka jaringan Elastic yang mereka miliki di VPC bersama.

AWS sumber daya dan subnet VPC bersama

Sumber daya Layanan AWS dukungan berikut di subnet VPC bersama. Untuk informasi lebih lanjut, ikuti tautan ke dokumentasi layanan yang sesuai.

- Amazon Aurora
- AWS Database Migration Service
- Amazon EC2
- Amazon ECS
- Amazon ElastiCache (Redis OSS)
- Amazon EFS
- Layanan Amazon Elastic Kubernetes
- Elastic Load Balancing
  - Penyeimbang Beban Aplikasi
  - Penyeimbang Beban Gateway
  - Penyeimbang Beban Jaringan
- Amazon EMR
- AWS Glue
- AWS Lambda
- Amazon MQ menjalankan Apache MQ (bukan Rabbit MQ)
- Amazon MSK
- AWS Network Manager
  - AWS Cloud WAN
  - Penganalisis Akses Jaringan
  - Reachability Analyzer
- OpenSearch Layanan Amazon
- AWS PrivateLink†
- Layanan Database Relasional Amazon (RDS)

- Amazon Redshift
- Rute Amazon 53
- Studio SageMaker Terpadu Amazon
- AWS Transit Gateway
- Akses Terverifikasi AWS
- Amazon VPC
  - Mengintip
  - Pencerminan Lalu Lintas
- Amazon VPC Lattice

† Anda dapat terhubung ke semua AWS layanan yang mendukung PrivateLink penggunaan titik akhir VPC di VPC bersama. Untuk daftar layanan yang mendukung PrivateLink, lihat AWS layanan yang terintegrasi dengan AWS PrivateLink dalam AWS PrivateLink Panduan.

Daftar ini dimaksudkan untuk menyertakan semua layanan yang mendukung peluncuran sumber daya di subnet VPC bersama. Terlepas dari upaya terbaik kami, mungkin ada layanan yang mendukung peluncuran sumber daya di subnet VPC bersama tetapi tidak tercantum di sini. Kami mendorong Anda untuk mengirimkan umpan balik dokumentasi jika Anda memiliki pertanyaan.

Memperluas VPC ke Zona Lokal, Zona Panjang Gelombang, atau Pos Terdepan

Anda dapat meng-host sumber daya VPC, seperti subnet, di beberapa lokasi di seluruh dunia. Lokasi ini terdiri dari Wilayah, Availability Zones, Local Zones, dan Wavelength Zones. Setiap Wilayah adalah wilayah geografis yang terpisah.

- Availability Zones adalah beberapa lokasi terisolasi di setiap Wilayah.
- Local Zones membuat Anda dapat menempatkan sumber daya, seperti komputasi dan penyimpanan, di beberapa lokasi yang lebih dekat dengan pengguna akhir Anda.
- AWS Outposts menghadirkan AWS layanan asli, infrastruktur, dan model operasi ke hampir semua pusat data, ruang co-location, atau fasilitas lokal.
- Wavelength Zone memungkinkan developer membangun aplikasi yang menghadirkan latensi sangat rendah ke perangkat 5G dan pengguna akhir. Wavelength menyebarkan layanan AWS komputasi dan penyimpanan standar ke tepi jaringan 5G operator telekomunikasi.

AWS mengoperasikan pusat data yang canggih dan sangat tersedia. Meskipun jarang terjadi, kegagalan dapat terjadi yang memengaruhi ketersediaan instans yang berada di lokasi yang sama. Jika Anda meng-host semua instans Anda di satu lokasi yang dipengaruhi oleh kegagalan, tidak ada instans Anda yang akan tersedia.

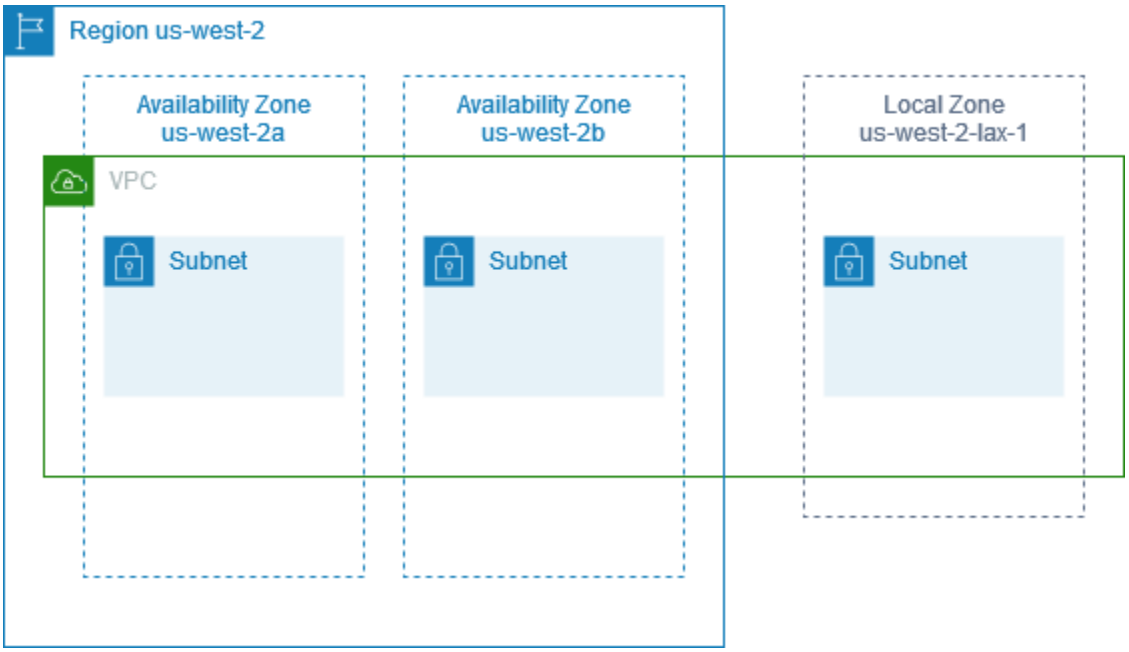
Subnets di AWS Zona Lokal

AWS Zona Lokal memungkinkan Anda menempatkan sumber daya lebih dekat dengan pengguna Anda, dan terhubung dengan mulus ke berbagai layanan di Wil AWS ayah, menggunakan API dan set alat yang sudah dikenal. Saat Anda membuat subnet di Zona Lokal, VPC Anda diperluas ke Zona Lokal tersebut.

Untuk menggunakan Zona Lokal, Anda menggunakan proses berikut:

- Pilih masuk ke Zona Lokal.
- Buat subnet di Zona Lokal.
- Luncurkan sumber daya di subnet Zona Lokal, sehingga aplikasi Anda lebih dekat dengan pengguna Anda.

Diagram berikut menggambarkan VPC di Wilayah AS Barat (Oregon) (`us-west-2`) yang mencakup Zona Ketersediaan dan Zona Lokal.



Saat Anda membuat VPC, Anda dapat memilih untuk menetapkan satu set alamat IP Amazon-provided publik ke VPC. Anda juga dapat mengatur grup perbatasan jaringan untuk alamat yang

membatasi alamat ke grup. Saat Anda menetapkan grup perbatasan jaringan, alamat IP tidak dapat berpindah antar grup perbatasan jaringan. Lalu lintas jaringan Zona Lokal akan langsung menuju ke internet atau ke titik-titik kehadiran (PoPs) tanpa melintasi Wilayah induk Zona Lokal, memungkinkan akses ke komputasi latensi rendah. Untuk daftar lengkap Zona Lokal dan Wilayah induknya yang sesuai, lihat Zona Lokal Ter sedia di Panduan AWS Pengguna Zona Lokal.

Aturan berikut berlaku untuk Local Zones:

- Subnet Zona Lokal mengikuti aturan perutean yang sama sebagaimana subnet Availability Zone, termasuk tabel rute, grup keamanan, dan ACL jaringan.
- Lalu lintas internet keluar meninggalkan suatu Zona Lokal dari Zona Lokal tersebut.
- Anda harus menyediakan alamat IP publik untuk digunakan di Zona Lokal. Bila Anda mengalokasikan alamat, Anda dapat menyebutkan lokasi yang darinya alamat IP diiklankan. Kami menyebut ini sebagai grup perbatasan jaringan, dan Anda dapat mengatur parameter ini untuk membatasi alamat ke lokasi ini. Setelah Anda menyediakan alamat IP, Anda tidak dapat memindahkannya dari Zona Lokal ke Wilayah induk atau sebaliknya (misalnya, dari `us-west-2-lax-1a` ke `us-west-2`).
- Jika Zona Lokal mendukung IPv6, Anda dapat meminta alamat Amazon-provided IP IPv6 dan mengaitkannya dengan grup perbatasan jaringan untuk VPC baru atau yang sudah ada. Untuk daftar Zona Lokal yang mendukung IPv6, lihat Per timbangan di Panduan Pengguna AWS Zona Lokal
- Anda tidak dapat membuat titik akhir VPC di subnet Zona Lokal.

Untuk informasi selengkapnya tentang bekerja dengan Zona Lokal, lihat Panduan Pengguna Zona AWS Lokal.

Pertimbangan untuk gateway internet

Pertimbangkan informasi berikut ketika Anda menggunakan gateway internet (di Wilayah induk) di Local Zones:

- Anda dapat menggunakan gateway internet di Local Zones dengan alamat IP Elastis atau alamat IP publik yang ditetapkan Amazon. Alamat IP Elastis yang Anda kaitkan harus mencakup grup perbatasan jaringan Zona Lokal. Untuk informasi selengkapnya, lihat the section called “Alamat IP elastis”.

  Anda tidak dapat mengaitkan alamat IP Elastis yang ditetapkan untuk Wilayah.

- Alamat IP Elastis yang digunakan dalam Local Zones memiliki kuota yang sama sebagaimana alamat IP Elastis di suatu Wilayah. Untuk informasi selengkapnya, lihat the section called “Alamat IP elastis”.
- Anda dapat menggunakan gateway internet di tabel rute yang terkait dengan sumber daya Zona Lokal. Untuk informasi selengkapnya, lihat the section called “Perutean ke gateway internet”.

Akses Local Zones menggunakan gateway Direct Connect

Pertimbangkan skenario di mana Anda ingin pusat data on-premise mengakses sumber daya yang berada di Zona Lokal. Anda menggunakan virtual private gateway untuk VPC yang terkait dengan Zona Lokal untuk terhubung ke gateway Direct Connect. Gateway Direct Connect terhubung ke Direct Connect lokasi di Wilayah. Pusat data lokal memiliki Direct Connect koneksi ke Direct Connect lokasi.

> **Note**
>
> Lalu lintas yang ditujukan untuk subnet di Zona Lokal menggunakan Direct Connect tidak berjalan melalui Wilayah induk Zona Lokal. Sebaliknya, lalu lintas mengambil jalur terpendek ke Zona Lokal. Ini mengurangi latensi dan membantu membuat aplikasi Anda lebih responsif.

Anda mengonfigurasi sumber daya berikut untuk konfigurasi ini:

- Sebuah virtual private gateway untuk VPC yang terkait dengan subnet Zona Lokal. Anda dapat melihat VPC untuk subnet di halaman detail subnet di konsol Amazon VPC, atau menggunakan perintah describe-subnets. https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-subnets.html

  Untuk informasi tentang cara membuat virtual private gateway, lihat Membuat gateway target di Panduan Pengguna AWS Site-to-Site VPN .
- Koneksi Direct Connect. Untuk performa latensi terbaik AWS , sarankan Anda menggunakan lokasi Direct Connect yang paling dekat dengan Zona Lokal tempat Anda akan memperluas subnet.

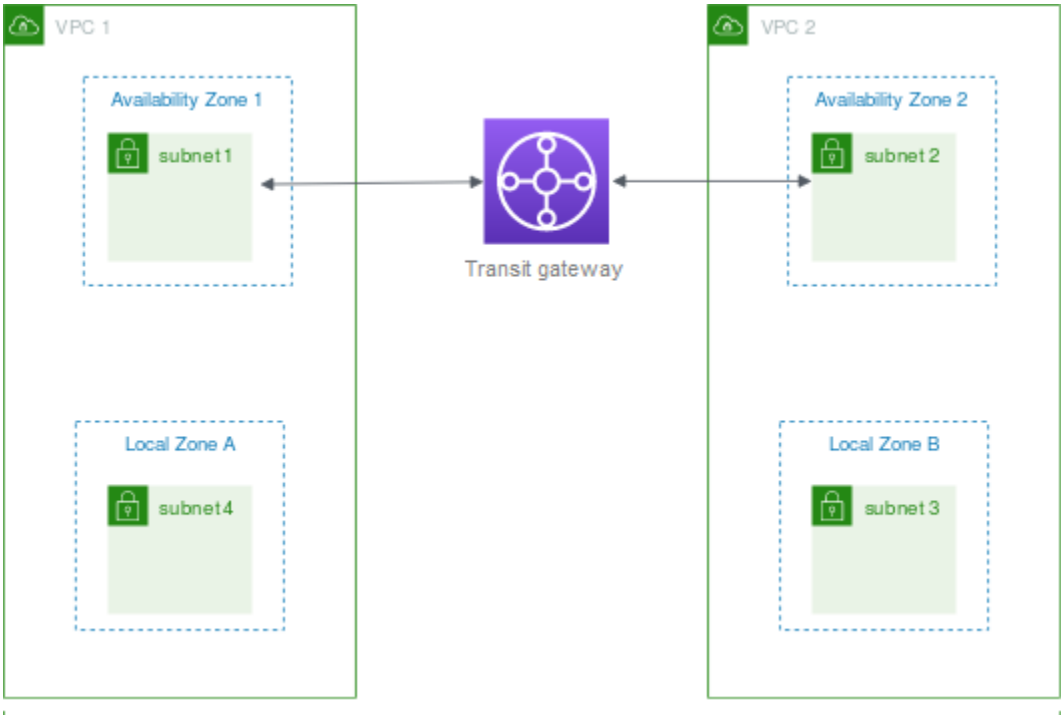
  Untuk informasi tentang memerintahkan koneksi, lihat Koneksi silang dalam Panduan Pengguna Direct Connect .
- Sebuah gateway Direct Connect. Untuk informasi tentang cara membuat gateway Direct Connect, lihat Membuat gateway Direct Connect di Panduan Pengguna Direct Connect .

- Pengaitan virtual private gateway untuk menghubungkan VPC ke gateway Direct Connect. Untuk informasi tentang cara membuat pengaitan virtual private gateway, lihat Mengaitkan dan memisahkan virtual private gateway di Panduan Pengguna Direct Connect .
- Antarmuka virtual pribadi pada koneksi dari Direct Connect lokasi ke pusat data lokal. Untuk informasi tentang cara membuat gateway Direct Connect, lihat Membuat antarmuka virtual privat ke gateway Direct Connect di Panduan Pengguna Direct Connect .

Connect subnet Zona Lokal ke transit gateway

Anda tidak dapat membuat lampiran gateway transit untuk subnet di Zona Lokal. Diagram berikut menunjukkan cara mengonfigurasi jaringan Anda sehingga subnet di Zona Lokal terhubung ke gateway transit melalui Zona Ketersediaan induk. Buat subnet di Zona Lokal dan subnet di Zona Ketersediaan induk. Hubungkan subnet di Zona Ketersediaan induk ke gateway transit, lalu buat rute di tabel rute untuk setiap VPC yang merutekan lalu lintas yang ditujukan untuk VPC CIDR lainnya ke antarmuka jaringan untuk lampiran gateway transit.

> **Note**
>
> Lalu lintas yang ditujukan untuk subnet di Zona Lokal yang berasal dari gateway transit pertama-tama akan melintasi Wilayah induk.



Buat sumber daya berikut untuk skenario ini:

- Sebuah subnet di setiap Zona Ketersediaan induk. Untuk informasi selengkapnya, lihat the section called “Membuat subnet”.
- Transit gateway. Untuk informasi selengkapnya, lihat Membuat gateway transit di Amazon VPC Transit Gateway.
- Lampiran gateway transit untuk setiap VPC menggunakan Zona Ketersediaan induk. Untuk informasi selengkapnya, lihat Membuat lampiran gateway transit ke VPC di Amazon VPC Transit Gateway.
- Sebuah tabel rute transit gateway yang terkait dengan transit gateway attachment. Untuk informasi selengkapnya, lihat Tabel rute gateway transit di Amazon VPC Transit Gateway.
- Untuk setiap VPC, entri dalam tabel rute subnet dari subnet Zona Lokal yang memiliki VPC CIDR lainnya sebagai tujuan, dan ID antarmuka jaringan untuk lampiran gateway transit sebagai target. Untuk menemukan antarmuka jaringan untuk lampiran gateway transit, cari deskripsi antarmuka jaringan Anda untuk ID lampiran gateway transit. Untuk informasi selengkapnya, lihat the section called “Perutean untuk Transit Gateway”.

Berikut ini adalah contoh tabel rute untuk VPC 1.

Tujuan	Target
VPC 1 CIDR	*local*
VPC 2 CIDR	*vpc1-attachment-network-interface-id*

Berikut ini adalah contoh tabel rute untuk VPC 2.

Tujuan	Target
VPC 2 CIDR	*local*
VPC 1 CIDR	*vpc2-attachment-network-interface-id*

Berikut ini adalah contoh tabel rute gateway transit. Blok CIDR untuk setiap VPC menyebar ke tabel rute gateway transit.

CIDR	Lampiran	Jenis rute
VPC 1 CIDR	*Attachment for VPC 1*	disebarkan
VPC 2 CIDR	*Attachment for VPC 2*	disebarkan

Subnets di AWS Wavelength

AWS Wavelength memungkinkan developer membangun aplikasi yang memberikan latensi yang sangat rendah ke perangkat seluler dan pengguna akhir. Wavelength men-deploy layanan komputasi dan penyimpanan AWS standar ke edge jaringan 5G operator telekomunikasi. Pengembang dapat memperluas cloud pribadi virtual (VPC) ke satu atau lebih Zona Panjang Gelombang, dan kemudian menggunakan AWS sumber daya seperti instans Amazon EC2 untuk menjalankan aplikasi yang memerlukan latensi sangat rendah dan terhubung ke Layanan AWS dalam Wilayah.

Untuk menggunakan Wavelength Zones, Anda harus terlebih dahulu memilih Zona tersebut. Selanjutnya, membuat subnet di Zona Wavelength. Anda dapat membuat instans Amazon EC2, volume Amazon EBS, dan subnet Amazon VPC dan gateway operator di Wavelength Zones. Anda juga dapat menggunakan layanan yang mengatur atau bekerja dengan EC2, EBS, dan VPC, seperti Amazon EC2 Auto Scaling, cluster Amazon EKS, cluster Amazon ECS, Amazon EC2 Systems Manager, Amazon, dan. CloudWatch AWS CloudTrail CloudFormation Layanan di Wavelength adalah bagian dari VPC yang terhubung melalui koneksi bandwidth tinggi yang andal ke Wil AWS ayah untuk akses mudah ke layanan termasuk Amazon DynamoDB dan Amazon RDS.

Aturan berikut berlaku untuk Wavelength Zones:

- Sebuah VPC meluas ke Zona Wavelength ketika Anda membuat subnet di VPC dan mengaitkannya dengan Zona Wavelength.
- Secara default, setiap subnet yang Anda buat di VPC yang mencakup Zona Wavelength mewarisi tabel rute VPC utama, termasuk rute lokal.
- Ketika Anda meluncurkan instans EC2 di subnet di Zona Wavelength, Anda menetapkan alamat IP operator untuk itu. Carrier operator menggunakan alamat untuk lalu lintas dari antarmuka ke

internet, atau perangkat seluler. Gateway operator menggunakan NAT untuk menerjemahkan alamat, dan kemudian mengirimkan lalu lintas ke tujuan. Lalu lintas dari rute jaringan operator telekomunikasi melalui gateway operator.

- Anda dapat mengatur target tabel rute VPC, atau subnet tabel rute di Zona Wavelength untuk gateway operator, yang memungkinkan lalu lintas masuk dari jaringan operator di lokasi tertentu, dan lalu lintas keluar ke jaringan operator dan internet. Untuk informasi lebih lanjut tentang pilihan perutean di Zona Wavelength, lihat Perutean di Panduan Developer AWS Wavelength .
- Subnet di Zona Panjang Gelombang memiliki komponen jaringan yang sama dengan subnet di Availability Zones, termasuk alamat IPv4, set opsi DHCP, dan ACL jaringan.
- Anda tidak dapat membuat lampiran gateway transit ke subnet di Zona Panjang Gelombang. Sebagai gantinya, buat lampiran melalui subnet di Zona Ketersediaan induk, lalu rute lalu lintas ke tujuan yang diinginkan melalui gateway transit. Sebagai contoh, lihat bagian berikut.

Pertimbangan untuk beberapa Wavelength

Instans EC2 yang berada di Wavelength Zones yang berbeda di VPC yang sama tidak diperbolehkan untuk berkomunikasi satu sama lain. Jika Anda memerlukan komunikasi Zona Panjang Gelombang ke Zona Panjang Gelombang AWS , sarankan Anda menggunakan beberapa VPC, satu untuk setiap Zona Panjang Gelombang. Anda dapat menggunakan transit gateway untuk menghubungkan VPC. Konfigurasi ini memungkinkan komunikasi antar instans di Wavelength Zones.

Rute lalu lintas Zona Panjang Gelombang ke Zona Panjang Gelombang melalui AWS Wilayah. Untuk informasi selengkapnya, lihat AWS Transit Gateway.

Diagram berikut menunjukkan cara mengkonfigurasi jaringan Anda sehingga instans dalam dua Zona Wavelength yang berbeda dapat berkomunikasi. Anda memiliki dua Zona Wavelength (Zona Wavelength A dan Zona Wavelength B). Anda perlu membuat sumber daya berikut untuk mengaktifkan komunikasi:

- Untuk setiap Zona Wavelength, subnet di Availability Zone yang merupakan Availability Zone induk untuk Zona Wavelength. Misalnya, Anda membuat subnet 1 dan subnet 2. Untuk informasi tentang membuat subnet, lihat the section called “Membuat subnet”. Gunakan perintah describe-availability-zones untuk menemukan zona induk.
- Transit gateway. Transit gateway menghubungkan VPC. Untuk informasi selengkapnya tentang membuat transit gateway, lihat Membuat transit gateway di Panduan Amazon VPC Transit Gateways.

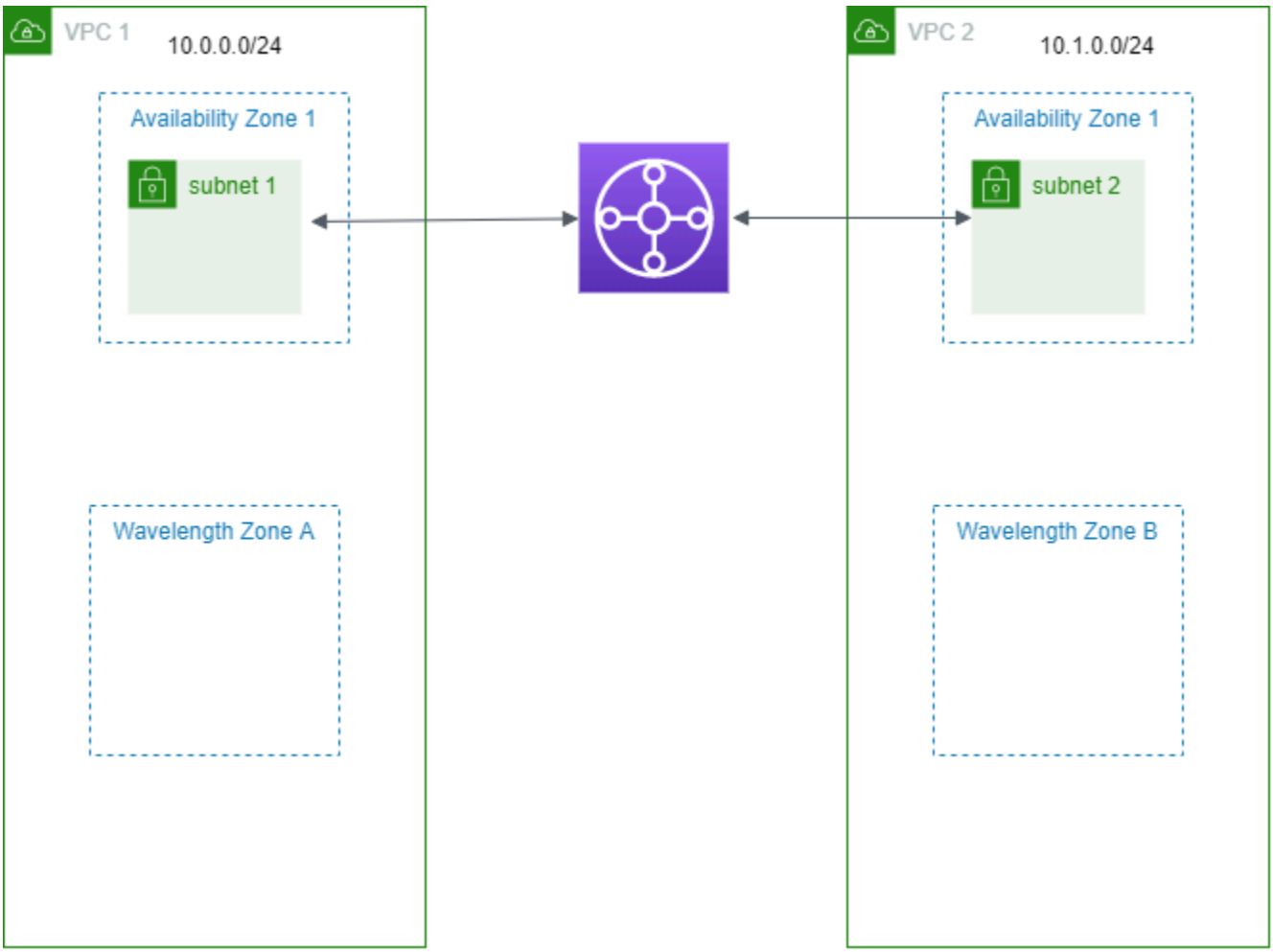
- Untuk setiap VPC, lampiran VPC ke gateway transit di Zona Ketersediaan induk Zona Panjang Gelombang. Untuk informasi selengkapnya, lihat Lampiran gateway transit ke VPC di Panduan Gerbang Transit Amazon VPC.
- Entri untuk setiap VPC dalam tabel rute transit gateway. Untuk informasi tentang membuat rute transit gateway, lihat Tabel rute transit gateway di Panduan Amazon VPC Transit Gateways.
- Untuk setiap VPC, entri dalam tabel rute VPC yang memiliki VPC CIDR lain sebagai tujuan, dan transit gateway ID sebagai target. Untuk informasi selengkapnya, lihat the section called “Perutean untuk Transit Gateway”.

  Misalnya, tabel rute untuk VPC 1 memiliki entri berikut:

Tujuan	Target
10.1.0. 0/24	tgw-22222222222222222

  Misalnya, tabel rute untuk VPC 2 memiliki entri berikut:

Tujuan	Target
10.0.0. 0/24	tgw-22222222222222222



Subnets di AWS Outposts

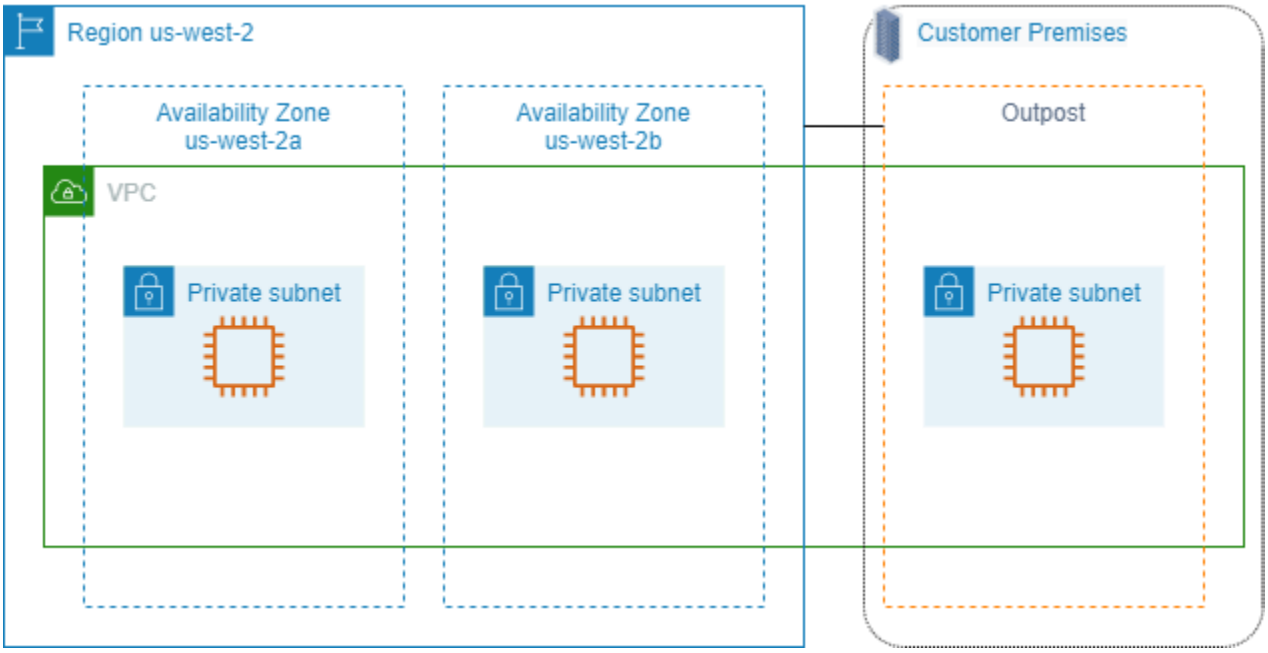
AWS Outposts menawarkan infrastruktur AWS perangkat keras, layanan, API, dan alat yang sama untuk membangun dan menjalankan aplikasi Anda di lokasi dan di cloud. AWS Outposts sangat ideal untuk beban kerja yang membutuhkan akses latensi rendah ke aplikasi atau sistem lokal, dan untuk beban kerja yang perlu menyimpan dan memproses data secara lokal. Untuk informasi lebih lanjut tentang AWS Outposts, lihat AWS Outposts.

VPC mencakup semua Zona Ketersediaan di suatu AWS Wilayah. Setelah menghubungkan Pos Terdepan ke Wilayah induknya, Anda dapat memperluas VPC apa pun di Wilayah ke Pos Terdepan Anda dengan membuat subnet untuk Pos Terdepan di VPC tersebut.

Aturan berikut berlaku untuk AWS Outposts:

- Subnet harus berada di satu lokasi Outpost.

- Anda membuat subnet untuk Outpost dengan menentukan Nama Sumber Daya Amazon (ARN) dari Outpost saat Anda membuat subnet.
- Rak pos terdepan - Gateway lokal menangani konektivitas jaringan antara VPC Anda dan jaringan lokal. Untuk informasi selengkapnya, lihat Gateway lokal di Panduan AWS Outposts Pengguna untuk rak pos terdepan.
- Server pos terdepan - Antarmuka jaringan lokal menangani konektivitas jaringan antara VPC Anda dan jaringan lokal. Untuk informasi selengkapnya, lihat Antarmuka jaringan lokal di Panduan AWS Outposts Pengguna untuk server Outpost.
- Secara default, setiap subnet yang Anda buat di VPC, termasuk subnet untuk Outpost Anda, secara implisit terkait dengan tabel rute utama untuk VPC. Atau, Anda dapat secara eksplisit mengaitkan tabel rute khusus dengan subnet di VPC Anda dan memiliki gateway lokal sebagai target next hop untuk semua lalu lintas yang ditujukan untuk jaringan lokal Anda.



Hapus VPC Anda

Setelah selesai dengan VPC, Anda dapat menghapusnya.

Persyaratan

Sebelum Anda dapat menghapus VPC, Anda harus terlebih dahulu menghentikan atau menghapus sumber daya apa pun yang membuat antarmuka jaringan yang dikelola pemohon di VPC. Misalnya,

Anda harus menghentikan EC2 instans dan menghapus penyeimbang beban, gateway NAT, lampiran VPC gateway transit, dan titik akhir VPC antarmuka.

> **Note**
>
> Jika Anda telah membuat log aliran untuk VPC yang Anda hapus, perhatikan bahwa log aliran untuk dihapus pada akhirnya akan dihapus VPCs secara otomatis.

Daftar Isi

- Hapus VPC menggunakan konsol
- Hapus VPC menggunakan baris perintah

Hapus VPC menggunakan konsol

Jika Anda menghapus VPC menggunakan konsol VPC Amazon, kami juga menghapus komponen VPC berikut untuk Anda:

- Opsi DHCP
- Gateway internet khusus egress
- Titik akhir Gateway
- Gateway internet
- Jaringan ACLs
- Tabel rute
- Grup keamanan
- Subnet

Untuk menghapus VPC Anda menggunakan konsol

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Akhiri semua instans di VPC. Untuk informasi selengkapnya, lihat Menghentikan Instans Anda di Panduan EC2 Pengguna Amazon.
3. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
4. Di panel navigasi, pilih Your VPCs.
5. Pilih VPC yang akan dihapus dan pilih Tindakan, Hapus VPC..

6. Jika ada sumber daya yang harus Anda hapus atau hentikan sebelum kami dapat menghapus VPC, kami menampilkannya. Hapus atau hentikan sumber daya ini dan kemudian coba lagi. Jika tidak, kami menampilkan sumber daya yang akan kami hapus selain VPC. Tinjau daftar dan kemudian lanjutkan ke langkah berikutnya.
7. (Opsional) Jika Anda memiliki koneksi Site-to-Site VPN, Anda dapat memilih opsi untuk menghapusnya. Jika Anda berencana untuk menggunakan gateway pelanggan dengan VPC lain, kami sarankan Anda menjaga koneksi Site-to-Site VPN dan gateway. Jika tidak, Anda harus mengonfigurasi perangkat gateway pelanggan Anda lagi setelah Anda membuat koneksi Site-to-Site VPN baru.
8. Saat diminta konfirmasi, masukkan **`delete`**, lalu pilih Hapus.

Hapus VPC menggunakan baris perintah

Sebelum Anda dapat menghapus VPC menggunakan baris perintah, Anda harus mengakhiri atau menghapus sumber daya apa pun yang membuat antarmuka jaringan yang dikelola pemohon di VPC. Anda juga harus menghapus atau melepaskan semua sumber daya VPC yang Anda buat, seperti subnet, grup keamanan, ACLs jaringan, tabel rute, gateway internet, dan gateway internet khusus egres. Anda tidak perlu menghapus grup keamanan default, tabel rute default, atau ACL jaringan default.

Prosedur berikut menunjukkan perintah yang Anda gunakan untuk menghapus sumber daya VPC umum dan kemudian menghapus VPC Anda. Anda harus menggunakan perintah ini dalam urutan ini. Jika Anda membuat sumber daya VPC tambahan, Anda juga harus menggunakan perintah hapus yang sesuai sebelum Anda dapat menghapus VPC.

Untuk menghapus VPC dengan menggunakan AWS CLI

1. Hapus grup keamanan Anda dengan menggunakan delete-security-groupperintah.

```
aws ec2 delete-security-group --group-id sg-id
```

2. Hapus setiap ACL jaringan dengan menggunakan delete-network-aclperintah.

```
aws ec2 delete-network-acl --network-acl-id acl-id
```

3. Hapus setiap subnet dengan menggunakan perintah delete-subnet.

```
aws ec2 delete-subnet --subnet-id subnet-id
```

4. Hapus setiap tabel rute kustom dengan menggunakan delete-route-tableperintah.

```
aws ec2 delete-route-table --route-table-id rtb-id
```

5. Lepaskan gateway internet Anda dari VPC Anda dengan menggunakan detach-internet-gatewayperintah.

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-id --vpc-id vpc-id
```

6. Hapus gateway internet Anda dengan menggunakan delete-internet-gatewayperintah.

```
aws ec2 delete-internet-gateway --internet-gateway-id igw-id
```

7. [Dual stack VPC] Hapus gateway internet khusus egress-Anda dengan menggunakan perintah - gateway. delete-egress-only-internet

```
aws ec2 delete-egress-only-internet-gateway --egress-only-internet-gateway-id eigw-id
```

8. Hapus VPC Anda dengan menggunakan perintah delete-vpc.

```
aws ec2 delete-vpc --vpc-id vpc-id
```

Hasilkan infrastruktur sebagai kode dari tindakan konsol VPC Anda dengan Console-to-Code

Konsol tersebut menyediakan jalur dengan panduan untuk membuat sumber daya dan menguji prototipe. Jika Anda ingin membuat sumber daya yang sama dalam skala besar, Anda memerlukan kode otomatisasi. Console-to-Code adalah fitur Amazon Q Developer yang dapat membantu Anda memulai dengan kode otomatisasi Anda. Console-to-Code merekam tindakan konsol Anda, termasuk nilai default dan parameter yang kompatibel. Kemudian menggunakan AI generatif untuk menyarankan kode dalam format infrastructure-as-code (IaC) pilihan Anda untuk tindakan yang Anda inginkan. Karena alur kerja konsol memastikan nilai parameter yang Anda tentukan valid bersama, kode yang Anda hasilkan dengan menggunakan Console-to-Code memiliki nilai parameter yang kompatibel. Anda dapat menggunakan kode sebagai titik awal, dan kemudian menyesuaikannya agar siap produksi untuk kasus penggunaan spesifik Anda.

Misalnya, dengan Console-to-Code Anda dapat merekam diri Anda menggunakan konsol VPC untuk membuat subnet, grup keamanan, NACL, tabel routing khusus, dan gateway internet dan menghasilkan kode dalam CloudFormation format JSON. Kemudian, Anda dapat menyalin kode itu dan menyesuaikannya untuk digunakan dalam CloudFormation template Anda.

Console-to-Code saat ini dapat menghasilkan infrastructure-as-code (IaC) dalam bahasa dan format berikut:

- CDK Java
- CDK Python
- CDK TypeScript
- CloudFormation JSON
- CloudFormation YAML

Untuk informasi selengkapnya dan petunjuk tentang cara menggunakan Console-to-Code, lihat Men gotomati AWS skan layanan dengan Amazon Q Developer Console-to-Code di Panduan Pengguna Pengembang Amazon Q.

Subnet untuk VPC Anda

Sebuah subnet adalah rentang alamat IP di VPC Anda. Anda dapat membuat AWS sumber daya, seperti instans EC2, di subnet tertentu.

Daftar Isi

- Dasar-Dasar Subnet
- Keamanan subnet
- Membuat subnet
- Menambahkan atau menghapus blok IPv6 CIDR dari subnet Anda
- Ubah atribut pengalamatan IP subnet Anda
- Reservasi CIDR subnet
- Konfigurasikan tabel rute
- Wisaya perutean Middlebox
- Hapus subnet

Dasar-Dasar Subnet

Setiap subnet harus berada sepenuhnya dalam satu Availability Zone dan tidak dapat memperluas zona. Dengan meluncurkan AWS sumber daya di Availability Zone terpisah, Anda dapat melindungi aplikasi Anda dari kegagalan satu Availability Zone.

Daftar Isi

- Rentang alamat IP subnet
- Jenis subnet
- Diagram subnet
- Perutean subnet
- Pengaturan subnet

Rentang alamat IP subnet

Saat Anda membuat subnet, Anda menentukan alamat IP-nya, tergantung pada konfigurasi VPC:

- Hanya IPv4 - Subnet memiliki blok CIDR IPv4 tetapi tidak memiliki blok CIDR IPv6. Sumber daya dalam IPv4-only subnet harus berkomunikasi melalui IPv4.
- Dual stack — Subnet memiliki blok IPv4 CIDR dan blok IPv6 CIDR. VPC harus memiliki blok IPv4 CIDR dan blok IPv6 CIDR. Sumber daya dalam subnet dual-stack dapat berkomunikasi melalui IPv4 dan IPv6.
- Hanya IPv6 - Subnet memiliki blok CIDR IPv6 tetapi tidak memiliki blok CIDR IPv4. VPC harus memiliki blok CIDR IPv6. Sumber daya dalam IPv6-only subnet harus berkomunikasi melalui IPv6.

> **Note**
>
> Sumber daya dalam IPv6-only subnet diberi alamat link-lokal IPv4 dari blok CIDR. 169.254.0.0/16 Alamat ini digunakan untuk berkomunikasi dengan layanan yang hanya tersedia di VPC. Sebagai contoh, lihat Link-local alamat di Panduan Pengguna Amazon EC2.

Untuk informasi selengkapnya, lihat Pengalamatan IP untuk VPC dan subnet Anda.

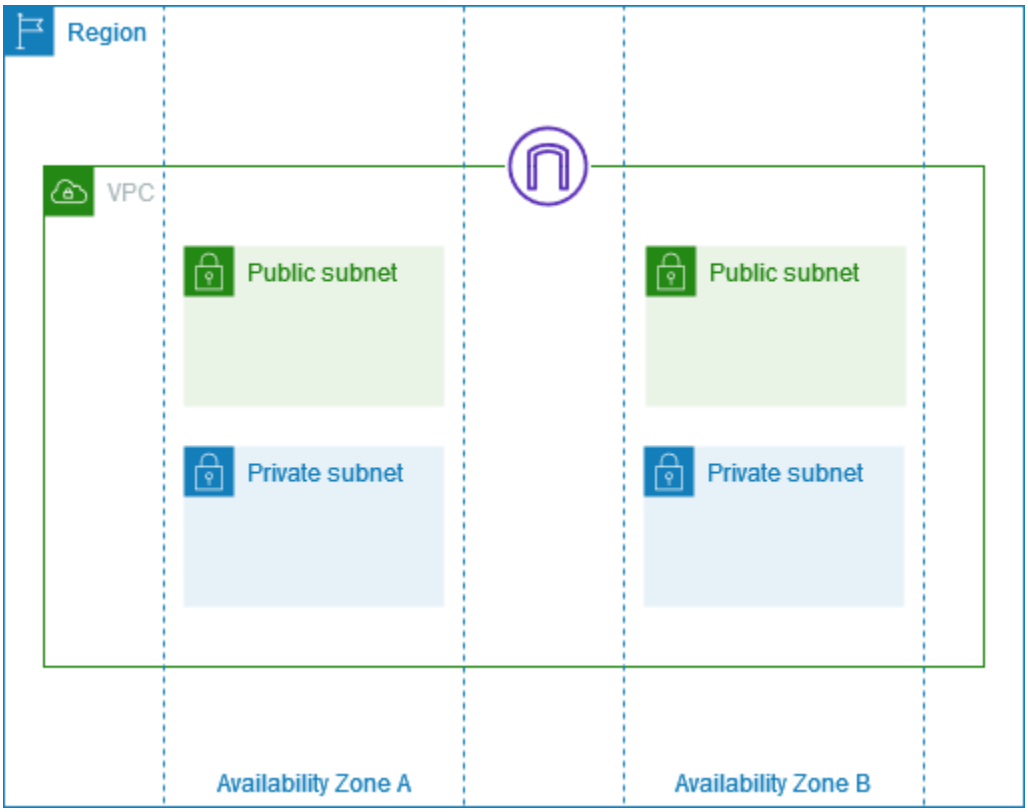
Jenis subnet

Jenis subnet ditentukan oleh bagaimana Anda mengkonfigurasi routing untuk subnet Anda. Contoh:

- Subnet publik — Subnet memiliki rute langsung ke gateway internet. Sumber daya dalam subnet publik dapat mengakses internet publik.
- Subnet pribadi — Subnet tidak memiliki rute langsung ke gateway internet. Sumber daya dalam subnet pribadi memerlukan perangkat NAT untuk mengakses internet publik.
- VPN-only subnet — Subnet memiliki rute ke koneksi Site-to-Site VPN melalui gateway pribadi virtual. Subnet tidak memiliki rute ke gateway internet.
- Subnet terisolasi — Subnet tidak memiliki rute ke tujuan di luar VPC-nya. Sumber daya dalam subnet terisolasi hanya dapat mengakses atau diakses oleh sumber daya lain dalam VPC yang sama.
- Subnet EVS - Jenis subnet ini dibuat menggunakan Amazon EVS. Untuk informasi selengkapnya, lihat subnet VLAN di Panduan Pengguna Amazon EVS.

Diagram subnet

Diagram berikut menunjukkan VPC dengan subnet di dua Availability Zones dan gateway internet. Setiap Availability Zone memiliki subnet publik dan subnet pribadi.



Untuk diagram yang menampilkan subnet di Local Zones dan Wavelength Zones, lihat Cara Kerja Local Zones dan Cara AWS Kerja. AWS Wavelength

Perutean subnet

Setiap subnet harus dikaitkan dengan sebuah tabel rute, yang menentukan rute yang diizinkan untuk lalu lintas outbound meninggalkan subnet. Setiap subnet yang Anda buat secara otomatis dikaitkan dengan tabel rute utama untuk VPC. Anda dapat mengubah pengaitan, dan Anda dapat mengubah isi dari tabel rute utama. Untuk informasi selengkapnya, lihat Konfigurasikan tabel rute.

Pengaturan subnet

Semua subnet memiliki atribut yang dapat dimodifikasi yang menentukan apakah antarmuka jaringan yang dibuat di subnet tersebut ditetapkan sebagai alamat IPv4 publik dan, jika berlaku, alamat IPv6. Ini termasuk antarmuka jaringan utama (misalnya, eth0) yang dibuat untuk sebuah instance saat

Anda meluncurkan instance di subnet tersebut. Terlepas dari atribut subnet, Anda masih dapat mengganti pengaturan ini untuk instans tertentu selama peluncuran.

Setelah Anda membuat subnet, Anda dapat mengubah pengaturan berikut untuk subnet:

- Auto-assign Pengaturan IP: Memungkinkan Anda mengonfigurasi pengaturan IP penetapan otomatis untuk secara otomatis meminta alamat IPv4 atau IPv6 publik untuk antarmuka jaringan baru di subnet ini.
- Resource-based Pengaturan nama (RBN): Memungkinkan Anda menentukan jenis nama host untuk instans EC2 di subnet ini dan mengonfigurasi bagaimana kueri catatan DNS A dan AAAA ditangani. Untuk informasi selengkapnya, lihat jenis nama host instans Amazon EC2 di Panduan Pengguna Amazon EC2.

Keamanan subnet

Untuk melindungi AWS sumber daya Anda, kami sarankan Anda menggunakan subnet pribadi. Gunakan host bastion atau perangkat NAT untuk menyediakan akses internet ke sumber daya, seperti instans EC2, di subnet pribadi.

AWS menyediakan fitur yang dapat Anda gunakan untuk meningkatkan keamanan sumber daya di VPC Anda. Grup keamanan memungkinkan lalu lintas masuk dan keluar untuk sumber daya terkait, seperti instans EC2. ACL jaringan memungkinkan atau menolak lalu lintas masuk dan keluar di tingkat subnet. Dalam kebanyakan kasus, kelompok keamanan dapat memenuhi kebutuhan Anda. Namun, Anda dapat menggunakan ACL jaringan jika Anda menginginkan lapisan keamanan tambahan. Untuk informasi selengkapnya, lihat the section called “Membandingkan grup keamanan dan ACL jaringan”.

Berdasarkan desain, setiap subnet harus dikaitkan dengan ACL jaringan. Setiap subnet yang Anda buat secara otomatis dikaitkan dengan ACL jaringan default untuk VPC. ACL jaringan default memungkinkan semua lalu lintas masuk dan keluar. Anda dapat memperbarui ACL jaringan default, atau membuat ACL jaringan khusus dan mengaitkannya dengan subnet Anda. Untuk informasi selengkapnya, lihat Kontrol lalu lintas subnet dengan daftar kontrol akses jaringan.

Anda dapat membuat log alur pada VPC atau subnet Anda untuk menangkap lalu lintas yang mengalir ke dan dari antarmuka jaringan di VPC atau subnet Anda. Anda juga dapat membuat log alur pada antarmuka jaringan individu. Lihat informasi yang lebih lengkap di Pencatatan lalu lintas IP menggunakan Log Aliran VPC.

Membuat subnet

Gunakan prosedur berikut untuk membuat subnet untuk virtual private cloud (VPC) Anda. Bergantung pada konektivitas yang Anda butuhkan, Anda mungkin juga perlu menambahkan gateway dan tabel rute.

Pertimbangan

- Anda harus menentukan blok IPv4 CIDR untuk subnet dari kisaran VPC Anda. Anda dapat secara opsional menentukan blok IPv6 CIDR untuk subnet jika ada blok IPv6 CIDR yang terkait dengan VPC. Untuk informasi selengkapnya, lihat Pengalamatan IP untuk VPC dan subnet Anda.
- Jika Anda membuat subnet IPv6 -only, perhatikan hal berikut. EC2 Instance yang diluncurkan di subnet IPv6 -only menerima IPv6 alamat tetapi bukan alamat. IPv4 Setiap instance yang Anda luncurkan ke subnet IPv6 -only harus berupa instance yang dibangun di Sistem Nitro.
- Untuk membuat subnet di Zona Lokal atau Zona Wavelength, Anda harus mengaktifkan Zona. Untuk informasi selengkapnya, lihat Wilayah dan Zona di Panduan EC2 Pengguna Amazon.

Untuk menambahkan subnet ke VPC Anda

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Subnet.
3. Pilih Buat subnet.
4. Di bawah VPC ID, pilih VPC untuk subnet.
5. (Opsional) Untuk nama Subnet, masukkan nama untuk subnet Anda. Melakukan hal itu akan menciptakan tag dengan kunci `Name` dan nilai yang Anda tentukan.
6. Untuk Availability Zone, Anda dapat memilih Zone untuk subnet Anda, atau meninggalkan default No Preference untuk membiarkan AWS memilih satu untuk Anda.
7. Untuk blok IPv4 CIDR, pilih Input manual untuk memasukkan blok IPv4 CIDR untuk subnet Anda (misalnya,**`10.0.1.0/24`**) atau pilih No CIDR. IPv4 Jika Anda menggunakan Amazon VPC IP Address Manager (IPAM) untuk merencanakan, melacak, dan memantau alamat IP untuk AWS beban kerja Anda, saat Anda membuat subnet, Anda memiliki opsi untuk mengalokasikan blok CIDR dari IPAM (dialokasikan IPAM). Untuk informasi selengkapnya tentang perencanaan ruang alamat IP VPC untuk alokasi IP subnet, lihat Tutorial: Merencanakan ruang alamat IP VPC untuk alokasi IP subnet di Panduan Pengguna Amazon VPC IPAM.

8. Untuk blok IPv6 CIDR, pilih Input manual untuk memilih IPv6 CIDR VPC yang ingin Anda buat subnet. Opsi ini hanya tersedia jika VPC memiliki blok IPv6 CIDR terkait. Jika Anda menggunakan Amazon VPC IP Address Manager (IPAM) untuk merencanakan, melacak, dan memantau alamat IP untuk AWS beban kerja Anda, saat Anda membuat subnet, Anda memiliki opsi untuk mengalokasikan blok CIDR dari IPAM (dialokasikan IPAM). Untuk informasi selengkapnya tentang perencanaan ruang alamat IP VPC untuk alokasi IP subnet, lihat Tutorial: Merencanakan ruang alamat IP VPC untuk alokasi IP subnet di Panduan Pengguna Amazon VPC IPAM.
9. Pilih blok IPv6 CIDR VPC.
10. Untuk blok CIDR IPv6 subnet, pilih CIDR untuk subnet yang sama dengan atau lebih spesifik daripada CIDR VPC. Misalnya, jika kumpulan VPC CIDR adalah /50, Anda dapat memilih panjang netmask antara /50 hingga /64 untuk subnet. Kemungkinan panjang IPv6 netmask adalah antara /44 dan /64 dengan kelipatan /4.
11. Pilih Buat subnet.

Untuk menambahkan subnet ke VPC Anda menggunakan AWS CLI

Gunakan perintah create-subnet.

Langkah berikutnya

Setelah Anda membuat subnet, Anda dapat mengkonfigurasinya sebagai berikut:

- Konfigurasikan perutean. Anda kemudian dapat membuat tabel rute khusus dan rute yang mengirim lalu lintas ke gateway yang terkait dengan VPC, seperti gateway internet. Untuk informasi selengkapnya, lihat Konfigurasikan tabel rute.
- Ubah perilaku pengalamatan IP. Anda dapat menentukan apakah instance yang diluncurkan di subnet menerima IPv4 alamat publik, IPv6 alamat, atau keduanya. Untuk informasi selengkapnya, lihat Ubah atribut pengalamatan IP subnet Anda.
- Ubah pengaturan nama berbasis sumber daya (RBN). Untuk informasi selengkapnya, lihat jenis nama host EC2 instans Amazon.
- Membuat atau memodifikasi jaringan Anda ACLs. Untuk informasi selengkapnya, lihat Kontrol lalu lintas subnet dengan daftar kontrol akses jaringan.
- Berbagi subnet dengan akun lain. Lihat informasi yang lebih lengkap di ???.

Menambahkan atau menghapus blok IPv6 CIDR dari subnet Anda

Anda dapat mengaitkan blok IPv6 CIDR dengan subnet yang ada di VPC Anda. Subnet tidak boleh memiliki blok IPv6 CIDR yang ada yang terkait dengannya.

Jika Anda tidak lagi menginginkan IPv6 dukungan di subnet Anda, tetapi Anda ingin terus menggunakan subnet Anda untuk membuat dan berkomunikasi dengan IPv4 sumber daya, Anda dapat menghapus blok IPv6 CIDR.

Sebelum Anda dapat menghapus blok IPv6 CIDR, Anda harus terlebih dahulu membatalkan penetapan IPv6 alamat apa pun yang ditetapkan ke instans apa pun di subnet Anda.

Untuk menambah atau menghapus blok IPv6 CIDR ke subnet

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Pengguna.
3. Pilih subnet Anda dan pilih Tindakan, Edit IPv6 CIDRs.
4. Untuk menambahkan CIDR, pilih Tambahkan IPv6 CIDR, pilih blok VPC CIDR, masukkan blok CIDR Subnet, dan pilih panjang netmask yang sama dengan atau lebih spesifik daripada panjang netmask dari VPC CIDR. Misalnya, jika kumpulan VPC CIDR adalah /50, Anda dapat memilih panjang netmask antara /50 hingga /64 untuk subnet. Kemungkinan panjang IPv6 netmask adalah antara /44 dan /64 dengan kelipatan /4.
5. Untuk menghapus CIDR, cari blok IPv6 CIDR dan pilih Hapus.
6. Pilih Simpan.

Untuk mengaitkan blok IPv6 CIDR dengan subnet menggunakan AWS CLI

Gunakan perintah associate-subnet-cidr-block.

Untuk memisahkan blok IPv6 CIDR dari subnet menggunakan AWS CLI

Gunakan perintah disassociate-subnet-cidr-block.

Ubah atribut pengalamatan IP subnet Anda

Secara default, subnet nondefault memiliki atribut pengalamatan IPv4 publik yang disetel `kefalse`, dan subnet default memiliki atribut ini disetel ke. `true` Pengecualian adalah subnet nondefault yang

dibuat oleh wizard instance EC2 peluncuran Amazon — wizard menyetel atribut ke. `true` Anda dapat mengubah atribut ini menggunakan konsol Amazon VPC.

Secara default, semua subnet memiliki atribut IPv6 pengalamatan yang disetel ke. `false` Anda dapat mengubah atribut ini menggunakan konsol Amazon VPC. Jika Anda mengaktifkan atribut IPv6 pengalamatan untuk subnet Anda, antarmuka jaringan yang dibuat di subnet menerima IPv6 alamat dari rentang subnet. Instans yang diluncurkan ke subnet menerima IPv6 alamat pada antarmuka jaringan utama.

Subnet Anda harus memiliki blok IPv6 CIDR terkait.

> **Note**
>
> Jika Anda mengaktifkan fitur IPv6 pengalamatan untuk subnet Anda, antarmuka jaringan atau instans Anda hanya menerima IPv6 alamat jika dibuat menggunakan versi `2016-11-15` atau yang lebih baru dari Amazon EC2 API. EC2 Konsol Amazon menggunakan versi API terbaru.

Untuk mengubah perilaku pengalamatan IP subnet Anda

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Pengguna.
3. Pilih subnet Anda dan pilih Tindakan, Edit pengaturan subnet.
4. Kotak centang Enable auto-assign public IPv4 address, jika dipilih, meminta IPv4 alamat publik untuk semua instance yang diluncurkan ke subnet yang dipilih. Pilih atau hapus kotak centang sesuai kebutuhan, lalu pilih Simpan.
5. Kotak centang Aktifkan IPv6 alamat tetapkan otomatis, jika dipilih, meminta IPv6 alamat untuk semua antarmuka jaringan yang dibuat di subnet yang dipilih. Pilih atau hapus kotak centang sesuai kebutuhan, lalu pilih Simpan.

Untuk memodifikasi atribut subnet menggunakan AWS CLI

Gunakan perintah modify-subnet-attribute.

Reservasi CIDR subnet

Reservasi CIDR subnet adalah rentang IPv4 atau IPv6 alamat yang Anda sisihkan sehingga tidak AWS akan menetapkannya ke antarmuka jaringan Anda. Ini memungkinkan Anda untuk memesan IPv4 atau blok IPv6 CIDR (juga disebut “awalan”) untuk digunakan dengan antarmuka jaringan Anda.

Saat Anda membuat reservasi CIDR subnet, Anda menentukan bagaimana Anda akan menggunakan alamat IP yang dicadangkan. Opsi berikut tersedia:

- Awalan - Memungkinkan Anda menetapkan awalan ke antarmuka jaringan tunggal. Untuk informasi selengkapnya, lihat Menetapkan awalan ke antarmuka EC2 jaringan Amazon di Panduan Pengguna Amazon. EC2
- Eksplisit - Memungkinkan Anda menetapkan alamat IP individual secara manual ke satu antarmuka jaringan.

Aturan berikut berlaku untuk reservasi CIDR subnet:

- Saat Anda membuat reservasi CIDR subnet, rentang alamat IP dapat mencakup alamat yang sudah digunakan. Membuat reservasi subnet tidak membatalkan penetapan alamat IP apa pun yang sudah digunakan.
- Anda dapat menyimpan beberapa rentang CIDR per subnet. Saat Anda memesan beberapa rentang CIDR dalam VPC yang sama, rentang CIDR tidak dapat tumpang tindih.
- Saat Anda memesan lebih dari satu rentang di subnet untuk Delegasi Awalan, dan Delegasi Awalan dikonfigurasi untuk penugasan otomatis, kami memilih alamat IP untuk ditetapkan ke antarmuka jaringan secara acak.
- Saat Anda menghapus reservasi subnet, alamat IP yang tidak digunakan tersedia untuk ditetapkan AWS ke antarmuka jaringan Anda. Menghapus reservasi subnet tidak membatalkan penetapan alamat IP apa pun yang sedang digunakan.
- Jenis reservasi mempengaruhi jumlah alamat IP yang tersedia untuk subnet. Jika Anda membuat reservasi awalan, hitungannya segera berkurang. Jika Anda membuat reservasi awalan eksplisit, hitungan berkurang saat alamat IP ditetapkan.

Untuk informasi selengkapnya tentang notasi Classless Inter-Domain Routing (CIDR), lihat. Penentuan alamat IP

Daftar Isi

- Bekerja dengan reservasi CIDR subnet menggunakan konsol
- Bekerja dengan reservasi CIDR subnet menggunakan AWS CLI

Bekerja dengan reservasi CIDR subnet menggunakan konsol

Anda dapat membuat dan mengelola reservasi CIDR subnet sebagai berikut.

Untuk mengedit reservasi CIDR subnet

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Pengguna.
3. Pilih subnet.
4. Pilih tab reservasi CIDR untuk mendapatkan informasi tentang reservasi CIDR subnet yang ada.
5. Untuk menambah atau menghapus reservasi CIDR subnet, pilih Tindakan, Edit reservasi CIDR, lalu lakukan hal berikut:
   - Untuk menambahkan reservasi IPv4 CIDR, pilih IPv4, Tambahkan reservasi IPv4 CIDR. Pilih jenis reservasi, masukkan rentang CIDR, dan pilih Tambah.
   - Untuk menambahkan reservasi IPv6 CIDR, pilih IPv6, Tambahkan reservasi IPv6 CIDR. Pilih jenis reservasi, masukkan rentang CIDR, dan pilih Tambah.
   - Untuk menghapus reservasi CIDR, pilih Hapus untuk reservasi CIDR subnet.

Bekerja dengan reservasi CIDR subnet menggunakan AWS CLI

Anda dapat menggunakan AWS CLI untuk membuat dan mengelola reservasi CIDR subnet.

Tugas

- Membuat reservasi CIDR subnet
- Tampilkan reservasi CIDR subnet
- Menghapus reservasi CIDR subnet

Membuat reservasi CIDR subnet

Anda dapat menggunakan create-subnet-cidr-reservationuntuk membuat reservasi CIDR subnet.

```
aws ec2 create-subnet-cidr-reservation --subnet-id subnet-03c51e2eEXAMPLE --
reservation-type prefix --cidr 2600:1f13:925:d240:3a1b::/80
```

Berikut ini adalah output contoh.

```
{
    "SubnetCidrReservation": {
        "SubnetCidrReservationId": "scr-044f977c4eEXAMPLE",
        "SubnetId": "subnet-03c51e2ef5EXAMPLE",
        "Cidr": "2600:1f13:925:d240:3a1b::/80",
        "ReservationType": "prefix",
        "OwnerId": "123456789012"
    }
}
```

Tampilkan reservasi CIDR subnet

Anda dapat menggunakan get-subnet-cidr-reservationsuntuk melihat detail reservasi CIDR subnet.

```
aws ec2 get-subnet-cidr-reservations --subnet-id subnet-05eef9fb78EXAMPLE
```

Menghapus reservasi CIDR subnet

Anda dapat menggunakan delete-subnet-cidr-reservationuntuk menghapus reservasi CIDR subnet.

```
aws ec2 delete-subnet-cidr-reservation --subnet-cidr-reservation-
id scr-044f977c4eEXAMPLE
```

Konfigurasikan tabel rute

Tabel rute berfungsi sebagai pengontrol lalu lintas untuk cloud pribadi virtual Anda (VPC). Setiap tabel rute berisi seperangkat aturan, yang disebut rute, yang menentukan ke mana lalu lintas jaringan dari subnet atau gateway Anda diarahkan. Saat Anda membuat VPC, kami juga membuat tabel rute utama untuk VPC. Anda dapat membuat tabel rute tambahan untuk VPC Anda, sehingga Anda memiliki kontrol yang lebih terperinci atas jalur jaringan untuk VPC Anda.

Anda dapat menggunakan tabel rute untuk menentukan jaringan mana yang dapat berkomunikasi dengan VPC Anda, seperti VPC lain atau jaringan lokal. Setiap rute menentukan tujuan (blok CIDR

atau daftar awalan) dan target (seperti gateway internet, gateway NAT, koneksi peering VPC, atau koneksi VPN). Lalu lintas dialihkan ke target berdasarkan alamat IP tujuannya. Tabel rute memungkinkan Anda membuat arsitektur jaringan kompleks yang mencakup subnet publik, subnet pribadi, subnet, dan VPN-only subnet terisolasi.

Daftar Isi

- Konsep tabel rute
- Tabel rute subnet
- Tabel rute gateway
- Cara kerja prioritas rute
- Opsi perutean contoh
- Buat tabel rute untuk VPC Anda
- Kelola tabel rute subnet
- Ganti tabel rute utama
- Kontrol lalu lintas yang memasuki VPC Anda menggunakan tabel rute gateway
- Mengganti atau memulihkan target untuk rute lokal
- Perutean lanjutan di VPC Anda
- Memecahkan masalah keterjangkauan di VPC Anda

Konsep tabel rute

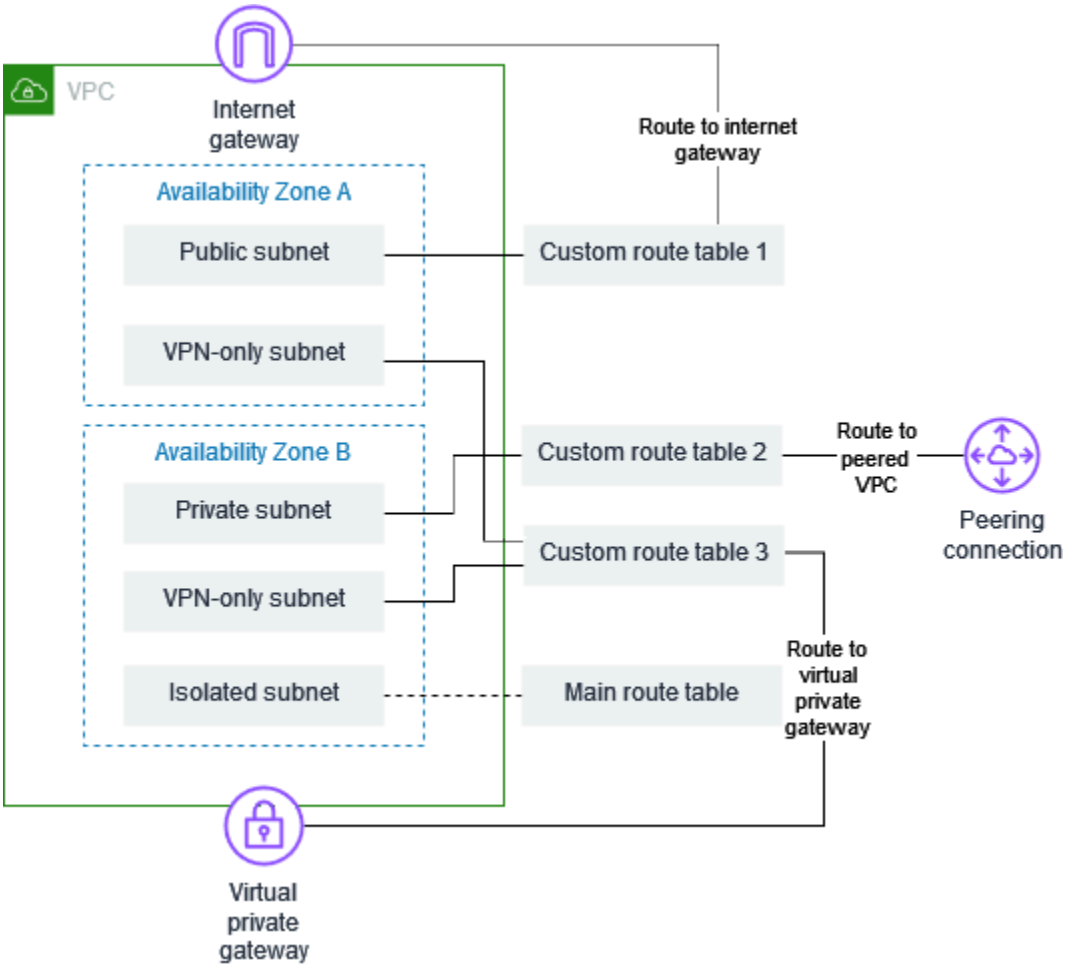
Berikut ini adalah konsep kunci untuk tabel rute:

- Tabel rute utama—Tabel rute yang secara otomatis bawaan di VPC Anda. Tabel rute utama mengendalikan perutean untuk semua subnet yang tidak secara eksplisit dikaitkan dengan tabel rute lainnya.
- Tabel rute kustom—Tabel rute yang Anda buat untuk VPC Anda.
- Tujuan—Kisaran alamat IP di mana Anda menginginkan adanya lalu lintas untuk pergi (CIDR tujuan). Misalnya, jaringan perusahaan eksternal dengan CIDR`172.16.0.0/12`.
- Target—Gateway, antarmuka jaringan, atau koneksi yang menjadi tempat untuk mengirim lalu lintas tujuan; misalnya, gateway internet.
- Rute lokal—Rute default untuk komunikasi dalam VPC. Jika VPC memiliki alamat IPv4 dan IPV6, ada rute lokal untuk IPv4 dan rute lokal untuk IPv6.

- Pengaitan tabel rute—Pengaitan antara tabel rute dan subnet, gateway internet, atau virtual private gateway.
- Tabel rute subnet—Sebuah tabel rute yang dikaitkan dengan sebuah subnet.
- Propagasi —Jika Anda telah melampirkan gateway pribadi virtual ke VPC Anda dan mengaktifkan propagasi rute, kami secara otomatis menambahkan rute untuk koneksi VPN Anda ke tabel rute subnet Anda. Ini berarti Anda tidak perlu menambahkan atau menghapus rute VPN secara manual. Untuk informasi selengkapnya, lihat opsi perutean Site-to-Site Site-to-Site VPN di Panduan Pengguna VPN.
- Tabel rute gateway—Tabel rute yang dikaitkan dengan sebuah gateway internet atau virtual private gateway.
- Pengaitan Edge—Sebuah tabel rute yang Anda gunakan untuk mengarahkan lalu lintas VPC inbound menuju ke perangkat. Anda kaitkan tabel rute dengan gateway internet atau virtual private gateway, dan tentukan antarmuka jaringan pada perangkat Anda sebagai target untuk lalu lintas VPC.
- Tabel rute gateway transit —Tabel rute yang terkait dengan gateway transit. Untuk informasi selengkapnya, lihat Tabel rute gateway transit di Amazon VPC Transit Gate way.
- Tabel rute gateway lokal—Tabel rute yang dikaitkan dengan gateway lokal Outposts. Untuk informasi selengkapnya, lihat Gateway lokal di Panduan AWS Outposts Pengguna.

Contoh VPC dengan tabel rute

Diagram berikut menunjukkan VPC dengan lima subnet, tabel rute utama, dan tiga tabel rute khusus. Keempat tabel rute memiliki rute lokal. Tabel rute kustom 1 memiliki rute ke gateway internet, dan dikaitkan dengan subnet publik di Zona Ketersediaan A. Tabel rute kustom 2 memiliki rute ke VPC yang diintip, dan dikaitkan dengan subnet pribadi di Zona Ketersediaan B. Tabel rute kustom 3 memiliki rute ke gateway pribadi virtual, dan dikaitkan dengan VPN-only subnet di kedua Zona Ketersediaan.



Tabel rute subnet

VPC Anda memiliki router implisit, dan Anda menggunakan tabel rute untuk mengendalikan ke mana lalu lintas jaringan diarahkan. Setiap subnet di VPC Anda harus dikaitkan dengan sebuah tabel rute, yang mengendalikan perutean untuk subnet (rute tabel subnet). Anda dapat secara eksplisit mengaitkan subnet dengan tabel rute khusus. Jika tidak, subnet secara implisit akan dikaitkan dengan tabel rute utama. Subnet hanya dapat dikaitkan dengan satu tabel rute dalam satu waktu, tetapi Anda dapat mengaitkan beberapa subnet dengan tabel rute subnet yang sama.

Daftar Isi

- Rute
- Tabel rute utama
- Tabel rute kustom
- Pengaitan tabel rute subnet

Rute

Setiap rute dalam sebuah tabel rute menentukan tujuan dan target. Misalnya, untuk mengaktifkan subnet Anda mengakses internet melalui gateway internet, tambahkan rute berikut ke tabel rute subnet Anda. Tujuan untuk rute tersebut adalah `0.0.0.0/0`, yang mewakili semua alamat IPv4. Targetnya adalah gateway internet yang melekat pada VPC Anda.

Tujuan	Target
0.0.0. 0/0	*igw-id*

Blok CIDR untuk IPv4 dan IPv6 diperlakukan secara terpisah. Misalnya, rute dengan CIDR tujuan `0.0.0.0/0` Tidak secara otomatis mencakup semua alamat IPv6. Anda harus membuat rute dengan tujuan CIDR dari `::/0` untuk semua alamat IPv6.

Jika Anda sering mereferensikan kumpulan blok CIDR yang sama di seluruh AWS sumber daya Anda, Anda dapat membuat daftar awalan yang dikelola pelanggan untuk mengelompokkan mereka bersama-sama. Anda kemudian dapat menentukan daftar prefiks sebagai tujuan dalam entri tabel rute Anda.

Setiap tabel rute berisikan rute lokal untuk berkomunikasi di dalam VPC. Rute ini ditambahkan secara default untuk semua tabel rute. Jika VPC Anda memiliki lebih dari satu blok CIDR IPv4, tabel rute Anda akan berisikan rute lokal untuk setiap blok CIDR IPv4. Jika Anda telah mengaitkan sebuah blok CIDR IPv6 dengan VPC Anda, tabel rute Anda berisikan rute lokal untuk blok CIDR IPv6. Anda dapat mengganti atau mengembalikan target setiap rute lokal sesuai kebutuhan.

Aturan dan pertimbangan

- Anda dapat menambahkan rute ke tabel rute yang lebih spesifik daripada rute lokal. Tujuan harus cocok dengan seluruh blok IPv4 atau IPv6 CIDR dari subnet di VPC Anda. Target harus berupa gateway NAT, antarmuka jaringan, atau titik akhir Gateway Load Balancer.
- Jika tabel rute Anda memiliki beberapa rute, kami menggunakan rute paling spesifik yang bersesuaian dengan lalu lintas (prefiks terpanjang yang sesuai) untuk menentukan cara merutekan lalu lintas.
- Anda tidak dapat menambahkan rute ke alamat IPv4 yang sama persis atau subset dari rentang berikut: 169.254.168. 0/22. Rentang ini berada dalam ruang alamat link-lokal dan dicadangkan untuk digunakan oleh AWS layanan. Misalnya, Amazon EC2 menggunakan alamat dalam rentang

ini untuk layanan yang hanya dapat diakses dari instans EC2, seperti Instance Metadata Service (IMDS) dan server Amazon DNS. Anda dapat menggunakan blok CIDR yang lebih besar dari tetapi tumpang tindih 169.254.168. 0/22, tetapi paket ditujukan untuk alamat di 169.254.168. 0/22 tidak akan diteruskan.

- Anda tidak dapat menambahkan rute ke alamat IPv6 yang sama persis atau subset dari rentang berikut: fd00:ec2: :/32. Rentang ini berada dalam ruang alamat lokal unik (ULA) dan disediakan untuk digunakan oleh AWS layanan. Misalnya, Amazon EC2 menggunakan alamat dalam rentang ini untuk layanan yang hanya dapat diakses dari instans EC2, seperti Instance Metadata Service (IMDS) dan server Amazon DNS. Anda dapat menggunakan blok CIDR yang lebih besar dari tetapi tumpang tindih fd00:ec2: :/32, tetapi paket yang ditujukan untuk alamat di fd00:ec2: :/32 tidak akan diteruskan.
- Anda dapat menambahkan peralatan middlebox ke jalur routing untuk VPC Anda. Untuk informasi selengkapnya, lihat the section called “Perutean untuk perangkat middlebox”.

Contoh

Dalam contoh berikut, anggaplah bahwa VPC memiliki blok IPv4 CIDR dan blok IPv6 CIDR. Lalu lintas IPv4 dan IPv6 diperlakukan secara terpisah, seperti yang ditunjukkan pada tabel rute berikut.

Tujuan	Target
10.0.0. 0/16	Local
2001:db8:1234:1a00::/56	Local
172.31.0. 0/16	pcx-11223344556677889
0.0.0. 0/0	igw-12345678901234567
::/0	eigw-aabbccddee1122334

- Lalu lintas IPv4 yang akan dirutekan dalam VPC (10.0.0. 0/16) ditutupi oleh Local rute.
- Lalu lintas IPv6 yang akan dirutekan dalam VPC (2001:db 8:1234:1 a00: :/56) dicakup oleh rute. Local
- Rute untuk 172.31.0. 0/16 mengirim lalu lintas ke koneksi peering.

- Rute untuk semua lalu lintas IPv4 (0.0.0. 0/0) mengirimkan lalu lintas ke gateway internet. Oleh karena itu, semua lalu lintas IPv4, kecuali untuk lalu lintas dalam VPC dan ke koneksi peering, dialihkan ke gateway internet.
- Rute untuk semua lalu lintas IPv6 (:: /0) mengirimkan lalu lintas ke gateway internet khusus keluar. Oleh karena itu, semua lalu lintas IPv6, kecuali untuk lalu lintas dalam VPC, dialihkan ke gateway internet khusus keluar.

Tabel rute utama

Ketika Anda membuat sebuah VPC, VPC secara otomatis memiliki tabel rute utama. Ketika subnet tidak memiliki tabel perutean eksplisit yang dikaitkan dengannya, tabel rute utama adalah yang digunakan secara default. Pada halaman Tabel rute di konsol Amazon VPC, Anda dapat melihat tabel rute utama untuk VPC dengan mencari Ya di kolom Utama.

Secara default, ketika Anda membuat sebuah VPC nondefault, tabel rute utama hanya berisikan rute lokal. Jika Anda Buat VPC memilih gateway NAT, Amazon VPC secara otomatis menambahkan rute ke tabel rute utama untuk gateway.

Aturan berikut berlaku untuk tabel rute utama:

- Anda dapat menambahkan, menghapus, dan memodifikasi rute di tabel rute utama.
- Anda tidak dapat menghapus tabel rute utama.
- Anda tidak dapat mengatur tabel rute gateway sebagai tabel rute utama.
- Anda dapat mengganti tabel rute utama dengan mengaitkan tabel rute khusus dengan subnet.
- Anda dapat secara eksplisit mengaitkan subnet dengan tabel rute utama, meskipun itu sudah terkait secara implisit.

  Anda mungkin ingin melakukan itu jika Anda mengubah tabel mana yang menjadi tabel rute utama. Ketika Anda mengubah tabel tertentu sebagai tabel rute utama, hal itu juga mengubah setelan default untuk subnet baru tambahan, atau untuk setiap subnet yang tidak secara eksplisit dikaitkan dengan tabel rute lainnya. Untuk informasi selengkapnya, lihat Ganti tabel rute utama.

Tabel rute kustom

Secara default, tabel rute berisi rute lokal untuk komunikasi dalam VPC. Jika Anda Buat VPC memilih subnet publik, Amazon VPC membuat tabel rute khusus dan menambahkan rute yang mengarah ke gateway internet. Salah satu cara untuk melindungi VPC Anda adalah dengan meninggalkan tabel

rute utama dalam keadaan default bawaan. Kemudian, secara eksplisit kaitkan setiap subnet baru yang Anda buat dengan salah satu tabel rute kustom yang telah Anda buat. Hal ini memastikan Anda secara eksplisit mengendalikan bagaimana setiap subnet mengarahkan lalu lintas.

Anda dapat menambahkan, menghapus, dan memodifikasi rute dalam tabel rute kustom. Anda dapat menghapus tabel rute kustom hanya jika tidak memiliki pengaitan dengan apapun.

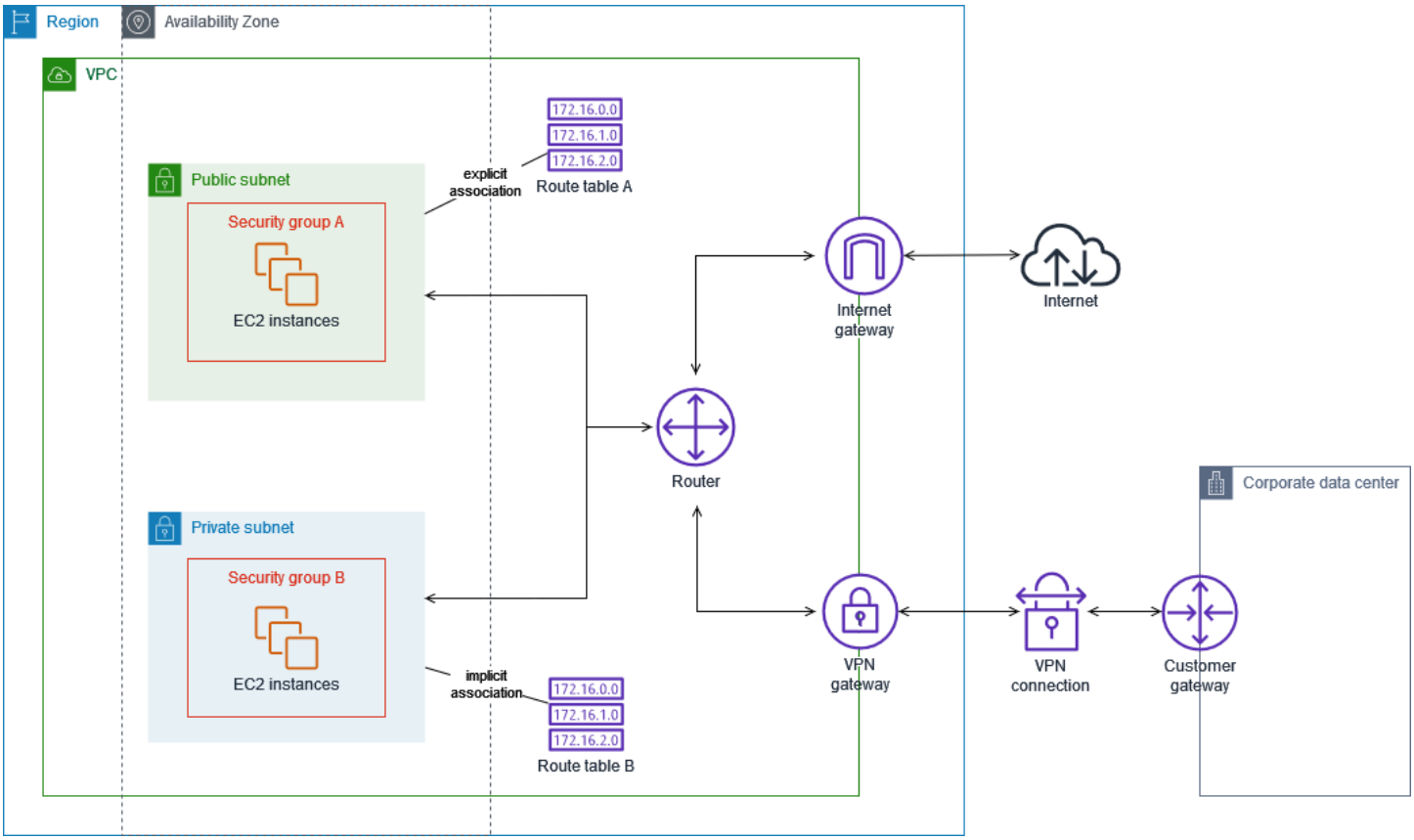
Pengaitan tabel rute subnet

Setiap subnet di VPC Anda harus dikaitkan dengan tabel rute. Subnet dapat secara eksplisit dikaitkan dengan tabel rute kustom, atau dikaitkan dengan tabel rute utama baik secara implisit ataupun eksplisit. Untuk informasi selengkapnya tentang melihat subnet dan pengaitan tabel rute, lihat Tentukan asosiasi eksplisit.

Subnet yang ada di VPC yang dikaitkan dengan Outposts dapat memiliki target tambahan jenis gateway lokal. Ini adalah satu-satunya perbedaan perutean dari subnet non-Outposts.

Contoh 1: pengaitan subnet implisit dan eksplisit

Diagram berikut menunjukkan routing untuk VPC dengan gateway internet, gateway pribadi virtual, subnet publik, dan subnet. VPN-only



Tabel rute A adalah tabel rute khusus yang secara eksplisit terkait dengan subnet publik. Ini memiliki rute yang mengirimkan semua lalu lintas ke gateway internet, yang membuat subnet menjadi subnet publik.

Tujuan	Target
VPC CIDR	Lokal:
0.0.0. 0/0	*igw-id*

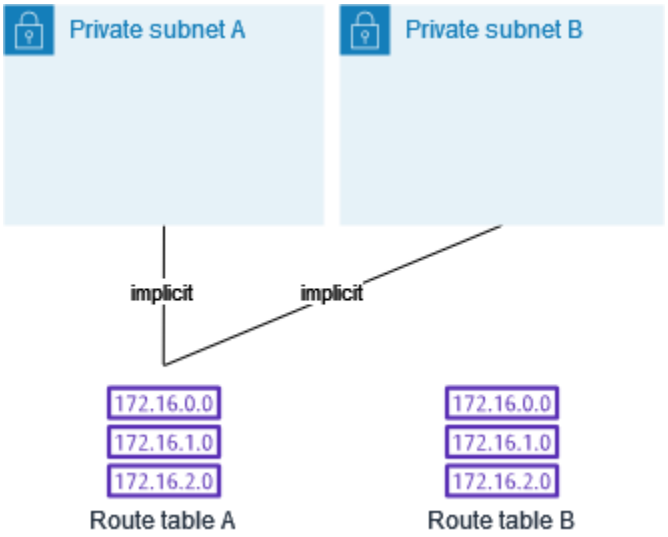
Tabel rute B adalah tabel rute utama. Ini secara implisit terkait dengan subnet pribadi. Ini memiliki rute yang mengirimkan semua lalu lintas ke gateway pribadi virtual, tetapi tidak ada rute ke gateway internet, yang membuat subnet menjadi VPN-only subnet. Jika Anda membuat subnet lain di VPC ini dan tidak mengaitkan tabel rute khusus, subnet juga akan secara implisit dikaitkan dengan tabel rute ini karena ini adalah tabel rute utama.

Tujuan	Target
VPC CIDR	Lokal:
0.0.0. 0/0	*vgw-id*

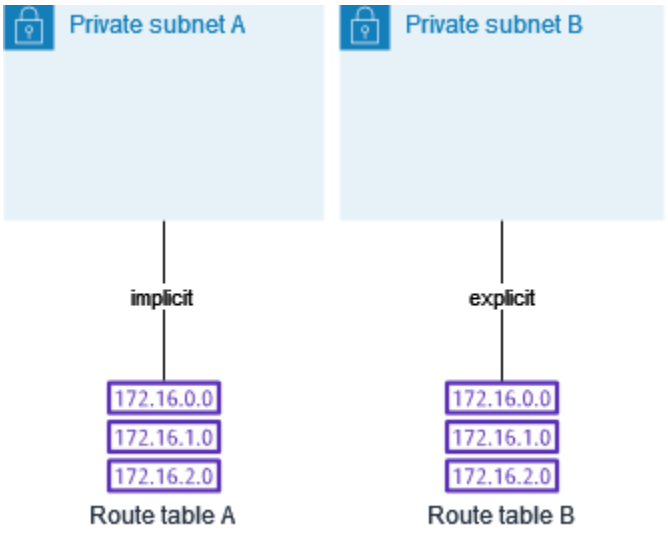
Contoh 2: Mengganti tabel rute utama

Anda mungkin ingin membuat perubahan ke tabel rute utama. Untuk menghindari gangguan pada lalu lintas Anda, sebaiknya Anda terlebih dahulu menguji perubahan rute menggunakan tabel rute kustom. Setelah Anda puas dengan pengujian tersebut, Anda dapat mengganti tabel rute utama dengan tabel kustom yang baru.

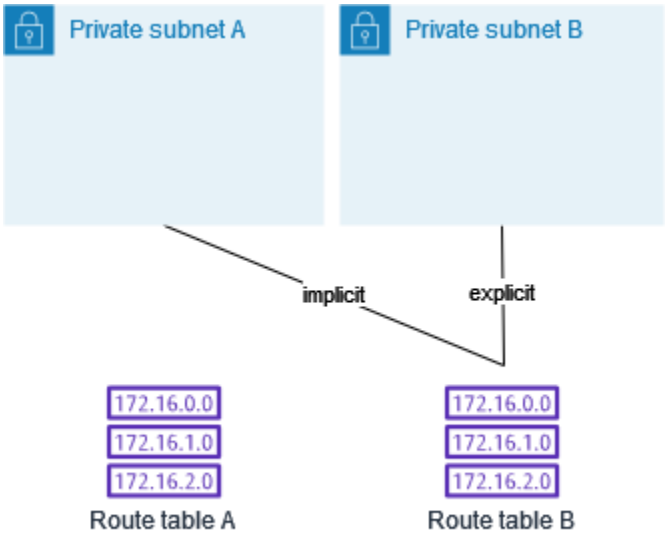
Diagram berikut menunjukkan dua subnet dan dua tabel rute. Subnet A secara implisit terkait dengan tabel rute A, tabel rute utama. Subnet B secara implisit terkait dengan tabel rute A. Tabel rute B, tabel rute khusus, tidak terkait dengan salah satu subnet.



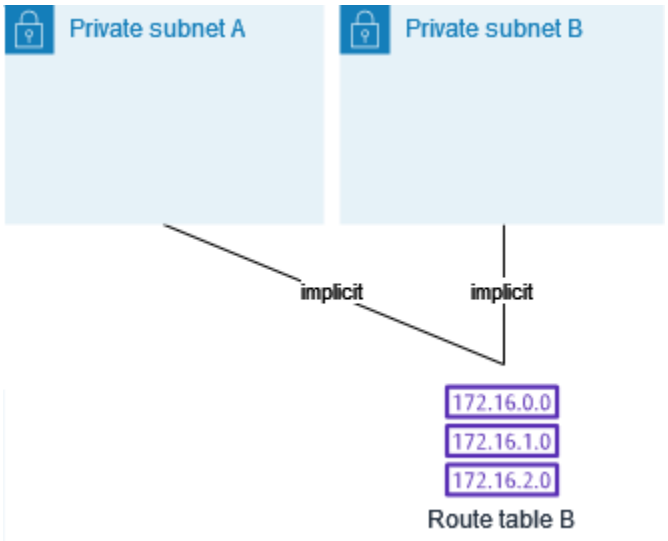
Untuk mengganti tabel rute utama, mulailah dengan membuat asosiasi eksplisit antara subnet B dan tabel rute B. Uji tabel rute B.



Setelah Anda menguji tabel rute B, jadikan tabel rute utama. Subnet B masih memiliki hubungan eksplisit dengan tabel rute B. Namun, subnet A sekarang memiliki asosiasi implisit dengan tabel rute B, karena tabel rute B adalah tabel rute utama yang baru. Tabel rute A tidak lagi terkait dengan salah satu subnet.



(Opsional) Jika Anda melepaskan subnet B dari tabel rute B, masih ada hubungan implisit antara subnet B dan tabel rute B. Jika Anda tidak lagi memerlukan tabel rute A, Anda dapat menghapusnya.



Tabel rute gateway

Anda dapat mengaitkan tabel rute dengan gateway internet atau virtual private gateway. Ketika tabel rute dikaitkan dengan gateway, itu direferensikan sebagai Tabel rute gateway. Anda dapat membuat tabel rute gateway untuk mengendalikan fine-grain atas jalur perutean lalu lintas yang memasuki VPC Anda. Misalnya, Anda dapat mencegat lalu lintas yang memasuki VPC Anda melalui gateway internet dengan mengarahkan lalu lintas ke perangkat middlebox (seperti perangkat keamanan) di VPC Anda.

Daftar Isi

- Rute tabel rute gateway
- Aturan dan pertimbangan

Rute tabel rute gateway

Tabel rute gateway yang terkait dengan gateway internet mendukung rute dengan target berikut:

- Rute lokal default
- Titik akhir Penyeimbang Beban Gateway
- Antarmuka jaringan untuk alat middlebox

Tabel rute gateway yang terkait dengan gateway pribadi virtual mendukung rute dengan target berikut:

- Rute lokal default
- Titik akhir Penyeimbang Beban Gateway
- Antarmuka jaringan untuk alat middlebox

Ketika target adalah titik akhir Penyeimbang Beban Gateway atau antarmuka jaringan, tujuan berikut diperbolehkan:

- Seluruh blok CIDR IPv4 atau IPv6 dari VPC Anda. Dalam kasus ini, Anda ganti target rute lokal default.
- Seluruh blok CIDR IPv4 atau IPv6 dari subnet di VPC Anda. Ini adalah rute yang lebih spesifik dari rute lokal default.

Jika Anda mengubah target rute lokal dalam sebuah tabel rute gerbang ke antarmuka jaringan di VPC Anda, Anda nanti dapat mengembalikannya ke target `local` default. Untuk informasi selengkapnya, lihat Mengganti atau memulihkan target untuk rute lokal.

Contoh

Dalam tabel rute gateway berikut, lalu lintas yang ditujukan untuk subnet dengan blok CIDR `172.31.0.0/20` diarahkan ke antarmuka jaringan tertentu. Lalu lintas yang ditujukan untuk semua subnet lain di VPC menggunakan rute lokal.

Tujuan	Target
172.31.0. 0/16	Lokal:
172.31.0. 0/20	*eni-id*

Contoh

Dalam tabel rute gateway berikut, target untuk rute lokal diganti dengan ID antarmuka jaringan. Lalu lintas yang ditujukan untuk semua subnet di dalam VPC diarahkan menuju antarmuka jaringan.

Tujuan	Target
172.31.0. 0/16	*eni-id*

Aturan dan pertimbangan

Anda tidak dapat mengaitkan sebuah tabel rute dengan gateway jika salah satu dari berikut ini berlaku:

- Tabel rute berisikan rute-rute yang ada dengan target selain dari antarmuka jaringan, titik akhir Penyeimbang Beban Gateway, atau rute lokal default.
- Tabel rute berisikan rute yang ada untuk blok CIDR di luar kisaran di VPC Anda.
- Rute propagasi diaktifkan untuk tabel rute.

Sebagai tambahan, aturan dan pertimbangan berikut berlaku:

- Anda tidak dapat menambahkan rute ke setiap blok CIDR di luar kisaran di VPC Anda, termasuk kisaran yang lebih besar dari masing-masing blok CIDR VPC.
- Anda hanya dapat menentukan `local`, titik akhir Penyeimbang Beban Gateway, atau antarmuka jaringan sebagai target. Anda tidak dapat menentukan jenis target lainnya, termasuk alamat IP host individu. Untuk informasi selengkapnya, lihat the section called “Opsi perutean contoh”.
- Anda tidak dapat menentukan daftar prefiks sebagai tujuan.
- Anda tidak dapat menggunakan tabel rute gateway untuk mengendalikan atau mencegat lalu lintas di luar VPC Anda, misalnya, lalu lintas melalui Transit Gateway yang terlampir. Anda dapat

mencegat lalu lintas yang memasuki VPC Anda dan mengarahkannya kembali ke target lain di VPC yang sama.

- Untuk memastikan lalu lintas mencapai perangkat middlebox Anda, antarmuka jaringan target harus dilampirkan ke instans yang sedang berjalan. Untuk lalu lintas yang mengalir melalui gateway internet, antarmuka jaringan target juga harus memiliki alamat IP publik.
- Saat mengkonfigurasi perangkat middlebox Anda, perhatikan Pertimbangan perangkat.
- Ketika Anda mengarahkan lalu lintas melalui perangkat middlebox, lalu lintas yang kembali dari subnet tujuan harus diarahkan melalui perangkat yang sama. Perutean asimetris tidak di-support.
- Aturan tabel rute berlaku untuk semua lalu lintas yang meninggalkan subnet. Lalu lintas yang meninggalkan subnet didefinisikan sebagai lalu lintas yang ditujukan ke alamat MAC router gateway subnet tersebut. Lalu lintas yang ditujukan untuk alamat MAC dari antarmuka jaringan lain di subnet menggunakan routing tautan data (lapisan 2) alih-alih jaringan (lapisan 3) sehingga aturan tidak berlaku untuk lalu lintas ini.
- Tidak semua Zona Lokal mendukung asosiasi tepi dengan gateway pribadi virtual. Untuk informasi selengkapnya tentang zona yang tersedia, lihat Pertimbangan di Panduan Pengguna Zona AWS Lokal.

Cara kerja prioritas rute

Secara umum, kami mengarahkan lalu lintas menggunakan rute paling spesifik yang sesuai dengan lalu lintas. Ini dikenal sebagai pertandingan awalan terpanjang. Jika tabel rute Anda memiliki rute yang tumpang tindih atau cocok, aturan tambahan berlaku.

Daftar berikut menunjukkan ringkasan prioritas rute dengan tautan ke bagian di bawah ini dengan informasi dan contoh yang lebih rinci:

1. Awalan terpanjang (misalnya, 10.10.2. 15/32 memiliki prioritas di atas 10.10.2. 0/24)
2. Rute statis (seperti peering VPC dan koneksi gateway internet)
3. Daftar rute awalan
4. Rute yang disebarkan
   a. Rute Direct Connect BGP (rute dinamis)
   b. Rute statis VPN
   c. Rute VPN BGP (rute dinamis) (seperti gateway pribadi virtual)

Pencocokan awalan terpanjang

Rute ke alamat IPv4 dan IPv6 atau blok CIDR tidak saling ketergantungan satu sama lain. Kami menggunakan rute yang paling spesifik yang sesuai baik lalu lintas IPv4 atau lalu lintas IPv6 untuk menentukan bagaimana mengarahkan lalu lintas.

Contoh tabel rute subnet berikut memiliki rute untuk lalu lintas internet IPv4 (`0.0.0.0/0`) yang menunjuk ke gateway internet, dan rute untuk lalu lintas `172.31.0.0/16` IPv4 yang menunjuk ke koneksi peering (). `pcx-11223344556677889` Setiap lalu lintas dari subnet yang ditujukan untuk kisaran alamat IP `172.31.0.0/16` menggunakan koneksi peering, karena rute ini lebih spesifik daripada rute untuk gateway internet. Setiap lalu lintas yang ditujukan untuk target di dalam VPC (`10.0.0.0/16`) tercakup oleh rute `local`, dan oleh karenanya lalu lintas diarahkan di dalam VPC. Semua lalu lintas lainnya dari subnet menggunakan gateway internet.

Tujuan	Target
10.0.0. 0/16	lokal
172.31.0. 0/16	pcx-11223344556677889
0.0.0. 0/0	igw-12345678901234567

Prioritas rute untuk rute statis dan disebarkan secara dinamis

Jika Anda telah melampirkan gateway pribadi virtual ke VPC dan mengaktifkan propagasi rute pada tabel rute subnet, rute yang mewakili koneksi Site-to-Site VPN Anda secara otomatis muncul sebagai rute yang disebarkan di tabel rute Anda.

Jika tujuan rute yang disebarkan identik dengan tujuan rute statis, rute statis diprioritaskan. Sumber daya berikut menggunakan rute statis:

- gateway internet
- Gateway NAT
- Antarmuka jaringan
- ID Instans
- VPC endpoint Gateway
- Transit Gateway

- Koneksi peering VPC
- Titik akhir Penyeimbang Beban Gateway

Untuk informasi selengkapnya, lihat Prioritas tabel rute dan rute VPN di AWS Site-to-Site VPN Panduan Pengguna.

Contoh tabel rute berikut memiliki rute statis ke gateway internet dan rute yang disebarkan ke gateway pribadi virtual. Kedua rute memiliki tujuan `172.31.0.0/24`. Karena rute statis ke gateway internet menjadi prioritas, semua lalu lintas yang ditakdirkan akan dialihkan ke gateway internet. `172.31.0.0/24`

Tujuan	Target	Diperbanyak
10.0.0. 0/16	lokal	Tidak
172.31.0. 0/24	vgw-11223344556677889	Ya
172.31.0. 0/24	igw-12345678901234567	Tidak

Prioritas rute untuk daftar prefiks

Jika tabel rute Anda mereferensikan daftar prefiks, aturan berikut berlaku:

- Jika tabel rute berisi rute yang disebarkan yang cocok dengan rute yang mereferensikan daftar awalan, rute yang mereferensikan daftar awalan akan diprioritaskan. Harap dicatat bahwa untuk rute yang tumpang tindih, rute yang lebih spesifik selalu diprioritaskan terlepas dari apakah itu rute yang disebarkan, rute statis, atau rute yang mereferensikan daftar awalan.
- Jika tabel rute Anda mereferensikan beberapa daftar prefiks yang memiliki blok-blok CIDR yang tumpang tindih ke target-target yang berbeda, kami secara acak memilih rute mana yang menjadi prioritas. Setelah itu, rute yang sama selalu menjadi prioritas.

Opsi perutean contoh

Topik berikut menjelaskan perutean untuk gateway atau koneksi tertentu di VPC Anda.

Daftar Isi

- Perutean ke gateway internet

- Perutean ke perangkat NAT
- Perutean ke virtual private gateway
- Perutean ke AWS Outposts gerbang lokal
- Perutean ke koneksi peering VPC
- Perutean ke VPC endpoint gateway
- Perutean ke gateway internet egress-only
- Perutean untuk Transit Gateway
- Perutean untuk perangkat middlebox
- Perutean menggunakan daftar prefiks
- Perutean ke titik akhir Penyeimbang Beban Gateway

Perutean ke gateway internet

Anda dapat membuat sebuah subnet menjadi subnet publik dengan menambahkan sebuah rute di tabel rute subnet Anda ke gateway internet. Untuk melakukannya, buat dan lampirkan gateway internet untuk VPC Anda, dan kemudian tambahkan rute dengan tujuan `0.0.0.0/0` untuk lalu lintas IPv4 atau lalu lintas IPv6 `::/0`, dan target ID gateway internet (`igw-xxxxxxxxxxxxxxxxx`).

Tujuan	Target
0.0.0. 0/0	*igw-id*
::/0	*igw-id*

Untuk informasi selengkapnya, lihat Aktifkan akses internet untuk VPC menggunakan gateway internet.

Perutean ke perangkat NAT

Untuk mengaktifkan instans di subnet pribadi agar terhubung ke internet, Anda dapat membuat gateway NAT atau meluncurkan instans NAT di subnet publik. Kemudian tambahkan rute untuk tabel rute subnet pribadi yang mengarahkan lalu lintas internet IPv4 (`0.0.0.0/0`) ke perangkat NAT.

Tujuan	Target
0.0.0. 0/0	*nat-gateway-id*

Anda juga dapat membuat rute yang lebih spesifik ke target lain untuk menghindari biaya pemrosesan data yang tidak perlu untuk menggunakan gateway NAT, atau untuk mengarahkan lalu lintas tertentu secara pribadi. Dalam contoh berikut, lalu lintas Amazon S3 (pl-xxxxxxxx, daftar awalan yang berisi rentang alamat IP untuk Amazon S3 di Wilayah tertentu) dialihkan ke titik akhir VPC gateway, dan 10.25.0. 0/16 lalu lintas dialihkan ke koneksi peering VPC. Rentang alamat IP ini lebih spesifik dari 0.0.0. 0/0. Ketika instans-instans mengirimkan lalu lintas ke Amazon S3 atau ke VPC rekan, lalu lintas dikirim ke VPC endpoint gateway atau koneksi peering VPC. Semua lalu lintas lainnya dikirim ke gateway NAT.

Tujuan	Target
0.0.0. 0/0	*nat-gateway-id*
pl- *xxxxxxxx*	*vpce-id*
10.25.0. 0/16	*pcx-id*

Untuk informasi selengkapnya, lihat Perangkat NAT.

Perutean ke virtual private gateway

Anda dapat menggunakan AWS Site-to-Site VPN koneksi untuk mengaktifkan instance di VPC Anda untuk berkomunikasi dengan jaringan Anda sendiri. Untuk melakukannya, buat dan lampirkan virtual private gateway ke VPC Anda. Kemudian tambahkan rute di tabel rute subnet Anda dengan tujuan jaringan Anda dan target virtual private gateway (`vgw-xxxxxxxxxxxxxxxxx`).

Tujuan	Target
10.0.0. 0/16	*vgw-id*

Anda kemudian dapat membuat dan mengkonfigurasi koneksi Site-to-Site VPN Anda. Untuk informasi selengkapnya, lihat Apa itu AWS Site-to-Site VPN? dan Tabel rute dan prioritas rute VPN di Panduan Pengguna AWS Site-to-Site VPN .

Koneksi Site-to-Site VPN pada gateway pribadi virtual tidak mendukung lalu lintas IPv6. Namun, kami men-support lalu lintas IPv6 diarahkan melalui virtual private gateway ke koneksi Direct Connect . Untuk informasi selengkapnya, silakan lihat Panduan Pengguna Direct Connect.

Perutean ke AWS Outposts gerbang lokal

Bagian ini menjelaskan konfigurasi tabel routing untuk routing ke gateway AWS Outposts lokal.

Daftar Isi

- Aktifkan lalu lintas antara subnet Outpost dan jaringan lokal Anda
- Aktifkan lalu lintas antar subnet di VPC yang sama di Pos Terdepan

Aktifkan lalu lintas antara subnet Outpost dan jaringan lokal Anda

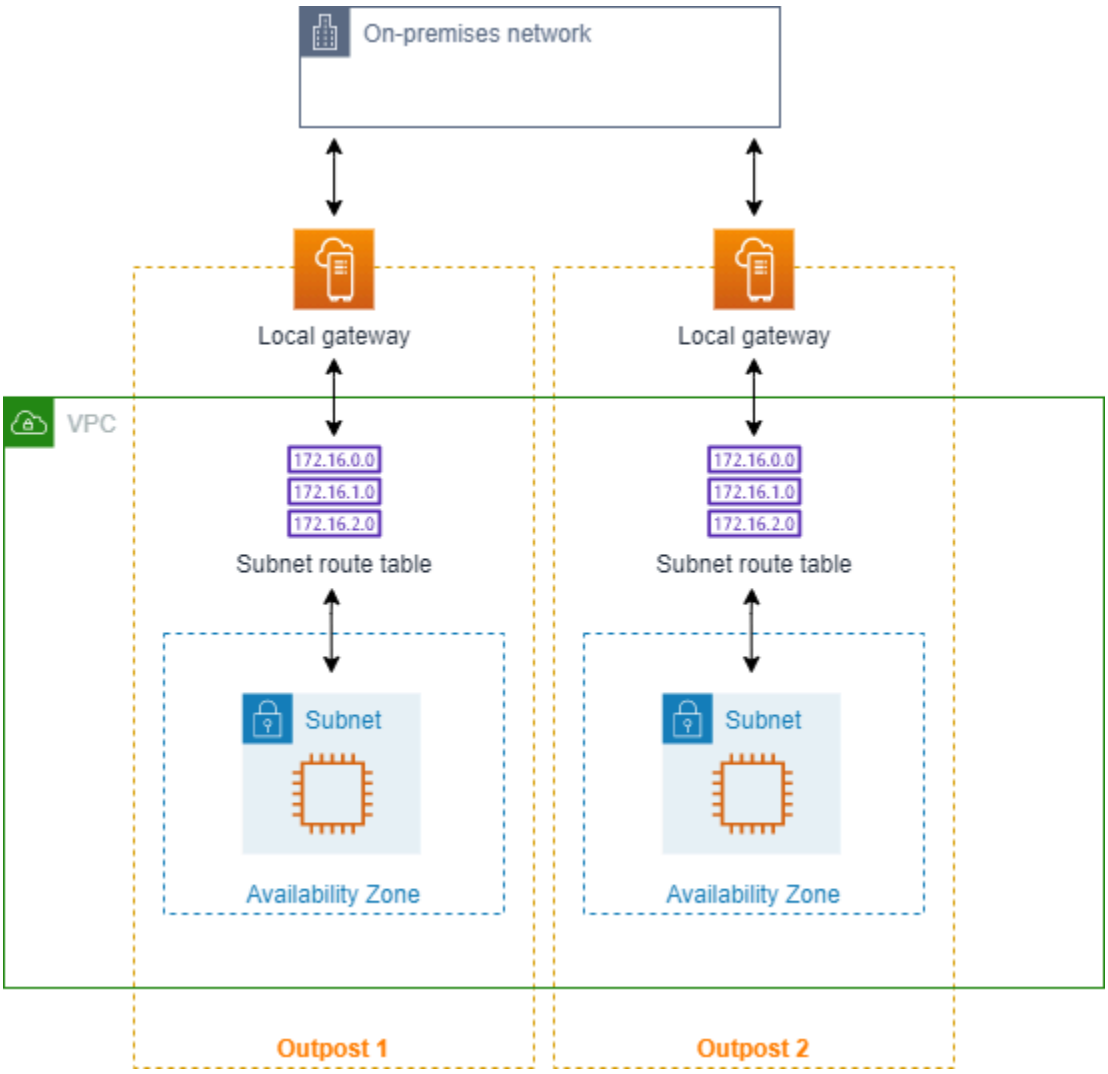
Subnet yang ada di VPC yang terkait dengan AWS Outposts dapat memiliki tipe target tambahan dari gateway lokal. Pertimbangkan kasus di mana Anda ingin memiliki lalu lintas rute gateway lokal dengan alamat tujuan 192.168.10. 0/24 ke jaringan pelanggan. Untuk melakukannya, tambahkan rute berikut dengan jaringan tujuan dan target gateway lokal (`lgw-xxxx`).

Tujuan	Target
192.168.10. 0/24	*lgw-id*

Aktifkan lalu lintas antar subnet di VPC yang sama di Pos Terdepan

Anda dapat membangun komunikasi antara subnet yang berada di VPC yang sama di pos terdepan yang berbeda menggunakan gateway lokal Outpost dan jaringan on-premise Anda.

Anda dapat menggunakan fitur ini untuk membangun arsitektur yang mirip dengan arsitektur Zona Multi-availabilitas (AZ) untuk aplikasi lokal Anda yang berjalan di rak Outposts dengan membangun konektivitas antara rak Outpost yang ditambatkan ke AZ yang berbeda.



Untuk mengaktifkan fitur ini, tambahkan rute ke tabel rute subnet rak Outpost yang lebih spesifik daripada rute lokal di tabel rute tersebut dan memiliki tipe target gateway lokal. Tujuan rute harus sesuai dengan seluruh blok IPv4 subnet di VPC Anda yang ada di Outpost lain. Ulangi konfigurasi ini untuk semua subnet Outpost yang perlu berkomunikasi.

Important

- Untuk menggunakan fitur ini, Anda harus menggunakan routing VPC langsung. Anda tidak dapat menggunakan alamat IP milik pelanggan Anda sendiri.
- Jaringan lokal Anda yang terhubung dengan gateway lokal Outposts harus memiliki routing yang diperlukan sehingga subnet dapat mengakses satu sama lain.

- Jika Anda ingin menggunakan grup keamanan untuk sumber daya di subnet, Anda harus menggunakan aturan yang menyertakan rentang alamat IP sebagai sumber atau tujuan di subnet Outpost. Anda tidak dapat menggunakan ID grup keamanan.
- Rak Pos Terdepan yang ada mungkin memerlukan pembaruan untuk mengaktifkan dukungan komunikasi intra-VPC di beberapa pos terdepan. Jika fitur ini tidak berfungsi untuk Anda, hubungi AWS Dukungan.

Example Contoh

Untuk VPC dengan CIDR 10.0.0. 0/16, subnet Outpost 1 dengan CIDR 10.0.1. 0/24, dan subnet Outpost 2 dengan CIDR 10.0.2. 0/24, entri untuk tabel rute subnet Outpost 1 adalah sebagai berikut:

Tujuan	Target
10.0.0. 0/16	Lokal:
10.0.2. 0/24	*lgw-1-id*

Entri untuk tabel rute subnet Outpost 2 adalah sebagai berikut:

Tujuan	Target
10.0.0. 0/16	Lokal:
10.0.1. 0/24	*lgw-2-id*

Perutean ke koneksi peering VPC

Koneksi peering VPC adalah koneksi jaringan antara dua VPC yang memungkinkan Anda mengarahkan lalu lintas di antara keduanya menggunakan alamat IPv4 pribadi. Instans-instans di VPC yang manapun dapat berkomunikasi satu sama lain seolah-olah mereka berada di jaringan yang sama.

Untuk mengaktifkan perutean lalu lintas antar VPC dalam koneksi peering VPC, Anda harus menambahkan rute ke satu atau lebih tabel rute subnet yang mengarah ke koneksi peering VPC. Ini memungkinkan Anda mengakses semua atau sebagian blok CIDR dari VPC yang lain dalam koneksi

peering. Demikian pula, pemilik VPC yang lain harus menambahkan rute ke tabel rute subnet mereka untuk mengarahkan lalu lintas kembali ke VPC Anda.

Misalnya, Anda memiliki koneksi peering VPC (`pcx-11223344556677889`) di antara dua VPC, dengan informasi berikut:

- VPC A: Blok CIDR adalah 10.0.0. 0/16
- VPC B: Blok CIDR adalah 172.31.0. 0/16

Untuk mengaktifkan lalu lintas antar VPC dan mengizinkan akses ke seluruh blok CIDR IPv4 dari VPC manapun, tabel rute VPC A dikonfigurasi sebagai berikut.

Tujuan	Target
10.0.0. 0/16	Lokal:
172.31.0. 0/16	pcx-11223344556677889

Tabel rute VPC B dikonfigurasi sebagai berikut.

Tujuan	Target
172.31.0. 0/16	Lokal:
10.0.0. 0/16	pcx-11223344556677889

Koneksi peering VPC Anda juga dapat men-support komunikasi IPv6 antar instans di VPC, jika VPC dan instans diaktifkan untuk komunikasi IPv6.

Untuk mengaktifkan routing lalu lintas IPv6 antara VPC, tambahkan rute ke tabel rute Anda yang menunjuk ke koneksi peering VPC untuk mengakses semua atau sebagian blok IPv6 CIDR dari VPC peer.

Misalnya, menggunakan koneksi peering VPC yang sama (`pcx-11223344556677889`) di atas, asumsikan VPC-VPC tersebut memiliki informasi berikut:

- VPC A: Blok CIDR IPv6 adalah `2001:db8:1234:1a00::/56`

- VPC B: Blok CIDR IPv6 adalah `2001:db8:5678:2b00::/56`

Untuk mengaktifkan komunikasi IPv6 melalui koneksi peering VPC, tambahkan rute berikut ke tabel rute subnet untuk VPC A.

Tujuan	Target
10.0.0. 0/16	Lokal:
172.31.0. 0/16	pcx-11223344556677889
2001:db8:5678:2b00::/56	pcx-11223344556677889

Tambahkan rute berikut ke tabel rute untuk VPC B.

Tujuan	Target
172.31.0. 0/16	Lokal:
10.0.0. 0/16	pcx-11223344556677889
2001:db8:1234:1a00::/56	pcx-11223344556677889

Untuk informasi selengkapnya tentang koneksi peering VPC, lihat Panduan Peering Amazon VPC.

Perutean ke VPC endpoint gateway

Titik akhir VPC gateway memungkinkan Anda membuat koneksi pribadi antara VPC Anda dan layanan lain AWS . Ketika Anda membuat titik akhir gateway, Anda menentukan tabel rute subnet di VPC Anda yang digunakan oleh titik akhir gateway. Sebuah rute secara otomatis ditambahkan ke masing-masing tabel rute dengan tujuan yang menentukan ID layanan daftar prefiks (`pl-xxxxxxxx`), dan target dengan ID titik akhir (`vpce-xxxxxxxxxxxxxxxxx`). Anda tidak dapat secara eksplisit menghapus atau memodifikasi rute titik akhir, tetapi Anda dapat mengubah tabel rute yang digunakan oleh titik akhir.

Untuk informasi lebih lanjut tentang perutean untuk titik akhir, dan implikasi untuk rute ke layanan AWS , lihat Perutean untuk titik akhir gateway.

Perutean ke gateway internet egress-only

Anda dapat membuat gateway internet egress-only untuk VPC Anda untuk mengaktifkan instans di subnet pribadi untuk mulai berkomunikasi outbound ke internet, tetapi mencegah internet untuk terhubung dengan instans. Gateway internet egress-only digunakan untuk lalu lintas IPv6 saja. Untuk mengonfigurasi perutean untuk gateway internet egress-only, tambahkan sebuah rute dalam tabel rute subnet pribadi yang mengarahkan lalu lintas internet IPv6 (`::/0`) ke gateway internet egress-only.

Tujuan	Target
::/0	*eigw-id*

Untuk informasi selengkapnya, lihat Aktifkan lalu lintas IPv6 keluar menggunakan gateway internet khusus keluar.

Perutean untuk Transit Gateway

Ketika Anda melampirkan sebuah VPC ke Transit Gateway, Anda perlu menambahkan rute ke tabel rute subnet Anda agar lalu lintas dapat terarahkan melalui Transit Gateway.

Pertimbangkan skenario berikut di mana Anda memiliki tiga VPC yang dipasangkan ke Transit Gateway. Dalam skenario ini, semua lampiran dikaitkan dengan tabel rute transit gateway dan mempropagasi tabel rute transit gateway. Oleh karena itu, semua lampiran dapat mengarahkan paket satu sama lain, dengan Transit Gateway yang berfungsi sebagai pusat IP 3 lapis sederhana.

Misalnya, Anda memiliki dua VPC, dengan informasi berikut:

- VPC A: 10.1.0. 0/16, ID lampiran tgw-attach-111111111111111
- VPCB: 10.2.0. 0/16, ID lampiran tgw-attach-22222222222222222

Untuk mengaktifkan lalu lintas antar VPC dan mengizinkan akses ke Transit Gateway, tabel rute VPC A dikonfigurasi sebagai berikut.

Tujuan	Target
10.1.0. 0/16	lokal

Tujuan	Target
10.0.0. 0/8	*tgw-id*

Berikut ini adalah contoh entri tabel rute Transit Gateway untuk pelampiran VPC.

Tujuan	Target
10.1.0. 0/16	tgw-attach-11111111111111111
10.2.0. 0/16	tgw-attach-22222222222222222

Untuk informasi selengkapnya tabel rute Transit Gateway, lihat Perutean di Transit Gateway Amazon VPC.

Perutean untuk perangkat middlebox

Anda dapat menambahkan peralatan middlebox ke jalur routing untuk VPC Anda. Berikut ini adalah kemungkinan kasus penggunaan:

- Cegat lalu lintas yang memasuki VPC Anda melalui gateway internet atau gateway pribadi virtual dengan mengarahkannya ke alat middlebox di VPC Anda. Anda dapat menggunakan wizard routing middlebox untuk AWS secara otomatis mengonfigurasi tabel rute yang sesuai untuk gateway, middlebox, dan subnet tujuan Anda. Untuk informasi selengkapnya, lihat the section called “Wisaya perutean Middlebox”.
- Arahkan lalu lintas antara dua subnet ke alat middlebox. Anda dapat melakukannya dengan membuat rute untuk satu tabel rute subnet yang cocok dengan CIDR subnet dari subnet lainnya dan menentukan titik akhir Gateway Load Balancer, gateway NAT, titik akhir Firewall Jaringan, atau antarmuka jaringan untuk alat sebagai target. Atau, untuk mengarahkan semua lalu lintas dari subnet ke subnet lain, ganti target rute lokal dengan titik akhir Gateway Load Balancer, gateway NAT, atau antarmuka jaringan.

Anda dapat mengonfigurasi perangkat menyesuaikan kebutuhan Anda. Misalnya, Anda dapat mengonfigurasi perangkat keamanan yang menyaring semua lalu lintas, atau perangkat akselerasi WAN. Perangkat ini digunakan sebagai instans Amazon EC2 di subnet di VPC Anda, dan diwakili oleh antarmuka jaringan elastis (antarmuka jaringan) di subnet Anda.

Jika Anda mengaktifkan propagasi rute untuk tabel rute subnet tujuan, perhatikan prioritas rute. Kami memprioritaskan rute yang paling spesifik, dan jika rute cocok, kami memprioritaskan rute statis atas rute yang disebarkan.

Tinjau rute Anda untuk memastikan bahwa lalu lintas dirutekan dengan benar dan tidak ada konsekuensi yang tidak diinginkan jika Anda mengaktifkan atau menonaktifkan propagasi rute (misalnya, propagasi rute diperlukan untuk Direct Connect koneksi yang mendukung bingkai jumbo).

Untuk mengarahkan lalu lintas VPC inbound ke sebuah perangkat, Anda kaitkan sebuah tabel rute dengan gateway internet atau virtual private gateway, dan tentukan antarmuka jaringan dari perangkat Anda sebagai target untuk lalu lintas VPC. Untuk informasi selengkapnya, lihat Tabel rute gateway. Anda juga dapat mengarahkan lalu lintas outbound dari subnet Anda ke sebuah perangkat middlebox di subnet lain.

Untuk contoh perutean middlebox, lihat. Skenario Middlebox

Daftar Isi

- Pertimbangan perangkat
- Perutean lalu lintas antara gateway dan alat
- Merutekan lalu lintas antar-subnet ke alat

Pertimbangan perangkat

Anda dapat memilih perangkat pihak ketiga dari AWS Marketplace, atau Anda dapat mengonfigurasi perangkat Anda sendiri. Saat Anda membuat atau mengonfigurasi sebuah perangkat, perhatikan hal berikut:

- Perangkat harus dikonfigurasi di subnet terpisah ke lalu lintas sumber atau tujuan.
- Anda harus menonaktifkan source/destination pengecekan pada alat. Untuk informasi selengkapnya, lihat Meng ubah Sumber atau Pemeriksaan Tujuan di Panduan Pengguna Amazon EC2.
- Anda tidak dapat mengarahkan lalu lintas antar host di subnet yang sama melalui sebuah perangkat.
- Alat tidak harus melakukan penerjemahan alamat jaringan (NAT).
- Anda dapat menambahkan rute ke tabel rute yang lebih spesifik daripada rute lokal. Anda dapat menggunakan rute yang lebih spesifik untuk mengarahkan lalu lintas antar subnet dalam VPC

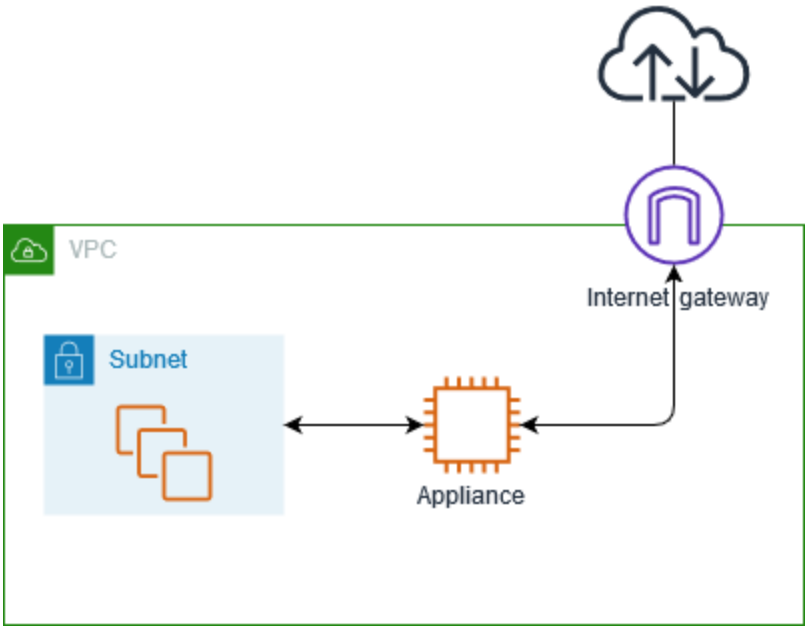
(East-West lalu lintas) ke alat middlebox. Tujuan rute harus cocok dengan seluruh blok CIDR IPv4 atau IPv6 dari subnet di VPC Anda.

- Untuk mencegat lalu lintas IPv6, pastikan bahwa VPC, subnet, dan alat Anda mendukung IPv6.
-

> **Important**
>
> Jangan merutekan lalu lintas AWS dari layanan yang dikelola — seperti gateway transit, gateway NAT, atau Network Load Balancer — melalui alat middlebox kembali ke subnet tempat layanan tersebut terpasang. Konfigurasi ini menyebabkan perilaku routing yang tidak dapat diprediksi dan tidak didukung.

Perutean lalu lintas antara gateway dan alat

Untuk mengarahkan lalu lintas VPC inbound ke sebuah perangkat, Anda kaitkan sebuah tabel rute dengan gateway internet atau virtual private gateway, dan tentukan antarmuka jaringan dari perangkat Anda sebagai target untuk lalu lintas VPC. Dalam contoh berikut, VPC memiliki gateway internet, alat, dan subnet dengan instance. Lalu lintas dari internet dialihkan melalui alat.



Kaitkan tabel rute ini dengan gateway internet atau virtual private gateway Anda. Entri pertama adalah rute lokal. Entri kedua mengirimkan lalu lintas IPv4 yang ditujukan untuk subnet ke antarmuka jaringan untuk alat. Rute ini lebih spesifik daripada rute lokal.

Tujuan	Target
VPC CIDR	Lokal:
Subnet CIDR	*Appliance network interface ID*

Atau, Anda dapat mengganti target untuk rute lokal dengan antarmuka jaringan alat. Anda dapat melakukan ini untuk memastikan bahwa semua lalu lintas secara otomatis dialihkan ke alat, termasuk lalu lintas yang ditujukan untuk subnet yang Anda tambahkan ke VPC di masa mendatang.

Tujuan	Target
VPC CIDR	*Appliance network interface ID*

Untuk mengarahkan lalu lintas dari subnet Anda ke perangkat di subnet lain, tambahkan rute ke tabel rute subnet Anda yang mengarahkan lalu lintas ke antarmuka jaringan perangkat. Tujuan seharusnya tidak lebih spesifik dibandingkan tujuan untuk rute lokal. Misalnya, untuk lalu lintas yang ditujukan untuk internet, tentukan `0.0.0.0/0` (semua alamat IPv4) untuk tujuan tersebut.

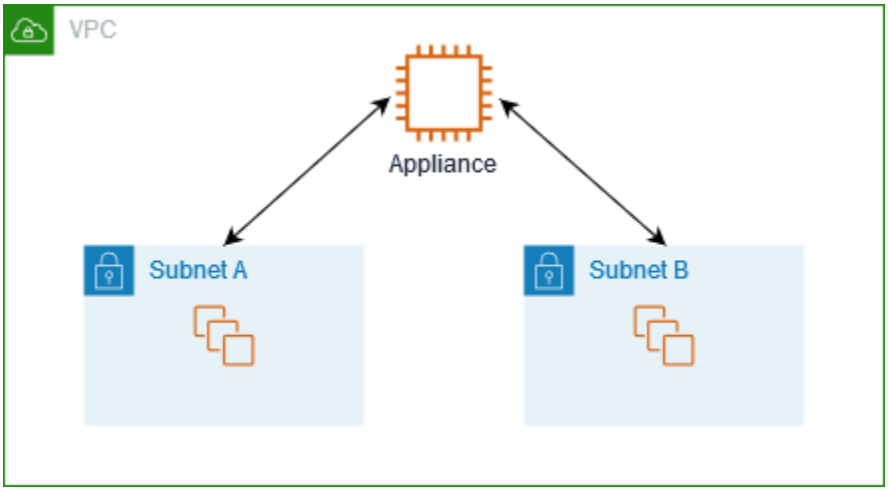
Tujuan	Target
VPC CIDR	Lokal:
0.0.0. 0/0	*Appliance network interface ID*

Kemudian, di tabel rute yang terkait dengan subnet alat, tambahkan rute yang mengirim lalu lintas kembali ke gateway internet atau gateway pribadi virtual.

Tujuan	Target
VPC CIDR	Lokal:
0.0.0. 0/0	*igw-id*

Merutekan lalu lintas antar-subnet ke alat

Anda dapat merutekan lalu lintas yang ditujukan untuk subnet tertentu ke antarmuka jaringan alat. Dalam contoh berikut, VPC berisi dua subnet dan alat. Lalu lintas antara subnet dirutekan melalui alat.



Grup keamanan

Saat Anda merutekan lalu lintas antar instans di subnet yang berbeda melalui alat middlebox, grup keamanan untuk kedua instans harus mengizinkan lalu lintas mengalir di antara instans. Grup keamanan untuk setiap instans harus mereferensikan alamat IP privat instans lain, atau rentang CIDR dari subnet yang berisi instans yang lain, sebagai sumbernya. Jika Anda mereferensikan grup keamanan instans lain sebagai sumbernya, hal ini tidak akan mengizinkan lalu lintas mengalir di antara instans.

Perutean

Berikut ini adalah contoh tabel rute untuk subnet A. Entri pertama memungkinkan instance di VPC untuk berkomunikasi satu sama lain. Entri kedua merutekan semua lalu lintas dari subnet A ke subnet B ke antarmuka jaringan alat.

Tujuan	Target
VPC CIDR	Lokal:
Subnet B CIDR	*Appliance network interface ID*

Berikut ini adalah contoh tabel rute untuk subnet B. Entri pertama memungkinkan instance di VPC untuk berkomunikasi satu sama lain. Entri kedua merutekan semua lalu lintas dari subnet B ke subnet A ke antarmuka jaringan alat.

Tujuan	Target
VPC CIDR	Lokal:
Subnet A CIDR	*Appliance network interface ID*

Atau, Anda dapat mengganti target untuk rute lokal dengan antarmuka jaringan alat. Anda dapat melakukan ini untuk memastikan bahwa semua lalu lintas secara otomatis dialihkan ke alat, termasuk lalu lintas yang ditujukan untuk subnet yang Anda tambahkan ke VPC di masa mendatang.

Tujuan	Target
VPC CIDR	*Appliance network interface ID*

Perutean menggunakan daftar prefiks

Jika Anda sering mereferensikan kumpulan blok CIDR yang sama di seluruh AWS sumber daya Anda, Anda dapat membuat daftar awalan yang dikelola pelanggan untuk mengelompokkan mereka bersama-sama. Anda kemudian dapat menentukan daftar prefiks sebagai tujuan dalam entri tabel rute Anda. Anda kemudian dapat menambah atau menghapus entri di daftar prefiks tanpa perlu memperbarui tabel rute Anda.

Misalnya, Anda memiliki Transit Gateway dengan beberapa lampiran VPC. VPC harus dapat berkomunikasi dengan dua lampiran VPC tertentu yang memiliki blok CIDR berikut:

- 10.0.0. 0/16
- 10.2.0. 0/16

Anda buat daftar prefiks dengan kedua entri. Dalam tabel rute subnet Anda, Anda membuat rute dan menentukan daftar prefiks sebagai tujuan, dan Transit Gateway sebagai target.

Tujuan	Target
172.31.0. 0/16	Lokal:
pl-123abc123abc123ab	*tgw-id*

Jumlah entri maksimal untuk daftar prefiks sama dengan jumlah entri dalam tabel rute.

Perutean ke titik akhir Penyeimbang Beban Gateway

Sebuah Penyeimbang Beban Gateway memungkinkan Anda untuk mendistribusikan lalu lintas ke sebuah armada perangkat virtual, seperti firewall. Anda dapat membuat Gateway Load Balancer, mengonfigurasi layanan titik akhir Gateway Load Balancer, dan kemudian membuat titik akhir Gateway Load Balancer di VPC Anda untuk menghubungkannya ke layanan.

Untuk mengarahkan lalu lintas Anda ke Penyeimbang Beban Gateway (misalnya, untuk pemeriksaan keamanan), tentukan titik akhir Penyeimbang Beban Gateway sebagai target di tabel rute Anda.

Untuk contoh peralatan keamanan di balik Gateway Load Balancer, lihatthe section called “Periksa lalu lintas menggunakan peralatan keamanan”.

Untuk menentukan titik akhir Penyeimbang Beban Gateway dalam tabel rute, gunakan ID pada VPC endpoint. Misalnya untuk merutekan lalu lintas untuk 10.0.1. 0/24 ke titik akhir Gateway Load Balancer, tambahkan rute berikut.

Tujuan	Target
10.0.1. 0/24	*vpc-endpoint-id*

Saat menggunakan titik akhir Gateway Load Balancer sebagai target, Anda tidak dapat menentukan daftar awalan sebagai tujuan. Jika Anda mencoba membuat atau mengganti rute daftar awalan yang menargetkan Titik Akhir VPC, Anda akan menerima kesalahan: “Tidak dapat membuat atau mengganti rute daftar awalan yang menargetkan Titik Akhir VPC.”

Untuk informasi selengkapnya, lihat Gateway Load Balancers.

Buat tabel rute untuk VPC Anda

Selesaikan tugas berikut untuk membuat dan mengonfigurasi tabel rute khusus untuk VPC Anda. Secara default tabel rute baru Anda berisi rute lokal yang memungkinkan komunikasi dalam VPC. Anda dapat menambahkan rute untuk mengarahkan lalu lintas jaringan ke target tertentu berdasarkan rentang alamat IP tujuan.

Agar tabel rute mengarah ke subnet khusus, Anda harus mengaitkan tabel rute dengan subnet. Sebuah tabel rute dapat dikaitkan dengan beberapa subnet. Namun, subnet hanya dapat dikaitkan dengan satu tabel rute pada satu waktu. Setiap subnet tidak secara eksplisit dikaitkan dengan tabel yang secara implisit dikaitkan dengan tabel rute utama secara default.

Anda dapat memutus pengaitan subnet dari tabel rute. Sebelum Anda mengaitkan subnet dengan tabel rute lain, subnet secara implisit terkait dengan tabel rute utama.

> **Note**
>
> Terdapat kuota jumlah tabel rute yang dapat Anda buat per VPC. Juga terdapat kuota jumlah rute yang dapat Anda tambahkan per tabel rute. Untuk informasi selengkapnya, lihat Kuota Amazon VPC.

Tugas

- Buat tabel rute
- Tambahkan rute ke tabel rute
- Mengaitkan subnet dengan tabel rute

Buat tabel rute

Untuk membuat tabel rute menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Tabel rute.
3. Pilih Buat tabel rute.
4. (Opsional) Untuk Nama, masukkan nama untuk tabel rute Anda.
5. Untuk VPC, pilih VPC Anda.

6. (Opsional) Untuk menambahkan tag, pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.
7. Pilih Buat tabel rute.

Untuk membuat tabel rute menggunakan AWS CLI

Gunakan perintah create-route-table.

Tambahkan rute ke tabel rute

Untuk menambahkan rute ke tabel rute menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Tabel rute, dan pilih tabel rute.
3. Pilih Tindakan, Sunting rute.
4. Pilih Tambahkan rute.
5. Untuk Tujuan masukkan salah satu dari berikut ini:
   - Rentang alamat IP - Misalnya, 192.168.0. 0/16
   - Alamat IP tunggal - Misalnya, 192.168.10. 1/32
   - ID daftar awalan - Misalnya, pl-0abcdef1234567890
6. Untuk Target, pilih jenis sumber daya (misalnya, antarmuka jaringan) dan kemudian masukkan ID sumber daya (misalnya, eni-11223344556677889).
7. Pilih Simpan perubahan.

Untuk menambahkan rute ke tabel rute menggunakan AWS CLI

Gunakan perintah create-route.

Mengaitkan subnet dengan tabel rute

Untuk mengaitkan tabel rute dengan subnet menggunakan konsol tersebut

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Tabel rute, lalu pilih tabel rute.
3. Pada tab Pengaitan subnet, pilih Sunting pengaitan subnet.

4. Pilih kotak centang untuk subnet yang akan diasosiasikan dengan tabel rute.
5. Pilih Simpan pengaitan.

Untuk mengaitkan atau memisahkan subnet dengan tabel rute menggunakan AWS CLI

- tabel rute asosiasi
- pisahkan-rute-tabel

Kelola tabel rute subnet

Gunakan prosedur berikut untuk mengelola routing VPC menggunakan tabel rute.

Tugas

- Tentukan tabel rute untuk subnet
- Tentukan asosiasi eksplisit
- Menambahkan, memodifikasi, dan menghapus rute
- Aktifkan atau nonaktifkan propagasi rute
- Ubah tabel rute untuk subnet

Tentukan tabel rute untuk subnet

Anda dapat menentukan tabel rute mana yang dikaitkan dengan sebuah subnet dengan melihat rincian subnet di konsol Amazon VPC.

Untuk menentukan tabel rute untuk subnet menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Pengguna.
3. Pilih subnet.
4. Pilih tab Tabel rute untuk melihat informasi tentang tabel rute dan rute-rutenya. Untuk menentukan apakah asosiasi tersebut ke tabel rute utama, dan jika asosiasi itu eksplisit, lihatTentukan asosiasi eksplisit.

Tentukan asosiasi eksplisit

Anda dapat menentukan seberapa banyak dan manakah subnet atau gateway yang secara eksplisit dikaitkan dengan tabel rute.

Tabel rute utama dapat memiliki pengaitan subnet yang eksplisit dan implisit. Tabel rute kustom hanya memiliki pengaitan yang eksplisit.

Subnet yang tidak dikaitkan secara eksplisit dengan tabel rute manapun memiliki pengaitan implisit dengan tabel rute utama. Anda dapat secara eksplisit mengaitkan sebuah subnet dengan tabel rute utama. Sebagai contoh apa alasan Anda mau mengaitkan itu, lihat Ganti tabel rute utama.

Untuk menentukan subnet manakah yang secara eksplisit dikaitkan menggunakan konsol tersebut

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Tabel rute.
3. Periksa kolom asosiasi subnet eksplisit untuk menentukan subnet yang terkait secara eksplisit dan kolom Utama untuk menentukan apakah ini adalah tabel rute utama.
4. Pilih tabel rute dan pilih tab Asosiasi subnet.
5. Subnet di bawah asosiasi subnet eksplisit secara eksplisit dikaitkan dengan tabel rute. Subnet di bawah Subnets tanpa asosiasi eksplisit milik VPC yang sama dengan tabel rute, tetapi tidak terkait dengan tabel rute apa pun, sehingga mereka secara implisit terkait dengan tabel rute utama untuk VPC.

Untuk menentukan gateway manakah yang secara eksplisit dikaitkan menggunakan konsol tersebut

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Tabel rute.
3. Pilih tabel rute dan pilih tab A sosiasi tepi.

Untuk menggambarkan satu atau lebih tabel rute dan melihat asosiasinya menggunakan AWS CLI

Gunakan perintah describe-route-tables.

Menambahkan, memodifikasi, dan menghapus rute

Anda dapat menambahkan, memodifikasi, dan menghapus rute untuk tabel rute Anda.

Untuk informasi selengkapnya tentang bekerja dengan rute statis untuk koneksi Site-to-Site VPN, lihat Mengedit Rute Statis untuk Koneksi Site-to-Site VPN di Panduan AWS Site-to-Site VPN Pengguna.

Pertimbangan-pertimbangan

- Anda hanya dapat memodifikasi rute yang telah Anda tambahkan.
- Saat Anda mengubah atau menghapus rute, koneksi yang ada yang menggunakan rute ini akan terpengaruh. Koneksi yang menggunakan rute lain tidak terpengaruh.
- Ada kuota pada jumlah rute yang dapat Anda tambahkan per tabel rute. Untuk informasi selengkapnya, lihat Kuota Amazon VPC.

Untuk memperbarui rute untuk tabel rute menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Tabel rute, dan pilih tabel rute.
3. Pilih Tindakan, Sunting rute.
4. Untuk menambahkan rute, pilih Tambah rute. Untuk Tujuan masukkan rentang alamat IP, alamat IP tunggal, atau ID daftar awalan. Untuk Target, pilih jenis sumber daya dan kemudian masukkan ID sumber daya.
5. Untuk mengubah rute, masukkan blok CIDR tujuan baru atau ID daftar awalan dan pilih target.
6. Untuk menghapus rute, pilih H apus.
7. Pilih Simpan perubahan.

Untuk memperbarui rute untuk tabel rute menggunakan AWS CLI

Jika Anda menambahkan rute menggunakan alat baris perintah atau API, blok CIDR tujuan secara otomatis berubah ke bentuk kanonisnya. Misalnya, jika Anda menentukan `100.68.0.18/18` untuk blok CIDR, kami membuat sebuah rute dengan blok CIDR tujuan `100.68.0.0/18`.

- buat-rute
- ganti rute
- hapus rute

Aktifkan atau nonaktifkan propagasi rute

Propagasi rute memungkinkan gateway pribadi virtual untuk secara otomatis menyebarkan rute ke tabel rute Anda. Ini berarti Anda tidak perlu menambahkan atau menghapus rute VPN secara manual.

Untuk menyelesaikan proses ini, Anda harus memiliki virtual private gateway.

Untuk informasi selengkapnya, lihat opsi perutean Site-to-Site Site-to-Site VPN di Panduan Pengguna VPN.

Untuk mengaktifkan atau menonaktifkan propagasi rute menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Tabel rute, lalu pilih tabel rute.
3. Pilih Tindakan, Sunting propagasi rute.
4. Pilih atau kosongkan kotak centang Aktifkan di sebelah gateway pribadi virtual.
5. Pilih Simpan.

Untuk mengaktifkan atau menonaktifkan propagasi rute menggunakan AWS CLI

- aktifkan-vgw-route-propagasi
- nonaktifkan-vgw-route-propagasi

Ubah tabel rute untuk subnet

Anda dapat mengubah pengaitan tabel rute untuk subnet.

Ketika Anda mengubah tabel rute, koneksi yang ada di subnet ditiadakan kecuali tabel rute yang baru berisikan rute untuk lalu lintas yang sama dengan target yang sama.

Untuk mengubah pengaitan tabel rute subnet menggunakan konsol tersebut

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Subnet, lalu pilih subnet.
3. Dari tab Tabel rute, pilih Edit asosiasi tabel rute.
4. Untuk ID tabel rute, pilih tabel rute baru.

5. Pilih Simpan.

Untuk mengubah tabel rute yang terkait dengan subnet menggunakan AWS CLI

Gunakan perintah replace-route-table-association.

Ganti tabel rute utama

Bagian ini menjelaskan cara mengubah tabel rute mana yang merupakan tabel rute utama di VPC Anda.

Untuk mengganti tabel rute utama menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Tabel rute, lalu pilih tabel rute utama yang baru.
3. Pilih T ind akan, Tetapkan tabel rute utama.
4. Saat diminta konfirmasi, masukkan**set**, lalu pilih OK.

Untuk mengganti tabel rute utama menggunakan AWS CLI

- Gunakan perintah replace-route-table-association.

Prosedur berikut ini menjelaskan cara menghapus pengaitan eksplisit antara subnet dan tabel rute utama. Hasilnya adalah pengaitan implisit antara subnet dan tabel rute utama. Proses ini sama dengan memutus pengaitan subnet apapun dari setiap tabel rute.

Untuk menghapus pengaitan eksplisit dengan tabel rute utama

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Tabel rute, lalu pilih tabel rute.
3. Dari tab A sosiasi subnet, pilih Edit asosiasi subnet.
4. Kosongkan kotak centang untuk subnet.
5. Pilih Simpan pengaitan.

Kontrol lalu lintas yang memasuki VPC Anda menggunakan tabel rute gateway

Untuk mengontrol lalu lintas yang memasuki VPC Anda dengan tabel rute gateway, Anda dapat mengaitkan atau memisahkan gateway internet atau gateway pribadi virtual dengan tabel rute. Untuk informasi selengkapnya, lihat Tabel rute gateway.

Untuk mengaitkan atau memutuskan hubungan gateway dengan tabel rute menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Tabel rute, lalu pilih tabel rute.
3. Dari tab Asosiasi tepi, pilih Edit asosiasi tepi.
4. Pilih atau hapus centang kotak untuk gateway.
5. Pilih Simpan perubahan.

Untuk mengaitkan gateway dengan tabel rute menggunakan AWS CLI

Gunakan perintah associate-route-table. Contoh berikut mengaitkan tabel rute yang ditentukan dengan gateway internet yang ditentukan.

```
aws ec2 associate-route-table
    --route-table-id rtb-01234567890123456 \
    --gateway-id igw-11aa22bb33cc44dd1
```

Untuk memisahkan gateway dari tabel rute menggunakan AWS CLI

Gunakan perintah disassociate-route-table. Tentukan ID asosiasi antara tabel rute dan gateway.

```
aws ec2 disassociate-route-table \
    --association-id rtbassoc-0abcdef1234567890
```

Mengganti atau memulihkan target untuk rute lokal

Anda dapat mengubah target rute lokal default. Jika Anda mengganti target rute lokal, Anda kemudian dapat mengembalikannya ke target `local` default. Jika VPC Anda memiliki beberapa blok CIDR, tabel rute Anda memiliki beberapa rute lokal—satu per blok CIDR. Anda dapat mengganti atau mengembalikan target dari masing-masing rute lokal sesuai kebutuhan.

Untuk mengganti rute lokal menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Tabel rute, lalu pilih tabel rute.
3. Dari tab Rute, pilih Edit rute.
4. Untuk rute lokal, hapus Target dan kemudian pilih target baru.
5. Pilih Simpan perubahan.

Untuk memulihkan target untuk rute lokal menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Tabel rute, lalu pilih tabel rute.
3. Pilih Tindakan, Sunting rute.
4. Untuk rute, hapus Target, lalu pilih lokal.
5. Pilih Simpan perubahan.

Untuk mengganti target untuk rute lokal menggunakan AWS CLI

Gunakan perintah replace-route. Contoh berikut menggantikan target rute lokal dengan antarmuka jaringan yang ditentukan.

```
aws ec2 replace-route \
    --route-table-id rtb-01234567890123456 \
    --destination-cidr-block 10.0.0.0/16 \
    --network-interface-id eni-11223344556677889
```

Untuk mengembalikan target untuk rute lokal menggunakan AWS CLI

Contoh berikut mengembalikan target lokal untuk tabel rute yang ditentukan.

```
aws ec2 replace-route \
    --route-table-id rtb-01234567890123456 \
    --destination-cidr-block 10.0.0.0/16 \
    --local-target
```

Perutean lanjutan di VPC Anda

Konfigurasikan skenario perutean lanjutan untuk VPC Anda. Bagian ini mencakup pendekatan perutean statis dan dinamis untuk mengelola arus lalu lintas:

- Perutean masuk statis: Konfigurasikan rute statis untuk mengarahkan lalu lintas internet masuk yang ditujukan untuk kumpulan alamat BYOIP (Bawa IP Anda Sendiri) ke antarmuka jaringan tertentu dalam VPC Anda.
- Perutean dinamis dengan VPC Route Server: Gunakan perutean dinamis berbasis BGP untuk memperbarui tabel rute gateway VPC dan internet secara otomatis, memberikan toleransi kesalahan dan failover otomatis untuk beban kerja Anda.

Konten

- Rute lalu lintas internet ke antarmuka jaringan tunggal
- Perutean dinamis di VPC Anda menggunakan VPC Route Server

Rute lalu lintas internet ke antarmuka jaringan tunggal

Anda dapat merutekan lalu lintas internet masuk yang ditujukan untuk kumpulan besar alamat IP publik ke antarmuka jaringan elastis tunggal (ENI) di VPC Anda.

Sebelumnya, gateway internet hanya menerima lalu lintas yang ditujukan untuk alamat IP publik yang secara langsung terkait dengan antarmuka jaringan di VPC. Jenis instans memiliki batasan jumlah alamat IP yang dapat dikaitkan dengan antarmuka jaringan, menciptakan tantangan bagi industri seperti Telekomunikasi dan Internet of Things (IoT) yang perlu menangani lalu lintas untuk kumpulan IP yang lebih besar dari batas ini.

Perutean ini menghilangkan terjemahan alamat kompleks pada koneksi internet masuk. Anda dapat membawa kolam IP publik Anda sendiri (BYOIP) dan mengonfigurasi gateway internet VPC Anda untuk menerima dan merutekan lalu lintas untuk seluruh kumpulan ke antarmuka jaringan tunggal. Fitur ini sangat berharga untuk:

- Telekomunikasi: Mengelola kumpulan IP pelanggan besar tanpa overhead terjemahan alamat
- Aplikasi IoT: Mengkonsolidasikan lalu lintas dari ribuan alamat IP perangkat
- Skenario apa pun: Memerlukan perutean lalu lintas di luar batas asosiasi ENI

Anda dapat mengintegrasikan routing ini dengan VPC Route Server untuk pembaruan rute dinamis selama skenario failover.

Manfaat utama

Pendekatan routing ini memberikan manfaat sebagai berikut:

- Tidak diperlukan terjemahan alamat - Perutean langsung menghilangkan kompleksitas NAT
- Melewati batas ENI - Tangani kumpulan IP yang lebih besar dari batas asosiasi instans
- Industry-optimized- Purpose-built untuk persyaratan Telco dan IoT
- Failover dinamis - Terintegrasi dengan Route Server untuk pembaruan otomatis

Ketersediaan

Anda dapat menggunakan fitur ini di semua wilayah AWS komersial, wilayah AWS China, dan AWS GovCloud wilayah.

Daftar Isi

- Sebelum Anda mulai
- Cara kerja fitur ini
- Langkah 1: Buat VPC
- Langkah 2: Buat dan lampirkan gateway internet
- Langkah 3: Buat subnet untuk instance target Anda
- Langkah 4: Buat tabel rute untuk subnet
- Langkah 5: Buat grup keamanan untuk instance target
- Langkah 6: Luncurkan instance EC2 target
- Langkah 7: Buat tabel rute gateway internet
- Langkah 8: Mengaitkan tabel rute dengan gateway internet
- Langkah 9: Asosiasikan kolam BYOIP Anda dengan gateway internet
- Langkah 10: Tambahkan rute statis untuk menargetkan instance Anda
- Langkah 11: Konfigurasikan instance target
- Langkah 12: Konfigurasikan instance untuk penanganan lalu lintas
- Langkah 13: Uji konektivitas

- Pemecahan masalah
- Opsi lanjutan: Integrasi server rute untuk perutean dinamis
- Bersihkan

Sebelum Anda mulai

Sebelum memulai tutorial ini, pastikan Anda memiliki:

1. Kumpulan BYOIP: Anda pasti sudah membawa rentang alamat IP Anda sendiri ke. AWS Selesaikan langkah-langkah di B awa alamat IP Anda sendiri (BYOIP) di Amazon EC2.
2. Verifikasi kumpulan BYOIP Anda: Konfirmasikan kolam Anda siap dengan menjalankan:

   ```
   aws ec2 describe-public-ipv4-pools --region us-east-1
   ```

   Cari kumpulan Anda di output dan pastikan `Available` alamat `PoolAddressRanges` pertunjukan.
3. Izin yang sesuai: Pastikan AWS akun Anda memiliki izin untuk membuat sumber daya VPC, instans EC2, dan mengelola kumpulan BYOIP.

Cara kerja fitur ini

Bagian ini menjelaskan konsep teknis di balik perutean masuk gateway internet dan bagaimana lalu lintas mengalir dari internet ke instance target Anda.

Mengapa menggunakan perutean masuk gateway internet

Sebelumnya, Anda perlu melakukan terjemahan alamat untuk mengkonsolidasikan lalu lintas untuk sejumlah besar alamat IP karena batas asosiasi ENI. Peningkatan ini menghilangkan kompleksitas itu dengan mengizinkan routing langsung kumpulan BYOIP ke instans target.

Cara kerja routing

Fitur ini hanya berfungsi dengan CIDR IP publik yang Anda bawa untuk AWS mengikuti proses BYOIP. Proses BYOIP memastikan bahwa akun Anda memiliki IP CIDR publik. Setelah Anda memiliki CIDR publik BYOIP:

1. Anda mengaitkan kumpulan alamat IP publik ini dengan tabel rute gateway internet. Gateway internet harus sudah dikaitkan dengan VPC. Asosiasi ini memungkinkan VPC menerima lalu lintas

yang ditujukan untuk IP CIDR. Pastikan bahwa gateway internet memiliki tabel rute khusus yang tidak dibagikan dengan subnet apa pun.

2. Sekarang setelah Anda mengaitkan kumpulan BYOIP dengan tabel rute gateway internet, Anda dapat memasukkan rute dengan tujuan yang sama dengan IP CIDR atau bagian darinya di tabel rute gateway internet. Target rute ini adalah ENI di mana Anda ingin mengarahkan lalu lintas Anda.
3. Ketika lalu lintas Anda yang ditujukan untuk BYOIP CIDR Anda masuk AWS, AWS lihat tabel rute gateway internet dan dengan demikian mengarahkan lalu lintas ke VPC yang relevan.
4. Di dalam VPC, gateway internet merutekan lalu lintas ke ENI target.
5. Target (antarmuka jaringan elastis yang terkait dengan beban kerja Anda) memproses lalu lintas.

Praktik terbaik

- Pisahkan tabel rute: Tabel rute gateway internet harus didedikasikan hanya untuk gateway internet. Jangan mengaitkan tabel rute ini dengan subnet VPC apa pun. Gunakan tabel rute terpisah untuk perutean subnet.
- Jangan langsung menetapkan IP BYOIP: Jangan mengaitkan alamat IP publik dari kumpulan BYOIP Anda secara langsung ke instans EC2 atau antarmuka jaringan. Fitur routing masuk gateway internet merutekan lalu lintas ke instance tanpa memerlukan asosiasi IP langsung.

> **Important**
>
> Jika Anda menggunakan VPC Block Public Access (BPA), ketika BPA diaktifkan, itu akan memblokir lalu lintas ke subnet menggunakan routing masuk, bahkan jika Anda telah menetapkan pengecualian BPA tingkat subnet. Subnet-levelpengecualian tidak berfungsi untuk routing masuk. Untuk mengizinkan lalu lintas routing masuk dengan BPA diaktifkan:
>
> - Nonaktifkan BPA sepenuhnya, atau
> - Gunakan peng VPC-level ecualian

Langkah 1: Buat VPC

Selesaikan langkah ini untuk membuat VPC yang akan meng-host instance target dan gateway internet Anda.

> **Note**
>
> Pastikan Anda belum mencapai batas kuota VPC Anda. Untuk informasi selengkapnya, lihat Kuota Amazon VPC.

AWS konsol

1. Buka konsol https://console.aws.amazon.com/vpc Amazon VPC.
2. Pada dasbor VPC, pilih Buat V PC.
3. Untuk Sumber Daya yang akan dibuat, pilih VPC saja.
4. Untuk Tag nama, masukkan nama untuk VPC Anda (misalnya,**IGW-Ingress-VPC**).
5. Untuk blok IPv4 CIDR, masukkan blok CIDR (misalnya,). **10.0.0.0/16**
6. Pilih Buat VPC.

AWS CLI

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --tag-specifications
 'ResourceType=vpc,Tags=[{Key=Name,Value=IGW-Ingress-VPC}]' --region us-east-1
```

Langkah 2: Buat dan lampirkan gateway internet

Selesaikan langkah ini untuk membuat gateway internet dan melampirkannya ke VPC Anda untuk mengaktifkan konektivitas internet.

AWS konsol

1. Buka konsol https://console.aws.amazon.com/vpc Amazon VPC.
2. Di konsol VPC, pilih gateway Internet.
3. Pilih Buat gateway internet.
4. Untuk Tag nama, masukkan nama untuk gateway internet Anda (misalnya,**IGW-Ingress-Gateway**).
5. Pilih Buat gateway internet.
6. Pilih gateway internet Anda dan pilih Tind akan, Lamp irkan ke VPC.
7. Pilih VPC Anda dan pilih Lamp irkan gateway internet.

AWS CLI

```
aws ec2 create-internet-gateway --tag-specifications 'ResourceType=internet-
gateway,Tags=[{Key=Name,Value=IGW-Ingress-Gateway}]' --region us-east-1

aws ec2 attach-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --vpc-id
 vpc-0123456789abcdef0 --region us-east-1
```

Catatan: Ganti ID sumber daya dengan ID aktual Anda dari langkah sebelumnya.

Langkah 3: Buat subnet untuk instance target Anda

Selesaikan langkah ini untuk membuat subnet tempat instance target Anda akan digunakan.

AWS konsol

1. Di panel navigasi konsol VPC, pilih Su bnets.
2. Pilih Buat subnet.
3. Di bawah ID VPC, pilih VPC Anda.
4. Untuk nama Subnet, masukkan nama (misalnya,**`Target-Subnet`**).
5. Untuk Zona Keter sediaan, Anda dapat memilih Zona untuk subnet Anda, atau meninggalkan default Tanpa Preferensi untuk mengizinkan AWS memilih satu untuk Anda.
6. Untuk blok IPv4 CIDR, pilih Input manual dan masukkan blok CIDR (misalnya,). **`10.0.1.0/24`**
7. Pilih Buat subnet.

AWS CLI

```
aws ec2 create-subnet \
    --vpc-id vpc-0123456789abcdef0 \
    --cidr-block 10.0.1.0/24 \
    --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Target-Subnet}]' \
    --region us-east-1
```

Langkah 4: Buat tabel rute untuk subnet

Selesaikan langkah ini untuk membuat tabel rute untuk subnet Anda dan kaitkan dengan subnet.

AWS konsol

1. Di panel navigasi konsol VPC, pilih Tabel rute.
2. Pilih Buat tabel rute.
3. Untuk Nama, masukkan nama untuk tabel rute Anda (misalnya,**`Target-Subnet-Route-Table`**).
4. Untuk VPC, pilih VPC Anda.
5. Pilih Buat tabel rute.
6. Pilih tabel rute Anda dan pilih Tindakan , Edit asosiasi subnet.
7. Pilih subnet Anda dan pilih S impan asosiasi.

AWS CLI

```
aws ec2 create-route-table \
    --vpc-id vpc-0123456789abcdef0 \
    --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=Target-Subnet-
Route-Table}]' \
    --region us-east-1

aws ec2 associate-route-table \
    --route-table-id rtb-0987654321fedcba0 \
    --subnet-id subnet-0123456789abcdef0 \
    --region us-east-1
```

Langkah 5: Buat grup keamanan untuk instance target

Selesaikan langkah ini untuk membuat grup keamanan yang akan mengontrol akses jaringan ke instance target Anda.

AWS konsol

1. Di panel navigasi konsol VPC, pilih Grup Keamanan.
2. Pilih Buat grup keamanan.
3. Untuk nama grup keamanan, masukkan nama (misalnya,**`IGW-Target-SG`**).
4. Untuk Deskripsi, masukkan **`Security group for IGW ingress routing target instance`**.
5. Untuk VPC, pilih VPC Anda.
6. Untuk menambahkan aturan masuk, pilih aturan masuk. Untuk setiap aturan, pilih Tambahkan aturan dan tentukan yang berikut:

- Tipe: Semua ICMP - IPv4, Sumber: 0.0.0. 0/0 (untuk pengujian ping).
- Jenis: SSH, Port: 22, Sumber: 0.0.0. 0/0 (untuk Koneksi Instans EC2).

> **Note**
>
> Grup keamanan ini membuka port SSH untuk semua lalu lintas internet untuk tutorial ini. Tutorial ini untuk tujuan pendidikan dan tidak boleh dikonfigurasi untuk lingkungan produksi. Dalam produksi, batasi akses SSH ke rentang IP tertentu.

- Pilih Buat grup keamanan.

AWS CLI

```
aws ec2 create-security-group \
    --group-name IGW-Target-SG \
    --description "Security group for IGW ingress routing target instance" \
    --vpc-id vpc-0123456789abcdef0 \
    --region us-east-1

aws ec2 authorize-security-group-ingress \
    --group-id sg-0123456789abcdef0 \
    --protocol icmp \
    --port -1 \
    --cidr 0.0.0.0/0 \
    --region us-east-1

aws ec2 authorize-security-group-ingress \
    --group-id sg-0123456789abcdef0 \
    --protocol tcp \
    --port 22 \
    --cidr 0.0.0.0/0 \
    --region us-east-1
```

Langkah 6: Luncurkan instance EC2 target

Selesaikan langkah ini untuk meluncurkan instans EC2 yang akan menerima lalu lintas dari kumpulan BYOIP Anda.

AWS konsol

1. Buka konsol Amazon EC2.
2. Pilih Luncurkan instans.
3. Untuk Nama, masukkan nama untuk instance Anda (misalnya,**IGW-Target-Instance**).
4. Untuk Gambar Aplikasi dan OS (Gambar Mesin Amazon), pilih Amazon Linux 2023 AMI.
5. Untuk Jenis Instance, pilih t2.micro (memenuhi syarat untuk tingkat gratis).
6. Untuk Pasangan kunci (login), pilih pasangan kunci yang ada atau buat yang baru.
7. Untuk Peng aturan jaringan, pilih Edit dan konfigurasikan:
   - VPC: Pilih VPC Anda
   - Subnet: Pilih subnet Anda
   - Auto-assign IP publik: Aktifkan
   - Firewall (grup keamanan): Pilih grup keamanan yang ada dan pilih grup keamanan Anda
8. Pilih Luncurkan instans.
9. Penting: Setelah peluncuran, buka detail instance dan catat ID antarmuka Jaringan (dimulai dengan “eni-”) - Anda akan memerlukan ini untuk Langkah 10.

AWS CLI

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name your-key-pair \
    --security-group-ids sg-0123456789abcdef0 \
    --subnet-id subnet-0123456789abcdef0 \
    --associate-public-ip-address \
    --tag-specifications 'ResourceType=instance,Tags=[{Key=Name,Value=IGW-Target-
Instance}]' \
    --region us-east-1
```

Untuk menemukan ID ENI di konsol:

1. Di konsol EC2, pilih instans Anda.
2. Buka tab Jaringan.

3. Perhatikan ID antarmuka Jaringan (misalnya,`eni-0abcdef1234567890`).

Untuk menemukan ID ENI menggunakan AWS CLI:

```
aws ec2 describe-instances --instance-ids i-0123456789abcdef0 --query
 'Reservations[0].Instances[0].NetworkInterfaces[0].NetworkInterfaceId' --output text
 --region us-east-1
```

Langkah 7: Buat tabel rute gateway internet

Selesaikan langkah ini untuk membuat tabel rute khusus untuk gateway internet yang akan menangani routing masuk.

AWS konsol

1. Di konsol VPC, pilih Tabel rute.
2. Pilih Buat tabel rute.
3. Untuk Nama, masukkan nama untuk tabel rute Anda (misalnya,**`IGW-Ingress-Route-Table`**).
4. Untuk VPC, pilih VPC Anda.
5. Pilih Buat tabel rute.
6. Pilih tabel rute Anda dan pilih tab A sosiasi tepi.
7. Pilih Edit asosiasi tepi.
8. Pilih gateway internet Anda dan pilih S impan perubahan.

AWS CLI

```
aws ec2 create-route-table \
    --vpc-id vpc-0123456789abcdef0 \
    --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=IGW-Ingress-
Route-Table}]' \
    --region us-east-1
```

Langkah 8: Mengaitkan tabel rute dengan gateway internet

Selesaikan langkah ini untuk mengaitkan tabel rute Anda dengan gateway internet untuk mengaktifkan fungsionalitas routing masuk.

AWS konsol

1. Di panel navigasi konsol VPC, pilih Tabel rute, lalu pilih tabel rute yang Anda buat.
2. Dari tab A sosiasi tepi, pilih Edit asosiasi tepi.
3. Pilih kotak centang untuk gateway internet.
4. Pilih Simpan perubahan.

AWS CLI

```
aws ec2 associate-route-table \
    --route-table-id rtb-0123456789abcdef0 \
    --gateway-id igw-0123456789abcdef0 \
    --region us-east-1
```

Langkah 9: Asosiasikan kolam BYOIP Anda dengan gateway internet

Selesaikan langkah ini untuk mengaitkan kumpulan BYOIP Anda dengan tabel rute gateway internet, memungkinkan VPC menerima lalu lintas untuk rentang IP Anda.

AWS konsol

1. Di panel navigasi konsol VPC, pilih Tabel rute, dan pilih tabel rute gateway internet yang Anda buat.
2. Pilih tab asosiasi kumpulan IPv4.
3. Pilih tombol Edit asosiasi.
4. Pilih kumpulan BYOIP Anda (misalnya,`pool-12345678901234567`).
5. Pilih tombol S impan asosiasi.

AWS CLI

```
aws ec2 associate-route-table \
    --route-table-id rtb-0123456789abcdef0 \
    --public-ipv4-pool pool-12345678901234567 \
    --region us-east-1
```

Catatan: Ganti `rtb-0123456789abcdef0` dengan ID tabel rute gateway internet Anda dan `pool-12345678901234567` dengan ID kumpulan BYOIP Anda.

Langkah 10: Tambahkan rute statis untuk menargetkan instance Anda

Selesaikan langkah ini untuk menambahkan rute yang mengarahkan lalu lintas dari rentang BYOIP Anda ke antarmuka jaringan instance target Anda.

AWS konsol

1. Di panel navigasi konsol VPC, pilih Tabel rute, dan pilih tabel rute gateway internet yang Anda buat.
2. Pilih Tindakan, Sunting rute.
3. Pilih Tambahkan rute.
4. Untuk Tujuan, masukkan BYOIP CIDR Anda atau subset (misalnya,). **`203.0.113.0/24`** Awalan harus antara /23 dan /28.
5. Untuk Target, pilih Antar muka jaringan dan masukkan ID ENI instans Anda (misalnya,`eni-0abcdef1234567890`).
6. Pilih Simpan perubahan.

AWS CLI

```
aws ec2 create-route \
    --route-table-id rtb-0123456789abcdef0 \
    --destination-cidr-block 203.0.113.0/24 \
    --network-interface-id eni-0abcdef1234567890 \
    --region us-east-1
```

Langkah 11: Konfigurasikan instance target

Selesaikan langkah ini untuk mengonfigurasi instance target Anda agar menangani lalu lintas yang ditujukan untuk alamat BYOIP dengan benar.

Penting: Selesaikan langkah konfigurasi instance ini sebelum menguji konektivitas (Langkah 12). Instans harus dikonfigurasi untuk merespons alamat BYOIP agar routing masuk berfungsi dengan baik.

AWS konsol

1. Hubungkan ke instans target menggunakan EC2 Instance Connect:
   - Di konsol EC2, pilih instans Anda.

- Pilih T indakan > Hu bungkan.
- Pilih tab Koneksi Instans EC2.
- Pilih Hubungkan.

2. Tambahkan alamat IP BYOIP tertentu ke antarmuka instance Anda:

   Pertama, temukan nama antarmuka jaringan Anda:

   ```
   ip link show
   ```

   Kemudian tambahkan alamat IP (ganti `203.0.113.10` dengan IP dari rentang BYOIP Anda):

   ```
   sudo ip addr add 203.0.113.10/32 dev eth0
   ```

   Catatan: Ganti `203.0.113.10` dengan alamat IP apa pun dari rentang BYOIP Anda yang ingin Anda uji. Nama antarmuka mungkin`eth0`,`ens5`, atau serupa tergantung pada jenis instans Anda.

3. Di konsol EC2, nonaktifkan source/destination cek:

   - Pilih instans Anda.
   - Buka tab Jaringan, pilih antarmuka jaringan.
   - Pilih T indakan, Ubah source/dest cek, N onaktifkan.

AWS CLI

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-0abcdef1234567890 \
    --no-source-dest-check \
    --region us-east-1
```

Langkah 12: Konfigurasikan instance untuk penanganan lalu lintas

Selesaikan langkah ini untuk menambahkan alamat BYOIP ke instans Anda dan nonaktifkan source/destination pemeriksaan untuk mengaktifkan penanganan lalu lintas yang tepat.

AWS konsol

1. Hubungkan ke instans target menggunakan EC2 Instance Connect:

- Di konsol EC2, pilih instans Anda.
- Pilih T indakan > Hu bungkan.
- Pilih tab Koneksi Instans EC2.
- Pilih Hubungkan.

2. Tambahkan alamat IP BYOIP tertentu ke antarmuka instance Anda:

   Pertama, temukan nama antarmuka jaringan Anda:

   ```
   ip link show
   ```

   Kemudian tambahkan alamat IP (ganti `ens5` dengan nama antarmuka Anda yang sebenarnya):

   ```
   sudo ip addr add 203.0.113.10/32 dev ens5
   ```

   Catatan: Ganti `203.0.113.10` dengan alamat IP apa pun dari rentang BYOIP Anda yang ingin Anda uji. Nama antarmuka mungkin`eth0`,`ens5`, atau serupa tergantung pada jenis instans Anda.

3. Di konsol EC2, nonaktifkan source/destination cek:

   - Pilih instans Anda.
   - Buka tab Jaringan, pilih antarmuka jaringan.
   - Pilih T indakan, Ubah source/dest cek, N onaktifkan.

AWS CLI

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-0abcdef1234567890 \
    --no-source-dest-check \
    --region us-east-1
```

Langkah 13: Uji konektivitas

Selesaikan langkah ini untuk memverifikasi bahwa lalu lintas internet diarahkan dengan benar ke instance target Anda melalui alamat BYOIP.

1. Pada instance target Anda, pantau lalu lintas masuk menggunakan tcpdump:

```
sudo tcpdump -i any icmp
```

2. Dari terminal atau komputer lain, uji konektivitas ke alamat IP BYOIP Anda:

```
ping 203.0.113.10
```

3. Hasil yang diharapkan:

   - Ping harus berhasil dan menunjukkan tanggapan dari alamat IP BYOIP Anda.
   - tcpdump harus menampilkan paket masuk untuk alamat BYOIP, mirip dengan:

```
12:34:56.789012 IP 203.0.113.100 > 203.0.113.10: ICMP echo request, id 1234, seq
 1, length 64
12:34:56.789123 IP 203.0.113.10 > 203.0.113.100: ICMP echo reply, id 1234, seq 1,
 length 64
```

   - Lalu lintas akan tampak berasal dari alamat IP eksternal, membuktikan perutean masuk gateway internet mengirimkan lalu lintas internet ke instance Anda.

Pemecahan masalah

Gunakan bagian ini untuk menyelesaikan masalah umum yang mungkin Anda temui saat menyiapkan perutean masuk gateway internet.

Lalu lintas tidak mencapai instance

- Verifikasi tabel rute memiliki ID ENI yang benar sebagai target.
- Konfirmasikan kumpulan BYOIP dikaitkan dengan tabel rute gateway internet.
- Periksa source/destination apakah pemeriksaan dinonaktifkan pada instance.
- Pastikan grup keamanan mengizinkan jenis lalu lintas yang Anda uji.

Pembuatan rute gagal

- Pastikan kumpulan BYOIP terkait dengan benar dengan tabel rute.
- Konfirmasikan CIDR tujuan berada dalam jangkauan BYOIP Anda.
- Periksa apakah ENI target ada dan dilampirkan ke instance yang sedang berjalan.
- Pastikan awalan BYOIP Anda berada di antara /23 dan /28 (awalan di luar rentang ini tidak didukung).

Ping/connectivity gagal

- Verifikasi alamat IP ditambahkan ke antarmuka instance.
- Periksa grup keamanan mengizinkan ICMP (untuk ping) atau port yang relevan.
- Konfirmasikan instance dalam keadaan berjalan.
- Uji dari beberapa lokasi eksternal.

Opsi lanjutan: Integrasi server rute untuk perutean dinamis

Untuk lingkungan yang membutuhkan failover otomatis, fitur ini terintegrasi dengan VPC Route Server untuk:

- Perbarui rute secara dinamis selama kegagalan instance.
- Hilangkan intervensi manual untuk manajemen rute.
- Menyediakan ketersediaan tingkat perusahaan untuk beban kerja kritis.

Hal ini sangat penting untuk kasus penggunaan Telco dan IoT di mana ketersediaan tinggi sangat penting.

> **Note**
>
> Saat menggunakan Route Server dengan beberapa rekan BGP, ketahuilah bahwa maksimal 32 rekan BGP dapat mengiklankan awalan yang sama ke tabel rute yang sama menggunakan server rute.

Untuk lingkungan yang membutuhkan routing dinamis, failover otomatis, dan distribusi beban di beberapa instans, pertimbangkan untuk mengintegrasikan dengan AWS Route Server. Route Server memungkinkan perutean BGP-based dinamis alih-alih rute statis, menyediakan:

- Iklan rute dinamis dari instance melalui BGP.
- Failover otomatis antara beberapa instans target.
- Distribusi beban di beberapa titik akhir.
- Manajemen rute terpusat melalui protokol BGP.

Ini adalah kasus penggunaan penting untuk penerapan perusahaan di mana ketersediaan tinggi dan kemampuan routing dinamis diperlukan. Untuk petunjuk penyiapan Route Server terperinci, lihat dokumentasi AWS Route Server.

Bersihkan

Untuk menghindari biaya yang sedang berlangsung, hapus sumber daya yang Anda buat dalam tutorial ini:

Langkah 1: Hentikan instance EC2

Selesaikan langkah ini untuk menghentikan instans EC2 dan berhenti menimbulkan biaya untuk sumber daya komputasi.

AWS konsol

1. Buka konsol Amazon EC2.
2. Di panel navigasi konsol EC2, pilih Inst ans.
3. Pilih instance Anda dan pilih Status Instance, H entikan instance.
4. Pilih H entikan untuk mengonfirmasi.

AWS CLI

```
aws ec2 terminate-instances --instance-ids i-0123456789abcdef0 --region us-east-1
```

Langkah 2: Lepaskan gateway internet dari VPC

Selesaikan langkah ini untuk melepaskan dan menghapus gateway internet dari VPC Anda.

AWS konsol

1. Buka konsol https://console.aws.amazon.com/vpc Amazon VPC.
2. Di panel navigasi konsol VPC, pilih gateway Internet.
3. Pilih gateway internet Anda dan pilih Tind akan, L epaskan dari V PC.
4. Pilih Lepaskan gateway internet.
5. Setelah melepaskan, pilih Tindakan , H apus gateway internet.
6. Pilih Hapus gateway internet.

AWS CLI

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --vpc-id
 vpc-0123456789abcdef0 --region us-east-1

aws ec2 delete-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --region
 us-east-1
```

Langkah 3: Hapus VPC

Selesaikan langkah ini untuk menghapus VPC dan semua sumber daya terkait untuk menyelesaikan proses pembersihan.

AWS konsol

1. Di konsol VPC, pilih V PC Anda.
2. Pilih VPC Anda dan pilih Tindakan , H apus V PC.
3. Ketik **`delete`** untuk mengonfirmasi dan pilih Hapus.

AWS CLI

```
aws ec2 delete-vpc --vpc-id vpc-0123456789abcdef0 --region us-east-1
```

> **Note**
>
> Menghapus VPC juga akan menghapus subnet terkait, tabel rute, dan grup keamanan.

> **Note**
>
> Kumpulan BYOIP Anda tetap tersedia untuk digunakan di masa mendatang dan tidak dihapus sebagai bagian dari proses pembersihan ini.

Perutean dinamis di VPC Anda menggunakan VPC Route Server

Amazon VPC Route Server menyederhanakan routing untuk lalu lintas antara beban kerja yang digunakan dalam VPC dan gateway internetnya. Dengan fitur ini, VPC Route Server secara dinamis memperbarui tabel rute VPC dan gateway internet dengan rute IPv4 atau IPv6 pilihan Anda untuk

mencapai toleransi kesalahan routing untuk beban kerja tersebut. Ini memungkinkan Anda untuk mengubah rute lalu lintas secara otomatis dalam VPC, yang meningkatkan pengelolaan routing VPC dan interoperabilitas dengan beban kerja pihak ketiga.

Server rute mendukung jenis tabel rute berikut:

- Tabel rute VPC tidak terkait dengan subnet
- Tabel rute subnet
- Tabel rute gateway internet

Server rute tidak mendukung tabel rute yang terkait dengan gateway pribadi virtual. Untuk menyebarkan rute ke tabel rute gateway transit, gunakan Transit Gateway Connect.

Kuota

Untuk kuota yang terkait dengan Amazon VPC Route Server, lihat Kuota server rute.

Harga

Untuk informasi tentang biaya yang terkait dengan Amazon VPC Route Server, lihat tab Server R ute VPC di halaman harga Amazon VPC.

Daftar Isi

- Terminologi
- Cara kerja Amazon VPC Route Server
- Pencatatan rekan server rute
- Mulai tutorial

Terminologi

Istilah-istilah berikut digunakan dalam panduan ini:

- FIB: Basis Informasi Penerusan (FIB) berfungsi sebagai tabel penerusan untuk apa yang telah ditentukan oleh server rute sebagai rute jalur terbaik di RIB setelah mengevaluasi semua informasi dan kebijakan routing yang tersedia. Rute FIB yang diinstal pada tabel rute. FIB dihitung ulang setiap kali ada perubahan pada RIB.
- RIB: Routing Information Base (RIB) berfungsi sebagai database yang menyimpan semua informasi routing dan data topologi jaringan yang dikumpulkan oleh router atau sistem routing,

seperti rute yang dipelajari dari rekan BGP. RIB terus diperbarui saat informasi routing baru diterima atau rute yang ada berubah. Ini memastikan bahwa server rute selalu memiliki tampilan terbaru dari topologi jaringan dan dapat membuat keputusan routing yang optimal.

- Server rute: Komponen server rute memperbarui tabel rute VPC dan gateway internet Anda dengan rute IPv4 atau IPv6 di Basis Informasi Penerusan (FIB) Anda. Server rute mewakili FIB tunggal dan Routing Information Base (RIB).
- Asosiasi server rute: Asosiasi server rute adalah koneksi yang dibuat antara server rute dan VPC.
- Titik akhir server rute: Titik akhir server rute adalah komponen yang AWS dikelola di dalam subnet yang membantu koneksi BGP (Border Gateway Protocol) antara server rute Anda dan rekan BGP Anda.
- Peer server rute: Peer server rute adalah sesi antara titik akhir server rute dan perangkat yang digunakan AWS (seperti alat firewall atau fungsi keamanan jaringan lainnya yang berjalan pada instance EC2). Perangkat harus memenuhi persyaratan ini:
  - Memiliki antarmuka jaringan elastis di VPC
  - Mendukung BGP (Protokol Gerbang Perbatasan)
  - Dapat memulai sesi BGP
- Propagasi server rute: Ketika diaktifkan, propagasi server rute menginstal rute di FIB pada tabel rute yang telah Anda tentukan. Server rute mendukung propagasi rute IPv4 dan IPv6.

Cara kerja Amazon VPC Route Server

Bagian ini menjelaskan cara kerja Amazon VPC Route Server dan membantu Anda memahami cara mencapai toleransi kesalahan routing untuk beban kerja Anda yang berjalan di subnet.

Daftar Isi

- Gambaran umum
- Diagram

Gambaran umum

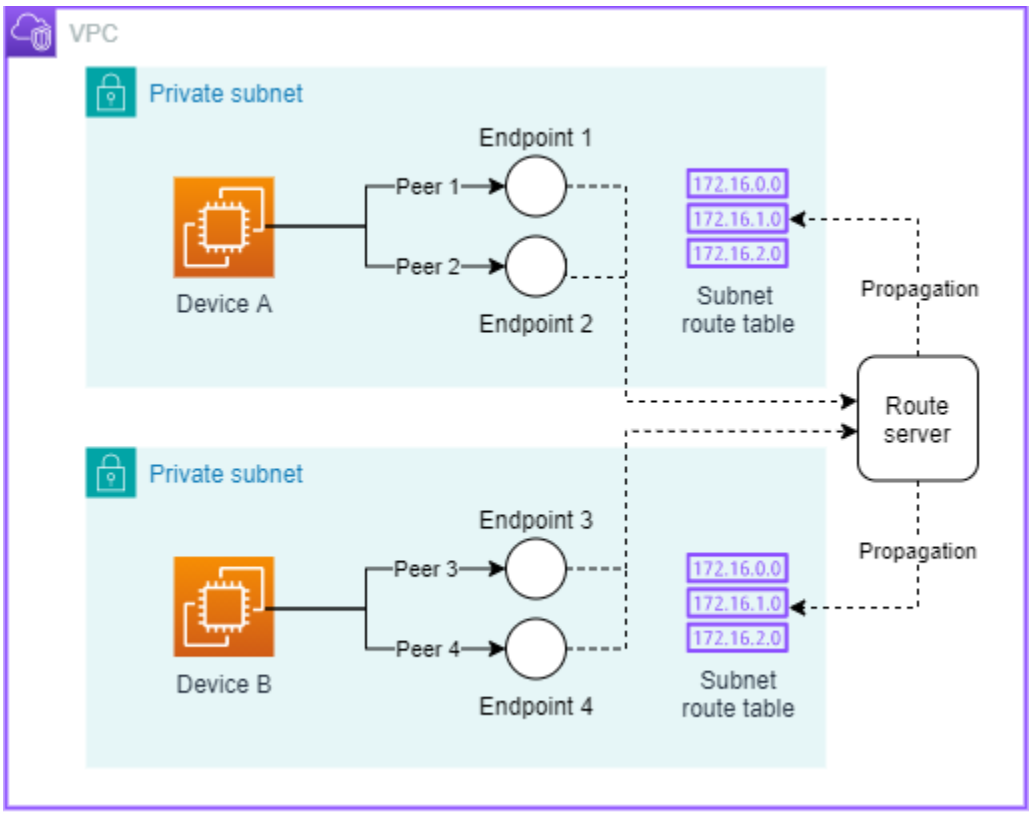
Cara kerja Amazon VPC Route Server:

1. Anda mengonfigurasi perangkat jaringan (seperti firewall yang berjalan pada instance EC2 di VPC) untuk menggunakan Amazon VPC Route Server.
2. Perangkat jaringan gagal.

3. Titik akhir server rute mendeteksi kegagalan melalui BFD (Bidirectional Forwarding Detection) yang dikonfigurasi pada peer server rute.
4. Titik akhir server rute memperbarui server rute untuk menarik rute di Routing Information Base (RIB) di mana perangkat yang gagal adalah lompatan berikutnya.
5. Server rute menghitung Forwar ding Information Base (FIB) dari RIB, memilih rute terbaik yang tersedia.
6. Server rute memperbarui tabel rute yang dikonfigurasi dengan rute dari FIB.
7. Semua lalu lintas baru diteruskan ke perangkat siaga.

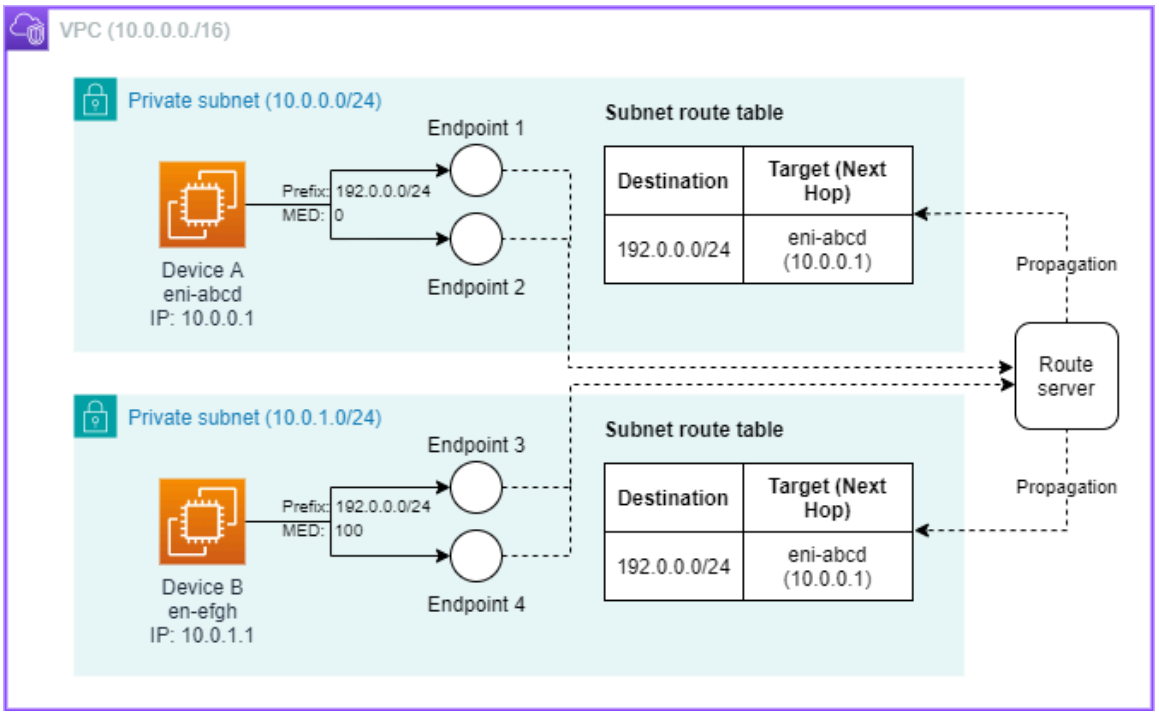
Diagram

Berikut ini adalah contoh diagram server rute VPC dengan titik akhir server rute yang dikonfigurasi untuk perangkat dalam dua subnet.

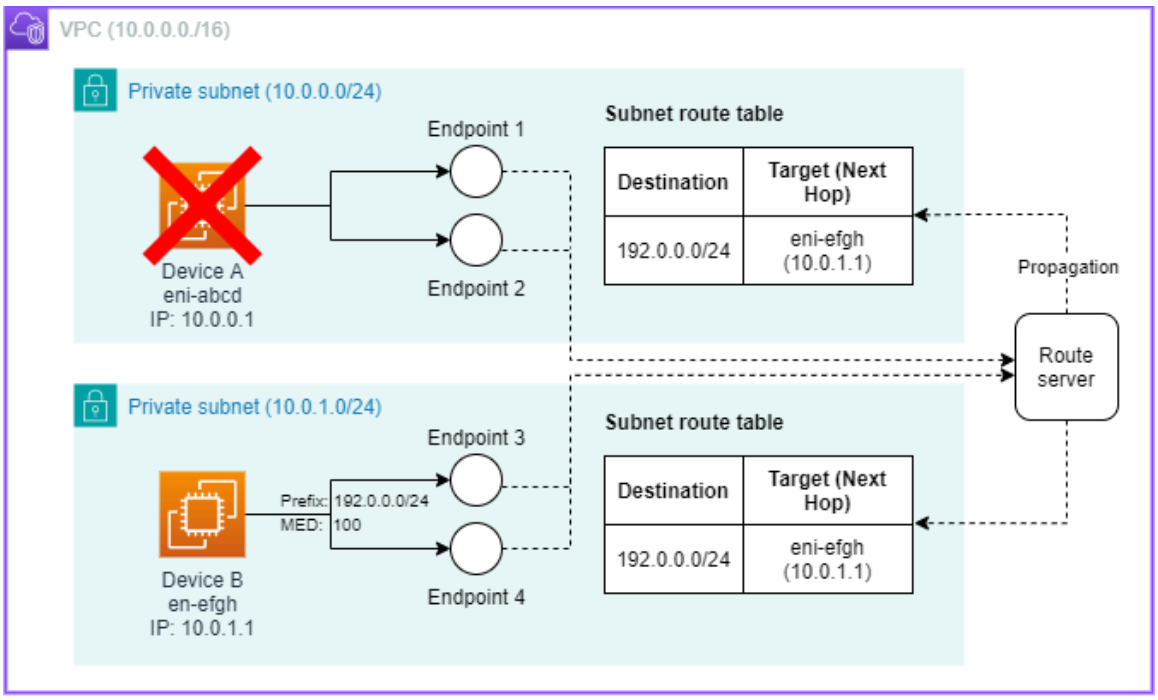


Dimulai dengan contoh di atas sebagai baseline, contoh di bawah ini menunjukkan desain yang lebih rinci, di mana Perangkat A dan Perangkat B beriklan melalui BGP bahwa mereka dapat menerima lalu lintas apa pun dengan IP tujuan dalam kisaran 192.0.0. 0/24 (dari 192.0.0.0 hingga 192.0.0.255). Atribut Multi-Exit MED (Discriminator) dari 0 memberi tahu server rute bahwa Perangkat A harus lebih disukai daripada Perangkat B. Server rute menerima rute dan atribut MED dari Perangkat A dan

menginstal rute tersebut di tabel rute subnet dengan antarmuka jaringan Perangkat A sebagai “hop berikutnya”. Akibatnya, setiap lalu lintas dalam subnet dengan IP tujuan di 192.0.0. 0/24 jangkauan dikirim ke Perangkat A. Perangkat A kemudian memproses lalu lintas dan mengirimkannya ke depan. Lalu lintas dalam salah satu subnet (10.0.0. 0/24 atau 10.0.1. 0/24) yang terikat untuk 192.0.0. 0/24 akan diarahkan ke Perangkat A eni-abcd (10.0.0.1) sebagai lompatan berikutnya.



Contoh terakhir di bawah ini menunjukkan bagaimana router server menangani failover. Sementara atribut MED yang lebih tinggi memberi tahu server rute bahwa Perangkat B kurang disukai daripada Perangkat A, jika Perangkat A eni-abcd (10.0.0.1) mati, server rute memperbarui tabel rute subnet, dan lalu lintas ke 192.0.0. 0/24 dialihkan ke Perangkat B eni-efgh (10.0.1.1) sebagai lompatan berikutnya.



Pencatatan rekan server rute

Gunakan pencatatan peer VPC Route Server saat Anda perlu:

- Pantau kesehatan sesi BGP dan BFD
- Memecahkan masalah koneksi
- Tinjau perubahan sesi historis
- Lacak status jaringan

Harga

- CloudWatch: Biaya penyerapan dan arsip data untuk log yang dijual berlaku saat Anda menerbitkan log peer server rute ke CloudWatch Log.
- S3: Biaya penyerapan dan arsip data untuk log yang dijual berlaku saat Anda menerbitkan log peer server rute ke Amazon S3.
- Data Firehose: Berlaku biaya konsumsi dan pengiriman standar.

Log yang dijual adalah log dari AWS layanan tertentu yang tersedia dengan harga berjenjang volume dan dikirimkan ke CloudWatch Logs, Amazon S3, atau Amazon Data Firehose. Untuk informasi selengkapnya, buka CloudWatch Harga Amazon, pilih Log dan temukan Log Dijual.

Contoh format log

```
{
    "resource_arn": "arn:aws:ec2:us-east-1:111122223333:route-server-peer/
rsp-1234567890abcdef0",
    "event_timestamp": 1746643505367,
    "type": "RouteStatus",
    "status": "ADVERTISED",
    "message": {
        "prefix": "10.24.34.0/32",
        "asPath": "65000",
        "med": 100,
        "nextHopIp": "10.24.34.1"
    }
}

{
    "resource_arn": "arn:aws:ec2:us-east-1:111122223333:route-server-peer/
rsp-1234567890abcdef0",
    "event_timestamp": 1746643490000,
    "type": "BGPStatus",
    "status": "UP",
    "message": null
}
```

Di mana:

- Ini `resource_arn` adalah ARN untuk peer server rute.
- Ini `event_timestamp` adalah stempel waktu acara.
- Per `type` istiwa log yang kami hasilkan (`RouteStatus`,`BGPStatus`,`BFDStatus`).
- `status`Bidang ini adalah pembaruan status.
  - Untuk `RouteStatus` jenis pesan
    - `ADVERTISED`(rute diiklankan oleh rekan)
    - `UPDATED`(rute yang ada diperbarui oleh rekan)
    - `WITHDRAWN`(rute ditarik oleh rekan)
  - Untuk `BFDStatus` dan `BGPStatus` pembaruan
    - `UP`, `DOWN`.

- Bid `message` ang saat ini hanya digunakan untuk atribut rute untuk jenis RouteStatus pesan tetapi dapat diisi dengan informasi yang relevan untuk jenis apa pun.

AWS Management Console

Untuk membuat log peer server rute:

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah Virtual private cloud, pilih Server rute.
3. Pada halaman Server rute, pilih Rute server peer.
4. Pilih tab Pengiriman log.
5. Pilih Tambahkan pengiriman log.
6. Pilih tujuan dan konfigurasikan pengaturan:
   - CloudWatch Log Amazon
     - Jenis log: Jenis log yang akan dikirimkan. Satu-satunya jenis log yang didukung adalah EVENT_LOGS.
     - Grup log tujuan: Grup CloudWatch log tempat log akan dikirim. Anda dapat memilih grup log yang ada atau membuat yang baru (contoh: aws/vpc /route-server-peer).
     - Pilihan bidang: Bidang data untuk disertakan dalam log Anda.
     - Format keluaran: Bagaimana log diformat:
       - JSON: Format terstruktur untuk pemrosesan komputer
       - Teks: Format teks biasa
     - Pembatas bidang: Saat menggunakan format teks, ini adalah karakter yang memisahkan bidang (contoh: koma, tab, spasi).
   - Amazon S3
     - Akun silang - Mengirim log ke AWS akun yang berbeda
       - Jenis log: Jenis log yang akan dikirimkan. Satu-satunya jenis log yang didukung adalah EVENT_LOGS.
       - Tujuan pengiriman ARN: Nama Sumber Daya Amazon dari bucket S3 di AWS akun lain tempat log akan dikirim.
       - Pilihan bidang: Bidang data untuk disertakan dalam log Anda.
       - Sufiks: Akhiran ditambahkan ke nama file log (contoh: .log, .txt)

        - Hive-compatible: Saat dihidupkan, atur log dalam struktur folder yang berfungsi dengan Hive-based alat agar pencarian lebih mudah dengan layanan seperti Amazon Athena.
        - Pembatas bidang: Saat menggunakan format teks, ini adalah karakter yang memisahkan bidang.
    - Dalam rekening giro
        - Jenis log: Jenis log yang akan dikirimkan. Satu-satunya jenis log yang didukung adalah EVENT_LOGS.
        - Bucket S3 Tujuan: Bucket S3 di akun Anda tempat log akan dikirim. Anda dapat menentukan jalur subfolder.
        - Pilihan bidang: Bidang data untuk disertakan dalam log Anda.
        - Sufiks: Akhiran ditambahkan ke nama file log (contoh: .log, .txt).
        - Hive-compatible: Saat dihidupkan, mengatur log dalam struktur folder yang berfungsi dengan Hive-based alat untuk pencarian yang lebih mudah.
        - Pembatas bidang: Saat menggunakan format teks, ini adalah karakter yang memisahkan bidang.
- Amazon Data Firehose
    - Akun silang
        - Jenis log: Jenis log yang akan dikirimkan. Satu-satunya jenis log yang didukung adalah EVENT_LOGS.
        - Tujuan pengiriman ARN: Nama Sumber Daya Amazon dari aliran pengiriman Firehose di AWS akun lain.
        - Pilihan bidang: Bidang data untuk disertakan dalam log Anda.
        - Pembatas bidang: Saat menggunakan format teks, ini adalah karakter yang memisahkan bidang.
    - Dalam rekening giro
        - Jenis log: Jenis log yang akan dikirimkan. Satu-satunya jenis log yang didukung adalah EVENT_LOGS.
        - Aliran tujuan pengiriman: Aliran pengiriman Firehose di akun Anda tempat log akan dikirim. Streaming harus menggunakan jenis sumber “Direct Put”.
        - Pilihan bidang: Bidang data untuk disertakan dalam log Anda.
        - Format keluaran: Bagaimana log diformat:

- JSON: Format terstruktur untuk pemrosesan komputer
- Teks: Format teks biasa

- Pembatas bidang: Saat menggunakan format teks, ini adalah karakter yang memisahkan bidang.

Command line

Perintah di bagian ini terhubung ke Referensi AWS CLI Perintah. Dokumentasi memberikan deskripsi rinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

Untuk membuat log peer server rute:

1. Gunakan perintah put-delivery-source.

   - Contoh permintaan

   ```
   aws logs put-delivery-source --name "source-rsp-1234567890abcdef0" --
   resource-arn "arn:aws:ec2:us-east-1:111122223333:route-server-peer/
   rsp-1234567890abcdef0" --log-type "EVENT_LOGS"
   ```

   - Contoh tanggapan

   ```
   {
        "deliverySource": {
           "name": "source-rsp-1234567890abcdef0",
           "arn": "arn:aws:logs:us-east-1:111122223333:delivery-source:source-
   rsp-1234567890abcdef0",
           "resourceArns": [
               "arn:aws:ec2:us-east-1:111122223333:route-server-peer/
   rsp-1234567890abcdef0"
           ],
           "service": "ec2",
           "logType": "EVENT_LOGS"
       }
   }
   ```

2. Gunakan perintah put-delivery-destination.

   - Contoh AWS CLI berikut membuat log server rute. Log dikirim ke grup log yang ditentukan.
   - Contoh permintaan

```
aws logs put-delivery-destination --name "destination-rsp-abcdef01234567890"
 --destination-resource-arn "arn:aws:logs:us-east-1:111122223333:log-group:/
aws/vendedlogs/ec2/route-server-peer/EVENT_LOGS/rsp-abcdef01234567890"
```

- Contoh tanggapan

```
{
     "deliveryDestination": {
        "name": "destination-rsp-abcdef01234567890",
        "arn": "arn:aws:logs:us-east-1:111122223333:delivery-
destination:destination-rsp-abcdef01234567890",
        "deliveryDestinationType": "CWL",
        "deliveryDestinationConfiguration": {
            "destinationResourceArn": "arn:aws:logs:us-
east-1:111122223333:log-group:/aws/vendedlogs/ec2/route-server-peer/
EVENT_LOGS/rsp-abcdef01234567890"
        }
    }
}
```

3. Gunakan perintah create-delivery.

- Contoh permintaan

```
aws logs create-delivery --delivery-source-name "source-rsp-1234567890abcdef0"
 --delivery-destination-arn "arn:aws:logs:us-east-1:111122223333:delivery-
destination:destination-rsp-abcdef01234567890"
```

- Contoh tanggapan

```
{
     "delivery": {
        "id": "1234567890abcdef0",
        "arn": "arn:aws:logs:us-
east-1:111122223333:delivery:1234567890abcdef0",
        "deliverySourceName": "source-rsp-1234567890abcdef0",
        "deliveryDestinationArn": "arn:aws:logs:us-
east-1:111122223333:delivery-destination:destination-rsp-abcdef01234567890",
        "deliveryDestinationType": "CWL",
        "recordFields": [
            "resource_arn",
            "event_timestamp",
```

```
            "type",
            "status",
            "message"
        ]
    }
}
```

Mulai tutorial

Tutorial ini memandu Anda melalui proses pengaturan dan konfigurasi VPC Route Server untuk mengaktifkan routing dinamis di VPC Anda. Anda akan belajar cara membuat dan mengkonfigurasi semua komponen yang diperlukan, membuat peering BGP, dan memverifikasi operasi yang tepat. Tutorial ini mencakup semuanya mulai dari pengaturan IAM awal hingga pengujian dan pembersihan.

Sebelum memulai tutorial ini, pastikan Anda memiliki:

- Akses administratif ke AWS akun Anda
- VPC dengan setidaknya dua subnet tempat Anda ingin mengaktifkan perutean dinamis
- Perangkat jaringan (seperti firewall yang berjalan pada instans EC2) yang mendukung BGP dan dapat berfungsi sebagai perangkat peer server rute
- Keakraban dasar dengan konsep BGP dan jaringan AWS

Langkah-langkah dapat diselesaikan menggunakan Konsol AWS Manajemen atau AWS CLI. Kedua metode disediakan untuk setiap langkah.

Perkiraan waktu untuk menyelesaikan: 15-30 menit

Langkah-langkah

- Langkah 1: Konfigurasikan izin peran IAM yang diperlukan
- Langkah 2: Buat server rute
- Langkah 3: Mengaitkan server rute dengan VPC
- Langkah 4: Buat titik akhir server rute
- Langkah 5: Aktifkan propagasi server rute
- Langkah 6: Buat peer server rute
- Langkah 7: Memulai sesi BGP dari perangkat

- Langkah 8: Pembersihan

Langkah 1: Konfigurasikan izin peran IAM yang diperlukan

Untuk menggunakan VPC Route Server, pastikan bahwa pengguna atau peran IAM yang Anda gunakan memiliki izin IAM yang diperlukan. Di bawah ini adalah panduan untuk izin mana yang diperlukan untuk setiap API:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CreateRouteServer",
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteRouteServer",
            "Effect": "Allow",
            "Action": [
                "sns:DeleteTopic"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateRouteServerEndpoint",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": "*"
```

```
        },
        {
            "Sid": "DeleteRouteServerEndpoint",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateRouteServerPeer",
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteRouteServerPeer",
            "Effect": "Allow",
            "Action": [
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Resource": "*"
        }
    ]
}
```

Langkah 2: Buat server rute

Selesaikan langkah-langkah di bagian ini untuk membuat server rute.

Komponen server rute memperbarui tabel rute VPC dan gateway internet Anda dengan rute IPv4 atau IPv6 di Basis Informasi Penerusan (FIB) Anda. Server rute mewakili FIB tunggal dan Routing Information Base (RIB).

AWS Management Console

Untuk membuat server rute

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah Virtual private cloud, pilih Server rute.
3. Pada halaman Server rute, pilih Buat server rute.
4. Pada halaman Buat server rute, konfigurasikan pengaturan berikut:
   - Untuk Nama, masukkan nama untuk server rute Anda (mis., “my-route-server-01"). Nama harus 255 karakter atau kurang panjangnya.
   - Untuk ASN Sisi Amazon, masukkan nilai ASN BGP. Nilai ini harus berada di kisaran 1-4294967295. Sebaiknya gunakan ASN pribadi dalam kisaran 64512—65534 (16-bit ASN) atau 4200000000—4294967294 (ASN 32-bit).
   - Untuk rute Pertahankan, pilih Aktifkan atau N onaktifkan. Opsi ini menentukan apakah rute harus dipertahankan setelah semua sesi BGP dihentikan:
     - Jika diaktifkan: Rute akan dipertahankan dalam database routing server rute meskipun semua sesi BGP berakhir
     - Jika dinonaktifkan: Rute akan dihapus dari database routing saat semua sesi BGP berakhir
   - Jika Anda mengaktifkan rute bertahan, untuk Durasi Per sist, masukkan nilai antara 1-5 menit. Durasi ini menentukan berapa lama server rute akan menunggu setelah BGP dibangun kembali untuk menghentikan rute. Misalnya, jika Anda menyetelnya ke 1 menit, perangkat Anda memiliki waktu 1 menit setelah membangun kembali BGP untuk mempelajari kembali dan mengiklankan rute sebelum server rute melanjutkan fungsi normal. Meskipun 1 menit biasanya cukup, Anda dapat mengatur hingga 5 menit jika jaringan BGP Anda membutuhkan lebih banyak waktu untuk sepenuhnya membangun kembali dan mempelajari kembali semua rute.
   - (Opsional) Untuk mengaktifkan notifikasi SNS untuk perubahan status BGP, aktifkan sakelar Aktifkan notifikasi SNS. Mengaktifkan notifikasi SNS mempertahankan perubahan status sesi BGP atau BFD pada rekan server rute dan pemberitahuan pemeliharaan untuk titik akhir server rute ke topik SNS yang disediakan oleh. AWS Untuk detail tentang notifikasi ini, lihat tabel detail notifikasi SNS di bawah ini.

5. (Opsional) Untuk menambahkan tag ke server rute Anda, gulir ke bawah ke bagian Tag - opsional dan pilih Tambahkan tag baru. Masukkan kunci dan nilai opsional untuk setiap tag. Anda dapat menambahkan hingga 50 tag.
6. Tinjau pengaturan Anda dan pilih Buat server rute.
7. Tunggu server rute dibuat. Setelah selesai, Anda akan diarahkan ke halaman server Rute, di mana Anda dapat melihat server rute baru Anda terdaftar dengan status Ter sedia.

Command line

Gunakan prosedur berikut untuk membuat server rute baru untuk mengelola perutean dinamis di VPC.

Untuk`--amazon-side-asn`, masukkan nilai ASN BGP. Nilai ini harus berada di kisaran 1-4294967295. Sebaiknya gunakan ASN pribadi dalam kisaran 64512—65534 (16-bit ASN) atau 4200000000—4294967294 (ASN 32-bit).

1. Perintah:

```
aws ec2 create-route-server --amazon-side-asn 65000
```

Respons:

```
{
    "RouteServer": {
        "RouteServerId": "rs-1",
        "AmazonSideAsn": 65000,
        "State": "pending"
    }
}
```

2. Tunggu server rute tersedia.

Perintah:

```
aws ec2 describe-route-servers
```

Respons:

```
{
```

```
    "RouteServer": {
        "RouteServerId": "rs-1",
        "AmazonSideAsn": 65000,
        "State": "available"
    }
}
```

Rincian notifikasi SNS

Tabel berikut menunjukkan detail tentang pesan yang akan dikirim Amazon VPC Route Server menggunakan Amazon SNS:

Bidang standar		Atribut pesan (Metadata)			
Pesan	Ketika dikirim	stempel waktu	Kode acara	rute ServerEndpointId	terpengaruh RouteServerPeerIds
Route Server Endpoint [ENDPOINT ID] sekarang sedang menjalani pemeliharaan. Sesi BFD dan BGP dapat terpengaruh.	Pemeliharaan titik akhir server rute	Format: 2025-02-17T15:55:00Z	ROUTE_SERVER_ENDPOINT_MAINTENANCE	ID titik akhir yang terpengaruh	Daftar ID rekan yang terpengaruh
Pesan	Ketika dikirim	stempel waktu	Kode acara	rute ServerPeerId	baru BgpStatus
BGP untuk Route Server Peer [PEER	Perubahan status BGP peer server rute	Format: 2025-02-17T15:55:00Z	ROUTE_SERVER_PEER_BGP_STATUS_CHANGE	ID rekan yang terpengaruh	NAIK atau BAWAH

Bidang standar		Atribut pesan (Metadata)			
ID] sekarang [UP/DOWN].					
Pesan	Ketika dikirim	stempel waktu	Kode acara	rute ServerPeerId	baru BfdStatus
BFD untuk Route Server Peer [PEER ID] sekarang [UP/DOWN].	Perubahan status BFD peer server rute	Format: 2025-02-17 T15:55:00Z	ROUTE_SERVER_PEER_BFD_STATUS_CHANGE	ID rekan yang terpengaruh	NAIK atau BAWAH

Langkah 3: Mengaitkan server rute dengan VPC

Selesaikan langkah-langkah di bagian ini untuk mengaitkan server rute dengan VPC.

Asosiasi server rute adalah koneksi yang dibuat antara server rute dan VPC. Ini adalah langkah konfigurasi mendasar yang memungkinkan server rute bekerja dengan peralatan di VPC Anda.

Saat Anda membuat asosiasi server rute:

- Ini menghubungkan server rute ke VPC tertentu.
- Ini memungkinkan server rute untuk berinteraksi dengan tabel rute dalam subnet VPC.
- Hal ini memungkinkan server rute untuk menerima dan menyebarkan rute dalam VPC terkait.
- Ini menetapkan ruang lingkup di mana server rute dapat beroperasi.

Aspek kunci dari asosiasi server rute:

- Setiap server rute dapat dikaitkan dengan satu VPC. Setiap VPC dapat memiliki hingga 5 asosiasi server rute terpisah secara default. Untuk informasi selengkapnya tentang kuota, lihat Kuota server rute.
- Asosiasi harus dibuat sebelum server rute dapat mengelola rute.
- Asosiasi dapat dipantau untuk melacak statusnya (seperti mengasosiasikan dan terkait).
- Asosiasi dapat dihapus (dipisahkan) jika Anda tidak lagi ingin server rute beroperasi di VPC itu.

AWS Management Console

Mengaitkan server rute dengan VPC

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah Virtual private cloud, pilih Server rute.
3. Pilih server rute yang ingin Anda kaitkan dengan VPC.
4. Pada tab A sosiasi, pilih Associate route server.
5. Dalam kotak dialog Associate route server:
   - Bidang ID server rute secara otomatis diisi dengan server rute yang Anda pilih
   - Untuk ID VPC, pilih VPC yang ingin Anda kaitkan dari daftar dropdown
6. Pilih Server rute Asosiasi.
7. Tunggu asosiasi selesai. Setelah selesai, Negara akan ditampilkan sebagai Ter kait pada tab A sosiasi.

Command line

Gunakan prosedur berikut untuk mengaitkan server rute dengan VPC.

1. Perintah:

```
aws ec2 associate-route-server --route-server-id rs-1 --vpc-id vpc-1
```

Respons:

```
{
    "RouteServerAssociation": {
        "RouteServerId": "rs-1",
        "VpcId": "vpc-1",
        "State": "associating"
    }
}
```

2. Tunggu asosiasi selesai.

Perintah:

```
aws ec2 get-route-server-associations --route-server-id rs-1
```

Respons:

```
{
    "RouteServerAssociation": {
        "RouteServerId": "rs-1",
        "VpcId": "vpc-1",
        "State": "associated"
    }
}
```

Langkah 4: Buat titik akhir server rute

Selesaikan langkah-langkah di bagian ini untuk membuat titik akhir server rute. Buat dua titik akhir per subnet untuk redundansi.

Titik akhir server rute adalah komponen yang AWS dikelola di dalam subnet yang membantu koneksi BGP (Border Gateway Protocol) antara server rute Anda dan rekan BGP Anda.

Titik akhir server rute adalah “titik kontak” di mana perangkat jaringan Anda membuat sesi BGP dengan server rute. Mereka adalah komponen yang benar-benar menangani koneksi BGP, sementara server rute itu sendiri mengelola keputusan routing dan propagasi rute.

> **Note**
>
> Titik akhir server rute dikenakan biaya $0,75 per jam.

AWS Management Console

Untuk membuat titik akhir server rute

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, di bawah Virtual private cloud, pilih Server rute.
3. Pilih server rute yang ingin Anda buat titik akhir.
4. Di panel bawah, pilih tab titik akhir server rute.
5. Pilih Buat titik akhir server rute.

6. Pada halaman Buat titik akhir server rute, konfigurasikan pengaturan berikut:
   - Untuk Nama, masukkan nama deskriptif untuk titik akhir Anda.
   - Untuk server rute, konfirmasikan bahwa server rute yang benar dipilih.
   - Untuk Subnet, pilih subnet tempat Anda ingin membuat titik akhir.
7. (Opsional) Untuk menambahkan tag ke titik akhir server rute Anda, gulir ke bawah ke bagian Tag - opsional dan pilih Tambahkan tag baru. Masukkan kunci dan nilai opsional untuk setiap tag.
8. Tinjau pengaturan Anda dan pilih Buat titik akhir server rute.
9. Tunggu titik akhir dibuat. Setelah selesai, Anda akan melihat pesan sukses.
10. Ulangi langkah 5-9 untuk membuat titik akhir kedua di subnet yang sama, menggunakan nama yang berbeda.
11. Ulangi langkah 5-10 untuk setiap subnet di mana Anda memerlukan titik akhir server rute.
12. Setelah membuat titik akhir, kembali ke tab titik akhir server rute untuk server rute Anda.
13. Pastikan Anda melihat dua titik akhir terdaftar untuk setiap subnet.
14. Periksa apakah Status untuk setiap titik akhir tersedia.

Command line

Gunakan prosedur berikut untuk membuat titik akhir server rute.

1. Perintah:

```
aws ec2 create-route-server-endpoint --route-server-id rs-1 --subnet-id subnet-1
```

Respons:

```
{
    "RouteServerEndpoint": {
        "RouteServerId": "rs-1",
        "RouteServerEndpointId": "rse-1",
        "VpcId": "vpc-1",
        "SubnetId": "subnet-1",
        "State": "pending"
    }
}
```

2. Anda mungkin perlu menunggu beberapa menit agar titik akhir tersedia sepenuhnya setelah pembuatan.

   Perintah:

   ```
   aws ec2 describe-route-server-endpoints
   ```

   Respons:

   ```
   {
       "RouteServerEndpoint": {
           "RouteServerId": "rs-1",
           "RouteServerEndpointId": "rse-1",
           "VpcId": "vpc-1",
           "SubnetId": "subnet-1",
           "EniId": "eni-123",
           "EniAddress": "10.1.2.3",
           "State": "available"
       }
   }
   ```

   Ulangi langkah-langkah untuk membuat titik akhir kedua di subnet yang sama menggunakan nama yang berbeda dan buat titik akhir untuk setiap subnet di mana Anda memerlukan titik akhir server rute.

Langkah 5: Aktifkan propagasi server rute

Selesaikan langkah ini untuk mengaktifkan propagasi server rute.

Saat diaktifkan, propagasi server rute menginstal rute di FIB pada tabel rute yang telah Anda tentukan. Server rute mendukung propagasi rute IPv4 dan IPv6.

Propagasi server rute adalah mekanisme yang mengotomatiskan pembaruan tabel rute - alih-alih memperbarui tabel rute secara manual, server rute secara otomatis menyebarkan rute yang sesuai ke tabel rute yang dikonfigurasi dengan rute dari FIB.

Aspek utama propagasi server rute:

- Konfigurasi
  - Menautkan server rute ke tabel rute tertentu

  - Menentukan tabel rute mana yang akan menerima pembaruan rute dinamis
  - Dapat diaktifkan atau dinonaktifkan per tabel rute
- Fungsionalitas
  - Secara otomatis memperbarui tabel rute dengan rute yang dipelajari dari rekan BGP
  - Menyebarkan rute terbaik yang tersedia berdasarkan atribut BGP
  - Mempertahankan konsistensi rute di seluruh tabel rute yang ditentukan
  - Memperbarui rute secara dinamis saat kondisi jaringan berubah
- Status
  - Dapat diaktifkan (rute sedang disebarkan)
  - Dapat dinonaktifkan (rute tidak disebarkan)

AWS Management Console

Untuk mengaktifkan propagasi server rute

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pilih server rute yang ingin Anda aktifkan propagasi.
3. Pilih tab Propagations di panel detail server rute.
4. Pilih Aktifkan propagasi.
5. Dalam dialog Aktifkan propagasi:
   - ID server Route akan diisi sebelumnya.
   - Di bawah Tabel rute, pilih tabel rute tujuan dari menu dropdown untuk rute yang baru disebarkan.
6. Pilih Aktifkan propag asi untuk mengonfirmasi.
7. Tunggu status propagasi berubah menjadi Tersedia dalam daftar Pro pagasi.
8. Verifikasi bahwa tabel rute yang dipilih muncul dalam daftar Propagasi dengan status Tersedia.

Command line

Gunakan prosedur berikut untuk mengaktifkan propagasi server rute.

1. Perintah:

```
aws ec2 enable-route-server-propagation --route-table-id rtb-1 --route-server-id
 rs-1
```

Respons:

```
{
    "RouteServerRoutePropagation": {
        "RouteServerId": "rs-1",
        "RouteTableId": "rtb-1",
        "State": "pending"
    }
}
```

2. Tunggu status propagasi berubah menjadi tersedia.

   Perintah:

```
aws ec2 get-route-server-propagations --route-server-id rs-1
```

   Respons:

```
{
    "RouteServerRoutePropagation": {
        "RouteServerId": "rs-1",
        "RouteTableId": "rtb-1",
        "State": "available"
    }
}
```

Langkah 6: Buat peer server rute

Peer server rute adalah sesi antara titik akhir server rute dan perangkat yang digunakan AWS (seperti alat firewall atau fungsi keamanan jaringan lainnya yang berjalan pada instance EC2). Perangkat harus memenuhi persyaratan ini:

- Memiliki antarmuka jaringan elastis di VPC
- Mendukung BGP (Protokol Gerbang Perbatasan)
- Dapat memulai sesi BGP

> **Note**
>
> Sebaiknya buat satu peer server rute per titik akhir server rute untuk redundansi.

AWS Management Console

Untuk membuat peer server rute

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di jalur navigasi, pilih VPC > Rute server peer > Buat peer server rute.
3. Di bawah Detail, konfigurasikan yang berikut ini:
   - Nama: Masukkan nama untuk peer server rute Anda (hingga 255 karakter). Contoh: my-route-server-peer-01
   - ID titik akhir server rute: Pilih titik akhir server rute dari dropdown. Secara opsional, pilih Buat titik akhir server rute untuk membuat yang baru.
   - Alamat peer: Masukkan alamat IPv4 dari rekan. Harus alamat IP yang valid. Alamat peer harus dapat dijangkau dari titik akhir server rute.
   - Peer ASN: Masukkan ASN (Autonomous System Number) untuk rekan BGP. Nilai harus dalam kisaran 1-4294967295. ASN biasanya harus menggunakan rentang pribadi (64512-65534 untuk 16-bit atau 4200000000-4294967294 untuk 32-bit)
   - Det eksi keaktifan teman sebaya:
     - BGP keepalive (default): Mekanisme tetap hidup BGP standar
     - BFD: Deteksi Penerusan Dua Arah untuk failover yang lebih cepat
   - (Opsional) Di bawah Tag, pilih Tambahkan tag baru untuk menambahkan tag pasangan kunci-nilai. Tag membantu mengidentifikasi dan melacak AWS sumber daya.
4. Tinjau pengaturan Anda dan pilih Buat peer server rute.

Command line

Gunakan prosedur berikut untuk membuat peer server rute.

1. Perintah:

```
aws ec2 create-route-server-peer --route-server-endpoint-id rse-1 --peer-address
 10.0.2.3 --bgp-options PeerAsn=65001,PeerLivenessDetection=bfd
```

Respons:

Dalam tanggapannya, nilai-nilai negara bisa`pending`|`available`|`deleting`|`deleted`.

```
{
    "RouteServerPeer": {
        "RouteServerPeerId": "rsp-1",
        "RouteServerId": "rs-1",
        "VpcId": "vpc-1",
        "SubnetId": "subnet-1",
        "State": "pending",
        "EndpointEniId": "eni-2,
        "EndpointEniAddress": "10.0.2.4",
        "PeerEniId": "eni-1",
        "PeerAddress": "10.0.2.3",
        "BgpOptions": {
            "PeerAsn": 65001,
   "PeerLivenessDetection": "bfd"
        },
        "BgpStatus": {
            "Status": "Up"
        }
    }
}
```

2. Tunggu status propagasi berubah menjadi tersedia.

   Perintah:

   ```
   aws ec2 describe-route-server-peers
   ```

   Respons:

   ```
   {
       "RouteServerPeer": {
           "RouteServerPeerId": "rsp-1",
           "RouteServerId": "rs-1",
           "VpcId": "vpc-1",
   ```

```
        "SubnetId": "subnet-1",
        "State": "available",
        "EndpointEniId": "eni-2,
        "EndpointEniAddress": "10.0.2.4",
        "PeerEniId": "eni-1",
        "PeerAddress": "10.0.2.3",
        "BgpOptions": {
            "PeerAsn": 65001,
   "PeerLivenessDetection": "bfd"
        },
        "BgpStatus": {
            "Status": "down"
        }
    }
}
```

Langkah 7: Memulai sesi BGP dari perangkat

Ketika status peer server rute tersedia, konfigurasikan beban kerja Anda untuk memulai sesi BGP dengan titik akhir server rute.

Memulai sesi BGP dari perangkat di subnet Anda berada di luar cakupan panduan ini. Titik akhir server rute tidak memulai sesi BGP.

Anda dapat memeriksa apakah fitur Server Rute VPC berfungsi dengan memverifikasi bahwa tabel rute berisi rute terbaik yang disebarkan oleh server rute.

Langkah 8: Pembersihan

Bagian pembangunan dari tutorial selesai. Selesaikan langkah-langkah di bagian ini untuk menghapus komponen Server Rute VPC yang Anda buat.

7.1: Tarik iklan BGP di perangkat

Menarik iklan BGP pada perangkat di subnet Anda berada di luar cakupan panduan ini. Lihat vendor pihak ketiga Anda untuk konfigurasi BGP Anda sesuai kebutuhan.

7.2: Nonaktifkan propagasi server rute

Gunakan prosedur berikut untuk menonaktifkan propagasi server rute.

AWS Management Console

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pilih server rute yang ingin Anda nonaktifkan propagasi.
3. Pilih T indakan > Ubah server rute.
4. Pilih tab Propagations di panel detail server rute.
5. Pilih propagasi yang ingin Anda nonaktifkan dan kemudian pilih Non aktifkan propagasi.
6. Di kotak dialog, pilih Non aktifkan propagasi server rute.

Command line

1. Nonaktifkan propagasi:

```
aws ec2 disable-route-server-route-propagation --route-table-id rtb-1 --route-server-id rs-1
```

2. Konfirmasikan bahwa propagasi telah dihapus:

```
aws ec2 get-route-server-route-propagations --route-server-id rs-1 [--route-table-id rtb-1]
```

7.3: Hapus rekan server rute

Gunakan prosedur berikut untuk menghapus peer server rute.

AWS Management Console

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di jalur navigasi, pilih Server rute > Rute server peer.
3. Pilih peer server rute.
4. Pilih T ind akan > Hapus peer server rute.

Command line

1. Hapus rekan-rekan:

```
aws ec2 delete-route-server-peer --route-server-peer-id rsp-1
```

2. Konfirmasikan penghapusan:

```
aws ec2 describe-route-server-peers [--route-server-peer-ids rsp-1] [--filters
 Key=RouteServerId|RouteServerEndpointId|VpcId]
```

7.4: Hapus titik akhir server rute

Gunakan prosedur berikut untuk menghapus titik akhir server rute.

AWS Management Console

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pilih server rute yang ingin Anda hapus titik akhir.
3. Pilih titik akhir server rute.
4. Pilih titik akhir dan pilih Tind akan > H apus titik akhir server rute.
5. Masukkan hapus dan pilih H apus.

Command line

1. Jelaskan titik akhir:

```
aws ec2 describe-route-server-endpoints
```

2. Hapus titik akhir server rute:

```
aws ec2 delete-route-server-endpoint --route-server-endpoint-id rse-1
```

3. Konfirmasikan bahwa titik akhir telah dihapus:

```
aws ec2 describe-route-server-endpoints [--route-server-endpoint-ids rsp-1] [--
filters Key=RouteServerId|VpcId|SubnetId]
```

7.5: Putuskan kaitannya server rute dari VPC

Gunakan prosedur berikut untuk melepaskan router server dari VPC.

AWS Management Console

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pilih server rute yang ingin Anda pisahkan.
3. Pilih A sosiasi.
4. Pilih Put uskan kaitkan server rute.
5. Konfirmasikan perubahan yang akan dilakukan dan pilih Disassociation route server.

Command line

1. Putuskan hubungan server rute dari VPC:

```
aws ec2 disassociate-route-server --route-server-id rs-1 --vpc-id vpc-1
```

2. Konfirmasikan disasosiasi:

```
aws ec2 get-route-server-associations --route-server-id rs-1
```

7.6 Hapus server rute

Gunakan prosedur berikut untuk menghapus server rute.

AWS Management Console

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pilih server rute yang akan dihapus.
3. Pilih T ind akan > Hapus server rute.
4. Masukkan hapus dan pilih H apus.

Command line

1. Hapus server rute:

```
aws ec2 delete-route-server --route-server-id rs-1
```

2. Konfirmasikan penghapusan:

```
aws ec2 describe-route-servers [--route-server-ids rs-1] [--filters Key=VpcId]
```

Tutorial Amazon VPC Route Server selesai.

Memecahkan masalah keterjangkauan di VPC Anda

Reachability Analyzer adalah alat analisis konfigurasi statis. Gunakan Reachability Analyzer untuk menganalisis dan men-debug jangkauan jaringan antara dua sumber daya di VPC Anda. Reachability Analyzer menghasilkan detail hop-by-hop dari jalur virtual antara sumber daya ini ketika mereka dapat dijangkau, dan mengidentifikasi komponen pemblokiran sebaliknya. Misalnya, dapat mengidentifikasi rute tabel rute yang hilang atau salah dikonfigurasi.

Untuk informasi selengkapnya, lihat Panduan Peng analisis Jangkauan.

Wisaya perutean Middlebox

Jika Anda ingin mengonfigurasi kontrol butir halus atas jalur perutean lalu lintas yang memasuki atau meninggalkan VPC Anda, misalnya, dengan mengarahkan lalu lintas ke alat keamanan, Anda dapat menggunakan wizard perutean middlebox di konsol VPC. Wizard routing middlebox membantu Anda dengan secara otomatis membuat tabel rute dan rute yang diperlukan (hop) untuk mengarahkan lalu lintas sesuai kebutuhan.

Wizard routing middlebox dapat membantu Anda mengonfigurasi perutean untuk skenario berikut:

- Merutekan lalu lintas ke perangkat middlebox, misalnya, instans Amazon EC2 yang dikonfigurasi sebagai alat keamanan.
- Merutekan lalu lintas ke Load Balancer Gateway. Untuk informasi selengkapnya, lihat Panduan Pengguna untuk Penyeimbang Beban Gateway.

Untuk informasi selengkapnya, lihat the section called “Skenario Middlebox”.

Daftar Isi

- Prasyarat wizard perutean Middlebox
- Arahkan lalu lintas VPC ke alat keamanan
- Pertimbangan wizard perutean Middlebox
- Skenario Middlebox

Prasyarat wizard perutean Middlebox

Ulasanthe section called “Pertimbangan wizard perutean Middlebox”. Kemudian, pastikan bahwa Anda memiliki informasi berikut sebelum Anda menggunakan middlebox routing wizard.

- VPC.
- Sumber daya tempat lalu lintas berasal dari atau memasuki VPC, misalnya, gateway internet, gateway pribadi virtual, atau antarmuka jaringan.
- Antarmuka jaringan middlebox atau titik akhir Gateway Load Balancer.
- Subnet tujuan untuk lalu lintas.

Arahkan lalu lintas VPC ke alat keamanan

Wizard perutean middlebox tersedia di konsol VPC Amazon.

Daftar Isi

- 1. Buat rute menggunakan wizard perutean middlebox
- 2. Ubah rute middlebox
- 3. Hapus konfigurasi wizard routing middlebox

1. Buat rute menggunakan wizard perutean middlebox

Untuk membuat rute menggunakan wizard routing middlebox

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Your VPCs.
3. Pilih VPC Anda, lalu pilih Tindakan, Kelola rute middlebox.
4. Pilih Buat rute.
5. Pada halaman Tentukan rute, lakukan hal berikut:

- Untuk Sumber, pilih sumber untuk lalu lintas Anda. Jika Anda memilih gateway pribadi virtual, untuk IPv4 CIDR Tujuan, masukkan CIDR untuk lalu lintas lokal yang memasuki VPC dari gateway pribadi virtual.
- Untuk Middlebox, pilih ID antarmuka jaringan yang terkait dengan alat middlebox Anda, atau saat Anda menggunakan titik akhir Load Balancer Gateway, pilih ID titik akhir VPC.
- Untuk subnet Tujuan, pilih subnet tujuan.

6. (Opsional) Untuk menambahkan subnet tujuan lain, pilih Tambahkan subnet tambahan, lalu lakukan hal berikut:

   - Untuk Middlebox, pilih ID antarmuka jaringan yang terkait dengan alat middlebox Anda, atau saat Anda menggunakan titik akhir Load Balancer Gateway, pilih ID titik akhir VPC.

     Anda harus menggunakan alat middlebox yang sama untuk beberapa subnet.
   - Untuk subnet Tujuan, pilih subnet tujuan.
7. (Opsional) Untuk menambahkan sumber lain, pilih Tambahkan sumber, lalu ulangi langkah sebelumnya.
8. Pilih Berikutnya.
9. Pada halaman Tinjau dan buat, verifikasi rute, lalu pilih Buat rute.

2. Ubah rute middlebox

Anda dapat mengedit konfigurasi rute Anda dengan mengubah gateway, middlebox, atau subnet tujuan.

Saat Anda melakukan modifikasi apa pun, wizard perutean middlebox secara otomatis melakukan operasi berikut:

- Membuat tabel rute baru untuk gateway, middlebox, dan subnet tujuan.
- Menambahkan rute yang diperlukan ke tabel rute baru.
- Memisahkan tabel rute saat ini yang dikaitkan dengan wizard perutean middlebox dengan sumber daya.
- Mengaitkan tabel rute baru yang dibuat oleh wizard routing middlebox dengan sumber daya.

Untuk memodifikasi rute middlebox menggunakan wizard perutean middlebox

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Your VPCs.
3. Pilih VPC Anda, lalu pilih Tindakan, Kelola rute middlebox.
4. Pilih Edit rute.
5. Untuk mengubah gateway, untuk Sumber, pilih gateway tempat lalu lintas memasuki VPC Anda. Jika Anda memilih gateway pribadi virtual, untuk Tujuan IPv4 CIDR, masukkan subnet tujuan CIDR.
6. Untuk menambahkan subnet tujuan lain, pilih Tambahkan subnet tambahan, lalu lakukan hal berikut:

   - Untuk Middlebox, pilih ID antarmuka jaringan yang terkait dengan alat middlebox Anda, atau saat Anda menggunakan titik akhir Load Balancer Gateway, pilih ID titik akhir VPC.

     Anda harus menggunakan alat middlebox yang sama untuk beberapa subnet.
   - Untuk subnet Tujuan, pilih subnet tujuan.
7. Pilih Berikutnya.
8. Pada halaman Tinjau dan perbarui, daftar tabel rute dan rutenya yang akan dibuat oleh wizard perutean middlebox ditampilkan. Verifikasi rute, lalu di kotak dialog konfirmasi, pilih Perbarui rute.

3. Hapus konfigurasi wizard routing middlebox

Jika Anda memutuskan bahwa Anda tidak lagi menginginkan konfigurasi wizard perutean middlebox, Anda harus menghapus tabel rute secara manual.

Untuk menghapus konfigurasi wizard routing middlebox

1. Lihat tabel rute wizard routing middlebox.

   Setelah Anda melakukan operasi, tabel rute yang dibuat wizard routing middlebox ditampilkan pada halaman tabel rute terpisah.
2. Hapus setiap tabel rute yang ditampilkan.

Pertimbangan wizard perutean Middlebox

Pertimbangkan hal berikut saat Anda menggunakan wizard perutean middlebox:

- Jika Anda ingin memeriksa lalu lintas, Anda dapat menggunakan gateway internet atau gateway pribadi virtual untuk sumbernya.
- Jika Anda menggunakan middlebox yang sama dalam beberapa konfigurasi middlebox dalam VPC yang sama, pastikan middlebox berada di posisi hop yang sama untuk kedua subnet.
- Alat harus dikonfigurasi dalam subnet terpisah dari subnet sumber atau tujuan.
- Anda harus menonaktifkan source/destination pemeriksaan pada alat. Untuk informasi selengkapnya, lihat Mengubah Pemeriksaan Sumber atau Tujuan di Panduan Pengguna Amazon EC2.
- Tabel rute dan rute yang dibuat oleh wizard routing middlebox dihitung terhadap kuota Anda. Untuk informasi selengkapnya, lihat the section called “Tabel rute”.
- Jika Anda menghapus sumber daya, misalnya antarmuka jaringan, asosiasi tabel rute dengan sumber daya akan dihapus. Jika sumber daya adalah target, tujuan rute diatur ke lubang hitam. Tabel rute tidak dihapus.
- Subnet middlebox dan subnet tujuan harus dikaitkan dengan tabel rute non-default.

> **Note**
>
> Sebaiknya gunakan wizard perutean middlebox untuk memodifikasi atau menghapus tabel rute apa pun yang Anda buat menggunakan wizard perutean middlebox.

- Jika Anda menggunakan perutean middlebox untuk merutekan melalui alat keamanan, grup keamanan yang mereferensikan antara sumber dan tujuan akhir setelah pemeriksaan tidak didukung.

Skenario Middlebox

Amazon Virtual Private Cloud (VPC) menyediakan berbagai kemampuan jaringan yang memungkinkan Anda menyesuaikan dan mengontrol perutean lalu lintas dalam jaringan virtual Anda. Salah satu fitur tersebut adalah wizard routing middlebox, yang memungkinkan kontrol halus atas jalur routing lalu lintas yang masuk atau keluar dari VPC Anda.

Jika Anda perlu mengalihkan lalu lintas ke alat keamanan, penyeimbang beban, atau perangkat jaringan lainnya untuk tujuan inspeksi, pemantauan, atau pengoptimalan, wizard perutean middlebox dapat menyederhanakan prosesnya. Wizard ini secara otomatis membuat tabel rute dan rute (hop) yang diperlukan untuk mengarahkan lalu lintas yang ditentukan sesuai kebutuhan, menghilangkan upaya manual yang diperlukan untuk menyiapkan konfigurasi routing yang kompleks.

Wizard routing middlebox mendukung beberapa skenario berbeda. Misalnya, Anda dapat menggunakannya untuk memeriksa lalu lintas yang ditujukan untuk subnet tertentu, mengonfigurasi routing lalu lintas middlebox dan inspeksi di seluruh VPC Anda, atau secara selektif memeriksa lalu lintas antara subnet tertentu. Kontrol terperinci atas perutean lalu lintas ini memungkinkan Anda menerapkan kebijakan keamanan tingkat lanjut, mengaktifkan pemantauan jaringan terpusat, atau mengoptimalkan kinerja aplikasi berbasis cloud Anda.

Contoh berikut menjelaskan skenario untuk wizard perutean middlebox.

Daftar Isi

- Memeriksa lalu lintas yang ditujukan untuk subnet
- Konfigurasikan perutean lalu lintas middlebox dan inspeksi di VPC
- Periksa lalu lintas antar subnet

Memeriksa lalu lintas yang ditujukan untuk subnet

Pertimbangkan skenario di mana Anda memiliki lalu lintas masuk ke VPC melalui gateway internet dan Anda ingin memeriksa semua lalu lintas yang ditujukan untuk subnet, katakanlah subnet B, menggunakan alat firewall yang diinstal pada instance EC2. Perangkat firewall harus diinstal dan dikonfigurasi pada instance EC2 di subnet terpisah dari subnet B di VPC Anda, katakanlah subnet C. Anda kemudian dapat menggunakan wizard routing middlebox untuk mengonfigurasi rute untuk lalu lintas antara subnet B dan gateway internet.

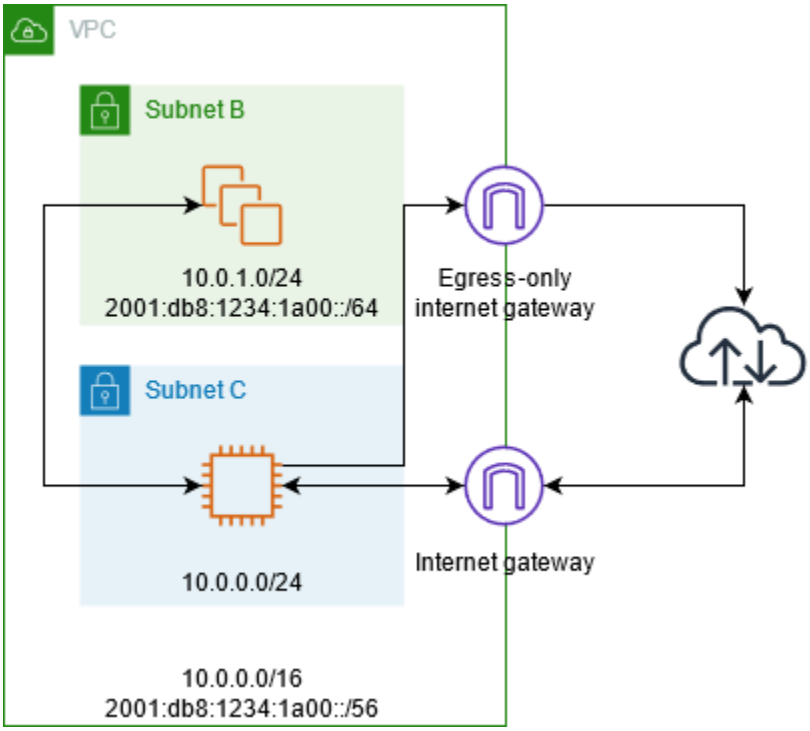
Wizard routing middlebox, secara otomatis melakukan operasi berikut:

- Membuat tabel rute berikut:
  - Tabel rute untuk gateway internet
  - Tabel rute untuk subnet tujuan
  - Tabel rute untuk subnet middlebox
- Menambahkan rute yang diperlukan ke tabel rute baru seperti yang dijelaskan di bagian berikut.
- Memisahkan tabel rute saat ini yang terkait dengan gateway internet, subnet B, dan subnet C.

- Mengaitkan tabel rute A dengan gateway internet (Sumber di wizard routing middlebox), tabel rute C dengan subnet C (Middlebox di wizard routing middlebox), dan tabel rute B dengan subnet B (Tujuan di wizard routing kotak tengah).
- Membuat tag yang menunjukkan bahwa itu dibuat oleh wizard routing middlebox, dan tag yang menunjukkan tanggal pembuatan.

Wizard routing middlebox tidak mengubah tabel rute yang ada. Ini membuat tabel rute baru, dan kemudian mengaitkannya dengan gateway dan sumber daya subnet Anda. Jika sumber daya Anda sudah secara eksplisit terkait dengan tabel rute yang ada, tabel rute yang ada pertama-tama dipisahkan, dan kemudian tabel rute baru dikaitkan dengan sumber daya Anda. Tabel rute yang ada tidak dihapus.

Jika Anda tidak menggunakan wizard perutean middlebox, Anda harus mengkonfigurasi secara manual, dan kemudian menetapkan tabel rute ke subnet dan gateway internet.



Tabel rute gateway internet

Tambahkan rute berikut ke tabel rute untuk gateway internet.

Tujuan	Target	Tujuan
10.0.0.0/16	Lokal:	Rute lokal untuk IPv4

Tujuan	Target	Tujuan
10.0.1.0/24	*appliance-eni*	Rute lalu lintas IPv4 yang ditujukan untuk subnet B ke middlebox
2001:db8:1234:1a00::/56	Lokal:	Rute lokal untuk IPv6
2001:db8:1234:1a00::/64	*appliance-eni*	Rute lalu lintas IPv6 yang ditujukan untuk subnet B ke middlebox

Ada hubungan tepi antara gateway internet dan VPC.

Saat Anda menggunakan wizard perutean middlebox, ia mengaitkan tag berikut dengan tabel rute:

- Kuncinya adalah “Origin” dan nilainya adalah “Middlebox wizard”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-T22:25:49.137Z 02-18 “)

Tabel rute subnet tujuan

Tambahkan rute berikut ke tabel rute untuk subnet tujuan (subnet B dalam diagram contoh).

Tujuan	Target	Tujuan
10.0.0.0/16	Lokal:	Rute lokal untuk IPv4
0.0.0. 0/0	*appliance-eni*	Rute lalu lintas IPv4 yang ditujukan untuk internet ke middlebox
2001:db8:1234:1a00::/56	Lokal:	Rute lokal untuk IPv6
::/0	*appliance-eni*	Rute lalu lintas IPv6 yang ditujukan untuk internet ke middlebox

Ada asosiasi subnet dengan subnet middlebox.

Saat Anda menggunakan wizard perutean middlebox, ia mengaitkan tag berikut dengan tabel rute:

- Kuncinya adalah “Origin” dan nilainya adalah “Middlebox wizard”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-T22:25:49.137Z 02-18 “)

Tabel rute subnet Middlebox

Tambahkan rute berikut ke tabel rute untuk subnet middlebox (subnet C dalam diagram contoh).

Tujuan	Target	Tujuan
10.0.0.0/16	Lokal:	Rute lokal untuk IPv4
0.0.0. 0/0	*igw-id*	Rute lalu lintas IPv4 ke gateway internet
2001:db8:1234:1a00::/56	Lokal:	Rute lokal untuk IPv6
::/0	*eigw-id*	Rute lalu lintas IPv6 ke gateway internet khusus keluar

Ada asosiasi subnet dengan subnet tujuan.

Saat Anda menggunakan wizard perutean middlebox, ia mengaitkan tag berikut dengan tabel rute:

- Kuncinya adalah “Origin” dan nilainya adalah “Middlebox wizard”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-T22:25:49.137Z 02-18 “)

Konfigurasikan perutean lalu lintas middlebox dan inspeksi di VPC

Pertimbangkan skenario di mana Anda perlu memeriksa lalu lintas yang memasuki VPC dari gateway internet dan ditujukan untuk subnet, menggunakan armada peralatan keamanan yang dikonfigurasi di belakang Gateway Load Balancer. Pemilik VPC konsumen layanan membuat titik akhir Gateway Load Balancer di subnet di VPC mereka (diwakili oleh antarmuka jaringan titik akhir). Semua lalu lintas yang memasuki VPC melalui gateway internet pertama-tama dialihkan ke titik akhir Gateway

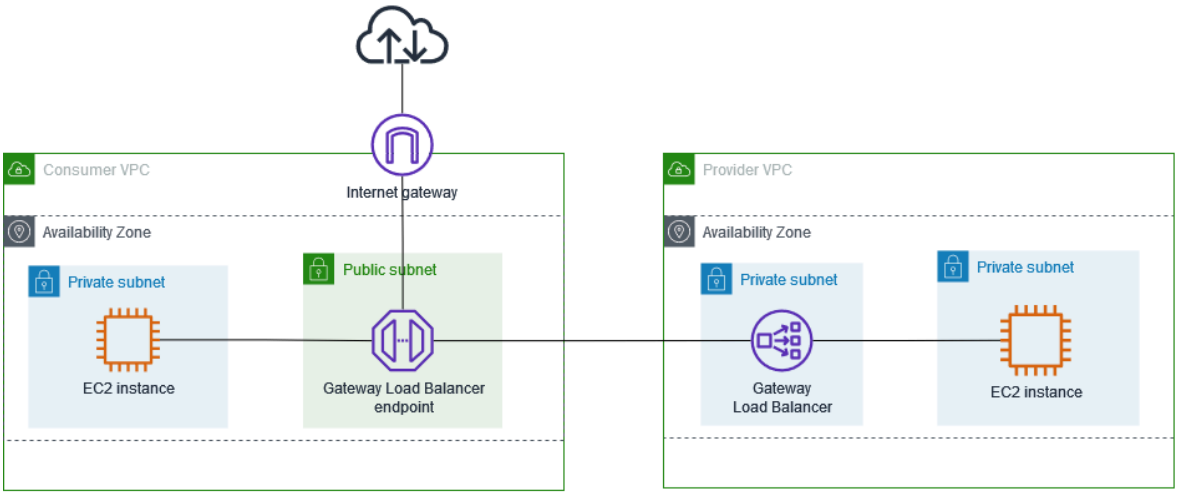
Load Balancer untuk diperiksa sebelum dialihkan ke subnet aplikasi. Demikian pula, semua lalu lintas yang meninggalkan subnet aplikasi pertama-tama dialihkan ke titik akhir Gateway Load Balancer untuk diperiksa sebelum dialihkan ke internet.

Wizard perutean middlebox secara otomatis melakukan operasi berikut:

- Membuat tabel rute.
- Menambahkan rute yang diperlukan ke tabel rute baru.
- Memutuskan hubungan tabel rute saat ini yang terkait dengan subnet.
- Mengaitkan tabel rute yang dibuat oleh wizard routing middlebox dengan subnet.
- Membuat tag yang menunjukkan bahwa itu dibuat oleh wizard routing middlebox, dan tag yang menunjukkan tanggal pembuatan.

Wizard routing middlebox tidak mengubah tabel rute yang ada. Ini membuat tabel rute baru, dan kemudian mengaitkannya dengan gateway dan sumber daya subnet Anda. Jika sumber daya Anda sudah secara eksplisit terkait dengan tabel rute yang ada, tabel rute yang ada pertama-tama dipisahkan, dan kemudian tabel rute baru dikaitkan dengan sumber daya Anda. Tabel rute yang ada tidak dihapus.

Jika Anda tidak menggunakan wizard perutean middlebox, Anda harus mengkonfigurasi secara manual, dan kemudian menetapkan tabel rute ke subnet dan gateway internet.



Tabel rute gateway internet

Tabel rute untuk gateway internet memiliki rute berikut.

Tujuan	Target	Tujuan
Consumer VPC CIDR	Lokal:	Rute lokal
Application subnet CIDR	*endpoint-id*	Merutekan lalu lintas yang ditujukan untuk subnet aplikasi ke titik akhir Gateway Load Balancer

Ada asosiasi tepi dengan gateway.

Saat Anda menggunakan wizard perutean middlebox, ia mengaitkan tag berikut dengan tabel rute:

- Kuncinya adalah “Origin” dan nilainya adalah “Middlebox wizard”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-T22:25:49.137Z 02-18 “)

Tabel rute subnet aplikasi

Tabel rute untuk subnet aplikasi memiliki rute berikut.

Tujuan	Target	Tujuan
Consumer VPC CIDR	Lokal:	Rute lokal
0.0.0. 0/0	*endpoint-id*	Rute lalu lintas dari server aplikasi ke titik akhir Gateway Load Balancer sebelum dialihkan ke internet

Saat Anda menggunakan wizard perutean middlebox, ia mengaitkan tag berikut dengan tabel rute:

- Kuncinya adalah “Origin” dan nilainya adalah “Middlebox wizard”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-T22:25:49.137Z 02-18 “)

Tabel rute subnet penyedia

Tabel rute untuk subnet penyedia memiliki rute berikut.

Tujuan	Target	Tujuan
Provider VPC CIDR	Lokal:	Rute lokal. Memastikan bahwa lalu lintas yang berasal dari internet dialihkan ke server aplikasi
0.0.0. 0/0	*igw-id*	Merutekan semua lalu lintas ke gateway internet

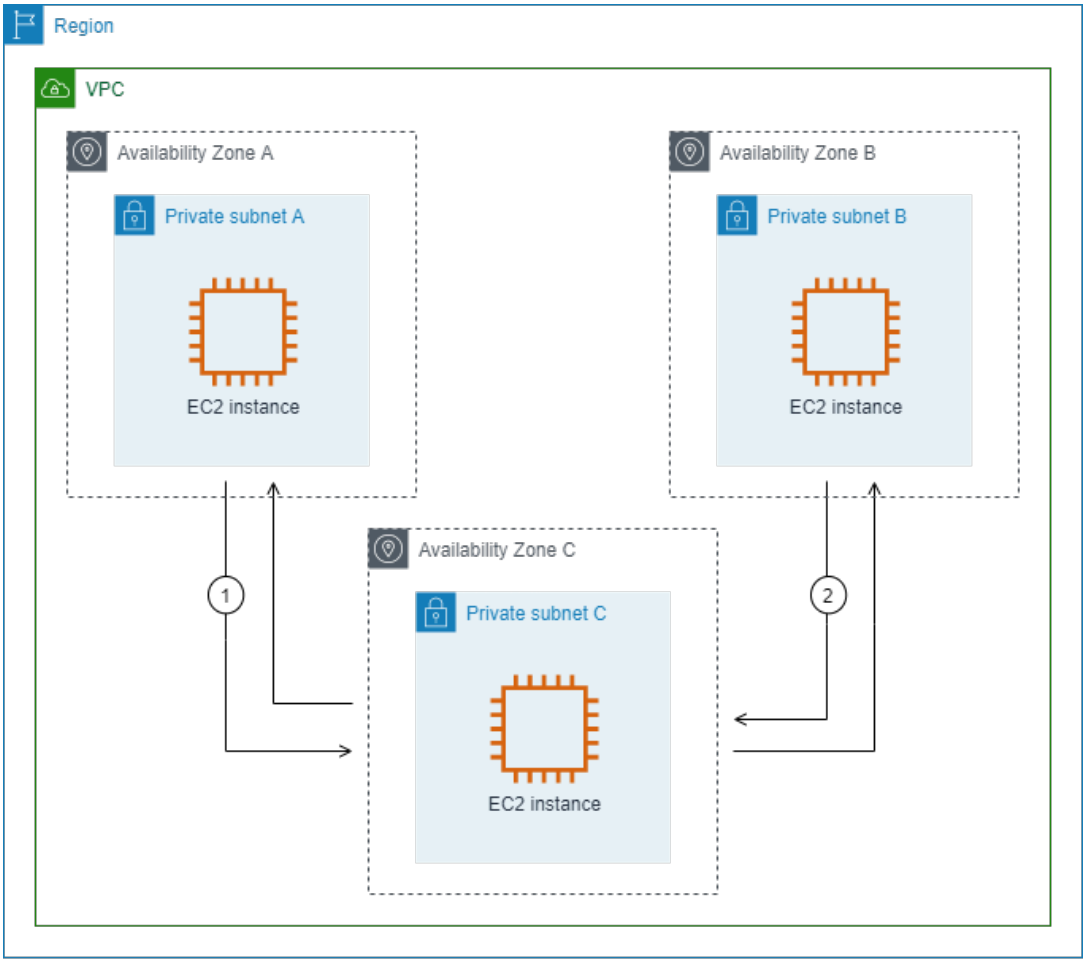
Saat Anda menggunakan wizard perutean middlebox, ia mengaitkan tag berikut dengan tabel rute:

- Kuncinya adalah “Origin” dan nilainya adalah “Middlebox wizard”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-T22:25:49.137Z 02-18 “)

Periksa lalu lintas antar subnet

Pertimbangkan skenario di mana Anda memiliki beberapa subnet dalam VPC dan Anda ingin memeriksa lalu lintas di antara mereka menggunakan alat firewall. Konfigurasikan dan instal alat firewall pada instans EC2 di subnet terpisah di VPC Anda.

Diagram berikut menunjukkan alat firewall yang diinstal pada instance EC2 di subnet C. Alat memeriksa semua lalu lintas yang bergerak dari subnet A ke subnet B (lihat 1) dan dari subnet B ke subnet A (lihat 2).



Anda menggunakan tabel rute utama untuk subnet VPC dan middlebox. Subnet A dan B masing-masing memiliki tabel rute khusus.

Wizard routing middlebox, secara otomatis melakukan operasi berikut:

- Membuat tabel rute.
- Menambahkan rute yang diperlukan ke tabel rute baru.
- Memisahkan tabel rute saat ini yang terkait dengan subnet.
- Mengaitkan tabel rute yang dibuat oleh wizard routing middlebox dengan subnet.
- Membuat tag yang menunjukkan bahwa itu dibuat oleh wizard routing middlebox, dan tag yang menunjukkan tanggal pembuatan.

Wizard routing middlebox tidak mengubah tabel rute yang ada. Ini membuat tabel rute baru, dan kemudian mengaitkannya dengan gateway dan sumber daya subnet Anda. Jika sumber daya Anda sudah secara eksplisit terkait dengan tabel rute yang ada, tabel rute yang ada pertama-tama

dipisahkan, dan kemudian tabel rute baru dikaitkan dengan sumber daya Anda. Tabel rute Anda yang ada tidak dihapus.

Jika Anda tidak menggunakan wizard perutean middlebox, Anda harus mengkonfigurasi secara manual, dan kemudian menetapkan tabel rute ke subnet dan gateway internet.

Tabel rute khusus untuk subnet A

Tabel rute untuk subnet A memiliki rute berikut.

Tujuan	Target	Tujuan
VPC CIDR	Lokal:	Rute lokal
Subnet B CIDR	*appliance-eni*	Rute lalu lintas yang ditujukan untuk subnet B ke middlebox

Saat Anda menggunakan wizard perutean middlebox, ia mengaitkan tag berikut dengan tabel rute:

- Kuncinya adalah “Origin” dan nilainya adalah “Middlebox wizard”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-T22:25:49.137Z 02-18 “)

Tabel rute khusus untuk subnet B

Tabel rute untuk subnet B memiliki rute berikut.

Tujuan	Target	Tujuan
VPC CIDR	Lokal:	Rute lokal
Subnet A CIDR	*appliance-eni*	Rute lalu lintas yang ditujukan untuk subnet A ke middlebox

Saat Anda menggunakan wizard perutean middlebox, ia mengaitkan tag berikut dengan tabel rute:

- Kuncinya adalah “Origin” dan nilainya adalah “Middlebox wizard”

- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-T22:25:49.137Z 02-18 “)

Tabel rute utama

Subnet C menggunakan tabel rute utama. Tabel rute utama memiliki rute berikut.

Tujuan	Target	Tujuan
VPC CIDR	Lokal:	Rute lokal

Saat Anda menggunakan wizard perutean middlebox, ia mengaitkan tag berikut dengan tabel rute:

- Kuncinya adalah “Origin” dan nilainya adalah “Middlebox wizard”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-T22:25:49.137Z 02-18 “)

Hapus subnet

Jika Anda tidak lagi membutuhkan subnet, Anda dapat menghapusnya. Anda tidak dapat menghapus subnet jika berisi antarmuka jaringan apa pun. Misalnya, Anda harus menghentikan instance apa pun di subnet sebelum Anda dapat menghapusnya.

Saat Anda menghapus subnet, blok CIDR yang terkait dengan subnet tersebut dikembalikan ke kumpulan alamat IP VPC yang tersedia. Ini berarti bahwa alamat IP dalam rentang CIDR subnet dapat dialokasikan kembali ke subnet atau sumber daya lain dalam VPC yang sama.

Penting untuk dicatat bahwa menghapus subnet tidak secara otomatis menghapus sumber daya di dalamnya. Anda harus terlebih dahulu menghentikan EC2 instance apa pun, menghapus antarmuka jaringan apa pun, dan menghapus sumber daya lain yang terkait dengan subnet sebelum Anda dapat melanjutkan penghapusan subnet.

Untuk menghapus subnet menggunakan konsol

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Mengakhiri semua instans di subnet. Untuk informasi selengkapnya, lihat Menghentikan instans Anda di Panduan EC2 Pengguna Amazon.

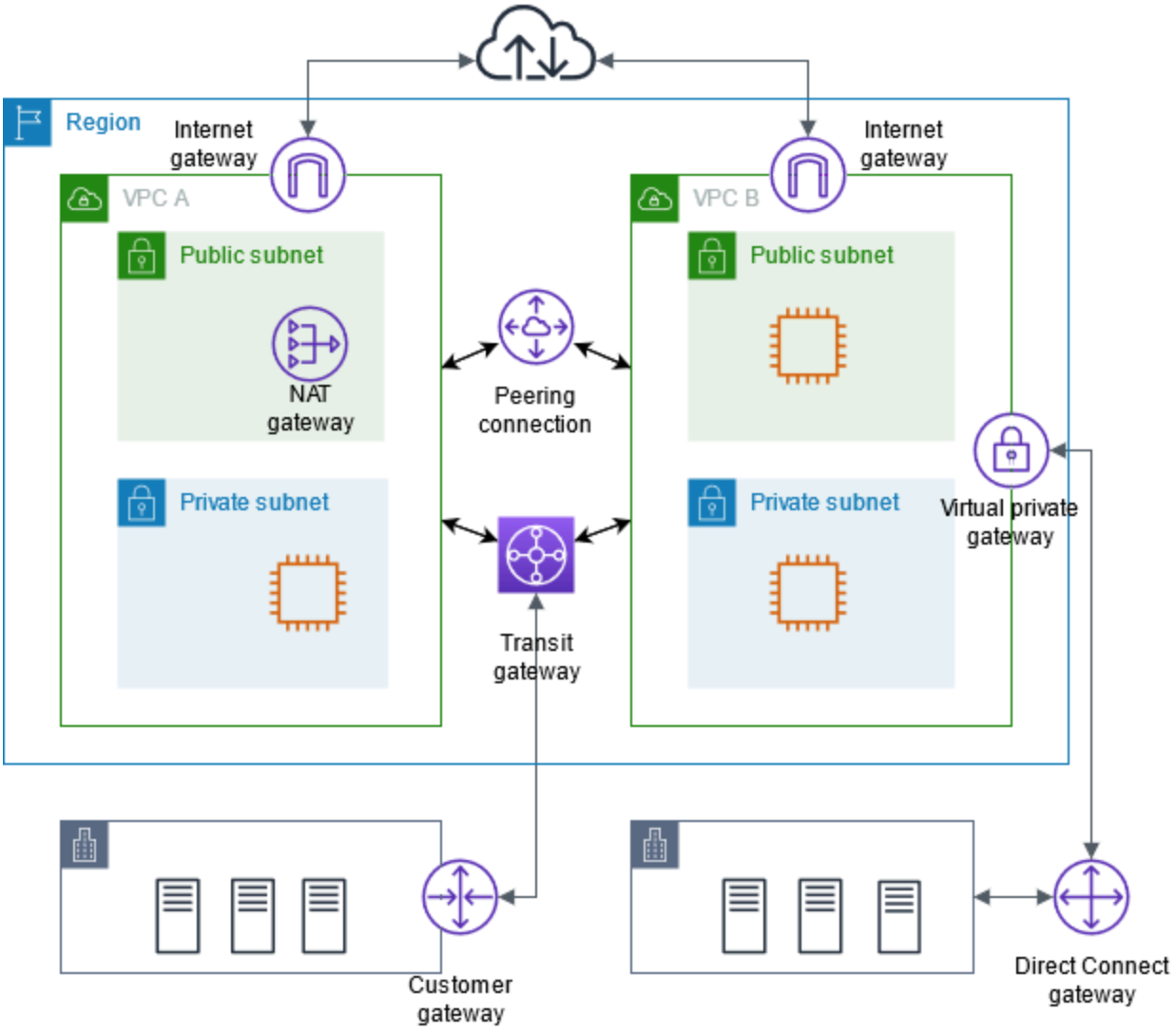
3. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
4. Di panel navigasi, pilih Pengguna.
5. Pilih subnet dan pilih Actions, Delete subnet.
6. Saat diminta konfirmasi, ketik **`delete`** lalu pilih Hapus.

Untuk menghapus subnet menggunakan AWS CLI

Gunakan perintah delete-subnet.

Hubungkan VPC Anda ke jaringan lain

Anda dapat menghubungkan virtual private cloud (VPC) ke jaringan lain, seperti VPC lain, internet, atau jaringan lokal Anda.



Anda dapat menghubungkan virtual private cloud (VPC) ke jaringan lain, seperti VPC lain, internet, atau jaringan lokal Anda.

Diagram menunjukkan beberapa opsi konektivitas ini. VPC A terhubung ke internet melalui gateway internet, dan instance EC2 di subnet pribadi dapat terhubung ke internet menggunakan gateway NAT di subnet publik. VPC B juga terhubung ke internet, tetapi melalui gateway internet langsung, memungkinkan instance EC2 di subnet publik untuk mengakses internet.

Selain itu, VPC A dan VPC B terhubung satu sama lain melalui koneksi peering VPC dan gateway transit. Gateway transit memiliki lampiran VPN ke pusat data, dan VPC B memiliki Direct Connect koneksi ke pusat data yang sama. Interkonektivitas ini memungkinkan organisasi untuk mengintegrasikan sumber daya cloud mereka dengan infrastruktur lokal, menciptakan lingkungan cloud hybrid.

Menghubungkan VPC ke jaringan lain adalah aspek penting dalam membangun infrastruktur cloud di dalamnya AWS. Ini menawarkan fleksibilitas dan kontrol organisasi atas konfigurasi jaringan mereka, memungkinkan mereka untuk merancang arsitektur VPC yang selaras dengan persyaratan bisnis dan kebutuhan keamanan mereka. Opsi konektivitas ini membantu aliran data yang efisien antara berbagai komponen lanskap TI terdistribusi, baik itu berada di dalam cloud atau lokal.

AWS menyediakan berbagai alat dan fitur untuk mengaktifkan koneksi VPC ini, termasuk gateway internet, gateway NAT, peering VPC, gateway transit, dan. Direct Connect Dengan menggunakan kemampuan ini, organisasi dapat menciptakan lingkungan cloud yang aman dan terintegrasi yang terintegrasi dengan mulus dengan infrastruktur TI mereka yang ada.

Anda dapat menghubungkan virtual private cloud (VPC) Anda ke jaringan lain. Misalnya, VPC lain, internet, atau jaringan lokal Anda.

Untuk informasi selengkapnya, lihat Opsi Konektivitas Cloud Pribadi Virtual Amazon.

Daftar Isi

- Aktifkan akses internet untuk VPC menggunakan gateway internet
- Aktifkan lalu lintas IPv6 keluar menggunakan gateway internet khusus keluar
- Sambungkan ke internet atau jaringan lain menggunakan perangkat NAT
- Mengaitkan alamat IP Elastic dengan sumber daya di VPC Anda
- Hubungkan VPC Anda ke VPC dan jaringan lain menggunakan gateway transit
- Hubungkan VPC Anda ke jaringan jarak jauh menggunakan AWS Virtual Private Network
- Hubungkan VPC menggunakan peering VPC

Aktifkan akses internet untuk VPC menggunakan gateway internet

Gateway internet diskalakan secara horizontal, berlebihan, dan merupakan komponen VPC yang sangat tersedia yang mengizinkan komunikasi antara VPC Anda dan internet. Ini mendukung lalu lintas IPv4 dan IPv6. Gateway internet tidak menimbulkan risiko ketersediaan atau kendala bandwidth pada lalu lintas jaringan Anda.

Gateway internet memungkinkan sumber daya di subnet publik Anda (seperti instans EC2) untuk terhubung ke internet jika sumber daya memiliki alamat IPv4 publik atau alamat IPv6. Demikian pula, sumber daya di internet dapat memulai koneksi ke sumber daya di subnet Anda menggunakan alamat IPv4 publik atau alamat IPv6. Misalnya, gateway internet memungkinkan Anda untuk terhubung ke instance EC2 AWS menggunakan komputer lokal Anda.

Gateway internet menyediakan target dalam tabel rute VPC Anda untuk lalu lintas yang dapat dirutekan internet. Untuk komunikasi menggunakan IPv4, gateway internet juga melakukan terjemahan alamat jaringan (NAT). Untuk informasi selengkapnya, lihat alamat IP dan NAT.

Harga

Tidak ada biaya untuk gateway internet, tetapi ada biaya transfer data untuk instans EC2 yang menggunakan gateway internet. Untuk informasi selengkapnya, lihat Harga Amazon EC2 On-Demand .

Daftar Isi

- Dasar-dasar gateway internet
- Menambahkan akses internet ke subnet
- Menghapus gateway internet

Dasar-dasar gateway internet

Untuk menggunakan gateway internet, Anda harus melampirkannya ke VPC dan mengkonfigurasi routing.

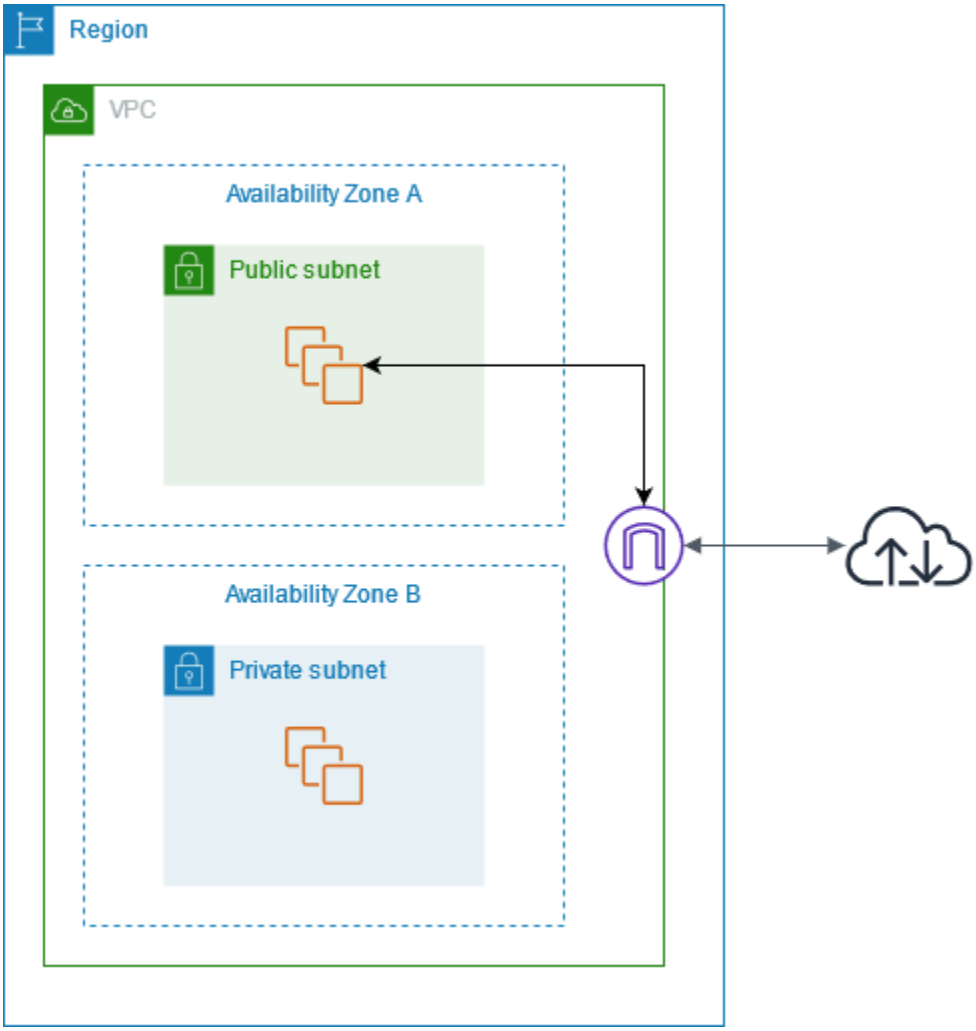
Konfigurasi perutean

Jika subnet dikaitkan dengan tabel rute yang memiliki rute ke gateway internet, hal ini dikenal sebagai subnet publik. Jika subnet dikaitkan dengan tabel rute yang tidak memiliki rute ke gateway internet, itu dikenal sebagai subnet pribadi.

Di tabel rute subnet publik Anda, Anda dapat menentukan rute untuk gateway internet ke semua tujuan yang tidak diketahui secara eksplisit oleh tabel rute (0.0.0. 0/0 untuk IPv4 atau: :/0 untuk IPv6). Atau, Anda dapat menjangkau rute ke rentang alamat IP yang lebih sempit; misalnya, alamat IPv4 publik dari titik akhir publik perusahaan Anda di luar AWS, atau alamat IP Elastic instans Amazon EC2 lainnya di luar VPC Anda.

Diagram gateway internet

Dalam diagram berikut, subnet di Availability Zone A adalah subnet publik karena tabel rute memiliki rute yang mengirimkan semua lalu lintas IPv4 terikat internet ke gateway internet. Instans di subnet publik harus memiliki alamat IP publik atau alamat IP elastis untuk memungkinkan komunikasi dengan internet melalui gateway internet. Sebagai perbandingan, subnet di Availability Zone B adalah subnet pribadi karena tabel rute tidak memiliki rute ke gateway internet. Karena tidak ada rute ke gateway internet, instance di subnet pribadi tidak dapat berkomunikasi dengan internet, bahkan jika mereka memiliki alamat IP publik.



Alamat IP dan NAT

Untuk mengaktifkan komunikasi melalui internet untuk IPv4, instans Anda harus memiliki alamat IPv4 publik. Anda dapat mengonfigurasi VPC untuk secara otomatis menetapkan alamat IPv4 publik ke instans Anda, atau Anda dapat menetapkan alamat IP Elastic ke instans Anda. Instans Anda hanya mengenal ruang alamat IP pribadi (internal) yang terdefinisi di dalam VPC dan subnet. Gateway internet secara logis menyediakan NAT satu-satu atas nama instans Anda, sehingga ketika lalu lintas meninggalkan subnet VPC Anda dan menuju internet, kolom alamat balasan diatur ke alamat

IPv4 publik atau alamat IP Elastis dari instans Anda, dan bukan alamat IP pribadi. Sebaliknya, lalu lintas yang ditujukan untuk alamat IPv4 publik atau alamat IP Elastis dari instans Anda yang memiliki alamat tujuannya ditranslasikan ke dalam instans alamat IPv4 pribadi sebelum lalu lintas dikirim ke VPC.

Untuk mengaktifkan komunikasi melalui internet untuk IPv6, VPC dan subnet Anda harus memiliki blok CIDR IPv6 terkait, dan instans Anda harus mendapat alamat IPv6 dari kisaran subnet. Alamat IPv6 secara global bersifat unik, dan karena itu secara default bersifat publik.

Akses Internet untuk VPC default dan nondefault

Tabel berikut memberikan gambaran umum tentang apakah VPC Anda secara otomatis dilengkapi dengan komponen yang diperlukan untuk akses internet melalui IPv4 atau IPv6.

Komponen	VPC Default	VPC Nondefault
gateway internet	Ya	Tidak
Tabel rute dengan rute ke gateway internet untuk lalu lintas IPv4 (0.0.0. 0/0)	Ya	Tidak
Tabel rute dengan rute ke gateway internet untuk lalu lintas IPv6 (:: /0)	Tidak	Tidak
Alamat IPv4 publik secara otomatis diberikan ke instans yang diluncurkan ke dalam subnet	Ya (subnet default)	Tidak ada (subnet nondefault)
Alamat IPv6 secara otomatis diberikan ke instans yang diluncurkan ke dalam subnet	Tidak (subnet default)	Tidak (subnet nondefault)

Menambahkan akses internet ke subnet

Berikut ini menjelaskan cara mendukung akses internet dari subnet di VPC nondefault menggunakan gateway internet. Anda harus membuat gateway internet, melampirkannya ke VPC, dan mengkonfigurasi routing untuk subnet.

Setelah Anda mengkonfigurasi akses internet untuk subnet Anda, Anda harus memastikan bahwa sumber daya di subnet dapat mengakses internet. Misalnya, instans EC2 Anda harus memiliki alamat IPv4 atau IPv6 publik, dan grup keamanan untuk instans Anda harus mengizinkan lalu lintas tertentu ke dan dari internet.

Atau, untuk menyediakan instans Anda dengan akses internet tanpa menetapkan alamat IP publik, gunakan perangkat NAT sebagai gantinya. Untuk informasi selengkapnya, lihat Perangkat NAT.

Untuk menghapus akses internet, Anda dapat melepaskan gateway internet dari VPC Anda dan kemudian menghapusnya. Untuk informasi selengkapnya, lihat the section called “Menghapus gateway internet”.

Tugas

- Langkah 1: Buat gateway internet
- Langkah 2: Pasang gateway internet ke VPC
- Langkah 3: Tambahkan rute ke tabel rute subnet

Langkah 1: Buat gateway internet

Gunakan prosedur berikut untuk membuat gateway internet.

Untuk membuat gateway internet menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Internet gateway.
3. Pilih Buat gateway internet.
4. (Opsional) Masukkan nama untuk gateway internet Anda.
5. (Opsional) Untuk menambahkan tag, pilih Tambahkan tag baru dan masukkan kunci tag dan nilai.
6. Pilih Buat gateway internet.

7. (Opsional) Untuk melampirkan gateway internet ke VPC sekarang, pilih Lamp irkan ke VPC dari spanduk di bagian atas layar, pilih VPC yang tersedia, lalu pilih Lamp irkan gateway internet. Jika tidak, Anda dapat melampirkan gateway internet Anda ke VPC di lain waktu.

Untuk membuat gateway internet menggunakan baris perintah

- create-internet-gateway (AWS CLI)
- New-EC2InternetGateway (AWS Tools for Windows PowerShell)

Langkah 2: Pasang gateway internet ke VPC

Untuk menggunakan gateway internet, Anda harus melampirkannya ke VPC.

Untuk melampirkan gateway internet ke VPC menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Internet gateway.
3. Pilih kotak centang untuk gateway internet.
4. Untuk melampirkannya, pilih T ind akan, Lampirkan ke VPC, pilih VPC yang tersedia, dan pilih Lamp irkan gateway internet.
5. Untuk melepaskannya, pilih Tind akan, L epaskan dari VPC dan pilih Lepaskan gateway internet. Saat diminta konfirmasi, pilih L epaskan gateway internet.

Untuk melampirkan gateway internet ke VPC menggunakan baris perintah

- attach-internet-gateway (AWS CLI)
- Add-EC2InternetGateway (AWS Tools for Windows PowerShell)

Langkah 3: Tambahkan rute ke tabel rute subnet

Tabel rute untuk subnet harus memiliki rute yang mengirimkan lalu lintas internet ke gateway internet.

Untuk mengkonfigurasi tabel rute subnet menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Tabel rute.

3. Pilih tabel rute untuk subnet. Secara default, subnet menggunakan tabel rute utama untuk VPC. Atau, Anda dapat membuat tabel rute dan kemudian mengaitkan subnet dengan tabel rute baru.
4. Pada tab Rute, pilih Edit rute lalu pilih Tambahkan rute.
5. Masukkan 0.0.0. 0/0 untuk Tujuan dan pilih gateway internet untuk Target.
6. Pilih Simpan perubahan.

Untuk mengkonfigurasi tabel rute subnet menggunakan baris perintah

- create-route (AWS CLI)
- New-EC2Route (AWS Tools for Windows PowerShell)

Menghapus gateway internet

Jika Anda tidak lagi memerlukan akses internet untuk VPC, Anda dapat melepaskan gateway internet dari VPC dan kemudian menghapusnya. Anda tidak dapat menghapus gateway internet jika masih terpasang ke VPC. Anda tidak dapat melepas gateway internet jika VPC memiliki sumber daya dengan alamat IP publik terkait atau alamat IP Elastis.

Untuk melepaskan gateway internet dari VPC menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Internet gateway.
3. Pilih kotak centang untuk gateway internet.
4. Untuk melampirkannya, pilih T ind akan, Lampirkan ke VPC, pilih VPC yang tersedia, dan pilih Lamp irkan gateway internet.
5. Untuk melepaskannya, pilih Tind akan, L epaskan dari VPC dan pilih Lepaskan gateway internet. Saat diminta konfirmasi, pilih L epaskan gateway internet.

Untuk menggambarkan gateway internet Anda, termasuk lampiran, menggunakan baris perintah

- describe-internet-gateways (AWS CLI)
- Get-EC2InternetGateway (AWS Tools for Windows PowerShell)

Untuk melepaskan gateway internet dari VPC menggunakan baris perintah

- detach-internet-gateway (AWS CLI)
- Dismount-EC2InternetGateway (AWS Tools for Windows PowerShell)

Untuk menghapus gateway internet menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Internet gateway.
3. Pilih kotak centang untuk gateway internet.
4. Pilih T ind akan, Hapus gateway internet.
5. Saat diminta konfirmasi, masukkan**delete**, lalu pilih H apus gateway internet.

Untuk menghapus gateway internet menggunakan baris perintah

- delete-internet-gateway (AWS CLI)
- Remove-EC2InternetGateway (AWS Tools for Windows PowerShell)

Aktifkan lalu lintas IPv6 keluar menggunakan gateway internet khusus keluar

Sebuah gateway internet egress-only adalah komponen VPC yang terskala secara horizontal, redundan, dan sangat tersedia yang memungkinkan komunikasi outbound melalui IPv6 pada instans di VPC Anda ke internet, dan mencegah internet memulai koneksi IPv6 dengan instans Anda.

Gateway internet egress-only adalah untuk digunakan bersama lalu lintas IPv6 saja. Untuk mengaktifkan komunikasi internet outbound-only melalui IPv4, gunakan gateway NAT sebagai gantinya. Untuk informasi selengkapnya, lihat Gateway NAT.

Harga

Tidak ada biaya untuk gateway internet khusus keluar, tetapi ada biaya transfer data untuk instans EC2 yang menggunakan gateway internet. Untuk informasi selengkapnya, lihat Harga Amazon EC2 On-Demand .

Daftar Isi

- Egress-only dasar-dasar gateway internet
- Tambahkan akses internet khusus egress ke subnet

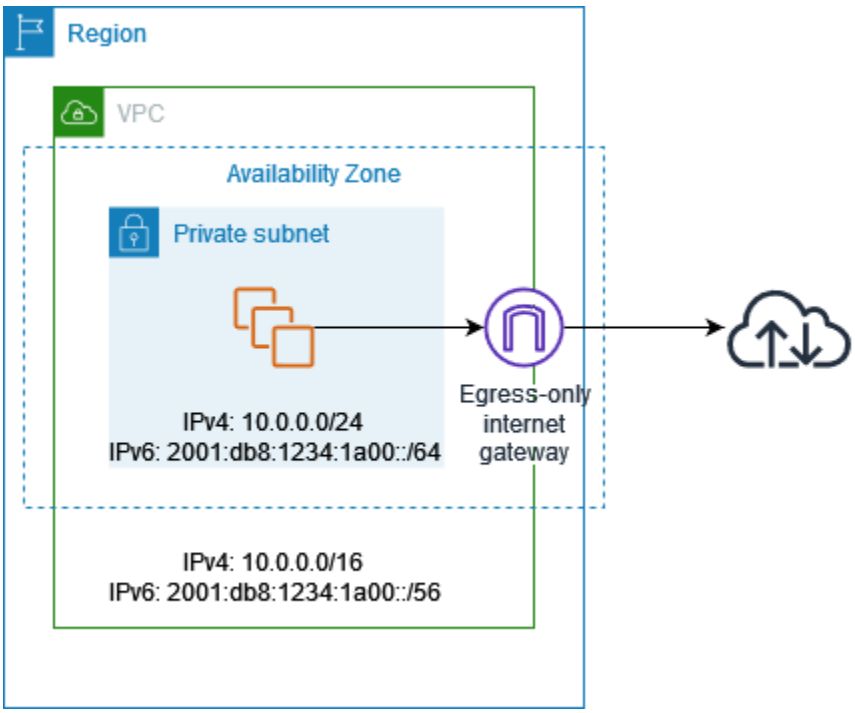
Egress-only dasar-dasar gateway internet

Alamat IPv6 bersifat unik secara global, dan oleh karenanya bersifat publik secara default. Jika Anda ingin instans Anda dapat mengakses internet, tetapi Anda ingin mencegah sumber daya di internet memulai komunikasi dengan instans Anda, Anda dapat menggunakan gateway internet yang egres-only. Untuk melakukannya, buat gateway internet egress-only di VPC Anda, dan kemudian tambahkan rute ke tabel rute Anda yang mengarah ke semua lalu lintas IPv6 (`::/0`) atau kisaran alamat IPv6 tertentu ke gateway internet egress-only. Lalu lintas IPv6 di subnet yang terkait dengan tabel rute diarahkan ke gateway internet egress-only.

Gateway internet khusus keluar bersifat stateful: gateway ini meneruskan lalu lintas dari instance di subnet ke internet atau AWS layanan lain, dan kemudian mengirimkan respons kembali ke instance.

Anda tidak dapat mengaitkan grup keamanan dengan gateway internet khusus keluar untuk mengontrol lalu lintas yang diizinkan untuk mencapai atau meninggalkan gateway internet khusus keluar. Anda dapat menggunakan ACL jaringan untuk mengontrol lalu lintas ke dan dari subnet yang mana gateway internet egress-only mengarahkan lalu lintas.

Dalam diagram berikut, VPC memiliki blok CIDR IPv4 dan IPv6, dan subnet kedua blok IPv4 dan IPv6 CIDR. VPC memiliki gateway internet khusus keluar.



Berikut ini adalah contoh tabel rute yang terkait dengan subnet. Ada rute yang mengirimkan semua lalu lintas IPv6 terikat internet (:: /0) ke gateway internet khusus keluar.

Tujuan	Target
10.0.0. 0/16	Lokal:
2001: db 8:1234:1 a00: /64	Lokal:
::/0	*eigw-id*

Tambahkan akses internet khusus egress ke subnet

Tugas berikut menjelaskan cara membuat gateway internet khusus keluar (keluar) untuk subnet pribadi Anda dan mengonfigurasi routing untuk subnet.

Tugas

- 1. Buat gateway internet egress-only
- 2. Membuat tabel rute kustom
- 3. Hapus gateway internet egress-only
- Ikhtisar baris perintah

1. Buat gateway internet egress-only

Anda dapat membuat gateway internet egress-only untuk VPC Anda menggunakan konsol Amazon VPC.

Untuk membuat gateway internet egress-only

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Gateway Internet Egress Only.
3. Pilih Buat Gateway Internet Egress Only.
4. (Opsional) Tambahkan atau hapus tag.

   [Menambahkan tanda] Pilih Tambahkan tanda baru dan lakukan hal berikut:

   - Untuk Kunci, masukkan nama kunci.
   - Untuk Nilai, masukkan nilai kunci.

   [Hapus tag] Pilih H apus di sebelah kanan Kunci dan Nilai tag.
5. Pilih VPC tempat untuk membuat gateway internet egress-only.
6. Pilih Buat.

2. Membuat tabel rute kustom

Untuk mengirimkan lalu lintas yang ditujukan di luar VPC untuk gateway internet egress-only, Anda harus membuat tabel rute kustom, menambahkan rute yang mengirimkan lalu lintas ke gateway, dan kemudian mengaitkannya dengan subnet Anda.

Untuk membuat tabel rute kustom dan menambahkan rute ke gateway internet egress-only

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Tabel Rute, Buat tabel.
3. Di kotak dialog Buat tabel rute, secara opsional namai tabel rute Anda, kemudian pilih VPC Anda dan pilih Buat tabel rute.
4. Pilih tabel rute kustom yang baru saja Anda buat. Panel rincian menampilkan tab untuk bekerja dengan rute, asosiasi, dan propagasi rute.

5. Pada tab Rute, pilih Edit rute, tentukan `::/0` di kotak Tujuan, pilih ID gateway internet egress-only di daftar Target, dan kemudian pilih Simpan perubahan.
6. Pada tab Keterkaitan subnet, pilih Sunting keterkaitan subnet, lalu pilih kotak centang untuk subnet. Pilih Simpan.

Atau, Anda dapat menambahkan rute ke tabel rute yang ada yang terkait dengan subnet Anda. Pilih tabel rute yang ada, dan ikuti langkah 5 dan 6 di atas untuk menambahkan rute untuk gateway internet egress-only.

Untuk informasi selengkapnya tentang tabel rute, lihat Konfigurasikan tabel rute.

3. Hapus gateway internet egress-only

Jika Anda tidak lagi memerlukan gateway internet egress-only, Anda dapat menghapusnya. Setiap rute dalam tabel rute yang mengarah ke gateway internet egress-only yang terhapus tetap berstatus `blackhole` hingga Anda menghapus atau memperbarui rute secara manual.

Untuk menghapus gateway internet egress-only

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih gateway Internet Egress Only, dan pilih gateway internet egress-only.
3. Pilih Hapus.
4. Pilih Hapus Gateway Internet Egress-Only di kotak dialog konfirmasi.

Ikhtisar baris perintah

Anda dapat melakukan tugas yang dijelaskan pada halaman ini menggunakan baris perintah.

Buat gateway internet egress-only

- create-egress-only-internet-gateway (AWS CLI)
- New-EC2EgressOnlyInternetGateway (AWS Tools for Windows PowerShell)

Jelaskan gateway internet egress-only

- describe-egress-only-internet-gateways (AWS CLI)
- Get-EC2EgressOnlyInternetGatewayList (AWS Tools for Windows PowerShell)

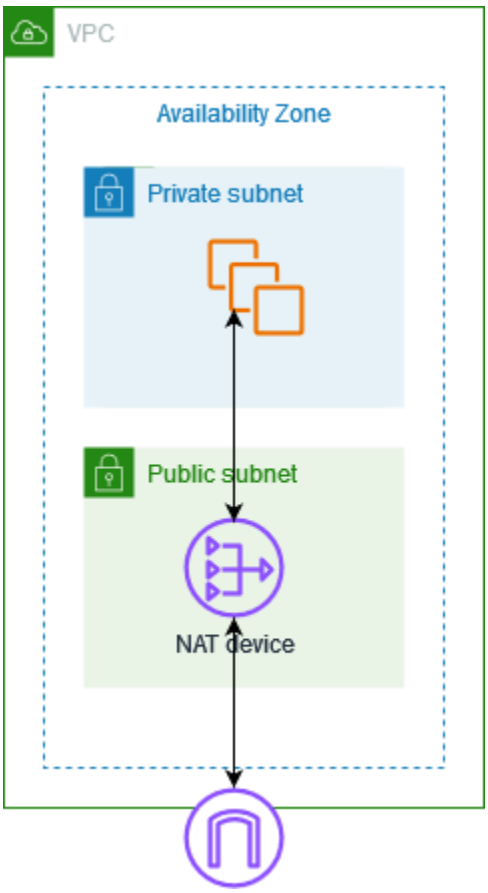
Hapus gateway internet egress-only

- delete-egress-only-internet-gateway (AWS CLI)
- Remove-EC2EgressOnlyInternetGateway (AWS Tools for Windows PowerShell)

Sambungkan ke internet atau jaringan lain menggunakan perangkat NAT

Anda dapat menggunakan perangkat NAT untuk mengizinkan sumber daya di subnet pribadi untuk terhubung ke internet, VPC lain, atau jaringan lokal. Instans ini dapat berkomunikasi dengan layanan di luar VPC, tetapi tidak dapat menerima permintaan koneksi yang tidak diminta.

Misalnya, diagram berikut menunjukkan perangkat NAT di subnet publik yang memungkinkan instans EC2 di subnet pribadi untuk terhubung ke internet melalui gateway internet. Perangkat NAT menggantikan alamat IPv4 sumber instans dengan alamat perangkat NAT. Saat mengirim lalu lintas respons ke instans, perangkat NAT menerjemahkan alamat kembali ke alamat IPv4 sumber asal.



> **Important**
>
> - Kami menggunakan istilah NAT dalam dokumentasi ini untuk mengikuti praktek IT umum, meskipun peran sebenarnya dari perangkat NAT adalah terjemahan alamat dan terjemahan alamat port (PAT).
> - Anda dapat menggunakan perangkat NAT terkelola yang ditawarkan oleh AWS, yang disebut gateway NAT, atau Anda dapat membuat perangkat NAT Anda sendiri pada instans EC2, yang disebut instance NAT. Kami menyarankan Anda menggunakan gateway NAT karena gateway NAT memberikan tingkat ketersediaan dan bandwidth yang lebih baik dan mudah bagi Anda untuk mengelolanya.

Daftar Isi

- Gateway NAT
- Instans NAT
- Bandingkan gateway NAT dan instans NAT

Gateway NAT

Gateway NAT adalah layanan Network Address Translation (NAT). Anda dapat menggunakan gateway NAT sehingga instans di subnet pribadi dapat terhubung ke layanan di luar VPC Anda tetapi layanan eksternal tidak dapat memulai koneksi dengan instans tersebut.

Ketika Anda membuat gateway NAT, Anda menentukan salah satu dari jenis konektivitas berikut:

- Publik — Instans (Default) di subnet pribadi dapat terhubung ke internet melalui gateway NAT publik, tetapi instans tidak dapat menerima koneksi masuk yang tidak diminta dari internet. Anda membuat gateway NAT publik di subnet publik dan harus mengaitkan alamat IP Elastic dengan gateway NAT saat pembuatan. Anda merutekan lalu lintas dari gateway NAT ke gateway internet untuk VPC. Atau, Anda dapat menggunakan gateway NAT publik untuk terhubung ke VPC lain atau jaringan on-premise Anda. Dalam hal ini, Anda merutekan lalu lintas dari gateway NAT melalui transit gateway atau virtual private gateway.
- Pribadi — Instans di subnet pribadi dapat terhubung ke VPC lain atau jaringan lokal Anda melalui gateway NAT pribadi, tetapi instans tidak dapat menerima koneksi masuk yang tidak diminta dari VPC lain atau jaringan lokal. Anda dapat merutekan lalu lintas dari gateway NAT melalui transit gateway atau virtual private gateway. Anda tidak dapat mengaitkan alamat IP Elastic dengan

gateway NAT pribadi. Anda dapat melampirkan gateway internet ke VPC dengan gateway NAT privat, tetapi jika Anda merutekan lalu lintas dari gateway NAT privat ke gateway internet, gateway internet akan menjatuhkan lalu lintas.

Gateway NAT digunakan dengan lalu lintas IPv4 atau IPv6 (menggunakanDNS64 dan NAT64). Pilihan lain untuk mengaktifkan komunikasi internet khusus keluar melalui IPv6 adalah menggunakan gateway internet khusus keluar. ???

Gerbang NAT pribadi dan publik memetakan alamat IPv4 pribadi sumber dari instance ke alamat IPv4 pribadi dari gateway NAT. Untuk gateway NAT publik, gateway internet kemudian memetakan alamat IPv4 pribadi dari gateway NAT publik ke alamat IP Elastic yang terkait dengan gateway NAT.

Saat mengirim lalu lintas respons ke instance, apakah itu gateway NAT publik atau pribadi, gateway NAT menerjemahkan alamat kembali ke alamat IP sumber asli.

Pertimbangan-pertimbangan

- Koneksi harus selalu dimulai dari dalam VPC yang berisi gateway NAT.
- Anda dapat menggunakan gateway NAT publik atau pribadi untuk merutekan lalu lintas ke gateway transit dan gateway pribadi virtual.
- Jika Anda menggunakan gateway NAT pribadi untuk terhubung ke gateway transit atau gateway pribadi virtual, lalu lintas ke tujuan akan datang dari alamat IP pribadi gateway NAT pribadi.
- Jika Anda menggunakan gateway NAT publik untuk terhubung ke gateway transit atau gateway pribadi virtual, lalu lintas ke tujuan akan datang dari alamat IP pribadi gateway NAT publik. Gateway NAT publik hanya menggunakan alamat IP Elasticnya sebagai alamat IP sumber bila digunakan bersama dengan gateway internet di VPC yang sama.

Daftar Isi

- Dasar gateway NAT
- Bekerja dengan gateway NAT
- Gerbang NAT regional untuk ekspansi multi-AZ otomatis
- Kasus penggunaan gateway NAT
- DNS64 dan NAT64
- Periksa lalu lintas dari gateway NAT
- Pantau gateway NAT dengan Amazon CloudWatch

- Memecahkan masalah gateway NAT
- Harga untuk NAT gateway

Dasar gateway NAT

Setiap gateway NAT dibuat di Availability Zone tertentu dan diimplementasikan dengan redundansi di zona tersebut. Ada kuota jumlah gateway NAT yang dapat Anda buat di setiap Availability Zone. Untuk informasi selengkapnya, lihat Gateway.

Jika Anda memiliki sumber daya di beberapa Zona Ketersediaan dan mereka berbagi satu gateway NAT, dan jika Zona Ketersediaan NAT gateway mati, sumber daya di Zona Ketersediaan lainnya kehilangan akses internet. Untuk meningkatkan ketahanan, buat gateway NAT di setiap Availability Zone, dan konfigurasikan routing Anda untuk memastikan bahwa sumber daya menggunakan gateway NAT di Availability Zone yang sama.

Karakteristik dan aturan berikut berlaku untuk gateway NAT:

- Gateway NAT support protokol berikut: TCP, UDP, dan ICMP.
- Gerbang NAT didukung untuk lalu lintas IPv4 atau IPv6. Untuk lalu lintas IPv6, NAT gateway melakukan NAT64. Dengan menggunakan ini bersama dengan DNS64 (tersedia di resolver Route 53), beban kerja IPv6 Anda di subnet di Amazon VPC dapat berkomunikasi dengan sumber daya IPv4. Layanan IPv4 ini mungkin ada di VPC yang sama (dalam subnet terpisah) atau VPC yang berbeda, di lingkungan lokal Anda atau di internet.
- Gateway NAT mendukung bandwidth 5 Gbps dan secara otomatis menskalakan hingga 100 Gbps. Jika Anda membutuhkan lebih banyak bandwidth, Anda dapat membagi sumber daya Anda menjadi beberapa subnet dan membuat gateway NAT di setiap subnet.
- Sebuah NAT gateway dapat memproses satu juta paket per detik dan secara otomatis menskalakan hingga 10 juta paket per detik. Di luar batas ini, gateway NAT akan menjatuhkan paket. Untuk mencegah kehilangan paket, bagi sumber daya Anda menjadi beberapa subnet dan buat gateway NAT terpisah untuk setiap subnet.
- Setiap alamat IPv4 dapat mendukung hingga 55.000 koneksi simultan ke setiap tujuan unik. Tujuan unik diidentifikasi oleh kombinasi unik alamat IP tujuan, port tujuan, dan protokol (TCP/UDP/ICMP). Anda dapat meningkatkan batas ini dengan mengaitkan hingga 8 alamat IPv4 ke gateway NAT Anda (1 alamat IPv4 primer dan 7 alamat IPv4 sekunder). Anda dibatasi untuk mengaitkan 2 alamat IP Elastic ke gateway NAT publik Anda secara default. Anda dapat meningkatkan batas ini dengan meminta penyesuaian kuota. Untuk informasi selengkapnya, lihat Alamat IP elastis.

- Saat Anda membuat gateway NAT, Anda dapat memilih alamat IPv4 pribadi utama untuk ditetapkan ke gateway NAT. Jika tidak, kami memilih satu atas nama Anda dari rentang alamat IPv4 subnet. Anda tidak dapat mengubah atau menghapus alamat IPv4 pribadi utama. Anda dapat menambahkan alamat IPv4 pribadi sekunder sesuai kebutuhan.
- Anda tidak dapat mengaitkan grup keamanan dengan gateway NAT. Anda dapat mengaitkan grup keamanan ke instans Anda untuk mengontrol lalu lintas masuk dan keluar.
- Kami membuat antarmuka jaringan yang dikelola permintaan untuk gateway NAT Anda. Anda dapat melihat antarmuka jaringan ini menggunakan konsol Amazon EC2. Cari ID gateway NAT dalam deskripsi. Anda dapat menambahkan tag ke antarmuka jaringan, tetapi Anda tidak dapat memodifikasi properti lain dari antarmuka jaringan ini.
- Anda dapat menggunakan ACL jaringan untuk mengontrol lalu lintas ke dan dari subnet untuk gateway NAT Anda. Gateway NAT menggunakan port 1024–65535. Untuk informasi selengkapnya, lihat ACL jaringan.
- Anda tidak dapat merutekan lalu lintas ke gateway NAT melalui koneksi peering VPC. Namun, lalu lintas dari gateway NAT melalui peering VPC ke tujuan di VPC yang diintip mendukung perilaku “Kembali ke Pengirim” - lalu lintas kembali secara otomatis dialihkan kembali ke gateway NAT asal bahkan tanpa rute kembali yang dikonfigurasi di VPC tujuan. Perilaku ini khusus untuk gateway NAT dan tidak berlaku untuk instans EC2 standar. Untuk mencegah hal ini, gunakan NACL untuk memblokir lalu lintas kembali.

  Tidak didukung:

  ```
  Client # Peering # NAT # Internet
  ```

  Didukung:

  ```
  Client # NAT # Peering # Destination
  ```

- Anda tidak dapat merutekan lalu lintas ke gateway NAT dari Site-to-Site VPN atau Direct Connect menggunakan gateway pribadi virtual. Anda dapat merutekan lalu lintas ke gateway NAT dari Site-to-Site VPN atau Direct Connect jika Anda menggunakan gateway transit alih-alih gateway pribadi virtual.
- Gerbang NAT mendukung lalu lintas dengan unit transmisi maksimum (MTU) 8500, tetapi penting untuk dicatat hal-hal berikut:

- MTU koneksi jaringan adalah ukuran, dalam byte, dari paket terbesar yang diizinkan yang dapat dilewatkan melalui koneksi. Semakin besar MTU suatu koneksi, semakin banyak data yang dapat dilewatkan dalam satu paket tunggal.
- Paket yang lebih besar dari 8500 byte yang tiba di gateway NAT dijatuhkan (atau terfragmentasi, jika ada).
- Untuk mencegah potensi kehilangan paket saat berkomunikasi dengan sumber daya melalui internet menggunakan gateway NAT publik, pengaturan MTU untuk instans EC2 Anda tidak boleh melebihi 1500 byte. Untuk informasi selengkapnya tentang memeriksa dan menyetel MTU pada instans, lihat MTU Jaringan untuk instans EC2 Anda di Panduan Pengguna Amazon EC2.
- NAT gateway mendukung Path MTU Discovery (PMTUD) melalui paket FRAG_NEEDED ICMPv4 dan paket ICMPv6 Packet Too Big (PTB).
- Gerbang NAT memberlakukan penjepitan Ukuran Segmen Maksimum (MSS) untuk semua paket. Untuk informasi lebih lanjut, lihat RFC879.

Bekerja dengan gateway NAT

Anda dapat menggunakan konsol Amazon VPC untuk membuat dan mengelola gateway NAT Anda.

Tugas

- Mengontrol penggunaan gateway NAT
- Buat gateway NAT
- Edit asosiasi alamat IP sekunder
- Menandai gateway NAT
- Menghapus gateway NAT
- Ikhtisar baris perintah

Mengontrol penggunaan gateway NAT

Secara default, pengguna tidak memiliki izin untuk bekerja dengan gateway NAT. Anda dapat membuat peran IAM dengan kebijakan terlampir yang memberikan izin kepada pengguna untuk membuat, menjelaskan, dan menghapus gateway NAT. Untuk informasi selengkapnya, lihat Identity and access management untuk Amazon VPC.

Buat gateway NAT

Gunakan prosedur berikut untuk membuat gateway NAT.

Kuota terkait

- Anda tidak akan dapat membuat gateway NAT publik jika Anda telah menghabiskan jumlah alamat IP Elastic yang dialokasikan ke akun Anda. Untuk informasi selengkapnya, lihat Alamat IP elastis.
- Anda dapat menetapkan hingga 8 alamat IPv4 pribadi ke gateway NAT pribadi Anda. Batas ini tidak dapat disesuaikan.
- Anda dibatasi untuk mengaitkan 2 alamat IP Elastic ke gateway NAT publik Anda secara default. Anda dapat meningkatkan batas ini dengan meminta penyesuaian kuota. Untuk informasi selengkapnya, lihat Alamat IP elastis.

Untuk membuat gateway NAT

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih NAT gateway.
3. Pilih Buat gateway NAT.
4. (Opsioonal) Tentukan nama untuk gateway NAT. Tindakan ini akan mebuat tag di mana kuncinya adalah **`Name`** dan nilainya adalah nama yang Anda tentukan.
5. Pilih subnet untuk menciptakan gateway NAT.
6. Untuk Jenis Konektivitas, tinggalkan pilihan Pu blik default untuk membuat gateway NAT publik atau pilih Pribadi untuk membuat gateway NAT pribadi. Untuk informasi selengkapnya tentang perbedaan antara gateway NAT publik dan pribadi, lihatGateway NAT.
7. Jika Anda memilih Pu blik, lakukan hal berikut; jika tidak, lewati ke langkah 8:

    1. Pilih ID alokasi IP Elas tic untuk menetapkan alamat IP Elastic ke gateway NAT atau pilih Alokasikan Elastic IP untuk mengalokasikan secara otomatis satu untuk gateway NAT publik. Anda dibatasi untuk mengaitkan 2 alamat IP Elastic ke gateway NAT publik Anda secara default. Anda dapat meningkatkan batas ini dengan meminta penyesuaian kuota. Untuk informasi selengkapnya, lihat Alamat IP elastis.

        > **Important**
        >
        > Saat Anda menetapkan alamat IP Elastic ke gateway NAT publik, grup perbatasan jaringan EIP harus cocok dengan grup perbatasan jaringan dari Availability Zone (AZ)

tempat Anda meluncurkan gateway NAT publik. Jika tidak sama, gateway NAT akan gagal diluncurkan. Anda dapat melihat grup perbatasan jaringan untuk AZ subnet dengan melihat detail subnet. Demikian pula, Anda dapat melihat grup perbatasan jaringan dari EIP dengan melihat detail alamat EIP. Untuk informasi selengkapnya, lihat 1. Alokasikan sebuah alamat IP Elastis.

2. (Opsional) Pilih Pengaturan tambahan dan, di bawah Alamat IP pribadi - opsional, masukkan alamat IPv4 pribadi untuk gateway NAT. Jika Anda tidak memasukkan alamat, AWS akan secara otomatis menetapkan alamat IPv4 pribadi ke gateway NAT Anda secara acak dari subnet tempat gateway NAT Anda berada.
3. Lewati ke langkah 11.

8. Jika Anda memilih Pri badi, untuk Peng aturan tambahan, metode penetapan alamat IPv4 pribadi, pilih salah satu dari berikut ini:

   - Auto-assign: AWS memilih alamat IPv4 pribadi utama untuk gateway NAT. Untuk Jumlah alamat IPv4 pribadi yang ditetapkan secara otomatis, Anda dapat secara opsional menentukan jumlah alamat IPv4 pribadi sekunder untuk gateway NAT. AWS memilih alamat IP ini secara acak dari subnet untuk gateway NAT Anda.
   - Kustom: Untuk alamat IPv4 pribadi primer, pilih alamat IPv4 pribadi utama untuk gateway NAT. Untuk alamat IPv4 pribadi sekunder, Anda dapat secara opsional menentukan hingga 7 alamat IPv4 pribadi sekunder untuk gateway NAT.

9. Jika Anda memilih K ustom di Langkah 8, lewati langkah ini. Jika Anda memilih Auto-assign, di bawah Jumlah alamat IP pribadi yang ditetapkan secara otomatis, pilih jumlah alamat IPv4 sekunder yang ingin Anda tet AWS apkan ke gateway NAT pribadi ini. Anda dapat memilih hingga 7 alamat IPv4.

   > **Note**
   >
   > Alamat IPv4 sekunder bersifat opsional dan harus ditetapkan atau dialokasikan ketika beban kerja Anda yang menggunakan gateway NAT melebihi 55.000 koneksi bersamaan ke satu tujuan (IP tujuan, port tujuan, dan protokol yang sama). Alamat IPv4 sekunder meningkatkan jumlah port yang tersedia, dan oleh karena itu mereka meningkatkan batas jumlah koneksi bersamaan yang dapat dibuat oleh beban kerja Anda menggunakan gateway NAT.

10. Jika Anda memilih Auto-assign di Langkah 9, lewati langkah ini. Jika Anda memilih Custom, lakukan hal berikut:

1. Di bawah Alamat IPv4 pribadi primer, masukkan alamat IPv4 pribadi.
2. Di bawah Alamat IPv4 pribadi sekunder, masukkan hingga 7 alamat IPv4 pribadi sekunder.

11. (Opsional) Untuk menambahkan tag ke gateway NAT, pilih Tambahkan tag baru dan masukkan nama kunci dan nilai. Anda dapat menambahkan hingga 50 tag.
12. Pilih Buat gateway NAT.
13. Status awal gateway NAT adalah `Pending`. Setelah perubahan status `Available`, gateway NAT siap digunakan. Pastikan untuk memperbarui tabel rute Anda sesuai kebutuhan. Sebagai contoh, lihat the section called “Kasus penggunaan”.

Jika status gateway NAT berubah menjadi `Failed`, ada kesalahan selama pembuatan. Untuk informasi selengkapnya, lihat Pembuatan gateway NAT gagal.

Edit asosiasi alamat IP sekunder

Setiap alamat IPv4 dapat mendukung hingga 55.000 koneksi simultan ke setiap tujuan unik. Tujuan unik diidentifikasi oleh kombinasi unik alamat IP tujuan, port tujuan, dan protokol (TCP/UDP/ICMP). Anda dapat meningkatkan batas ini dengan mengaitkan hingga 8 alamat IPv4 ke gateway NAT Anda (1 alamat IPv4 primer dan 7 alamat IPv4 sekunder). Anda dibatasi untuk mengaitkan 2 alamat IP Elastic ke gateway NAT publik Anda secara default. Anda dapat meningkatkan batas ini dengan meminta penyesuaian kuota. Untuk informasi selengkapnya, lihat Alamat IP elastis.

Anda dapat menggunakan CloudWatch metrik NAT gateway ErrorPortAllocation dan PacketsDropCount untuk menentukan apakah gateway NAT Anda menghasilkan kesalahan alokasi port atau menjatuhkan paket. Untuk mengatasi masalah ini, tambahkan alamat IPv4 sekunder ke gateway NAT Anda.

Pertimbangan-pertimbangan

- Anda dapat menambahkan alamat IPv4 pribadi sekunder saat membuat gateway NAT pribadi atau setelah Anda membuat gateway NAT menggunakan prosedur di bagian ini. Anda dapat menambahkan alamat IP Elastic ke gateway NAT publik hanya setelah Anda membuat gateway NAT dengan menggunakan prosedur di bagian ini.
- Gateway NAT Anda dapat memiliki hingga 8 alamat IPv4 yang terkait dengannya (1 alamat IPv4 primer dan 7 alamat IPv4 sekunder). Anda dapat menetapkan hingga 8 alamat IPv4 pribadi ke gateway NAT pribadi Anda. Anda dibatasi untuk mengaitkan 2 alamat IP Elastic ke gateway NAT publik Anda secara default. Anda dapat meningkatkan batas ini dengan meminta penyesuaian kuota. Untuk informasi selengkapnya, lihat Alamat IP elastis.

Untuk mengedit asosiasi alamat IPv4 sekunder

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih NAT gateway.
3. Pilih gateway NAT yang asosiasi alamat IPv4 sekundernya ingin Anda edit.
4. Pilih T ind akan, lalu pilih Edit asosiasi alamat IP sekunder.
5. Jika Anda mengedit asosiasi alamat IPv4 sekunder dari gateway NAT pribadi, di bawah Tindakan, pilih Tet apkan alamat IPv4 baru atau Batalkan penetapan alamat IPv4 yang ada. Jika Anda mengedit asosiasi alamat IPv4 sekunder dari gateway NAT publik, di bawah Tindakan, pilih Meng aitkan alamat IPv4 baru atau Putuskan hubungan alamat IPv4 yang ada.
6. Lakukan salah satu tindakan berikut:

   - Jika Anda memilih untuk menetapkan atau mengaitkan alamat IPv4 baru, lakukan hal berikut:

     1. Langkah ini diperlukan. Anda harus memilih alamat IPv4 pribadi. Pilih metode penetapan alamat IPv4 pribadi:

        - Auto-assign: AWS secara otomatis memilih alamat IPv4 pribadi primer dan Anda memilih apakah Anda ingin menetapkan AWS hingga 7 alamat IPv4 pribadi sekunder untuk ditetapkan ke gateway NAT. AWS secara otomatis memilih dan menetapkannya untuk Anda secara acak dari subnet tempat gateway NAT Anda berada.
        - Kustom: Pilih alamat IPv4 pribadi utama dan hingga 7 alamat IPv4 pribadi sekunder untuk ditetapkan ke gateway NAT.

     2. Di bawah ID alokasi IP elastis, pilih alamat IP Elastic untuk ditambahkan dengan alamat IPv4 sekunder. Langkah ini diperlukan. Anda harus memilih alamat IP Elastic bersama dengan alamat IPv4 pribadi. Jika Anda memilih Custom untuk metode penetapan alamat IP Pribadi, Anda juga harus memasukkan alamat IPv4 pribadi untuk setiap alamat IP Elastic yang Anda tambahkan.

        > **Important**
        >
        > Saat Anda menetapkan EIP sekunder ke gateway NAT publik, grup perbatasan jaringan EIP harus cocok dengan grup perbatasan jaringan dari Availability Zone (AZ) tempat gateway NAT publik berada. Jika tidak sama, EIP akan gagal menetapkan. Anda dapat melihat grup perbatasan jaringan untuk AZ subnet dengan melihat detail subnet. Demikian pula, Anda dapat melihat grup perbatasan jaringan

dari EIP dengan melihat detail alamat EIP. Untuk informasi selengkapnya, lihat 1. Alokasikan sebuah alamat IP Elastis.

Gateway NAT Anda dapat memiliki hingga 8 alamat IP yang terkait dengannya. Jika ini adalah gateway NAT publik, ada batas kuota default untuk alamat IP Elastic per Wilayah. Untuk informasi selengkapnya, lihat Alamat IP elastis.

- Jika Anda memilih untuk membatalkan penetapan atau memisahkan alamat IPv4 baru, selesaikan hal berikut ini:
  1. Di bawah Alamat IP sekunder yang ada untuk dibatalkan penet apan, pilih alamat IP sekunder yang ingin Anda batalkan tetapannya.
  2. (opsional) Di bawah Durasi pembuangan koneksi, masukkan jumlah waktu maksimum untuk menunggu (dalam detik) sebelum melepaskan alamat IP secara paksa jika koneksi masih berlangsung. Jika Anda tidak memasukkan nilai, nilai defaultnya adalah 350 detik.

7. Pilih Simpan perubahan.

Jika status gateway NAT berubah menjadi `Failed`, ada kesalahan selama pembuatan. Untuk informasi selengkapnya, lihat Pembuatan gateway NAT gagal.

Menandai gateway NAT

Anda dapat menandai gateway NAT Anda untuk membantu mengidentifikasi atau mengkategorikannya sesuai dengan kebutuhan organisasi Anda. Untuk informasi tentang bekerja dengan tag, lihat Men andai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

Tag alokasi biaya didukung untuk gateway NAT. Oleh karena itu, Anda juga dapat menggunakan tag untuk mengatur AWS tagihan Anda dan mencerminkan struktur biaya Anda sendiri. Untuk informasi selengkapnya, lihat Menggunakan tanda alokasi biaya dalam Panduan Pengguna AWS Billing . Untuk informasi selengkapnya tentang menyiapkan laporan alokasi biaya dengan tag, lihat Laporan alokasi biaya bulanan di Tentang Penagihan AWS Akun.

Untuk menandai gateway NAT

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih NAT gateway.
3. Pilih gateway NAT yang ingin Anda tag dan pilih Tind akan. Kemudian pilih Kelola tag.

4. Pilih Tambahkan tag baru, dan tentukan Kunci dan Nilai untuk tag. Anda dapat menambahkan hingga 50 tag.
5. Pilih Simpan.

Menghapus gateway NAT

Jika Anda tidak lagi memerlukan gateway NAT, Anda dapat menghapusnya. Setelah Anda menghapus gateway NAT, entri tetap terlihat di konsol Amazon VPC selama sekitar satu jam, setelah itu otomatis dihapus. Anda tidak dapat menghapus entri ini sendiri.

Menghapus gateway NAT akan memisahkan alamat IP Elastis-nya, tetapi tidak melepaskan alamat dari akun Anda. Jika Anda menghapus gateway NAT, rute gateway NAT tetap dalam keadaan `blackhole` sampai Anda menghapus atau memperbarui rute.

Untuk menghapus gateway NAT

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih NAT gateway.
3. Pilih tombol radio untuk gateway NAT, lalu pilih Tindakan, Hapus gateway NAT.
4. Saat diminta konfirmasi, masukkan **`delete`**, lalu pilih Hapus.
5. Jika Anda tidak lagi memerlukan alamat IP Elastis yang terkait dengan gateway NAT publik, kami sarankan Anda melepaskannya. Untuk informasi selengkapnya, lihat 5. Melepas alamat IP Elastis.

Ikhtisar baris perintah

Anda dapat melakukan tugas yang dijelaskan pada halaman ini menggunakan baris perintah.

Menetapkan alamat IPv4 pribadi ke gateway NAT pribadi

- tetapkan alamat-pribadi-nat-gateway-address () AWS CLI
- Register-EC2PrivateNatGatewayAddress (AWS Tools for Windows PowerShell)

Mengaitkan alamat IP Elastic dan alamat IPv4 pribadi dengan gateway NAT publik

- alamat gerbang asosiasi-nat-nat-() AWS CLI
- Register-EC2NatGatewayAddress (AWS Tools for Windows PowerShell)

Buat gateway NAT

- create-nat-gateway (AWS CLI)
- New-EC2NatGateway (AWS Tools for Windows PowerShell)

Menghapus gateway NAT

- delete-nat-gateway (AWS CLI)
- Remove-EC2NatGateway (AWS Tools for Windows PowerShell)

Menjelaskan gateway NAT

- menjelaskan-nat-gateway (AWS CLI)
- Get-EC2NatGateway (AWS Tools for Windows PowerShell)

Memisahkan alamat IP Elastis sekunder dari gateway NAT publik

- pisahkan alamat gateway-nat-nat-() AWS CLI
- Unregister-EC2NatGatewayAddress (AWS Tools for Windows PowerShell)

Menandai gateway NAT

- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)

Menghapus alamat IPv4 sekunder dari gateway NAT pribadi

- hapus alamat gerbang pribadi-nat-nat-alamat () AWS CLI
- Unregister-EC2PrivateNatGatewayAddress (AWS Tools for Windows PowerShell)

Gerbang NAT regional untuk ekspansi multi-AZ otomatis

Gunakan gateway NAT regional saat Anda ingin menyederhanakan arsitektur jaringan, meningkatkan postur keamanan, dan mengonfigurasi ketersediaan tinggi secara default. Gateway NAT regional secara otomatis diperluas di seluruh Availability Zone berdasarkan keberadaan beban kerja Anda.

Tidak seperti gateway NAT standar (disebut sebagai gateway NAT zonal), yang beroperasi di Zona Ketersediaan tunggal, gateway NAT regional mengikuti beban kerja Anda untuk memberikan ketersediaan tinggi otomatis.

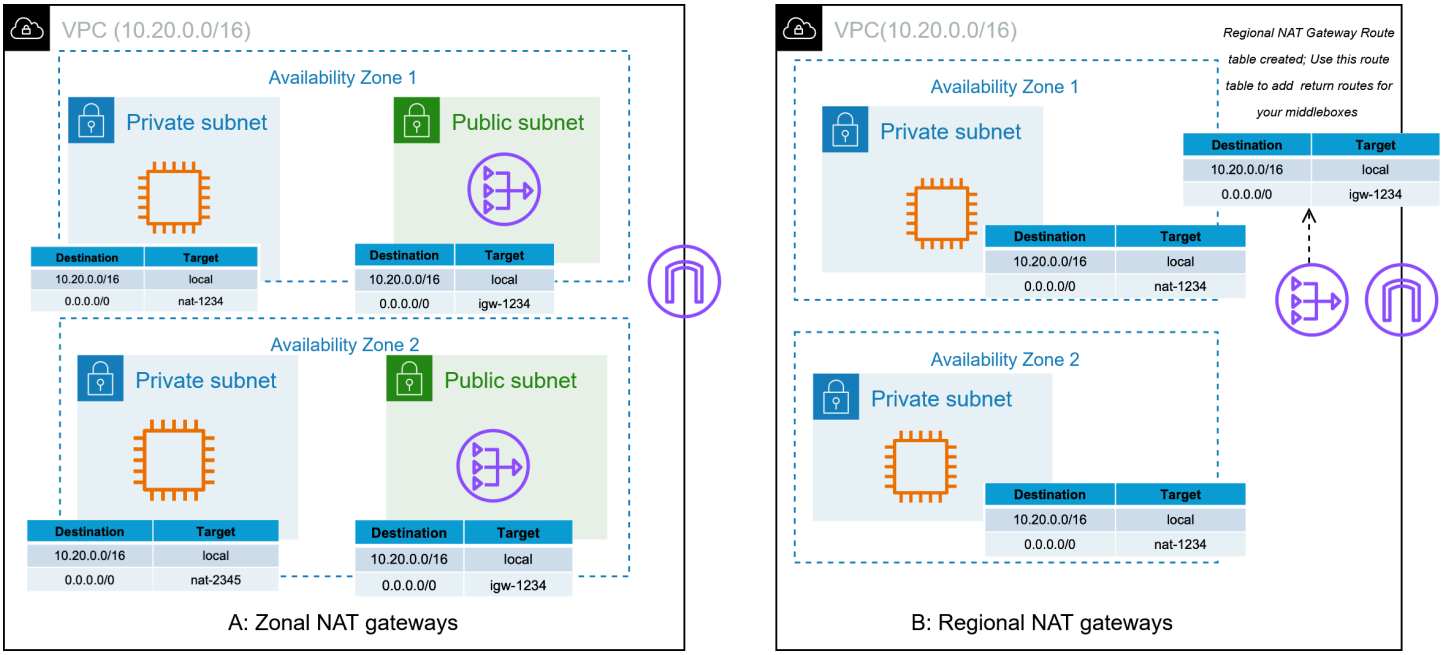


Diagram A di sebelah kiri mewakili pengaturan saat ini dengan NAT Gateway zonal. Pertama-tama Anda membuat Gerbang NAT zonal per Zona Ketersediaan dan meng-host NAT Anda di subnet publik. Anda kemudian mengonfigurasi rute terpisah per Zona Ketersediaan dari subnet pribadi Anda ke NAT di Zona Ketersediaan tersebut. Anda mengulangi langkah ini setiap kali beban kerja Anda diperluas ke Zona Ketersediaan baru, untuk ketersediaan tinggi. Selain itu, Anda perlu menambahkan rute untuk gateway internet di tabel rute subnet NAT Anda per Availability Zone.

Di sisi lain, dengan NAT Gateway regional, Anda tidak perlu membuat subnet publik untuk meng-hostingnya. Anda juga tidak perlu membuat dan menghapus NAT Gateway dan mengedit tabel rute setiap kali beban kerja Anda diperluas ke Zona Ketersediaan baru. Sebagai gantinya, Anda cukup membuat NAT Gateway dengan mode regional, memilih VPC Anda, dan secara otomatis memperluas dan berkontraksi di semua AZ berdasarkan keberadaan beban kerja Anda untuk menawarkan ketersediaan tinggi. Seperti yang ditunjukkan pada diagram B, Anda dapat merutekan lalu lintas dari sumber daya Anda di subnet pribadi di semua AZ ke ID Gateway NAT regional tunggal ini, atau menggunakan tabel rute yang sama di seluruh subnet di AZ Anda untuk melakukan terjemahan alamat jaringan. Setelah Anda membuat NAT Gateway regional Anda, AWS secara otomatis membuat tabel rute untuknya, yang dilengkapi dengan rute pra-konfigurasi ke gateway internet. Anda dapat menggunakan tabel rute ini untuk menambahkan rute kembali ke kotak tengah Anda.

Manfaat

Gerbang NAT regional memberikan manfaat berikut:

- Pengaturan yang disederhanakan — Gunakan satu NAT ID di semua Availability Zone yang memiliki antarmuka jaringan, sehingga Anda dapat menggunakan entri rute yang sama untuk subnet di Zona Ketersediaan yang berbeda.
- Keamanan yang ditingkatkan - Tidak diperlukan subnet publik. NAT Gateway regional adalah sumber daya mandiri dengan tabel rute sendiri dan Anda tidak memerlukan subnet publik di VPC Anda untuk meng-host NAT Gateway regional, yang mengurangi kemungkinan salah konfigurasi sumber daya pribadi di subnet dengan konektivitas publik.
- Ketersediaan tinggi otomatis — Secara otomatis memperluas dan mengontraksi dengan jejak beban kerja Anda untuk mempertahankan afinitas zona yang memberikan ketersediaan tinggi secara default.
- Batas port dan IP yang lebih tinggi — Gerbang NAT regional Anda mendukung hingga 32 alamat IP per Zona Ketersediaan (dibandingkan dengan 8 untuk gateway NAT zonal). Setiap alamat IP meningkatkan batas koneksi bersamaan ke tujuan populer (diidentifikasi oleh kombinasi unik IP tujuan, port tujuan, dan protokol) sebesar 55.000.

Kapan menggunakan gateway NAT regional

Pertimbangkan untuk menggunakan Regional NAT Gateway untuk semua kasus penggunaan kecuali yang memerlukan konektivitas pribadi. Gerbang NAT Regional tidak menawarkan konektivitas pribadi dan sebaiknya gunakan NAT Gateway Anda dalam mode ketersediaan zona untuk kasus penggunaan NAT pribadi.

Cara kerja gateway NAT regional

Saat Anda meluncurkan sumber daya di Zona Ketersediaan baru, gateway NAT regional mendeteksi keberadaan antarmuka jaringan (ENI) di Zona Ketersediaan tersebut dan secara otomatis memperluas ke zona tersebut. Demikian pula, NAT Gateway mengontrak dari Availability Zone yang tidak memiliki beban kerja aktif.

Gerbang NAT regional Anda mungkin memerlukan waktu hingga 60 menit untuk memperluas ke Zona Ketersediaan baru setelah sumber daya dibuat di sana. Sampai ekspansi ini selesai, lalu lintas yang relevan dari sumber daya ini diproses di seluruh zona oleh NAT Gateway regional Anda di salah satu Zona Ketersediaan yang ada.

Gateway NAT regional mendukung dua mode:

- Mode otomatis - Dalam mode ini, AWS secara otomatis mengelola alamat IP dan perluasan Zona Ketersediaan (disarankan). Jika Anda ingin menggunakan alamat IP Anda sendiri dalam mode ini dan menggunakan Amazon VPC IPAM, lihat Men entukan strategi alokasi IPv4 publik dengan kebijakan IPAM di Panduan Pengguna Amazon VPC IPAM.
- Mode manual — Dalam mode ini, Anda mengelola alamat IP secara manual dan mengontrol terjemahan alamat jaringan untuk setiap Zona Ketersediaan. Dalam mode manual, Anda bertanggung jawab untuk memperluas dan mengontrak gateway NAT Anda di seluruh Availability Zone.

> **Important**
>
> Gerbang NAT regional mendukung AWS Transit Gateway sebagai rute yang valid di tabel rute gateway NAT regional. Gerbang NAT regional tidak mendukung NAT pribadi. Jika Anda membutuhkan NAT pribadi, gunakan gateway NAT zonal sebagai gantinya. Gerbang NAT regional tidak didukung di Zona Ketersediaan terbatas.

Harga

Untuk informasi harga, lihat Harga Amazon VPC.

Buat gateway NAT regional

Menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih NAT gateway.
3. Pilih Buat gateway NAT.
4. Untuk mode Ketersediaan, pilih Regional. Anda tidak perlu menentukan subnet apa pun saat memilih ketersediaan regional
5. Pilih VPC.
6. Lengkapi konfigurasi yang tersisa dan pilih Buat gateway NAT.

Menggunakan AWS CLI

Buat gateway NAT regional

```
aws ec2 create-nat-gateway --vpc-id vpc-12345678 --availability-mode regional
```

Lihat detail NAT gateway

```
aws ec2 describe-nat-gateways --nat-gateway-ids nat-12345678
```

Tambahkan alamat IP (mode manual)

```
aws ec2 associate-nat-gateway-address --nat-gateway-id nat-12345678 --availability-zone
 us-east-1b --allocation-ids eipalloc-12345678
```

Hapus alamat IP

```
aws ec2 disassociate-nat-gateway-address --nat-gateway-id nat-12345678 --association-
ids eipassoc-12345678
```

Menghapus gateway NAT regional

```
aws ec2 delete-nat-gateway --nat-gateway-id nat-12345678
```

Konversi dari gateway NAT zonal ke regional

> **Important**
>
> Ini akan mengatur ulang koneksi Anda yang ada. Kami menyarankan Anda menyelesaikan langkah-langkah ini di jendela pemeliharaan Anda.

Anda dapat mengonversi gateway NAT zonal yang ada ke gateway NAT regional menggunakan salah satu dari dua pendekatan:

Jika Anda setuju dengan menggunakan NAT Gateway regional dengan alamat IP baru:

1. Buat gateway NAT regional baru
2. Perbarui tabel rute untuk menunjuk ke gateway NAT regional
3. Hapus gateway NAT zonal lama

Pendekatan ini menggunakan alamat IP baru dan mengatur ulang koneksi yang ada saat rute diperbarui.

Jika Anda ingin menggunakan kembali alamat IP yang ada dengan NAT Gateway regional:

1. Hapus gateway NAT zonal yang ada untuk merilis alamat IP mereka
2. Buat gateway NAT regional menggunakan alamat IP yang dirilis
3. Perbarui tabel rute untuk menunjuk ke gateway NAT regional

Pendekatan ini mempertahankan alamat IP tetapi memerlukan jendela pemeliharaan karena lalu lintas terganggu selama transisi.

Kasus penggunaan gateway NAT

Berikut ini adalah contoh kasus penggunaan untuk gateway NAT publik dan privat.

Skenario

- Mengakses internet dari subnet privat
- Akses jaringan Anda menggunakan alamat IP yang terdaftar diizinkan
- Aktifkan komunikasi antara jaringan yang tumpang tindih

Mengakses internet dari subnet privat

Anda dapat menggunakan gateway NAT publik untuk mengaktifkan instance di subnet pribadi untuk mengirim lalu lintas keluar ke internet, sambil mencegah internet membuat koneksi ke instans.

Daftar Isi

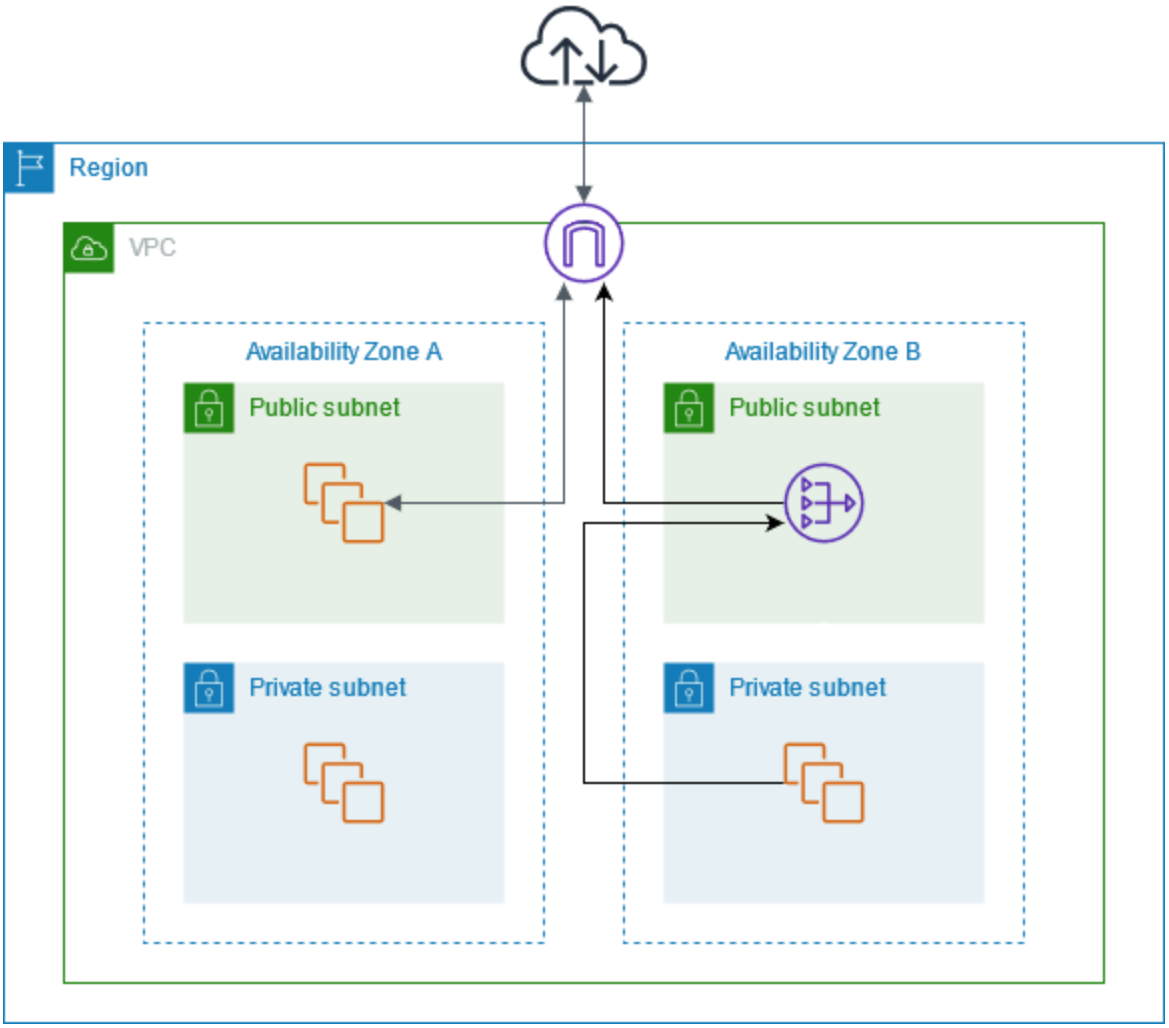
- Gambaran umum
- Perutean
- Uji gateway NAT publik

Gambaran umum

Diagram berikut menggambarkan kasus penggunaan ini. Ada dua Zona Ketersediaan, dengan dua subnet di setiap Zona Ketersediaan. Tabel rute untuk setiap subnet menentukan bagaimana lalu lintas dirutekan. Di Availability Zone A, instance di subnet publik dapat mencapai internet melalui

rute ke gateway internet, sedangkan instance di subnet pribadi tidak memiliki rute ke internet. Di Availability Zone B, subnet publik berisi gateway NAT, dan instance di subnet pribadi dapat mencapai internet melalui rute ke gateway NAT di subnet publik.

Gerbang NAT pribadi dan publik memetakan alamat IPv4 pribadi sumber dari instance ke alamat IPv4 pribadi dari gateway NAT pribadi, tetapi dalam kasus gateway NAT publik, gateway internet kemudian memetakan alamat IPv4 pribadi dari gateway NAT publik ke alamat IP Elastic yang terkait dengan gateway NAT. Saat mengirim lalu lintas respons ke instance, apakah itu gateway NAT publik atau pribadi, gateway NAT menerjemahkan alamat kembali ke alamat IP sumber asli.



Perhatikan bahwa jika instance di subnet pribadi di Availability Zone A juga perlu menjangkau internet, Anda dapat membuat rute dari subnet ini ke gateway NAT di Availability Zone B. Atau, Anda dapat meningkatkan ketahanan dengan membuat gateway NAT di setiap Availability Zone yang berisi sumber daya yang memerlukan akses internet. Untuk contoh diagram, lihatthe section called “Server pribadi”.

Perutean

Berikut ini adalah tabel rute yang terkait dengan subnet publik di Availability Zone A. Entri pertama adalah rute lokal; ini memungkinkan instans di subnet untuk berkomunikasi dengan instans lain di VPC menggunakan alamat IP pribadi. Entri kedua mengirimkan semua lalu lintas subnet lainnya ke gateway internet, yang memungkinkan instans di subnet untuk mengakses internet.

Tujuan	Target
VPC CIDR	lokal
0.0.0. 0/0	*internet-gateway-id*

Berikut ini adalah tabel rute yang terkait dengan subnet pribadi di Availability Zone A. Entri adalah rute lokal, yang memungkinkan instans di subnet berkomunikasi dengan instans lain di VPC menggunakan alamat IP pribadi. Instans di subnet ini tidak memiliki akses ke internet.

Tujuan	Target
VPC CIDR	lokal

Berikut ini adalah tabel rute yang terkait dengan subnet publik di Availability Zone B. Entri pertama adalah rute lokal, yang memungkinkan instans di subnet berkomunikasi dengan instans lain di VPC menggunakan alamat IP pribadi. Entri kedua mengirimkan semua lalu lintas subnet lainnya ke gateway internet, yang memungkinkan gateway NAT di subnet untuk mengakses internet.

Tujuan	Target
VPC CIDR	lokal
0.0.0. 0/0	*internet-gateway-id*

Berikut ini adalah tabel rute yang terkait dengan subnet pribadi di Availability Zone B. Entri pertama adalah rute lokal; ini memungkinkan instance di subnet untuk berkomunikasi dengan instance lain di VPC menggunakan alamat IP pribadi. Entri kedua mengirimkan semua lalu lintas subnet lainnya ke gateway NAT.

Tujuan	Target
VPC CIDR	lokal
0.0.0. 0/0	*nat-gateway-id*

Untuk informasi selengkapnya, lihat the section called “Kelola tabel rute subnet”.

Uji gateway NAT publik

Setelah Anda membuat gateway NAT dan memperbarui tabel rute, Anda dapat mengirimkan ping alamat jarak jauh di internet dari sebuah instans di subnet privat untuk menguji apakah perangkat tersebut dapat tersambung ke internet. Untuk contoh cara melakukannya, lihat Menguji koneksi internet.

Jika Anda dapat terhubung ke internet, Anda juga dapat menguji apakah lalu lintas internet dirutekan melalui gateway NAT:

- Melacak rute lalu lintas dari sebuah instans di subnet privat Anda. Untuk melakukannya, jalankan perintah `traceroute` dari instans Linux di subnet privat Anda. Dalam output, Anda harus melihat alamat IP privat gateway NAT di salah satu hop (biasanya hop pertama).
- Gunakan situs web atau alat pihak ke tiga yang menampilkan alamat IP sumber saat Anda tersambung dari instans di subnet privat Anda. Alamat IP sumber harus alamat IP elastis dari gateway NAT.

Jika percobaan ini gagal, lihat Memecahkan masalah gateway NAT.

Menguji koneksi internet

Contoh berikut menunjukkan cara untuk menguji apakah sebuah instans di subnet privat dapat terhubung ke internet.

1. Luncurkan sebuah instans di subnet publik Anda (gunakan ini sebagai host bastion). Pada lauch wizard, pastikan bahwa Anda memilih Amazon Linux AMI, dan menetapkan alamat IP publik untuk instans Anda.

   Pastikan aturan grup keamanan Anda mengizinkan lalu lintas SSH masuk dari kisaran alamat IP untuk jaringan lokal Anda, dan lalu lintas SSH keluar ke rentang alamat IP subnet pribadi

Anda. Anda juga dapat menggunakan `0.0.0.0/0` untuk lalu lintas SSH masuk dan keluar untuk pengujian ini.

2. Luncurkan sebuah instans di subnet privat Anda. Dalam launch wizard, pastikan bahwa Anda memilih Amazon Linux AMI. Jangan menetapkan alamat IP publik ke instans Anda. Pastikan bahwa aturan grup keamanan Anda mengizinkan lalu lintas SSH masuk dari alamat IP privat instans Anda yang diluncurkan di subnet publik, dan semua lalu lintas ICMP keluar. Anda harus memilih pasangan kunci yang sama yang Anda gunakan untuk meluncurkan instans Anda di subnet publik.
3. Mengkonfigurasi SSH agent forwarding pada komputer lokal Anda, dan terhubung ke host bastion Anda di subnet publik. Untuk informasi selengkapnya, lihat Untuk mengkonfigurasi SSH agent forwarding untuk Linux atau macOS atau Untuk mengkonfigurasi penerusan agen SSH untuk Windows.
4. Dari host bastion Anda, terhubung ke instans Anda di subnet privat, dan kemudian menguji koneksi internet dari instans Anda di subnet privat. Untuk informasi selengkapnya, lihat Untuk menguji koneksi internet.

Untuk mengkonfigurasi SSH agent forwarding untuk Linux atau macOS

1. Dari mesin lokal Anda, tambahkan kunci privat Anda ke agen autentikasi.

   Untuk Linux, gunakan perintah berikut.

   ```
   ssh-add -c mykeypair.pem
   ```

   Untuk macOS, gunakan perintah berikut.

   ```
   ssh-add -K mykeypair.pem
   ```

2. Connect ke instans Anda di subnet publik menggunakan pilihan `-A` untuk mengaktifkan SSH agent forwarding, dan menggunakan alamat publik instans, seperti yang ditunjukkan dalam contoh berikut.

   ```
   ssh -A ec2-user@54.0.0.123
   ```

Untuk mengkonfigurasi penerusan agen SSH untuk Windows

Anda dapat menggunakan klien OpenSSH yang tersedia di Windows, atau menginstal klien SSH pilihan Anda (misalnya, PuTTY).

OpenSSH

Instal OpenSSH untuk Windows seperti yang dijelaskan dalam artikel ini: Mem ulai dengan OpenSSH untuk Windows. Kemudian tambahkan kunci Anda ke agen otentikasi. Untuk informasi selengkapnya, lihat Key-based otentikasi di OpenSSH untuk Windows.

PuTTY

1. Unduh dan instal Pageant dari halaman pengunduhan PuTTY, jika belum diinstal.
2. Ubah kunci privat Anda ke format .ppk. Untuk informasi selengkapnya, lihat Mengonversi kunci pribadi Anda menggunakan PuttyGen di Panduan Pengguna Amazon EC2.
3. Mulai Pageant, buka menu konteks untuk ikon Kontes di bilah tugas (mungkin tersembunyi), dan pilih Tam bah Kunci. Pilih file .ppk yang Anda buat, masukkan frasa sandi jika perlu, dan pilih Buka.
4. Mulai sesi PuTTY dan hubungkan ke instans Anda di subnet publik menggunakan alamat IP publiknya. Untuk informasi selengkapnya, lihat Menghubungkan ke instance Linux menggunakan PuTTY. Di Kategori Autentikasi, pastikan bahwa Anda memilih pilihan Izinkan agent forwarding, dan biarkan kotak File kunci privat untuk autentikasi tetap kosong.

Untuk menguji koneksi internet

1. Dari instans Anda di subnet publik, hubungkan ke instans Anda di subnet privat Anda dengan menggunakan alamat IP privat seperti yang ditunjukkan dalam instans berikut.

```
ssh ec2-user@10.0.1.123
```

2. Dari instans pribadi Anda, uji bahwa Anda dapat terhubung ke internet dengan menjalankan perintah `ping` untuk situs web yang memiliki ICMP diaktifkan.

```
ping ietf.org
```

```
PING ietf.org (4.31.198.44) 56(84) bytes of data.
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=1 ttl=47 time=86.0 ms
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=2 ttl=47 time=75.6 ms
...
```

Tekan Ctrl+C pada keyboard Anda untuk membatalkan perintah `ping`. Jika perintah `ping` gagal, lihat Instans tidak dapat mengakses internet.

3. (Opsioonal) Jika Anda tidak lagi memerlukan instans Anda, hentikan. Untuk informasi selengkapnya, lihat Menghentikan instans Anda di Panduan Pengguna Amazon EC2.

Akses jaringan Anda menggunakan alamat IP yang terdaftar diizinkan

Anda dapat menggunakan gateway NAT pribadi untuk mengaktifkan komunikasi dari VPC ke jaringan lokal menggunakan kumpulan alamat yang terdaftar diizinkan.

Alih-alih menetapkan setiap instans alamat IP terpisah dari rentang yang terdaftar diizinkan, Anda dapat merutekan lalu lintas dari subnet melalui gateway NAT pribadi dengan alamat IP dari rentang yang terdaftar diizinkan.

Daftar Isi

- Gambaran umum
- Sumber daya
- Perutean

Gambaran umum

Diagram berikut menunjukkan bagaimana instance dapat mengakses sumber daya lokal melalui Site-to-Site VPN. Lalu lintas dari instans dialihkan ke gateway pribadi virtual, melalui koneksi VPN, ke gateway pelanggan, dan kemudian ke tujuan di jaringan lokal. Namun, misalkan tujuan mengizinkan lalu lintas hanya dari rentang alamat IP tertentu, seperti 100.64.1. 0/28. Ini akan mencegah lalu lintas dari instans ini mencapai jaringan lokal.

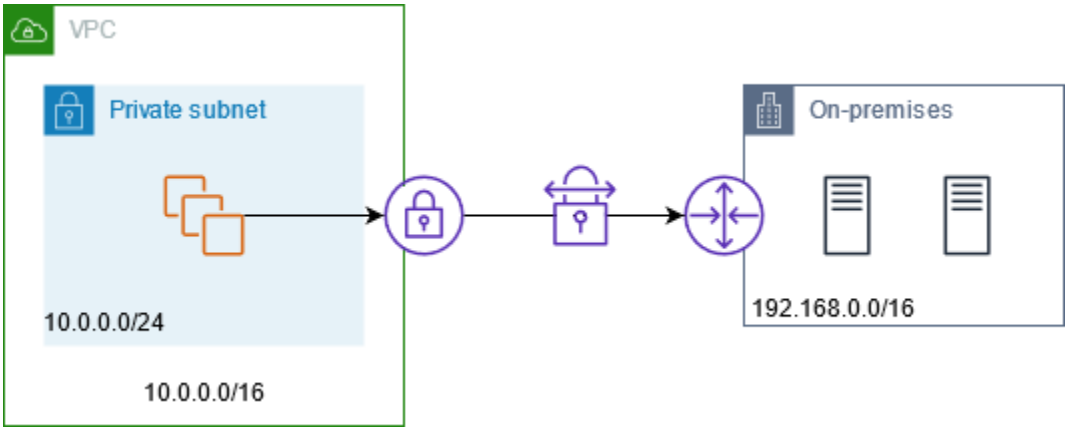
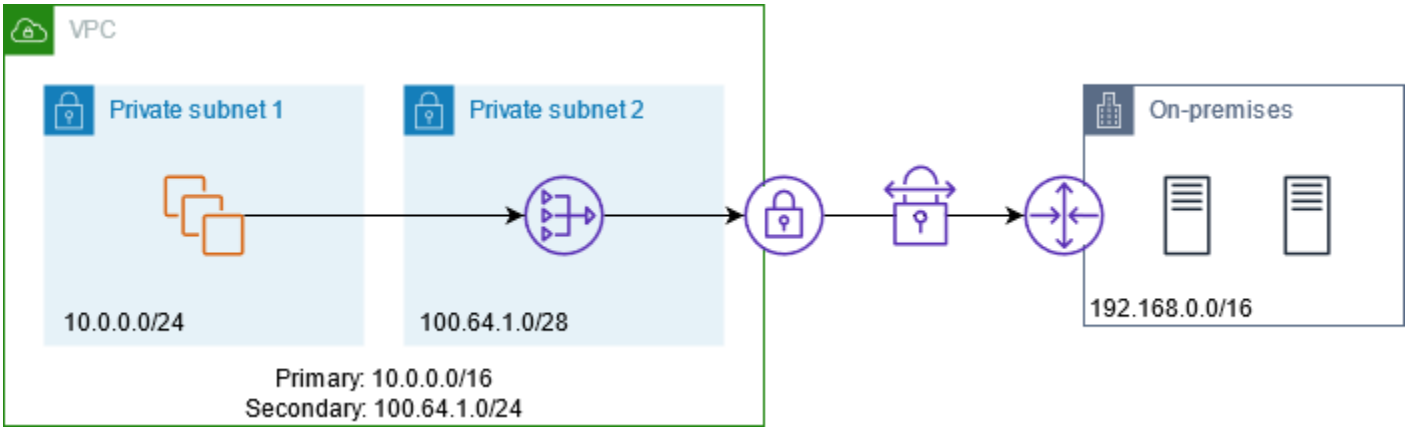


Diagram berikut menunjukkan komponen kunci konfigurasi untuk skenario ini. VPC memiliki rentang alamat IP asli ditambah rentang alamat IP yang diizinkan. VPC memiliki subnet dari rentang alamat IP yang diizinkan dengan gateway NAT pribadi. Lalu lintas dari instans yang ditujukan untuk jaringan lokal dikirim ke gateway NAT sebelum dialihkan ke koneksi VPN. Jaringan lokal menerima lalu lintas dari instance dengan alamat IP sumber gateway NAT, yang berasal dari rentang alamat IP yang diizinkan.



Sumber daya

Buat atau perbarui sumber daya sebagai berikut:

- Kaitkan rentang alamat IP yang diizinkan dengan VPC.
- Buat subnet di VPC dari rentang alamat IP yang diizinkan.
- Buat gateway NAT pribadi di subnet baru.
- Perbarui tabel rute untuk subnet dengan instans untuk mengirim lalu lintas yang ditujukan untuk jaringan lokal ke gateway NAT. Tambahkan rute ke tabel rute untuk subnet dengan gateway NAT pribadi yang mengirimkan lalu lintas yang ditujukan untuk jaringan lokal ke gateway pribadi virtual.

Perutean

Berikut ini adalah tabel rute yang terkait dengan subnet pertama. Ada rute lokal untuk setiap VPC CIDR. Rute lokal memungkinkan sumber daya di subnet untuk berkomunikasi dengan sumber daya lain di VPC menggunakan alamat IP pribadi. Entri ketiga mengirimkan lalu lintas yang ditujukan untuk jaringan lokal ke gateway NAT pribadi.

Tujuan	Target
10.0.0.0/16	lokal

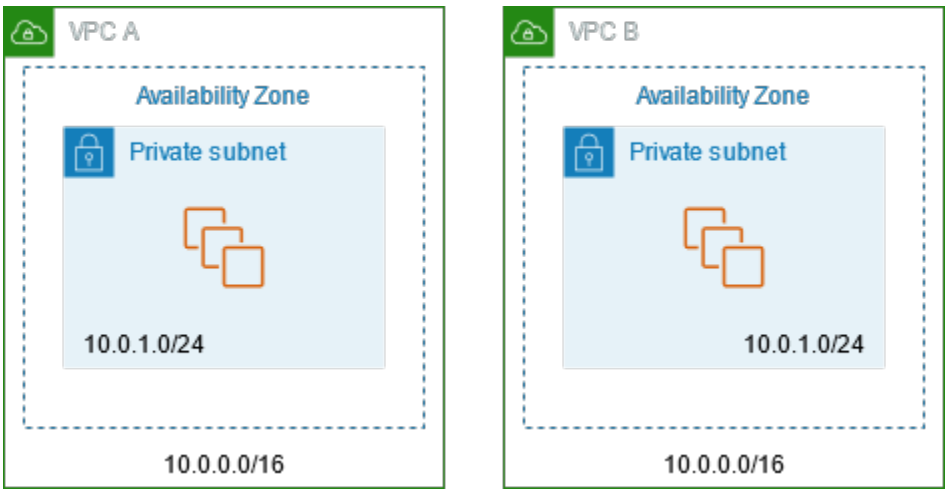
Tujuan	Target
100.64.1.0/24	lokal
192.168.0.0/16	*nat-gateway-id*

Berikut ini adalah tabel rute yang terkait dengan subnet kedua. Ada rute lokal untuk setiap VPC CIDR. Rute lokal memungkinkan sumber daya di subnet untuk berkomunikasi dengan sumber daya lain di VPC menggunakan alamat IP pribadi. Entri ketiga mengirimkan lalu lintas yang ditujukan untuk jaringan lokal ke gateway pribadi virtual.

Tujuan	Target
10.0.0.0/16	lokal
100.64.1.0/24	lokal
192.168.0.0/16	*vgw-id*

Aktifkan komunikasi antara jaringan yang tumpang tindih

Anda dapat menggunakan gateway NAT pribadi untuk mengaktifkan komunikasi antar jaringan meskipun mereka memiliki rentang CIDR yang tumpang tindih. Misalnya, contoh di VPC A perlu mengakses layanan yang disediakan oleh instance di VPC B.



Daftar Isi

- Gambaran umum
- Sumber daya
- Perutean

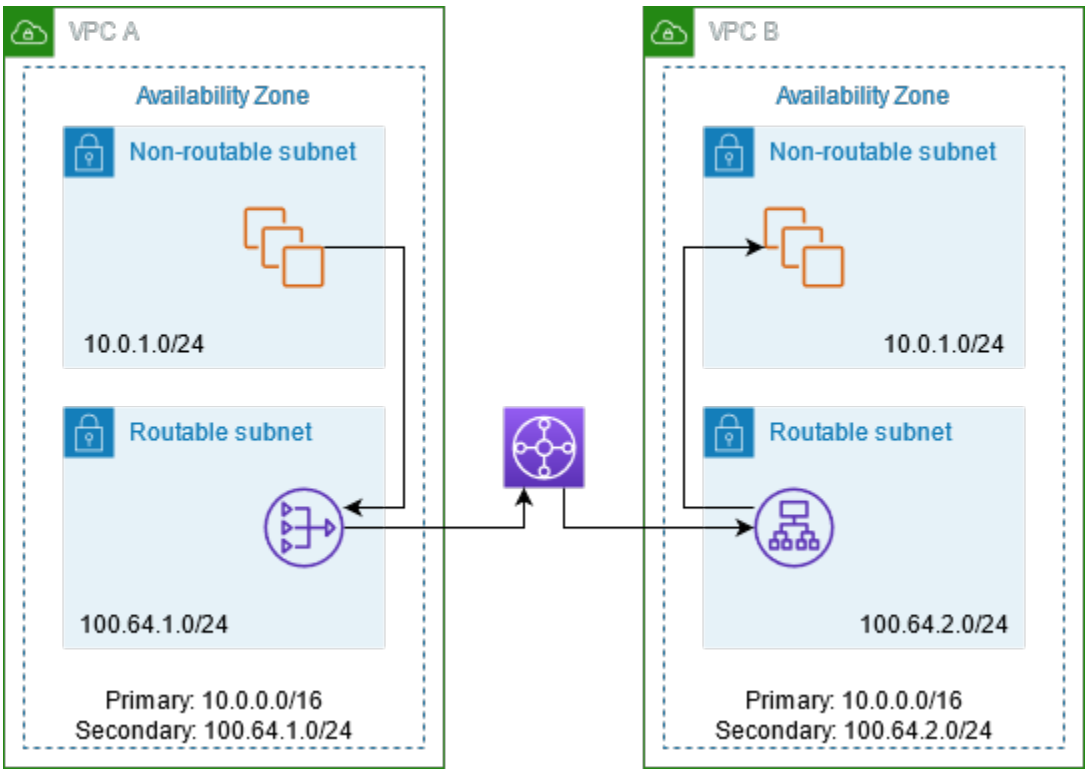
Gambaran umum

Diagram berikut menunjukkan komponen kunci konfigurasi untuk skenario ini. Pertama, tim manajemen IP Anda menentukan rentang alamat mana yang dapat tumpang tindih (rentang alamat yang tidak dapat dialihkan) dan mana yang tidak dapat (rentang alamat yang dapat dirutekan). Tim manajemen IP mengalokasikan rentang alamat dari kumpulan rentang alamat yang dapat dirutekan ke proyek berdasarkan permintaan.

Setiap VPC memiliki rentang alamat IP aslinya, yang tidak dapat dirutekan, ditambah rentang alamat IP yang dapat dirutekan oleh tim manajemen IP. VPC A memiliki subnet dari jangkauan yang dapat dirutekan dengan gateway NAT pribadi. Gerbang NAT pribadi mendapatkan alamat IP dari subnetnya. VPC B memiliki subnet dari jangkauan yang dapat dirutekan dengan Application Load Balancer. Application Load Balancer mendapatkan alamat IP dari subnetnya.

Lalu lintas dari instance di subnet non-routable VPC A yang ditujukan untuk instans di subnet non-routable VPC B dikirim melalui gateway NAT pribadi. Kemudian diarahkan ke gateway transit.

Gateway transit mengirimkan lalu lintas ke Application Load Balancer, yang merutekan lalu lintas ke salah satu instance target di subnet non-routable VPC B. Lalu lintas dari gateway transit ke Application Load Balancer memiliki alamat IP sumber dari gateway NAT pribadi. Oleh karena itu, lalu lintas respons dari load balancer menggunakan alamat gateway NAT pribadi sebagai tujuannya. Lalu lintas respons dikirim ke gateway transit dan kemudian dialihkan ke gateway NAT pribadi, yang menerjemahkan tujuan ke instance di subnet non-routable VPC A.



Sumber daya

Buat atau perbarui sumber daya sebagai berikut:

- Kaitkan rentang alamat IP yang dapat dirutekan yang ditetapkan dengan VPC masing-masing.
- Buat subnet di VPC A dari rentang alamat IP yang dapat dirutekan, dan buat gateway NAT pribadi di subnet baru ini.
- Buat subnet di VPC B dari rentang alamat IP yang dapat dirutekan, dan buat Application Load Balancer di subnet baru ini. Daftarkan instance di subnet yang tidak dapat dirutekan dengan grup target untuk penyeimbang beban.
- Buat gateway transit untuk menghubungkan VPC. Pastikan untuk menonaktifkan propagasi rute. Saat Anda melampirkan setiap VPC ke gateway transit, gunakan rentang alamat yang dapat dirutekan dari VPC.
- Perbarui tabel rute subnet non-routable di VPC A untuk mengirim semua lalu lintas yang ditujukan untuk rentang alamat yang dapat dirutekan dari VPC B ke gateway NAT pribadi. Perbarui tabel rute subnet yang dapat dirutekan di VPC A untuk mengirim semua lalu lintas yang ditujukan untuk rentang alamat yang dapat dirutekan dari VPC B ke gateway transit.
- Perbarui tabel rute subnet yang dapat dirutekan di VPC B untuk mengirim semua lalu lintas yang ditujukan untuk rentang alamat yang dapat dirutekan dari VPC A ke gateway transit.

Perutean

Berikut ini adalah tabel rute untuk subnet yang tidak dapat dirutekan di VPC A.

Tujuan	Target
10.0.0.0/16	lokal
100.64.1.0/24	lokal
100.64.2.0/24	*nat-gateway-id*

Berikut ini adalah tabel rute untuk subnet yang dapat dirutekan di VPC A.

Tujuan	Target
10.0.0.0/16	lokal
100.64.1.0/24	lokal
100.64.2.0/24	*transit-gateway-id*

Berikut ini adalah tabel rute untuk subnet yang tidak dapat dirutekan di VPC B.

Tujuan	Target
10.0.0.0/16	lokal
100.64.2.0/24	lokal

Berikut ini adalah tabel rute untuk subnet yang dapat dirutekan di VPC B.

Tujuan	Target
10.0.0.0/16	lokal
100.64.2.0/24	lokal

Tujuan	Target
100.64.1.0/24	*transit-gateway-id*

Berikut ini adalah tabel rute gateway transit.

CIDR	Lampiran	Jenis rute
100.64.1.0/24	*Attachment for VPC A*	Statis
100.64.2.0/24	*Attachment for VPC B*	Statis

DNS64 dan NAT64

Gateway NAT mendukung terjemahan alamat jaringan dari IPv6 ke IPv4, yang dikenal sebagai NAT64. NAT64 membantu AWS sumber daya IPv6 Anda berkomunikasi dengan sumber daya IPv4 di VPC yang sama atau VPC yang berbeda, di jaringan lokal Anda atau melalui internet. Anda dapat menggunakan NAT64 dengan DNS64 di Amazon Route 53 Resolver atau menggunakan server DNS64 Anda sendiri.

Daftar Isi

- Apa itu DNS64?
- Apa itu NAT64?
- Konfigurasikan DNS64 dan NAT64

Apa itu DNS64?

Beb IPv6-only an kerja Anda yang berjalan di VPC hanya dapat mengirim dan menerima paket jaringan IPv6. Tanpa DNS64, permintaan DNS untuk IPv4-only layanan akan menghasilkan alamat tujuan IPv4 sebagai tanggapan dan IPv6-only layanan Anda tidak dapat berkomunikasi dengannya. Untuk menjembatani kesenjangan komunikasi ini, Anda dapat mengaktifkan DNS64 untuk subnet dan itu berlaku untuk semua AWS sumber daya dalam subnet itu. Dengan DNS64, Amazon Route 53 Resolver mencari catatan DNS untuk layanan yang Anda tanyakan dan melakukan salah satu hal berikut:

- Jika catatan berisi alamat IPv6, ia mengembalikan catatan asli dan koneksi dibuat tanpa terjemahan apa pun melalui IPv6.
- Jika tidak ada alamat IPv6 yang terkait dengan tujuan dalam catatan DNS, Route 53 Resolver mensintesis satu dengan mengawali `/96` awalan terkenal, yang didefinisikan dalam RFC6052 (`64:ff9b::/96`), ke alamat IPv4 dalam catatan.

  IPv6-only Layanan Anda mengirimkan paket jaringan ke alamat IPv6 yang disintesis. Anda kemudian merutekan lalu lintas ini melalui gateway NAT, yang melakukan terjemahan yang diperlukan pada lalu lintas untuk memungkinkan layanan IPv6 di subnet Anda mengakses layanan IPv4 di luar subnet itu.

Anda dapat mengaktifkan atau menonaktifkan DNS64 pada subnet menggunakan atribut modify-subnet menggunakan AWS CLI atau dengan konsol VPC dengan memilih subnet dan memilih Actions > Edit subnet settings.

Apa itu NAT64?

NAT64 memungkinkan IPv6-only layanan Anda di Amazon VPC untuk berkomunikasi dengan IPv4-only layanan dalam VPC yang sama (di subnet yang berbeda) atau VPC yang terhubung, di jaringan lokal Anda, atau melalui internet.

NAT64 secara otomatis tersedia di gateway NAT yang ada atau pada gateway NAT baru yang Anda buat. Ini bukan fitur yang Anda aktifkan atau nonaktifkan. Subnet tempat gateway NAT berada tidak perlu menjadi subnet dual-stack agar NAT64 dapat berfungsi.

Setelah Anda mengaktifkan DNS64, jika IPv6-only layanan Anda mengirimkan paket jaringan ke alamat IPv6 yang disintesis melalui gateway NAT, hal berikut terjadi:

- Dari `64:ff9b::/96` awalan, gateway NAT mengenali bahwa tujuan aslinya adalah IPv4 dan menerjemahkan paket IPv6 ke IPv4 dengan mengganti:
  - Sumber IPv6 dengan IP pribadinya sendiri yang diterjemahkan ke alamat IP Elastic oleh gateway internet.
  - Tujuan IPv6 ke IPv4 dengan memotong awalan. `64:ff9b::/96`
- Gerbang NAT mengirimkan paket IPv4 yang diterjemahkan ke tujuan melalui gateway internet, gateway pribadi virtual, atau gateway transit dan memulai koneksi.
- IPv4-only Host mengirimkan kembali paket respons IPv4. Setelah koneksi dibuat, NAT gateway menerima respon paket IPv4 dari host eksternal.

- Paket respons IPv4 ditujukan untuk gateway NAT, yang menerima paket dan de-NATS mereka dengan mengganti IP (IP tujuan) dengan alamat IPv6 host dan menunggu kembali `64:ff9b::/96` ke alamat IPv4 sumber. Paket kemudian mengalir ke host mengikuti rute lokal.

Dengan cara ini, gateway NAT memungkinkan IPv6-only beban kerja Anda di subnet untuk berkomunikasi dengan IPv4-only layanan di luar subnet.

Konfigurasikan DNS64 dan NAT64

Ikuti langkah-langkah di bagian ini untuk mengkonfigurasi DNS64 dan NAT64 untuk mengaktifkan komunikasi dengan layanan. IPv4-only

Daftar Isi

- Aktifkan komunikasi dengan IPv4-only layanan di internet dengan AWS CLI
- Aktifkan komunikasi dengan IPv4-only layanan di lingkungan lokal

Aktifkan komunikasi dengan IPv4-only layanan di internet dengan AWS CLI

Jika Anda memiliki subnet dengan IPv6-only beban kerja yang perlu berkomunikasi dengan IPv4-only layanan di luar subnet, contoh ini menunjukkan cara mengaktifkan IPv6-only layanan ini untuk berkomunikasi dengan IPv4-only layanan di internet.

Anda harus terlebih dahulu mengkonfigurasi gateway NAT di subnet publik (terpisah dari subnet yang berisi beban IPv6-only kerja). Misalnya, subnet yang berisi gateway NAT harus memiliki `0.0.0.0/0` rute yang menunjuk ke gateway internet.

Selesaikan langkah-langkah ini untuk mengaktifkan IPv6-only layanan ini untuk terhubung dengan IPv4-only layanan di internet:

1. Tambahkan tiga rute berikut ke tabel rute subnet yang berisi beban IPv6-only kerja:

   - Rute IPv4 (jika ada) menunjuk ke gateway NAT.
   - `64:ff9b::/96`rute menunjuk ke gateway NAT. Ini akan memungkinkan lalu lintas dari IPv6-only beban kerja Anda yang ditujukan untuk IPv4-only layanan dirutekan melalui gateway NAT.
   - `::/0`Rute IPv6 menunjuk ke gateway internet khusus keluar (atau gateway internet).

   Perhatikan bahwa menunjuk `::/0` ke gateway internet akan memungkinkan host IPv6 eksternal (di luar VPC) untuk memulai koneksi melalui IPv6.

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-cidr-block
0.0.0.0/0 --nat-gateway-id nat-05dba92075d71c408
```

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-ipv6-cidr-block
64:ff9b::/96 --nat-gateway-id nat-05dba92075d71c408
```

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-ipv6-cidr-block
::/0 --egress-only-internet-gateway-id eigw-c0a643a9
```

2. Aktifkan kemampuan DNS64 di subnet yang berisi beban kerja. IPv6-only

```
aws ec2 modify-subnet-attribute --subnet-id subnet-1a2b3c4d --enable-dns64
```

Sekarang, sumber daya di subnet pribadi Anda dapat membuat koneksi stateful dengan layanan IPv4 dan IPv6 di internet. Konfigurasikan grup keamanan dan NACL Anda dengan tepat untuk memungkinkan lalu lintas keluar dan masuk ke `64:ff9b::/96` lalu lintas.

Aktifkan komunikasi dengan IPv4-only layanan di lingkungan lokal

Amazon Route 53 Resolver memungkinkan Anda meneruskan kueri DNS dari VPC ke jaringan lokal dan sebaliknya. Anda dapat melakukan ini dengan melakukan hal berikut:

- Anda membuat titik akhir outbound Route 53 Resolver di VPC dan menetapkannya alamat IPv4 yang Anda inginkan untuk meneruskan kueri dari Route 53 Resolver. Untuk resolver DNS lokal Anda, ini adalah alamat IP yang berasal dari kueri DNS dan, oleh karena itu, harus alamat IPv4.
- Anda membuat satu atau beberapa aturan yang menentukan nama domain dari kueri DNS yang ingin Route 53 Resolver diteruskan ke resolver lokal Anda. Anda juga menentukan alamat IPv4 dari resolver lokal.
- Sekarang setelah Anda menyiapkan titik akhir outbound Route 53 Resolver, Anda perlu mengaktifkan DNS64 pada subnet yang berisi beban kerja Anda. IPv6-only Anda juga perlu merutekan data apa pun yang ditujukan untuk jaringan lokal Anda melalui gateway NAT.

Cara kerja DNS64 untuk IPv4-only tujuan di jaringan lokal:

1. Anda menetapkan alamat IPv4 ke titik akhir keluar Route 53 Resolver di VPC Anda.
2. Kueri DNS dari layanan IPv6 Anda pergi ke Route 53 Resolver melalui IPv6. Route 53 Resolver mencocokkan kueri dengan aturan penerusan dan mendapatkan alamat IPv4 untuk resolver lokal Anda.
3. Route 53 Resolver mengubah paket query dari IPv6 ke IPv4 dan meneruskannya ke titik akhir keluar. Setiap alamat IP titik akhir mewakili satu ENI yang meneruskan permintaan ke alamat IPv4 lokal dari resolver DNS Anda.
4. Resolver lokal mengirimkan paket respons melalui IPv4 kembali melalui titik akhir keluar ke Route 53 Resolver.
5. Dengan asumsi kueri dibuat dari DNS64-enabled subnet, Route 53 Resolver melakukan dua hal:

    a. Memeriksa isi paket respons. Jika ada alamat IPv6 dalam catatan, itu menyimpan konten apa adanya, tetapi jika hanya berisi catatan IPv4. Ini mensintesis catatan IPv6 juga dengan mendahului `64:ff9b::/96` ke alamat IPv4.

    b. Kemas ulang konten dan mengirimkannya ke layanan di VPC Anda melalui IPv6.

Periksa lalu lintas dari gateway NAT

Anda dapat melampirkan Proxy Firewall Jaringan ke NAT Gateway Anda untuk memeriksa dan memfilter lalu lintas di NAT Gateway Anda. Kontrol keamanan ini memungkinkan Anda untuk mencegah kebocoran data di luar perimeter tepercaya Anda dan memblokir respons masuk yang tidak diinginkan.

Cara kerjanya

Saat membuat Proxy Firewall Jaringan, Anda harus memilih Gateway NAT yang ada untuk melampirkan Proxy. Setelah dibuat, Proxy:

- Proxy dilengkapi dengan nama domain yang sepenuhnya memenuhi syarat dan Anda perlu mengatur aplikasi Anda untuk mengirim permintaan http dan https connect ke Proxy. Proxy pertama menyaring nama domain dalam permintaan connect berdasarkan aturan yang dimasukkan oleh pelanggan. Jika diizinkan oleh pelanggan, proxy kemudian membuat query DNS untuk mendapatkan alamat IP domain. Kemudian membangun koneksi TCP dengan tujuan akhir. Berdasarkan apakah dekripsi TLS diaktifkan, proxy kemudian memfilter koneksi TLS pada alamat IP dan atribut header dan hanya membuat koneksi TLS dengan tujuan jika atribut IP dan header (termasuk tindakan header dan jalur url) diizinkan oleh kebijakan.
- Alat memeriksa dan menyaring lalu lintas.

- Lalu lintas yang diizinkan berlanjut ke tujuan (di internet atau lingkungan di prem atau VPC lain).

Memasang peralatan

Peralatan terpasang ke Gateway NAT melalui Network Firewall AWS . Untuk langkah-langkah dalam membuat dan melampirkan peralatan, lihat Panduan Pengembang Proxy Firewall Jaringan.

Melihat peralatan yang terpasang

Untuk melihat peralatan yang terpasang pada NAT Gateway Anda, gunakan describe-nat-gatewaysperintah:

```
aws ec2 describe-nat-gateways --nat-gateway-ids nat-1234567890abcdef0
```

Responsnya mencakup `AttachedAppliances` bidang yang menunjukkan:

- Jenis - Jenis alat (mis.,`network-firewall-proxy`)
- ApplianceArn— ARN dari alat yang terpasang
- AttachmentState— Status lampiran saat ini (`attached`,`detaching`,`detached`,`attach_failed`,`detach_failed`)
- ModificationState— Status modifikasi saat ini (`modifying`,`completed`,`failed`)
- VpcEndpointId— ID titik akhir VPC yang digunakan untuk merutekan lalu lintas dari aplikasi ke proxy VPCs untuk inspeksi dan penyaringan
- FailureCode— Kode kegagalan jika pemasangan alat atau operasi modifikasi gagal
- FailureMessage— Pesan deskriptif yang menjelaskan kegagalan jika lampiran alat atau operasi modifikasi gagal

Pantau gateway NAT dengan Amazon CloudWatch

Anda dapat memantau gateway NAT menggunakan CloudWatch, yang mengumpulkan informasi dari gateway NAT Anda dan membuat metrik yang dapat dibaca dan hampir real-time. Anda dapat menggunakan informasi ini untuk memantau dan memecahkan masalah gateway NAT Anda. Metrik ini memberi Anda visibilitas ke dalam kesehatan dan kinerja gateway NAT Anda, memungkinkan Anda memantau operasinya dengan cermat dan memecahkan masalah dengan cepat.

Metrik NAT gateway yang dikumpulkan oleh CloudWatch mencakup titik data seperti byte yang diproses, jumlah paket, jumlah koneksi, dan tingkat kesalahan. Ini memungkinkan Anda untuk benar-

benar memahami lalu lintas yang mengalir melalui gateway NAT Anda dan mengidentifikasi anomali atau hambatan apa pun. CloudWatch memberikan data metrik ini pada interval 1 menit, memberi Anda tampilan terperinci dan terkini tentang perilaku gateway NAT Anda.

Selain itu CloudWatch , simpan data metrik gateway NAT ini untuk jangka waktu 15 bulan yang lama, memungkinkan Anda menganalisis tren dan pola dari waktu ke waktu. Anda dapat menggunakan data historis ini untuk perencanaan kapasitas, pengoptimalan kinerja, dan memahami evolusi jangka panjang penggunaan gateway NAT Anda.

Untuk menggunakan kemampuan pemantauan yang kuat ini, Anda dapat membuat CloudWatch dasbor dan alarm khusus yang disesuaikan dengan kebutuhan spesifik Anda. Misalnya, Anda dapat mengatur peringatan untuk memberi tahu Anda setiap kali transfer data keluar gateway NAT Anda melebihi ambang batas tertentu, memungkinkan Anda untuk secara proaktif mengatasi kendala bandwidth potensial.

Untuk informasi selengkapnya tentang harga, lihat CloudWatch Harga Amazon.

Daftar Isi

- Metrik dan dimensi gateway NAT
- Lihat CloudWatch metrik NAT gateway
- Buat CloudWatch alarm untuk memantau gateway NAT

Metrik dan dimensi gateway NAT

Metrik berikut tersedia untuk gateway NAT Anda. Kolom deskripsi mencakup deskripsi setiap metrik serta unit dan statistik.

Metrik	Deskripsi
`ActiveConnectionCount`	Jumlah total koneksi TCP aktif bersamaan melalui gateway NAT. Nilai nol menunjukkan bahwa tidak ada koneksi aktif melalui gateway NAT. Unit: Hitungan Statistik: Statistik yang paling berguna adalah`Max`.

Metrik	Deskripsi
BytesInFromDestination	Jumlah byte yang diterima oleh gateway NAT dari tujuan. Jika nilai untuk BytesOutToSource kurang dari nilai untukBytesInFromDestination, mungkin ada kehilangan data selama pemrosesan gateway NAT, atau lalu lintas diblokir secara aktif oleh gateway NAT. Unit: Byte Statistik: Statistik yang paling berguna adalahSum.
BytesInFromSource	Jumlah byte yang diterima oleh gateway NAT dari klien di VPC Anda. Jika nilai untuk BytesOutToDestination kurang dari nilai untukBytesInFromSource, mungkin ada kehilangan data selama pemrosesan gateway NAT. Unit: Byte Statistik: Statistik yang paling berguna adalahSum.

Metrik	Deskripsi
BytesOutToDestination	Jumlah byte yang dikirim melalui gateway NAT ke tujuan. Nilai yang lebih besar dari nol menunjukkan bahwa ada lalu lintas pergi ke internet dari klien yang berada di belakang gateway NAT. Jika nilai untuk BytesOutToDestination kurang dari nilai untukBytesInFromSource , mungkin ada kehilangan data selama pemrosesan gateway NAT. Unit: Bita Statistik: Statistik yang paling berguna adalahSum.
BytesOutToSource	Jumlah byte yang dikirim melalui gateway NAT untuk klien di VPC Anda. Nilai yang lebih besar dari nol menunjukkan bahwa ada lalu lintas yang datang dari internet ke klien yang berada di belakang gateway NAT. Jika nilai untuk BytesOutToSource kurang dari nilai untukBytesInFromDestination , mungkin ada kehilangan data selama pemrosesan gateway NAT, atau lalu lintas diblokir secara aktif oleh gateway NAT. Unit: Byte Statistik: Statistik yang paling berguna adalahSum.

Metrik	Deskripsi
ConnectionAttemptCount	Jumlah upaya koneksi yang dilakukan melalui gateway NAT. Ini hanya mencakup SYN awal. Dalam beberapa kasus, ConnectionAttemptCount mungkin lebih rendah daripada ConnectionEstablishedCount karena transmisi ulang SYN. Jika nilai untuk ConnectionEstablishedCount kurang dari nilai untuk ConnectionAttemptCount, ini menunjukkan bahwa klien di belakang gateway NAT berusaha untuk membangun koneksi baru yang untuknya tidak ada respon. Unit: Jumlah Statistik: Statistik yang paling berguna adalahSum.
ConnectionEstablishedCount	Jumlah koneksi yang dibuat melalui gateway NAT. Ini termasuk transmisi ulang SYN dan SYN. Jika nilai untuk ConnectionEstablishedCount kurang dari nilai untuk ConnectionAttemptCount, ini menunjukkan bahwa klien di belakang gateway NAT berusaha untuk membangun koneksi baru yang untuknya tidak ada respon. Unit: Jumlah Statistik: Statistik yang paling berguna adalahSum.

Metrik	Deskripsi
`ErrorPortAllocation`	Berapa kali gateway NAT tidak dapat mengalokasikan port sumber. Nilai yang lebih besar dari nol menunjukkan bahwa terlalu banyak koneksi bersamaan terbuka melalui gateway NAT. Unit: Hitungan Statistik: Statistik yang paling berguna adalah`Sum`.
`IdleTimeoutCount`	Jumlah koneksi yang beralih dari status aktif ke status siaga. Transisi koneksi aktif ke siaga jika itu tidak ditutup dengan baik dan tidak ada aktivitas selama 350 detik terakhir. Nilai yang lebih besar dari nol menunjukkan bahwa ada koneksi yang telah dipindahkan ke status siaga. Jika nilai untuk `IdleTimeoutCount` meningkat, itu mungkin menunjukkan bahwa klien di belakang gateway NAT menggunakan kembali koneksi basi. Unit: Jumlah Statistik: Statistik yang paling berguna adalah`Sum`.

Metrik	Deskripsi
PacketsDropCount	Jumlah paket yang dijatuhkan oleh gateway NAT. Untuk menghitung jumlah paket yang dijatuhkan sebagai persentase dari keseluruhan lalu lintas paket, gunakan rumus ini: PacketsDropCount/(PacketsInFromSource+PacketsInFromDestination)*100 Jika nilai ini melebihi 0,01 persen dari total lalu lintas pada gateway NAT, mungkin ada masalah dengan layanan Amazon VPC. Gunakan dasbor kesehatan AWS layanan untuk mengidentifikasi masalah dengan layanan yang mungkin menyebabkan gateway NAT menjatuhkan paket. Unit: Hitungan Statistik: Statistik yang paling berguna adalahSum.
PacketsInFromDestination	Jumlah paket yang diterima oleh gateway NAT dari tujuan. Jika nilai untuk PacketsOutToSource kurang dari nilai untukPacketsInFromDestination , mungkin ada kehilangan data selama pemrosesan gateway NAT, atau lalu lintas diblokir secara aktif oleh gateway NAT. Unit: Jumlah Statistik: Statistik yang paling berguna adalahSum.

Metrik	Deskripsi
PacketsInFromSource	Jumlah paket yang diterima oleh gateway NAT dari klien di VPC Anda. Jika nilai untuk PacketsOutToDestination kurang dari nilai untukPacketsInFromSource , mungkin ada kehilangan data selama pemrosesan gateway NAT. Unit: Jumlah Statistik: Statistik yang paling berguna adalahSum.
PacketsOutToDestination	Jumlah paket yang dikirim melalui gateway NAT ke tujuan. Nilai yang lebih besar dari nol menunjukkan bahwa ada lalu lintas pergi ke internet dari klien yang berada di belakang gateway NAT. Jika nilai untuk PacketsOutToDestination kurang dari nilai untukPacketsInFromSource , mungkin ada kehilangan data selama pemrosesan gateway NAT. Unit: Jumlah Statistik: Statistik yang paling berguna adalahSum.

Metrik	Deskripsi
PacketsOutToSource	Jumlah paket yang dikirim melalui gateway NAT untuk klien di VPC Anda. Nilai yang lebih besar dari nol menunjukkan bahwa ada lalu lintas yang datang dari internet ke klien yang berada di belakang gateway NAT. Jika nilai untuk PacketsOutToSource kurang dari nilai untukPacketsInFromDestination , mungkin ada kehilangan data selama pemrosesan gateway NAT, atau lalu lintas diblokir secara aktif oleh gateway NAT. Unit: Jumlah Statistik: Statistik yang paling berguna adalahSum.
PeakBytesPerSecond	Metrik ini melaporkan rata-rata byte 10 detik per detik tertinggi dalam satu menit tertentu. Unit: Hitungan Statistik: Statistik yang paling berguna adalahMaximum.
PeakPacketsPerSecond	Metrik ini menghitung kecepatan paket rata-rata (paket yang diproses per detik) setiap 10 detik selama 60 detik dan kemudian melaporkan maksimum dari enam tingkat (tingkat paket rata-rata tertinggi). Unit: Hitungan Statistik: Statistik yang paling berguna adalahMaximum.

Untuk memfilter data metrik, gunakan dimensi berikut.

Dimensi	Deskripsi
`NatGatewayId`	Filter data metrik berdasarkan ID gateway NAT. Gerbang NAT zonal hanya menggunakan dimensi ini. Gerbang NAT regional menggunakan dimensi ini bersama dengan`AvailabilityZone` .
`AvailabilityZone`	Filter data metrik berdasarkan Availability Zone. Gerbang NAT regional menggunakan dimensi ini bersama dengan`NatGatewayId` . Gateway NAT zonal tidak menggunakan dimensi ini.

Lihat CloudWatch metrik NAT gateway

Metrik NAT gateway dikirim CloudWatch pada interval 1 menit. Metrik dikelompokkan pertama oleh namespace layanan, dan kemudian oleh kemungkinan kombinasi dimensi dalam setiap namespace. Anda dapat melihat metrik gateway NAT Anda sebagai berikut.

Untuk melihat metrik menggunakan CloudWatch konsol

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pada panel navigasi, silakan pilih Metrik, Semua metrik.
3. Pilih namespace metrik NATGateway.
4. Pilih dimensi metrik.

Untuk melihat metrik menggunakan AWS CLI

Pada prompt perintah, gunakan perintah berikut untuk mencantumkan metrik yang tersedia untuk layanan gateway NAT.

```
aws cloudwatch list-metrics --namespace "AWS/NATGateway"
```

Buat CloudWatch alarm untuk memantau gateway NAT

Anda dapat membuat CloudWatch alarm yang mengirimkan pesan Amazon SNS saat alarm berubah status. Alarm mengawasi satu metrik selama suatu periode waktu yang Anda tentukan. Alarm

mengirimkan pemberitahuan ke topik Amazon SNS berdasarkan nilai metrik relatif terhadap ambang batas tertentu selama beberapa periode waktu.

Misalnya, Anda dapat membuat alarm yang memantau jumlah lalu lintas yang masuk atau meninggalkan gateway NAT. Alarm berikut memonitor jumlah lalu lintas keluar dari klien di VPC Anda melalui gateway NAT ke internet. Ini mengirimkan pemberitahuan ketika jumlah byte mencapai ambang batas 5.000.000 selama periode 15 menit.

Untuk membuat alarm untuk lalu lintas keluar melalui gateway NAT

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pada panel navigasi, pilih Alarm, Semua alarm.
3. Pilih Buat alarm.
4. Pilih Pilih Metrik.
5. Pilih namespace metrik NATGateway dan kemudian pilih dimensi metrik. Saat Anda masuk ke metrik, pilih kotak centang di sebelah BytesOutToDestination metrik untuk gateway NAT, lalu pilih Pilih metrik.
6. Konfigurasikan alarm sebagai berikut, lalu pilih Next (Selanjutnya):
   - Untuk Statistik pilih Jumlah.
   - Untuk Peri ode, pilih 15 menit.
   - Untuk Kapan saja, pilih Greater/Equal dan masukkan `5000000` ambang batas.
7. Untuk Pem beritahuan, pilih topik SNS yang ada atau pilih Buat topik baru untuk membuat topik baru. Pilih Berikutnya.
8. Masukkan nama dan deskripsi untuk alarm dan pilih Ber ikutnya.
9. Setelah Anda selesai mengkonfigurasi alarm, pilih Buat alarm.

Sebagai contoh lain, Anda dapat membuat alarm yang memantau kesalahan alokasi port dan mengirimkan pemberitahuan ketika nilainya lebih besar dari nol (0) selama tiga periode 5 menit berturut-turut.

Membuat alarm untuk memantau kesalahan alokasi port

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pada panel navigasi, pilih Alarm, Semua alarm.
3. Pilih Buat alarm.

4. Pilih Pilih Metrik.
5. Pilih namespace metrik NATGateway dan kemudian pilih dimensi metrik. Saat Anda masuk ke metrik, pilih kotak centang di sebelah ErrorPortAllocation metrik untuk gateway NAT, lalu pilih Pilih metrik.
6. Konfigurasikan alarm sebagai berikut, lalu pilih Next (Selanjutnya):
   - Untuk Statistik, pilih Maksimum.
   - Untuk Peri ode, pilih 5 menit.
   - Untuk Kapan saja, pilih Lebih Besar dan masukkan 0 untuk ambang batas.
   - Untuk Konfigurasi tambahan, titik data untuk alarm, masukkan 3.
7. Untuk Pem beritahuan, pilih topik SNS yang ada atau pilih Buat topik baru untuk membuat topik baru. Pilih Berikutnya.
8. Masukkan nama dan deskripsi untuk alarm dan pilih Ber ikutnya.
9. Setelah selesai mengkonfigurasi alarm, pilih Buat alarm.

Untuk informasi selengkapnya, lihat Menggunakan CloudWatch alarm Amazon di Panduan CloudWatch Pengguna Amazon.

Memecahkan masalah gateway NAT

Topik berikut membantu Anda memecahkan masalah umum yang mungkin Anda temui saat membuat atau menggunakan gateway NAT.

Masalah

- Pembuatan gateway NAT gagal
- Kuota gateway NAT
- Kuota alamat IP Elastis
- Availability Zone tidak didukung
- gateway NAT tidak lagi terlihat
- gateway NAT tidak menanggapi perintah ping
- Instans tidak dapat mengakses internet
- Koneksi TCP ke tujuan gagal
- Output Traceroute tidak menampilkan alamat IP privat gateway NAT

- Koneksi internet terputus setelah 350 detik
- IPsec koneksi tidak dapat dibuat
- Tidak dapat memulai lebih banyak koneksi

Pembuatan gateway NAT gagal

Masalah

Anda membuat gateway NAT dan berubah ke status `Failed`.

> **Note**
>
> Gateway NAT yang gagal dihapus secara otomatis, biasanya sekitar satu jam.

Penyebab

Terjadi kesalahan saat gateway NAT dibuat. Pesan status kembali memberikan alasan untuk kesalahan.

Solusi

Untuk melihat pesan kesalahan, buka konsol Amazon VPC, dan kemudian pilih Gateway NAT. Pilih tombol radio untuk gateway NAT Anda, dan kemudian temukan Pesan status pada tab Detail.

Tabel berikut mencantumkan kemungkinan penyebab kegagalan seperti yang ditunjukkan dalam konsol Amazon VPC. Setelah menerapkan salah satu langkah perbaikan yang ditunjukkan, Anda dapat mencoba membuat gateway NAT lagi.

Kesalahan ditampilkan	Penyebab	Solusi
Subnet memiliki alamat gratis yang tidak mencukupi untuk membuat gateway NAT ini	Subnet yang Anda tentukan tidak memiliki alamat IP privat gratis. Gateway NAT memerlukan antarmuka jaringan dengan alamat IP privat yang dialokasikan dari rentang subnet ini.	Periksa berapa banyak alamat IP yang tersedia di subnet Anda dengan membuka halaman Subnet di konsol Amazon VPC. Anda dapat melihat Tersedia IPs di panel detail untuk subnet Anda.

Kesalahan ditampilkan	Penyebab	Solusi
		Untuk membuat alamat IP gratis di subnet Anda, Anda dapat menghapus antarmuka jaringan yang tidak terpakai, atau mengakhiri instans yang tidak Anda butuhkan.
Jaringan vpc-xxxxxxxx tidak memiliki gateway internet terpasang	Gateway NAT harus dibuat dalam VPC dengan gateway internet.	Buat dan lampirkan gateway internet ke VPC Anda. Untuk informasi selengkapnya, lihat Menambahkan akses internet ke subnet.
Alamat IP Elastis eipalloc-xxxxxxxx siap diasosiasikan	Alamat IP Elastis yang Anda tentukan sudah dikaitkan dengan sumber daya lain, dan tidak dapat dikaitkan dengan gateway NAT.	Periksa sumber daya mana yang terkait dengan alamat IP Elastis. Buka IPs halaman Elastic di konsol VPC Amazon, dan lihat nilai yang ditentukan untuk ID instance atau ID antarmuka jaringan. Jika Anda tidak memerluka n alamat IP Elastis untuk sumber daya tersebut, Anda dapat memisahkannya. Atau, alokasikan alamat IP Elastis baru ke akun Anda. Untuk informasi selengkapnya, lihat Mulai gunakan alamat IP Elastic.

Kuota gateway NAT

Ketika Anda mencoba untuk membuat gateway NAT, Anda akan menerima pesan kesalahan berikut.

```
Performing this operation would exceed the limit of 5 NAT gateways
```

Penyebab

Anda telah mencapai kuota untuk jumlah gateway NAT untuk Availability Zone tersebut.

Solusi

Jika Anda telah mencapai kuota gateway NAT ini untuk akun Anda, Anda dapat melakukan salah satu hal berikut:

- Meminta peningkatan Gateway NAT per kuota Availability Zone menggunakan konsol Service Quotas.
- Periksa status gateway NAT Anda. Status dari `Pending`, `Available`, atau `Deleting` dihitung dari kuota Anda. Jika Anda baru saja menghapus gateway NAT, tunggu beberapa menit hingga status berjalan dari `Deleting` ke `Deleted`. Kemudian coba buat gateway NAT baru.
- Jika Anda tidak memerlukan gateway NAT di Availability Zone tertentu, coba buat gateway NAT di Availability Zone yang belum mencapai kuota.

Untuk informasi selengkapnya, lihat Kuota Amazon VPC.

Kuota alamat IP Elastis

Masalah

Ketika Anda mencoba untuk mengalokasikan alamat IP elastis untuk gateway NAT publik Anda, Anda mendapatkan galat berikut.

```
The maximum number of addresses has been reached.
```

Penyebab

Anda telah mencapai kuota untuk jumlah alamat IP Elastis untuk akun Anda untuk Wilayah tersebut.

Solusi

Jika Anda telah mencapai kuota alamat IP Elastis, Anda dapat memisahkan alamat IP Elastis dari sumber daya lain. Atau, Anda dapat meminta peningkatan IPs kuota Elastis menggunakan konsol Service Quotas.

Availability Zone tidak didukung

Masalah

Ketika Anda mencoba untuk membuat gateway NAT, Anda akan menerima pesan kesalahan berikut. `NotAvailableInZone`.

Penyebab

Anda mungkin mencoba untuk membuat gateway NAT di Availability Zone terbatas - zona di mana kemampuan kita untuk memperluas dibatasi.

Solusi

Kami tidak dapat mendukung gateway NAT di Availability Zone ini. Anda dapat membuat gateway NAT di Availability Zone yang berbeda dan menggunakannya untuk subnet privat di zona dibatasi. Anda juga dapat memindahkan sumber daya Anda ke Availability Zone yang tidak terbatas sehingga sumber daya dan gateway NAT Anda berada di zona yang sama.

gateway NAT tidak lagi terlihat

Masalah

Anda membuat gateway NAT tapi tidak lagi terlihat di konsol Amazon VPC.

Penyebab

Mungkin ada kesalahan selama pembuatan gateway NAT Anda, dan pembuatan gagal. Sebuah gateway NAT dengan status `Failed` terlihat di konsol Amazon VPC selama sekitar satu jam). Setelah satu jam, secara otomatis dihapus.

Solusi

Tinjau informasi di Pembuatan gateway NAT gagal, dan coba buat gateway NAT baru.

gateway NAT tidak menanggapi perintah ping

Masalah

Ketika Anda mencoba untuk mengirim ping ke alamat IP Elastis gateway NAT atau alamat IP privat dari internet (misalnya, dari komputer rumah Anda) atau dari sebuah instans di VPC Anda, Anda tidak mendapatkan respons.

Penyebab

Sebuah gateway NAT hanya melewati lalu lintas dari sebuah instans dalam sebuah subnet privat ke internet.

Solusi

Untuk menguji apakah gateway NAT Anda berfungsi, lihat Uji gateway NAT publik.

Instans tidak dapat mengakses internet

Masalah

Anda membuat gateway NAT publik dan mengikuti langkah-langkah untuk mengujinya, tetapi perintah `ping` gagal, atau instans Anda di subnet privat tidak dapat mengakses internet.

Penyebab

Penyebab dari masalah ini mungkin salah satu dari yang berikut:

- Gateway NAT tidak siap untuk melayani lalu lintas.
- Tabel rute Anda tidak dikonfigurasi dengan benar.
- Grup atau jaringan keamanan ACLs Anda memblokir lalu lintas masuk atau keluar.
- Anda menggunakan protokol yang tidak didukung.

Solusi

Perhatikan informasi berikut:

- Periksa bahwa gateway NAT dalam keadaan `Available`. Di konsol VPC Amazon, buka halaman gateway NAT dan lihat informasi status di panel detail. Jika gateway NAT dalam keadaan gagal, mungkin ada kesalahan saat dibuat. Untuk informasi selengkapnya, lihat Pembuatan gateway NAT gagal.
- Periksa apakah Anda telah mengonfigurasi tabel rute dengan benar:
  - Gateway NAT harus berada di subnet publik dengan tabel rute yang merutekan lalu lintas internet ke gateway internet.
  - Instans Anda harus dalam subnet privat dengan tabel rute yang merutekan lalu lintas internet ke gateway NAT.
  - Periksa bahwa tidak ada entri tabel rute lain yang merutekan semua atau sebagian lalu lintas internet ke perangkat lain, bukan gateway NAT.
- Pastikan bahwa aturan grup keamanan untuk instans pribadi Anda mengizinkan lalu lintas internet keluar. Agar perintah `ping` bekerja, aturan juga harus mengizinkan lalu lintas ICMP keluar.

Gateway NAT itu sendiri mengizinkan semua lalu lintas keluar dan lalu lintas yang diterima dalam menanggapi permintaan keluar (oleh karena itu bersifat stateful).

- Pastikan ACLs bahwa jaringan yang terkait dengan subnet pribadi dan subnet publik tidak memiliki aturan yang memblokir lalu lintas internet masuk atau keluar. Agar perintah `ping` bekerja, aturan juga harus mengizinkan lalu lintas ICMP masuk dan keluar.

  Anda dapat mengaktifkan log alur untuk membantu Anda mendiagnosis koneksi yang terputus karena ACL jaringan atau aturan grup keamanan. Untuk informasi selengkapnya, lihat Pencatatan lalu lintas IP menggunakan Log Aliran VPC.
- Jika Anda menggunakan perintah `ping`, pastikan bahwa Anda mengirim ping ke host yang mengaktifkan ICMP. Jika ICMP tidak diaktifkan, Anda tidak akan menerima balasan paket. Untuk menguji ini, kirimkan perintah `ping` yang sama dari terminal baris perintah pada komputer Anda sendiri.
- Periksa apakah instans Anda dapat mengirimkan ping ke sumber daya lain, misalnya, instans lain di subnet privat (dengan asumsi bahwa aturan grup keamanan mengizinkan ini).
- Pastikan bahwa koneksi Anda menggunakan protokol TCP, UDP, atau ICMP saja.

Koneksi TCP ke tujuan gagal

Masalah

Beberapa koneksi TCP Anda dari instans di subnet privat untuk tujuan tertentu melalui gateway NAT berhasil, tetapi beberapa gagal atau waktu habis.

Penyebab

Penyebab dari masalah ini mungkin salah satu dari yang berikut:

- Titik akhir tujuan merespons dengan paket TCP terfragmentasi. gateway NAT tidak support fragmentasi IP untuk TCP atau ICMP. Untuk informasi selengkapnya, lihat Bandingkan gateway NAT dan instans NAT.
- Opsi `tcp_tw_recycle` diaktifkan pada server jarak jauh, yang diketahui menyebabkan masalah ketika ada beberapa koneksi dari belakang perangkat NAT.

Solusi

Verifikasi apakah titik akhir yang Anda coba koneksikan merespons dengan paket TCP terfragmentasi dengan melakukan hal berikut:

1. Gunakan instans di subnet publik dengan alamat IP publik untuk memicu respons yang cukup besar untuk menyebabkan fragmentasi dari titik akhir tertentu.
2. Gunakan utilitas `tcpdump` untuk memverifikasi bahwa titik akhir mengirim paket terfragmentasi.

   > **Important**
   >
   > Anda harus menggunakan instans di subnet publik untuk melakukan pemeriksaan ini. Anda tidak dapat menggunakan instans dari mana koneksi asal gagal, atau instans di subnet privat di belakang gateway NAT atau instans NAT.

   Alat diagnostik yang mengirim atau menerima paket ICMP besar akan melaporkan kehilangan paket. Misalnya, perintah `ping -s 10000 example.com` tidak bekerja di belakang gateway NAT.
3. Jika titik akhir mengirimkan paket TCP terfragmentasi, Anda dapat menggunakan instans NAT bukannya gateway NAT.

Jika Anda memiliki akses ke server jarak jauh, Anda dapat memverifikasi apakah opsi `tcp_tw_recycle` diaktifkan dengan melakukan hal berikut:

1. Dari server, jalankan perintah berikut.

   ```
   cat /proc/sys/net/ipv4/tcp_tw_recycle
   ```

   Jika outputnya `1`, maka opsi `tcp_tw_recycle` diaktifkan.
2. Jika `tcp_tw_recycle` diaktifkan, kami sarankan menonaktifkannya. Jika Anda perlu menggunakan kembali koneksi, `tcp_tw_reuse` adalah opsi yang lebih aman.

Jika Anda tidak memiliki akses ke server jarak jauh, Anda dapat melakukan pengujian dengan menonaktifkan sementara opsi `tcp_timestamps` pada instans di subnet privat. Kemudian koneksikan ke server jarak jauh lagi. Jika koneksi berhasil, penyebab kegagalan sebelumnya mungkin terjadi karena `tcp_tw_recycle` diaktifkan pada server jarak jauh. Jika dimungkinkan,

hubungi pemilik server jarak jauh untuk memverifikasi apakah opsi ini diaktifkan dan memintanya untuk dinonaktifkan.

Output Traceroute tidak menampilkan alamat IP privat gateway NAT

Masalah

Instans Anda dapat mengakses internet, tetapi ketika Anda melakukan perintah `traceroute`, output tidak menampilkan alamat IP privat gateway NAT.

Penyebab

Instans Anda mengakses internet menggunakan gateway yang berbeda, seperti gateway internet.

Solusi

Dalam tabel rute subnet di mana instans Anda berada, periksa informasi berikut:

- Pastikan bahwa ada rute yang mengirimkan lalu lintas internet ke gateway NAT.
- Pastikan tidak ada rute yang lebih spesifik yang mengirim lalu lintas internet ke perangkat lain, seperti virtual private gateway atau gateway internet.

Koneksi internet terputus setelah 350 detik

Masalah

Instans Anda dapat mengakses internet, namun koneksi akan terputus setelah 350 detik.

Penyebab

Jika koneksi yang menggunakan gateway NAT siaga selama 350 detik atau lebih, waktu koneksi akan habis.

Ketika waktu koneksi habis, gateway NAT mengembalikan paket RST untuk sumber daya di belakang gateway NAT yang mencoba untuk melanjutkan koneksi (tidak mengirim paket FIN).

Solusi

Untuk mencegah koneksi terhenti, Anda dapat memulai lebih banyak lalu lintas melalui koneksi tersebut. Atau, Anda dapat mengaktifkan TCP keepalive pada instans dengan nilai kurang dari 350 detik.

IPsec koneksi tidak dapat dibuat

Masalah

Anda tidak dapat membuat IPsec koneksi ke tujuan.

Penyebab

Gateway NAT saat ini tidak mendukung protokol. IPsec

Solusi

Anda dapat menggunakan NAT-traversal (NAT-T) untuk merangkum IPsec lalu lintas di UDP, yang merupakan protokol yang didukung untuk gateway NAT. Pastikan Anda menguji NAT-T dan IPsec konfigurasi Anda untuk memverifikasi bahwa IPsec lalu lintas Anda tidak turun.

Tidak dapat memulai lebih banyak koneksi

Masalah

Anda memiliki koneksi yang ada ke tujuan melalui gateway NAT, tetapi Anda tidak dapat membuat lebih banyak koneksi.

Penyebab

Anda mungkin telah mencapai batas untuk koneksi simultan untuk gateway NAT tunggal. Untuk informasi selengkapnya, lihat Dasar gateway NAT. Jika instans Anda di subnet privat membuat sejumlah besar koneksi, Anda mungkin mencapai batas ini.

Solusi

Lakukan salah satu tindakan berikut:

- Buat gateway NAT per Availability Zone dan sebarkan klien Anda di seluruh zona tersebut.
- Buat gateway NAT tambahan di subnet publik dan pisahkan klien Anda menjadi beberapa subnet privat, masing-masing dengan rute ke gateway NAT yang berbeda.
- Batasi jumlah koneksi ke tujuan yang dapat dibuat klien Anda.
- Gunakan `IdleTimeoutCount`metrik CloudWatch untuk memantau peningkatan koneksi idle. Tutup koneksi siaga untuk melepaskan kapasitas.
- Buat gateway NAT dengan beberapa alamat IP atau tambahkan alamat IP sekunder ke gateway NAT yang ada. Setiap IPv4 alamat baru dapat mendukung hingga 55.000 koneksi bersamaan. Untuk informasi selengkapnya, lihat Buat gateway NAT atau Edit asosiasi alamat IP sekunder.

Harga untuk NAT gateway

Saat Anda menyediakan gateway NAT, Anda dikenakan biaya untuk setiap jam ketika gateway NAT Anda tersedia dan setiap gigabyte data yang diprosesnya. Untuk informasi lebih lanjut, lihat Harga Amazon VPC.

Strategi berikut dapat membantu Anda mengurangi biaya transfer data untuk gateway NAT Anda:

- Jika AWS sumber daya Anda mengirim atau menerima volume lalu lintas yang signifikan di seluruh Zona Ketersediaan, pastikan bahwa sumber daya berada di Zona Ketersediaan yang sama dengan gateway NAT. Atau, buat gateway NAT di setiap Zona Ketersediaan dengan sumber daya.
- Jika sebagian besar lalu lintas melalui gateway NAT Anda menuju AWS layanan yang mendukung titik akhir antarmuka atau titik akhir gateway, pertimbangkan untuk membuat titik akhir antarmuka atau titik akhir gateway untuk layanan ini. Untuk informasi selengkapnya tentang potensi penghematan biaya, lihat AWS PrivateLink harga.

Instans NAT

Sebuah instance NAT menyediakan terjemahan alamat jaringan (NAT). Anda dapat menggunakan instance NAT untuk mengizinkan sumber daya di subnet pribadi berkomunikasi dengan tujuan di luar cloud pribadi virtual (VPC), seperti internet atau jaringan lokal. Sumber daya di subnet pribadi dapat memulai lalu lintas IPv4 keluar ke internet, tetapi mereka tidak dapat menerima lalu lintas masuk yang dimulai di internet.

> **Important**
>
> NAT AMI dibangun di atas versi terakhir dari Amazon Linux AMI, 2018.03, yang mencapai akhir dukungan standar pada 31 Desember 2020 dan akhir dukungan pemeliharaan pada 31 Desember 2023. Untuk informasi selengkapnya, lihat postingan blog berikut: Akhir masa pakai AMI Amazon Linux.
> Jika Anda menggunakan NAT AMI yang ada, sar AWS ankan Anda bermigrasi ke gateway NAT. Gerbang NAT memberikan ketersediaan yang lebih baik, bandwidth yang lebih tinggi, dan membutuhkan lebih sedikit upaya administratif. Untuk informasi selengkapnya, lihat Bandingkan gateway NAT dan instans NAT.
> Jika instans NAT lebih cocok untuk kasus penggunaan Anda daripada gateway NAT, Anda dapat membuat NAT AMI Anda sendiri dari versi Amazon Linux saat ini seperti yang dijelaskan dalamthe section called “3. Buat NAT AMI”.

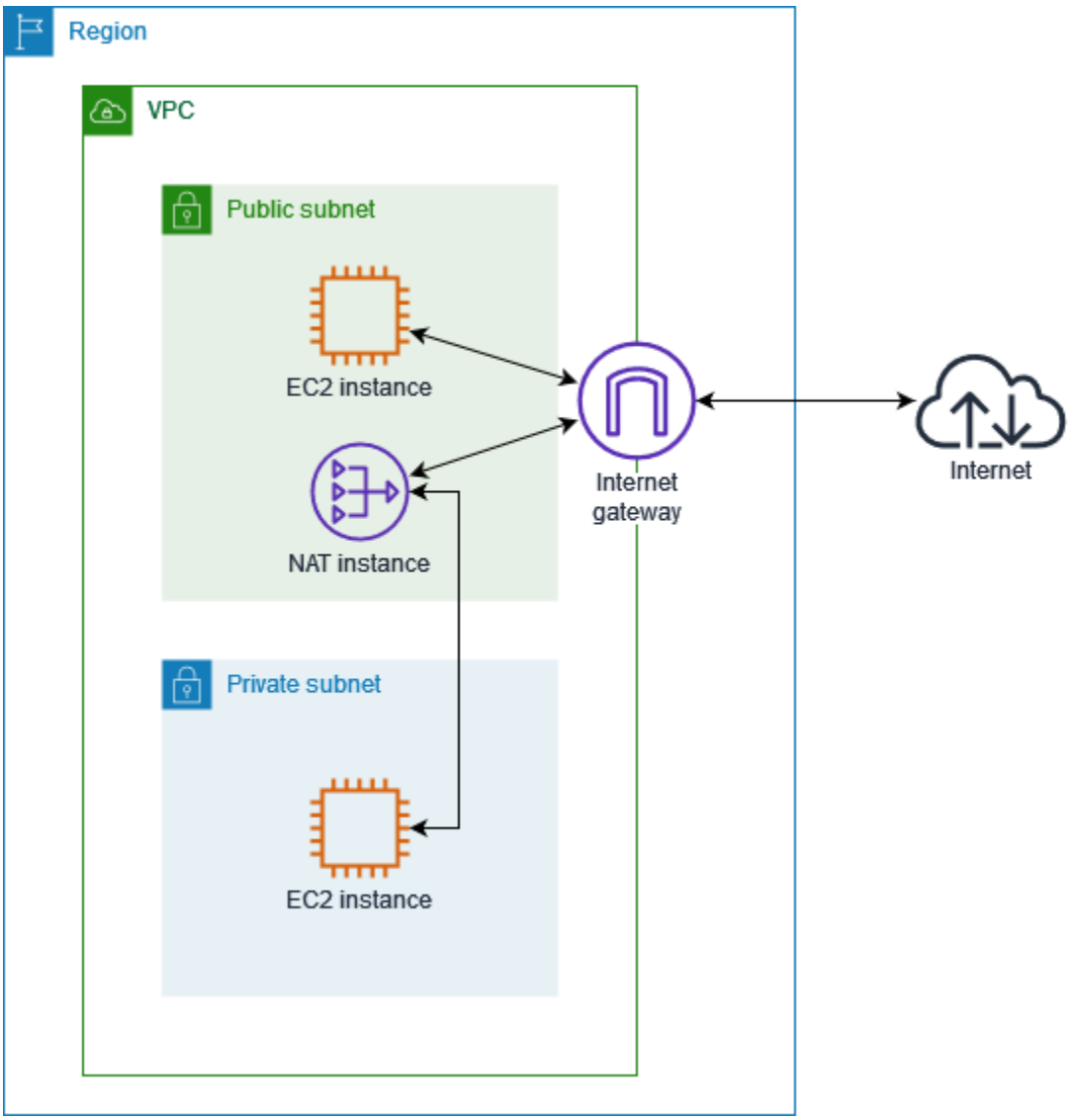
Daftar Isi

- Dasar-dasar instans NAT
- Aktifkan sumber daya pribadi untuk berkomunikasi di luar VPC

Dasar-dasar instans NAT

Gambar berikut mengilustrasikan dasar-dasar NAT. Tabel rute yang terkait dengan subnet pribadi mengirimkan lalu lintas internet dari instance di subnet pribadi ke instance NAT di subnet publik. Instans NAT kemudian mengirimkan lalu lintas ke gateway internet. Lalu lintas dikaitkan dengan alamat IP publik dari instance NAT. Instans NAT menentukan nomor port yang tinggi untuk respon; jika respon datang kembali, instans NAT mengirimkannya ke sebuah instans di subnet privat berdasarkan nomor port untuk respon.

Instans NAT harus memiliki akses internet, sehingga harus berada di subnet publik (subnet yang memiliki tabel rute dengan rute ke gateway internet), dan harus memiliki alamat IP publik atau alamat IP Elastic.



Untuk memulai dengan instans NAT, buat NAT AMI, buat grup keamanan untuk instance NAT, dan luncurkan instance NAT ke VPC Anda.

Kuota instans NAT Anda tergantung pada kuota instans Anda untuk Wilayah. Untuk informasi selengkapnya, lihat kuota layanan Amazon EC2 di Referensi Umum AWS.

Aktifkan sumber daya pribadi untuk berkomunikasi di luar VPC

Bagian ini menjelaskan cara membuat dan bekerja dengan instans NAT untuk mengaktifkan sumber daya di subnet pribadi untuk berkomunikasi di luar cloud pribadi virtual.

Tugas

- 1. Membuat VPC untuk instance NAT

- 2. Membuat grup keamanan untuk instance NAT
- 3. Buat NAT AMI
- 4. Luncurkan instance NAT
- 5. Nonaktifkan source/destination pemeriksaan
- 6. Perbarui tabel rute
- 7. Menguji instans NAT Anda

1. Membuat VPC untuk instance NAT

Gunakan prosedur berikut untuk membuat VPC dengan subnet publik dan subnet pribadi.

Untuk membuat VPC

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pilih Buat VPC.
3. Untuk Sumber Daya yang akan dibuat, pilih VPC dan lainnya.
4. Untuk Pembuatan otomatis tanda nama, masukkan nama untuk VPC.
5. Untuk mengkonfigurasi subnet, lakukan hal berikut:
    a. Untuk Jumlah Zona Ketersediaan, pilih 1 atau 2, tergantung kebutuhan Anda.
    b. Untuk Jumlah subnet publik, pastikan Anda memiliki satu subnet publik per Zona Ketersediaan.
    c. Untuk Jumlah subnet pribadi, pastikan Anda memiliki satu subnet pribadi per Zona Ketersediaan.
6. Pilih Buat VPC.

2. Membuat grup keamanan untuk instance NAT

Buat grup keamanan dengan aturan yang dijelaskan dalam tabel berikut. Aturan ini memungkinkan instance NAT Anda menerima lalu lintas terikat internet dari instans di subnet pribadi, serta lalu lintas SSH dari jaringan Anda. Instans NAT juga dapat mengirim lalu lintas ke internet, yang membuat instans di subnet privat bisa mendapatkan pembaruan perangkat lunak.

Berikut ini adalah aturan inbound yang direkomendasikan.

Sumber	Protokol	Rentang Port	Komentar
Private subnet CIDR	TCP	80	Izinkan lalu lintas HTTP masuk dari server di subnet privat
Private subnet CIDR	TCP	443	Izinkan lalu lintas HTTPS masuk dari server di subnet privat
Public IP address range of your network	TCP	22	Izinkan akses SSH masuk ke instance NAT dari jaringan Anda (melalui gateway internet)

Berikut ini adalah aturan keluar yang direkomendasikan.

Tujuan	Protokol	Rentang Port	Komentar
0.0.0. 0/0	TCP	80	Izinkan akses HTTP keluar ke internet
0.0.0. 0/0	TCP	443	Izinkan akses HTTPS keluar ke internet

Untuk membuat grup keamanan

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Grup keamanan.
3. Pilih Buat grup keamanan.
4. Masukkan nama dan deskripsi untuk grup keamanan tersebut.
5. Untuk VPC, pilih ID VPC untuk instance NAT Anda.
6. Tambahkan aturan untuk lalu lintas masuk di bawah aturan Inbound sebagai berikut:
    a. Pilih Tambahkan aturan. Pilih HTTP untuk Jenis dan masukkan rentang alamat IP subnet pribadi Anda untuk Sumber.

b. Pilih Tambahkan aturan. Pilih HTTPS untuk Jenis dan masukkan rentang alamat IP subnet pribadi Anda untuk Sumber.

c. Pilih Tambahkan aturan. Pilih SSH untuk Jenis dan masukkan rentang alamat IP jaringan Anda untuk Sumber.

7. Tambahkan aturan untuk lalu lintas keluar di bawah aturan Outbound sebagai berikut:

a. Pilih Tambahkan aturan. Pilih HTTP untuk Type dan masukkan 0.0.0. 0/0 untuk tujuan.

b. Pilih Tambahkan aturan. Pilih HTTPS untuk Type dan masukkan 0.0.0. 0/0 untuk tujuan.

8. Pilih Buat grup keamanan.

Untuk informasi selengkapnya, lihat Grup keamanan.

3. Buat NAT AMI

NAT AMI dikonfigurasi untuk menjalankan NAT pada instance EC2. Anda harus membuat NAT AMI dan kemudian meluncurkan instance NAT Anda menggunakan NAT AMI Anda.

Jika Anda berencana menggunakan sistem operasi selain Amazon Linux untuk NAT AMI Anda, lihat dokumentasi untuk sistem operasi ini untuk mempelajari cara mengkonfigurasi NAT. Pastikan untuk menyimpan pengaturan ini sehingga tetap ada bahkan setelah reboot instance.

Cara membuat NAT AMI untuk Amazon Linux

1. Luncurkan instance EC2 yang menjalankan AL2023 atau Amazon Linux 2. Pastikan untuk menentukan grup keamanan yang Anda buat untuk instance NAT.
2. Hubungkan ke instance Anda dan jalankan perintah berikut pada instance untuk mengaktifkan iptables.

```
sudo yum install iptables-services -y
sudo systemctl enable iptables
sudo systemctl start iptables
```

3. Lakukan hal berikut pada instance untuk mengaktifkan penerusan IP sehingga tetap ada setelah reboot:

a. Menggunakan editor teks, seperti nano atauvim, buat file konfigurasi berikut:`/etc/sysctl.d/custom-ip-forwarding.conf`.

b. Tambahkan baris berikut ke file konfigurasi.

```
net.ipv4.ip_forward=1
```

c. Simpan file konfigurasi dan keluar dari editor teks.

d. Jalankan perintah berikut untuk menerapkan file konfigurasi.

```
sudo sysctl -p /etc/sysctl.d/custom-ip-forwarding.conf
```

4. Jalankan perintah berikut pada instance, dan catat nama antarmuka jaringan utama. Anda akan membutuhkan informasi ini untuk langkah selanjutnya.

```
netstat -i
```

Dalam contoh berikut output, `docker0` adalah antarmuka jaringan yang dibuat oleh docker, `eth0` adalah antarmuka jaringan utama, dan `lo` merupakan antarmuka loopback.

```
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
docker0   1500        0      0      0 0             0      0      0      0 BMU
eth0      9001  7276052      0      0 0       5364991      0      0      0 BMRU
lo       65536   538857      0      0 0        538857      0      0      0 LRU
```

Dalam contoh output berikut, antarmuka jaringan utama adalah`enX0`.

```
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enX0      9001     1076      0      0 0          1247      0      0      0 BMRU
lo       65536       24      0      0 0            24      0      0      0 LRU
```

Dalam contoh output berikut, antarmuka jaringan utama adalah`ens5`.

```
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
ens5      9001    14036      0      0 0          2116      0      0      0 BMRU
lo       65536       12      0      0 0            12      0      0      0 LRU
```

5. Jalankan perintah berikut pada instance untuk mengkonfigurasi NAT. Jika antarmuka jaringan utama tidak`eth0`, ganti *`eth0`* dengan antarmuka jaringan utama yang Anda catat pada langkah sebelumnya.

```
sudo /sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
sudo /sbin/iptables -F FORWARD
```

```
sudo service iptables save
```

6. Buat NAT AMI dari instance EC2. Untuk informasi selengkapnya, lihat Membuat AMI Linux dari instance di Panduan Pengguna Amazon EC2.

4. Luncurkan instance NAT

Gunakan prosedur berikut untuk meluncurkan instance NAT menggunakan VPC, grup keamanan, dan NAT AMI yang Anda buat.

Untuk meluncurkan instance NAT

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada dasbor, pilih Luncurkan instans.
3. Untuk Nama, masukkan nama untuk instance NAT Anda.
4. Untuk Gambar Aplikasi dan OS, pilih NAT AMI Anda (pilih Jelajahi lebih banyak AMI, AMI Saya).
5. Untuk Jenis Instance, pilih jenis instans yang menyediakan sumber daya komputasi, memori, dan penyimpanan yang dibutuhkan instans NAT Anda.
6. Untuk Pasangan kunci, pilih pasangan kunci yang ada atau pilih Buat pasangan kunci baru.
7. Untuk pengaturan jaringan, lakukan hal berikut:
   a. Pilih Edit.
   b. Untuk VPC, pilih VPC yang Anda buat.
   c. Untuk Subnet, pilih subnet publik yang Anda buat.
   d. Untuk IP Auto-assign publik, pilih Aktifkan. Atau, setelah Anda meluncurkan instance NAT, alokasikan alamat IP Elastic dan tetapkan ke instance NAT.
   e. Untuk Firewall, pilih Pilih grup keamanan yang ada dan kemudian pilih grup keamanan yang Anda buat.
8. Pilih Luncurkan instans. Pilih ID instance untuk membuka halaman detail instance. Tunggu status instance berubah menjadi Run ning dan pemeriksaan status berhasil.
9. N source/destination onaktifkan pemeriksaan untuk instance NAT (lihat5. Nonaktifkan source/destination pemeriksaan).
10. Perbarui tabel rute untuk mengirim lalu lintas ke instance NAT (lihat6. Perbarui tabel rute).

5. Nonaktifkan source/destination pemeriksaan

Setiap instans EC2 melakukan source/destination pemeriksaan secara default. Ini berarti bahwa instans harus menjadi sumber atau tujuan dari setiap lalu lintas yang dikirim atau diterima. Namun, instans NAT harus dapat mengirim dan menerima lalu lintas ketika sumber atau tujuan bukan dirinya sendiri. Oleh karena itu, Anda harus menonaktifkan source/destination pemeriksaan pada instance NAT.

Untuk menonaktifkan peng source/destination ecekan

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Instans.
3. Pilih instance NAT.
4. Pilih T ind akan, Jaringan, Ubah source/destination cek.
5. Untuk Source/destination memeriksa, pilih Stop.
6. Pilih Simpan.
7. Jika instans NAT memiliki antarmuka jaringan sekunder, pilih dari Antarmuka jaringan pada tab Jaringan. Pilih ID antarmuka untuk membuka halaman antarmuka jaringan. Pilih T ind akan, U source/dest bah. cent ang, hapus Aktifkan, dan pilih Simpan.

6. Perbarui tabel rute

Tabel rute untuk subnet pribadi harus memiliki rute yang mengirimkan lalu lintas internet ke instance NAT.

Untuk memperbarui tabel rute

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Tabel rute.
3. Pilih tabel rute untuk subnet pribadi.
4. Pada tab Rute, pilih Edit rute, lalu pilih Tambahkan rute.
5. Masukkan 0.0.0. 0/0 untuk Tujuan dan ID instance dari instance NAT untuk Target.
6. Pilih Simpan perubahan.

Untuk informasi selengkapnya, lihat Konfigurasikan tabel rute.

7. Menguji instans NAT Anda

Setelah Anda meluncurkan instance NAT dan menyelesaikan langkah-langkah konfigurasi di atas, Anda dapat menguji apakah instance di subnet pribadi Anda dapat mengakses internet melalui instance NAT dengan menggunakan instance NAT sebagai server bastion.

Tugas

- Langkah 1: Perbarui grup keamanan instance NAT
- Langkah 2: Luncurkan instance uji di subnet pribadi
- Langkah 3: Ping ICMP-enabled situs web
- Langkah 4: Membersihkan

Langkah 1: Perbarui grup keamanan instance NAT

Untuk mengizinkan instans di subnet pribadi mengirim lalu lintas ping ke instance NAT, tambahkan aturan untuk mengizinkan lalu lintas ICMP masuk dan keluar. Untuk mengizinkan instance NAT berfungsi sebagai server bastion, tambahkan aturan untuk mengizinkan lalu lintas SSH keluar ke subnet pribadi.

Untuk memperbarui grup keamanan instans NAT

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Grup keamanan.
3. Pilih kotak centang untuk grup keamanan yang terkait dengan instans NAT Anda.
4. Pada tab Inbound rules (Aturan ke dalam), pilih Edit inbound rules (Edit aturan ke dalam).
5. Pilih Tambahkan aturan. Pilih Semua ICMP - IPv4 untuk Tipe. Pilih Kustom untuk Sumber dan masukkan rentang alamat IP subnet pribadi Anda. Pilih Simpan aturan.
6. Pada tab Aturan keluar, pilih Edit aturan keluar.
7. Pilih Tambahkan aturan. Pilih SSH untuk Tipe. Pilih Kustom untuk Tujuan dan masukkan rentang alamat IP subnet pribadi Anda.
8. Pilih Tambahkan aturan. Pilih Semua ICMP - IPv4 untuk Tipe. Pilih Di Mana Saja - IPv4 untuk Tujuan. Pilih Simpan aturan.

Langkah 2: Luncurkan instance uji di subnet pribadi

Luncurkan sebuah instans ke subnet privat Anda. Anda harus mengizinkan akses SSH dari instance NAT, dan Anda harus menggunakan pasangan kunci yang sama yang Anda gunakan untuk instance NAT.

Untuk meluncurkan instance uji di subnet pribadi

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada dasbor, pilih Luncurkan instans.
3. Pilih subnet pribadi Anda.
4. Jangan menetapkan alamat IP publik ke instance ini.
5. Pastikan grup keamanan untuk instance ini mengizinkan akses SSH masuk dari instans NAT Anda, atau dari rentang alamat IP subnet publik Anda, dan lalu lintas ICMP keluar.
6. Pilih pasangan kunci yang sama yang Anda gunakan untuk instance NAT.

Langkah 3: Ping ICMP-enabled situs web

Untuk memverifikasi bahwa instance pengujian di subnet pribadi Anda dapat menggunakan instance NAT Anda untuk berkomunikasi dengan internet, jalankan ping perintah.

Untuk menguji koneksi internet dari instance pribadi Anda

1. Dari komputer lokal Anda, konfigurasikan penerusan agen SSH, sehingga Anda dapat menggunakan instance NAT sebagai server bastion.

   Linux and macOS

   ```
   ssh-add key.pem
   ```

   Windows

   Unduh dan instal Pageant, jika belum diinstal.

   Konversikan kunci pribadi Anda menggunakan PuttyGen.

   Mulai Pageant, buka menu konteks untuk ikon Pageant di bilah tugas (mungkin tersembunyi), dan pilih Tam bah Kunci. Pilih file.ppk yang Anda buat, masukkan frasa sandi jika diperlukan, dan pilih Buka.

2. Dari komputer lokal Anda, sambungkan ke instance NAT Anda.

   Linux and macOS

   ```
   ssh -A ec2-user@nat-instance-public-ip-address
   ```

   Windows

   Hubungkan ke instance NAT Anda menggunakan PuTTY. Untuk Auth, Anda harus memilih lz inkan penerusan agen dan biarkan file kunci pribadi untuk otentikasi kosong.

3. Dari instance NAT, jalankan ping perintah, tentukan situs web yang diaktifkan untuk ICMP.

   ```
   [ec2-user@ip-10-0-4-184]$ ping ietf.org
   ```

   Untuk mengonfirmasi bahwa instance NAT Anda memiliki akses internet, verifikasi bahwa Anda menerima output seperti berikut ini, lalu tekan Ctrl+C untuk membatalkan ping perintah. Jika tidak, verifikasi bahwa instance NAT berada di subnet publik (tabel rute memiliki rute ke gateway internet).

   ```
   PING ietf.org (104.16.45.99) 56(84) bytes of data.
   64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=1 ttl=33 time=7.88 ms
   64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=2 ttl=33 time=8.09 ms
   64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=3 ttl=33 time=7.97 ms
   ...
   ```

4. Dari instance NAT Anda, sambungkan ke instance Anda di subnet pribadi Anda dengan menggunakan alamat IP pribadinya.

   ```
   [ec2-user@ip-10-0-4-184]$ ssh ec2-user@private-server-private-ip-address
   ```

5. Dari instance pribadi Anda, uji apakah Anda dapat terhubung ke internet dengan menjalankan ping perintah.

   ```
   [ec2-user@ip-10-0-135-25]$ ping ietf.org
   ```

   Untuk mengonfirmasi bahwa instance pribadi Anda memiliki akses internet melalui instans NAT, verifikasi bahwa Anda menerima output seperti berikut ini, lalu tekan Ctrl+C untuk membatalkan ping perintah.

```
PING ietf.org (104.16.45.99) 56(84) bytes of data.
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=1 ttl=33 time=8.76 ms
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=2 ttl=33 time=8.26 ms
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=3 ttl=33 time=8.27 ms
...
```

Pemecahan masalah

Jika ping perintah gagal dari server di subnet pribadi, gunakan langkah-langkah berikut untuk memecahkan masalah:

- Verifikasi bahwa Anda melakukan ping ke situs web yang mengaktifkan ICMP. Jika tidak, server Anda tidak dapat menerima paket balasan. Untuk menguji ini, jalankan ping perintah yang sama dari terminal baris perintah di komputer Anda sendiri.
- Pastikan grup keamanan untuk instans NAT Anda mengizinkan lalu lintas ICMP masuk dari subnet pribadi Anda. Jika tidak, instance NAT Anda tidak dapat menerima ping perintah dari instance pribadi Anda.
- Verifikasi bahwa Anda menonaktifkan source/destination pengecekan untuk instans NAT Anda. Untuk informasi selengkapnya, lihat 5. Nonaktifkan source/destination pemeriksaan.
- Pastikan Anda mengonfigurasi tabel rute dengan benar. Untuk informasi selengkapnya, lihat 6. Perbarui tabel rute.

Langkah 4: Membersihkan

Jika Anda tidak lagi memerlukan server pengujian di subnet pribadi, hentikan instans sehingga Anda tidak lagi ditagih untuk itu. Untuk informasi selengkapnya, lihat Menghentikan instans Anda di Panduan Pengguna Amazon EC2.

Jika Anda tidak lagi memerlukan instans NAT, Anda dapat menghentikan atau menghentikannya, sehingga Anda tidak lagi ditagih untuk itu. Jika Anda membuat NAT AMI, Anda dapat membuat instance NAT baru kapan pun Anda membutuhkannya.

Bandingkan gateway NAT dan instans NAT

Berikut ini adalah rangkuman tingkat tinggi tentang perbedaan antara gateway NAT dan instans NAT. Kami menyarankan Anda menggunakan gateway NAT karena gateway NAT memberikan tingkat ketersediaan dan bandwidth yang lebih baik dan mudah bagi Anda untuk mengelolanya.

Atribut	Gateway NAT	Instans NAT
Ketersediaan	Hampir selalu tersedia. Gateway NAT di setiap Availability Zone diimplementasikan dengan redundansi. Buat gateway NAT di setiap Availability Zone untuk memastikan arsitektur yang tidak tergantung zona.	Gunakan skrip untuk mengelola failover antara instans.
Bandwidth	Skala hingga 100 Gbps.	Tergantung pada bandwidth dari tipe instans.
Maintenance	Dikelola oleh AWS. Anda tidak perlu melakukan perawatan apa pun.	Dikelola oleh Anda, misalnya, dengan menginstal pembaruan perangkat lunak atau patch sistem operasi pada instans.
Performa	Software dioptimalkan untuk menangani lalu lintas NAT.	AMI generik yang dikonfigurasi untuk melakukan NAT.
Biaya	Dibebankan tergantung pada jumlah gateway NAT yang Anda gunakan, durasi penggunaan, dan jumlah data yang Anda kirim melalui gateway NAT.	Dibebankan tergantung pada jumlah instans NAT yang Anda gunakan, durasi penggunaan, dan tipe dan ukuran instans.
Tipe dan ukuran	Penawaran seragam; Anda tidak perlu memutuskan jenis atau ukuran.	Pilih tipe dan ukuran instans yang sesuai, sesuai dengan beban kerja yang Anda perkirakan.
Alamat IP publik	Pilih alamat IP Elastis untuk dikaitkan dengan gateway NAT publik saat pembuatan.	Gunakan alamat IP Elastis atau alamat IP publik dengan instans NAT. Anda dapat mengubah alamat IP publik kapan saja dengan mengaitkan alamat IP Elastis baru dengan instans.
Alamat IP privat	Secara otomatis dipilih dari rentang alamat IP subnet saat Anda ketika Anda membuat gateway.	Tetapkan alamat IP privat tertentu dari rentang alamat IP subnet saat Anda meluncurkan instans.
Grup keamanan	Anda tidak dapat mengaitkan grup keamanan dengan gateway NAT. Anda	Kaitkan instans NAT Anda dan sumber daya di belakang instans NAT Anda

Atribut	Gateway NAT	Instans NAT
	dapat mengaitkannya dengan sumber daya di belakang gateway NAT untuk mengontrol lalu lintas masuk dan keluar.	guna mengontrol lalu lintas masuk dan keluar.
ACL jaringan	Anda dapat menggunakan ACL jaringan untuk mengontrol lalu lintas ke dan dari subnet tempat gateway NAT Anda berada.	Menggunakan ACL jaringan untuk mengontrol lalu lintas ke dan dari subnet tempat instans NAT Anda berada.
Log alur	Gunakan log alur untuk menangkap lalu lintas.	Gunakan log alur untuk menangkap lalu lintas.
Penerusan port	Tidak didukung.	Secara manual menyesuaikan konfigurasi untuk mendukung penerusan port.
Server bastion	Tidak didukung.	Gunakan sebagai server bastion.
Metrik lalu lintas	Lihat CloudWatch metrik untuk gateway NAT.	Lihat CloudWatch metrik untuk instance.
Perilaku waktu habis	Ketika waktu koneksi habis, gateway NAT mengembalikan paket RST ke sumber daya di belakang gateway NAT yang mencoba untuk melanjutkan koneksi (tidak mengirim paket FIN).	Ketika waktu koneksi habis, instans NAT mengirimkan paket FIN untuk sumber daya di belakang instans NAT untuk menutup koneksi.
Fragmentasi IP	Mendukung penerusan paket terfragmentasi IP untuk protokol UDP. Tidak mendukung fragmentasi untuk protokol TCP dan ICMP. Paket terfragmentasi untuk protokol ini akan turun.	Mendukung perakitan kembali paket terfragmentasi IP untuk protokol UDP, TCP, dan ICMP.

Migrasi dari instance NAT ke gateway NAT

Jika Anda sudah menggunakan instance NAT, kami sarankan Anda menggantinya dengan gateway NAT. Anda dapat membuat gateway NAT di subnet yang sama dengan instance NAT Anda, lalu mengganti rute yang ada di tabel rute yang menunjuk ke instance NAT dengan rute yang mengarah ke gateway NAT. Untuk menggunakan alamat IP Elastic yang sama untuk gateway NAT yang saat ini Anda gunakan untuk instans NAT, Anda harus terlebih dahulu melepaskan alamat IP Elastic dari instans NAT Anda dan kemudian mengaitkannya dengan gateway NAT saat Anda membuat gateway.

Jika Anda mengubah perutean Anda dari instans NAT untuk gateway NAT, atau jika Anda memisahkan alamat IP Elastis dari instans NAT Anda, koneksi saat ini dijatuhkan dan harus kembali disambungkan kembali. Pastikan bahwa Anda tidak memiliki tugas-tugas penting (atau tugas-tugas lain yang beroperasi melalui instans NAT) yang berjalan.

Mengaitkan alamat IP Elastic dengan sumber daya di VPC Anda

Alamat IP Elastic adalah alamat IPv4 publik statis yang dirancang khusus untuk sifat dinamis komputasi awan. Fitur ini memungkinkan Anda untuk mengaitkan alamat IP Elastic dengan instance atau antarmuka jaringan apa pun dalam Virtual Private Cloud (VPC) apa pun di AWS akun Anda. Dengan menggunakan alamat IP Elastic, Anda dapat membuka sejumlah manfaat yang menyederhanakan pengelolaan dan ketahanan infrastruktur berbasis cloud Anda.

Salah satu keuntungan utama dari alamat IP Elastic adalah kemampuannya untuk menutupi kegagalan sebuah instance. Jika instans mengalami pemadaman tak terduga atau perlu diganti, Anda dapat memetakan ulang alamat IP Elastic terkait ke instance lain dalam VPC Anda. Proses failover ini memastikan bahwa aplikasi dan layanan Anda mempertahankan titik akhir publik yang konsisten dan andal, meminimalkan downtime dan memberikan pengalaman pengguna yang unggul.

Selain itu, alamat IP Elastic menawarkan fleksibilitas dalam cara Anda mengelola sumber daya jaringan Anda. Anda dapat mengaitkan dan memisahkan alamat ini secara terprogram sesuai kebutuhan, memungkinkan Anda mengarahkan lalu lintas ke instans yang berbeda berdasarkan kebutuhan bisnis Anda yang terus berkembang. Alokasi dinamis alamat IP publik ini memberdayakan Anda untuk beradaptasi dengan perubahan permintaan, meningkatkan skala infrastruktur Anda, dan menerapkan arsitektur inovatif tanpa kendala penugasan IP statis.

Di luar penggunaannya misalnya failover, alamat IP Elastic juga dapat berfungsi sebagai pengidentifikasi stabil untuk sumber daya berbasis cloud Anda. Ini dapat bermanfaat saat

mengonfigurasi layanan eksternal, seperti catatan DNS atau aturan firewall, untuk berkomunikasi dengan aplikasi yang AWS di-host. Dengan mengaitkan alamat IP publik yang persisten, Anda dapat memastikan konfigurasi jaringan Anda di masa mendatang dan menghindari kebutuhan untuk memperbarui referensi eksternal saat instance yang mendasarinya diganti atau diskalakan.

Daftar Isi

- Konsep dan aturan alamat IP Elastis
- Mulai gunakan alamat IP Elastic

Konsep dan aturan alamat IP Elastis

Untuk menggunakan alamat IP Elastis, pertama-tama alokasikan alamat IP Elastis untuk digunakan di akun Anda. Kemudian, Anda dapat mengaitkannya dengan sebuah instans atau antarmuka jaringan di VPC Anda. Alamat IP Elastic Anda tetap dialokasikan ke AWS akun Anda sampai Anda secara eksplisit melepaskannya.

Alamat IP Elastis adalah properti antarmuka jaringan. Anda dapat mengaitkan sebuah alamat IP Elastis dengan suatu instans dengan memperbarui antarmuka jaringan yang dilampirkan ke instans tersebut. Keuntungan dari mengaitkan alamat IP Elastis dengan antarmuka jaringan alih-alih langsung mengaitkannya dengan instans adalah bahwa Anda dapat memindahkan semua atribut antarmuka jaringan dari satu instans ke instans lain dalam satu langkah saja. Untuk informasi selengkapnya, lihat Antarmuka jaringan elastis di Panduan Pengguna Amazon EC2.

Aturan-aturan berikut berlaku:

- Sebuah alamat IP Elastis dapat dikaitkan dengan sebuah instans atau antarmuka jaringan.
- Anda dapat memindahkan alamat IP Elastis dari satu instans atau antarmuka jaringan ke instans lainnya.
- Jika Anda mengaitkan alamat IP Elastic dengan antarmuka jaringan utama instans Anda, alamat IPv4 publik saat ini (jika ada) dilepaskan ke kumpulan alamat IP publik. Jika Anda memutuskan alamat IP Elastic, antarmuka jaringan utama secara otomatis ditetapkan alamat IPv4 publik baru dalam beberapa menit. Ini tidak berlaku jika Anda sudah melampirkan antarmuka jaringan kedua ke instans Anda.
- Anda dibatasi hingga lima alamat IP Elastis. Untuk membantu menyimpannya, Anda dapat menggunakan perangkat NAT. Untuk informasi selengkapnya, lihat Sambungkan ke internet atau jaringan lain menggunakan perangkat NAT.

- Alamat IP Elastis untuk IPv6 tidak di-support.
- Anda dapat memberi tag alamat IP Elastis yang dialokasikan untuk digunakan di VPC, namun, tag alokasi biaya tidak di-support. Jika Anda memulihkan alamat IP Elastis, tag tidak ikut terpulihkan.
- Anda dapat mengakses alamat IP Elastis dari internet ketika grup keamanan dan ACL jaringan mengizinkan lalu lintas dari alamat IP sumber. Lalu lintas balasan dari dalam VPC kembali ke internet akan memerlukan gateway internet. Untuk informasi selengkapnya, lihat Grup keamanan dan ACL jaringan.
- Anda dapat menggunakan salah satu opsi berikut untuk alamat IP Elastis:
  - Biarkan Amazon menyediakan alamat IP Elastis. Saat Anda memilih opsi ini, Anda dapat mengaitkan alamat-alamat IP Elastis dengan grup border jaringan. Ini adalah lokasi tempat kita mengiklankan blok CIDR. Mengatur grup perbatasan jaringan membatasi blok CIDR ke grup ini.
  - Gunakan alamat-alamat IP Anda sendiri. Untuk informasi tentang membawa alamat IP Anda sendiri, lihat Mem bawa alamat IP Anda sendiri (BYOIP) di Panduan Pengguna Amazon EC2.
- Alamat IPv4 publik mendukung tag alokasi biaya. Jika Anda menerapkan tag ke alamat IP Elastic, Anda dapat menggunakan tag tersebut untuk melacak biaya alamat IPv4 publik di AWS Cost Explorer.

  Sebelum Anda dapat menggunakan tag sebagai tag alokasi biaya, Anda harus mengaktifkan tag. Untuk informasi selengkapnya, lihat Mengaktifkan tag alokasi biaya yang ditentukan AWS Billing pengguna di Panduan Pengguna. Perhatikan bahwa setelah Anda membuat dan menerapkan tag yang ditentukan pengguna ke sumber daya Anda, diperlukan waktu hingga 24 jam agar kunci tag muncul di halaman tag alokasi biaya untuk aktivasi.

  Setelah tag alokasi biaya diaktifkan...

  - Untuk semua alamat IPv4 publik (termasuk alamat IPv4 publik yang ditetapkan ke instans EC2 dan alamat IP Elastic) yang terkait dengan antarmuka jaringan elastis, Anda dapat melihat biaya yang terkait dengan alamat IPv4 publik di Cost Explorer dengan memilih Jenis Penggunaan > PublicIPv4InUseAddress (Jam).
  - Jika alamat IP Elastic yang ditandai tidak terkait dengan ENI atau dikaitkan dengan sumber daya yang dihentikan (seperti instans EC2 yang dihentikan), alamat tersebut dianggap sebagai alamat IPv4 yang tidak aktif. Anda dapat melihat biaya yang terkait dengan alamat IPv4 idle di Cost Explorer dengan memilih Jenis Penggunaan > PublicIPv4IdleAddress (Jam).

  Untuk informasi selengkapnya tentang Cost Explorer, lihat Meng analisis biaya Anda dengan AWS Cost Explorer dalam Panduan AWS Billing Pengguna.

Alamat IP Elastis bersifat regional. Untuk informasi selengkapnya tentang penggunaan Global Accelerator untuk menyediakan alamat IP global, lihat Penggunaan alamat IP statis global alih-alih alamat IP statis regional di AWS Global Accelerator Panduan Developer.

Untuk informasi selengkapnya tentang harga untuk alamat IP Elastic, lihat Alamat IPv4 Publik di Harga Amazon VPC.

Mulai gunakan alamat IP Elastic

Bagian berikut menjelaskan bagaimana Anda bisa mulai menggunakan alamat IP Elastic.

Tugas

- 1. Alokasikan sebuah alamat IP Elastis
- 2. Kaitkan sebuah alamat IP Elastis
- 3. Pisahkan alamat IP Elastis
- 4. Transfer alamat IP Elastis
- 5. Melepas alamat IP Elastis
- 6. Memulihkan alamat IP Elastis
- Ikhtisar baris perintah

1. Alokasikan sebuah alamat IP Elastis

Sebelum Anda menggunakan IP Elastic, Anda harus mengalokasikan satu IP Elastis untuk digunakan di VPC Anda.

Untuk mengalokasikan Alamat IP elastis

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih IP Elastis.
3. Pilih Alokasi alamat IP elastis.
4. (Opsional) Ketika Anda mengalokasikan alamat IP elastis (EIP), Anda memilih grup batas jaringan untuk mengalokasikan EIP. Grup perbatasan jaringan adalah kumpulan Zona Ketersediaan (AZ), Zona Lokal, atau Zona Panjang Gelombang yang mengiklan AWS kan alamat IP publik. Zona Lokal dan Zona Panjang Gelombang mungkin memiliki grup perbatasan jaringan yang berbeda dari AZ di Wilayah untuk memastikan latensi minimum atau jarak fisik antara AWS jaringan dan pelanggan yang mengakses sumber daya di Zona ini.

> **Important**
>
> Anda harus mengalokasikan EIP dalam grup perbatasan jaringan yang sama dengan AWS sumber daya yang akan dikaitkan dengan EIP. EIP dalam satu grup perbatasan jaringan hanya dapat diiklankan di zona dalam grup perbatasan jaringan tersebut dan tidak di zona lain yang diwakili oleh grup perbatasan jaringan lainnya.

Jika Anda mengaktifkan Local Zones atau Wavelength Zone (untuk informasi selengkapnya, lihat Mengaktifkan Local Zones atau Mengaktifkan Wavelength Zone), Anda dapat memilih grup perbatasan jaringan untuk AZ, Local Zones, atau Wavelength Zone. Pilih grup perbatasan jaringan dengan hati-hati karena EIP dan AWS sumber daya yang terkait dengannya harus berada di grup perbatasan jaringan yang sama. Anda dapat menggunakan konsol EC2 untuk melihat grup perbatasan jaringan tempat Zona Ketersediaan, Local Zones, atau Wavelength Zone berada (lihat Local Zones). Biasanya, semua Zona Ketersediaan di Wilayah milik grup perbatasan jaringan yang sama, sedangkan Local Zones atau Wavelength Zone milik grup perbatasan jaringan mereka sendiri yang terpisah.

Jika Anda tidak mengaktifkan Local Zones atau Wavelength Zone, saat Anda mengalokasikan EIP, grup perbatasan jaringan yang mewakili semua AZ untuk Wilayah tersebut (seperti `us-west-2`) telah ditentukan sebelumnya untuk Anda dan Anda tidak dapat mengubahnya. Ini berarti bahwa EIP yang Anda alokasikan ke grup perbatasan jaringan ini akan diiklankan di semua AZ di Wilayah tempat Anda berada.

5. Untuk Kumpulan alamat IPv4 publik, pilih salah satu dari berikut ini:

   - Kumpulan alamat IP Amazon—Jika Anda menginginkan sebuah alamat IPv4 dialokasikan dari kumpulan alamat IP Amazon.
   - Kumpulan alamat IPv4 publik saya —Jika Anda ingin mengalokasikan alamat IPv4 dari kumpulan alamat IP yang telah Anda bawa ke akun Anda. AWS Opsi ini dinonaktifkan jika Anda tidak memiliki kumpulan alamat IP.
   - Kumpulan alamat IPv4 yang dimiliki pelanggan—Jika Anda ingin mengalokasikan sebuah alamat IPv4 dari kumpulan alamat yang dibuat dari jaringan on-premise Anda untuk digunakan dengan sebuah Outpost. Opsi ini hanya tersedia jika Anda memiliki Pos Terdepan.

6. (Opsional) Tambahkan atau hapus tanda.

   [Menambahkan tanda] Pilih Tambahkan tanda baru dan lakukan hal berikut:

- Untuk Kunci, masukkan nama kunci.
- Untuk Nilai, masukkan nilai kunci.

[Hapus tag] Pilih H apus di sebelah kanan Kunci dan Nilai tag.

7. Pilih Alokasikan.

2. Kaitkan sebuah alamat IP Elastis

Anda dapat mengaitkan alamat IP Elastis dengan instans atau antarmuka jaringan yang sedang berjalan di VPC Anda.

Setelah Anda mengaitkan alamat IP Elastis dengan instans Anda, instans tersebut menerima nama host DNS publik jika nama host DNS diaktifkan. Untuk informasi selengkapnya, lihat Atribut DNS untuk VPC Anda.

Untuk mengaitkan sebuah alamat IP Elastis dengan sebuah instans atau antarmuka jaringan

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di jendela navigasi, pilih IP Elastis.
3. Pilih alamat IP Elastis yang dialokasikan untuk digunakan dengan VPC (kolom Cakupan memiliki nilai `vpc`), lalu pilih Tindakan, Alamat IP Elastis.
4. Pilih Instans atau Antarmuka jaringan, dan kemudian pilih instans atau ID antarmuka jaringan. Pilih alamat IP pribadi yang untuk dikaitkan dengan alamat IP Elastis. Pilih Kaitkan.

3. Pisahkan alamat IP Elastis

Untuk mengubah sumber daya yang terkait dengan alamat IP elastis, Anda harus terlebih dahulu memisahkan alamat IP elastis dari sumber daya yang terkait saat ini.

Untuk memisahkan alamat IP Elastis

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di jendela navigasi, pilih IP Elastis.
3. Pilih alamat IP Elastis, dan lalu pilih Tindakan, Pisahkan alamat IP Elastis.
4. Saat diminta, pilih Pisahkan.

4. Transfer alamat IP Elastis

Bagian ini menjelaskan cara mentransfer alamat IP Elastis dari satu Akun AWS ke yang lain. Mentransfer alamat IP Elastis dapat membantu dalam situasi berikut:

- Restrukturisasi organisasi — Gunakan transfer alamat IP elastis untuk memindahkan beban kerja dengan cepat dari satu Akun AWS ke yang lain. Anda tidak perlu menunggu alamat IP Elastis baru diizinkan terdaftar di grup keamanan dan NACL Anda.
- Administrasi keamanan terpusat — Gunakan akun AWS keamanan terpusat untuk melacak dan mentransfer alamat IP Elastic yang telah diperiksa untuk kepatuhan keamanan.
- Pemulihan bencana - Gunakan transfer alamat IP Elastis untuk memetakan ulang IP dengan cepat untuk beban kerja internet yang dihadapi publik selama peristiwa darurat.

Tidak ada biaya untuk mentransfer alamat IP Elastis.

Tugas

- Aktifkan transfer alamat IP Elastis
- Nonaktifkan transfer alamat IP Elastis
- Menerima alamat IP Elastis yang ditransfer

Aktifkan transfer alamat IP Elastis

Bagian ini menjelaskan cara menerima alamat IP Elastis yang ditransfer. Perhatikan batasan berikut yang terkait dengan mengaktifkan alamat IP Elastis untuk transfer:

- Anda dapat mentransfer alamat IP Elastic dari apa pun Akun AWS (akun sumber) ke AWS akun lain di Wil AWS ayah yang sama (akun transfer).
- Saat Anda mentransfer alamat IP Elastis, ada jabat tangan dua langkah di antara. Akun AWS Ketika akun sumber memulai transfer, akun transfer memiliki tujuh hari untuk menerima transfer alamat IP Elastis. Selama tujuh hari tersebut, akun sumber dapat melihat transfer yang tertunda (misalnya di AWS konsol atau dengan menggunakan perintah describe-address- AWS CLI transfer). Setelah tujuh hari, transfer berakhir dan kepemilikan alamat IP Elastis kembali ke akun sumber.
- Transfer yang diterima terlihat ke akun sumber (misalnya di AWS konsol atau dengan menggunakan AWS CLI perintah describe-address-transfer) selama 14 hari setelah transfer diterima.

- AWS tidak memberi tahu akun transfer tentang permintaan transfer alamat IP Elastic yang tertunda. Pemilik akun sumber harus memberi tahu pemilik akun transfer bahwa ada permintaan transfer alamat IP Elastis yang harus mereka terima.
- Tanda apa pun yang terkait dengan alamat IP Elastis yang ditransfer diatur ulang saat transfer selesai.
- Anda tidak dapat mentransfer alamat IP Elastic yang dialokasikan dari kumpulan alamat IPv4 publik yang Anda Akun AWS bawa ke kumpulan alamat Bring Your Own IP (BYOIP).
- Jika Anda mencoba mentransfer alamat IP Elastic yang memiliki catatan DNS terbalik yang terkait dengannya, Anda dapat memulai proses transfer. Namun, akun transfer tidak dapat menerima transfer sampai catatan DNS terkait dihapus.
- Jika Anda telah mengaktifkan dan mengonfigurasi AWS Outposts, Anda mungkin telah mengalokasikan alamat IP Elastic dari kumpulan alamat IP milik pelanggan (CoIP). Anda tidak dapat mentransfer alamat IP Elastis yang dialokasikan dari CoIP. Namun, Anda dapat menggunakan AWS RAM untuk berbagi CoIP dengan akun lain. Untuk informasi selengkapnya, lihat alamat Customer-owned IP di Panduan AWS Outposts Pengguna.
- Anda dapat menggunakan Amazon VPC IPAM untuk melacak transfer alamat IP Elastis ke akun di organisasi AWS Organizations. Untuk informasi selengkapnya, lihat Lihat riwayat alamat IP. Jika alamat IP Elastis ditransfer ke Akun AWS di luar organisasi, riwayat audit IPAM dari alamat IP Elastis akan hilang.

Langkah-langkah ini harus diselesaikan oleh akun sumber.

Untuk mengaktifkan transfer alamat IP Elastis

1. Pastikan Anda menggunakan AWS akun sumber.
2. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
3. Di panel navigasi, pilih IP Elastis.
4. Pilih satu atau beberapa alamat IP elastis untuk mengaktifkan transfer dan pilih Tindakan, Aktifkan transfer.
5. Jika Anda mentransfer beberapa alamat IP Elastic, Anda akan melihat opsi Jenis Transfer. Pilih salah satu opsi berikut:
   - Pilih Akun tunggal jika Anda mentransfer alamat IP Elastic ke satu AWS akun.
   - Pilih Beberapa akun jika Anda mentransfer alamat IP Elastic ke beberapa AWS akun.
6. Di bawah Transfer ID akun, masukkan ID akun AWS yang ingin Anda transfer alamat IP Elastis.

7. Konfirmasikan transfer dengan memasukkan **`enable`** dalam kotak teks.
8. Pilih Kirim.
9. Untuk menerima transfer, lihat Menerima alamat IP Elastis yang ditransfer. Untuk menonaktifkan transfer, lihat Nonaktifkan transfer alamat IP Elastis.

Nonaktifkan transfer alamat IP Elastis

Bagian ini menjelaskan cara menonaktifkan transfer IP Elastis setelah transfer diaktifkan.

Langkah-langkah ini harus diselesaikan oleh akun sumber yang mengaktifkan transfer.

Untuk menonaktifkan transfer alamat IP Elastis

1. Pastikan Anda menggunakan AWS akun sumber.
2. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
3. Di panel navigasi, pilih IP Elastis.
4. Dalam daftar sumber daya IP Elastis, pastikan properti Anda diaktifkan yang menampilkan status Transfer kolom.
5. Pilih satu atau beberapa alamat IP elastis yang memiliki status Transfer Tertunda, dan pilih Tindakan, Nonaktifkan transfer.
6. Konfirmasikan dengan memasukkan **`disable`** di kotak teks.
7. Pilih Kirim.

Menerima alamat IP Elastis yang ditransfer

Bagian ini menjelaskan cara menerima alamat IP Elastis yang ditransfer.

Saat Anda mentransfer alamat IP Elastis, ada jabat tangan dua langkah di antara. Akun AWS Ketika akun sumber memulai transfer, akun transfer memiliki tujuh hari untuk menerima transfer alamat IP Elastis. Selama tujuh hari tersebut, akun sumber dapat melihat transfer yang tertunda (misalnya di AWS konsol atau dengan menggunakan perintah describe-address- AWS CLI transfer). Setelah tujuh hari, transfer berakhir dan kepemilikan alamat IP Elastis kembali ke akun sumber.

Saat menerima transfer, perhatikan pengecualian berikut yang mungkin terjadi dan cara mengatasinya:

- AddressLimitExceeded: Jika akun transfer Anda telah melebihi kuota alamat IP Elastic, akun sumber dapat mengaktifkan transfer alamat IP Elastic, tetapi pengecualian ini terjadi ketika akun

transfer mencoba menerima transfer. Secara default, semua AWS akun dibatasi hingga 5 alamat IP elastis per Wilayah. Lihat Batas alamat IP elastis di Panduan Pengguna Amazon EC2 untuk petunjuk tentang meningkatkan batas.

- InvalidTransfer.AddressCustomPtrSet: Alamat IP Elastic yang Anda coba transfer dikonfigurasi untuk menggunakan pencarian DNS terbalik. Akun sumber dapat mengaktifkan transfer untuk alamat IP Elastic. Namun, pengecualian ini terjadi ketika akun transfer mencoba menerima transfer. Untuk mengatasi masalah ini, akun sumber harus menghapus catatan DNS untuk alamat IP Elastis. Untuk informasi selengkapnya, lihat Mengh apus catatan DNS terbalik di Panduan Pengguna Amazon EC2.
- InvalidTransfer.AddressAssociated: Jika alamat IP Elastic dikaitkan dengan instans ENI atau EC2, akun sumber dapat mengaktifkan transfer untuk alamat IP Elastic, tetapi pengecualian ini terjadi ketika akun transfer mencoba menerima transfer. Untuk mengatasi masalah ini, akun sumber harus memisahkan alamat IP Elastis. Untuk informasi selengkapnya, lihat Memisahkan alamat IP Elas tic di Panduan Pengguna Amazon EC2.

Untuk pengecualian lainnya, hubungi Dukungan.

Langkah-langkah ini harus diselesaikan oleh akun transfer.

Untuk menerima transfer alamat IP Elastis

1. Pastikan Anda menggunakan akun transfer.
2. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
3. Di panel navigasi, pilih IP Elastis.
4. Pilih Tindakan, Terima transfer.
5. Tidak ada tanda yang terkait dengan alamat IP Elastis yang ditransfer dengan alamat IP Elastis saat Anda menerima transfer. Jika Anda ingin menentukan tanda Nama untuk alamat IP Elastis yang Anda terima, pilih Buat tanda dengan kunci 'Nama' dan nilai yang Anda tentukan.
6. Masukkan alamat IP Elastis yang ingin Anda transfer.
7. Jika Anda menerima beberapa alamat IP Elastis yang ditransfer, pilih Tambah alamat untuk memasukkan alamat IP Elastis tambahan.
8. Pilih Kirim.

5. Melepas alamat IP Elastis

Jika Anda tidak lagi memerlukan alamat IP Elastis, kami menyarankan Anda melepaskannya. Anda dikenakan biaya untuk alamat IP Elastic yang dialokasikan untuk digunakan dengan VPC meskipun tidak terkait dengan instance. Alamat IP Elastis tersebut tidak boleh terkait dengan sebuah instans ataupun antarmuka jaringan.

Untuk melepaskan alamat IP Elastis

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di jendela navigasi, pilih IP Elastis.
3. Pilih alamat IP Elastis, lalu pilih Tindakan, Melepas alamat IP Elastis.
4. Saat diminta, pilih Lepas.

6. Memulihkan alamat IP Elastis

Jika Anda merilis alamat IP Elastic tetapi berubah pikiran, Anda mungkin dapat memulihkannya. Anda tidak dapat memulihkan alamat IP Elastic jika telah dialokasikan ke AWS akun lain, atau jika memulihkannya mengakibatkan Anda melebihi kuota alamat IP Elastic Anda.

Anda dapat memulihkan alamat IP Elastic dengan menggunakan Amazon EC2 API atau alat baris perintah.

Untuk memulihkan alamat IP Elastic menggunakan AWS CLI

Gunakan perintah allocate-address dan tentukan alamat IP menggunakan parameter `--address`.

```
aws ec2 allocate-address --domain vpc --address 203.0.113.3
```

Ikhtisar baris perintah

Anda dapat melakukan tugas yang dijelaskan di bagian ini menggunakan baris perintah atau API. Untuk informasi selengkapnya tentang antarmuka baris perintah dan daftar API yang tersedia, lihat Bekerja dengan Amazon VPC.

Terima transfer alamat IP elastis

- menerima-alamat-transfer () AWS CLI

- Approve-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Mengalokasikan alamat IP Elastis

- allocate-address (AWS CLI)
- New-EC2Address (AWS Tools for Windows PowerShell)

Kaitkan alamat IP Elastis dengan instans atau antarmuka jaringan

- associate-address (AWS CLI)
- Register-EC2Address (AWS Tools for Windows PowerShell)

Jelaskan transfer alamat IP elastis

- deskripsi-alamat-transfer () AWS CLI
- Get-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Nonaktifkan transfer alamat IP Elastis

- nonaktifkan alamat-transfer () AWS CLI
- Disable-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Pisahkan alamat IP Elastis

- disassociate-address (AWS CLI)
- Unregister-EC2Address (AWS Tools for Windows PowerShell)

Aktifkan transfer alamat IP Elastis

- mengaktifkan-alamat-transfer () AWS CLI
- Enable-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Merilis alamat IP Elastis

- release-address (AWS CLI)

- Remove-EC2Address (AWS Tools for Windows PowerShell)

Menandai alamat IP Elastis

- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)

Lihat alamat IP Elastis Anda

- describe-addresses (AWS CLI)
- Get-EC2Address (AWS Tools for Windows PowerShell)

Hubungkan VPC Anda ke VPC dan jaringan lain menggunakan gateway transit

Anda dapat menghubungkan cloud pribadi virtual (VPC) dan jaringan lokal menggunakan gateway transit, yang bertindak sebagai hub pusat, merutekan lalu lintas antara VPC, koneksi VPN, dan koneksi. Direct Connect

Salah satu manfaat utama menggunakan gateway transit adalah kemampuan untuk memusatkan dan menyederhanakan pengelolaan konektivitas antara VPC Anda dan jaringan lokal. Alih-alih mengonfigurasi beberapa koneksi VPN atau tautan Direct Connect, Anda dapat menggunakan gateway transit sebagai satu titik integrasi, yang dapat membantu mengurangi kompleksitas keseluruhan dan overhead operasional arsitektur jaringan Anda.

Harga untuk menggunakan gateway transit didasarkan pada volume data yang ditransfer melalui gateway. Ada tarif per GB untuk data yang ditransfer masuk dan keluar dari gateway transit, serta tarif per jam terpisah untuk sumber daya gateway transit itu sendiri. Harga spesifik dapat bervariasi menurut AWS Wilayah dan dapat berubah, jadi penting untuk merujuk ke halaman AWS Transit Gateway harga saat ini untuk informasi terbaru. Dengan memahami model penetapan harga untuk gateway transit, Anda dapat merencanakan dan menganggarkan biaya berkelanjutan yang terkait dengan layanan AWS jaringan ini dengan lebih baik. Hal ini, dikombinasikan dengan efisiensi operasional dan manfaat konektivitas, menjadikan gateway transit pilihan menarik bagi organisasi yang ingin membangun solusi cloud hybrid yang dapat diskalakan dan hemat biaya.

Tabel berikut menjelaskan beberapa kasus penggunaan umum untuk gateway transit. Untuk informasi selengkapnya tentang setiap kasus penggunaan, lihat Contoh skenario gateway transit di Panduan AWS Transit Gateway Pengguna.

Contoh	Penggunaan
Router terpusat	Konfigurasikan gateway transit Anda sebagai router terpusat yang menghubungkan semua VPC, AWS Direct Connect, dan AWS Site-to-Site VPN koneksi Anda.
VPC Terisolasi	Konfigurasikan gateway transit Anda sebagai beberapa router terisolasi. Hal ini mirip dengan menggunakan beberapa transit gateway, tetapi memberikan lebih banyak fleksibilitas dalam kasus di mana rute dan lampiran mungkin berubah.
VPC terisolasi dengan layanan bersama	Konfigurasikan gateway transit Anda sebagai beberapa router terisolasi yang menggunakan layanan bersama. Hal ini mirip dengan menggunakan beberapa transit gateway, tetapi memberikan lebih banyak fleksibilitas dalam kasus di mana rute dan lampiran mungkin berubah.

Untuk informasi selengkapnya, lihat AWS Transit Gateway.

Hubungkan VPC Anda ke jaringan jarak jauh menggunakan AWS Virtual Private Network

Anda dapat menghubungkan VPC Anda ke jaringan jarak jauh dan pengguna menggunakan opsi konektivitas VPN berikut.

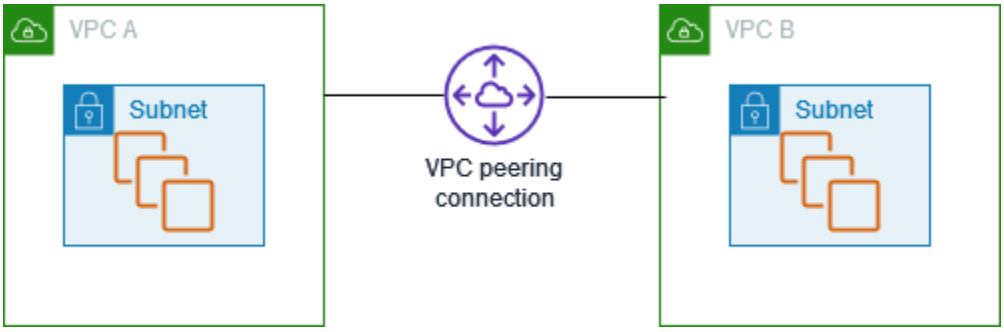
Opsi koneksi VPN	Deskripsi
AWS Site-to-Site VPN	Anda dapat membuat koneksi IPsec VPN antara VPC Anda dan jaringan jarak jauh Anda. Di AWS sisi koneksi Site-to-Site VPN, gateway pribadi virtual atau gateway transit menyediakan dua titik akhir VPN (terowongan) untuk failover otomatis. Anda mengonfigurasi perangkat gateway pelanggan Anda di sisi jarak jauh koneksi Site-to-Site VPN.

Opsi koneksi VPN	Deskripsi
	Untuk informasi selengkapnya, lihat Panduan AWS Site-to-Site VPN Pengguna.
AWS Client VPN	AWS Client VPN adalah layanan VPN berbasis klien terkelola yang memungkinkan Anda mengakses AWS sumber daya atau jaringan lokal Anda dengan aman. Dengan AWS Client VPN, Anda mengonfigurasi titik akhir yang dapat dihubungkan oleh pengguna Anda untuk membuat sesi TLS VPN yang aman. Ini memungkinkan klien untuk mengakses sumber daya di AWS atau lokal dari lokasi mana pun menggunakan klien VPN berbasis OpenVPN. Untuk informasi selengkapnya, lihat Panduan Administrator AWS Client VPN.
AWS VPN CloudHub	Jika Anda memiliki lebih dari satu jaringan jarak jauh (misalnya, beberapa kantor cabang), Anda dapat membuat beberapa AWS Site-to-Site VPN koneksi melalui gateway pribadi virtual Anda untuk mengaktif kan komunikasi antara jaringan ini. Untuk informasi selengkapnya, lihat Menyediakan komunikasi aman antar situs yang menggunakan VPN CloudHub di Panduan AWS Site-to-Site VPN Pengguna.
Peralatan VPN perangkat lunak pihak ke tiga	Anda dapat membuat koneksi VPN ke jaringan jarak jauh Anda dengan menggunakan EC2 instans Amazon di VPC Anda yang menjalank an perangkat lunak VPN pihak ketiga. AWS tidak menyediakan atau memelihara perangkat lunak VPN pihak ketiga; namun, Anda dapat memilih dari berbagai produk yang disediakan oleh mitra dan komunitas open source. Temukan peralatan VPN perangkat lunak pihak ke tiga di AWS Marketplace.

Anda juga dapat menggunakan Direct Connect untuk membuat koneksi pribadi khusus dari jaringan jarak jauh ke VPC Anda. Anda dapat menggabungkan koneksi ini dengan AWS Site-to-Site VPN untuk membuat koneksi IPsec -terenkripsi. Untuk informasi lebih lanjut, lihat Apa itu Direct Connect? dalam Direct Connect User Guide.

Hubungkan VPC menggunakan peering VPC

Koneksi peering VPC adalah fitur jaringan yang memungkinkan komunikasi aman dan langsung antara dua virtual private cloud (VPC) dalam infrastruktur. AWS Koneksi pribadi ini memungkinkan sumber daya di VPC yang diintip untuk berinteraksi satu sama lain seolah-olah mereka adalah bagian dari jaringan yang sama, menghilangkan kebutuhan untuk melintasi internet publik.



Proses pembuatan koneksi peering VPC menggunakan infrastruktur VPC yang ada untuk membuat koneksi ini, tanpa persyaratan gateway AWS Site-to-Site VPN, atau perangkat keras fisik tambahan apa pun. Desain ini memastikan bahwa tidak ada satu titik kegagalan atau hambatan bandwidth.

Salah satu keuntungan utama dari koneksi peering VPC adalah kemampuan untuk menghubungkan VPC di AWS akun yang berbeda atau bahkan Wilayah yang berbeda. AWS Fleksibilitas ini memungkinkan organisasi untuk mengintegrasikan sumber daya cloud mereka dengan mulus, apakah mereka berada dalam akun yang sama atau tersebar di beberapa akun dan lokasi geografis. Sifat pribadi koneksi juga memastikan bahwa semua lalu lintas data antara VPC yang diintip tetap berada di dalam AWS jaringan, tanpa pernah melintasi internet publik.

Kasus penggunaan untuk koneksi peering VPC sangat luas. Organisasi dapat menggunakan fitur ini untuk mengaktifkan komunikasi yang aman antara berbagai tingkatan aplikasi (seperti server web dan server database), membantu berbagi sumber daya antara beberapa tim atau unit bisnis, atau bahkan mengaktifkan arsitektur cloud hybrid dengan menghubungkan jaringan lokal ke VPC mereka AWS .

Suatu koneksi peering VPC adalah koneksi jaringan antara dua VPC yang memungkinkan Anda merutekan lalu lintas di antara keduanya secara privat. Sumber daya dalam VPC yang diintip dapat berkomunikasi satu sama lain seolah-olah mereka berada dalam jaringan yang sama. Anda dapat membuat koneksi peering VPC antara VPC Anda sendiri, dengan VPC di VPC lain Akun AWS, atau dengan VPC di Wilayah yang berbeda. AWS Lalu lintas antara VPC yang diintip tidak pernah melintasi internet publik.

Untuk informasi selengkapnya, lihat Panduan Peering Amazon VPC.

Memantau VPC Anda

Anda dapat menggunakan alat berikut untuk memantau lalu lintas atau akses jaringan di cloud pribadi virtual (VPC) Anda.

Log Alur VPC

Anda dapat menggunakan VPC Flow Logs untuk menangkap informasi terperinci tentang lalu lintas yang menuju dan dari antarmuka jaringan di Anda. VPCs

Monitor CloudWatch Internet Amazon

Anda dapat menggunakan Internet Monitor untuk visibilitas tentang bagaimana masalah internet memengaruhi kinerja dan ketersediaan antara aplikasi yang di-host AWS dan pengguna akhir Anda. Anda juga dapat menjelajahi, dalam waktu dekat, cara meningkatkan latensi yang diproyeksikan aplikasi Anda dengan beralih menggunakan layanan lain, atau dengan mengalihkan lalu lintas ke beban kerja Anda melalui yang berbeda. Wilayah AWS Untuk informasi selengkapnya, lihat Menggunakan Amazon CloudWatch Internet Monitor.

Manajer Alamat IP VPC Amazon (IPAM)

Anda dapat menggunakan IPAM untuk merencanakan, melacak, dan memantau alamat IP untuk beban kerja Anda. Untuk informasi selengkapnya, lihat Manajer Alamat IP.

Pencerminan Lalu lintas

Anda dapat menggunakan fitur ini untuk menyalin lalu lintas jaringan dari antarmuka jaringan instans Amazon EC2 dan mengirimkannya ke peralatan out-of-band keamanan dan pemantauan untuk pemeriksaan paket mendalam. Anda dapat mendeteksi anomali jaringan dan keamanan, mendapatkan wawasan operasional, menerapkan kepatuhan dan kontrol keamanan, dan memecahkan masalah. Untuk informasi selengkapnya, lihat Pencerminan Lalu Lintas.

Reachability Analyzer

Anda dapat menggunakan alat ini untuk menganalisis dan men-debug jangkauan jaringan antara dua sumber daya di VPC Anda. Setelah Anda menentukan sumber dan sumber daya tujuan, Reachability Analyzer hop-by-hop menghasilkan detail jalur virtual di antara mereka saat dapat dijangkau, dan mengidentifikasi komponen pemblokiran saat tidak dapat dijangkau. Untuk informasi selengkapnya, lihat Reachability Analyzer.

Penganalisis Akses Jaringan

Anda dapat menggunakan Network Access Analyzer untuk memahami akses jaringan ke sumber daya Anda. Ini membantu Anda mengidentifikasi peningkatan postur keamanan jaringan Anda dan menunjukkan bahwa jaringan Anda memenuhi persyaratan kepatuhan tertentu. Untuk informasi selengkapnya, lihat Network Access Analyzer.

CloudTrail log

AWS CloudTrail log panggilan API untuk Amazon VPC, seperti:

- Panggilan API mana yang dilakukan (seperti tindakan seperti membuat atau memodifikasi sumber daya VPC)
- Alamat IP sumber panggilan
- Siapa yang membuat panggilan
- Saat panggilan dilakukan

Log terpisah dibuat untuk`CreateVpc`, `DeleteVpc` dan `CreateDefaultVpc` tindakan. Log ini juga menyertakan sumber daya default (seperti gateway internet default atau grup keamanan default) yang dibuat dan dikaitkan dengan VPC.

Untuk informasi selengkapnya, lihat Log panggilan API Amazon EC2 menggunakan AWS CloudTrail dalam Panduan Pengguna Amazon EC2.

Pencatatan lalu lintas IP menggunakan Log Aliran VPC

Log Alur VPC adlaah fitur yang membuat Anda dapat menangkap informasi tentang lalu lintas IP yang pergi ke dan dari antarmuka jaringan. Data log aliran dapat dipublikasikan ke lokasi berikut: Amazon CloudWatch Logs, Amazon S3, atau Amazon Data Firehose. Jalur pengiriman yang dikonfigurasi dan izin yang memungkinkan log lalu lintas jaringan dikirim ke tujuan seperti CloudWatch Log atau S3 disebut sebagai langganan. Setelah membuat log alur, Anda dapat mengambil dan melihat catatan log alur di grup log, bucket, atau aliran pengiriman yang Anda konfigurasi.

Log alur dapat membantu Anda dengan sejumlah tugas, seperti:

- Mendiagnosis aturan grup keamanan yang terlalu ketat
- Memantau lalu lintas yang mencapai instans Anda
- Menentukan arah lalu lintas ke dan dari antarmuka jaringan

Data log alur dikumpulkan di luar jalur lalu lintas jaringan Anda, dan oleh karena itu tidak mempengaruhi throughput atau latensi jaringan. Anda dapat membuat atau menghapus log alur tanpa risiko dampak terhadap kinerja jaringan.

> **Note**
>
> Bagian ini hanya berbicara tentang log aliran untuk VPC. Untuk informasi tentang log alur untuk gateway transit yang diperkenalkan di versi 6, lihat Pencatatan lalu lintas jaringan menggunakan Log Aliran Gateway Transit di Panduan Pengguna Amazon VPC Transit Gateway.

Daftar Isi

- Dasar-dasar log alur
- Catatan log alur
- Contoh catatan log alur
- Batasan log alur
- Harga
- Bekerja dengan log alur
- Publikasikan log alur ke CloudWatch Log
- Terbitkan log alur ke Amazon S3
- Publikasikan log alur ke Amazon Data Firehose
- Log alur kueri menggunakan Amazon Athena
- Identitas dan manajemen akses di Log Aliran VPC
- Mengatasi masalah Log Alur VPC

Dasar-dasar log alur

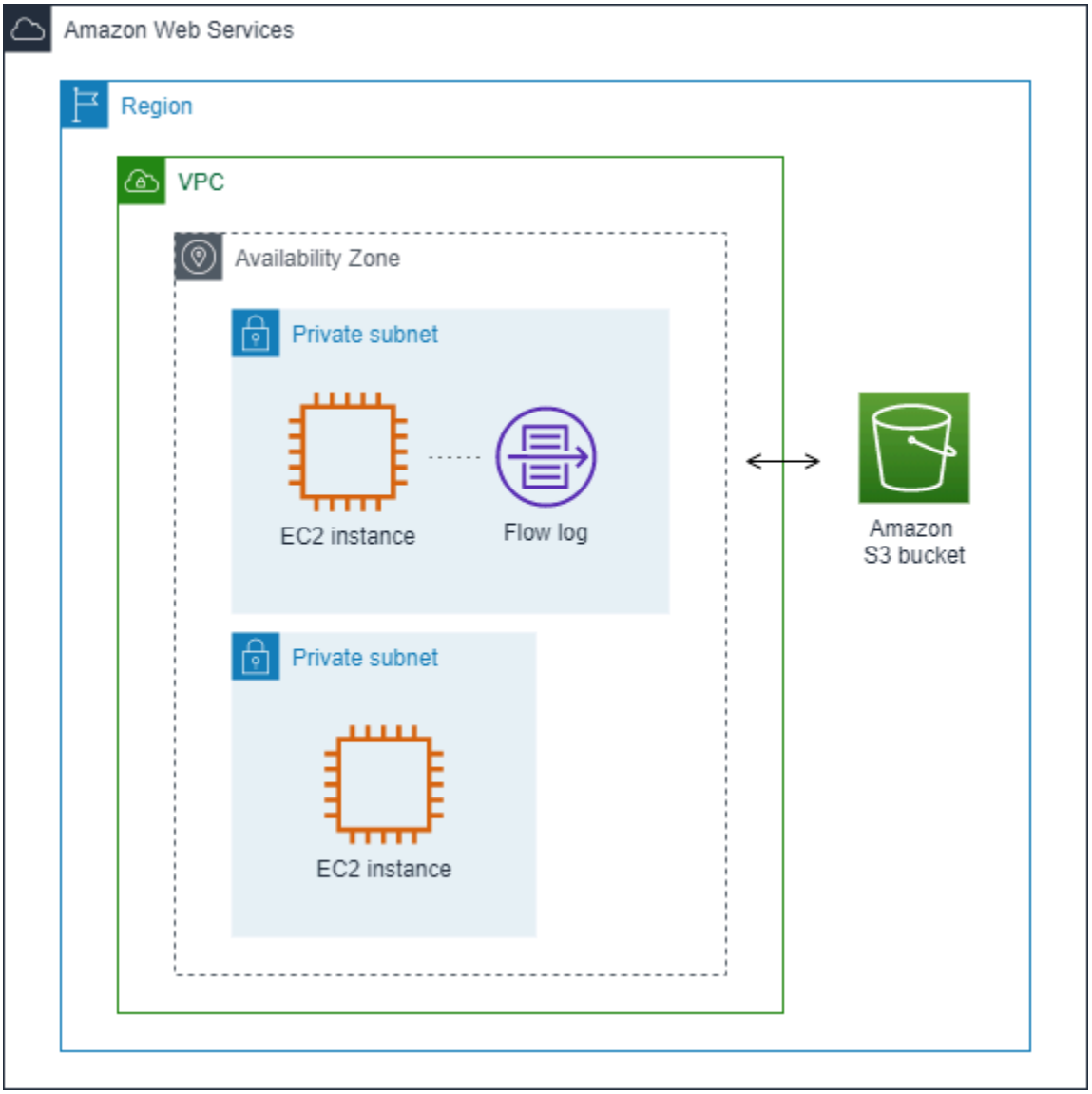
Anda dapat membuat log alur untuk VPC, subnet, atau antarmuka jaringan. Jika Anda membuat log alur untuk subnet atau VPC, setiap antarmuka jaringan di subnet atau VPC dipantau.

Data log alur untuk antarmuka jaringan yang dipantau dicatat sebagai Catatan log alur, yang merupakan log acara yang terdiri dari bidang yang menggambarkan aliran lalu lintas. Untuk informasi selengkapnya, lihat Catatan log alur.

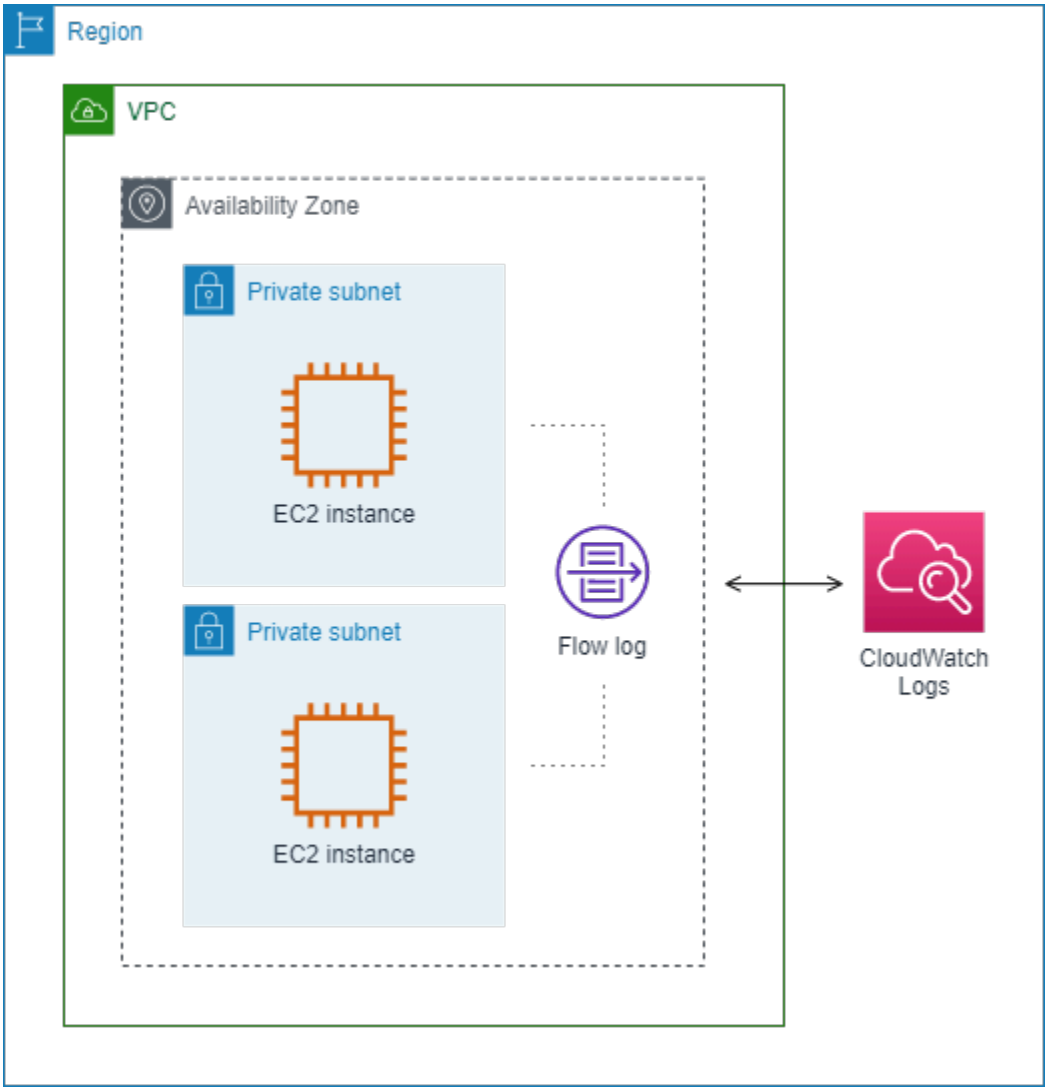
Untuk membuat log alur, Anda menentukan:

- Sumber daya untuk membuat log alur
- Jenis lalu lintas untuk menangkap (lalu lintas yang diterima, lalu lintas yang ditolak, atau semua lalu lintas)
- Tujuan publikasi data log alur Anda

Dalam contoh berikut, Anda membuat log alur yang menangkap lalu lintas yang diterima untuk antarmuka jaringan untuk salah satu instans EC2 di subnet pribadi dan menerbitkan catatan log alur ke bucket Amazon S3.



Dalam contoh berikut, log aliran menangkap semua lalu lintas untuk subnet dan menerbitkan catatan log alur ke Amazon CloudWatch Logs. Log aliran menangkap lalu lintas untuk semua antarmuka jaringan di subnet.



Setelah Anda membuat log alur, perlu beberapa menit untuk mulai mengumpulkan dan menerbitkan data ke tujuan yang dipilih. Log alur tidak menangkap pengaliran log waktu nyata untuk antarmuka jaringan Anda. Untuk informasi selengkapnya, lihat 2. Membuat log alur.

Jika Anda meluncurkan instance ke subnet setelah membuat log alur untuk subnet atau VPC, kami membuat aliran log (untuk CloudWatch Log) atau objek file log (untuk Amazon S3) untuk antarmuka jaringan baru. Aliran log atau objek file dibuat segera setelah lalu lintas jaringan terjadi pada antarmuka.

Anda dapat membuat log alur untuk antarmuka jaringan yang dibuat oleh layanan AWS lainnya, seperti:

- Elastic Load Balancing
- Amazon RDS
- Amazon ElastiCache
- Amazon Redshift
- Amazon WorkSpaces
- Gateway NAT
- Transit gateway

Terlepas dari jenis antarmuka jaringan, Anda harus menggunakan konsol Amazon EC2 atau Amazon EC2 API untuk membuat log alur untuk antarmuka jaringan.

Anda dapat memberikan tag ke log alur Anda. Setiap tanda terdiri dari sebuah kunci dan sebuah nilai opsional, yang keduanya Anda tentukan. Tag dapat membantu Anda mengatur log alur, misalnya berdasarkan tujuan atau pemilik.

Jika Anda tidak lagi membutuhkan log alur, Anda dapat menghapusnya. Menghapus log alur akan menonaktifkan layanan log alur untuk sumber daya, sehingga tidak ada catatan log alur baru yang dibuat atau diterbitkan. Menghapus log alur tidak menghapus data log alur yang ada. Setelah menghapus log alur, Anda dapat menghapus data log alur langsung dari tujuan ketika Anda selesai menggunakannya. Untuk informasi selengkapnya, lihat 4. Menghapus log alur.

Catatan log alur

Catatan log alur mewakili aliran jaringan di VPC Anda. Secara default, setiap catatan menangkap aliran lalu lintas jaringan internet protocol (IP) (ditandai dengan 5-tuple per antarmuka jaringan) yang terjadi dalam interval agregasi, juga disebut sebagai window pengambilan.

Setiap catatan adalah string dengan bidang yang dipisahkan oleh spasi. Sebuah catatan termasuk nilai-nilai untuk komponen yang berbeda dari aliran IP, misalnya, sumber, tujuan, dan protokol.

Ketika Anda membuat log alur, Anda dapat menggunakan format default untuk catatan log alur, atau Anda dapat menentukan format kustom.

Daftar Isi

- Interval agregasi
- Format default
- Format kustom

- Bidang yang tersedia

Interval agregasi

Interval agregasi adalah periode waktu di mana aliran tertentu ditangkap dan dikumpulkan ke dalam catatan log alur. Secara default, interval agregasi maksimum adalah 10 menit. Ketika Anda membuat log alur, Anda dapat menentukan interval agregasi maksimum 1 menit. Log alur dengan interval agregasi maksimum 1 menit menghasilkan volume catatan log alur yang lebih tinggi daripada log alur dengan interval agregasi maksimum 10 menit.

Ketika antarmuka jaringan dilampirkan ke Nitro-based instance, interval agregasi selalu 1 menit atau kurang, terlepas dari interval agregasi maksimum yang ditentukan.

Setelah data ditangkap dalam interval agregasi, dibutuhkan waktu tambahan untuk memproses dan mempublikasikan data ke CloudWatch Logs atau Amazon S3. Layanan log aliran biasanya mengirimkan CloudWatch log ke Log dalam waktu sekitar 5 menit dan ke Amazon S3 dalam waktu sekitar 10 menit. Namun, pengiriman log dilakukan berdasarkan upaya terbaik, dan log Anda mungkin tertunda di luar waktu pengiriman khas.

Format default

Dengan format default, catatan log alur termasuk bidang versi 2, dalam urutan yang ditunjukkan dalam tabel bidang yang tersedia. Anda tidak dapat menyesuaikan atau mengubah format default. Untuk menangkap bidang tambahan atau subset bidang yang berbeda, tentukan format kustom sebagai gantinya.

Format kustom

Dengan format kustom, Anda menentukan bidang yang disertakan dalam catatan log alur dan urutannya. Hal ini mengizinkan Anda untuk membuat log alur yang kustom untuk kebutuhan Anda dan untuk menghilangkan bidang yang tidak relevan. Menggunakan format kustom dapat mengurangi kebutuhan untuk proses terpisah untuk mengekstrak informasi spesifik dari log alur yang diterbitkan. Anda dapat menentukan berapa pun bidang log alur yang tersedia, tetapi Anda harus menentukan setidaknya satu bidang log alur.

Bidang yang tersedia

Tabel berikut menjelaskan semua bidang yang tersedia untuk catatan log alur. Kolom Versi menunjukkan versi Log Alur VPC di mana bidang diperkenalkan. Format default mencakup 2 bidang semua versi, dalam urutan yang sama sebagaimana yang tercantum di tabel.

Saat menerbitkan data log aliran ke Amazon S3, tipe data untuk bidang tergantung pada format log alur. Jika formatnya adalah teks biasa, semua bidang adalah tipeSTRING. Jika formatnya adalah Parquet, lihat tabel untuk jenis data bidang.

Jika suatu bidang tidak berlaku atau tidak dapat dihitung untuk catatan tertentu, catatan akan menampilkan simbol '-' untuk entri tersebut. Bidang metadata yang tidak datang langsung dari header paket merupakan perkiraan upaya terbaik, dan nilai-nilainya mungkin meleset atau tidak akurat.

Bidang	Deskripsi	Versi
version	Versi Log Alur VPC. Jika Anda menggunakan format default, versinya adalah 2. Jika Anda menggunakan format kustom, versinya adalah versi tertinggi di antara bidang yang ditentukan. Misalnya, jika Anda menentukan hanya bidang dari versi 2, maka versinya adalah 2. Jika Anda menentukan campuran bidang dari versi 2, 3, dan 4, maka versinya adalah 4. Jenis data parket: INT_32	2
account-id	ID AWS akun pemilik antarmuka jaringan sumber yang lalu lintasnya direkam. Jika antarmuka jaringan dibuat oleh AWS layanan, misalnya saat membuat titik akhir VPC atau Network Load Balancer, catatan mungkin ditampilkan unknown untuk bidang ini. Tipe data parket: STRING	2
interface-id	ID antarmuka jaringan yang lalu lintasnya dicatat. Mengembalikan simbol '-' untuk aliran yang terkait dengan gateway NAT regional. Tipe data parket: STRING	2
srcaddr	Untuk lalu lintas masuk, ini adalah alamat IP dari sumber lalu lintas. Untuk lalu lintas keluar, ini adalah alamat IPv4 pribadi atau alamat IPv6 dari antarmuka jaringan yang mengirim lalu lintas. Untuk lalu lintas keluar dari gateway NAT regional, ini adalah alamat IP sumber tingkat paket yang sama seperti di. pkt-srcaddr Lihat juga pkt-srcaddr. Tipe data parket: STRING	2

Bidang	Deskripsi	Versi
dstaddr	Alamat tujuan untuk lalu lintas keluar, atau alamat IPv4 atau IPv6 dari antarmuka jaringan untuk lalu lintas masuk pada antarmuka jaringan. Alamat IPv4 antarmuka jaringan selalu merupakan alamat IPv4 privatnya. Untuk lalu lintas masuk ke gateway NAT regional, ini adalah alamat IP tujuan tingkat paket yang sama seperti di. pkt-dstaddr Lihat juga pkt-dstaddr. Tipe data parket: STRING	2
srcport	Port sumber lalu lintas. Jenis data parket: INT_32	2
dstport	Port tujuan lalu lintas. Jenis data parket: INT_32	2
protocol	Nomor protokol IANA lalu lintas. Untuk informasi selengkapnya, lihat Nomor Protokol Internet yang Ditugaskan. Jenis data parket: INT_32	2
packets	Jumlah paket yang ditransfer selama aliran. Tipe data parket: INT_64	2
bytes	Jumlah byte yang ditransfer selama aliran. Tipe data parket: INT_64	2
start	Waktu, dalam detik Unix, ketika paket pertama aliran diterima dalam interval agregasi. Ini mungkin hingga 60 detik sebelum paket diterima di antarmuka jaringan atau hingga 60 detik setelah paket dikirim. Tipe data parket: INT_64	2

Bidang	Deskripsi	Versi
end	Waktu, dalam detik Unix, ketika paket terakhir dari aliran diterima dalam interval agregasi. Ini mungkin sampai 60 detik setelah paket ditransmisikan atau diterima pada antarmuka jaringan. Tipe data parket: INT_64	2
action	Tindakan yang terkait dengan lalu lintas: • ACCEPTLalu lintas diterima. • REJECTLalu lintas ditolak. Misalnya, lalu lintas tidak diizinkan oleh grup keamanan atau ACL jaringan, atau paket tiba setelah koneksi ditutup. Tipe data parket: STRING	2
log-status	Status pencatatan log alur: • OK — Data log secara normal ke tujuan yang dipilih. • NODATA — Tidak ada lalu lintas jaringan ke atau dari antarmuka jaringan selama interval agregasi. • SKIPDATA — Beberapa catatan log alur dilewati selama interval agregasi. Ini mungkin karena kendala kapasitas internal, atau kesalahan internal. Beberapa catatan log aliran dapat dilewati selama interval agregasi (lihat log-status di). Bidang yang tersedia Hal ini mungkin disebabkan oleh kendala AWS kapasitas internal atau kesalahan internal. Jika Anda menggunakan AWS Cost Explorer untuk melihat biaya log aliran VPC dan beberapa log aliran dilewati selama interval agregasi log aliran, jumlah log aliran yang dilaporkan AWS Cost Explorer akan lebih tinggi daripada jumlah log aliran yang diterbitkan oleh Amazon VPC. Tipe data parket: STRING	2

Bidang	Deskripsi	Versi
vpc-id	ID VPC yang berisi antarmuka jaringan yang lalu lintasnya dicatat. Tipe data parket: STRING	3
subnet-id	ID subnet yang berisi antarmuka jaringan yang lalu lintasnya dicatat. Mengembalikan simbol '-' untuk aliran yang terkait dengan gateway NAT regional. Tipe data parket: STRING	3
instance-id	ID instans yang terkait dengan antarmuka jaringan yang lalu lintasnya dicatat, jika instans dimiliki oleh Anda. Mengembalikan simbol '-' untuk Antarmuka jaringan yang dikelola peminta; sebagai contoh, antaramuka untuk NAT gateway. Tipe data parket: STRING	3

Bidang	Deskripsi	Versi
tcp-flags	Nilai bitmask untuk bendera TCP berikut: • FIN — 1 • SYN — 2 • RST — 4 • SYN-ACK -- 18 Jika tidak ada flag yang didukung yang direkam, nilai flag TCP adalah 0. Misalnya, karena tcp-flag tidak mendukung logging flag ACK atau PSH, catatan untuk lalu lintas dengan flag yang tidak didukung ini akan menghasilkan nilai tcp-flag 0. Namun, jika bendera yang tidak didukung disertai dengan bendera yang didukung, kami akan melaporkan nilai bendera yang didukung. Misalnya, jika ACK adalah bagian dari SYN-ACK, ia melaporkan 18. Dan jika ada catatan seperti SYN+ECE, karena SYN adalah flag yang didukung dan ECE tidak, nilai flag TCP adalah 2. Jika karena alasan tertentu kombinasi bendera tidak valid dan nilainya tidak dapat dihitung, nilainya adalah '-'. Jika tidak ada flag yang dikirim, nilai flag TCP adalah 0. Bendera TCP dapat berada OR-ed selama interval agregasi. Untuk koneksi pendek, flag dapat diatur pada baris yang sama dalam catatan log aliran, misalnya, 19 untuk SYN-ACK dan FIN, dan 3 untuk SYN dan FIN. Sebagai contoh, lihat Urutan bendera TCP. Untuk informasi umum tentang flag TCP (seperti arti bendera seperti FIN, SYN, dan ACK), lihat Struktur segmen TCP di Wikipedia. Jenis data parket: INT_32	3
type	Jenis lalu lintas. Nilai yang mungkin adalah: IPv4 | IPv6 |EFA. Untuk informasi selengkapnya, lihat Adaptor Elastic Fabric. Tipe data parket: STRING	3

Bidang	Deskripsi	Versi
pkt-srcaddr	Alamat IP sumber tingkat paket (asli) lalu lintas. Gunakan bidang ini dengan bidang srcaddr untuk membedakan antara alamat IP dari lapisan menengah yang dilalui alairan lalu lintas, dan alamat IP sumber asal dari lalu lintas. Misalnya, lalu lintas mungkin mengalir melalui antarmuka jaringan untuk gateway NAT. Kasus lain adalah di mana alamat IP pod di Amazon EKS berbeda dari alamat IP antarmuka jaringan dari node instance tempat pod berjalan (untuk komunikasi dalam VPC). Tipe data parket: STRING	3
pkt-dstaddr	Alamat IP tujuan tingkat paket (asli) untuk lalu lintas. Gunakan bidang ini dengan bidang dstaddr untuk membedakan antara alamat IP dari lapisan menengah yang dilalui alairan lalu lintas, dan alamat IP tujuan akhir dari lalu lintas. Misalnya, lalu lintas mungkin mengalir melalui antarmuka jaringan untuk gateway NAT. Kasus lain adalah di mana alamat IP pod di Amazon EKS berbeda dari alamat IP antarmuka jaringan dari node instance tempat pod berjalan (untuk komunikasi dalam VPC). Jenis data parket: STRING	3
region	Wilayah yang berisi antarmuka jaringan yang lalu lintasnya dicatat. Jenis data parket: STRING	4
az-id	ID dari Availability Zone yang berisi antarmuka jaringan yang lalu lintasnya dicatat. Jika lalu lintas berasal dari sublokasi, catatan akan menampilkan simbol '-' untuk bidang ini. Jenis data parket: STRING	4

Bidang	Deskripsi	Versi
sublocation-type	Jenis sublokasi yang dikembalikan dalam bidang sublocation-id. Nilai yang mungkin adalah: wavelength | outpost | localzone. Jika lalu lintas bukan dari sublokasi, catatan menampilkan simbol '-' untuk bidang ini. Jenis data parket: STRING	4
sublocation-id	ID sublokasi yang berisi antarmuka jaringan yang lalu lintasnya dicatat. Jika lalu lintas bukan dari sublokasi, catatan menampilkan simbol '-' untuk bidang ini. Jenis data parket: STRING	4
pkt-src-aws-service	Nama subset dari Rentang alamat IP untuk bidang pkt-srcad dr ,jika alamat IP sumber adalah untuk layanan AWS . Jika alamat IP sumber milik rentang tumpang tindih, hanya pkt-src-aws-service menampilkan salah satu kode AWS layanan. Nilai yang mungkin adalah: `AMAZON | AMAZON_APPFLOW AMAZON_CONNECT | API_GATEWAY | AURORA_DSQL | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRONT | CLOUDFRONT_ORIGIN_FACING | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTANCE_CONNECT | GLOBALACCELERATOR | IVS_LOW_LATENCY IVS_REALTIME | KINESIS_VIDEO_STREAMS | MEDIA_PACKAGE_V2 | ROUTE53 | ROUTE53_HEALTHCHECKS | ROUTE53_HEALTHCHECKS_PUBLISHING | ROUTE53_RESOLVER | S3 |WORKSPACES_GATEWAYS` . Jenis data parket: STRING	5
pkt-dst-aws-service	Nama subset dari rentang alamat IP untuk pkt-dstaddr bidang, jika alamat IP tujuan adalah untuk AWS layanan. Untuk daftar kemungkinan nilai, lihat bidang pkt-src-aws-service. Jenis data parket: STRING	5

Bidang	Deskripsi	Versi
flow-direction	Arah aliran sehubungan dengan antarmuka di mana lalu lintas ditangkap. Kemungkinan nilai adalah: ingress | egress. Jenis data parket: STRING	5
traffic-path	Jalan yang dilalui lalu lintas egress untuk ke tujuan. Untuk menentukan apakah lalu lintas merupakan lalu lintas keluar, periksa bidang flow-direction. Kemungkinan nilainya adalah sebagai berikut. Jika tidak ada nilai yang berlaku, bidang diatur ke -. • 1 — Melalui sumber daya lain di VPC yang sama, termasuk antarmuka jaringan AWS yang dikelola atau gateway lokal Outpost • 2 — Melalui gateway internet atau gateway VPC endpoint • 3 — Melalui virtual private gateway • 4 — Melalui koneksi peering VPC dalam wilayah • 5 — Melalui koneksi peering VPC antar wilayah • 6 - Melalui Zona Lokal atau Zona Panjang Gelombang • 7 — Melalui titik akhir VPC gateway • 8 — Melalui gateway internet Jenis data parket: INT_32	5
ecs-cluster-arn	AWS Nama Sumber Daya (ARN) dari cluster ECS jika lalu lintas berasal dari tugas ECS yang sedang berjalan. Untuk menyertak an bidang ini dalam langganan Anda, Anda memerlukan izin untuk memanggil ecs:ListClusters. Tipe data parket: STRING	7
ecs-cluster-nama	Nama cluster ECS jika lalu lintas berasal dari tugas ECS yang sedang berjalan. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerlukan izin untuk memanggil ecs:ListClusters. Tipe data parket: STRING	7

Bidang	Deskripsi	Versi
ecs-container-instance-arn	ARN dari instance kontainer ECS jika lalu lintas berasal dari tugas ECS yang sedang berjalan pada instans EC2. Jika penyedia kapasitas adalah AWS Fargate, bidang ini akan menjadi '-'. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerlukan izin untuk memanggil ecs: ListClusters dan ecs:. ListContainerInstances Tipe data parket: STRING	7
ecs-container-id instance-id	ID instance kontainer ECS jika lalu lintas berasal dari tugas ECS yang sedang berjalan pada instans EC2. Jika penyedia kapasitas adalah AWS Fargate, bidang ini akan menjadi '-'. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerlukan izin untuk memanggil ecs: ListClusters dan ecs:. ListContainerInstances Tipe data parket: STRING	7
ecs-kontainer-id	Docker runtime ID dari container jika lalu lintas berasal dari tugas ECS yang sedang berjalan. Jika ada satu atau lebih wadah dalam tugas ECS, ini akan menjadi ID runtime docker dari wadah pertama. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerlukan izin untuk memanggil ecs:ListClusters. Tipe data parket: STRING	7
ecs-id-kontainer kedua	Docker runtime ID dari container jika lalu lintas berasal dari tugas ECS yang sedang berjalan. Jika ada lebih dari satu wadah dalam tugas ECS, ini akan menjadi ID runtime Docker dari wadah kedua. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerlukan izin untuk memanggil ecs:ListClusters. Tipe data parket: STRING	7

Bidang	Deskripsi	Versi
ecs-nama-layanan	Nama layanan ECS jika lalu lintas berasal dari tugas ECS yang sedang berjalan dan tugas ECS dimulai oleh layanan ECS. Jika tugas ECS tidak dimulai oleh layanan ECS, bidang ini akan menjadi '-'. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerlukan izin untuk memanggil ecs: ListClusters dan ecs:. ListServices Tipe data parket: STRING	7
ecs-task-definition-arn	ARN dari definisi tugas ECS jika lalu lintas berasal dari tugas ECS yang sedang berjalan. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerlukan izin untuk memanggil ecs: ListClusters dan ecs: ListTaskDefinitions Tipe data parket: STRING	7
ecs-task-arn	ARN tugas ECS jika lalu lintas berasal dari tugas ECS yang sedang berjalan. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerlukan izin untuk memanggil ecs: ListClusters dan ecs:. ListTasks Tipe data parket: STRING	7
ecs-id tugas	ID tugas ECS jika lalu lintas berasal dari tugas ECS yang sedang berjalan. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerlukan izin untuk memanggil ecs: ListClusters dan ecs:. ListTasks Tipe data parket: STRING	7

Bidang	Deskripsi	Versi
alasan penolakan	Alasan Mengapa Lalu Lintas Ditolak Nilai yang mungkin: BPA, EC. Mengembalikan '-' untuk alasan penolakan lainnya. • BPA — Untuk informasi selengkapnya tentang VPC Block Public Access (BPA), lihat. Blokir akses publik ke VPC dan subnet • EC — Aliran ditolak oleh VPC Endpoint karena kontrol enkripsi. Untuk informasi selengkapnya tentang Kontrol Enkripsi VPC, lihatMenerapkan enkripsi VPC saat transit. Tipe data parket: STRING	8
resource-id	ID gateway NAT regional yang berisi antarmuka jaringan tempat lalu lintas direkam. Mengembalikan simbol '-' untuk arus lalu lintas yang tidak terkait dengan gateway NAT regional. Untuk informasi selengkapnya tentang gateway NAT regional, lihatGerbang NAT regional untuk ekspansi multi-AZ otomatis. Tipe data parket: STRING	9

Bidang	Deskripsi	Versi

enkripsi-status	Status enkripsi aliran. Untuk informasi selengkapnya tentang Kontrol Enkripsi VPC, lihatMenerapkan enkripsi VPC saat transit. Nilai yang mungkin adalah:
	• 0 - tidak dienkripsi.
	• 1 — dienkripsi nitro. Ini dienkripsi oleh perangkat keras sistem Nitro.
	• 2 — aplikasi terenkripsi. Hanya yang berikut ini dianggap sebagai enkripsi aplikasi:
	  • mengalir pada port TCP 443 untuk titik akhir antarmuka ke layanan* AWS
	  • mengalir pada port TCP 443 untuk titik akhir gateway*
	  • mengalir ke cluster Redshift terenkripsi melalui titik akhir VPC**
	• 3 — dienkripsi nitro dan dienkripsi aplikasi.
	
	Nilainya adalah '-' jika Kontrol Enkripsi VPC tidak diaktifkan, atau jika FlowLog tidak bisa mendapatkan status.
	
	Note
	* Untuk titik akhir antarmuka dan gateway, AWS tidak melihat data paket untuk menentukan status enkripsi, kami malah mengandalkan port yang digunakan untuk mengasumsikan status enkripsi.
	** Untuk titik akhir AWS terkelola yang ditentukan AWS , tentukan status enkripsi berdasarkan persyaratan untuk TLS dalam konfigurasi layanan.
	
	Jenis data parket: INT_32
		10

Bidang	Deskripsi	Versi
tag instance	Nilai tag untuk tag instance pertama yang disertakan dalam Anda TagFieldSpecifications. Nilai tag ditampilkan menerjemahkan semua karakter khusus dengan UTF-8 persen pengkodean. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerluka n izin untuk memanggil ec2: DescribeTags dan iam:. CreateSer viceLinkedRole Untuk informasi tentang Peran Tertaut Layanan Log Alur Amazon EC2 Tags, lihatMenggunakan peran terkait layanan untuk Log Aliran VPC. Tipe data parket: STRING	11
tag-instance-2	Nilai tag untuk tag instance kedua yang disertakan dalam Anda TagFieldSpecifications. Nilai tag ditampilkan menerjemahkan semua karakter khusus dengan UTF-8 persen pengkodean. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerluka n izin untuk memanggil ec2: DescribeTags dan iam:. CreateSer viceLinkedRole Untuk informasi tentang Peran Tertaut Layanan Log Alur Amazon EC2 Tags, lihatMenggunakan peran terkait layanan untuk Log Aliran VPC. Tipe data parket: STRING	11
tag antarmuka	Nilai tag untuk tag antarmuka jaringan pertama yang disertaka n dalam Anda. TagFieldSpecifications Nilai tag ditampilkan menerjemahkan semua karakter khusus dengan UTF-8 persen pengkodean. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerlukan izin untuk memanggil ec2: DescribeTags dan iam:. CreateServiceLinkedRole Untuk informasi tentang Peran Tertaut Layanan Log Alur Amazon EC2 Tags, lihatMenggunakan peran terkait layanan untuk Log Aliran VPC. Tipe data parket: STRING	11

Bidang	Deskripsi	Versi
antarmuka tag-2	Nilai tag untuk tag antarmuka jaringan kedua yang disertakan dalam Anda. TagFieldSpecifications Nilai tag ditampilkan menerjemahkan semua karakter khusus dengan UTF-8 persen pengkodean. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerluka n izin untuk memanggil ec2: DescribeTags dan iam:. CreateSer viceLinkedRole Untuk informasi tentang Peran Tertaut Layanan Log Alur Amazon EC2 Tags, lihatMenggunakan peran terkait layanan untuk Log Aliran VPC. Tipe data parket: STRING	11
tag asg	Nilai tag untuk tag grup penskalaan otomatis pertama yang disertakan dalam tag Anda. TagFieldSpecifications Nilai tag ditampilkan menerjemahkan semua karakter khusus dengan UTF-8 persen pengkodean. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerlukan izin untuk memanggil autoscali ng: DescribeTags dan iam:. CreateServiceLinkedRole Anda harus memiliki setidaknya satu CloudTrail jejak yang diaktifkan di akun Anda agar nilai tag grup Penskalaan Otomatis dapat dilacak dan diperbarui dengan benar secara real time. Untuk informasi tentang Peran Tertaut Layanan Log Alur Amazon EC2 Tags, lihatMenggunakan peran terkait layanan untuk Log Aliran VPC. Tipe data parket: STRING	11

Bidang	Deskripsi	Versi
asg-tag-2	Nilai tag untuk tag grup penskalaan otomatis kedua yang disertakan dalam tag Anda. TagFieldSpecifications Nilai tag ditampilkan menerjemahkan semua karakter khusus dengan UTF-8 persen pengkodean. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerlukan izin untuk memanggil autoscaling: DescribeTags dan iam:. CreateServiceLinkedRole Anda harus memiliki setidaknya satu CloudTrail jejak yang diaktifkan di akun Anda agar nilai tag grup Penskalaan Otomatis dapat dilacak dan diperbarui dengan benar secara real time. Untuk informasi tentang Peran Tertaut Layanan Log Alur Amazon EC2 Tags, lihatMenggunakan peran terkait layanan untuk Log Aliran VPC. Tipe data parket: STRING	11
tipe antarmuka	Jenis antarmuka jaringan lokal yang menangkap aliran. Nilai yang didukung adalah: `nat_gateway` | `network_load_balancer` | `regional_nat_gateway` | `transit_gateway` | `vpc_endpoint` . Jika antarmuka jaringan tidak memiliki layanan asosiasi, atau layanan tidak didukung, nilainya adalah '-'. Tipe data parket: STRING	11
id antarmuka berikutnya	ID antarmuka jaringan hop berikutnya. Untuk lalu lintas keluar, ini adalah antarmuka yang menerima lalu lintas. Untuk lalu lintas masuk, ini adalah antarmuka yang mengirimkan lalu lintas. Jenis data parket: STRING	11
next-hop-subnet-id	ID subnet yang berisi antarmuka jaringan hop berikutnya. Jenis data parket: STRING	11
next-hop-az-id	ID Zona Ketersediaan yang berisi antarmuka jaringan hop berikutnya. Jenis data parket: STRING	11

Bidang	Deskripsi	Versi
next-hop-vpc-id	ID VPC yang berisi antarmuka jaringan hop berikutnya. Jenis data parket: STRING	11
tipe antarmuka next-hop	Jenis antarmuka jaringan hop berikutnya. Untuk daftar nilai yang mungkin, lihat bidang tipe antarmuka Jenis data parket: STRING	11

Contoh catatan log alur

Berikut ini adalah contoh catatan log alur yang menangkap arus lalu lintas tertentu.

Untuk informasi selengkapnya tentang format pencatatan log alur, lihat Catatan log alur. Untuk informasi tentang cara membuat log alur, lihat Bekerja dengan log alur.

Daftar Isi

- Lalu lintas yang diterima dan ditolak
- Tidak ada data dan catatan yang dilewati
- Aturan grup keamanan dan ACL jaringan
- Lalu lintas IPv6
- Urutan bendera TCP
- Lalu lintas melalui gateway NAT zonal
- Lalu lintas melalui gateway NAT regional
- Lalu lintas melalui transit gateway
- Nama layanan, jalur lalu lintas, dan arah aliran

Lalu lintas yang diterima dan ditolak

Berikut ini adalah contoh catatan log alur default.

Dalam contoh ini, lalu lintas SSH (port tujuan 22, protokol TCP) dari alamat IP 172.31.16.139 ke antarmuka jaringan dengan alamat IP pribadi adalah 172.31.16.21 dan ID eni-1235b8ca123456789 di akun 123456789010 diizinkan.

```
2 123456789010 eni-1235b8ca123456789 172.31.16.139 172.31.16.21 20641 22 6 20 4249
 1418530010 1418530070 ACCEPT OK
```

Dalam contoh ini, lalu lintas RDP (port tujuan 3389, protokol TCP) untuk antarmuka jaringan eni-1235b8ca123456789 di akun 123456789010 ditolak.

```
2 123456789010 eni-1235b8ca123456789 172.31.9.69 172.31.9.12 49761 3389 6 20 4249
 1418530010 1418530070 REJECT OK
```

Tidak ada data dan catatan yang dilewati

Berikut ini adalah contoh catatan log alur default.

Dalam contoh ini, tidak ada data yang dicatat selama interval agregasi.

```
2 123456789010 eni-1235b8ca123456789 - - - - - - - 1431280876 1431280934 - NODATA
```

Log Aliran VPC melewatkan catatan jika tidak dapat menangkap data log aliran selama interval agregasi karena melebihi kapasitas internal. Satu catatan yang dilewati dapat mewakili beberapa aliran yang tidak ditangkap untuk antarmuka jaringan selama interval agregasi.

```
2 123456789010 eni-11111111aaaaaaaaa - - - - - - - 1431280876 1431280934 - SKIPDATA
```

> **Note**
>
> Beberapa catatan log aliran dapat dilewati selama interval agregasi (lihat log-status di). Bidang yang tersedia Hal ini mungkin disebabkan oleh kendala AWS kapasitas internal atau kesalahan internal. Jika Anda menggunakan AWS Cost Explorer untuk melihat biaya log aliran VPC dan beberapa log aliran dilewati selama interval agregasi log aliran, jumlah log aliran yang dilaporkan AWS Cost Explorer akan lebih tinggi daripada jumlah log aliran yang diterbitkan oleh Amazon VPC.

Aturan grup keamanan dan ACL jaringan

Jika Anda menggunakan log alur untuk mendiagnosis aturan grup keamanan yang terlalu ketat atau longgar atau aturan ACL jaringan, perhatikan tingkat stateful sumber daya ini. Grup keamanan

bersifat stateful - ini berarti bahwa respon untuk ke lalu lintas yang diizinkan juga diizinkan, bahkan jika aturan dalam grup keamanan Anda tidak mengizinkannya. Sebaliknya, ACL jaringan bersifat stateless, oleh karena itu respon terhadap lalu lintas yang diizinkan tunduk pada aturan ACL jaringan.

Misalnya, Anda menggunakan perintah ping dari komputer rumah Anda (alamat IP adalah 203.0.113.12) ke instans Anda (alamat IP privat antarmuka jaringan adalah 172.31.16.139). Aturan masuk grup keamanan mengizinkan lalu lintas ICMP tetapi aturan keluar tidak mengizinkan lalu lintas ICMP. Karena grup keamanan bersifat stateful, ping respon dari instans Anda diizinkan. ACL jaringan Anda mengizinkan lalu lintas ICMP masuk tetapi tidak mengizinkan lalu lintas ICMP keluar. Karena ACL jaringan bersifat stateless, ping respon dijatuhkan dan tidak mencapai komputer rumah Anda. Dalam log alur default, ini ditampilkan sebagai dua catatan log alur:

- Catatan ACCEPT untuk ping asal yang diizinkan oleh ACL jaringan dan grup keamanan, dan oleh karena itu diizinkan untuk mencapai instans Anda.
- Catatan REJECT untuk ping respon yang ditolak ACL jaringan.

```
2 123456789010 eni-1235b8ca123456789 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027
 1432917142 ACCEPT OK
```

```
2 123456789010 eni-1235b8ca123456789 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094
 1432917142 REJECT OK
```

Jika ACL jaringan Anda mengizinkan lalu lintas ICMP keluar, log alur menampilkan dua catatan ACCEPT (satu untuk ping asal dan satu untuk ping respon). Jika grup keamanan Anda menolak lalu lintas ICMP masuk, log alur menampilkan catatan REJECT, karena lalu lintas tidak diizinkan untuk mencapai instans Anda.

Lalu lintas IPv6

Berikut ini adalah contoh catatan log alur default. Dalam contoh, lalu lintas SSH (port 22) dari alamat IPv6 2001:db8:1234:a100:8d6e:3477:df66:f105 ke antarmuka jaringan eni-1235b8ca123456789 di akun 123456789010 diizinkan.

```
2 123456789010 eni-1235b8ca123456789 2001:db8:1234:a100:8d6e:3477:df66:f105
 2001:db8:1234:a102:3304:8879:34cf:4071 34892 22 6 54 8855 1477913708 1477913820 ACCEPT
 OK
```

Urutan bendera TCP

Bagian ini berisi contoh log alur kustom yang menangkap bidang berikut dalam urutan berikut.

```
version vpc-id subnet-id instance-id interface-id account-id type srcaddr dstaddr
 srcport dstport pkt-srcaddr pkt-dstaddr protocol bytes packets start end action tcp-
flags log-status
```

Bid tcp-flags ang dalam contoh di bagian ini diwakili oleh nilai kedua hingga terakhir dalam log aliran. Bendera TCP dapat membantu Anda mengidentifikasi arah lalu lintas, misalnya, server mana yang memulai koneksi.

> **Note**
>
> Untuk informasi selengkapnya tentang tcp-flags opsi dan penjelasan masing-masing flag TCP, lihatBidang yang tersedia.

Dalam catatan berikut (mulai pukul 7:47:55 sore dan berakhir pada 7:48:53 sore), dua koneksi dimulai oleh klien ke server yang berjalan pada port 5001. Dua bendera SYN (2) diterima oleh server dari klien dari port sumber yang berbeda pada klien (43416 dan 43418). Untuk setiap SYN, SYN-ACK a dikirim dari server ke klien (18) pada port yang sesuai.

```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43416 5001
 52.213.180.42 10.0.0.62 6 568 8 1566848875 1566848933 ACCEPT 2 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43416 10.0.0.62
 52.213.180.42 6 376 7 1566848875 1566848933 ACCEPT 18 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43418 5001
 52.213.180.42 10.0.0.62 6 100701 70 1566848875 1566848933 ACCEPT 2 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43418 10.0.0.62
 52.213.180.42 6 632 12 1566848875 1566848933 ACCEPT 18 OK
```

Pada interval agregasi kedua, salah satu koneksi yang terbentuk selama aliran sebelumnya sekarang ditutup. Server mengirim flag FIN (1) ke klien untuk koneksi pada port 43418. Klien merespons dengan FIN ke server pada port 43418.

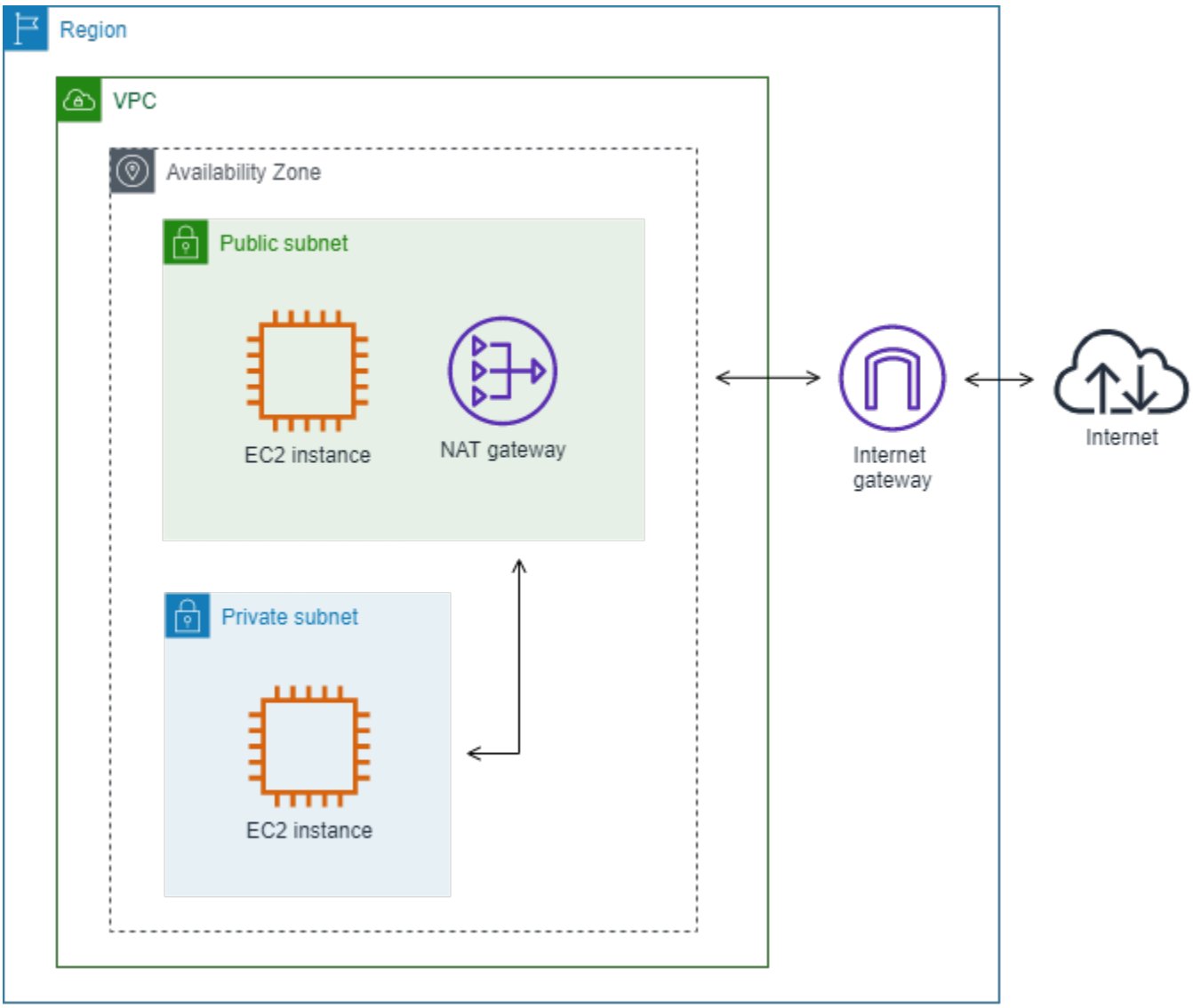
```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43418 10.0.0.62
 52.213.180.42 6 63388 1219 1566848933 1566849113 ACCEPT 1 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43418 5001
 52.213.180.42 10.0.0.62 6 23294588 15774 1566848933 1566849113 ACCEPT 1 OK
```

Untuk koneksi pendek yang membuka dan menutup dalam interval agregasi tunggal, flag mungkin diatur pada baris yang sama dalam catatan log aliran untuk aliran lalu lintas ke arah yang sama. Pada contoh berikut, koneksi dibuat dan selesai dalam interval agregasi yang sama. Pada baris pertama, nilai bendera TCP adalah 3, yang menunjukkan bahwa ada pesan SYN dan FIN yang dikirim dari klien ke server. Pada baris kedua, nilai flag TCP adalah 19, yang menunjukkan bahwa ada SYN-ACK dan pesan FIN dikirim dari server ke klien.

```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43638 5001
 52.213.180.42 10.0.0.62 6 1260 17 1566933133 1566933193 ACCEPT 3 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43638  10.0.0.62
 52.213.180.42 6 967 14 1566933133 1566933193 ACCEPT 19 OK
```

Lalu lintas melalui gateway NAT zonal

Dalam contoh ini, contoh di subnet pribadi mengakses internet melalui gateway NAT zonal yang ada di subnet publik.



Log alur kustom berikut untuk antarmuka jaringan gateway NAT zonal menangkap bidang berikut dalam urutan berikut.

```
instance-id interface-id srcaddr dstaddr pkt-srcaddr pkt-dstaddr
```

Log aliran menunjukkan aliran lalu lintas dari alamat IP instance (10.0.1.5) melalui antarmuka jaringan gateway NAT zonal ke host di internet (203.0.113.5). Antarmuka jaringan gateway NAT zonal adalah antarmuka jaringan yang dikelola permintaan, oleh karena itu catatan log aliran menampilkan simbol '-' untuk bidang tersebut. instance-id Baris berikut menunjukkan lalu lintas dari instance sumber ke antarmuka jaringan gateway NAT zonal. Nilai-nilai untuk bidang dstaddr dan pkt-dstaddr berbeda. Bid dstaddr ang menampilkan alamat IP pribadi dari antarmuka jaringan gateway NAT zonal, dan pkt-dstaddr bidang menampilkan alamat IP tujuan akhir dari host di internet.

```
- eni-1235b8ca123456789 10.0.1.5 10.0.0.220 10.0.1.5 203.0.113.5
```

Dua baris berikutnya menunjukkan lalu lintas dari antarmuka jaringan gateway NAT zonal ke host target di internet, dan lalu lintas respons dari host ke antarmuka jaringan gateway NAT.

```
- eni-1235b8ca123456789 10.0.0.220 203.0.113.5 10.0.0.220 203.0.113.5
- eni-1235b8ca123456789 203.0.113.5 10.0.0.220 203.0.113.5 10.0.0.220
```

Baris berikut menunjukkan lalu lintas respons dari antarmuka jaringan gateway NAT zonal ke instance sumber. Nilai-nilai untuk bidang srcaddr dan pkt-srcaddr berbeda. srcaddrBidang menampilkan alamat IP pribadi dari antarmuka jaringan gateway NAT zonal, dan pkt-srcaddr bidang menampilkan alamat IP host di internet.

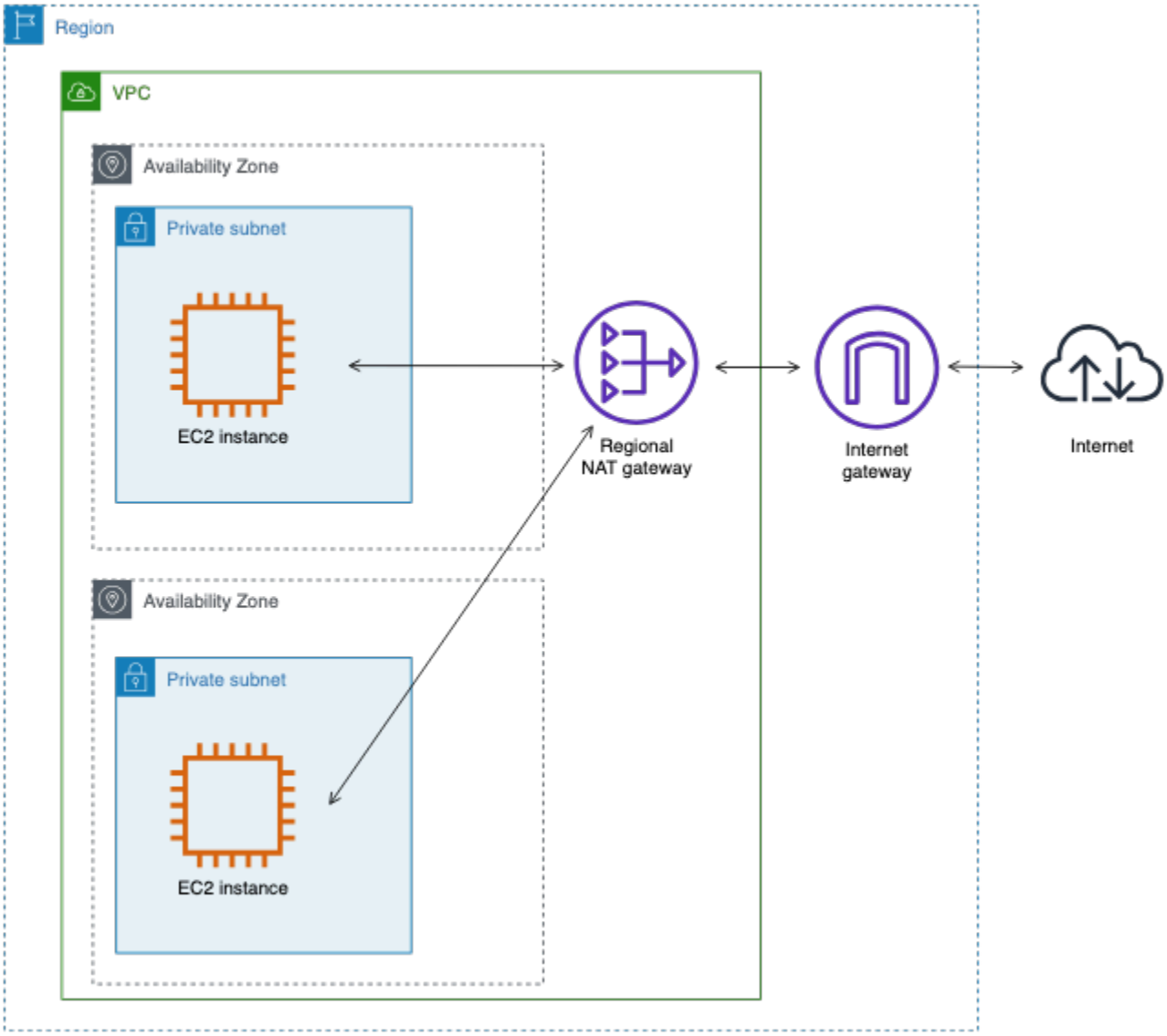
```
- eni-1235b8ca123456789 10.0.0.220 10.0.1.5 203.0.113.5 10.0.1.5
```

Anda membuat log alur kustom lain menggunakan set bidang di atas. Anda membuat log alur untuk antarmuka jaringan untuk instans di subnet privat. Dalam hal ini, instance-id bidang mengembalikan ID instance yang terkait dengan antarmuka jaringan. Tidak ada perbedaan antara pkt-dstaddr bidang dstaddr dan atau pkt-srcaddr bidang srcaddr dan. Berbeda dengan antarmuka jaringan untuk gateway NAT zonal, antarmuka jaringan ini bukan antarmuka jaringan perantara untuk lalu lintas.

```
i-01234567890123456 eni-1111aaaa2222bbbb3 10.0.1.5 203.0.113.5 10.0.1.5 203.0.113.5
 #Traffic from the source instance to host on the internet
i-01234567890123456 eni-1111aaaa2222bbbb3 203.0.113.5 10.0.1.5 203.0.113.5 10.0.1.5
 #Response traffic from host on the internet to the source instance
```

Lalu lintas melalui gateway NAT regional

Gateway NAT regional dapat terhubung ke beberapa subnet di Zona Ketersediaan yang berbeda. Dalam contoh ini, dua contoh di subnet pribadi dari dua Zona Ketersediaan yang berbeda mengakses internet melalui gateway NAT regional yang sama. Log aliran berikut menunjukkan lalu lintas dari salah satu instance ke internet melalui gateway NAT regional.



Log alur kustom berikut untuk gateway NAT regional menangkap bidang berikut dalam urutan berikut.

```
resource-id instance-id interface-id subnet-id srcaddr dstaddr pkt-srcaddr pkt-dstaddr
```

Log aliran menunjukkan aliran lalu lintas dari alamat IP instance (10.0.1.5) melalui gateway NAT regional ke host di internet (203.0.113.5). instance-id,interface-id, dan subnet-id tidak berlaku untuk gateway NAT regional. Oleh karena itu, catatan log aliran menampilkan simbol '-' untuk bidang ini. Sebagai gantinya, resource-id bidang menampilkan ID gateway NAT regional. pkt-dstaddrBid dstaddr ang dan menampilkan alamat IP tujuan akhir dari host di internet.

```
nat-1234567890abcdef - - - 10.0.1.5 203.0.113.5 10.0.1.5 203.0.113.5
```

Dua baris berikutnya menunjukkan lalu lintas dari gateway NAT regional (alamat IP publik 107.22.182.139) ke host target di internet. Mereka juga menunjukkan lalu lintas respons dari host ke gateway NAT regional.

```
nat-1234567890abcdef - - - 107.22.182.139 203.0.113.5 107.22.182.139 203.0.113.5
nat-1234567890abcdef - - - 203.0.113.5 107.22.182.139 203.0.113.5 107.22.182.139
```

Baris berikut menunjukkan lalu lintas respons dari gateway NAT regional ke instance sumber. pkt-srcaddrBidang srcaddr dan menampilkan alamat IP host di internet.

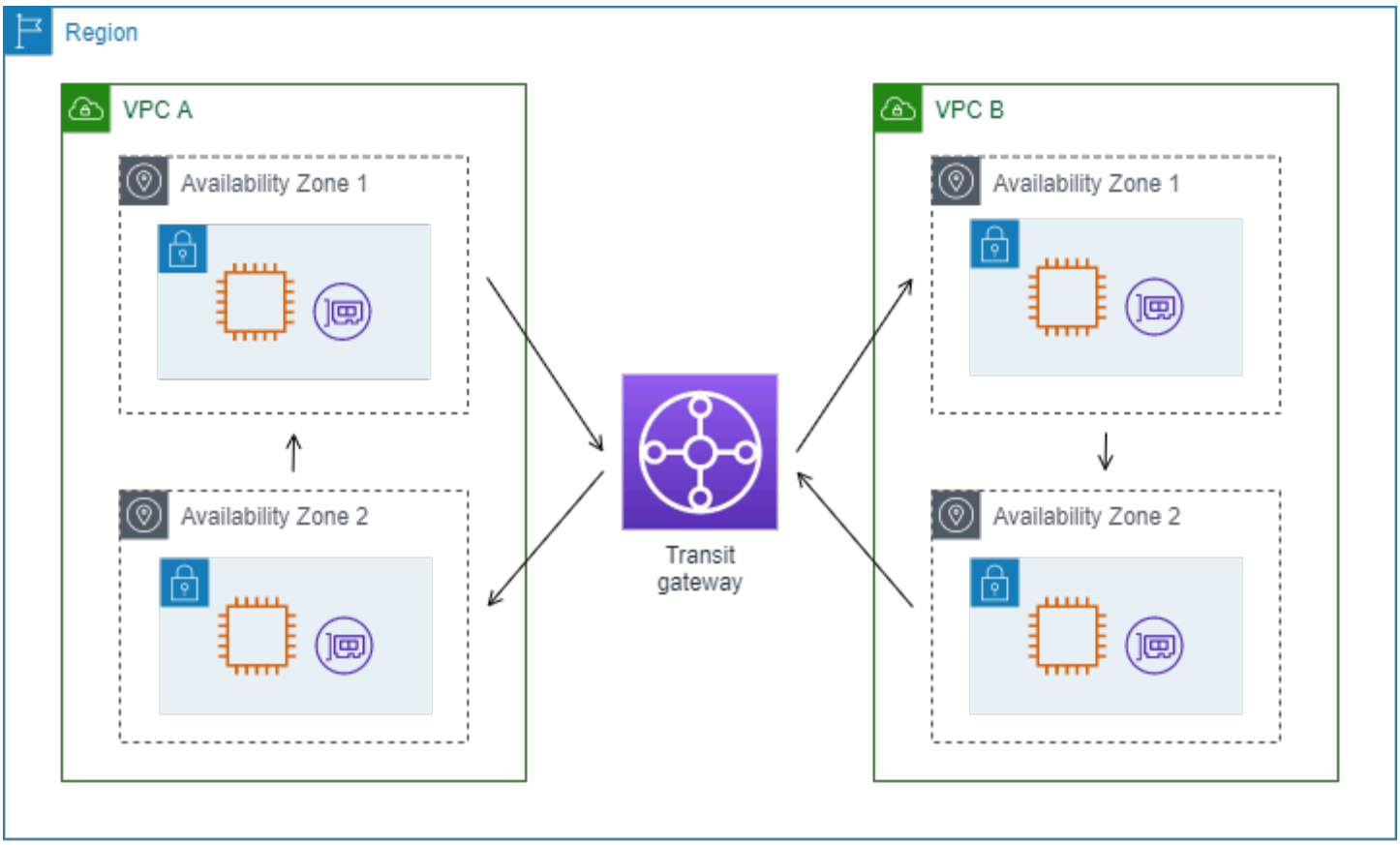
```
nat-1234567890abcdef - - - 203.0.113.5 10.0.1.5 203.0.113.5 10.0.1.5
```

Anda membuat log alur kustom lain menggunakan set bidang di atas. Anda membuat log alur untuk antarmuka jaringan untuk instans di subnet privat. Dalam hal ini, instance-id bidang mengembalikan ID instance yang terkait dengan antarmuka jaringan, dan resource-id adalah '-'. Tidak ada perbedaan antara pkt-dstaddr bidang dstaddr dan dan pkt-srcaddr bidang srcaddr dan.

```
- i-01234567890123456 eni-1111aaaa2222bbbb3 subnet-aaaaaaaa012345678 10.0.1.5
 203.0.113.5 10.0.1.5 203.0.113.5 #Traffic from the source instance to host on the
 internet
- i-01234567890123456 eni-1111aaaa2222bbbb3 subnet-aaaaaaaa012345678 203.0.113.5
 10.0.1.5 203.0.113.5 10.0.1.5 #Response traffic from host on the internet to the
 source instance
```

Lalu lintas melalui transit gateway

Dalam contoh ini, klien di VPC A terhubung ke server web di VPC B melalui transit gateway. Klien dan server berada di Availability Zone yang berbeda. Lalu lintas tiba di server di VPC B menggunakan satu ID antarmuka jaringan elastis (dalam contoh ini, katakanlah ID adalah eni-1111111111111111111) dan meninggalkan VPC B menggunakan yang lain (misalnya eni-22222222222222222).



Anda membuat log alur kustom untuk VPC B dengan format berikut.

```
version interface-id account-id vpc-id subnet-id instance-id srcaddr dstaddr srcport
 dstport protocol tcp-flags type pkt-srcaddr pkt-dstaddr action log-status
```

Baris berikut dari catatan log alur menunjukkan aliran lalu lintas pada antarmuka jaringan untuk web server. Baris pertama adalah lalu lintas permintaan dari klien, dan baris terakhir adalah lalu lintas respon dari server web.

```
3 eni-33333333333333333 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb
 i-01234567890123456 10.20.33.164 10.40.2.236 39812 80 6 3 IPv4 10.20.33.164
 10.40.2.236 ACCEPT OK
...
3 eni-33333333333333333 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb
 i-01234567890123456 10.40.2.236 10.20.33.164 80 39812 6 19 IPv4 10.40.2.236
 10.20.33.164 ACCEPT OK
```

Baris berikut adalah lalu lintas permintaan di eni-11111111111111111, antarmuka jaringan yang dikelola peminta untuk transit gateway di subnet subnet-11111111aaaaaaaaa. Oleh karena itu

catatan log alur menampilkan simbol '-' untuk bidang instance-id. Bidang srcaddr menampilkan alamat IP privat antarmuka jaringan transit gateway, dan bidang pkt-srcaddr menampilkan alamat IP sumber klien di VPC A.

```
3 eni-11111111111111111 123456789010 vpc-abcdefab012345678 subnet-11111111aaaaaaaaa -
 10.40.1.175 10.40.2.236 39812 80 6 3 IPv4 10.20.33.164 10.40.2.236 ACCEPT OK
```

Baris berikut adalah lalu lintas respon pada eni-22222222222222222, antarmuka jaringan yang dikelola peminta untuk transit gateway di subnet subnet-22222222bbbbbbbbb. Bidang dstaddr menampilkan alamat IP privat antarmuka jaringan transit gateway, dan bidang pkt-dstaddr menampilkan alamat IP klien di VPC A.

```
3 eni-22222222222222222 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb -
 10.40.2.236 10.40.2.31 80 39812 6 19 IPv4 10.40.2.236 10.20.33.164 ACCEPT OK
```

Nama layanan, jalur lalu lintas, dan arah aliran

Berikut ini adalah contoh bidang untuk catatan log alur kustom.

```
version srcaddr dstaddr srcport dstport protocol start end type packets bytes account-
id vpc-id subnet-id instance-id interface-id region az-id sublocation-type sublocation-
id action tcp-flags pkt-srcaddr pkt-dstaddr pkt-src-aws-service pkt-dst-aws-service
 traffic-path flow-direction log-status
```

Dalam contoh berikut, versinya 5 karena catatan meliputi bidang versi 5. Instans EC2 memanggil layanan Amazon S3. Log alur ditangkap pada antarmuka jaringan untuk instans. Catatan pertama memiliki arah aliran ingress dan catatan kedua memiliki arah aliran egress. Untuk catatan egress, traffic-path-nya 8, menunjukkan bahwa lalu lintas melewati gateway internet. Bidang traffic-path tidak didukung untuk lalu lintas ingress. Saat pkt-srcaddr atau pkt-dstaddr adalah alamat IP publik, nama layanan ditampilkan.

```
5 52.95.128.179 10.0.0.71 80 34210 6 1616729292 1616729349 IPv4 14 15044
 123456789012 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-0c50d5961bcb2d47b
 eni-1235b8ca123456789 ap-southeast-2 apse2-az3 - - ACCEPT 19 52.95.128.179 10.0.0.71
 S3 - - ingress OK
5 10.0.0.71 52.95.128.179 34210 80 6 1616729292 1616729349 IPv4 7 471 123456789012 vpc-
abcdefab012345678 subnet-aaaaaaaa012345678 i-0c50d5961bcb2d47b eni-1235b8ca123456789
 ap-southeast-2 apse2-az3 - - ACCEPT 3 10.0.0.71 52.95.128.179 - S3 8 egress OK
```

Batasan log alur

Untuk menggunakan log alur , Anda perlu memahami batasan-batasan berikut:

- Setelah membuat log alur, Anda tidak akan melihat data log aliran sampai ada lalu lintas aktif untuk antarmuka jaringan, subnet, atau VPC yang Anda pilih.
- Anda tidak dapat mengaktifkan log alur untuk VPC yang di-peering-kan dengan VPC Anda kecuali VPC peer berada di akun Anda.
- Setelah membuat log alur, Anda tidak dapat mengubah konfigurasi atau format catatan log alur. Misalnya, Anda tidak dapat mengaitkan IAM role yang berbeda dengan log alur, atau menambahkan atau menghapus bidang dalam catatan log alur. Sebaliknya, Anda dapat menghapus log alur dan membuat yang baru dengan konfigurasi yang diperlukan.
- Jika antarmuka jaringan Anda memiliki beberapa alamat IPv4 dan lalu lintas dikirim ke alamat IPv4 privat sekunder, log alur menampilkan alamat IPv4 privat utama di bidang `dstaddr`. Untuk menangkap alamat IP tujuan asal, buat log alur dengan bidang `pkt-dstaddr`.
- Jika lalu lintas dikirim ke antarmuka jaringan dan tujuan bukan salah satu alamat IP antarmuka jaringan, log alur menampilkan alamat IPv4 privat utama di bidang `dstaddr`. Untuk menangkap alamat IP tujuan asal, buat log alur dengan bidang `pkt-dstaddr`.
- Jika lalu lintas dikirim dari antarmuka jaringan dan sumbernya bukan salah satu alamat IP antarmuka jaringan, perilaku tergantung pada arah aliran. Untuk aliran keluar, log aliran menampilkan alamat IPv4 pribadi utama di `srcaddr` bidang. Untuk menangkap alamat IP sumber asal, buat log alur dengan bidang `pkt-srcaddr`.

  Jika catatan log adalah untuk aliran masuk ke antarmuka jaringan, IP pribadi utama dari antarmuka jaringan tidak akan ditampilkan di `srcaddr` lapangan.
- Ketika antarmuka jaringan Anda dilampirkan ke Nitro-based instance, interval agregasi selalu 1 menit atau kurang, terlepas dari interval agregasi maksimum yang ditentukan.
- Untuk `pkt-dstaddr` bidang `pkt-srcaddr` dan, jika lapisan perantara mengaktifkan Pelestarian alamat IP Klien, bidang ini mungkin menampilkan IP Klien yang dipertahankan alih-alih alamat IP dari lapisan perantara.
- Untuk `traffic-path` bidang, nilainya sama untuk aliran melalui sumber daya di VPC yang sama dan aliran melalui gateway lokal Outpost.
- Beberapa catatan log aliran dapat dilewati selama interval agregasi (lihat log-status di). Bidang yang tersedia Hal ini mungkin disebabkan oleh kendala AWS kapasitas internal atau kesalahan internal. Jika Anda menggunakan AWS Cost Explorer untuk melihat biaya log aliran VPC dan

beberapa log aliran dilewati selama interval agregasi log aliran, jumlah log aliran yang dilaporkan AWS Cost Explorer akan lebih tinggi daripada jumlah log aliran yang diterbitkan oleh Amazon VPC.

- Jika Anda menggunakan VPC Block Public Access (BPA):
  - Log aliran untuk VPC BPA tidak menyertakan catatan yang dile wati.
  - Log alur untuk VPC BPA tidak disertakan `bytes` meskipun Anda menyertakan `bytes` bidang tersebut dalam log alur Anda.
- VPC Flow Logs mendukung maksimal 250 langganan per sumber daya per akun. Untuk membuat langganan tambahan pada sumber daya yang telah mencapai batas ini, Anda harus terlebih dahulu menghapus langganan yang ada.

Log alur tidak menangkap semua lalu lintas IP. Jenis lalu lintas berikut tidak dicatat:

- Lalu lintas yang dihasilkan oleh instans ketika menghubungi server DNS Amazon. Jika Anda menggunakan server DNS Anda sendiri, maka semua lalu lintas ke server DNS tersebut dicatat.
- Lalu lintas yang dihasilkan oleh instans Windows untuk aktivasi lisensi Amazon Windows.
- Lalu lintas ke dan dari `169.254.169.254` untuk metadata instans.
- Lalu lintas ke dan dari `169.254.169.123` untuk layanan Amazon Time Sync.
- Lalu lintas DHCP.
- Lalu lintas mencerminkan lalu lintas sumber. Anda hanya akan melihat lalu lintas yang dicerminkan oleh lalu lintas target.
- Lalu lintas ke alamat IP yang dipesan untuk router VPC default.
- Lalu lintas antara antarmuka jaringan titik akhir dan antarmuka jaringan Penyeimbang Beban Jaringan.
- Lalu lintas Protokol Resolusi Alamat (ARP).
- Lalu lintas pada gateway NAT regional berumur pendek, yang dihapus beberapa menit setelah pembuatan.

Batasan khusus untuk bidang ECS tersedia di versi 7:

- Bidang ECS tidak dihitung jika tugas ECS yang mendasarinya tidak dimiliki oleh pemilik langganan log alur.

  Misalnya, Anda berbagi subnet (`SubnetA`) dengan account lain (`AccountB`), lalu Anda membuat langganan log alur untuk`SubnetA`. Jika `AccountB` meluncurkan tugas ECS di subnet bersama,

langganan Anda menerima log lalu lintas dari tugas-tugas tersebut. Namun, bidang ECS untuk log ini tidak dihitung karena masalah keamanan.

- Jika Anda membuat langganan log alur dengan bidang ECS di tingkat VPC/Subnet sumber daya, lalu lintas apa pun yang dihasilkan untuk antarmuka jaringan non-ECS juga akan dikirimkan untuk langganan Anda. Nilai untuk bidang ECS adalah '-' untuk lalu lintas IP non-ECS. Misalnya, Anda memiliki subnet (`subnet-000000`) dan Anda membuat langganan log alur untuk subnet ini dengan bidang ECS (). `fl-00000000` Di`subnet-000000`, Anda meluncurkan instance EC2 (`i-0000000`) yang terhubung ke internet dan secara aktif menghasilkan lalu lintas IP. Anda juga meluncurkan tugas ECS (`ECS-Task-1`) yang sedang berjalan di subnet yang sama. Karena `ECS-Task-1` keduanya `i-0000000` dan menghasilkan lalu lintas IP, langganan log aliran Anda `fl-00000000` akan mengirimkan log lalu lintas untuk kedua entitas. Namun, hanya `ECS-Task-1` akan memiliki metadata ECS aktual untuk bidang ECS yang Anda sertakan dalam LogFormat Anda. Untuk lalu lintas `i-0000000` terkait, bidang ini akan memiliki nilai '-'.
- `ecs-container-id`dan `ecs-second-container-id` dipesan saat layanan VPC Flow Logs menerimanya dari aliran acara ECS. Mereka tidak dijamin berada dalam urutan yang sama seperti yang Anda lihat di konsol ECS atau dalam panggilan DescribeTask API. Jika kontainer memasuki status STOP saat tugas masih berjalan, itu mungkin terus muncul di log Anda.
- Metadata ECS dan log lalu lintas IP berasal dari dua sumber yang berbeda. Kami mulai menghitung lalu lintas ECS Anda segera setelah kami memperoleh semua informasi yang diperlukan dari dependensi hulu.

  Setelah Anda memulai tugas baru, kami mulai menghitung bidang ECS Anda ketika kedua kondisi berikut terpenuhi: kami menerima lalu lintas IP untuk antarmuka jaringan yang mendasarinya, dan kami menerima peristiwa ECS yang berisi metadata untuk tugas ECS Anda untuk menunjukkan tugas sedang berjalan.

  Setelah Anda menghentikan tugas, kami berhenti menghitung bidang ECS Anda ketika kedua kondisi berikut terpenuhi: kami tidak lagi menerima lalu lintas IP untuk antarmuka jaringan yang mendasarinya (atau kami menerima lalu lintas IP yang tertunda selama lebih dari satu hari), dan kami menerima peristiwa ECS yang berisi metadata untuk tugas ECS Anda untuk menunjukkan tugas Anda tidak lagi berjalan.
- Hanya tugas ECS yang diluncurkan dalam mode `awsvpc` jaringan yang didukung.

Batasan khusus untuk `encryption-status` bidang:

- Status enkripsi mungkin '-' (tidak tersedia) di beberapa aliran, karena keterbatasan beberapa alat jaringan untuk melaporkan status enkripsi. Pengguna dapat mengabaikan alur ini dalam analisis.
- Menampilkan sebagai terenkripsi dalam mode monitor tidak berarti aliran akan diizinkan dalam mode menegakkan. Begitu juga sebaliknya.
  - Jika aliran dienkripsi dalam mode monitor, mungkin tidak sesuai dalam mode menegakkan:
    - Jika alur melibatkan ENI yang dibuat oleh AWS layanan, maka layanan perlu mendukung Kontrol Enkripsi.
    - Jika aliran melewati peering VPC, VPC yang diintip mungkin tidak memaksa Kontrol Enkripsi.
  - Jika aliran tidak dienkripsi dalam mode monitor, itu mungkin masih sesuai dalam mode menegakkan, mengingat layanan yang terkait dengan aliran ditambahkan sebagai pengecualian.

Batasan khusus untuk Flow Log bidang Tag Amazon EC2 tersedia di versi 11:

- Bidang tag tidak dihitung jika tag pada sumber daya tidak dimiliki oleh pemilik langganan log alur.

  Misalnya, Anda berbagi subnet (`SubnetA`) dengan account lain (`AccountB`), dan kemudian Anda membuat langganan log alur untuk `SubnetA` dengan bidang tag pada antarmuka jaringan. Jika `AccountB` meluncurkan antarmuka jaringan yang ditandai dengan kunci yang Anda konfigurasikan, langganan Anda menerima log lalu lintas untuk antarmuka jaringan yang diluncurkan oleh`AccountB`, tetapi bidang tag yang dikonfigurasi oleh langganan Anda tidak dihitung karena masalah keamanan. Anda dapat menandai antarmuka jaringan yang diluncurkan oleh `AccountB` untuk menampilkan tag jika diinginkan.
- Jika Anda membuat langganan log alur dengan bidang Tag di tingkat VPC/Subnet sumber daya, lalu lintas apa pun yang dihasilkan untuk antarmuka jaringan yang tidak diberi tag juga akan dikirimkan untuk langganan Anda. Nilai untuk bidang Tag akan menjadi '-' untuk sumber daya yang tidak diberi tag.
- Grup Penskalaan Otomatis tidak akan dapat menampilkan tag apa pun jika diberi nama '-' karena ini adalah karakter yang dicadangkan untuk menunjukkan missing/no nilai.
- Pembuatan langganan Flow Logs dengan bidang Tag akan menghasilkan pembuatan beberapa sumber daya atas nama pelanggan. Untuk mengkonsumsi pembaruan pada nilai tag Anda, EventBridge Aturan Terkelola akan dibuat untuk mengirim perubahan tag ke layanan Log Aliran. A EventBridge turan Terkelola ini akan dibersihkan secara otomatis jika semua langganan dengan bidang Tag dihapus. Jangan menghapus Aturan Terkel EventBridge ola ini secara manual. Melakukannya akan mengakibatkan penundaan besar memperbarui nilai tag. Untuk mengontrol ini

creation/cleanup dan memberikan akses ke nilai tag, Peran Tertaut Layanan akan dibuat di akun Anda. Lihat Menggunakan peran terkait layanan untuk Log Aliran VPC untuk detail selengkapnya.

- Karena penguraian Amazon CloudWatch Logs dan batasan penguraian Athena, semua karakter khusus dalam nilai tag akan dikodekan menggunakan UTF-8 pengkodean persen. Ini dapat didekodekan secara asli di Athena menggunakan `url_decode` atau dapat didekodekan oleh URL atau decoder URI apa pun.
- Untuk jam pertama setelah langganan baru dibuat, nilai tag mungkin hilang atau tidak akurat. Setelah jam pertama ini, nilai tag akan dapat secara akurat mencerminkan nilai sumber daya yang ditandai dengan perincian 1 menit.
- Jika beberapa perubahan tag dilakukan pada sumber daya yang sama dalam detik yang sama, ada potensi pembaruan hilang, mengakibatkan nilai tag basi hingga satu jam.
- Untuk bidang tag grup Penskalaan Otomatis, Anda harus memiliki setidaknya satu CloudTrail jejak yang diaktifkan di akun Anda. Tanpa jejak yang diaktifkan, nilai tag grup Auto Scaling mungkin basi atau tidak akurat.

Batasan khusus untuk `next-hop-` bidang:

- Bidang hop berikutnya tidak dihitung jika antarmuka jaringan hop berikutnya tidak dimiliki oleh pemilik langganan log alur, kecuali untuk`next-hop-az-id`.
- Bidang hop berikutnya tidak tersedia jika hop berikutnya tidak memiliki antarmuka jaringan (Misalnya, lalu lintas ke gateway internet).
- Bidang hop berikutnya tidak tersedia untuk lalu lintas lintas wilayah.
- Bidang hop berikutnya tidak tersedia untuk lalu lintas masuk dari beberapa layanan jaringan (misalnya, gateway transit dan Network Load Balancer).
- Jika lalu lintas melewati middlebox (misalnya, transit gateway atau Network Load Balancer), antarmuka jaringan hop berikutnya adalah antarmuka yang terkait dengan middlebox (seperti lampiran gateway transit), bukan tujuan akhir lalu lintas

Harga

Biaya penyerapan dan arsip data untuk log yang dijual berlaku saat Anda menerbitkan log alur. Untuk informasi selengkapnya tentang harga saat menerbitkan log yang dijual, buka CloudWatch Harga Amazon, pilih Log dan temukan Log yang Di jual.

Untuk melacak biaya dari penerbitan log alur, Anda dapat menerapkan tag alokasi biaya ke sumber daya tujuan Anda. Setelah itu, laporan alokasi AWS biaya Anda mencakup penggunaan dan biaya yang digabungkan oleh tag ini. Anda dapat menerapkan tag yang mewakili kategori bisnis (seperti pusat biaya, nama aplikasi, atau pemilik) untuk mengatur biaya Anda. Untuk informasi selengkapnya, lihat berikut ini:

- Menggunakan Tanda Alokasi Biaya dalam AWS Billing Panduan Pengguna
- Menandai grup log di Amazon CloudWatch Log di Panduan Pengguna Amazon CloudWatch Logs
- Menggunakan tag bucket S3 alokasi biaya di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon
- Menandai Aliran Pengiriman Anda di Panduan Peng embang Amazon Data Firehose

Bekerja dengan log alur

Anda dapat bekerja dengan log aliran menggunakan konsol untuk Amazon EC2 dan Amazon VPC.

Tugas

- 1. Kontrol penggunaan log aliran dengan IAM
- 2. Membuat log alur
- 3. Menandai log alur
- 4. Menghapus log alur
- Ikhtisar baris perintah

1. Kontrol penggunaan log aliran dengan IAM

Secara default, pengguna tidak memiliki izin untuk bekerja dengan log aliran. Anda dapat membuat peran IAM dengan kebijakan terlampir yang memberi pengguna izin untuk membuat, menjelaskan, dan menghapus log alur.

Berikut ini adalah contoh kebijakan yang memberikan izin penuh kepada pengguna untuk membuat, menjelaskan, dan menghapus log alur.

JSON

```
{
  "Version":"2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteFlowLogs",
        "ec2:CreateFlowLogs",
        "ec2:DescribeFlowLogs"
      ],
      "Resource": "*"
    }
  ]
}
```

Untuk informasi selengkapnya, lihat the section called “Bagaimana cara Amazon VPC bekerja sama dengan IAM”.

2. Membuat log alur

Anda dapat membuat log alur untuk VPC, subnet, atau antarmuka jaringan. Saat Anda membuat log alur, Anda harus menentukan tujuan untuk log alur. Untuk informasi selengkapnya, lihat berikut ini:

- the section called “Buat log alur yang menerbitkan ke CloudWatch Log”
- the section called “Membuat log alur yang menerbitkan ke Amazon S3”
- the section called “Buat log alur yang diterbitkan ke Amazon Data Firehose”

3. Menandai log alur

Anda dapat menambahkan atau menghapus tag untuk log alur kapan saja.

Untuk mengelola tag untuk log alur

1. Lakukan salah satu tindakan berikut:
   - Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/. Di panel navigasi, pilih Antarmuka Jaringan. Pilih kotak centang untuk antarmuka jaringan.
   - Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Pada panel navigasi, pilih VPC Anda. Pilih kotak centang untuk VPC.
   - Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Di panel navigasi, pilih Pengguna. Pilih kotak centang untuk subnet.

2. Pilih Log Aliran.
3. Pilih Tindakan, Kelola tag.
4. Untuk menambahkan tag baru, pilih Tambahkan tag baru dan masukkan kunci dan nilai. Untuk menghapus sebuah tag, pilih Hapus.
5. Setelah selesai menambahkan atau menghapus tag, pilih S impan.

4. Menghapus log alur

Anda dapat menghapus log alur kapan saja. Setelah Anda menghapus log alur, perlu beberapa menit untuk menghentikan pengumpulan data.

Menghapus log alur tidak menghapus data log dari tujuan atau mengubah sumber daya tujuan. Anda harus menghapus data log alur yang ada langsung dari tujuan, dan membersihkan sumber daya tujuan, menggunakan konsol untuk layanan tujuan.

Untuk menghapus log alur

1. Lakukan salah satu tindakan berikut:
   - Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/. Di panel navigasi, pilih Antarmuka Jaringan. Pilih kotak centang untuk antarmuka jaringan.
   - Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Pada panel navigasi, pilih VPC Anda. Pilih kotak centang untuk VPC.
   - Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Di panel navigasi, pilih Pengguna. Pilih kotak centang untuk subnet.
2. Pilih Log Aliran.
3. Pilih T ind akan, Hapus log alur.
4. Saat diminta konfirmasi, ketik **`delete`** lalu pilih H apus.

Ikhtisar baris perintah

Anda dapat melakukan tugas yang dijelaskan pada halaman ini menggunakan baris perintah.

Membuat log alur

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

Jelaskan log aliran

- describe-flow-logs (AWS CLI)
- Get-EC2FlowLog (AWS Tools for Windows PowerShell)

Menandai log alur

- buat-tag dan hapus tag () AWS CLI
- New-EC2Tagdan Remove-EC2Tag (AWS Tools for Windows PowerShell)

Menghapus log alur

- delete-flow-logs (AWS CLI)
- Remove-EC2FlowLog (AWS Tools for Windows PowerShell)

Publikasikan log alur ke CloudWatch Log

Log aliran dapat mempublikasikan data log aliran langsung ke Amazon CloudWatch. Amazon CloudWatch adalah layanan pemantauan dan pengamatan yang komprehensif. Ini mengumpulkan dan melacak metrik, log, dan data peristiwa dari berbagai AWS sumber daya, serta aplikasi dan layanan Anda sendiri. CloudWatch memberikan visibilitas ke dalam pemanfaatan sumber daya, kinerja aplikasi, dan kesehatan operasional, memungkinkan Anda mendeteksi dan menanggapi perubahan kinerja di seluruh sistem dan masalah potensial. Dengan CloudWatch, Anda dapat mengatur alarm, memvisualisasikan log dan metrik, dan secara otomatis bereaksi untuk mengumpulkan dan mengoptimalkan sumber daya cloud Anda. Ini adalah alat penting untuk memastikan keandalan, ketersediaan, dan kinerja infrastruktur dan aplikasi berbasis cloud Anda.

Saat menerbitkan ke CloudWatch Log, data log aliran dipublikasikan ke grup log, dan setiap antarmuka jaringan memiliki aliran log unik di grup log. Pengaliran log berisi catatan log alur. Anda dapat membuat beberapa log alur yang menerbitkan data ke grup log yang sama. Jika antarmuka jaringan yang sama hadir dalam satu atau lebih pengaliran log dalam grup log yang sama, maka akan memiliki satu pengaliran log gabungan. Jika Anda telah menetapkan bahwa satu log alur harus menangkap lalu lintas yang ditolak, dan log alur lainnya harus menangkap lalu lintas yang diterima, maka pengaliran log gabungan menangkap semua lalu lintas.

Di CloudWatch Log, bidang stempel waktu sesuai dengan waktu mulai yang ditangkap dalam catatan log alur. Bid ang IngestionTime menunjukkan tanggal dan waktu ketika catatan log alur

diterima oleh CloudWatch Log. Stempel waktu ini lebih lambat dari waktu akhir yang ditangkap dalam catatan log alur.

Untuk informasi selengkap CloudWatch nya tentang Log, lihat Log dikirim ke CloudWatch Log di Panduan CloudWatch Pengguna Amazon Log.

Harga

Biaya penyerapan dan arsip data untuk log yang dijual berlaku saat Anda menerbitkan log alur ke CloudWatch Log. Untuk informasi selengkapnya, buka CloudWatch Harga Amazon, pilih Log dan temukan Log Dijual.

Daftar Isi

- Peran IAM untuk menerbitkan log alur ke Log CloudWatch
- Buat log alur yang menerbitkan ke CloudWatch Log
- Lihat catatan log alur dengan CloudWatch Log
- Cari catatan log alur
- Proses catatan log alur di CloudWatch Log

Peran IAM untuk menerbitkan log alur ke Log CloudWatch

Peran IAM yang terkait dengan log alur Anda harus memiliki izin yang cukup untuk menerbitkan log alur ke grup log yang ditentukan di CloudWatch Log. Peran IAM harus milik AWS akun Anda.

Kebijakan IAM yang dilampirkan ke IAM role Anda harus menyertakan setidaknya izin berikut.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
```

```
        "logs:DescribeLogStreams"
      ],
      "Resource": "*"
    }
  ]
}
```

Pastikan peran Anda memiliki kebijakan kepercayaan berikut, yang memungkinkan layanan log aliran untuk mengambil peran tersebut.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Kami menyarankan Anda menggunakan kunci syarat `aws:SourceAccount` dan `aws:SourceArn` untuk melindungi diri Anda dari masalah wakil yang membingungkan. Misalnya, Anda dapat menambahkan blok kondisi berikut ke kebijakan kepercayaan sebelumnya. Akun sumber adalah pemilik log aliran dan ARN sumber adalah log aliran ARN. Jika Anda tidak mengetahui ID log alur, Anda dapat mengganti bagian ARN tersebut dengan wildcard (*) dan kemudian memperbarui kebijakan setelah Anda membuat log alur.

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:region:account_id:vpc-flow-log/flow-log-id"
    }
```

```
}
```

Membuat peran IAM untuk log aliran

Anda dapat memperbarui peran yang ada seperti dijelaskan di atas. Atau, Anda dapat menggunakan prosedur berikut untuk membuat peran baru untuk digunakan dengan log aliran. Anda akan menentukan peran ini saat membuat log alur.

Untuk membuat IAM role untuk log alur

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Kebijakan.
3. Pilih Buat kebijakan.
4. Pada halaman Buat kebijakan, lakukan hal berikut:
   a. PilihJSON.
   b. Ganti isi jendela ini dengan kebijakan izin di awal bagian ini.
   c. Pilih Berikutnya.
   d. Masukkan nama untuk kebijakan Anda dan deskripsi dan tag opsional, lalu pilih Buat kebijakan.
5. Di panel navigasi, pilih Peran.
6. Pilih Buat peran.
7. Untuk Ti pe entitas tepercaya, pilih Kebijakan kepercayaan kustom. Untuk Kebijakan kepercayaan kustom, ganti `"Principal": {},` dengan yang berikut, lalu pilih Ber ikutnya.

   ```
   "Principal": {
      "Service": "vpc-flow-logs.amazonaws.com"
   },
   ```

8. Pada halaman Tambah izin, pilih kotak centang untuk kebijakan yang Anda buat sebelumnya dalam prosedur ini, lalu pilih Ber ikutnya.
9. Masukkan nama untuk peran Anda dan berikan deskripsi secara opsional.
10. Pilih Buat peran.

Buat log alur yang menerbitkan ke CloudWatch Log

Anda dapat membuat log alur untuk VPC, subnet, atau antarmuka jaringan. Jika Anda melakukan langkah-langkah ini sebagai pengguna menggunakan peran IAM tertentu, pastikan peran tersebut memiliki izin untuk menggunakan `iam:PassRole` tindakan tersebut.

Prasyarat

Verifikasi bahwa prinsipal IAM yang Anda gunakan untuk membuat permintaan memiliki izin untuk memanggil `iam:PassRole` tindakan.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/flow-log-role-name"
        }
    ]
}
```

Untuk membuat log alur menggunakan konsol

1. Lakukan salah satu tindakan berikut:
   - Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/. Di panel navigasi, pilih Antarmuka Jaringan. Pilih kotak centang untuk antarmuka jaringan.
   - Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Pada panel navigasi, pilih VPC Anda. Pilih kotak centang untuk VPC.
   - Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Di panel navigasi, pilih Pengguna. Pilih kotak centang untuk subnet.
2. Pilih T ind akan, Buat log alur.
3. Untuk Filter, tentukan jenis lalu lintas ke log. Pilih Semua ke log lalu lintas diterima dan ditolak, Tolak ke log hanya lalu lintas yang ditolak, atau Terima ke log hanya lalu lintas yang diterima.

4. Untuk Interval agregasi maksimum, pilih periode waktu maksimum selama aliran ditangkap dan dikumpulkan ke dalam satu catatan log alur.
5. Untuk Tujuan, pilih Kirim ke CloudWatch Log.
6. Untuk Grup log tujuan, pilih nama grup log yang ada atau masukkan nama grup log baru. Jika Anda memasukkan nama, kami membuat grup log ketika ada lalu lintas untuk log.
7. Untuk akses Layanan, pilih peran layanan IAM yang ada yang memiliki izin untuk menerbitkan CloudWatch log ke Log atau pilih untuk membuat peran layanan baru.
8. Untuk Format catatan log, pilih format untuk catatan log alur.
   - Untuk menggunakan format default, pilih format default AWS .
   - Untuk menggunakan format kustom, pilih Format kustom dan kemudian pilih bidang dari Format log.
9. Untuk Metadata tambahan, pilih apakah Anda ingin menyertakan metadata dari Amazon ECS dalam format log.
10. (Opsional) Pilih Tambahkan tag baru untuk menerapkan tag ke log alur.
11. Pilih Buat log alur.

Untuk membuat log alur menggunakan baris perintah

Gunakan salah satu perintah berikut ini.

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

AWS CLI Contoh berikut membuat log alur yang menangkap semua lalu lintas yang diterima untuk subnet yang ditentukan. Log alur dikirim ke grup log yang ditentukan. `--deliver-logs-permission-arn`Parameter menentukan peran IAM yang diperlukan untuk menerbitkan ke CloudWatch Log.

```
aws ec2 create-flow-logs --resource-type Subnet --resource-ids subnet-1a2b3c4d --
traffic-type ACCEPT --log-group-name my-flow-logs --deliver-logs-permission-arn
 arn:aws:iam::123456789101:role/publishFlowLogs
```

Lihat catatan log alur dengan CloudWatch Log

Anda dapat melihat catatan log alur menggunakan konsol CloudWatch Logs. Setelah Anda membuat log alur, mungkin perlu beberapa menit agar log tersebut terlihat di konsol.

Untuk melihat catatan log alur yang dipublikasikan ke CloudWatch Log menggunakan konsol

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, pilih Log, Grup log.
3. Pilih nama grup log yang berisi log alur Anda untuk membuka halaman detailnya.
4. Pilih nama aliran log yang berisi catatan log alur. Untuk informasi selengkapnya, lihat Catatan log alur.

Untuk melihat catatan log alur yang diterbitkan ke CloudWatch Log menggunakan baris perintah

- get-log-events (AWS CLI)
- Get-CWLLogEvent (AWS Tools for Windows PowerShell)

Cari catatan log alur

Anda dapat mencari catatan log alur yang dipublikasikan ke CloudWatch Log menggunakan konsol CloudWatch Log. Anda dapat menggunakan filter metrik untuk menyaring catatan log alur. Catatan log alur adalah ruang yang dibatasi.

Untuk mencari catatan log alur menggunakan konsol CloudWatch Logs

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, pilih Log, Grup log.
3. Pilih grup log yang berisi log alur Anda, lalu pilih aliran log, jika Anda tahu antarmuka jaringan yang Anda cari. Atau, pilih Cari grup log. Tindakan ini mungkin membutuhkan waktu lama jika ada banyak antarmuka jaringan di grup log Anda, atau tergantung pada rentang waktu yang Anda pilih.
4. Di bawah Filter peristiwa, masukkan string di bawah ini. Ini mengasumsikan bahwa catatan log alur menggunakan format default.

```
[version, accountid, interfaceid, srcaddr, dstaddr, srcport, dstport, protocol,
 packets, bytes, start, end, action, logstatus]
```

5. Ubah filter sesuai kebutuhan dengan menentukan nilai untuk bidang. Contoh berikut adalah filter berdasarkan alamat IP sumber tertentu.

```
[version, accountid, interfaceid, srcaddr = 10.0.0.1, dstaddr, srcport, dstport,
 protocol, packets, bytes, start, end, action, logstatus]
[version, accountid, interfaceid, srcaddr = 10.0.2.*, dstaddr, srcport, dstport,
 protocol, packets, bytes, start, end, action, logstatus]
```

   Contoh berikut adalah filter berdasarkan port tujuan, jumlah byte, dan apakah lalu lintas ditolak.

```
[version, accountid, interfaceid, srcaddr, dstaddr, srcport, dstport = 80 ||
 dstport = 8080, protocol, packets, bytes, start, end, action, logstatus]
[version, accountid, interfaceid, srcaddr, dstaddr, srcport, dstport = 80 ||
 dstport = 8080, protocol, packets, bytes >= 400, start, end, action = REJECT,
 logstatus]
```

Proses catatan log alur di CloudWatch Log

Anda dapat memproses catatan log alur seperti yang Anda lakukan dengan peristiwa log lainnya yang dikumpulkan oleh CloudWatch Log. Untuk informasi selengkapnya tentang memantau data log dan filter metrik, lihat Membuat metrik dari peristiwa log menggunakan filter di Panduan CloudWatch Pengguna Amazon Log.

Contoh: Membuat filter CloudWatch metrik dan alarm untuk log aliran

Dalam contoh ini, Anda memiliki log alur untuk `eni-1a2b3c4d`. Anda ingin membuat alarm yang memperingatkan Anda jika ada 10 percobaan penolakan atau lebih untuk terkoneksi ke instans Anda melalui TCP port 22 (SSH) dalam jangka waktu 1 jam. Pertama, Anda harus membuat filter metrik yang sesuai dengan pola lalu lintas yang untuknya harus membuat alarm. Setelah itu, Anda dapat membuat alarm untuk filter metrik.

Untuk membuat filter metrik untuk lalu lintas SSH yang ditolak dan membuat alarm untuk filter

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, pilih Log, Grup log.
3. Pilih kotak centang untuk grup log, lalu pilih Tindakan , Buat filter metrik.
4. Untuk Pola Filter, masukkan string berikut.

```
[version, account, eni, source, destination, srcport, destport="22", protocol="6",
 packets, bytes, windowstart, windowend, action="REJECT", flowlogstatus]
```

5. Untuk Pilih data log untuk diuji, pilih aliran log untuk antarmuka jaringan Anda. (Opsional) Untuk melihat baris data log yang cocok dengan pola filter, pilih P ola uji.
6. Saat Anda siap, pilih Berikutnya.
7. Masukkan nama filter, namespace metrik, dan nama metrik. Atur nilai metrik ke 1. Setelah selesai, pilih Ber ikutnya, lalu pilih Buat filter metrik.
8. Pada panel navigasi, pilih Alarm, Semua alarm.
9. Pilih Buat alarm.
10. Pilih nama metrik yang Anda buat, lalu pilih Pilih metrik.
11. Konfigurasikan alarm sebagai berikut, lalu pilih Next (Selanjutnya):
    - Untuk Statistik pilih Jumlah. Ini memastikan bahwa Anda menangkap jumlah total titik data untuk periode waktu yang ditentukan.
    - Untuk Peri ode, pilih 1 jam.
    - Karena kapan pun TimeSinceLastActive ... , pilih Greater/Equal dan masukkan 10 untuk ambang batas.
    - Untuk konfigurasi tambahan, titik data untuk alarm, biarkan default 1.
12. Pilih Berikutnya.
13. Untuk Pem beritahuan, pilih topik SNS yang ada atau pilih Buat topik baru untuk membuat topik baru. Pilih Berikutnya.
14. Masukkan nama dan deskripsi untuk alarm dan pilih Ber ikutnya.
15. Setelah selesai melihat pratinjau alarm, pilih Buat alarm.

Terbitkan log alur ke Amazon S3

Arus log dapat menerbitkan data log alur ke Amazon S3. Amazon S3 (Simple Storage Service) adalah layanan penyimpanan objek yang sangat skalabel dan tahan lama. Ini dirancang untuk menyimpan dan mengambil sejumlah data, dari mana saja di web. S3 menawarkan daya tahan dan ketersediaan terdepan di industri, dengan fitur bawaan untuk pembuatan versi data, enkripsi, dan kontrol akses.

Ketika menerbitkan ke Amazon S3, data log alur diterbitkan ke bucket Amazon S3 yang ada yang Anda tentukan. Catatan log alur untuk semua antarmuka jaringan yang dipantau diterbitkan untuk serangkaian objek file berkas log yang disimpan dalam bucket. Jika log alur menangkap data untuk VPC, log alur menerbitkan catatan log alur untuk semua antarmuka jaringan di VPC yang dipilih.

Untuk membuat bucket Amazon S3 untuk digunakan dengan log aliran, lihat Membuat bucket di Panduan Pengguna Amazon S3.

Untuk informasi selengkapnya tentang cara merampingkan penyerapan log aliran VPC, pemrosesan log aliran, dan visualisasi log aliran, lihat Pencatatan Terpusat dengan OpenSearch di Pustaka AWS Solusi.

Untuk informasi selengkap CloudWatch nya tentang Log, lihat Log yang dikirim ke Amazon S3 di Panduan CloudWatch Pengguna Amazon Log.

Harga

Biaya penggunaan dan pengarsipan data untuk log penjual otomatis berlaku saat Anda menerbitkan log alur ke Amazon S3. Untuk informasi selengkapnya, buka CloudWatch Harga Amazon, pilih Log dan temukan Log Dijual.

Daftar Isi

- Berkas log alur
- Izin bucket Amazon S3 untuk log alur
- Kebijakan kunci yang diperlukan untuk digunakan dengan SSE-KMS
- Izin file berkas log Amazon S3
- Membuat log alur yang menerbitkan ke Amazon S3
- Lihat catatan log alur dengan Amazon S3

Berkas log alur

VPC Flow Logs mengumpulkan data tentang lalu lintas IP yang menuju dan dari VPC Anda ke dalam catatan log, menggabungkan catatan tersebut ke dalam file log, dan kemudian menerbitkan file log ke bucket Amazon S3 dengan interval 5 menit. Beberapa file dapat dipublikasikan dan setiap file log mungkin berisi beberapa atau semua catatan log aliran untuk lalu lintas IP yang direkam dalam 5 menit sebelumnya.

Dalam Amazon S3, bidang Terakhir diubah untuk berkas log alur menunjukkan tanggal dan waktu di mana file diunggah ke Amazon S3 bucket. Ini lebih lambat dari stempel waktu dalam nama file, dan berbeda dengan jumlah waktu yang dibutuhkan untuk mengunggah file ke bucket Amazon S3.

Format file log

Anda dapat menentukan salah satu format berikut untuk file log. Setiap file dikompresi menjadi satu file Gzip.

- Teks — Teks biasa. Ini adalah format default.
- Parket — Apache Parquet adalah format data kolumnar. Kueri pada data dalam format Parquet 10 hingga 100 kali lebih cepat dibandingkan dengan kueri pada data dalam teks biasa. Data dalam format Parquet dengan kompresi Gzip membutuhkan ruang penyimpanan 20 persen lebih sedikit daripada teks biasa dengan kompresi Gzip.

> **Note**
>
> Jika data dalam format Parquet dengan kompresi Gzip kurang dari 100 KB per periode agregasi, menyimpan data dalam format Parquet mungkin memakan lebih banyak ruang daripada teks biasa dengan kompresi Gzip karena persyaratan memori file Parquet.

Opsi file log

Anda dapat secara opsional menentukan opsi berikut.

- Hive-compatible Awalan S3 - Aktifkan aw Hive-compatible alan alih-alih mengimpor partisi ke alat Anda Hive-compatible . Sebelum Anda menjalankan query, gunakan MSCK REPAIR TABLE perintah.
- Partisi per jam — Jika Anda memiliki volume log yang besar dan biasanya menargetkan kueri ke jam tertentu, Anda bisa mendapatkan hasil yang lebih cepat dan menghemat biaya kueri dengan mempartisi log setiap jam.

Struktur bucket file log S3

File log disimpan ke bucket Amazon S3 yang ditentukan menggunakan struktur folder yang didasarkan pada ID log alur, Wilayah, tanggal pembuatan, dan opsi tujuan.

Secara default, file dikirim ke lokasi berikut.

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/
```

Jika Anda mengaktifkan prefiks Hive-compatible S3, file dikirim ke lokasi berikut.

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/aws-service=vpcflowlogs/
aws-region=region/year=year/month=month/day=day/
```

Jika Anda mengaktifkan partisi per jam, file dikirim ke lokasi berikut.

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/hour/
```

Jika Anda mengaktifkan Hive-compatible partisi dan mempartisi log alur per jam, file dikirim ke lokasi berikut.

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/aws-service=vpcflowlogs/
aws-region=region/year=year/month=month/day=day/hour=hour/
```

Nama file log

Nama file dari file log didasarkan pada ID log alur, Wilayah, dan tanggal dan waktu pembuatan. Nama file menggunakan format berikut.

```
aws_account_id_vpcflowlogs_region_flow_log_id_YYYYMMDDTHHmmZ_hash.log.gz
```

Berikut ini adalah contoh file log untuk log alur yang dibuat oleh AWS akun123456789012, untuk sumber daya di us-east-1 Wilayah, June 20, 2018 di16:20 UTC. File berisi catatan log aliran dengan waktu akhir antara 16:20:00 dan16:24:59.

```
123456789012_vpcflowlogs_us-east-1_fl-1234abcd_20180620T1620Z_fe123456.log.gz
```

Izin bucket Amazon S3 untuk log alur

Objek dan bucket Amazon S3 secara default bersifat privat. Hanya pemilik bucket yang bisa mengakses bucket dan objek yang tersimpan di dalamnya. Namun, pemilik bucket dapat memberikan akses kepada sumber daya dan pengguna lain dengan menulis kebijakan akses.

Jika pengguna yang membuat log alur memiliki bucket `PutBucketPolicy` dan memiliki `GetBucketPolicy` izin untuk bucket, kami secara otomatis melampirkan kebijakan berikut ke bucket. Kebijakan ini akan menggantikan kebijakan yang sebelumnya sudah melekat pada bucket.

Jika tidak, pemilik bucket harus menambahkan kebijakan ini ke bucket, menentukan ID AWS akun pembuat log alur, atau pembuatan log alur gagal. Untuk informasi selengkapnya, lihat Menggunakan kebijakan bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "s3:x-amz-acl": "bucket-owner-full-control"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:us-east-1:123456789012:*"
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
```

```
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:us-east-1:123456789012:*"
                }
            }
        }
    ]
}
```

ARN yang Anda tentukan *my-s3-arn* tergantung pada apakah Anda menggunakan prefik Hive-compatible s S3.

- Awalan default

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/account_id/*
```

- Hive-compatible Awalan S3

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/aws-account-id=account_id/*
```

Ini adalah praktik terbaik untuk memberikan izin ini ke prinsipal layanan pengiriman log alih-alih Akun AWS ARN individu. Ini juga merupakan praktik terbaik untuk menggunakan kunci `aws:SourceAccount` dan `aws:SourceArn` kondisi untuk melindungi dari masalah wakil yang membingungkan. Akun sumber adalah pemilik log alur dan ARN sumber adalah wildcard (*) ARN dari layanan log.

Perhatikan bahwa layanan pengiriman log memanggil tindakan `HeadBucket` Amazon S3 API untuk memverifikasi keberadaan dan lokasi bucket S3. Anda tidak diharuskan memberikan izin layanan pengiriman log untuk memanggil tindakan ini. Layanan masih mengirimkan log aliran VPC meskipun tidak dapat mengonfirmasi bahwa bucket S3 ada. Namun, akan ada `AccessDenied` kesalahan untuk panggilan ke `HeadBucket` CloudTrail log Anda.

Kebijakan kunci yang diperlukan untuk digunakan dengan SSE-KMS

Anda dapat melindungi data di bucket Amazon S3 Anda dengan mengaktifkan En Server-Side kripsi dengan Amazon S3-Managed Keys (SSE-S3) atau Server-Side Enkripsi dengan KMS Keys (SSE-KMS) di bucket S3 Anda. Untuk informasi selengkapnya, lihat Melindungi data menggunakan enkripsi sisi server di Panduan Pengguna Amazon S3.

Jika Anda memilih SSE-S3, tidak diperlukan konfigurasi tambahan. Amazon S3 menangani kunci enkripsi.

Jika Anda memilih SSE-KMS, Anda harus menggunakan kunci yang dikelola pelanggan ARN. Jika Anda menggunakan ID kunci, Anda dapat mengalami LogDestination tidak terkirim kesalahan saat membuat log alur. Selain itu, Anda harus memperbarui kebijakan kunci untuk kunci yang dikelola pelanggan sehingga akun pengiriman log dapat menulis ke bucket S3 Anda. Untuk informasi selengkapnya tentang kebijakan kunci yang diperlukan untuk digunakan SSE-KMS, lihat enkripsi sisi server bucket Amazon S3 di Panduan Pengguna Amazon CloudWatch Logs.

Izin file berkas log Amazon S3

Selain kebijakan bucket yang diperlukan, Amazon S3 menggunakan daftar kontrol akses (ACL) untuk mengelola akses ke berkas log yang dibuat oleh log alur. Secara default, pemilik bucket memiliki izin `FULL_CONTROL` pada setiap file berkas log. Pemilik pengiriman log, jika berbeda dari pemilik bucket, tidak memiliki izin. Akun pengiriman log memiliki izin `READ` dan `WRITE`. Untuk informasi selengkapnya, lihat ikhtisar daftar kontrol akses (ACL) di Panduan Pengguna Amazon S3.

Membuat log alur yang menerbitkan ke Amazon S3

Setelah membuat dan mengonfigurasi bucket Amazon S3, Anda dapat membuat log alur untuk antarmuka jaringan, subnet, dan VPC.

Prasyarat

Prinsip IAM yang membuat log alur harus menggunakan peran IAM yang memiliki izin berikut, yang diperlukan untuk menerbitkan log alur ke bucket Amazon S3 tujuan.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource": "*"
    }
```

```
  ]
}
```

Untuk membuat log alur menggunakan konsol

1. Lakukan salah satu tindakan berikut:
   - Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/. Di panel navigasi, pilih Antarmuka Jaringan. Pilih kotak centang untuk antarmuka jaringan.
   - Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Pada panel navigasi, pilih VPC Anda. Pilih kotak centang untuk VPC.
   - Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Di panel navigasi, pilih Pengguna. Pilih kotak centang untuk subnet.
2. Pilih T ind akan, Buat log alur.
3. Untuk Filter, tentukan jenis data lalu lintas IP ke log.
   - Terima — Log hanya lalu lintas yang diterima.
   - Tolak — Catat hanya lalu lintas yang ditolak.
   - Semua — Log lalu lintas diterima dan ditolak.
4. Untuk Interval agregasi maksimum, pilih periode waktu maksimum untuk penangkapan alur dan pengumpulan ke dalam satu catatan log alur.
5. Untuk Tujuan, pilih Kirim ke bucket Amazon S3.
6. Untuk ARN bucket S3, tentukan Amazon Resource Name (ARN) dari bucket Amazon S3 yang ada. Anda dapat secara opsional menyertakan subfolder. Misalnya, untuk menentukan subfolder bernama `my-logs` dalam sebuah bucket bernama `my-bucket`, gunakan ARN berikut:

   ```
   arn:aws:s3:::my-bucket/my-logs/
   ```

   Bucket tidak dapat menggunakan `AWSLogs` sebagai nama subfolder, karena ini adalah istilah yang dicadangkan.

   Jika Anda memiliki bucket, kami secara otomatis membuat kebijakan sumber daya dan melampirkannya ke bucket. Untuk informasi selengkapnya, lihat Izin bucket Amazon S3 untuk log alur.
7. Untuk Format catatan log, tentukan format untuk catatan log alur.
   - Untuk menggunakan format catatan log alur default, pilih format default AWS .

- Untuk membuat format kustom, pilih Format kustom. Untuk Format log, pilih bidang untuk disertakan dalam catatan log alur.

8. Untuk Metadata tambahan, pilih apakah Anda ingin menyertakan metadata dari Amazon ECS dalam format log.
9. Untuk Format file log, tentukan format untuk file log.

   - Teks — Teks biasa. Ini adalah format default.
   - Parket — Apache Parquet adalah format data kolumnar. Kueri pada data dalam format Parquet 10 hingga 100 kali lebih cepat dibandingkan dengan kueri pada data dalam teks biasa. Data dalam format Parquet dengan kompresi Gzip membutuhkan ruang penyimpanan 20 persen lebih sedikit daripada teks biasa dengan kompresi Gzip.

10. (Opsional) Untuk menggunakan prefiks Hive-compatible S3, pilih Hive-compatible S3 awalan, Akti fkan.
11. (Opsional) Untuk mempartisi log alur Anda per jam, pilih Setiap 1 jam (60 menit).
12. (Opsional) Untuk menambahkan tag ke log alur, pilih Tambahkan tag baru dan tentukan kunci tag dan nilai.
13. Pilih Buat log alur.

Untuk membuat log alur yang diterbitkan ke Amazon S3 menggunakan baris perintah

Gunakan salah satu perintah berikut:

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

AWS CLI Contoh berikut membuat log alur yang menangkap semua lalu lintas untuk VPC yang ditentukan dan mengirimkan log alur ke bucket Amazon S3 yang ditentukan. Parameter `--log-format` menentukan format kustom untuk catatan log alur.

```
aws ec2 create-flow-logs --resource-type VPC --resource-ids vpc-00112233344556677 --
traffic-type ALL --log-destination-type s3 --log-destination arn:aws:s3:::flow-log-
bucket/custom-flow-logs/ --log-format '${version} ${vpc-id} ${subnet-id} ${instance-
id} ${srcaddr} ${dstaddr} ${srcport} ${dstport} ${protocol} ${tcp-flags} ${type} ${pkt-
srcaddr} ${pkt-dstaddr}'
```

Lihat catatan log alur dengan Amazon S3

Anda dapat melihat catatan log alur menggunakan konsol Amazon S3. Setelah Anda membuat log alur, mungkin perlu beberapa menit agar log tersebut terlihat di konsol.

Berkas log dikompresi. Jika Anda membuka berkas log menggunakan konsol Amazon S3, berkas log akan didekompresi dan catatan log alur ditampilkan. Jika Anda mengunduh berkas, Anda harus mendekompresi mereka untuk melihat catatan log alur.

Untuk melihat catatan log alur yang diterbitkan ke Amazon S3

1. Buka konsol Amazon S3 di https://console.aws.amazon.com/s3/.
2. Pilih nama bucket untuk membuka halaman detailnya.
3. Arahkan ke folder dengan file log. Misalnya, *prefix* /awsLogs// vpcflowlogs///*account_id*/*region*/*year*/*month*/*day*
4. Pilih kotak centang di sebelah nama file, lalu pilih Unduh.

Anda juga dapat meminta catatan log alur dalam berkas log menggunakan Amazon Athena. Amazon Athena adalah layanan kueri interaktif yang memudahkan analisa data di Amazon S3 menggunakan SQL standar. Untuk informasi lebih lanjut, lihat Meminta Log Alur Amazon VPC dalam Panduan Pengguna Amazon Athena.

Publikasikan log alur ke Amazon Data Firehose

Log aliran dapat mempublikasikan data log aliran langsung ke Amazon Data Firehose. Amazon Data Firehose adalah layanan yang dikelola sepenuhnya yang mengumpulkan, mengubah, dan mengirimkan aliran data real-time ke berbagai penyimpanan AWS data dan layanan analitik. Ini menangani penyerapan data atas nama Anda.

Ketika datang ke log aliran VPC, Firehose dapat berguna. Log aliran VPC menangkap informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan di VPC Anda. Data ini sangat penting untuk pemantauan keamanan, analisis kinerja, dan kepatuhan terhadap peraturan. Namun, mengelola penyimpanan dan pemrosesan aliran data log yang berkelanjutan ini dapat menjadi tugas yang kompleks dan padat sumber daya.

Dengan mengintegrasikan Firehose dengan log aliran VPC Anda, Anda dapat mengirimkan data ini ke tujuan pilihan Anda, seperti Amazon S3 atau Amazon Redshift. Firehose akan menskalakan untuk menangani konsumsi, transformasi, dan pengiriman log aliran VPC Anda, membebaskan Anda

dari beban operasional. Ini memungkinkan Anda untuk fokus menganalisis log dan memperoleh wawasan, daripada mengkhawatirkan infrastruktur yang mendasarinya.

Selain itu, Firehose menawarkan fitur seperti transformasi data, kompresi, dan enkripsi, yang dapat meningkatkan efisiensi dan keamanan pipa pemrosesan log aliran VPC Anda. Menggunakan Firehose untuk log aliran VPC dapat menyederhanakan manajemen data Anda dan memungkinkan Anda memperoleh wawasan dari data lalu lintas jaringan Anda.

Saat menerbitkan ke Amazon Data Firehose, data log aliran dipublikasikan ke aliran pengiriman Amazon Data Firehose, dalam format teks biasa.

Harga

Biaya konsumsi dan pengiriman standar berlaku. Untuk informasi selengkapnya, buka CloudWatch Harga Amazon, pilih Log dan temukan Log yang Dijual.

Daftar Isi

- Peran IAM untuk pengiriman lintas akun
- Buat log alur yang diterbitkan ke Amazon Data Firehose

Peran IAM untuk pengiriman lintas akun

Saat memublikasikan ke Amazon Data Firehose, Anda dapat memilih aliran pengiriman yang ada di akun yang sama dengan sumber daya yang akan dipantau (akun sumber), atau di akun yang berbeda (akun tujuan). Untuk mengaktifkan pengiriman log alur lintas akun ke Amazon Data Firehose, Anda harus membuat peran IAM di akun sumber dan peran IAM di akun tujuan.

Peran

- Peran akun sumber
- Peran akun tujuan

Peran akun sumber

Di akun sumber, buat peran yang memberikan izin berikut. Dalam contoh ini, nama peran adalah`mySourceRole`, tetapi Anda dapat memilih nama yang berbeda untuk peran ini. Pernyataan terakhir memungkinkan peran dalam akun tujuan untuk mengambil peran ini. Pernyataan kondisi memastikan bahwa peran ini hanya diteruskan ke layanan pengiriman log, dan hanya saat memantau

sumber daya yang ditentukan. Saat membuat kebijakan, tentukan VPC, antarmuka jaringan, atau subnet yang Anda pantau dengan kunci kondisi. `iam:AssociatedResourceARN`

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::123456789012:role/mySourceRole",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "delivery.logs.amazonaws.com"
                },
                "StringLike": {
                    "iam:AssociatedResourceARN": [
                        "arn:aws:ec2:us-
east-1:123456789012:vpc/vpc-00112233344556677"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:ListLogDeliveries",
                "logs:GetLogDelivery"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::111122223333:role/
AWSLogDeliveryFirehoseCrossAccountRole"
        }
    ]
}
```

Pastikan peran ini memiliki kebijakan kepercayaan berikut, yang memungkinkan layanan pengiriman log untuk mengambil peran tersebut.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Dari akun sumber, gunakan prosedur berikut untuk membuat peran.

Untuk membuat peran akun sumber

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Kebijakan.
3. Pilih Buat kebijakan.
4. Pada halaman Buat kebijakan, lakukan hal berikut:
   a. PilihJSON.
   b. Ganti isi jendela ini dengan kebijakan izin di awal bagian ini.
   c. Pilih Berikutnya.
   d. Masukkan nama untuk kebijakan Anda dan deskripsi dan tag opsional, lalu pilih Buat kebijakan.
5. Di panel navigasi, pilih Peran.
6. Pilih Buat peran.
7. Untuk Ti pe entitas tepercaya, pilih Kebijakan kepercayaan kustom. Untuk kebijakan kepercayaan kustom, ganti `"Principal": {},` dengan yang berikut, yang menentukan layanan pengiriman log. Pilih Berikutnya.

```
"Principal": {
   "Service": "delivery.logs.amazonaws.com"
},
```

8. Pada halaman Tambah izin, pilih kotak centang untuk kebijakan yang Anda buat sebelumnya dalam prosedur ini, lalu pilih Ber ikutnya.
9. Masukkan nama untuk peran Anda dan berikan deskripsi secara opsional.
10. Pilih Buat peran.

Peran akun tujuan

Di akun tujuan, buat peran dengan nama yang dimulai dengan AWSLogDeliveryFirehoseCrossAccountRole. Peran ini harus memberikan izin berikut.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
          "iam:CreateServiceLinkedRole",
          "firehose:TagDeliveryStream"
      ],
      "Resource": "*"
    }
  ]
}
```

Pastikan peran ini memiliki kebijakan kepercayaan berikut, yang memungkinkan peran yang Anda buat di akun sumber untuk mengambil peran ini.

JSON

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/mySourceRole"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Dari akun tujuan, gunakan prosedur berikut untuk membuat peran.

Untuk membuat peran akun tujuan

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Kebijakan.
3. Pilih Buat kebijakan.
4. Pada halaman Buat kebijakan, lakukan hal berikut:
   a. PilihJSON.
   b. Ganti isi jendela ini dengan kebijakan izin di awal bagian ini.
   c. Pilih Berikutnya.
   d. Masukkan nama untuk kebijakan Anda yang dimulai dengan AWSLogDeliveryFirehoseCrossAccountRole, lalu pilih Buat kebijakan.
5. Di panel navigasi, pilih Peran.
6. Pilih Buat peran.
7. Untuk Ti pe entitas tepercaya, pilih Kebijakan kepercayaan kustom. Untuk kebijakan kepercayaan kustom, ganti `"Principal": {},` dengan yang berikut, yang menentukan peran akun sumber. Pilih Berikutnya.

```
"Principal": {
   "AWS": "arn:aws:iam::source-account:role/mySourceRole"
},
```

8. Pada halaman Tambah izin, pilih kotak centang untuk kebijakan yang Anda buat sebelumnya dalam prosedur ini, lalu pilih Ber ikutnya.

9. Masukkan nama untuk peran Anda dan berikan deskripsi secara opsional.
10. Pilih Buat peran.

Buat log alur yang diterbitkan ke Amazon Data Firehose

Anda dapat membuat log alur untuk VPC, subnet, atau antarmuka jaringan.

Prasyarat

- Buat aliran pengiriman Amazon Data Firehose tujuan. Gunakan Direct Put sebagai sumbernya. Untuk informasi selengkapnya, lihat Membuat aliran pengiriman Amazon Data Firehose.
- Akun yang membuat log alur harus menggunakan peran IAM yang memberikan izin berikut untuk menerbitkan log alur ke Amazon Data Firehose.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery",
                "iam:CreateServiceLinkedRole",
                "firehose:TagDeliveryStream"
            ],
            "Resource": "*"
        }
    ]
}
```

- Jika Anda menerbitkan log alur ke akun lain, buat peran IAM yang diperlukan, seperti yang dijelaskan dalamthe section called “Peran IAM untuk pengiriman lintas akun”.

Untuk membuat log alur yang diterbitkan ke Amazon Data Firehose

1. Lakukan salah satu tindakan berikut:
   - Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/. Di panel navigasi, pilih Antarmuka Jaringan. Pilih kotak centang untuk antarmuka jaringan.

- Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Pada panel navigasi, pilih VPC Anda. Pilih kotak centang untuk VPC.
- Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Di panel navigasi, pilih Pengguna. Pilih kotak centang untuk subnet.

2. Pilih T ind akan, Buat log alur.
3. Untuk Filter, tentukan jenis lalu lintas ke log.
   - Terima — Log hanya lalu lintas yang diterima
   - Tolak — Catat hanya lalu lintas yang ditolak
   - Semua — Log lalu lintas diterima dan ditolak
4. Untuk Interval agregasi maksimum, pilih periode waktu maksimum selama aliran ditangkap dan dikumpulkan ke dalam satu catatan log alur.
5. Untuk Tujuan, pilih salah satu opsi berikut:
   - Kirim ke Amazon Data Firehose di akun yang sama — Aliran pengiriman dan sumber daya yang akan dipantau berada di akun yang sama.
   - Kirim ke Amazon Data Firehose di akun yang berbeda — Aliran pengiriman dan sumber daya untuk dipantau ada di akun yang berbeda.
6. Untuk nama aliran Amazon Data Firehose, pilih aliran pengiriman yang Anda buat.
7. [Hanya pengiriman lintas akun] Untuk akses Layanan, pilih peran layanan IAM yang ada untuk pengiriman lintas akun yang memiliki izin untuk menerbitkan log. Atau, pilih Atur izin untuk membuka konsol IAM dan membuat peran layanan.
8. Untuk Format catatan log, tentukan format untuk catatan log alur.
   - Untuk menggunakan format catatan log alur default, pilih format default AWS .
   - Untuk membuat format kustom, pilih Format kustom. Untuk Format log, pilih bidang untuk disertakan dalam catatan log alur.
9. Untuk Metadata tambahan, pilih apakah Anda ingin menyertakan metadata dari Amazon ECS dalam format log.
10. (Opsional) Pilih Tambah tag untuk menerapkan tag ke log alur.
11. Pilih Buat log alur.

Untuk membuat log alur yang diterbitkan ke Amazon Data Firehose menggunakan baris perintah

Gunakan salah satu perintah berikut:

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

AWS CLI Contoh berikut membuat log alur yang menangkap semua lalu lintas untuk VPC yang ditentukan dan mengirimkan log alur ke aliran pengiriman Amazon Data Firehose yang ditentukan di akun yang sama.

```
aws ec2 create-flow-logs --traffic-type ALL \
  --resource-type VPC \
  --resource-ids vpc-00112233344556677 \
  --log-destination-type kinesis-data-firehose \
  --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream/flowlogs_stream
```

AWS CLI Contoh berikut membuat log alur yang menangkap semua lalu lintas untuk VPC tertentu dan mengirimkan log alur ke aliran pengiriman Amazon Data Firehose yang ditentukan di akun yang berbeda.

```
aws ec2 create-flow-logs --traffic-type ALL \
  --resource-type VPC \
  --resource-ids vpc-00112233344556677 \
  --log-destination-type kinesis-data-firehose \
  --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream/flowlogs_stream \
  --deliver-logs-permission-arn arn:aws:iam::source-account:role/mySourceRole \
  --deliver-cross-account-role arn:aws:iam::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole
```

Sebagai hasil dari pembuatan log alur, Anda bisa mendapatkan data log alur dari tujuan yang Anda konfigurasi untuk aliran pengiriman.

Log alur kueri menggunakan Amazon Athena

Amazon Athena adalah layanan kueri interaktif yang memungkinkan Anda menganalisis data di Amazon S3 seperti log alur Anda menggunakan SQL standar. Anda dapat menggunakan Athena

dengan log alur VPC untuk dengan cepat mendapatkan wawasan yang dapat ditindaklanjuti terkait lalu lintas yang melalui VPC Anda. Misalnya, Anda dapat mengidentifikasi sumber daya mana di virtual private cloud (VPC) yang merupakan pembicara teratas atau mengidentifikasi alamat IP dengan koneksi TCP yang paling sering ditolak.

Opsi

- Anda dapat merampingkan dan mengotomatiskan integrasi log aliran VPC Anda dengan Athena. Buat CloudFormation template yang membuat AWS sumber daya yang diperlukan dan kueri yang telah ditentukan untuk mendapatkan wawasan tentang lalu lintas yang mengalir melalui VPC Anda.
- Anda dapat membuat kueri Anda sendiri menggunakan Athena. Untuk informasi selengkapnya, lihat Log alur kueri menggunakan Amazon Athena di Panduan Pengguna Amazon Athena.

Harga

Anda dikenai Biaya Amazon Athena standar untuk menjalankan kueri. Anda dikenai Biaya AWS Lambda standar untuk fungsi Lambda yang memuat partisi baru pada jadwal berulang (ketika Anda menentukan frekuensi beban partisi tetapi tidak menentukan tanggal mulai dan akhir.)

Untuk menggunakan kueri yang telah ditentukan

- Hasilkan CloudFormation template menggunakan konsol
- Buat CloudFormation template menggunakan AWS CLI
- Menjalankan kueri yang sudah ditentukan sebelumnya

Hasilkan CloudFormation template menggunakan konsol

Setelah log aliran pertama dikirimkan ke bucket S3 Anda, Anda dapat mengintegrasikan dengan Athena dengan membuat CloudFormation template dan menggunakan template untuk membuat tumpukan.

Persyaratan

- Wilayah yang dipilih harus mendukung AWS Lambda dan Amazon Athena.
- Bucket Amazon S3 harus berada di Wilayah yang dipilih.
- Format catatan log untuk log alur harus menyertakan bidang yang digunakan oleh kueri standar tertentu yang ingin Anda jalankan.

Untuk menghasilkan templat menggunakan konsol

1. Lakukan salah satu tindakan berikut:
   - Buka konsol Amazon VPC. Di panel navigasi, pilih VPC Anda dan kemudian pilih VPC Anda.
   - Buka konsol Amazon VPC. Di panel navigasi, pilih Subnet, lalu pilih subnet Anda.
   - Buka konsol Amazon EC2. Di panel navigasi, pilih Antarmuka Jaringan, lalu pilih antarmuka jaringan Anda.
2. Pada tab Log Alur, pilih log alur yang menerbitkan ke Amazon S3 dan kemudian pilih Tindakan, Hasilkan Integrasi Athena.
3. Tentukan frekuensi beban partisi. Jika Anda memilih Tidak ada, Anda harus menentukan tanggal mulai dan akhir partisi, menggunakan tanggal yang ada di masa lalu. Jika Anda memilih Harian, Mingguan, atau Bulanan, tanggal mulai dan akhir partisi bersifat opsional. Jika Anda tidak menentukan tanggal mulai dan akhir, CloudFormation template membuat fungsi Lambda yang memuat partisi baru pada jadwal berulang.
4. Pilih atau buat bucket S3 untuk templat yang dihasilkan, dan bucket S3 untuk hasil kueri.
5. Pilih Hasilkan Integrasi Athena.
6. (Opsional) Dalam pesan sukses, pilih tautan untuk menavigasi ke bucket yang Anda tentukan untuk CloudFormation template, dan sesuaikan templat.
7. Dalam pesan sukses, pilih Buat CloudFormation tumpukan untuk membuka wizard Create Stack di CloudFormation konsol. URL untuk CloudFormation template yang dihasilkan ditentukan di bagian Template. Menyelesaikan wizard untuk membuat sumber daya yang ditentukan dalam templat.

Sumber daya yang dibuat oleh CloudFormation template

- Database Athena. Nama basis data adalah vpcflowlogsathenadatabase<flow-logs-subscription-id>.
- Athena workgroup. Nama workgroup adalah <flow-log-subscription-id><partition-load-frequency><start-date><end-date>workgroup
- Sebuah tabel Athena dipartisi yang sesuai dengan catatan log alur Anda. Nama tabel adalah <flow-log-subscription-id><partition-load-frequency><start-date><end-date>.
- Satu set Athena bernama kueri. Untuk informasi selengkapnya, lihat Kueri yang ditentukan sebelumnya.
- Fungsi Lambda yang memuat partisi baru ke tabel pada jadwal yang ditentukan (harian, mingguan, atau bulanan).

- IAM role yang memberikan izin untuk menjalankan fungsi Lambda.

Buat CloudFormation template menggunakan AWS CLI

Setelah log aliran pertama dikirim ke bucket S3 Anda, Anda dapat membuat dan menggunakan CloudFormation template untuk diintegrasikan dengan Athena.

Gunakan perintah get-flow-logs-integration-template berikut untuk menghasilkan template. CloudFormation

```
aws ec2 get-flow-logs-integration-template --cli-input-json file://config.json
```

Berikut ini adalah contoh file `config.json`.

```
{
    "FlowLogId": "fl-12345678901234567",
    "ConfigDeliveryS3DestinationArn": "arn:aws:s3:::my-flow-logs-athena-integration/
templates/",
    "IntegrateServices": {
        "AthenaIntegrations": [
            {
                "IntegrationResultS3DestinationArn": "arn:aws:s3:::my-flow-logs-
analysis/athena-query-results/",
                "PartitionLoadFrequency": "monthly",
                "PartitionStartDate": "2021-01-01T00:00:00",
                "PartitionEndDate": "2021-12-31T00:00:00"
            }
        ]
    }
}
```

Gunakan perintah create-stack berikut untuk membuat tumpukan menggunakan template yang dihasilkan CloudFormation .

```
aws cloudformation create-stack --stack-name my-vpc-flow-logs --template-body file://
my-cloudformation-template.json
```

Menjalankan kueri yang sudah ditentukan sebelumnya

CloudFormation Template yang dihasilkan menyediakan serangkaian kueri yang telah ditentukan sebelumnya yang dapat Anda jalankan untuk mendapatkan wawasan yang berarti tentang lalu lintas

di AWS jaringan Anda dengan cepat. Setelah Anda membuat tumpukan dan memverifikasi bahwa semua sumber daya dibuat dengan benar, Anda dapat menjalankan salah satu kueri yang telah ditetapkan.

Untuk menjalankan kueri yang telah ditetapkan menggunakan konsol

1. Membuka konsol Athena.
2. Di navigasi kiri, pilih Editor kueri. Di bawah Workgroup, pilih workgroup yang dibuat oleh template. CloudFormation
3. Pilih Kueri tersimpan, pilih kueri, ubah parameter sesuai kebutuhan, dan jalankan kueri. Untuk daftar kueri yang telah ditentukan sebelumnya yang tersedia, lihat Kueri yang telah ditentukan sebelumnya.
4. Di bawah Hasil kueri, lihat hasil kueri.

Kueri yang ditentukan sebelumnya

Berikut ini adalah daftar lengkap kueri bernama Athena. Kueri yang telah ditentukan sebelumnya yang disediakan saat Anda membuat template bergantung pada bidang yang merupakan bagian dari format catatan log untuk log alur. Oleh karena itu, template mungkin tidak berisi semua kueri yang telah ditentukan sebelumnya.

- VpcFlowLogsAcceptedTraffic— Koneksi TCP yang diizinkan berdasarkan grup keamanan Anda dan ACL jaringan.
- VpcFlowLogsAdminPortTraffic— 10 alamat IP teratas dengan lalu lintas terbanyak, seperti yang dicatat oleh aplikasi yang melayani permintaan di port administratif.
- VpcFlowLogsIPv4Traffic— Jumlah byte lalu lintas IPv4 yang direkam.
- VpcFlowLogsIPv6Traffic— Total byte lalu lintas IPv6 yang direkam.
- VpcFlowLogsRejectedTCPTraffic— Koneksi TCP yang ditolak berdasarkan grup keamanan atau ACL jaringan Anda.
- VpcFlowLogsRejectedTraffic— Lalu lintas yang ditolak berdasarkan grup keamanan atau ACL jaringan Anda.
- VpcFlowLogsSshRdpTraffic- Lalu lintas SSH dan RDP.
- VpcFlowLogsTopTalkers— 50 alamat IP dengan lalu lintas terbanyak yang tercatat.
- VpcFlowLogsTopTalkersPacketLevel— 50 alamat IP tingkat paket dengan lalu lintas terbanyak yang tercatat.

- VpcFlowLogsTopTalkingInstances— ID dari 50 instans dengan lalu lintas terbanyak yang tercatat.
- VpcFlowLogsTopTalkingSubnets— ID dari 50 subnet dengan lalu lintas terbanyak yang tercatat.
- VpcFlowLogsTopTCPTraffic— Semua lalu lintas TCP direkam untuk alamat IP sumber.
- VpcFlowLogsTotalBytesTransferred— 50 pasang alamat IP sumber dan tujuan dengan byte terbanyak yang direkam.
- VpcFlowLogsTotalBytesTransferredPacketLevel— 50 pasang sumber tingkat paket dan alamat IP tujuan dengan byte terbanyak yang direkam.
- VpcFlowLogsTrafficFrmSrcAddrLalu lintas yang direkam untuk alamat IP sumber tertentu.
- VpcFlowLogsTrafficToDstAddrLalu lintas yang direkam untuk alamat IP tujuan tertentu.

Identitas dan manajemen akses di Log Aliran VPC

AWS menggunakan kredentif keamanan untuk mengidentifikasi Anda dan memberi Anda akses ke AWS sumber daya Anda. Anda dapat menggunakan fitur AWS Identity and Access Management (IAM) untuk mengizinkan pengguna, layanan, dan aplikasi lain menggunakan AWS sumber daya Anda sepenuhnya atau dengan cara terbatas, tanpa membagikan kredentif keamanan Anda.

Bagian ini menjelaskan peran AWS terkait layanan yang dibuat khusus untuk Log Aliran VPC dan kebijakan terkelola yang dilampirkan ke peran terkait layanan Log Aliran VPC. Untuk informasi selengkapnya tentang peran dan kebijakan AWS IAM, lihat Persyaratan dan konsep peran di Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang manajemen identitas dan akses untuk VPC, lihat Identitas dan manajemen akses untuk Amazon VPC di Panduan Pengguna Amazon VPC.

Daftar Isi

- Menggunakan peran terkait layanan untuk Log Aliran VPC
- AWS kebijakan terkelola untuk Log Aliran VPC

Menggunakan peran terkait layanan untuk Log Aliran VPC

Log Aliran VPC menggunakan peran AWS Identity and Access Management terkait layanan (IAM). Peran terkait layanan adalah jenis peran IAM unik yang ditautkan langsung ke Log Aliran VPC. Service-linked peran telah ditentukan sebelumnya oleh Log Aliran VPC dan menyertakan semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran yang ditautkan layanan membuat pengaturan Log Aliran VPC lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Log Aliran VPC mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya Log Aliran VPC yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi sumber daya Log Aliran VPC Anda karena Anda tidak dapat menghapus izin untuk mengakses sumber daya secara tidak sengaja.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat AWS layanan yang bekerja dengan IAM dan cari layanan yang memiliki Ya di kolom peran. Service-linked Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Service-linked izin peran untuk Log Aliran VPC

Log Aliran VPC menggunakan peran terkait layanan bernama AWSServiceRoleForVPCFlowLogs — Peran terkait layanan ini memungkinkan Log Aliran VPC untuk membuat dan EventBridge mengelola Aturan Terkelola dan memanggil DescribeTag API atas nama Anda untuk secara otomatis melacak pembaruan nilai Tag EC2 yang terkait dengan sumber daya di bawah langganan Log Aliran yang menyertakan bidang tag..

Per AWSServiceRoleForVPCFlowLogs an terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `vpc-flow-logs.amazonaws.com`

Kebijakan izin peran yang dinamai AWSVPCFlowLogsServiceRolePolicy memungkinkan Log Aliran VPC menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: `autoscaling:DescribeTags` pada Grup Penskalaan Otomatis EC2 untuk memvalidasi nilai tag.

  Tindakan: `tag:GetResources` pada instans EC2 dan ElasticNetworkInterfaces untuk memvalidasi nilai tag.

  Tindakan: `events:PutRule` pada Aturan Terkelola baru dari sumber `aws.tag` dan `aws.autoscaling` untuk tipe detail yang terkait dengan peristiwa perubahan tag.

Tindakan: `events:DeleteRule` pada Aturan Terkelola yang dibuat oleh Log Aliran VPC bernama `VPCFlowLogsEC2TagsManagedRule` and/or `VPCFlowLogsASGTagsManagedRule`.

Tindakan: `events:DescribeRule` pada Aturan Terkelola yang dibuat oleh Log Aliran VPC bernama `VPCFlowLogsEC2TagsManagedRule` and/or `VPCFlowLogsASGTagsManagedRule`.

Tindakan: `events:PutTargets` pada Aturan Terkelola yang dibuat oleh Log Aliran VPC bernama `VPCFlowLogsEC2TagsManagedRule` and/or `VPCFlowLogsASGTagsManagedRule`.

Tindakan: `events:RemoveTargets` pada Aturan Terkelola yang dibuat oleh Log Aliran VPC bernama `VPCFlowLogsEC2TagsManagedRule` and/or `VPCFlowLogsASGTagsManagedRule`.

Anda harus mengonfigurasi izin untuk mengizinkan pengguna, grup, atau peran Anda membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat izin Service-linked peran di Panduan Pengguna IAM.

Membuat peran terkait layanan untuk Log Aliran VPC

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda CreateFlowLogs menggunakan bidang tag dalam format log dan TagFieldSpecifications parameter terkait di Konsol Manajemen AWS,, atau AWS API AWS CLI, Log Aliran VPC membuat peran terkait layanan untuk Anda.

> **Important**
>
> Peran tertaut layanan ini dapat muncul di akun Anda jika Anda menyelesaikan tindakan di layanan lain yang menggunakan fitur yang disupport oleh peran ini. Untuk mempelajari lebih lanjut, lihat Peran baru muncul di saya Akun AWS.

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda CreateFlowLogs menggunakan bidang tag dalam format log dan TagFieldSpecifications parameter terkait, Log Aliran VPC membuat peran terkait layanan untuk Anda lagi.

Anda juga dapat menggunakan konsol IAM untuk membuat peran terkait layanan dengan kasus penggunaan. AWSServiceRoleForVPCFlowLogs Di AWS API AWS CLI atau, buat peran terkait layanan dengan nama `vpc-flow-logs.amazonaws.com` layanan. Untuk informasi selengkapnya,

lihat Membuat peran tertaut layanan dalam Panduan Pengguna IAM. Jika Anda menghapus peran tertaut layanan ini, Anda dapat mengulang proses yang sama untuk membuat peran tersebut lagi.

Mengedit peran terkait layanan untuk Log Aliran VPC

Log Aliran VPC tidak mengizinkan Anda mengedit peran terkait AWSServiceRoleForVPCFlowLogs layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin merujuk peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran terkait layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Log Aliran VPC

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami merekomendasikan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Tetapi, Anda harus membersihkan sumber daya peran terkait layanan sebelum menghapusnya secara manual.

> **Note**
>
> Jika layanan Log Aliran VPC menggunakan peran saat Anda mencoba menghapus sumber daya, penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus sumber daya VPC Flow Logs yang digunakan oleh AWSServiceRoleForVPCFlowLogs

1. Hapus semua langganan VPC Flow Logs yang menggunakan bidang tag dalam format log.
2. Tunggu setidaknya satu jam hingga Log Aliran VPC memproses bahwa semua langganan tag untuk akun Anda telah dihapus dan secara otomatis membersihkan Aturan Terkel EventBridge ola yang dibuat untuk mendukung pengayaan log.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, AWS CLI, atau AWS API untuk menghapus peran terkait AWSServiceRoleForVPCFlowLogs layanan. Untuk informasi selengkapnya, lihat Menghapus peran terkait layanan dalam Panduan Pengguna IAM.

Wilayah yang Didukung untuk peran terkait layanan Log Aliran VPC

Log Aliran VPC tidak mendukung penggunaan peran terkait layanan di setiap Wilayah tempat layanan tersedia. Anda dapat menggunakan AWSServiceRoleForVPCFlowLogs peran di Wilayah berikut.

Nama wilayah	Identitas wilayah	Dukungan dalam Log Aliran VPC
US East (Northern Virginia)	us-east-1	Ya
US East (Ohio)	us-east-2	Ya
US West (N. California)	us-west-1	Ya
US West (Oregon)	us-west-2	Ya
Africa (Cape Town)	af-south-1	Ya
Asia Pasifik (Hong Kong)	ap-east-1	Ya
Asia Pasifik (Jakarta)	ap-southeast-3	Ya
Asia Pacific (Mumbai)	ap-south-1	Ya
Asia Pacific (Osaka)	ap-northeast-3	Ya
Asia Pacific (Seoul)	ap-northeast-2	Ya
Asia Pacific (Singapore)	ap-southeast-1	Ya
Asia Pacific (Sydney)	ap-southeast-2	Ya
Asia Pacific (Tokyo)	ap-northeast-1	Ya
Canada (Central)	ca-sentral-1	Ya
Eropa (Frankfurt)	eu-central-1	Ya
Eropa (Irlandia)	eu-west-1	Ya
Eropa (London)	eu-west-2	Ya

Nama wilayah	Identitas wilayah	Dukungan dalam Log Aliran VPC
Europe (Milan)	eu-south-1	Ya
Europe (Paris)	eu-west-3	Ya
Eropa (Stockholm)	eu-north-1	Ya
Timur Tengah (Bahrain)	me-south-1	Ya
Timur Tengah (UAE)	me-central-1	Ya
South America (São Paulo)	sa-east-1	Ya
AWS GovCloud (US-East)	us-gov-east-1	Ya
AWS GovCloud (US-West)	us-gov-west-1	Ya

AWS kebijakan terkelola untuk Log Aliran VPC

Jika Anda menggunakan Log Aliran VPC dan membuat langganan dengan bidang tag dan TagFieldSpecifications parameter terkait, kebijakan AWSVPCFlowLogsServiceRolePolicyterkelola secara otomatis dibuat di akun IAM Anda dan dilampirkan ke peran terkait layanan. AWSServiceRoleForVPCFlowLogs

Kebijakan terkelola ini memungkinkan Log Aliran VPC melakukan hal berikut:

- Buat dan EventBridge kelola Aturan Terkelola untuk mengirim peristiwa pembaruan tag ke layanan VPC Flow Logs.
- Panggil API atas nama pelanggan untuk memvalidasi kesegaran nilai tag untuk pengayaan log.

Contoh berikut menunjukkan detail kebijakan terkelola yang dibuat.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "AllowPutRuleOnSpecificSourcesAndDetailTypes",
            "Effect": "Allow",
            "Action": "events:PutRule",
            "Resource": [
                "arn:aws:events:*:*:rule/VPCFlowLogsEC2TagsManagedRule",
                "arn:aws:events:*:*:rule/VPCFlowLogsASGTagsManagedRule"
            ],
            "Condition": {
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.tag",
                        "aws.autoscaling"
                    ],
                    "events:detail-type": [
                        "AWS API Call via CloudTrail",
                        "Tag Change on Resource"
                    ]
                },
                "Null": {
                    "events:source": "false",
                    "events:detail-type": "false"
                },
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "AllowOtherOperationsOnRulesManagedByVPCFlowLogs",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:DescribeRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": [
                "arn:aws:events:*:*:rule/VPCFlowLogsEC2TagsManagedRule",
                "arn:aws:events:*:*:rule/VPCFlowLogsASGTagsManagedRule"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
```

```
                }
            }
        },
        {
            "Sid": "AllowDescribeTagsOnAllEC2Resources",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources",
                "autoscaling:DescribeTags"
            ],
            "Resource": "*"
        }
    ]
}
```

Pernyataan pertama dalam contoh sebelumnya memungkinkan Log Aliran VPC untuk membuat Aturan EventBridge Terkelola di AWS akun Anda untuk sumber `aws.tag` dan `aws.autoscaling` untuk tipe detail yang terkait dengan peristiwa perubahan tag.

Pernyataan kedua dalam contoh sebelumnya memungkinkan Log Aliran VPC untuk mengontrol siklus hidup Aturan Terkelola yang dibuat di akun Anda untuk sumber daya bernama. AWS `VPCFlowLogsEC2TagsManagedRule` and/or `VPCFlowLogsASGTagsManagedRule`

Pernyataan ketiga dalam contoh sebelumnya memungkinkan VPC Flow Logs memanggil API tag atas nama pelanggan untuk memvalidasi kesegaran nilai tag untuk pengayaan log.

AWS kebijakan terkelola: AWSVPCFlowLogsServiceRolePolicy

Anda dapat melampirkan kebijakan `AWSVPCFlowLogsServiceRolePolicy` ke identitas IAM Anda. Kebijakan ini memberikan izin yang memungkinkan Log Aliran VPC untuk membuat dan mengelola Aturan EventBridge Terkelola dan memanggil DescribeTag API atas nama Anda untuk secara otomatis melacak pembaruan nilai Tag EC2 yang terkait dengan sumber daya di bawah langganan Log Aliran yang menyertakan bidang tag.

Untuk melihat izin kebijakan ini, lihat AWSVPCFlowLogsServiceRolePolicy di Referensi Kebijakan AWS Terkelola.

Pembaruan untuk AWS Kebijakan terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Log Aliran VPC sejak layanan ini mulai melacak perubahan ini.

Ubah	Deskripsi	Date
the section called “AWSVPCFlowLogsServiceRolePolicy ” – Kebijakan baru	AWSVPCFlowLogsServiceRolePolicy Kebijakan baru memungkinkan Log Aliran VPC untuk membuat dan mengelola Aturan EventBridge Terkelola dan memanggil DescribeTag API atas nama Anda untuk secara otomatis melacak pembaruan nilai Tag EC2 yang terkait dengan sumber daya di bawah langganan Log Aliran yang menyertakan bidang tag.	Maret 31, 2026
VPC Flow Logs mulai melacak perubahan	VPC Flow Logs mulai melacak perubahan untuk kebijakan AWS terkelolanya.	Maret 31, 2026

Mengatasi masalah Log Alur VPC

Berikut ini adalah masalah yang mungkin Anda miliki saat bekerja dengan log alur.

Masalah

- Catatan log alur tidak lengkap
- Log alur aktif, tetapi tidak ada catatan log alur atau grup log
- Kesalahan LogDestinationNotFoundException '' atau 'Akses Ditolak untuk LogDestination '
- Melebihi batas kebijakan bucket Amazon S3
- LogDestination tidak terkirim
- Ukuran data log aliran tidak sesuai dengan data penagihan

Catatan log alur tidak lengkap

Masalah

Catatan log alur Anda tidak lengkap atau tidak lagi dipublikasikan.

Penyebab

Mungkin ada masalah saat mengirimkan log alur ke grup CloudWatch log log atau SkipData entri mungkin ada.

Solusi

Periksa tab Log aliran untuk antarmuka VPC, subnet, atau jaringan. Anda tidak dapat menjelaskan log alur untuk VPC atau subnet yang dibagikan dengan Anda. Namun, Anda dapat menjelaskan log alur untuk antarmuka jaringan yang Anda buat di VPC atau subnet yang dibagikan dengan Anda. Jika ada kesalahan, mereka muncul di kolom Status. Atau, gunakan perintah describe-flow-logs, dan periksa nilai yang dikembalikan dalam bidang `DeliverLogsErrorMessage`.

Berikut ini adalah kemungkinan nilai kesalahan untuk status:

- `Rate limited`: Kesalahan ini dapat terjadi ketika jumlah catatan log aliran untuk antarmuka jaringan melebihi jumlah maksimum yang dapat dipublikasikan dalam jangka waktu tertentu. Kesalahan ini juga dapat terjadi jika Anda telah mencapai kuota untuk jumlah CloudWatch grup log log yang dapat Anda buat. Untuk informasi selengkapnya, lihat kuota CloudWatch layanan di Panduan CloudWatch Pengguna Amazon.
- `Access error`: Kesalahan ini dapat terjadi karena salah satu alasan berikut:
  - Peran IAM untuk log alur Anda tidak memiliki izin yang cukup untuk menerbitkan catatan log alur ke grup CloudWatch log
  - IAM role tidak memiliki hubungan kepercayaan dengan layanan log alur
  - Hubungan kepercayaan tidak menentukan layanan log alur sebagai prinsipal

  Untuk informasi selengkapnya, lihat Peran IAM untuk menerbitkan log alur ke Log CloudWatch.
- `Unknown error`: Terjadi kesalahan internal dalam layanan log alur.

Log alur aktif, tetapi tidak ada catatan log alur atau grup log

Masalah

Anda membuat log alur, dan konsol Amazon VPC atau Amazon EC2 menampilkan log alur sebagai. `Active` Namun, Anda tidak dapat melihat aliran log apa pun di CloudWatch Log atau file log di bucket Amazon S3 Anda.

Kemungkinan penyebab

- Log alur masih dibuat. Dalam beberapa kasus, diperlukan waktu 10 menit atau lebih setelah Anda membuat log alur untuk grup log yang akan dibuat, dan agar data ditampilkan.
- Belum ada lalu lintas yang dicatat untuk antarmuka jaringan Anda. Grup log di CloudWatch Log hanya dibuat ketika lalu lintas direkam.

Solusi

Tunggu beberapa menit untuk membuat grup log, atau mencatat lalu lintas.

Kesalahan LogDestinationNotFoundException '' atau 'Akses Ditolak untuk LogDestination '

Masalah

Anda mendapatkan `LogDestinationNotFoundException` kesalahan `Access Denied for LogDestination` atau kesalahan saat membuat log alur.

Kemungkinan penyebab

- Saat membuat log alur yang menerbitkan data ke bucket Amazon S3, kesalahan ini menunjukkan bahwa bucket S3 yang ditentukan tidak dapat ditemukan. Ini juga dapat berarti bahwa kebijakan bucket tidak mengizinkan log dikirim ke bucket.
- Saat membuat log alur yang menerbitkan data ke Amazon CloudWatch Logs, kesalahan ini menunjukkan bahwa peran IAM tidak mengizinkan log dikirimkan ke grup log.

Solusi

- Saat menerbitkan ke Amazon S3, pastikan bahwa Anda telah menentukan ARN untuk bucket S3 yang ada, dan ARN dalam format yang benar. Jika Anda tidak memiliki bucket S3, verifikasi bahwa kebijakan bucket memiliki izin yang diperlukan dan menggunakan ID akun dan nama bucket yang benar di ARN.
- Saat menerbitkan ke CloudWatch Log, verifikasi bahwa peran IAM memiliki izin yang diperlukan.

Melebihi batas kebijakan bucket Amazon S3

Masalah

Anda mendapatkan kesalahan berikut ketika Anda mencoba untuk membuat log alur: `LogDestinationPermissionIssueException`.

Kemungkinan penyebab

Kebijakan bucket Amazon S3 dibatasi hingga ukuran 20 KB.

Setiap kali Anda membuat log alur yang menerbitkan ke Amazon S3 bucket, kita secara otomatis menambahkan ARN bucket tertentu, yang mencakup jalur folder, untuk unsur `Resource` dalam kebijakan bucket ini.

Membuat beberapa log alur yang menerbitkan ke bucket yang sama dapat menyebabkan Anda melebihi batas kebijakan bucket.

Solusi

- Bersihkan kebijakan bucket dengan menghapus entri log alur yang tidak lagi diperlukan.
- Memberikan izin untuk seluruh bucket dengan mengganti entri log alur individu dengan berikut ini.

  ```
  arn:aws:s3:::bucket_name/*
  ```

  Jika Anda memberikan izin untuk seluruh bucket, langganan log alur baru tidak menambahkan izin baru untuk bucket kebijakan.

LogDestination tidak terkirim

Masalah

Anda mendapatkan kesalahan berikut ketika Anda mencoba untuk membuat log alur: `LogDestination <bucket name> is undeliverable`.

Kemungkinan penyebab

Bucket Amazon S3 target dienkripsi menggunakan enkripsi sisi server dengan AWS KMS (SSE-KMS) dan enkripsi default bucket adalah ID kunci KMS.

Solusi

Nilai harus berupa kunci KMS ARN. Ubah tipe enkripsi S3 default dari ID kunci KMS menjadi kunci KMS ARN. Untuk informasi selengkapnya, lihat Meng onfigurasi enkripsi default di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Ukuran data log aliran tidak sesuai dengan data penagihan

Masalah

Ukuran data total log alur Anda tidak sesuai dengan ukuran yang dilaporkan oleh data penagihan.

Kemungkinan penyebab

Mungkin ada entri SKIPDATA di log alur Anda. Lihat Tidak ada data dan catatan yang dilewati untuk penjelasan entri SKIPDATA.

Solusi

Konfirmasikan bahwa entri SKIPDATA ada di entri log Anda dengan menanyakan log Anda untuk entri yang berbeda di bidang log-status.

Contoh kueri untuk memeriksa SKIPDATA:

Wawasan CW:

```
fields @timestamp, @message, @logStream, @log
| filter interfaceId = 'eni-123'
| stats count(*) by interfaceId, logStatus
| sort by interfaceId, logStatus
```

Athena:

```
SELECT log_status, interface_id, count(1)
FROM vpc_flow_logs
WHERE interface_id IN ('eni-1', 'eni-2', 'eni-3')
GROUP BY log_status, interface_id
```

CloudWatch metrik untuk Anda VPCs

Amazon VPC menerbitkan data tentang Anda ke VPCs Amazon. CloudWatch Anda dapat mengambil statistik tentang Anda VPCs sebagai kumpulan data deret waktu yang diurutkan, yang dikenal sebagai metrik. Pikirkan metrik sebagai variabel untuk dipantau dan data sebagai nilai variabel itu dari waktu ke waktu. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

Daftar Isi

- Metrik dan dimensi NAU
- Mengaktifkan atau menonaktifkan pemantauan NAU
- Contoh CloudWatch alarm NAU

Metrik dan dimensi NAU

Penggunaan Alamat Jaringan(NAU) adalah metrik yang diterapkan pada sumber daya di jaringan virtual Anda untuk membantu Anda merencanakan dan memantau ukuran VPC Anda. Tidak ada biaya untuk memantau NAU. Memantau NAU sangat membantu karena jika Anda menghabiskan NAU atau kuota NAU peered untuk VPC Anda, Anda tidak dapat meluncurkan instance EC2 baru atau menyediakan sumber daya baru, seperti Network Load Balancers, titik akhir VPC, fungsi Lambda, lampiran gateway transit, dan gateway NAT.

Jika Anda telah mengaktifkan pemantauan Penggunaan Alamat Jaringan untuk VPC, Amazon VPC mengirimkan metrik yang terkait dengan NAU ke Amazon. CloudWatch Ukuran VPC diukur dengan jumlah unit Network Address Usage (NAU) yang terkandung dalam VPC.

Anda dapat menggunakan metrik ini untuk memahami tingkat pertumbuhan VPC Anda, memperkirakan kapan VPC Anda akan mencapai batas ukurannya, atau membuat alarm saat ambang batas ukuran dilintasi.

`AWS/EC2`Namespace menyertakan metrik berikut untuk memantau NAU.

Metrik	Deskripsi
`NetworkAddressUsage`	Hitungan NAU per VPC. Kriteria pelaporan • Setiap 24 jam. Dimensi • Nama:`Per-VPC Metrics`, Nilai: ID VPC.
`NetworkAddressUsagePeered`	Jumlah NAU untuk VPC dan VPCs semua yang diintip. Kriteria pelaporan

Metrik	Deskripsi
	• Setiap 24 jam. Dimensi • Nama:`Per-VPC Metrics`, Nilai: ID VPC.

`AWS/Usage`Namespace menyertakan metrik berikut untuk memantau NAU.

Metrik	Deskripsi
`ResourceCount`	Hitungan NAU per VPC. Kriteria pelaporan • Setiap 24 jam. Dimensi • Nama:`Service`, Nilai: `EC2` • Nama:`Type`, Nilai: `Resource` • Nama:`Resource`, Nilai: ID VPC. • Nama:`Class`, Nilai: `NetworkAddressUsage`
`ResourceCount`	Jumlah NAU untuk VPC dan VPCs semua yang diintip. Kriteria pelaporan • Setiap 24 jam. Dimensi • Nama:`Service`, Nilai: `EC2` • Nama:`Type`, Nilai: `Resource`

Metrik	Deskripsi
	• Nama:`Resource`, Nilai: ID VPC. • Nama:`Class`, Nilai: `NetworkAddressUsagePeered`
`ResourceCount`	Tampilan gabungan penggunaan NAU di seluruh VPCs. Kriteria pelaporan • Setiap 24 jam. Dimensi • Nama:`Service`, Nilai: `EC2` • Nama:`Type`, Nilai: `Resource` • Nama:`Resource`, Nilai: `VPC` • Nama:`Class`, Nilai: `NetworkAddressUsage`
`ResourceCount`	Tampilan gabungan penggunaan NAU di seluruh VPCs peered. Kriteria pelaporan • Setiap 24 jam. Dimensi • Nama:`Service`, Nilai: `EC2` • Nama:`Type`, Nilai: `Resource` • Nama:`Resource`, Nilai: `VPC` • Nama:`Class`, Nilai: `NetworkAddressUsagePeered`

Mengaktifkan atau menonaktifkan pemantauan NAU

Untuk melihat metrik NAU CloudWatch, Anda harus terlebih dahulu mengaktifkan pemantauan pada setiap VPC untuk dipantau.

Untuk mengaktifkan atau menonaktifkan pemantauan NAU

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Your VPCs.
3. Pilih kotak centang untuk VPC.
4. Pilih Tindakan, Edit pengaturan VPC.
5. Lakukan salah satu tindakan berikut:
   - Untuk mengaktifkan pemantauan, pilih Setelan metrik unit pemetaan jaringan, Aktifkan metrik penggunaan alamat jaringan.
   - Untuk menonaktifkan pemantauan, hapus pengaturan metrik unit pemetaan jaringan, Aktifkan metrik penggunaan alamat jaringan.

Untuk mengaktifkan atau menonaktifkan pemantauan menggunakan baris perintah

- modify-vpc-attribute (AWS CLI)
- Edit-EC2VpcAttribute (AWS Tools for Windows PowerShell)

Contoh CloudWatch alarm NAU

Anda dapat menggunakan AWS CLI perintah dan contoh berikut `.json` untuk membuat CloudWatch alarm Amazon dan pemberitahuan SNS yang melacak pemanfaatan NAU VPC dengan 50.000 sebagai ambang batas. NAUs Contoh ini mengharuskan Anda untuk terlebih dahulu membuat topik Amazon SNS. Untuk informasi lebih lanjut, lihat Memulai dengan Amazon SNS di Panduan Developer Amazon Simple Notification Service.

```
aws cloudwatch put-metric-alarm --cli-input-json file://nau-alarm.json
```

Berikut adalah contoh `nau-alarm.json`.

```
{
```

```
    "Namespace": "AWS/EC2",
    "MetricName": "NetworkAddressUsage",
    "Dimensions": [{
        "Name": "Per-VPC Metrics",
        "Value": "vpc-0123456798"
    }],
    "AlarmActions": ["arn:aws:sns:us-west-1:123456789012:my_sns_topic"],
    "ComparisonOperator": "GreaterThanThreshold",
    "Period": 86400,
    "EvaluationPeriods": 1,
    "Threshold": 50000,
    "AlarmDescription": "Tracks NAU utilization of the VPC with 50k NAUs as the
 threshold",
    "AlarmName": "VPC NAU Utilization",
    "Statistic": "Maximum"
}
```

Memahami kode untuk Amazon VPC dalam laporan penagihan dan penggunaan

Saat Anda menggunakan Amazon VPC, kami menyertakan kode terkait dalam laporan AWS penagihan dan penggunaan Anda. Meninjau kode ini membantu Anda memahami biaya dan pola penggunaan untuk Amazon VPC. Melacak dan mengelola pengeluaran Anda sangat penting untuk mengoptimalkan biaya Anda.

Tabel berikut menjelaskan kode untuk Amazon VPC yang muncul di laporan penagihan dan penggunaan Anda. Untuk daftar kode Wilayah yang digunakan dalam laporan penagihan dan penggunaan, lihat Kode penagihan AWS wilayah.

Kode penagihan untuk:

- Manajemen alamat IP
- Titik akhir VPC
- Transit gateway
- Analisis jaringan
- Mirroring lalu lintas
- Kisi VPC
- Sumber daya lintas akun/wilayah

Sumber daya terkait

- Harga Amazon VPC
- AWS PrivateLink harga
- AWS Transit Gateway harga
- Harga Amazon VPC Lattice

Manajemen alamat IP

Kode	Deskripsi	Unit	Granularitas
region-PublicIPv4:InUseAddress	Waktu IPv4 alamat publik digunakan oleh sumber daya.	Jam	Per-detik
region-PublicIPv4:IdleAddress	Waktu dimana IPv4 alamat publik tidak digunakan oleh sumber daya.	Jam	Per-detik
region-PublicIPv4:ContiguousBlock	Penggunaan IPv4 alamat publik di blok IPv4 bersebelahan yang disediakan Amazon.	Jam	Per Jam
region-IPAddressManager-IP-Hours	Waktu alamat IP dikelola oleh IPAM Advanced Tier.	Jam	Per Jam

Titik akhir VPC

Kode	Deskripsi	Unit	Granularitas
region-VpcEndpoint-Hours	Waktu dimana titik akhir VPC antarmuka disediakan.	Jam	Per Jam
region-VpcEndpoint-Bytes	Data diproses oleh titik akhir VPC antarmuka.	GB	Per Jam
region-VpcEndpoint-GWLBE-Hours	Waktu dimana titik akhir Load Balancer Gateway disediakan.	Jam	Per Jam
region-VpcEndpoint-GWLBE-Bytes	Data diproses oleh titik akhir Load Balancer Gateway.	GB	Per Jam

Transit gateway

Kode	Deskripsi	Unit	Granularitas
region-TransitGateway-Hours	Penggunaan lampiran gateway transit.	Jam	Per Jam
region-TransitGateway-Bytes	Data diproses oleh gateway transit.	GB	Per Jam

Kode	Deskripsi	Unit	Granularitas
region-TGW-Multicast-Consumer-Bytes	Data yang diproses oleh instance penerima multicast.	GB	Per Jam

Analisis jaringan

Kode	Deskripsi	Unit	Granularitas
region-Analysis-Runs	Jumlah jalur jaringan yang dianalisis oleh Reachability Analyzer.	Hitungan	Per analisis
region-NetworkInterface-Assessment	Jumlah antarmuka jaringan yang dianalisis oleh Network Access Analyzer.	Hitungan	Per penilaian

Mirroring lalu lintas

Kode	Deskripsi	Unit	Granularitas
region-ENI-Mirror	Waktu antarmuka jaringan dikonfigurasi untuk pencerminan lalu lintas.	Jam	Per Jam

Kisi VPC

Kode	Deskripsi	Unit	Granularitas
region-VPCLattice-Service-Hourly	Waktu berjalan untuk layanan VPC Lattice.	Jam	Per Jam
region-VPCLattice-DataProcessing-Bytes	Data diproses oleh layanan VPC Lattice.	GB	Per Jam
region-VPCLattice-RequestCount-Free	Permintaan HTTP gratis dan koneksi TCP.	Hitungan	Per Jam
region-VpcLattice-Service-Network-Resource-Hours	Waktu berjalan untuk jaringan layanan VPC Lattice.	Jam	Per Jam

Sumber daya lintas akun/wilayah

Kode	Deskripsi	Unit	Granularitas
region-VpcResou	Data yang ditransfer dari sumber penyedia di seluruh akun atau Wilayah.	GB	Per Jam

Kode	Deskripsi	Unit	Granularitas
`rce-Provi der-Bytes`			
`region``- VpcResou rce-Consu mer-Bytes`	Data yang ditransfer oleh sumber daya konsumen di seluruh akun atau Wilayah.	GB	Per Jam

Jelaskan arsitektur jaringan VPC Anda

Amazon VPC memungkinkan Anda untuk mendefinisikan jaringan virtual yang terisolasi secara logis di AWS Cloud, yang dikenal sebagai virtual private cloud (VPC). Buat VPC terpisah untuk mengisolasi infrastruktur berdasarkan beban kerja atau entitas organisasi. Anda dapat mengonfigurasi VPC Anda dengan memilih rentang alamat IP, mengonfigurasi routing, dan menambahkan gateway jaringan untuk menghubungkan VPC Anda satu sama lain, internet, atau ke jaringan perusahaan Anda sendiri. Anda meluncurkan AWS sumber daya, seperti instans EC2 atau instans RDS, di VPC Anda.

Tabel berikut menjelaskan karakteristik utama jaringan VPC. Administrator jaringan dapat menggunakan panduan ini untuk menjelaskan arsitektur dan konfigurasi jaringan VPC Anda. Memiliki informasi ini memungkinkan mereka untuk mengkonfigurasi jaringan yang setara secara fungsional di tempat atau menggunakan Penyedia Cloud lain.

Karakteristik	Deskripsi
Lokasi geografis	Amazon VPC dihosting di semua Wilayah di AWS seluruh dunia. Anda dapat memilih Wilayah untuk jaringan VPC Anda yang menempatkan AWS sumber daya Anda paling dekat dengan pelanggan Anda.
Subnet	Subnet yang Anda tentukan untuk VPC menentukan batas jaringan dan menentuka n alamat IP untuk sumber daya Anda AWS .

Karakteristik	Deskripsi
	Anda dapat menambahkan subnet di beberapa Zona Ketersediaan untuk meningkatkan ketersediaan sumber daya Anda.
Konektivitas Jaringan	Gateway yang Anda lampirkan ke VPC atau subnet untuk menyediakan konektivitas antara jaringan VPC Anda dan jaringan lain, seperti VPC atau subnet lain, internet, atau jaringan lokal Anda.
Kontrol keamanan	Grup keamanan yang Anda buat untuk VPC mengontrol lalu lintas ke dan dari sumber daya terkait, seperti sumber daya komputasi, sumber daya basis data, dan penyeimbang beban. Setiap subnet memiliki ACL jaringan yang mengontrol lalu lintas masuk dan meninggalkan subnet.
Manajemen lalu lintas	Aturan routing mengontrol aliran lalu lintas antara subnet, VPC, dan lokasi eksternal. Penyeimbang beban yang disediakan oleh Elastic Load Balancing mendistribusikan lalu lintas masuk ke beberapa target, seperti instans EC2, wadah, dan fungsi Lambda.

Lokasi geografis

Amazon VPC tersedia di setiap Wilayah di AWS seluruh dunia. Setiap Wilayah adalah wilayah geografis yang terpisah. Anda dapat menurunkan latensi jaringan saat membuat VPC untuk sumber daya Anda di Wilayah yang dekat dengan sebagian besar pengguna Anda.

Anda dapat menggunakan Amazon EC2 Global View untuk membuat daftar VPC Anda di semua Wilayah menggunakan antarmuka pengguna grafis (tidak ada antarmuka terprogram yang setara). Dengan konsol Amazon VPC, AWS API, dan antarmuka baris AWS perintah, Anda harus mencantumkan sumber daya VPC dan VPC untuk setiap Wilayah secara individual.

Mengapa hal ini penting

Setelah Anda menentukan di mana VPC Anda berada, Anda dapat memutuskan apakah akan mengkonfigurasi jaringan yang setara secara fungsional di lokasi yang sama atau lokasi yang berbeda, tergantung pada kebutuhan Anda.

Untuk mendapatkan ringkasan VPC Anda di semua Wilayah

1. Buka konsol Amazon EC2 Global View di https://console.aws.amazon.com/ec2globalview/home.
2. Pada tab Penjelajah wilayah, di bawah Ring kasan, periksa jumlah sumber daya untuk VPC, yang mencakup jumlah VPC dan jumlah Wilayah. Ini termasuk VPC default yang AWS dibuat atas nama Anda dan VPC nondefault yang Anda buat. Pilih teks yang digarisbawahi untuk melihat bagaimana jumlah VPC tersebar di seluruh Wilayah. Jika suatu Wilayah hanya memiliki satu VPC, kemungkinan besar VPC default untuk Wilayah tersebut.
3. Pada tab Pencarian global, pilih filter klien Jenis sumber daya = Vpc. Anda dapat memfilter hasil lebih lanjut dengan menentukan Region atau tag.

Untuk mendapatkan VPC di Wilayah menggunakan AWS CLI

Gunakan perintah describe-vpcs berikut. Anda harus menjalankan perintah ini di setiap Wilayah tempat Anda memiliki VPC. `--query`Parameter hanya mencakup ID VPC dalam output. Anda dapat menyertakan bidang tambahan sesuai kebutuhan.

```
aws ec2 describe-vpcs \
    --region us-east-2 \
    --query "Vpcs[*].VpcId"
```

Setiap Wilayah dilengkapi dengan VPC default. Jika Anda tidak menggunakan VPC default, Anda dapat mengecualikannya dari hasil dengan menambahkan filter berikut.

```
--filters Name=is-default,Values=false
```

Subnet

Subnet adalah batas jaringan logis dalam VPC. Saat Anda membuat subnet, Anda menetapkan blok alamat IP. Sumber daya yang Anda luncurkan ke subnet diberi alamat IP dari blok alamat IP untuk subnet. Alamat IP memungkinkan sumber daya untuk berkomunikasi satu sama lain melalui jaringan lokal atau internet.

Peta sumber daya di konsol Amazon VPC menyediakan representasi visual dari subnet untuk VPC Anda.

Mengapa hal ini penting

Subnets memungkinkan administrator jaringan untuk menerapkan batas keamanan dan mengontrol lalu lintas antar tingkatan aplikasi. Dengan mencatat alamat IP subnet Anda, Anda dapat membantu memastikan bahwa sumber daya dalam jaringan yang setara secara fungsional dapat berkomunikasi dengan klien atau aplikasi yang sama dengan yang dapat mereka lakukan di jaringan VPC Anda.

Untuk melihat subnet untuk VPC menggunakan peta sumber daya

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih VPC.
3. Pilih kotak centang untuk VPC.
4. Pilih tab Peta sumber daya.
5. Di panel VPC, pilih Tampilkan rincian. Panel Subnets mencantumkan semua subnet di VPC dan menunjukkan rentang alamat IP mereka. Arahkan kursor ke subnet untuk menyorot tabel rute terkait dan koneksi jaringan. Untuk detail lebih lanjut, pilih tautan untuk membuka halaman detail subnet.

Untuk menggambarkan subnet untuk VPC menggunakan AWS CLI

Gunakan perintah describe-subnets berikut. `--filters`Parameter mencakup pencarian untuk menggambarkan subnet untuk VPC yang ditentukan. `--query`Parameter hanya mencakup bidang yang ditentukan dalam output. Anda dapat menyertakan bidang tambahan sesuai kebutuhan.

```
aws ec2 describe-subnets \
    --filters Name=vpc-id,Values=vpc-1234567890abcdef0 \
    --query Subnets[*].
[SubnetId,AvailabilityZoneId,CidrBlock,Ipv6CidrBlockAssociationSet[0].Ipv6CidrBlock] \
    --output table
```

Berikut ini adalah output contoh. Kolom adalah ID subnet, ID AZ, rentang alamat IPv4, dan rentang alamat IPv6 pertama (jika ada).

```
-------------------------------------------------------------------------------
|                                DescribeSubnets                              |
```

```
+--------------------------+-----------+----------------+--------------------------+
|  subnet-0d2d1b81e0bc9c6d4 |  usw2-az1 |  10.0.144.0/20 |  2600:1f14:1e6e:a003::/64  |
|  subnet-0e01d500780bb7468 |  usw2-az1 |  10.0.16.0/20  |  2600:1f14:1e6e:a001::/64  |
|  subnet-0eb17d85f5dfd33b1 |  usw2-az2 |  10.0.128.0/20 |  2600:1f14:1e6e:a002::/64  |
|  subnet-0e990c67809773b19 |  usw2-az2 |  10.0.0.0/20   |  2600:1f14:1e6e:a000::/64  |
+--------------------------+-----------+----------------+--------------------------+
```

Konektivitas Jaringan

Opsi konektivitas yang disediakan oleh Amazon VPC memungkinkan Anda membuat jaringan yang mencakup VPC di beberapa akun dan Wilayah dan jaringan jarak jauh.

Anda dapat menggunakan peta sumber daya di konsol Amazon VPC untuk mengetahui apakah VPC Anda menggunakan gateway internet, gateway internet khusus keluar, gateway NAT, atau titik akhir VPC gateway. Peta sumber daya tidak menampilkan gateway transit, koneksi peering, gateway pribadi virtual, atau jenis titik akhir VPC lainnya yang sedang digunakan. Anda bisa mendapatkan daftar lengkap gateway dan koneksi peering untuk VPC dengan menjelaskannya satu per satu menggunakan konsol, API, atau antarmuka baris perintah.

Mengapa hal ini penting

Setelah memahami konektivitas yang disediakan oleh jaringan VPC Anda, Anda dapat memastikan bahwa sumber daya dalam jaringan yang setara secara fungsional dapat berkomunikasi dengan sumber daya lokal dan jarak jauh yang sama.

Untuk melihat koneksi jaringan untuk VPC menggunakan peta sumber daya

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih VPC.
3. Pilih kotak centang untuk VPC.
4. Pilih tab Peta sumber daya.
5. Di panel VPC, pilih Tampilkan rincian. Panel koneksi jaringan mencantumkan semua gateway internet, gateway internet khusus keluar, gateway NAT, dan titik akhir VPC gateway. Jika jenis sumber daya tidak jelas, arahkan kursor ke ikon tautan untuk koneksi jaringan dan periksa URL yang dihasilkan. URL ini adalah tautan ke sumber daya di konsol, dan berisi jenis sumber daya dan ID sumber daya (misalnya,internetGatewayId=igw-0123456780abcdef).

Untuk mendapatkan koneksi jaringan untuk VPC Anda menggunakan AWS CLI

1. Gunakan perintah describe-internet-gateways berikut untuk mendapatkan gateway internet untuk Wilayah yang ditentukan. `--query`Parameter hanya mencakup bidang yang ditentukan dalam output. Anda dapat menyertakan bidang tambahan sesuai kebutuhan.

```
aws ec2 describe-internet-gateways \
    --region us-east-2 \
    --query InternetGatewaysAttachments[0].VpcId,InternetGatewayId] \
    --output table
```

   Berikut ini adalah output contoh. Kolom menunjukkan ID VPC dan ID gateway internet.

```
-----------------------------------------------------
|             DescribeInternetGateways              |
+------------------------+--------------------------+
|  None                  |  igw-04c61dba10EXAMPLE   |
|  vpc-0bf4c2739bEXAMPLE |  igw-09737a4029EXAMPLE   |
|  vpc-060415a18fEXAMPLE |  igw-0c562bd22aEXAMPLE   |
|  vpc-0ea9d41094EXAMPLE |  igw-0e06f7033dEXAMPLE   |
|  vpc-03b86de356EXAMPLE |  igw-0a9ff72d05EXAMPLE   |
+------------------------+--------------------------+
```

2. Gunakan perintah describe-egress-only-internet-gateways berikut untuk mendapatkan gateway internet khusus egress untuk Wilayah yang ditentukan. `--query`Parameter hanya mencakup bidang yang ditentukan dalam output. Anda dapat menyertakan bidang tambahan sesuai kebutuhan.

```
aws ec2 describe-egress-only-internet-gateways \
    --region us-east-2 \
    --query EgressOnlyInternetGateways[*].
[Attachments[0].VpcId,EgressOnlyInternetGatewayId] \
    --output table
```

   Berikut ini adalah output contoh. Kolom menunjukkan ID VPC dan ID gateway internet khusus keluar.

```
-----------------------------------------------------
|        DescribeEgressOnlyInternetGateways         |
+------------------------+--------------------------+
```

```
|  vpc-060415a18fEXAMPLE |  eigw-0b8ca558acEXAMPLE  |
+------------------------+--------------------------+
```

3. Gunakan perintah describe-nat-gateways berikut untuk mendapatkan gateway NAT untuk Wilayah yang ditentukan. `--query`Parameter hanya mencakup bidang yang ditentukan dalam output. Anda dapat menyertakan bidang tambahan sesuai kebutuhan.

```
aws ec2 describe-nat-gateways \
    --region us-east-2 \
    --query NatGateways[*].[VpcId,NatGatewayId,SubnetId] \
    --output table
```

Berikut ini adalah output contoh. Kolom menunjukkan ID VPC, ID gateway NAT, dan ID subnet.

```
-------------------------------------------------------------------------------
|                            DescribeNatGateways                              |
+------------------------+------------------------+---------------------------+
|  vpc-060415a18fEXAMPLE |  nat-026316334aEXAMPLE  |  subnet-0eb17d85f5EXAMPLE  |
|  vpc-060415a18fEXAMPLE |  nat-0f08bc5f52EXAMPLE  |  subnet-0d2d1b81e0EXAMPLE  |
+------------------------+------------------------+---------------------------+
```

4. Gunakan perintah describe-transit-gateway-vpc-attachments berikut untuk mendapatkan lampiran VPC gateway transit untuk Wilayah yang ditentukan. `--query`Parameter hanya mencakup bidang yang ditentukan dalam output. Anda dapat menyertakan bidang tambahan sesuai kebutuhan.

```
aws ec2 describe-transit-gateway-vpc-attachments \
    --region us-east-2 \
    --query TransitGatewayVpcAttachments[*].
[VpcId,TransitGatewayId,length(SubnetIds[])] \
    --output table
```

Berikut ini adalah output contoh. Kolom menunjukkan ID VPC, ID gateway transit, dan jumlah subnet.

```
-----------------------------------------------------------
|         DescribeTransitGatewayVpcAttachments          |
+------------------------+------------------------+----+
|  vpc-0bf4c2739bEXAMPLE |  tgw-055dc4e47bEXAMPLE  |  4 |
|  vpc-0ea9d41094EXAMPLE |  tgw-055dc4e47bEXAMPLE  |  2 |
```

```
+-----------------------+-------------------------+----+
```

5. Gunakan perintah describe-vpc-peering-connections berikut untuk mendapatkan koneksi peering untuk VPC di Wilayah yang ditentukan. `--query`Parameter hanya mencakup bidang yang ditentukan dalam output. Anda dapat menyertakan bidang tambahan sesuai kebutuhan.

```
aws ec2 describe-vpc-peering-connections \
    --region us-east-2 \
    --query VpcPeeringConnections[*].[AccepterVpcInfo.VpcId,RequesterVpcInfo.VpcId]
 \
    --output table
```

Berikut ini adalah output contoh. Kolom menunjukkan ID VPC aksepter, pemilik VPC aksepter, ID VPC pemohon, dan pemilik VPC pemohon.

```
-------------------------------------------------------------------------------
|                          DescribeVpcPeeringConnections
 |
+-----------------------+--------------+-----------------------+---------------
+
|  vpc-0ea9d41094EXAMPLE |  123456789012 |  vpc-03b86de356EXAMPLE |  123456789012
 |
+-----------------------+--------------+-----------------------+---------------
+
```

6. Gunakan perintah describe-vpn-gateways berikut untuk mendapatkan gateway pribadi virtual untuk Wilayah yang ditentukan. `--query`Parameter hanya mencakup bidang yang ditentukan dalam output. Anda dapat menyertakan bidang tambahan sesuai kebutuhan.

```
aws ec2 describe-vpn-gateways \
    --region us-east-2 \
    --query VpnGateways[*].[VpcAttachments[0].VpcId,VpnGatewayId] \
    --output table
```

Berikut ini adalah output contoh. Kolom menunjukkan ID VPC dan ID gateway pribadi virtual.

```
-------------------------------------------------
|               DescribeVpnGateways             |
+-----------------------+-----------------------+
|  vpc-0bf4c2739bEXAMPLE |  vgw-0cb3226c4aEXAMPLE  |
```

```
+-----------------------+------------------------+
```

7. Gunakan perintah describe-vpc-endpoints berikut untuk mendapatkan titik akhir VPC untuk Wilayah yang ditentukan. `--query`Parameter hanya mencakup bidang yang ditentukan dalam output. Anda dapat menyertakan bidang tambahan sesuai kebutuhan.

```
aws ec2 describe-vpc-endpoints \
    --region us-east-2 \
    --query 'VpcEndpoints[*].[VpcId,VpcEndpointType,ServiceName||
ServiceNetworkArn||ResourceConfigurationArn]' \
    --output table
```

Berikut ini adalah output contoh. Kolom pertama menunjukkan ID VPC dan kolom kedua menunjukkan tipe titik akhir VPC. Kolom ketiga tergantung pada tipe titik akhir, dan menunjukkan nama layanan, konfigurasi sumber daya ARN, atau ARN jaringan layanan.

```
----------------------------------------------------------------------------------------------
|                                                    DescribeVpcEndpoints
                                                 |
+-----------------------+-----------------
+-------------------------------------------------------------------------------------------
+
|  vpc-060415a18fcc9afde |  Interface      |  com.amazonaws.vpce.us-west-2.vpce-
svc-007832a03d60fc387                              |
|  vpc-060415a18fcc9afde |  Interface      |  com.amazonaws.vpce.us-west-2.vpce-
svc-007832a03d60fc387                              |
|  vpc-0bf4c2739bc05a694 |  Gateway        |  com.amazonaws.us-west-2.s3
                                                   |
|  vpc-0ea9d410947d27b7d |  Interface      |  com.amazonaws.us-west-2.logs
                                                   |
|  vpc-0bf4c2739bc05a694 |  Resource       |  arn:aws:vpc-lattice:us-
east-2:123456789012:resourceconfiguration/rcfg-07129f3acded87625  |
|  vpc-0bf4c2739bc05a694 |  ServiceNetwork |  arn:aws:vpc-lattice:us-
east-2:123456789012:servicenetwork/sn-0808d1748faee0c1e           |
|  vpc-0bf4c2739bc05a694 |  ServiceNetwork |  arn:aws:vpc-lattice:us-
east-2:123456789012:servicenetwork/sn-0808d1748faee0c1e           |
+-----------------------+-----------------
+-------------------------------------------------------------------------------------------
+
```

Kontrol keamanan

Kontrol keamanan yang disediakan oleh Amazon VPC menentukan akses jaringan ke VPC Anda dan sumber daya yang digunakan di VPC Anda.

Mengapa hal ini penting

Setelah Anda menentukan lalu lintas masuk yang diizinkan untuk mencapai subnet dan sumber daya dan lalu lintas keluaran yang diizinkan meninggalkan subnet dan sumber daya Anda, Anda dapat merencanakan aturan firewall yang diperlukan untuk jaringan yang setara secara fungsional.

Kontrol keamanan

- Grup keamanan
- ACL jaringan

Grup keamanan

Grup keamanan memungkinkan lalu lintas masuk dan keluar tertentu di tingkat sumber daya. Grup keamanan adalah mekanisme utama untuk mengontrol akses ke sumber daya di VPC Anda.

Untuk mendapatkan grup keamanan untuk VPC Anda

Gunakan perintah describe-security-groups berikut untuk menampilkan grup keamanan untuk VPC yang ditentukan.

```
aws ec2 describe-security-groups \
    --filters Name=vpc-id,Values=vpc-1234567890abcdef0 \
    --query SecurityGroups[*].GroupId
```

Untuk mendapatkan aturan masuk untuk grup keamanan

Gunakan perintah describe-security-group-rules berikut untuk menampilkan aturan untuk grup keamanan yang ditentukan di mana berada. `IsEgress` `false`

```
aws ec2 describe-security-group-rules \
    --filters Name=group-id,Values=sg-0abcdef1234567890 \
    --query 'SecurityGroupRules[?IsEgress==`false`]'
```

Untuk mendapatkan aturan keluar untuk grup keamanan

Gunakan perintah describe-security-group-rules berikut untuk menampilkan aturan untuk grup keamanan yang ditentukan di mana berada. `IsEgress` `true`

```
aws ec2 describe-security-group-rules \
    --filters Name=group-id,Values=sg-0abcdef1234567890 \
    --query 'SecurityGroupRules[?IsEgress==`true`]'
```

ACL jaringan

Daftar kontrol akses jaringan (ACL) memungkinkan atau menolak lalu lintas masuk dan keluar tertentu di tingkat subnet. Anda dapat menggunakan ACL jaringan sebagai pertahanan mendalam jika sumber daya digunakan tanpa grup keamanan yang benar.

Untuk mendapatkan ACL jaringan untuk subnet Anda

Gunakan perintah describe-network-acls berikut untuk menampilkan ACL jaringan untuk VPC tertentu dan asosiasi subnetnya.

```
aws ec2 describe-network-acls \
    --filters Name=vpc-id,Values=vpc-1234567890abcdef0 \
    --query "NetworkAcls[*].{ID:NetworkAclId,Subnets:Associations[].SubnetId}"
```

Untuk mendapatkan aturan masuk untuk ACL jaringan

Gunakan perintah describe-network-acls berikut untuk menampilkan aturan untuk ACL jaringan yang ditentukan di mana berada. `Egress` `false`

```
aws ec2 describe-network-acls \
    --network-acl-ids acl-0abcdef1234567890 \
    --query 'NetworkAcls[*].Entries[?Egress==`false`]'
```

Untuk mendapatkan aturan keluar untuk ACL jaringan

Gunakan perintah describe-network-acls berikut untuk menampilkan aturan untuk ACL jaringan yang ditentukan di mana berada. `Egress` `true`

```
aws ec2 describe-network-acls \
    --network-acl-ids acl-0abcdef1234567890 \
    --query 'NetworkAcls[*].Entries[?Egress==`true`]'
```

Manajemen lalu lintas

Manajemen lalu lintas yang efektif menggabungkan keputusan routing tingkat jaringan yang disediakan oleh tabel rute dengan strategi distribusi tingkat aplikasi yang disediakan oleh load balancing.

Mengapa hal ini penting

Administrator jaringan harus merancang subnet, routing, resolusi DNS, dan penyeimbangan beban untuk mengoptimalkan aliran lalu lintas sambil mempertahankan batas keamanan dan persyaratan kinerja. Dengan mencatat konfigurasi komponen-komponen ini di jaringan VPC Anda, Anda dapat membantu memastikan bahwa sumber daya dalam jaringan yang setara secara fungsional dapat berkomunikasi dengan klien atau perangkat yang sama dengan yang dapat mereka lakukan di jaringan VPC Anda.

Manajemen lalu lintas

- Tabel rute
- Pengaturan opsi DHCP
- Penyeimbang beban

Tabel rute

Tabel rute menentukan bagaimana lalu lintas jaringan mengalir melintasi batas-batas jaringan seperti subnet, VPC, jaringan lokal, dan internet.

Peta sumber daya di konsol Amazon VPC menyediakan representasi visual dari tabel rute untuk VPC Anda.

Untuk melihat tabel rute untuk VPC menggunakan peta sumber daya

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih VPC.
3. Pilih kotak centang untuk VPC.
4. Pilih tab Peta sumber daya.
5. Panel tabel rute mencantumkan semua tabel rute untuk VPC. Arahkan kursor ke tabel rute untuk menyorot subnet dan koneksi jaringan yang terkait. Untuk detail lebih lanjut, pilih tautan untuk membuka halaman detail tabel rute.

Untuk menggambarkan tabel rute Anda

Gunakan perintah describe-route-tables untuk menjelaskan tabel rute untuk VPC tertentu dan asosiasi subnetnya.

```
aws ec2 describe-route-tables \
    --filters Name=vpc-id,Values=vpc-1234567890abcdef0 \
    --query "RouteTables[*].{ID:RouteTableId,Subnets:Associations[].SubnetId}"
```

Untuk mendapatkan rute untuk tabel rute

Gunakan perintah describe-route-tables untuk menjelaskan rute untuk tabel rute yang ditentukan.

```
aws ec2 describe-route-tables \
    --route-table-ids rtb-02ec01715bEXAMPLE \
    --query RouteTables[*].Routes
```

Pengaturan opsi DHCP

VPC Anda memiliki set opsi DHCP yang dapat Anda gunakan untuk mengkonfigurasi berbagai pengaturan jaringan. Misalnya, Anda dapat mengonfigurasi server DNS kustom sehingga instans EC2 Anda dapat menyelesaikan nama host internal menggunakan infrastruktur DNS yang ada. Untuk informasi selengkapnya, lihat the section called “Konsep set opsi DHCP”.

Untuk menjelaskan opsi DHCP untuk VPC Anda

Gunakan perintah describe-dhcp-options untuk menjelaskan opsi DHCP yang ditentukan. Contoh ini juga mendapatkan ID opsi DHCP untuk VPC yang ditentukan menggunakan perintah descri be-vpcs.

```
aws ec2 describe-dhcp-options \
    --dhcp-options-id "$(aws ec2 describe-vpcs \
        --vpc-id vpc-1234567890abcdef0 \
        --query Vpcs[].DhcpOptionsId --output text)"
```

Berikut ini adalah contoh output untuk VPC yang menggunakan opsi DHCP default.

```
{
    "DhcpOptions": [
        {
            "OwnerId": "415546850671",
            "Tags": [],
```

```
            "DhcpOptionsId": "dopt-1234567890abcdef0",
            "DhcpConfigurations": [
                {
                    "Key": "domain-name",
                    "Values": [
                        {
                            "Value": "us-west-2.compute.internal"
                        }
                    ]
                },
                {
                    "Key": "domain-name-servers",
                    "Values": [
                        {
                            "Value": "AmazonProvidedDNS"
                        }
                    ]
                }
            ]
        }
    ]
}
```

Penyeimbang beban

Load balancing mendistribusikan lalu lintas masuk dari klien di beberapa target. Penyeimbang beban memantau kesehatan target dan secara otomatis menghapus target yang tidak sehat dari distribusi lalu lintas, memastikan bahwa hanya target sehat yang digunakan. Ini meningkatkan ketersediaan dan kinerja aplikasi Anda dan mengoptimalkan pemanfaatan sumber daya. Untuk informasi selengkapnya, silakan lihat Panduan Pengguna Penyeimbang Beban Elastis.

Untuk menggambarkan penyeimbang beban Anda

Gunakan perintah describe-load-balancers untuk menampilkan penyeimbang beban untuk VPC yang ditentukan.

```
aws elbv2 describe-load-balancers \
    --query 'LoadBalancers[?VpcId==`vpc-1234567890abcdef0`].LoadBalancerArn'
```

Sumber daya terkait

Berikut ini adalah layanan atau fitur opsional yang mungkin Anda gunakan di jaringan VPC Anda:

- Direct Connect
- AWS Network Firewall
- IPAM
- Pencerminan lalu lintas
- Log aliran VPC

Mengelola tanggung jawab keamanan untuk Amazon Virtual Private Cloud

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama AWS antara Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Third-party auditor secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program Kep AWS atuhan Program Kep . Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon Virtual Private Cloud, lihat Layanan dalam Lingkup berdasarkan AWS .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, termasuk sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Amazon VPC. Topik berikut menunjukkan cara mengonfigurasi Amazon VPC untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Amazon VPC Anda.

Daftar Isi

- Memastikan perlindungan data di Amazon Virtual Private Cloud
- Menerapkan enkripsi VPC saat transit
- Identity and access management untuk Amazon VPC
- Keamanan infrastruktur di Amazon VPC
- Kontrol lalu lintas ke Anda AWS sumber daya menggunakan grup keamanan
- Kontrol lalu lintas subnet dengan daftar kontrol akses jaringan
- Ketahanan di Amazon Virtual Private Cloud
- Validasi kepatuhan untuk Amazon Virtual Private Cloud

- Blokir akses publik ke VPC dan subnet
- Praktik terbaik keamanan untuk VPC Anda

Memastikan perlindungan data di Amazon Virtual Private Cloud

Model tanggung jawab AWS https://aws.amazon.com/compliance/shared-responsibility-model/ berlaku untuk perlindungan data di Amazon Virtual Private Cloud. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat FAQ Privasi Data Ket . Untuk informasi tentang perlindungan data di Eropa, lihat Pusat Peraturan Umum Perlindungan Data (GDPR).

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredenSIAL dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang menggunakan CloudTrail jalur untuk menangkap AWS aktivitas, lihat Bekerja dengan CloudTrail jejak di Panduan AWS CloudTrail Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Amazon VPC atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Memastikan privasi lalu lintas antar jaringan di Amazon VPC

Amazon Virtual Private Cloud menyediakan fitur yang dapat Anda gunakan untuk meningkatkan dan memantau keamanan untuk virtual private cloud (VPC) Anda:

- Grup keamanan: Grup keamanan mengizinkan lalu lintas masuk dan keluar tertentu di tingkat sumber daya (seperti instans EC2). Saat meluncurkan instance, Anda dapat mengaitkannya dengan satu atau beberapa grup keamanan. Setiap instans di VPC Anda bisa menjadi milik grup keamanan yang berbeda. Jika Anda tidak menentukan grup keamanan saat meluncurkan instance, instans secara otomatis dikaitkan dengan grup keamanan default untuk VPC-nya. Untuk informasi selengkapnya, lihat Grup keamanan.
- Daftar kontrol akses jaringan (ACL): ACL jaringan memungkinkan atau menolak lalu lintas masuk dan keluar tertentu di tingkat subnet. Untuk informasi selengkapnya, lihat Kontrol lalu lintas subnet dengan daftar kontrol akses jaringan.
- Log alur: Log alur menangkap informasi tentang lalu lintas IP ke dan dari antarmuka jaringan di VPC Anda. Anda dapat membuat log alur untuk VPC, subnet, atau antarmuka jaringan individu. Data log aliran dipublikasikan ke Log CloudWatch s atau Amazon S3, dan ini dapat membantu Anda mendiagnosis grup keamanan dan aturan ACL jaringan yang terlalu ketat atau terlalu permisif. Untuk informasi selengkapnya, lihat Pencatatan lalu lintas IP menggunakan Log Aliran VPC.
- Mirroring lalu lintas: Anda dapat menyalin lalu lintas jaringan dari antarmuka jaringan elastis dari instans Amazon EC2. Anda kemudian dapat mengirim lalu lintas ke peralatan keamanan dan pemantauan di luar band. Untuk informasi lebih lanjut, lihat Panduan Mirroring Lalu Lintas.

Menerapkan enkripsi VPC saat transit

Kontrol Enkripsi VPC adalah fitur keamanan dan kepatuhan yang menawarkan kontrol otoritatif terpusat untuk memantau status enkripsi arus lalu lintas Anda, membantu Anda mengidentifikasi sumber daya yang memungkinkan komunikasi cleartext, dan akhirnya memberi Anda mekanisme untuk menerapkan enkripsi dalam transit di dalam dan di seluruh VPC Anda di suatu wilayah

Kontrol Enkripsi VPC menggunakan enkripsi lapisan aplikasi dan enkripsi bawaan dalam kemampuan transit perangkat keras sistem AWS nitro untuk memastikan penegakan enkripsi. Fitur ini juga memperluas enkripsi lapisan perangkat keras asli di luar instance Nitro modern ke AWS layanan lain termasuk Fargate, Application Load Balancer, Transit Gateway dan banyak lainnya.

Fitur ini dirancang untuk siapa saja yang ingin memastikan visibilitas dan kontrol ke dalam status enkripsi semua lalu lintas mereka. Ini sangat berguna dalam industri, di mana enkripsi data sangat penting untuk memenuhi standar kepatuhan seperti HIPAA, FedRamp dan PCI DSS. Administrator keamanan dan arsitek cloud dapat menggunakannya untuk menerapkan enkripsi secara terpusat dalam kebijakan transit di seluruh AWS lingkungan mereka

Fitur ini dapat digunakan dalam dua mode: mode monitor dan mode menegakkan.

Mode Kontrol Enkripsi

Mode monitor

Dalam mode monitor, Kontrol Enkripsi memberikan visibilitas ke dalam status enkripsi arus lalu lintas antara AWS sumber daya Anda di dalam dan di seluruh VPC. Ini juga membantu Anda mengidentifikasi sumber daya VPC yang tidak menerapkan enkripsi saat transit. Anda dapat mengonfigurasi log aliran VPC Anda untuk memancarkan bidang yang diperkaya - `encryption-status` - yang memberi tahu Anda apakah lalu lintas Anda dienkripsi. Anda juga dapat menggunakan konsol atau `GetVpcResourcesBlockingEncryptionEnforcement` perintah untuk mengidentifikasi sumber daya yang tidak menerapkan enkripsi saat transit.

> **Note**
>
> VPC yang ada hanya dapat diaktifkan dalam Mode Monitor terlebih dahulu. Ini memberi Anda visibilitas ke sumber daya yang memungkinkan atau mungkin mengizinkan lalu lintas cleartext. Anda hanya dapat mengaktifkan mode paksa pada VPC setelah sumber daya ini mulai menerapkan enkripsi (atau Anda membuat pengecualian untuk mereka).

Menegakkan mode

Dalam mode menegakkan, Kontrol Enkripsi VPC mencegah Anda menggunakan fitur atau layanan apa pun yang memungkinkan lalu lintas tidak terenkripsi dalam batas VPC. Anda tidak dapat mengaktifkan Kontrol Enkripsi dalam mode menegakkan langsung pada VPC yang ada. Anda harus terlebih dahulu mengaktifkan Kontrol Enkripsi dalam mode monitor, mengidentifikasi dan memodifikasi sumber daya yang tidak sesuai untuk menerapkan enkripsi saat transit, lalu mengaktifkan mode paksa. Namun Anda dapat mengaktifkan Kontrol Enkripsi dalam mode menegakkan untuk VPC baru selama pembuatan.

Saat diaktifkan, mode paksa mencegah Anda membuat atau melampirkan sumber daya VPC yang tidak terenkripsi seperti instans EC2 lama yang tidak mendukung enkripsi bawaan asli, atau gateway internet, dll. Jika Anda ingin menjalankan sumber daya yang tidak sesuai di VPC yang diberlakukan enkripsi, Anda harus membuat pengecualian untuk sumber daya tersebut.

Memantau status Enkripsi Arus Lalu Lintas

Anda dapat mengaudit status enkripsi arus lalu lintas di dalam VPC menggunakan `encryption-status` bidang di Log Aliran VPC Anda. Ini dapat memiliki nilai-nilai berikut:

- `0`= tidak dienkripsi
- `1`= nitro-terenkripsi (dikelola oleh Kontrol Enkripsi VPC)
- `2`= dienkripsi aplikasi
  - mengalir pada port TCP 443 untuk titik akhir antarmuka ke AWS layanan*
  - mengalir pada port TCP 443 untuk titik akhir gateway*
  - mengalir ke cluster Redshift terenkripsi melalui titik akhir VPC**
- `3`= baik nitro DAN aplikasi dienkripsi
- `(-)`= Status Enkripsi Tidak diketahui atau kontrol enkripsi VPC tidak aktif

Catatan:

* Untuk titik akhir antarmuka dan gateway, AWS tidak melihat data paket untuk menentukan status enkripsi, kami malah mengandalkan port yang digunakan untuk mengasumsikan status enkripsi.

** Untuk titik akhir AWS terkelola yang ditentukan AWS , tentukan status enkripsi berdasarkan persyaratan untuk TLS dalam konfigurasi layanan.

Batasan Log Aliran VPC

- Untuk mengaktifkan log alur untuk Kontrol Enkripsi VPC, Anda perlu membuat log alur baru dengan bidang status enkripsi secara manual. Bidang status enkripsi tidak ditambahkan secara otomatis ke log alur yang ada.
- Disarankan untuk menambahkan bidang $ {traffic-path} dan $ {flow-direction} ke log aliran untuk informasi lebih rinci dalam log alur.

  Contoh:

```
aws ec2 create-flow-logs \
--resource-type VPC \
--resource-ids vpc-12345678901234567 \
--traffic-type ALL \
--log-group-name my-flow-logs \
--deliver-logs-permission-arn arn:aws:iam::123456789101:role/publishFlowLogs
--log-format '${encryption-status} ${srcaddr} ${dstaddr} ${srcport} ${dstport}
 ${protocol} ${traffic-path} ${flow-direction} ${reject-reason}'
```

Pengecualian Kontrol Enkripsi VPC

Kontrol enkripsi VPC menegakkan mode mengharuskan semua sumber daya Anda di VPC menerapkan enkripsi. Ini memastikan enkripsi AWS di dalam suatu wilayah. Namun, Anda mungkin memiliki sumber daya seperti gateway internet, gateway NAT atau gateway pribadi virtual yang memungkinkan konektivitas di luar AWS jaringan tempat Anda bertanggung jawab untuk mengonfigurasi dan memelihara enkripsi ujung ke ujung. Untuk menjalankan sumber daya ini dalam VPC yang dipaksakan enkripsi, Anda dapat membuat pengecualian sumber daya. Pengecualian menciptakan pengecualian yang dapat diaudit untuk sumber daya di mana pelanggan bertanggung jawab untuk mempertahankan enkripsi (biasanya di lapisan aplikasi).

Hanya ada 8 pengecualian yang didukung untuk Kontrol Enkripsi VPC. Jika Anda memiliki sumber daya ini di VPC dan ingin pindah ke mode menegakkan, Anda harus menambahkan pengecualian ini saat beralih dari monitor ke mode menegakkan. Tidak ada sumber daya lain yang dapat dikecualikan. Anda dapat memigrasikan VPC untuk menerapkan mode dengan membuat pengecualian untuk sumber daya ini. Anda bertanggung jawab atas enkripsi arus lalu lintas ke dan dari sumber daya ini

- Gerbang Internet
- Gerbang NAT

- Egress-only Gerbang Internet
- Koneksi VPC Peering ke VPC yang tidak dipaksakan enkripsi (lihat bagian dukungan peering VPC untuk skenario terperinci)
- Gerbang Pribadi Virtual
- Fungsi Lambda di dalam VPC Anda
- VPC Lattice
- Sistem File Elastis

Alur kerja implementasi

1. Aktifkan pemantauan - Buat kontrol enkripsi VPC dalam mode monitor
2. Analisis lalu lintas - Tinjau Log Alur untuk memantau status enkripsi arus lalu lintas
3. Analisis Sumber Daya - Gunakan konsol atau `GetVpcResourcesBlockingEncryptionEnforcement` perintah untuk mengidentifikasi sumber daya yang tidak menerapkan enkripsi saat transit.
4. Siapkan [Opsional] - Rencanakan migrasi sumber daya dan pengecualian yang diperlukan jika Anda ingin mengaktifkan mode paksa
5. Terapkan [Opsional] - Beralih ke mode menegakkan dengan pengecualian yang diperlukan dikonfigurasi
6. Audit - Pemantauan kepatuhan berkelanjutan melalui Log Aliran

Untuk petunjuk penyiapan terperinci, lihat blog Memperkenalkan kontrol enkripsi VPC: menerapkan enkripsi dalam transit di dalam dan di seluruh VPC di suatu wilayah.

Status Kontrol Enkripsi VPC

Kontrol Enkripsi VPC dapat memiliki salah satu status berikut:

menciptakan

Kontrol enkripsi VPC sedang dibuat pada VPC.

modifikasi dalam proses

Kontrol Enkripsi VPC sedang dimodifikasi pada VPC

menghapus

Kontrol Enkripsi VPC sedang dihapus pada VPC

tersedia

Kontrol Enkripsi VPC berhasil menerapkan mode monitor atau menerapkan mode pada VPC

AWS dukungan layanan dan kompatibilitas

Agar sesuai dengan enkripsi, sumber daya harus selalu menerapkan enkripsi saat transit, baik di lapisan perangkat keras atau di lapisan aplikasi. Untuk sebagian besar sumber daya, tidak ada tindakan yang diperlukan dari Anda.

Layanan dengan kepatuhan otomatis

Sebagian besar AWS layanan yang didukung oleh PrivateLink, termasuk Cross-Region PrivateLinks akan menerima lalu lintas terenkripsi di lapisan aplikasi. Anda tidak diharuskan untuk membuat perubahan apa pun pada sumber daya ini. AWS secara otomatis menjatuhkan lalu lintas apa pun yang tidak dienkripsi lapisan aplikasi. Beberapa pengecualian termasuk cluster Redshift (baik yang disediakan maupun tanpa server - di mana Anda perlu memigrasikan sumber daya yang mendasarinya secara manual)

Sumber daya yang bermigrasi secara otomatis

Network Load Balancers, Application Load Balancers, Fargate Cluster, EKS Control Plane akan secara otomatis bermigrasi ke perangkat keras yang secara asli mendukung enkripsi setelah Anda mengaktifkan mode monitor. Anda tidak diharuskan untuk memodifikasi sumber daya ini. AWS menangani migrasi secara otomatis.

Sumber daya yang membutuhkan migrasi manual

Sumber daya dan layanan VPC tertentu mengharuskan Anda memilih jenis instans yang mendasarinya. Semua instans EC2 modern mendukung enkripsi saat transit. Anda tidak perlu melakukan perubahan apa pun jika layanan Anda sudah menggunakan instans EC2 modern. Anda dapat menggunakan konsol atau GetVpcResourcesBlockingEncryptionEnforcement perintah untuk mengidentifikasi apakah salah satu layanan ini menggunakan instance yang lebih lama. Jika Anda mengidentifikasi sumber daya tersebut, Anda harus memutakhirkannya ke salah satu instans EC2 modern yang mendukung enkripsi asli perangkat keras sistem nitro. Layanan ini termasuk instans EC2, Grup Penskalaan Otomatis, RDS (Semua Database dan Document-DB),

Elasticache Provisioned, Amazon Redshift Provisioned Clusters, EKS, Provisioned dan EMR. ECS-EC2 OpenSearch

Sumber daya yang kompatibel:

Sumber daya berikut kompatibel dengan Kontrol Enkripsi VPC:

- Nitro-based Instans EC2
- Penyeimbang Beban Jaringan (dengan keterbatasan)
- Application Load Balancer
- AWS Cluster Fargate
- Amazon Elastic Kubernetes Service (EKS)
- Amazon EC2 Auto Scaling Groups
- Layanan Database Relasional Amazon (RDS - Semua Basis Data)
- Cluster ElastiCache berbasis node Amazon
- Cluster Amazon Redshift yang Disediakan dan Tanpa Server
- Amazon Elastic Container Service (ECS) - Instans kontainer EC2
- OpenSearch Layanan Amazon
- Amazon Elastis MapReduce (EMR)
- Amazon Managed Streaming for Apache Kafka (Amazon MSK)
- Kontrol Enkripsi VPC memberlakukan enkripsi pada lapisan aplikasi untuk semua AWS layanan yang diakses melalui PrivateLink. Lalu lintas apa pun yang tidak dienkripsi di lapisan aplikasi dijatuhkan oleh PrivateLink titik akhir yang dihosting di dalam VPC dengan kontrol Enkripsi dalam mode menegakkan

Service-specific keterbatasan

Batasan Penyeimbang Beban Jaringan

Konfigurasi TLS: Anda tidak dapat menggunakan pendengar TLS untuk memindahkan pekerjaan enkripsi dan dekripsi ke penyeimbang beban Anda saat menerapkan Kontrol Enkripsi pada VPC yang berisi. Namun Anda dapat mengonfigurasi target Anda untuk melakukan enkripsi dan dekripsi TLS

Redshift Disediakan dan Tanpa Server

Pelanggan tidak dapat pindah ke mode Enforce pada VPC yang memiliki kluster/titik akhir yang ada. Untuk menggunakan Kontrol Enkripsi VPC dengan Redshift, Anda harus memulihkan cluster atau

namespace dari snapshot. Untuk Cluster yang Disediakan, buat snapshot dari cluster Redshift yang ada dan kemudian pulihkan dari snapshot menggunakan operasi pemulihan dari snapshot cluster. Untuk Tanpa Server, buat snapshot dari namespace yang ada dan kemudian pulihkan dari snapshot menggunakan operasi pemulihan dari snapshot pada workgroup tanpa server Anda. Perhatikan bahwa Kontrol Enkripsi VPC tidak dapat diaktifkan pada cluster atau ruang nama yang ada tanpa melakukan proses snapshot dan pemulihan. Lihat dokumentasi Amazon Redshift untuk pembuatan snapshot.

Amazon MSK (Streaming terkelola untuk Apache Kafka)

Fungsionalitas ini didukung di cluster baru untuk 4.1 di VPC mereka sendiri. Langkah-langkah berikut akan membantu Anda menggunakan Enkripsi VPC dengan MSK.

- Pelanggan mengaktifkan Enkripsi VPC pada VPC tanpa cluster MSK lainnya
- Pelanggan membuat cluster dengan Kafka versi 4.1 dan tipe instance sebagai M7g

Gateway Load Balancer dan AWS Network Firewall

Gateway Load Balancer dan AWS Network Firewall tidak didukung dengan VPC dalam mode menegakkan. Jika sumber daya ini ada di VPC Anda, Anda harus menjalankan VPC Anda dalam mode monitor.

Batasan regional dan zona

- Subnet Zona Lokal: Tidak didukung dalam mode menegakkan - harus dihapus dari VPC

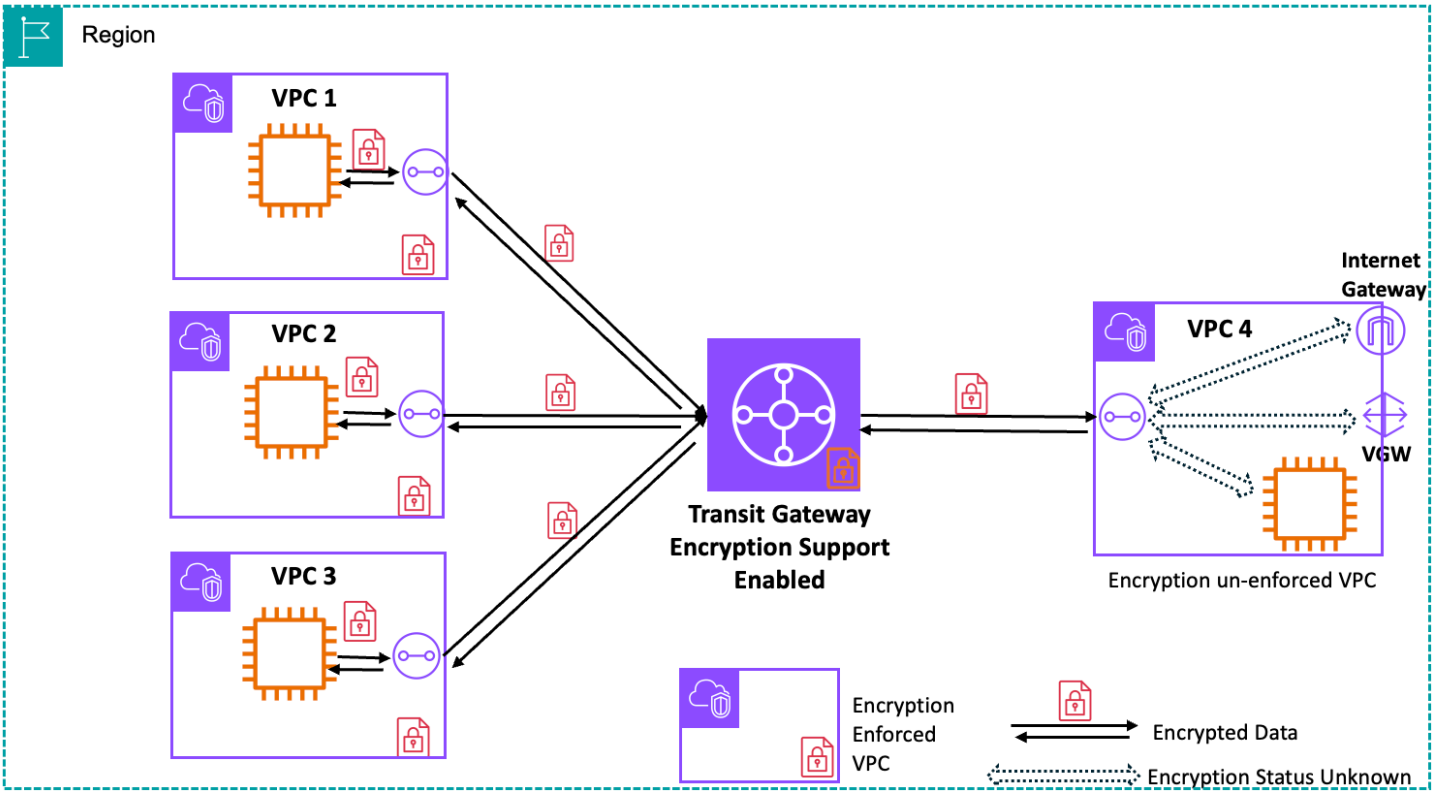
Dukungan peering VPC

Untuk memastikan enkripsi dalam transit dengan peering VPC antara dua VPC, kedua VPC harus berada di wilayah yang sama dan mengaktifkan kontrol enkripsi dalam mode menegakkan tanpa pengecualian apa pun. Anda harus membuat pengecualian peering jika ingin meng-peer VPC yang dipaksakan enkripsi ke VPC lain yang berada di wilayah berbeda atau tidak mengaktifkan kontrol enkripsi dalam mode menegakkan (tanpa pengecualian).

Jika dua VPC berada dalam mode menegakkan dan mengintip satu sama lain, Anda tidak dapat mengubah mode dari menegakkan ke monitor. Anda harus membuat pengecualian peering terlebih dahulu, sebelum memodifikasi mode Kontrol Enkripsi VPC untuk dipantau.

Dukungan enkripsi Transit Gateway

Anda harus mengaktifkan dukungan enkripsi pada Transit Gateway secara eksplisit untuk mengenkripsi lalu lintas antara VPC Anda yang mengaktifkan kontrol enkripsi. Mengaktifkan enkripsi pada Transit Gateway yang ada tidak mengganggu arus lalu lintas yang ada dan migrasi lampiran VPC ke jalur terenkripsi akan terjadi dengan mulus dan otomatis. Lalu lintas antara dua VPC dalam mode menegakkan (tanpa pengecualian) melalui Transit Gateway melintasi jalur terenkripsi 100%. Enkripsi pada Transit Gateway juga memungkinkan Anda untuk menghubungkan dua VPC yang berada dalam mode Kontrol Enkripsi yang berbeda juga. Anda harus menggunakannya saat ingin menerapkan kontrol enkripsi di VPC yang terhubung ke VPC yang tidak diberlakukan enkripsi. Dalam skenario seperti itu, semua lalu lintas Anda di dalam VPC yang diberlakukan enkripsi Anda, termasuk lalu lintas antar VPC dienkripsi. Lalu lintas antar-VPC dienkripsi antara sumber daya di VPC yang diberlakukan enkripsi dan Gateway Transit. Di luar itu, enkripsi tergantung pada sumber daya yang akan dituju lalu lintas di VPC yang tidak dipaksakan dan tidak dijamin akan dienkripsi (karena VPC tidak dalam mode menegakkan). Semua VPC harus berada di wilayah yang sama. (lihat detailnya di sini).



- Dalam diagram ini, VPC 1, VPC 2 dan VPC3 memiliki kontrol enkripsi dalam mode menegakkan dan mereka terhubung ke VPC 4 yang memiliki Kontrol Enkripsi yang berjalan dalam mode monitor.

- Semua lalu lintas antara VPC1, VPC2 dan VPC3 akan dienkripsi.
- Untuk menguraikannya, setiap lalu lintas antara sumber daya di VPC 1 dan sumber daya di VPC 4 akan dienkripsi sampai Transit Gateway menggunakan enkripsi yang ditawarkan oleh perangkat keras sistem nitro. Di luar itu status enkripsi tergantung pada sumber daya di VPC 4 dan tidak dijamin akan dienkripsi.

Untuk detail selengkapnya tentang dukungan enkripsi Transit Gateway, lihat dokumentasi gateway transit.

Aktifkan Kontrol Enkripsi VPC di tingkat Akun

Account-level Kontrol Enkripsi VPC memungkinkan Anda mengatur mode kontrol enkripsi dan pengecualian sumber daya yang berlaku untuk semua VPC di akun Anda. Ini menyediakan pengelolaan kebijakan enkripsi terpusat tanpa perlu mengkonfigurasi setiap VPC secara individual.

Account-level kontrol enkripsi mendukung delapan pengecualian sumber daya yang sama dengan VPC-level kontrol: Internet Gateway, NAT Gateway, Egress-only Internet Gateway, VPC Peering, Virtual Private Gateway, Lambda, VPC Lattice, dan Elastic File System.

Account-level Mode Kontrol Enkripsi

Anda dapat mengatur mode berikut di tingkat akun:

Tidak dikelola

Kontrol Enkripsi VPC tetap dalam mode saat ini dan dapat dikelola di tingkat VPC.

Monitor Percobaan

Upaya untuk mentransisi semua VPC di akun ke mode monitor. Mengidentifikasi sumber daya yang tidak dienkripsi tanpa memblokir pembuatan.

Mencoba Menegakkan

Mencoba transisi semua VPC di akun untuk menerapkan mode. Memblokir pembuatan sumber daya yang tidak dienkripsi.

Account-level Status Kontrol Enkripsi

Account-level Kontrol Enkripsi VPC dapat memiliki salah satu status berikut:

keadaan default

Kontrol Enkripsi VPC tingkat akun belum diaktifkan.

transisi-dalam proses

VPC di akun sedang dialihkan ke mode yang ditentukan.

transisi-sebagian berhasil

Satu atau lebih VPC tidak beralih ke mode yang diharapkan.

transisi-sukses

Semua VPC berhasil beralih ke mode yang diharapkan.

transisi-gagal

Semua VPC gagal bertransisi ke mode yang diharapkan.

Aktifkan Kontrol Enkripsi VPC di tingkat Organisasi

Jika Anda menggunakan AWS Organisasi untuk mengelola akun di organisasi Anda, Anda dapat menggunakan kebijakan deklaratif Organisasi untuk menerapkan Kontrol Enkripsi VPC pada akun di AWS organisasi. Untuk informasi selengkapnya tentang kebijakan deklaratif Kontrol Enkripsi VPC, lihat Kebijakan deklaratif yang didukung di Panduan Pengguna AWS Organisasi.

Harga

Untuk informasi harga, lihat Harga Amazon VPC.

AWS CLI referensi perintah

Penyiapan dan konfigurasi

- aws ec2 buat-kontrol enkripsi vpc
- aws ec2 modify-vpc-enkripsi-kontrol
- aws ec2 modifikasi-akun-vpc-enkripsi-kontrol
- aws ec2 menjelaskan-akun-vpc-enkripsi-kontrol
- aws ec2 tgw gerbang transit modifikasi

Pemantauan dan pemecahan masalah

- aws ec2 menjelaskan-kontrol enkripsi vpc
- aws ec2 mendapatkan sumber daya-vpc-memblokir-enkripsi-penegakan
- aws ec2 buat log aliran
- aws ec2 menjelaskan-alur-log
- kueri log aws

Pembersihan

- aws ec2 hapus-kontrol enkripsi vpc

Sumber daya tambahan

Untuk petunjuk penyiapan terperinci, lihat blog Memperkenalkan kontrol enkripsi VPC: menerapkan enkripsi dalam transit di dalam dan di seluruh VPC di suatu wilayah.

Untuk informasi API lebih rinci, lihat Panduan Referensi API EC2.

Identity and access management untuk Amazon VPC

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengendalikan siapa yang dapat diautentikasi (masuk) dan diotorisasi (memiliki izin) untuk menggunakan sumber daya Amazon VPC. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Daftar Isi

- Audiens
- Mengautentikasi menggunakan identitas
- Mengelola akses menggunakan kebijakan
- Bagaimana cara Amazon VPC bekerja sama dengan IAM
- Contoh kebijakan Amazon VPC
- Pecahkan masalah identitas dan akses Amazon VPC
- AWS kebijakan terkelola untuk Amazon Virtual Private Cloud

- Menggunakan peran terkait layanan untuk VPC

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Amazon VPC.

Pengguna layanan – Jika Anda menggunakan layanan Amazon VPC untuk melakukan tugas, maka administrator Anda akan memberikan kredensial dan izin yang dibutuhkan. Saat Anda menggunakan lebih banyak fitur di Amazon VPC untuk melakukan pekerjaan, Anda mungkin memerlukan izin tambahan. Memahami bagaimana akses yang dikelola dapat membantu Anda untuk meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Amazon VPC, lihat Pecahkan masalah identitas dan akses Amazon VPC.

Administrator layanan – Jika Anda bertanggung jawab atas sumber daya Amazon VPC di perusahaan Anda, Anda mungkin memiliki akses penuh ke Amazon VPC. Anda bertanggung jawab untuk menentukan fitur-fitur Amazon VPC dan sumber daya mana yang dapat diakses oleh karyawan Anda. Anda harus mengirimkan permintaan ke administrator IAM Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar IAM. Untuk mempelajari selengkapnya tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Amazon VPC, lihat Bagaimana cara Amazon VPC bekerja sama dengan IAM.

Administrator IAM – Jika Anda seorang administrator IAM, Anda mungkin ingin mempelajari detail tentang bagaimana Anda dapat menulis kebijakan untuk mengelola akses ke Amazon VPC. Untuk melihat contoh kebijakan, lihat Contoh kebijakan Amazon VPC.

Mengautentikasi menggunakan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredentif identitas Anda. Anda harus diautentikasi sebagai Pengguna root akun AWS, pengguna IAM, atau dengan mengambil peran IAM.

Anda dapat masuk sebagai identitas federasi menggunakan kredenSIAL dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), otentikasi masuk tunggal, atau kredenSIAL. Google/ Facebook Untuk informasi selengkapnya tentang cara masuk, lihat Cara masuk ke Akun AWS Anda dalam Panduan Pengguna AWS Sign-In .

Untuk akses terprogram, AWS menyediakan SDK dan CLI untuk menandatangani permintaan kriptografis. Untuk informasi selengkapnya, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut pengguna Akun AWS root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Pengguna dan grup IAM

Pengguna IAM adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk informasi selengkapnya, lihat Memerlukan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredenSIAL sementara di Panduan Pengguna IAM.

Grup IAM menentukan kumpulan pengguna IAM dan mempermudah pengelolaan izin untuk pengguna dalam jumlah besar. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk pengguna IAM dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan beralih dari pengguna ke peran IAM (konsol) atau dengan memanggil operasi AWS CLI AWS API. Untuk informasi selengkapnya, lihat Metode untuk mengambil peran dalam Panduan Pengguna IAM.

Peran IAM berguna untuk akses pengguna terfederasi, izin pengguna IAM sementara, akses lintas akun, akses lintas layanan, dan aplikasi yang berjalan di Amazon EC2. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan menentukan izin saat dikaitkan dengan identitas atau sumber daya. AWS mengevaluasi kebijakan ini ketika kepala sekolah membuat permintaan. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Menggunakan kebijakan, administrator menentukan siapa yang memiliki akses ke apa dengan mendefinisikan principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Administrator IAM membuat kebijakan IAM dan menambahkannya ke peran, yang kemudian dapat diambil oleh pengguna. Kebijakan IAM mendefinisikan izin terlepas dari metode yang Anda gunakan untuk melakukan operasinya.

Identity-based kebijakan

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan dalam Panduan Pengguna IAM.

Identity-based kebijakan dapat berupa kebijakan sebaris (disematkan langsung ke dalam satu identitas) atau kebijakan ter kelola (kebijakan mandiri yang dilampirkan ke beberapa identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat Pilih antara kebijakan terkelola dan kebijakan inline dalam Panduan Pengguna IAM.

Resource-based kebijakan

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contohnya termasuk kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Anda harus menentukan principal dalam kebijakan berbasis sumber daya.

Resource-based kebijakan adalah kebijakan sebaris yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACL)

Daftar kontrol akses (ACL) mengendalikan principal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, lihat Gambaran umum daftar kontrol akses (ACL) dalam Panduan Developer Amazon Simple Storage Service.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang dapat mengatur izin maksimum yang diberikan oleh jenis kebijakan yang lebih umum:

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) – Menentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan dalam Panduan Pengguna AWS Organizations .
- Kebijakan kontrol sumber daya (RCP) – Menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat Kebijakan kontrol sumber daya (RCP) dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan ketika beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana cara Amazon VPC bekerja sama dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Amazon EKS, Anda harus memahami fitur-fitur IAM apa saja yang tersedia untuk digunakan bersama Amazon VPC. Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Amazon VPC dan AWS layanan lainnya dengan IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Daftar Isi

- Tindakan
- Sumber daya
- Kunci syarat
- kebijakan berbasis sumber daya Amazon VPC

- Otorisasi berdasarkan tanda
- Peran IAM

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan tindakan yang diizinkan atau ditolak. Untuk beberapa tindakan, Anda dapat menentukan sumber daya dan syarat apakah suatu tindakan diizinkan atau ditolak. Amazon VPC men-support tindakan, sumber daya, dan kunci syarat tertentu. Untuk mempelajari semua elemen yang Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan IAM JSON dalam Panduan Pengguna IAM.

Tindakan

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Sertakan tindakan dalam sebuah kebijakan untuk memberikan izin pelaksanaan operasi terkait.

Amazon VPC berbagi namespace API dengan Amazon EC2. Tindakan kebijakan di Amazon VPC menggunakan prefiks berikut ini sebelum tindakan: `ec2:`. Misalnya, untuk memberikan izin pengguna untuk membuat VPC menggunakan operasi `CreateVpc` API, Anda memberikan akses ke `ec2:CreateVpc` tindakan tersebut. Pernyataan kebijakan harus memuat elemen `Action` atau `NotAction`.

Untuk menetapkan beberapa tindakan dalam satu pernyataan, pisahkan dengan koma seperti yang ditunjukkan dalam contoh berikut.

```
"Action": [
      "ec2:action1",
      "ec2:action2"
]
```

Anda dapat menentukan beberapa tindakan menggunakan wildcard (*). Misalnya, untuk menentukan semua tindakan yang dimulai dengan kata `Describe`, sertakan tindakan berikut.

```
"Action": "ec2:Describe*"
```

Untuk melihat daftar tindakan Amazon VPC, lihat Tindakan yang ditentukan oleh Amazon EC2 di Referensi Otorisasi Layanan.

Sumber daya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Sumber daya VPC memiliki ARN yang ditunjukkan dalam contoh berikut.

```
arn:${Partition}:ec2:${Region}:${Account}:vpc/${VpcId}
```

Misalnya, untuk menentukan VPC `vpc-1234567890abcdef0` dalam pernyataan Anda, gunakan ARN yang ditunjukkan dalam contoh berikut ini.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-1234567890abcdef0"
```

Untuk menentukan semua VPC di Wilayah tertentu milik akun tertentu, gunakan wildcard (*).

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/*"
```

Beberapa tindakan Amazon VPC, seperti membuat sumber daya, tidak dapat dilakukan pada sumber daya tertentu. Dalam kasus tersebut, Anda harus menggunakan wildcard (*).

```
"Resource": "*"
```

Banyak tindakan API Amazon EC2 yang melibatkan beberapa sumber daya. Untuk menentukan beberapa sumber daya dalam satu pernyataan tunggal, pisahkan ARN dengan koma.

```
"Resource": [
```

```
        "resource1",
        "resource2"
]
```

Untuk melihat daftar jenis sumber daya Amazon VPC dan ARN-nya, lihat Jenis sumber daya yang ditentukan oleh Amazon EC2 di Referensi Otorisasi Layanan.

Kunci syarat

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Condition` menentukan ketika pernyataan dieksekusi berdasarkan kriteria yang ditetapkan. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Semua tindakan Amazon EC2 mendukung kunci syarat `aws:RequestedRegion` dan `ec2:Region`. Untuk informasi selengkapnya, lihat Contoh: Membatasi akses ke Wilayah tertentu.

Amazon VPC menentukan pengaturan kunci syaratnya sendiri dan juga men-support penggunaan beberapa kunci syarat global. Untuk melihat daftar kunci kondisi Amazon VPC, lihat Kunci kondisi untuk Amazon EC2 di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya mana Anda dapat menggunakan kunci kondisi, lihat Tindakan yang ditentukan oleh Amazon EC2.

kebijakan berbasis sumber daya Amazon VPC

Resource-based kebijakan adalah dokumen kebijakan JSON yang menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya Amazon VPC dan dalam kondisi apa.

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan seluruh akun atau entitas IAM di akun lain sebagai prinsipal di kebijakan berbasis sumber daya. Menambahkan principal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berada di AWS akun yang berbeda, Anda juga harus memberikan izin entitas utama untuk mengakses sumber daya. Berikan izin dengan melampirkan kebijakan berbasis identitas ke entitas tersebut. Namun, jika kebijakan berbasis sumber daya memberikan akses ke principal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Otorisasi berdasarkan tanda

Anda dapat melampirkan tag ke sumber daya Amazon VPC atau meneruskan tag dalam sebuah permintaan. Untuk mengontrol akses berdasarkan tag, Anda memberikan informasi tag di elemen https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_condition.html kondisi kebijakan menggunakan kunci kondisi. Untuk informasi selengkapnya, lihat Memberikan izin untuk menandai sumber daya selama pembuatan di Panduan Pengguna Amazon EC2.

Untuk melihat contoh kebijakan berbasis identitas untuk membatasi akses ke sumber daya berdasarkan tag pada sumber daya tersebut, lihat Meluncurkan instans ke VPC tertentu.

Peran IAM

Peran IAM adalah entitas di dalam Anda Akun AWS yang memiliki izin tertentu.

Gunakan kredensial sementara

Anda dapat menggunakan kredensial sementara untuk masuk dengan gabungan, menjalankan IAM role, atau menjalankan peran lintas akun. Anda mendapatkan kredentif keamanan sementara dengan memanggil operasi AWS STS API seperti AssumeRole atau GetFederationToken.

Amazon VPC men-support penggunaan kredensial sementara.

Service-linked peran

Service-linked peran memungkinkan AWS layanan mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Service-linked peran muncul di akun IAM Anda dan dimiliki oleh layanan. Administrator IAM dapat melihat tetapi tidak dapat menyunting izin untuk peran tertaut layanan.

Transit Gateway men-support peran yang tertaut dengan layanan.

Peran layanan

Fitur ini memungkinkan layanan untuk menerima peran layanan atas nama Anda. Peran ini mengizinkan layanan untuk mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Peran layanan muncul di akun IAM Anda dan dimiliki oleh akun tersebut. Ini berarti administrator IAM dapat mengubah izin untuk peran ini. Namun, melakukan hal itu dapat merusak fungsionalitas layanan.

Amazon VPC men-support peran layanan untuk log alur. Saat Anda membuat log alur, Anda harus memilih peran yang memungkinkan layanan log aliran mengakses CloudWatch Log. Untuk informasi selengkapnya, lihat the section called “Peran IAM untuk menerbitkan log alur ke Log CloudWatch”.

Contoh kebijakan Amazon VPC

Secara default, peran IAM tidak memiliki izin untuk membuat atau memodifikasi sumber daya VPC. Mereka juga tidak dapat melakukan tugas menggunakan Konsol Manajemen AWS, AWS CLI, atau AWS API. Administrator IAM harus membuat kebijakan IAM yang memberikan izin peran untuk melakukan operasi API tertentu pada sumber daya tertentu yang mereka butuhkan. Administrator kemudian harus melampirkan kebijakan tersebut ke peran IAM yang memerlukan izin tersebut.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM di Panduan Pengguna IAM.

Daftar Isi

- Praktik terbaik kebijakan
- Gunakan konsol Amazon VPC
- Buat sebuah VPC dengan subnet publik
- Modifikasi dan hapus sumber daya VPC
- Mengelola grup keamanan
- Mengelola aturan grup keamanan
- Luncurkan instans ke dalam subnet tertentu
- Meluncurkan instans ke VPC tertentu
- Blokir akses publik ke VPC dan subnet
- Contoh kebijakan Amazon VPC tambahan

Praktik terbaik kebijakan

Identity-based kebijakan menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Amazon VPC di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa terendah — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan terkel AWS ola

yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.

- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan kondisi untuk memberikan akses ke tindakan layanan jika digunakan melalui tindakan tertentu Layanan AWS, seperti CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan dengan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) — Jika Anda memiliki skenario yang memerlukan pengguna IAM atau pengguna root Akun AWS, aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Amankan akses API dengan MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM dalam Panduan Pengguna IAM.

Gunakan konsol Amazon VPC

Untuk mengakses konsol Amazon VPC, Anda harus memiliki satu set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Amazon VPC di AWS akun Anda. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana dimaksudkan untuk entitas (peran IAM) dengan kebijakan tersebut.

Kebijakan berikut memberikan izin peran untuk mencantumkan sumber daya di konsol VPC, tetapi tidak untuk membuat, memperbarui, atau menghapusnya.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeClassicLinkInstances",
                "ec2:DescribeClientVpnEndpoints",
                "ec2:DescribeCustomerGateways",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeEgressOnlyInternetGateways",
                "ec2:DescribeFlowLogs",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeManagedPrefixLists",
                "ec2:DescribeMovingAddresses",
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePrefixLists",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroupReferences",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeStaleSecurityGroups",
```

```
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeTrafficMirrorFilters",
                "ec2:DescribeTrafficMirrorSessions",
                "ec2:DescribeTrafficMirrorTargets",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeTransitGatewayVpcAttachments",
                "ec2:DescribeTransitGatewayRouteTables",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcEndpointConnectionNotifications",
                "ec2:DescribeVpcEndpointConnections",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:GetManagedPrefixListAssociations",
                "ec2:GetManagedPrefixListEntries"
            ],
            "Resource": "*"
        }
    ]
}
```

Anda tidak perlu mengizinkan izin konsol minimum untuk peran yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang cocok dengan operasi API yang perlu dilakukan peran tersebut.

Buat sebuah VPC dengan subnet publik

Contoh berikut memungkinkan peran untuk membuat VPC, subnet, tabel rute, dan gateway internet. Peran juga dapat melampirkan gateway internet ke VPC dan membuat rute dalam tabel rute. T `ec2:ModifyVpcAttribute` indakan ini memungkinkan peran untuk mengaktifkan nama host DNS untuk VPC, sehingga setiap instance yang diluncurkan ke VPC menerima nama host DNS.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateInternetGateway",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:ModifyVpcAttribute"
      ],
      "Resource": "*"
    }
   ]
}
```

Kebijakan sebelumnya juga memungkinkan peran untuk membuat VPC di konsol Amazon VPC.

Modifikasi dan hapus sumber daya VPC

Anda mungkin ingin mengontrol sumber daya VPC yang dapat diubah atau dihapus oleh peran. Misalnya, kebijakan berikut memungkinkan peran bekerja dengan dan menghapus tabel rute yang memiliki tag`Purpose=Test`. Kebijakan ini juga menetapkan bahwa peran hanya dapat menghapus gateway internet yang memiliki tag`Purpose=Test`. Peran tidak dapat bekerja dengan tabel rute atau gateway internet yang tidak memiliki tag ini.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteInternetGateway",
```

```
            "Resource": "arn:aws:ec2:*:*:internet-gateway/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Purpose": "Test"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteRouteTable",
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": "arn:aws:ec2:*:*:route-table/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Purpose": "Test"
                }
            }
        }
    ]
}
```

Mengelola grup keamanan

Kebijakan berikut mengizinkan peran untuk mengelola grup keamanan. Pernyataan pertama memungkinkan peran untuk menghapus grup keamanan apa pun dengan tag `Stack=test` dan untuk mengelola aturan masuk dan keluar untuk grup keamanan apa pun dengan tag. `Stack=test` Pernyataan kedua membutuhkan peran untuk menandai grup keamanan apa pun yang mereka buat dengan tag`Stack=Test`. Pernyataan ketiga memungkinkan peran untuk membuat tag saat membuat grup keamanan. Pernyataan keempat memungkinkan peran untuk melihat grup keamanan dan aturan grup keamanan apa pun. Pernyataan kelima memungkinkan peran untuk membuat grup keamanan dalam VPC.

> **Note**
>
> Kebijakan ini tidak dapat digunakan oleh AWS CloudFormation layanan untuk membuat grup keamanan dengan tag yang diperlukan. Jika Anda menghapus kondisi pada `ec2:CreateSecurityGroup` tindakan yang memerlukan tag, kebijakan akan berfungsi.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup",
                "ec2:ModifySecurityGroupRules",
                "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
            ],
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Stack": "test"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Stack": "test"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "Stack"
                }
```

```
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSecurityGroup"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeVpcs",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:vpc/*"
        }
    ]
}
```

Untuk mengizinkan peran mengubah grup keamanan yang terkait dengan instance, tambahkan `ec2:ModifyInstanceAttribute` tindakan ke kebijakan Anda.

Untuk mengizinkan peran mengubah grup keamanan untuk antarmuka jaringan, tambahkan `ec2:ModifyNetworkInterfaceAttribute` tindakan ke kebijakan Anda.

Mengelola aturan grup keamanan

Kebijakan berikut memberikan izin peran untuk melihat semua grup keamanan dan aturan grup keamanan, menambah dan menghapus aturan masuk dan keluar untuk grup keamanan untuk VPC tertentu, dan mengubah deskripsi aturan untuk VPC tertentu. Pernyataan pertama menggunakan kunci syarat `ec2:Vpc` untuk membatasi cakupan izin untuk VPC tertentu.

Pernyataan kedua memberikan izin peran untuk menjelaskan semua grup keamanan, aturan grup keamanan, dan tag. Ini memungkinkan peran untuk melihat aturan grup keamanan untuk memodifikasinya.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
                "ec2:ModifySecurityGroupRules"
            ],
            "Resource": "arn:aws:ec2:us-east-1:123456789012:security-group/*",
            "Condition": {
                "ArnEquals": {
                    "ec2:Vpc": "arn:aws:ec2:us-
east-1:123456789012:vpc/vpc-1234567890abcdef0"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeTags"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifySecurityGroupRules"
            ],
```

```
            "Resource": "arn:aws:ec2:us-east-1:123456789012:security-group-rule/
*"
        }
    ]
}
```

Luncurkan instans ke dalam subnet tertentu

Kebijakan berikut memberikan izin peran untuk meluncurkan instans ke subnet tertentu dan menggunakan grup keamanan tertentu dalam permintaan. Kebijakan melakukan ini dengan menentukan ARN untuk subnet dan ARN untuk grup keamanan. Jika peran mencoba meluncurkan instance ke subnet yang berbeda atau menggunakan grup keamanan yang berbeda, permintaan akan gagal (kecuali kebijakan atau pernyataan lain memberikan izin peran untuk melakukannya).

Kebijakan ini juga memberikan izin untuk menggunakan sumber daya antarmuka jaringan. Saat meluncurkan ke subnet, `RunInstances` permintaan membuat antarmuka jaringan utama secara default, sehingga peran memerlukan izin untuk membuat sumber daya ini saat meluncurkan instance.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:us-east-1::image/ami-*",
                "arn:aws:ec2:us-east-1:123456789012:instance/*",
                "arn:aws:ec2:us-
east-1:123456789012:subnet/subnet-1234567890abcdef0",
                "arn:aws:ec2:us-east-1:123456789012:network-interface/*",
                "arn:aws:ec2:us-east-1:123456789012:volume/*",
                "arn:aws:ec2:us-east-1:123456789012:key-pair/*",
                "arn:aws:ec2:us-east-1:123456789012:security-
group/sg-0abcdef1234567890"
            ]
        }
    ]
}
```

Meluncurkan instans ke VPC tertentu

Kebijakan berikut memberikan izin peran untuk meluncurkan instans ke subnet apa pun dalam VPC tertentu. Kebijakan tersebut dapat berbuat demikian dengan menerapkan kunci syarat (`ec2:Vpc`) ke sumber daya subnet.

Kebijakan ini juga memberikan izin peran untuk meluncurkan instans hanya menggunakan AMI yang memiliki tag "`department=dev`".

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:123456789012:subnet/*",
            "Condition": {
                "ArnEquals": {
                    "ec2:Vpc": "arn:aws:ec2:us-
east-1:123456789012:vpc/vpc-1234567890abcdef0"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/department": "dev"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:us-east-1:123456789012:instance/*",
                "arn:aws:ec2:us-east-1:123456789012:volume/*",
                "arn:aws:ec2:us-east-1:123456789012:network-interface/*",
```

```
                "arn:aws:ec2:us-east-1:123456789012:key-pair/*",
                "arn:aws:ec2:us-east-1:123456789012:security-group/*"
            ]
        }
    ]
}
```

Blokir akses publik ke VPC dan subnet

Contoh kebijakan berikut memberikan izin peran untuk bekerja dengan fitur VPC Block Public Access (BPA) untuk memblokir akses publik ke sumber daya di VPC dan subnet.

Contoh 1 - Izinkan akses baca-saja ke pengaturan seluruh akun VPC BPA dan pengecualian VPC BPA.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "VPCBPAReadOnlyAccess",
      "Action": [
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeVpcBlockPublicAccessExclusions"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Contoh 2 - Izinkan akses baca dan tulis penuh ke pengaturan seluruh akun VPC BPA dan pengecualian BPA VPC.

JSON

```
{
  "Version":"2012-10-17",
```

```
  "Statement": [
    {
      "Sid": "VPCBPAFullAccess",
      "Action": [
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeVpcBlockPublicAccessExclusions",
        "ec2:ModifyVpcBlockPublicAccessOptions",
        "ec2:CreateVpcBlockPublicAccessExclusion",
        "ec2:ModifyVpcBlockPublicAccessExclusion",
        "ec2:DeleteVpcBlockPublicAccessExclusion"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Contoh 3 - Izinkan akses ke semua API EC2 kecuali memodifikasi pengaturan BPA VPC dan membuat pengecualian.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "EC2FullAccess",
            "Action": [
                "ec2:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "VPCBPAPartialAccess",
            "Action": [
                "ec2:ModifyVpcBlockPublicAccessOptions",
                "ec2:CreateVpcBlockPublicAccessExclusion"
            ],
            "Effect": "Deny",
            "Resource": "*"
```

```
        }
    ]
}
```

Contoh kebijakan Amazon VPC tambahan

Anda dapat menemukan contoh tambahan kebijakan IAM yang terkait dengan Amazon VPC dalam dokumentasi berikut:

- Daftar awalan terkelola
- Pencerminan lalu lintas
- Gerbang transit
- Titik akhir VPC dan layanan titik akhir VPC ()AWS PrivateLink
- Pengintaian VPC

Pecahkan masalah identitas dan akses Amazon VPC

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan mengatasi masalah umum yang mungkin Anda temui saat bekerja menggunakan Amazon VPC dan IAM.

Masalah

- Saya tidak berwenang untuk melakukan tindakan di Amazon VPC
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang-orang di luar saya AWS akun untuk mengakses sumber daya Amazon VPC saya

Saya tidak berwenang untuk melakukan tindakan di Amazon VPC

Jika member Konsol Manajemen AWS itahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, maka Anda harus menghubungi administrator Anda untuk mendapatkan bantuan. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Contoh kesalahan berikut terjadi ketika pengguna `mateojackson` IAM mencoba menggunakan konsol untuk melihat detail tentang subnet tetapi milik peran IAM yang tidak memiliki izin. `ec2:DescribeSubnets`

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:DescribeSubnets on resource: subnet-id
```

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakan untuk memungkinkannya mengakses subnet.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan tersebut, kebijakan Anda harus diperbarui untuk memungkinkan Anda meneruskan peran ke Amazon VPC.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan itu alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi saat pengguna IAM bernama `marymajor` mencoba menggunakan konsol tersebut untuk melaksanakan tindakan di Amazon VPC. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang-orang di luar saya AWS akun untuk mengakses sumber daya Amazon VPC saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah Amazon VPC men-support fitur-fitur ini, lihat Bagaimana cara Amazon VPC bekerja sama dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM lainnya Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyedi Akun AWS akan akses milik pihak ketiga di Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

AWS kebijakan terkelola untuk Amazon Virtual Private Cloud

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS kebijakan terkelola dirancang untuk memberikan izin untuk banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan ter AWS kelola mungkin tidak memberikan izin hak istimewa terkecil untuk kasus penggunaan spesifik Anda karena kebijakan tersebut tersedia untuk digunakan semua AWS pelanggan. Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan ter AWS kelola ketika yang baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat Kebijakan terkelola AWS dalam Panduan Pengguna IAM.

AWS kebijakan yang dikelola: AmazonVPCFullAccess

Anda dapat melampirkan kebijakan `AmazonVPCFullAccess` ke identitas IAM Anda. Kebijakan ini memberikan izin yang memungkinkan akses penuh ke Amazon VPC.

Untuk melihat izin kebijakan ini, lihat AmazonVPCFullAccess di Referensi Kebijakan AWS Terkelola.

AWS kebijakan yang dikelola: AmazonVPCReadOnlyAccess

Anda dapat melampirkan kebijakan `AmazonVPCReadOnlyAccess` ke identitas IAM Anda. Kebijakan ini memberikan izin akses baca saja ke Amazon VPC.

Untuk melihat izin kebijakan ini, lihat AmazonVPCReadOnlyAccess di Referensi Kebijakan AWS Terkelola.

AWS kebijakan yang dikelola: AmazonVPCCrossAccountNetworkInterfaceOperations

Anda dapat melampirkan kebijakan `AmazonVPCCrossAccountNetworkInterfaceOperations` ke identitas IAM Anda. Kebijakan ini memberikan izin yang memungkinkan identitas untuk membuat antarmuka jaringan dan melampirkannya ke sumber daya lintas akun.

Untuk melihat izin kebijakan ini, lihat AmazonVPCCrossAccountNetworkInterfaceOperations di Referensi Kebijakan AWS Terkelola.

AWS kebijakan yang dikelola: AWSServiceRoleForNATGateway

Anda dapat melampirkan kebijakan `AWSServiceRoleForNATGateway` ke identitas IAM Anda. Kebijakan ini memberikan izin yang memungkinkan identitas bekerja atas nama Anda untuk secara otomatis menskalakan Gerbang NAT regional.

Untuk melihat izin kebijakan ini, lihat AWSServiceRoleForNATGateway di Referensi Kebijakan AWS Terkelola.

Amazon VPC memperbarui ke AWS kebijakan terkelola

Lihat detail tentang pembaruan kebijakan ter AWS kelola untuk Amazon VPC sejak layanan ini mulai melacak perubahan ini pada Maret 2021.

Ubah	Deskripsi	Tanggal
the section called “AmazonVPCFullAccess” — Permbaruan ke kebijakan yang sudah ada	Tindakan ditambahkan ke kebijakan AWSIPAMServiceRolePolicy terkelola (ec2:ModifyManagedPrefixList,ec2:DescribeManagedPrefixLists, danec2:GetManagedPrefixListEntries) untuk	Oktober 31, 2025

Ubah	Deskripsi	Tanggal
	mengaktifkan IPAM mengubah dan membaca daftar awalan terkelola.	
the section called “AWSServiceRoleForNATGateway ” – Kebijakan baru	AWSServiceRoleForNATGateway Kebijakan baru memungkinkan identitas untuk secara otomatis menskalakan NAT Gateway regional.	November 19, 2025
the section called “AmazonVPCFullAccess” – Pembaruan ke kebijakan yang ada	MenambahkanAssociateSecurityGroupVpc,DescribeSecurityGroupVpcAssociations, dan DisassociateSecurityGroupVpc tindakan, yang memungkinkan Anda untuk mengaitkan, memisahkan, dan melihat asosiasi grup keamanan dengan VPC.	Desember 9, 2024
the section called “AmazonVPCReadOnlyAccess” – Pembaruan ke kebijakan yang ada	Menambahkan DescribeSecurityGroupVpcAssociations tindakan, yang memungkinkan Anda untuk melihat asosiasi grup keamanan dengan VPC.	Desember 9, 2024
the section called “AmazonVPCFullAccess” – Pembaruan ke kebijakan yang ada	Menambahkan GetSecurityGroupsForVpc tindakan, yang memungkinkan Anda untuk mendapatkan grup keamanan yang dapat digunakan di VPC Anda.	Februari 8, 2024

Ubah	Deskripsi	Tanggal
the section called “AmazonVPCReadOnlyAccess” – Pembaruan ke kebijakan yang ada	Menambahkan GetSecurityGroupsForVpc tindakan, yang memungkinkan Anda untuk mendapatkan grup keamanan yang dapat digunakan di VPC Anda.	Februari 8, 2024
the section called “AmazonVPCCrossAccountNetworkInterfaceOperations” – Pembaruan ke kebijakan yang ada	Menambahkan UnassignIpv6Addresses tindakan AssignIpv6Addresses dan, yang memungkinkan Anda untuk mengelola alamat IPv6 yang terkait dengan antarmuka jaringan.	25 September 2023
the section called “AmazonVPCReadOnlyAccess” – Pembaruan ke kebijakan yang ada	Menambahkan DescribeSecurityGroupRules tindakan, yang memungkinkan Anda untuk melihat aturan grup keamanan.	2 Agustus 2021
the section called “AmazonVPCFullAccess” – Pembaruan ke kebijakan yang ada	Menambahkan ModifySecurityGroupRules tindakan DescribeSecurityGroupRules dan, yang memungkinkan Anda untuk melihat dan memodifikasi aturan grup keamanan.	2 Agustus 2021
the section called “AmazonVPCFullAccess” – Pembaruan ke kebijakan yang ada	Tindakan tambahan untuk gateway operator, kumpulan IPv6, gateway lokal, dan tabel rute gateway lokal.	23 Juni 2021

Ubah	Deskripsi	Tanggal
the section called “AmazonVPCReadOnlyAccess” – Pembaruan ke kebijakan yang ada	Tindakan tambahan untuk gateway operator, kumpulan IPv6, gateway lokal, dan tabel rute gateway lokal.	23 Juni 2021

Menggunakan peran terkait layanan untuk VPC

Amazon VPC menggunakan peran terkait AWS Identity and Access Management layanan (IAM). Peran terkait layanan adalah jenis peran IAM unik yang ditautkan langsung ke VPC. Service-linked peran telah ditentukan sebelumnya oleh VPC dan menyertakan semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan VPC lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. VPC mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya VPC yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi sumber daya VPC Anda karena Anda tidak dapat menghapus izin untuk mengakses sumber daya secara tidak sengaja.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat AWS layanan yang bekerja dengan IAM dan cari layanan yang memiliki Ya di kolom peran. Service-linked Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Service-linked izin peran untuk VPC

VPC menggunakan peran terkait layanan bernama AWSServiceRoleForNATGateway — Peran terkait layanan ini memungkinkan Amazon VPC mengalokasikan alamat IP Elastic atas nama Anda untuk secara otomatis menskalakan NAT Gateway regional, untuk mengaitkan dan memisahkan IP Elastic Anda yang ada ke Gerbang NAT regional sesuai permintaan Anda, dan untuk menjelaskan Antarmuka Jaringan untuk mengidentifikasi infrastruktur yang ada agar secara otomatis diperluas ke Zona Ketersediaan baru.

Per AWSServiceRoleForNATGateway an terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `ec2-nat-gateway.amazonaws.com`

Kebijakan izin peran yang dinam AWSNATGatewayServiceRolePolicy ai memungkinkan VPC menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: `AllocateAddress` pada EIP yang Dikelola Layanan untuk mengalokasikan EIP atas nama Anda. Service Managed EIP menangani penandaan berikutnya dengan tag yang dikelola layanan dan ReleaseAddress secara otomatis.
- Tindakan: `AssociateAddress` pada alamat IP Elastic yang sudah ada sebelumnya untuk mengaitkannya secara manual ke NAT Gateway regional Anda atas permintaan Anda.
- Tindakan: `DisassociateAddress` pada alamat IP Elastic yang sudah ada sebelumnya untuk menghapusnya dari NAT Gateway regional atas permintaan Anda.
- Tindakan: `DescribeAddresses` untuk mendapatkan informasi Alamat IP Publik dari EIP yang disediakan pelanggan pada asosiasi.
- Tindakan: `DescribeNetworkInterface` pada Antarmuka Jaringan Anda yang ada untuk secara otomatis mengidentifikasi Zona Ketersediaan tempat infrastruktur Anda berada untuk secara otomatis menskalakan ke zona baru.

Anda harus mengonfigurasi izin untuk mengizinkan pengguna, grup, atau peran Anda membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat izin Service-linked peran di Panduan Pengguna IAM.

Membuat peran terkait layanan untuk VPC

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat NAT Gateway dengan Mode Ketersediaan “regional” di Konsol Manajemen AWS, AWS CLI, atau AWS API, VPC membuat peran terkait layanan untuk Anda.

> **Important**
>
> Peran tertaut layanan ini dapat muncul di akun Anda jika Anda menyelesaikan tindakan di layanan lain yang menggunakan fitur yang disupport oleh peran ini. Selain itu, jika Anda menggunakan layanan VPC sebelum 1 Januari 2017, ketika mulai mendukung peran terkait layanan, maka VPC membuat peran tersebut AWSServiceRoleForNATGateway di akun Anda. Untuk mempelajari lebih lanjut, lihat Peran baru muncul di saya Akun AWS.

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda membuat NAT Gateway dengan Mode Ketersediaan “regional”, VPC membuat peran terkait layanan untuk Anda lagi.

Anda juga dapat menggunakan konsol IAM untuk membuat peran terkait layanan dengan kasus penggunaan. AWSServiceRoleForNATGateway Di AWS API AWS CLI atau, buat peran terkait layanan dengan nama `ec2-nat-gateway.amazonaws.com` layanan. Untuk informasi selengkapnya, lihat Membuat peran tertaut layanan dalam Panduan Pengguna IAM. Jika Anda menghapus peran tertaut layanan ini, Anda dapat mengulang proses yang sama untuk membuat peran tersebut lagi.

Mengedit peran terkait layanan untuk VPC

VPC tidak mengizinkan Anda mengedit peran terkait AWSServiceRoleForNATGateway layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin merujuk peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran terkait layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk VPC

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami merekomendasikan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Tetapi, Anda harus membersihkan sumber daya peran terkait layanan sebelum menghapusnya secara manual.

> **Note**
>
> Jika layanan VPC menggunakan peran saat Anda mencoba menghapus sumber daya, penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus sumber daya VPC yang digunakan oleh AWSServiceRoleForNATGateway

- Hapus semua Gerbang NAT regional di semua Wilayah tempat Gerbang tersebut telah digunakan.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, AWS CLI, atau AWS API untuk menghapus peran terkait AWSServiceRoleForNATGateway layanan. Untuk informasi selengkapnya, lihat Menghapus peran terkait layanan dalam Panduan Pengguna IAM.

Wilayah yang Didukung untuk peran terkait layanan VPC

VPC mendukung penggunaan peran terkait layanan di semua Wilayah tempat layanan tersedia. Untuk informasi selengkapnya, lihat AWS Wilayah dan titik akhir.

VPC tidak mendukung penggunaan peran terkait layanan di setiap Wilayah tempat layanan tersedia. Anda dapat menggunakan AWSServiceRoleForNATGateway peran di Wilayah berikut.

Nama wilayah	Identitas wilayah	Dukungan dalam VPC
US East (Northern Virginia)	us-east-1	Ya
US East (Ohio)	us-east-2	Ya
US West (N. California)	us-west-1	Ya
US West (Oregon)	us-west-2	Ya
Africa (Cape Town)	af-south-1	Ya
Asia Pasifik (Hong Kong)	ap-east-1	Ya
Asia Pasifik (Taipei)	ap-east-2	Ya
Asia Pasifik (Jakarta)	ap-southeast-3	Ya
Asia Pacific (Mumbai)	ap-south-1	Ya
Asia Pasifik (Hyderabad)	ap-south-2	Ya
Asia Pacific (Osaka)	ap-northeast-3	Ya
Asia Pacific (Seoul)	ap-northeast-2	Ya
Asia Pacific (Singapore)	ap-southeast-1	Ya

Nama wilayah	Identitas wilayah	Dukungan dalam VPC
Asia Pacific (Sydney)	ap-southeast-2	Ya
Asia Pacific (Tokyo)	ap-northeast-1	Ya
Asia Pacific (Melbourne)	ap-southeast-4	Ya
Asia Pasifik (Malaysia)	ap-southeast-5	Ya
Asia Pasifik (Selandia Baru)	ap-Southeast-6	Ya
Asia Pasifik (Thailand)	ap-Southeast-7	Ya
Canada (Central)	ca-sentral-1	Ya
Kanada Barat (Calgary)	ca-west-1	Ya
Eropa (Frankfurt)	eu-central-1	Ya
Europe (Zurich)	eu-central-2	Ya
Eropa (Irlandia)	eu-west-1	Ya
Eropa (London)	eu-west-2	Ya
Europe (Milan)	eu-south-1	Ya
Eropa (Spanyol)	eu-south-2	Ya
Europe (Paris)	eu-west-3	Ya
Eropa (Stockholm)	eu-north-1	Ya
Israel (Tel Aviv)	il-central-1	Ya
Timur Tengah (Bahrain)	me-south-1	Ya
Timur Tengah (UAE)	me-central-1	Ya
Timur Tengah (Arab Saudi)	me-west-1	Ya

Nama wilayah	Identitas wilayah	Dukungan dalam VPC
Meksiko (Tengah)	mx-sentral-1	Ya
South America (São Paulo)	sa-east-1	Ya
AWS GovCloud (US-East)	us-gov-east-1	Tidak
AWS GovCloud (US-West)	us-gov-west-1	Tidak

Keamanan infrastruktur di Amazon VPC

Sebagai layanan terkelola, Amazon Virtual Private Cloud dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat AWS Keamanan Cloud. Untuk merancang AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infra struktur di Security Pillar AWS Well-Architected Framework.

Anda menggunakan panggilan API yang di AWS publikasikan untuk mengakses Amazon VPC melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Suite Cipher dengan kerahasiaan maju sempurna (PFS) seperti DHE (Ephemeral) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Isolasi jaringan

Virtual Private Cloud (VPC) adalah jaringan virtual di area Anda sendiri yang terisolasi secara logis di AWS Cloud. Gunakan VPC yang terpisah untuk melakukan isolasi terhadap infrastruktur berdasarkan beban kerja atau entitas organisasi.

subnet adalah serangkaian alamat IP di VPC. Saat Anda meluncurkan instans, Anda meluncurkan instans tersebut ke dalam subnet dalam VPC Anda. Gunakan subnet untuk melakukan isolasi terhadap jenjang-jenjang aplikasi Anda (misalnya web, aplikasi, dan basis data) dalam satu VPC. Gunakan subnet privat untuk instans Anda jika instan tersebut tidak dapat diakses secara langsung dari internet.

Anda dapat menggunakannya AWS PrivateLink untuk mengaktifkan sumber daya di VPC Anda untuk terhubung Layanan AWS menggunakan alamat IP pribadi, seolah-olah layanan tersebut dihosting langsung di VPC Anda. Oleh karena itu, Anda tidak perlu menggunakan gateway internet atau perangkat NAT untuk mengakses Layanan AWS.

Mengendalikan lalu lintas jaringan

Pertimbangkan opsi berikut untuk mengontrol lalu lintas jaringan ke sumber daya di VPC Anda, seperti instans EC2:

- Gunakan grup keamanan sebagai mekanisme utama untuk mengontrol akses jaringan ke VPC Anda. Bila perlu, gunakan ACL jaringan untuk menyediakan kontrol jaringan berbutir kasar tanpa status. Grup keamanan lebih fleksibel daripada ACL jaringan, karena kemampuannya untuk melakukan pemfilteran paket stateful dan membuat aturan yang mereferensikan grup keamanan lainnya. ACL jaringan dapat efektif sebagai kontrol sekunder (misalnya, untuk menolak subset lalu lintas tertentu) atau sebagai rel pelindung subnet tingkat tinggi. Juga, karena ACL jaringan berlaku untuk seluruh subnet, mereka dapat digunakan sebagai pertahanan mendalam jika instance pernah diluncurkan tanpa grup keamanan yang benar.
- Gunakan subnet privat untuk instans Anda jika instan tersebut tidak dapat diakses secara langsung dari internet. Gunakan host bastion atau gateway NAT untuk akses internet dari instance di subnet pribadi.
- Konfigurasikan tabel rute subnet dengan rute jaringan minimum untuk mendukung persyaratan konektivitas Anda.
- Pertimbangkan untuk menggunakan grup keamanan tambahan atau antarmuka jaringan untuk mengontrol dan meng-audit lalu lintas pengelolaan instans Amazon EC2 secara terpisah dari lalu lintas aplikasi reguler. Oleh karena itu, Anda dapat menerapkan kebijakan IAM khusus untuk kontrol perubahan, sehingga lebih mudah untuk mengaudit perubahan pada aturan grup keamanan atau skrip verifikasi aturan otomatis. Beberapa antarmuka jaringan juga menyediakan opsi tambahan untuk mengendalikan lalu lintas jaringan, termasuk kemampuan untuk membuat kebijakan routing berbasis host atau menggunakan aturan routing subnet VPC yang berbeda berdasarkan antarmuka jaringan yang ditetapkan ke subnet.
- Gunakan AWS Virtual Private Network atau Direct Connect untuk membuat koneksi pribadi dari jaringan jarak jauh Anda ke VPC Anda. Untuk informasi selengkapnya, lihat opsi konektivitas Network-to-Amazon VPC.
- Gunakan Log Aliran VPC untuk memantau lalu lintas yang menjangkau instans Anda.

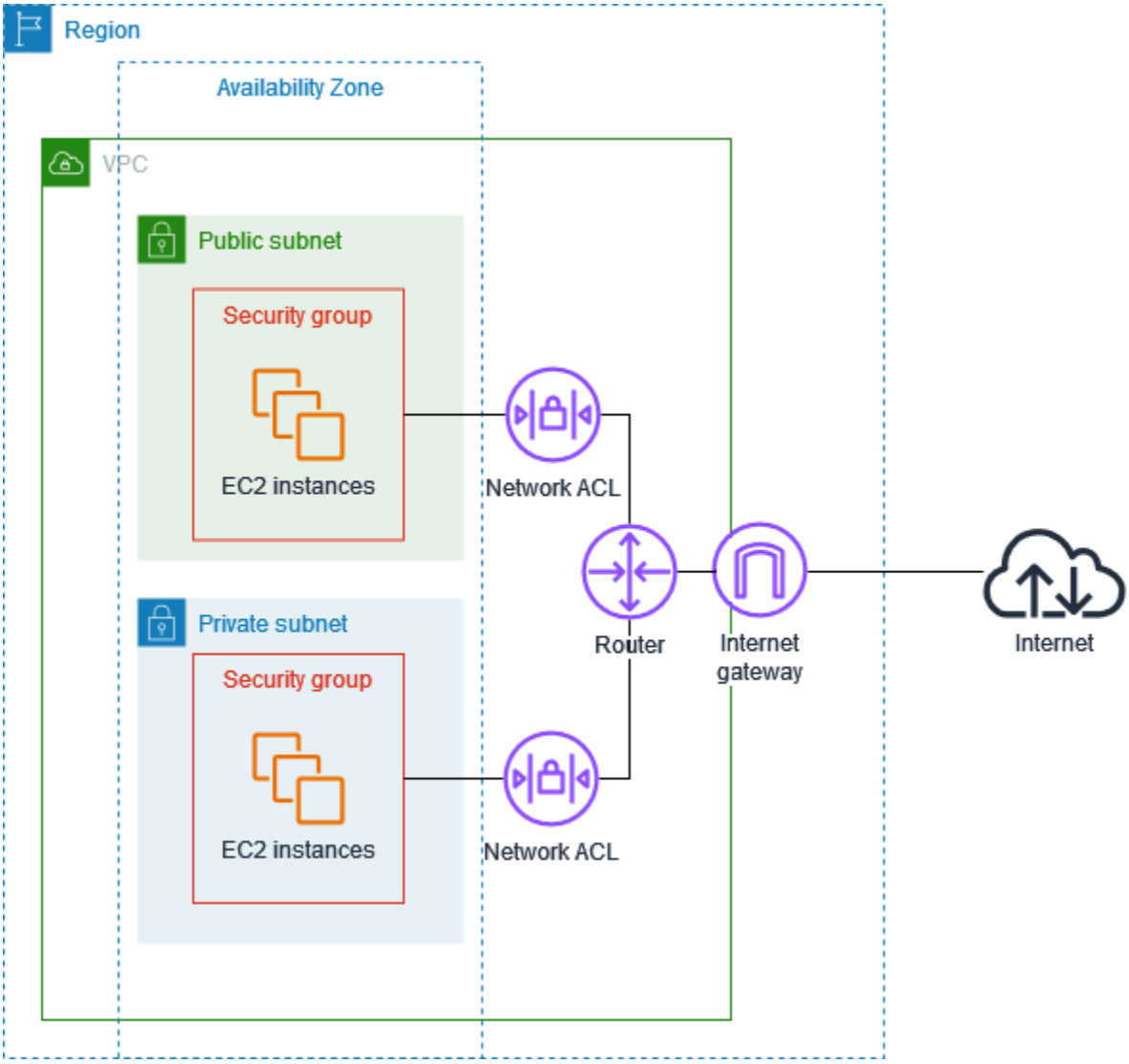
- Gunakan AWS Security Hub CSPM untuk memeriksa aksesibilitas jaringan yang tidak disengaja pada instans Anda.
- Gunakan AWS Network Firewall untuk melindungi subnet di VPC Anda dari ancaman jaringan umum.

Membandingkan grup keamanan dan ACL jaringan

Tabel berikut merangkum dasar perbedaan antara grup keamanan dan ACL jaringan.

Karakteristik	Grup keamanan	ACL jaringan
Tingkat operasi	Tingkat instans	Tingkat subnet
Lingkup	Berlaku untuk semua instance yang terkait dengan grup keamanan	Berlaku untuk semua instance di subnet terkait
Jenis aturan	Izinkan aturan saja	Izinkan dan tolak aturan
Evaluasi aturan	Mengevaluasi semua aturan sebelum memutuskan apakah akan mengizinkan lalu lintas	Mengevaluasi aturan dalam urutan menaik hingga kecocokan untuk lalu lintas ditemukan
Kembali lalu lintas	Diizinkan secara otomatis (stateful)	Harus diizinkan secara eksplisit (tanpa kewarganegaraan)

Diagram berikut menggambarkan lapisan keamanan yang disediakan oleh grup keamanan dan ACL jaringan. Sebagai contoh, lalu lintas dari gateway internet dirutekan ke subnet yang sesuai menggunakan rute dalam tabel perutean. Aturan ACL jaringan yang terkait dengan kontrol subnet yang lalu lintas diperbolehkan untuk subnet. Aturan grup keamanan yang terkait dengan kontrol instans yang lalu lintasnya diizinkan untuk instans tersebut.



Anda dapat mengamankan instans Anda hanya menggunakan grup keamanan. Namun, Anda dapat menambahkan ACL jaringan sebagai lapisan pertahanan tambahan. Untuk informasi selengkapnya, lihat Contoh: Kontrol akses ke instans dalam subnet.

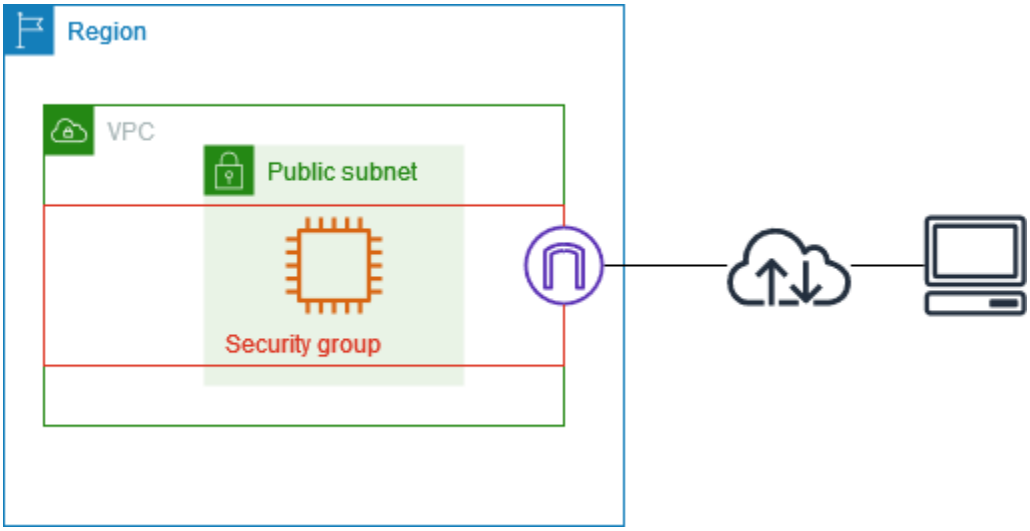
Kontrol lalu lintas ke Anda AWS sumber daya menggunakan grup keamanan

Grup keamanan mengontrol lalu lintas yang diizinkan untuk menjangkau dan meninggalkan sumber daya yang terkait dengannya. Misalnya, setelah Anda mengaitkan grup keamanan dengan instans EC2, grup tersebut akan mengontrol lalu lintas masuk dan keluar untuk instans tersebut.

Saat Anda membuat VPC, ia dilengkapi dengan grup keamanan default. Anda dapat membuat grup keamanan tambahan untuk VPC, masing-masing dengan aturan masuk dan keluar mereka sendiri.

Anda dapat menentukan sumber, rentang port, dan protokol untuk setiap aturan masuk. Anda dapat menentukan tujuan, rentang port, dan protokol untuk setiap aturan keluar.

Diagram berikut menunjukkan VPC dengan subnet, gateway internet, dan grup keamanan. Subnet berisi instance EC2. Grup keamanan ditugaskan ke instance. Grup keamanan bertindak sebagai firewall virtual. Satu-satunya lalu lintas yang mencapai instance adalah lalu lintas yang diizinkan oleh aturan grup keamanan. Misalnya, jika grup keamanan berisi aturan yang mengizinkan lalu lintas ICMP ke instance dari jaringan Anda, maka Anda dapat melakukan ping instans dari komputer Anda. Jika grup keamanan tidak berisi aturan yang mengizinkan lalu lintas SSH, maka Anda tidak dapat terhubung ke instance Anda menggunakan SSH.



Daftar Isi

- Dasar-dasar grup keamanan
- Contoh grup keamanan
- Aturan grup keamanan
- Grup keamanan default untuk VPC Anda
- Membuat grup keamanan untuk VPC Anda
- Mengonfigurasi aturan grup keamanan
- Menghapus grup keamanan
- Mengaitkan grup keamanan dengan beberapa VPC
- Bagikan grup keamanan dengan AWS Organizations

Harga

Tidak ada biaya tambahan untuk menggunakan grup keamanan.

Dasar-dasar grup keamanan

- Anda dapat menetapkan grup keamanan ke sumber daya yang dibuat di VPC yang sama dengan grup keamanan atau ke sumber daya di VPC lain jika menggunakan fitur Asosiasi VPC Grup Keamanan untuk mengaitkan grup keamanan ke VPC lain di Wilayah yang sama. Anda juga dapat menetapkan beberapa grup keamanan ke satu sumber daya.
- Saat Anda membuat grup keamanan, Anda harus memberi nama dan deskripsi untuknya. Aturan-aturan berikut berlaku:
  - Nama grup keamanan harus unik di VPC.
  - Nama grup keamanan tidak peka huruf besar/kecil.
  - Nama dan deskripsi dapat memiliki panjang hingga 255 karakter.
  - Nama dan deskripsi terbatas pada karakter berikut: a-z,, 0-9A-Z, spasi, dan ._-:/() #, @ [] +=&; {}! $*.
  - Ketika nama berisi spasi belakang, kita memangkas spasi di akhir nama. Sebagai contoh, jika Anda memasukkan "Grup Keamanan Pengujian " sebagai namanya, maka kami menyimpannya sebagai "Grup Keamanan Pengujian".
  - Nama grup keamanan tidak dapat dimulai dengan`sg-`.
- Grup keamanan bersifat stateful. Misalnya, jika Anda mengirim permintaan dari instance, lalu lintas respons untuk permintaan tersebut diizinkan untuk mencapai instans terlepas dari aturan grup keamanan masuk. Respons terhadap lalu lintas masuk yang diizinkan diizinkan untuk meninggalkan instance, terlepas dari aturan outbound.
- Grup keamanan tidak menyaring lalu lintas yang ditujukan ke dan dari berikut ini:
  - Layanan Nama Domain Amazon (DNS)
  - Protokol Konfigurasi Host Dinamis (DHCP)
  - Metadata instans Amazon EC2
  - Titik akhir metadata tugas Amazon ECS
  - Aktivasi lisensi untuk instans Windows
  - Layanan Amazon Time Sync
  - Alamat IP cadangan yang digunakan oleh router VPC default
- Ada kuota jumlah grup keamanan yang dapat Anda buat per VPC, jumlah aturan yang dapat Anda tambahkan ke setiap grup keamanan, dan jumlah grup keamanan yang dapat Anda kaitkan dengan antarmuka jaringan.

Untuk informasi selengkapnya, lihat Kuota Amazon VPC.

Praktik terbaik

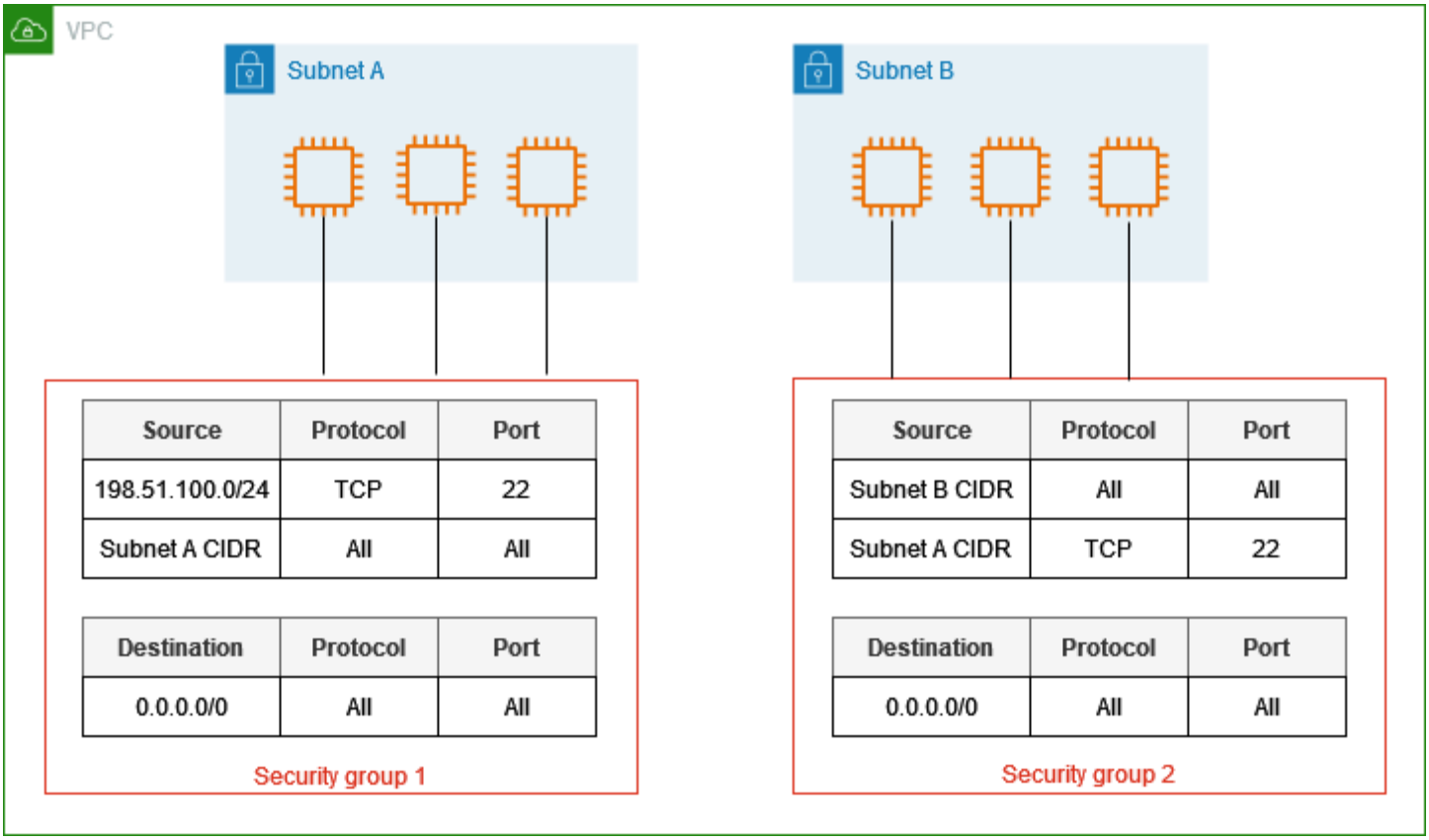
- Otorisasi hanya prinsipal IAM tertentu untuk membuat dan memodifikasi grup keamanan.
- Buat jumlah minimum grup keamanan yang Anda butuhkan, untuk mengurangi risiko kesalahan. Gunakan setiap grup keamanan untuk mengelola akses ke sumber daya yang memiliki fungsi dan persyaratan keamanan yang serupa.
- Saat menambahkan aturan masuk untuk port 22 (SSH) atau 3389 (RDP) sehingga Anda dapat mengakses instans EC2, otorisasi hanya rentang alamat IP tertentu. Jika Anda menentukan 0.0.0.0/0 (IPv4) dan: :/ (IPv6), ini memungkinkan siapa saja untuk mengakses instance Anda dari alamat IP apa pun menggunakan protokol yang ditentukan.
- Jangan membuka rentang port yang besar. Pastikan akses melalui setiap port terbatas pada sumber atau tujuan yang membutuhkannya.
- Pertimbangkan untuk membuat ACL jaringan dengan aturan yang mirip dengan grup keamanan Anda, untuk menambahkan lapisan keamanan tambahan ke VPC Anda. Untuk informasi lebih lanjut tentang perbedaan antara grup keamanan dan ACL jaringan, lihat Membandingkan grup keamanan dan ACL jaringan.

Contoh grup keamanan

Diagram berikut menunjukkan VPC dengan dua grup keamanan dan dua subnet. Instans di subnet A memiliki persyaratan konektivitas yang sama, sehingga mereka terkait dengan grup keamanan 1. Instans di subnet B memiliki persyaratan konektivitas yang sama, sehingga mereka terkait dengan grup keamanan 2. Aturan grup keamanan mengizinkan lalu lintas sebagai berikut:

- Aturan masuk pertama di grup keamanan 1 memungkinkan lalu lintas SSH ke instance di subnet A dari rentang alamat yang ditentukan (misalnya, rentang di jaringan Anda sendiri).
- Aturan masuk kedua dalam grup keamanan 1 memungkinkan instance di subnet A untuk berkomunikasi satu sama lain menggunakan protokol dan port apa pun.
- Aturan inbound pertama di grup keamanan 2 memungkinkan instance di subnet B untuk berkomunikasi satu sama lain menggunakan protokol dan port apa pun.
- Aturan inbound kedua di grup keamanan 2 memungkinkan instance di subnet A untuk berkomunikasi dengan instance di subnet B menggunakan SSH.

- Kedua grup keamanan menggunakan aturan keluar default, yang memungkinkan semua lalu lintas.



Aturan grup keamanan

Aturan grup keamanan mengontrol lalu lintas masuk yang diizinkan untuk mencapai sumber daya yang terkait dengan grup keamanan. Aturan-aturan tersebut juga mengontrol lalu lintas ke luar yang diperbolehkan untuk meninggalkannya.

Anda dapat menambahkan atau menghapus aturan untuk sebuah grup keamanan (juga disebut sebagai memberikan otorisasi atau mencabut akses masuk atau keluar). Suatu aturan berlaku baik untuk lalu lintas masuk (ingress) atau lalu lintas keluar (egress). Anda dapat memberikan akses ke sumber atau tujuan tertentu.

Daftar Isi

- Dasar-dasar aturan grup keamanan
- Komponen aturan grup keamanan
- Referensi grup keamanan
- Ukuran grup keamanan

- Aturan grup keamanan yang kedaluwarsa

Dasar-dasar aturan grup keamanan

Berikut ini adalah karakteristik dari aturan-aturan grup keamanan:

- Anda dapat menentukan untuk mengizinkan aturan, tetapi tidak menolak aturan.
- Saat Anda pertama kali membuat grup keamanan, grup keamanan tersebut tidak memiliki aturan masuk. Oleh karena itu, tidak ada lalu lintas masuk yang diizinkan sampai Anda menambahkan aturan masuk ke grup keamanan.
- Saat pertama kali membuat grup keamanan, grup tersebut memiliki aturan keluar yang memungkinkan semua lalu lintas keluar dari sumber daya. Anda dapat menghapus aturan dan menambahkan aturan keluar yang hanya mengizinkan lalu lintas keluar tertentu. Jika grup keamanan Anda tidak memiliki aturan keluar, lalu lintas keluar tidak diizinkan.
- Saat Anda mengaitkan beberapa grup keamanan dengan sumber daya, aturan dari setiap grup keamanan digabungkan untuk membentuk satu set aturan yang digunakan untuk menentukan apakah akan mengizinkan akses.
- Saat Anda menambahkan, memperbarui, atau menghapus aturan, perubahan diterapkan secara otomatis ke semua sumber daya yang terkait dengan grup keamanan. Untuk petunjuk, lihat Mengonfigurasi aturan grup keamanan.
- Dampak dari beberapa perubahan aturan dapat bergantung pada cara pelacakan lalu lintas yang digunakan. Untuk informasi selengkapnya, lihat Pelacakan koneksi di Panduan Pengguna Amazon EC2.
- Saat Anda membuat aturan grup keamanan, AWS menetapkan ID unik untuk aturan tersebut. Anda dapat menggunakan ID aturan tersebut ketika Anda menggunakan API atau CLI untuk mengubah atau menghapus aturan tersebut.

Batasan

Grup keamanan tidak dapat memblokir permintaan DNS ke atau dari Route 53 Resolver, kadang-kadang disebut sebagai 'alamat IP VPC+2' (lihat Amazon Route 53 Resolver di Panduan Pengembang Amazon Route 53), atau sebagai DNS. AmazonProvided Untuk memfilter permintaan DNS melalui Route 53 Resolver, gunakan Route 53 Resolver DNS Firewall.

Komponen aturan grup keamanan

Berikut ini adalah komponen aturan grup keamanan masuk dan keluar:

- Protocol: Protokol yang akan diizinkan. Protokol yang paling umum adalah 6 (TCP), 17 (UDP), dan 1 (ICMP).
- Port range: Untuk TCP, UDP, atau protokol kustom, ada rentang port yang diizinkan. Anda dapat menentukan satu nomor port (misalnya, `22`), atau rentang nomor port (misalnya, `7000-8000`).
- Tipe dan kode ICMP: Untuk ICMP, jenis dan kode ICMP. Sebagai contoh, gunakan tipe 8 untuk ICMP Echo Request atau tipe 128 untuk ICMPv6 Echo Request. Untuk informasi selengkapnya, lihat A turan untuk ping/ICMP di Panduan Pengguna Amazon EC2.
- Source or destination: Sumber (aturan ke dalam) atau tujuan (aturan ke luar) untuk lalu lintas yang akan diizinkan. Tentukan satu dari yang berikut ini:
  - Satu alamat IPv4. Anda harus menggunakan panjang awalan `/32`. Sebagai contoh, `203.0.113.1/32`.
  - Satu alamat IPv6. Anda harus menggunakan panjang awalan `/128`. Sebagai contoh, `2001:db8:1234:1a00::123/128`.
  - Rentang alamat IPv4, dalam notasi blok CIDR. Sebagai contoh, `203.0.113.0/24`.
  - Rentang alamat IPv6, dalam notasi blok CIDR. Sebagai contoh, `2001:db8:1234:1a00::/64`.
  - ID daftar awalan. Sebagai contoh, `pl-1234abc1234abc123`. Untuk informasi selengkapnya, lihat Daftar prefiks terkelola.
  - ID grup keamanan. Sebagai contoh, `sg-1234567890abcdef0`. Untuk informasi selengkapnya, lihat the section called “Referensi grup keamanan”.
- (Opsional) Deskripsi: Anda dapat menambahkan deskripsi untuk aturan, yang dapat membantu Anda untuk mengidentifikasinya nanti. deskripsi dapat memiliki panjang hingga 255 karakter. Karakter yang diizinkan adalah a-z, A-Z, 0-9, spasi, dan ._-:/() #, @ [] +=; {}! $*.

Sebagai contoh, lihat A turan grup keamanan untuk kasus penggunaan yang berbeda di Panduan Pengguna Amazon EC2.

Referensi grup keamanan

Saat Anda menentukan grup keamanan sebagai sumber atau tujuan untuk aturan, aturan akan memengaruhi semua instance yang terkait dengan grup keamanan. Instans dapat berkomunikasi

dalam arah yang ditentukan, menggunakan alamat IP pribadi dari instance, melalui protokol dan port yang ditentukan.

Misalnya, berikut ini mewakili aturan masuk untuk grup keamanan yang mereferensikan grup keamanan sg-0abcdef1234567890. Aturan ini memungkinkan lalu lintas SSH masuk dari instance yang terkait dengan sg-0abcdef1234567890.

Sumber	Protokol	Rentang port
sg-0abcdef1234567890	TCP	22

Saat mereferensikan grup keamanan dalam aturan grup keamanan, perhatikan hal berikut:

- Anda dapat mereferensikan grup keamanan dalam aturan masuk grup keamanan lain jika salah satu dari berikut ini benar:
  - Grup keamanan dikaitkan dengan VPC yang sama.
  - Ada koneksi peering antara VPC yang terkait dengan grup keamanan.
  - Ada gateway transit antara VPC yang terkait dengan grup keamanan.
- Anda dapat mereferensikan grup keamanan dalam aturan keluar jika salah satu dari berikut ini benar:
  - Grup keamanan dikaitkan dengan VPC yang sama.
  - Ada koneksi peering antara VPC yang terkait dengan grup keamanan.
- Tidak ada aturan dari grup keamanan yang direferensikan ditambahkan ke grup keamanan yang mereferensikannya.
- Untuk aturan masuk, instans EC2 yang terkait dengan grup keamanan dapat menerima lalu lintas masuk dari alamat IP pribadi dari antarmuka jaringan untuk instans EC2 yang terkait dengan grup keamanan yang direferensikan.
- Untuk aturan keluar, instans EC2 yang terkait dengan grup keamanan dapat mengirim lalu lintas keluar ke alamat IP pribadi dari antarmuka jaringan untuk instans EC2 yang terkait dengan grup keamanan yang direferensikan.
- Kami tidak memberikan otorisasi terhadap grup keamanan yang direferensikan dalam tindakan berikut:`AuthorizeSecurityGroupIngress`,`AuthorizeSecurityGroupEgress`,`RevokeSecurityG` dan`RevokeSecurityGroupEgress`. Kami hanya memeriksa apakah grup keamanan ada. Ini menghasilkan yang berikut:

- Menentukan grup keamanan yang direferensikan dalam kebijakan IAM untuk tindakan ini tidak berpengaruh.
- Ketika grup keamanan yang direferensikan dimiliki oleh akun lain, akun pemilik tidak menerima CloudTrail peristiwa untuk tindakan ini.

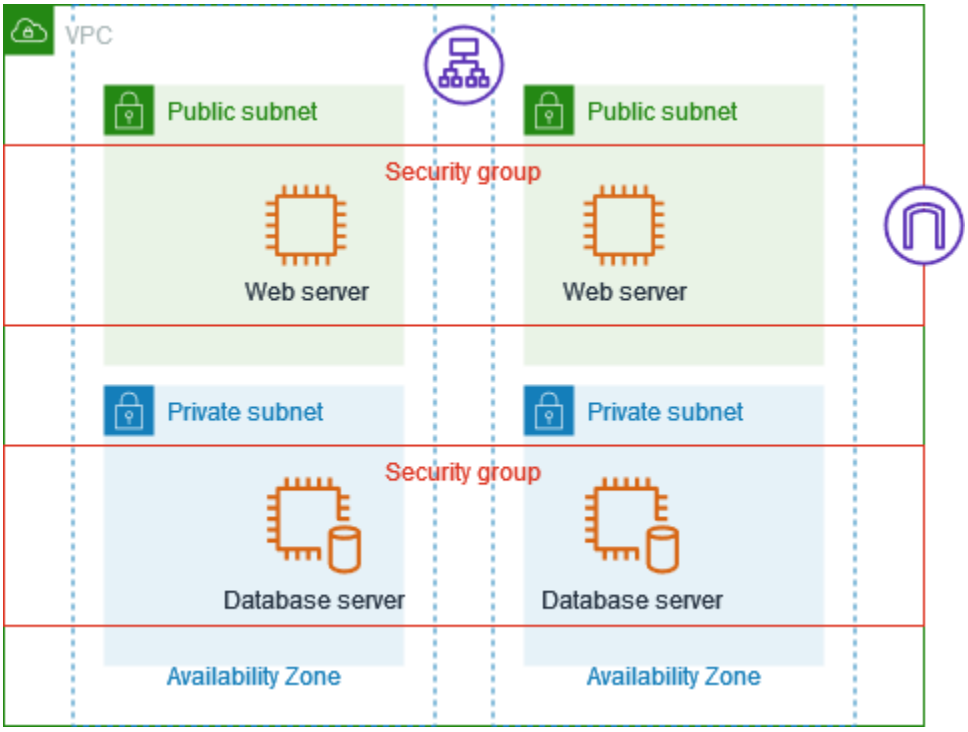
Batasan

Jika Anda mengonfigurasi rute untuk meneruskan lalu lintas antara dua instans di subnet yang berbeda melalui perangkat middlebox, Anda harus memastikan bahwa grup keamanan untuk kedua instans tersebut mengizinkan lalu lintas mengalir di antara instans. Grup keamanan untuk setiap instance harus mereferensikan alamat IP pribadi dari instance lain atau rentang CIDR dari subnet yang berisi instance lain sebagai sumber. Jika Anda mereferensikan grup keamanan instans lain sebagai sumbernya, hal ini tidak akan mengizinkan lalu lintas mengalir di antara instans.

Contoh

Diagram berikut menunjukkan VPC dengan subnet di dua Availability Zone, gateway internet, dan Application Load Balancer. Setiap Availability Zone memiliki subnet publik untuk server web dan subnet pribadi untuk server database. Ada grup keamanan terpisah untuk penyeimbang beban, server web, dan server database. Buat aturan grup keamanan berikut untuk mengizinkan lalu lintas.

- Tambahkan aturan ke grup keamanan load balancer untuk mengizinkan lalu lintas HTTP dan HTTPS dari internet. Sumbernya adalah 0.0.0. 0/0.
- Tambahkan aturan ke grup keamanan untuk server web untuk mengizinkan lalu lintas HTTP dan HTTPS hanya dari penyeimbang beban. Sumbernya adalah grup keamanan untuk penyeimbang beban.
- Tambahkan aturan ke grup keamanan untuk server database untuk mengizinkan permintaan database dari server web. Sumbernya adalah grup keamanan untuk server web.



Ukuran grup keamanan

Jenis sumber atau tujuan menentukan bagaimana setiap aturan dihitung terhadap jumlah maksimum aturan yang dapat Anda miliki per grup keamanan.

- Aturan yang mereferensikan blok CIDR dihitung sebagai satu aturan.
- Aturan yang mereferensikan grup keamanan lain dihitung sebagai satu aturan, tidak peduli ukuran grup keamanan yang direferensikan.
- Aturan yang mereferensikan daftar awalan yang dikelola pelanggan dihitung sebagai ukuran maksimum daftar awalan. Misalnya, jika ukuran maksimum daftar awalan Anda adalah 20, aturan yang mereferensikan daftar awalan ini dihitung sebagai aturan 20.
- Aturan yang mereferensi AWS kan daftar awalan yang dikelola dihitung sebagai bobot daftar awalan. Misalnya, jika bobot daftar awalan adalah 10, aturan yang mereferensikan daftar awalan ini dihitung sebagai 10 aturan. Untuk informasi selengkapnya, lihat the section called “Available AWS Daftar prefiks yang dikelola”.

Aturan grup keamanan yang kedaluwarsa

Jika VPC Anda memiliki koneksi peering VPC dengan VPC lain, atau jika menggunakan VPC yang dibagikan oleh akun lain, aturan grup keamanan di VPC Anda dapat mereferensikan grup

keamanan di VPC peer atau VPC bersama tersebut. Hal ini memungkinkan sumber daya yang terkait dengan grup keamanan yang direferensikan dan sumber daya yang terkait dengan grup keamanan referensi untuk berkomunikasi satu sama lain. Untuk informasi selengkapnya, lihat Memperbarui grup keamanan Anda untuk mereferensikan grup keamanan rekan di Panduan Peering Amazon VPC.

Jika Anda memiliki aturan grup keamanan yang mereferensikan grup keamanan di VPC peer atau VPC bersama, aturan tersebut ditandai sebagai basi saat grup keamanan yang direferensikan dihapus atau koneksi peering VPC dihapus. Anda dapat menghapus aturan grup keamanan kedaluwarsa seperti yang Anda lakukan terhadap aturan grup keamanan lainnya.

Grup keamanan default untuk VPC Anda

VPC default Anda dan VPC apa pun yang Anda buat dilengkapi dengan grup keamanan default. Nama grup keamanan default adalah "default".

Sebaiknya buat grup keamanan untuk sumber daya tertentu atau grup sumber daya alih-alih menggunakan grup keamanan default. Namun, jika Anda tidak mengaitkan grup keamanan dengan beberapa sumber daya pada saat pembuatan, kami mengaitkannya dengan grup keamanan default. Misalnya, jika Anda tidak menentukan grup keamanan saat meluncurkan instans EC2, kami mengaitkan instans dengan grup keamanan default untuk VPC-nya.

Dasar-dasar grup keamanan default

- Anda dapat mengubah aturan untuk grup keamanan default.
- Anda tidak dapat menghapus grup keamanan default. Jika Anda mencoba menghapus grup keamanan default, kami akan menampilkan kode kesalahan berikut: `Client.CannotDelete`.

Peraturan default

Tabel berikut menjelaskan aturan masuk default untuk grup keamanan default.

Sumber	Protokol	Rentang Port	Deskripsi
sg-1234567890abcdef0	Semua	Semua	Mengizinkan lalu lintas jalur masuk dari semua sumber daya

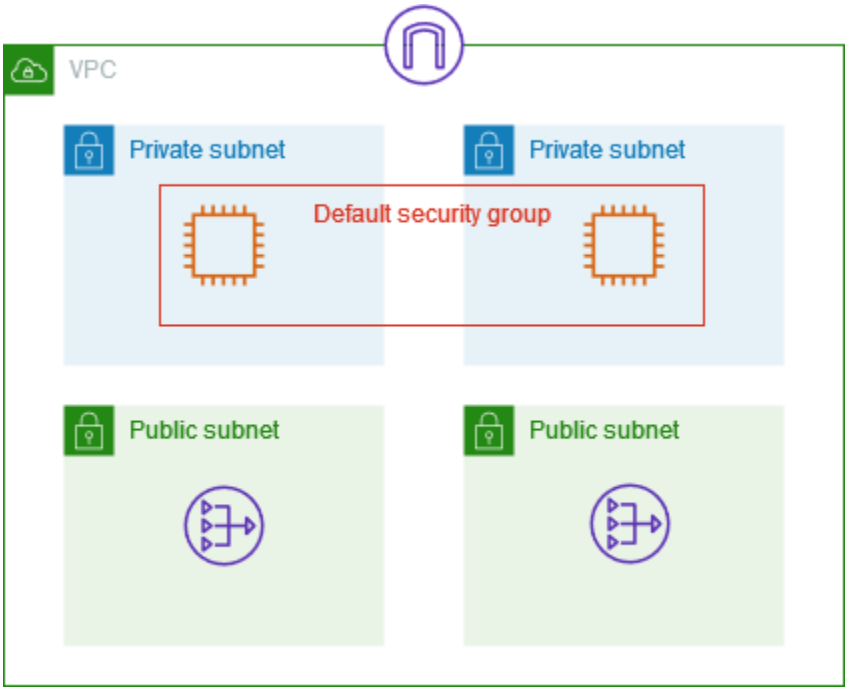
Sumber	Protokol	Rentang Port	Deskripsi
			yang ditetapkan untuk grup keamanan ini. Sumbernya adalah ID dari grup keamanan ini.

Tabel berikut menjelaskan aturan keluar default untuk grup keamanan default.

Tujuan	Protokol	Rentang Port	Deskripsi
0.0.0. 0/0	Semua	Semua	Mengizinkan semua lalu lintas IPv4 ke luar.
::/0	Semua	Semua	Mengizinkan semua lalu lintas IPv6 ke luar. Aturan ini ditambahkan hanya jika VPC Anda memiliki blok CIDR IPv6 yang dikaitkan.

Contoh

Diagram berikut menunjukkan VPC dengan grup keamanan default, gateway internet, dan gateway NAT. Keamanan default hanya berisi aturan defaultnya, dan dikaitkan dengan dua instans EC2 yang berjalan di VPC. Dalam skenario ini, setiap instance dapat menerima lalu lintas masuk dari instance lain pada semua port dan protokol. Aturan default tidak mengizinkan instance menerima lalu lintas dari gateway internet atau gateway NAT. Jika instans Anda harus menerima lalu lintas tambahan, sebaiknya buat grup keamanan dengan aturan yang diperlukan dan mengaitkan grup keamanan baru dengan instans alih-alih grup keamanan default.



Membuat grup keamanan untuk VPC Anda

Virtual Private Cloud (VPC) Anda dilengkapi dengan grup keamanan default. Anda dapat membuat grup keamanan tambahan. Grup keamanan hanya dapat digunakan dengan sumber daya di VPC yang dibuat.

Secara default, grup keamanan baru dimulai hanya dengan aturan keluar yang memungkinkan semua lalu lintas meninggalkan sumber daya. Anda harus menambahkan aturan-aturan lain untuk mengizinkan lalu lintas ke dalam atau membatasi lalu lintas ke luar. Anda dapat menambahkan aturan saat membuat grup keamanan atau yang lebih baru. Untuk informasi selengkapnya, lihat Aturan grup keamanan.

Izin yang diperlukan

Sebelum Anda mulai, pastikan Anda memiliki izin yang diperlukan. Untuk informasi selengkapnya, lihat berikut ini:

- Mengelola grup keamanan
- Mengelola aturan grup keamanan

Untuk membuat grup keamanan menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.

2. Pada panel navigasi, pilih Grup keamanan.
3. Pilih Buat grup keamanan.
4. Masukkan nama dan deskripsi untuk grup keamanan tersebut. Anda tidak dapat mengubah nama dan deskripsi grup keamanan setelah dibuat.
5. Untuk VPC, pilih VPC tempat Anda akan membuat sumber daya yang akan Anda kaitkan dengan grup keamanan.
6. (Opsional) Untuk menambahkan aturan masuk, pilih aturan masuk. Untuk setiap aturan, pilih Tambahkan aturan dan tentukan protokol, port, dan sumber. Untuk informasi selengkapnya, lihat Mengonfigurasi aturan grup keamanan.
7. (Opsional) Untuk menambahkan aturan keluar, pilih Aturan keluar. Untuk setiap aturan, pilih Tambahkan aturan dan tentukan protokol, port, dan tujuan.
8. (Opsional) Untuk menambahkan tag, pilih Tambahkan tag baru dan masukkan kunci tag dan nilai.
9. Pilih Buat grup keamanan.

Untuk membuat grup keamanan menggunakan AWS CLI

Gunakan perintah create-security-group.

Sebagai alternatif, Anda dapat membuat grup keamanan baru dengan menyalin grup yang sudah ada. Saat Anda menyalin grup keamanan, kami secara otomatis menambahkan aturan masuk dan keluar yang sama dengan grup keamanan asli dan menggunakan VPC yang sama dengan grup keamanan asli. Anda dapat memasukkan nama dan deskripsi untuk grup keamanan baru. Anda dapat memilih VPC yang berbeda secara opsional, dan Anda dapat memodifikasi aturan masuk dan keluar sesuai kebutuhan. Namun, Anda tidak dapat menyalin grup keamanan dari satu Wilayah ke Wilayah lain.

Untuk membuat grup keamanan berdasarkan grup yang sudah ada

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Grup keamanan.
3. Pilih grup keamanan.
4. Pilih T ind akan, Salin ke grup keamanan baru.
5. Masukkan nama dan deskripsi untuk grup keamanan tersebut.
6. (Opsional) Pilih VPC yang berbeda jika diperlukan.

7. (Opsional) Tambahkan, hapus, atau edit aturan grup keamanan sesuai kebutuhan.
8. Pilih Buat grup keamanan.

Mengonfigurasi aturan grup keamanan

Setelah membuat grup keamanan, Anda dapat menambahkan, memperbarui, dan menghapus aturan grup keamanannya. Saat Anda menambahkan, memperbarui, atau menghapus aturan, perubahan secara otomatis diterapkan ke sumber daya yang terkait dengan grup keamanan.

Izin yang diperlukan

Sebelum Anda mulai, pastikan Anda memiliki izin yang diperlukan. Untuk informasi selengkapnya, lihat Mengelola aturan grup keamanan.

Protokol dan Port

- Dengan konsol, ketika Anda memilih jenis yang telah ditentukan, jang kauan Protokol dan Port ditentukan untuk Anda. Untuk memasukkan rentang port, Anda harus memilih salah satu jenis kustom berikut: C ustom TCP atau C ustom UD P.
- Dengan AWS CLI, Anda dapat menambahkan aturan tunggal dengan satu port menggunakan `--port` opsi `--protocol` dan. Untuk menambahkan beberapa aturan, atau aturan dengan rentang port, gunakan `--ip-permissions` opsi sebagai gantinya.

Sumber dan tujuan

- Dengan konsol, Anda dapat menentukan berikut ini sebagai sumber untuk aturan masuk atau tujuan untuk aturan keluar:
  - Kustom — Blok IPv4 CIDR, blok IPv6 CIDR, grup keamanan, atau daftar awalan.
  - Anywhere-IPv4— 0.0.0. 0/0 Blok IPv4 CIDR.
  - Anywhere-IPv6- Blok CIDR IPv6: :/0.
  - IP Saya — Alamat IPv4 publik komputer lokal Anda.
- Dengan AWS CLI, Anda dapat menentukan blok IPv4 CIDR menggunakan `--cidr` opsi atau grup keamanan menggunakan opsi. `--source-group` Untuk menentukan daftar awalan atau blok CIDR IPv6, gunakan opsi. `--ip-permissions`

> **Warning**
>
> Jika Anda memilih Anywhere-IPv4, Anda mengizinkan lalu lintas dari semua alamat IPv4. Jika Anda memilih Anywhere-IPv6, Anda mengizinkan lalu lintas dari semua alamat IPv6. Ini adalah praktik terbaik untuk mengotorisasi hanya rentang alamat IP tertentu yang memerlukan akses ke sumber daya Anda.

Untuk mengkonfigurasi aturan grup keamanan menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Grup keamanan.
3. Pilih grup keamanan.
4. Untuk mengedit aturan masuk, pilih Edit aturan masuk dari Tindakan atau tab Aturan masuk.
   a. Untuk menambahkan aturan, pilih Tambahkan aturan dan masukkan jenis, protokol, port, dan sumber untuk aturan tersebut.

      Jika jenisnya TCP atau UDP, Anda harus memasukkan rentang port untuk mengizinkan. Untuk ICMP kustom, Anda harus memilih jenis ICMP dari Protokol, dan, jika memungkinkan, nama kode dari Rentang port. Untuk jenis lainnya, protokol dan rentang port akan dikonfigurasikan untuk Anda.
   b. Untuk memperbarui aturan, ubah protokol, deskripsi, dan sumbernya sesuai kebutuhan. Namun, Anda tidak dapat mengubah jenis sumber. Misalnya, jika sumbernya adalah blok CIDR IPv4, Anda tidak dapat menentukan blok CIDR IPv6, daftar awalan, atau grup keamanan.
   c. Untuk menghapus aturan, pilih tombol Delete.
5. Untuk mengedit aturan keluar, pilih Edit aturan keluar dari Tindakan atau tab Aturan keluar.
   a. Untuk menambahkan aturan, pilih Tambahkan aturan dan masukkan jenis, protokol, port, dan tujuan untuk aturan tersebut. Anda juga dapat memasukkan deskripsi opsional.

      Jika jenisnya TCP atau UDP, Anda harus memasukkan rentang port untuk mengizinkan. Untuk ICMP kustom, Anda harus memilih jenis ICMP dari Protokol, dan, jika memungkinkan, nama kode dari Rentang port. Untuk jenis lainnya, protokol dan rentang port akan dikonfigurasikan untuk Anda.

b. Untuk memperbarui aturan, ubah protokol, deskripsi, dan sumbernya sesuai kebutuhan. Namun, Anda tidak dapat mengubah jenis sumber. Misalnya, jika sumbernya adalah blok CIDR IPv4, Anda tidak dapat menentukan blok CIDR IPv6, daftar awalan, atau grup keamanan.

c. Untuk menghapus aturan, pilih tombol Delete.

6. Pilih Simpan aturan.

Untuk mengkonfigurasi aturan grup keamanan menggunakan AWS CLI

- Tambah — Gunakan perintah authorize-security-group- ingress dan authorize-security-group-egress. https://docs.aws.amazon.com/cli/latest/reference/ec2/authorize-security-group-egress.html
- Hapus — Gunakan perintah revoke-security-group- ingress dan revoke-security-group-egress. https://docs.aws.amazon.com/cli/latest/reference/ec2/revoke-security-group-egress.html
- Modifikasi — Gunakan perintah modify-security-group-rules, update-security-group-rule-descriptions-ingress, dan update-security-group-rule-descriptions-egress. https://docs.aws.amazon.com/cli/latest/reference/ec2/update-security-group-rule-descriptions-ingress.html https://docs.aws.amazon.com/cli/latest/reference/ec2/update-security-group-rule-descriptions-egress.html

Menghapus grup keamanan

Ketika Anda selesai dengan grup keamanan yang Anda buat, Anda dapat menghapusnya.

Persyaratan

- Grup keamanan tidak dapat dikaitkan dengan sumber daya apa pun.
- Grup keamanan tidak dapat direferensikan oleh aturan di grup keamanan lain.
- Grup keamanan tidak dapat menjadi grup keamanan default untuk VPC.

Untuk menghapus grup keamanan menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Grup keamanan.
3. Pilih grup keamanan lalu pilih Tindakan, Hapus Grup Keamanan.

4. Jika Anda memilih lebih dari satu grup keamanan, Anda akan diminta untuk konfirmasi. Jika beberapa grup keamanan tidak dapat dihapus, kami menampilkan status setiap grup keamanan, yang menunjukkan apakah grup tersebut akan dihapus. Untuk mengonfirmasi penghapusan, masukkan Delete.
5. Pilih Hapus.

Untuk menghapus grup keamanan menggunakan AWS CLI

Gunakan perintah delete-security-group.

Mengaitkan grup keamanan dengan beberapa VPC

Jika Anda memiliki beban kerja yang berjalan di beberapa VPC yang berbagi persyaratan keamanan jaringan, Anda dapat menggunakan fitur Asosiasi VPC Grup Keamanan untuk mengaitkan grup keamanan dengan beberapa VPC di Wilayah yang sama. Ini memungkinkan Anda mengelola dan memelihara grup keamanan di satu tempat untuk beberapa VPC di akun Anda.

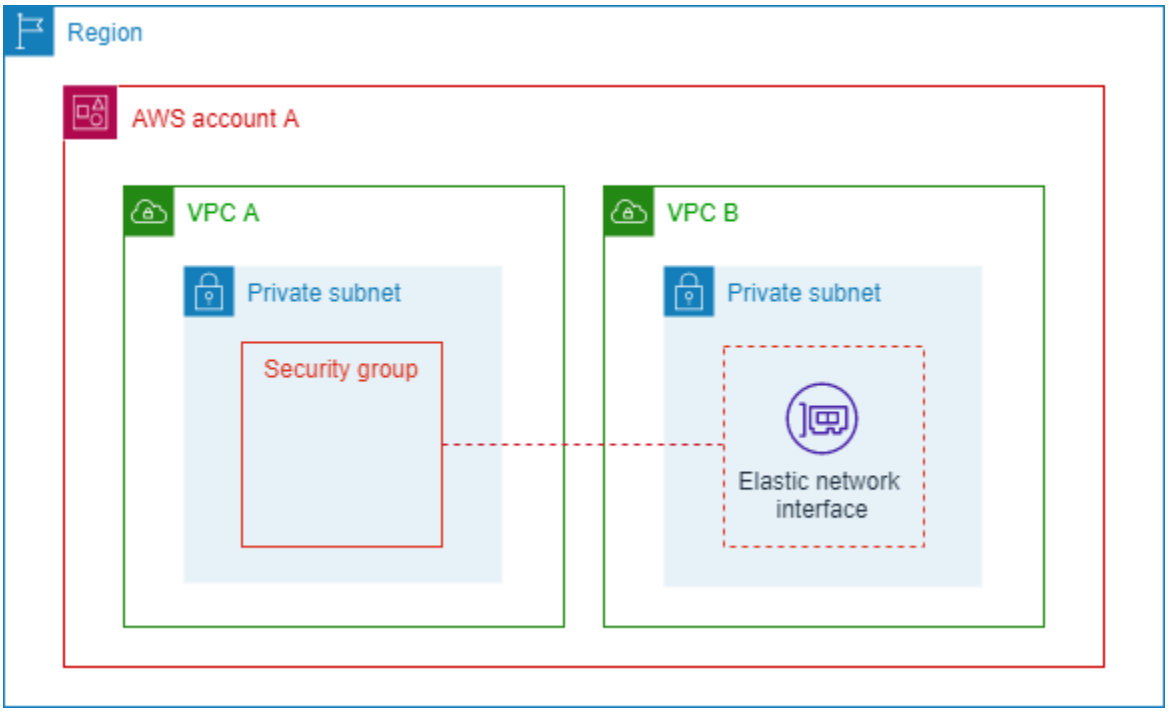


Diagram di atas menunjukkan AWS akun A dengan dua VPC di dalamnya. Setiap VPC memiliki beban kerja yang berjalan di subnet pribadi. Dalam hal ini, beban kerja di subnet VPC A dan B berbagi persyaratan lalu lintas jaringan yang sama, sehingga Akun A dapat menggunakan fitur asosiasi VPC Grup Keamanan untuk mengaitkan grup keamanan di VPC A dengan VPC B.

Pembaruan apa pun yang dilakukan pada grup keamanan terkait secara otomatis diterapkan ke lalu lintas ke beban kerja di subnet VPC B.

Persyaratan fitur Asosiasi VPC Grup Keamanan

- Anda harus memiliki VPC atau memiliki salah satu subnet VPC yang dibagikan dengan Anda untuk mengaitkan grup keamanan dengan VPC.
- VPC dan grup keamanan harus berada di Wilayah yang sama AWS .
- Anda tidak dapat mengaitkan grup keamanan default dengan VPC lain atau mengaitkan grup keamanan dengan VPC default.
- Baik pemilik grup keamanan maupun pemilik VPC dapat melihat asosiasi VPC grup keamanan.

Layanan yang mendukung fitur ini

- Gerbang API Amazon (hanya REST API)
- AWS Auto Scaling
- CloudFormation
- Amazon EC2
- Amazon EFS
- Amazon EKS
- Amazon FSx
- AWS PrivateLink
- Amazon Route 53
- Elastic Load Balancing
  - Penyeimbang Beban Aplikasi
  - Penyeimbang Beban Jaringan

Mengaitkan grup keamanan dengan VPC lain

Bagian ini menjelaskan cara menggunakan Konsol Manajemen AWS dan AWS CLI mengaitkan grup keamanan dengan VPC.

AWS Management Console

Untuk mengaitkan grup keamanan dengan VPC lain

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi kiri, pilih Grup keamanan.
3. Pilih grup keamanan untuk melihat detailnya.
4. Pilih tab asosiasi VPC.
5. Pilih Kaitkan VPC.
6. Di bawah ID VPC, pilih VPC untuk dikaitkan dengan grup keamanan.
7. Pilih Kaitkan VPC.

Command line

Untuk mengaitkan grup keamanan dengan VPC lain

1. Buat asosiasi VPC dengan associ ate-security-group-vpc.
2. Periksa status asosiasi VPC dengan describe-security-group-vpc- association dan tunggu statusnya. `associated`

VPC sekarang dikaitkan dengan grup keamanan.

Setelah Anda menghubungkan VPC dengan grup keamanan, Anda dapat, misalnya, meluncurkan instance ke VPC dan memilih grup keamanan baru ini atau mereferensikan grup keamanan ini dalam aturan grup keamanan yang ada.

Memutuskan hubungan grup keamanan dari VPC lain

Bagian ini menjelaskan cara menggunakan Konsol Manajemen AWS dan AWS CLI memisahkan grup keamanan dari VPC. Anda mungkin ingin melakukan ini jika tujuan Anda adalah menghapus grup keamanan. Grup keamanan tidak dapat dihapus jika mereka terkait. Anda hanya dapat mengasosiasikan grup keamanan jika tidak ada antarmuka jaringan di VPC terkait menggunakan grup keamanan tersebut.

AWS Management Console

Memutuskan hubungan grup keamanan dari VPC

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi kiri, pilih Grup keamanan.
3. Pilih grup keamanan untuk melihat detailnya.
4. Pilih tab asosiasi VPC.
5. Pilih Put uskan hubungan V PC.
6. Di bawah ID VPC, pilih VPC untuk dipisahkan dari grup keamanan.
7. Pilih Put uskan hubungan V PC.
8. Lihat Status dis asosiasi di tab asosiasi VPC dan tunggu statusnya. `disassociated`

Command line

Memutuskan hubungan grup keamanan dari VPC

1. Putuskan hubungan VPC dengan disassociate-security-group-vpc.
2. Periksa status disasosiasi VPC dengan describe-security-group-v pc-association dan tunggu statusnya. `disassociated`

VPC sekarang dipisahkan dengan grup keamanan.

Bagikan grup keamanan dengan AWS Organizations

Fitur Grup Keamanan Bersama memungkinkan Anda berbagi grup keamanan dengan akun AWS Organisasi lain dalam Wil AWS ayah yang sama dan membuat grup keamanan tersedia untuk digunakan oleh akun tersebut.

Diagram berikut menunjukkan bagaimana Anda dapat menggunakan fitur Grup Keamanan Bersama untuk menyederhanakan manajemen grup keamanan di seluruh akun di AWS Organisasi Anda:

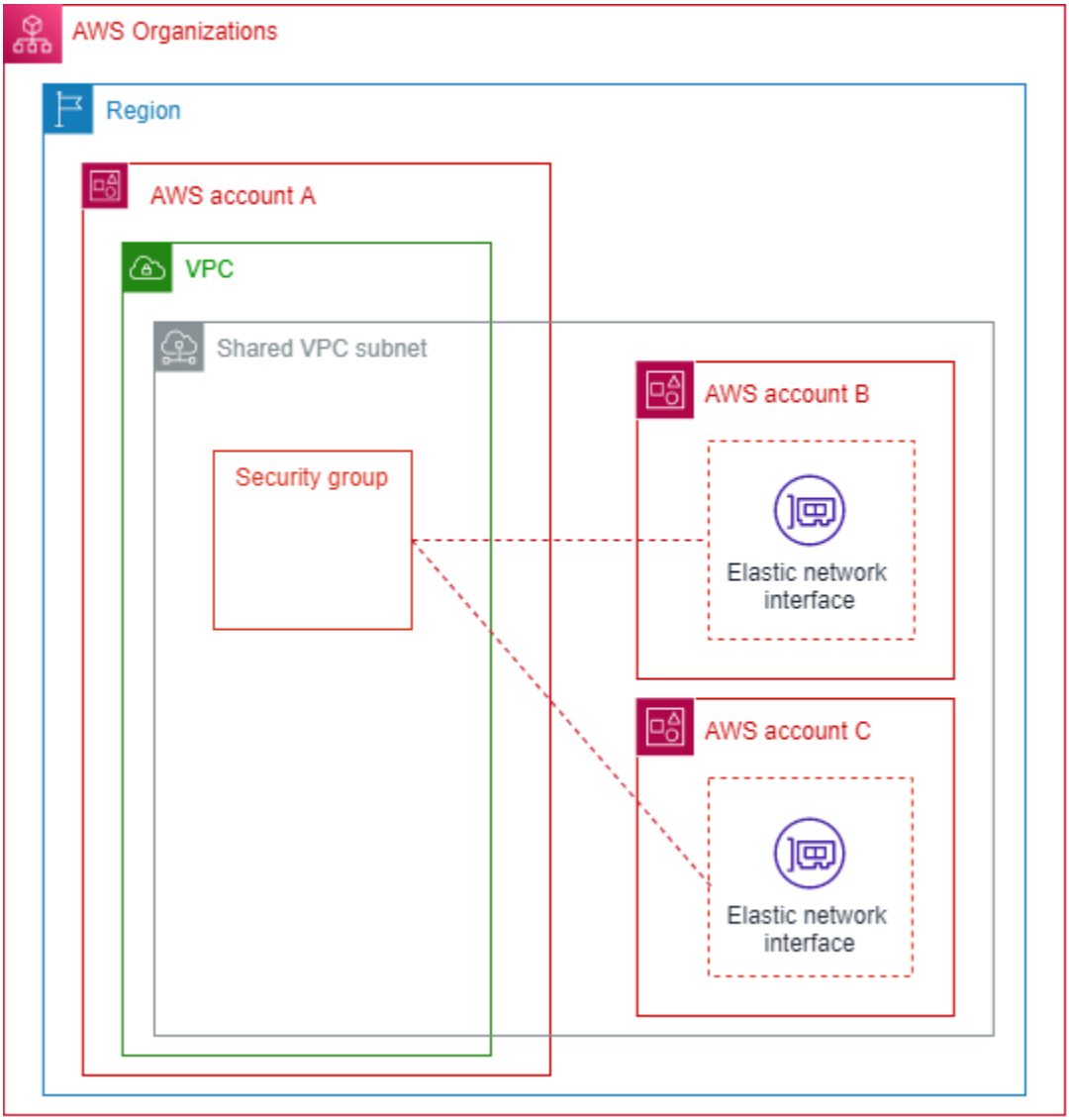


Diagram ini menunjukkan tiga akun yang merupakan bagian dari Organisasi yang sama. Akun A berbagi subnet VPC dengan Akun B dan C. Akun A berbagi grup keamanan dengan Akun B dan C menggunakan fitur Grup Keamanan Bersama. Akun B dan C kemudian menggunakan grup keamanan itu ketika mereka meluncurkan instance di subnet bersama. Ini memungkinkan Akun A untuk mengelola grup keamanan; setiap pembaruan pada grup keamanan berlaku untuk sumber daya yang dijalankan Akun B dan C di subnet VPC bersama.

Persyaratan fitur Grup Keamanan Bersama

- Fitur ini hanya tersedia untuk akun di Organisasi yang sama di AWS Organisasi. Berbagi sumber daya harus diaktifkan di AWS Organisasi.
- Akun yang berbagi grup keamanan harus memiliki VPC dan grup keamanan.

- Anda tidak dapat berbagi grup keamanan default.
- Anda tidak dapat berbagi grup keamanan yang berada di VPC default.
- Akun peserta dapat membuat grup keamanan di VPC bersama tetapi mereka tidak dapat berbagi grup keamanan tersebut.
- Seperangkat izin minimum diperlukan bagi prinsipal IAM untuk berbagi grup keamanan. AWS RAM Gunakan kebijakan IAM `AmazonEC2FullAccess` dan `AWSResourceAccessManagerFullAccess` dikelola untuk memastikan kepala sekolah IAM Anda memiliki izin yang diperlukan untuk berbagi dan menggunakan grup keamanan bersama. Jika Anda menggunakan kebijakan IAM khusus, `ec2:DeleteResourcePolicy` tindakan `c2:PutResourcePolicy` dan diperlukan. Ini adalah tindakan IAM khusus izin. Jika prinsipal IAM tidak memiliki izin ini diberikan, kesalahan akan terjadi saat mencoba berbagi grup keamanan menggunakan. AWS RAM

Layanan yang mendukung fitur ini

- Amazon API Gateway
- Amazon EC2
- Amazon ECS
- Amazon EFS
- Amazon EKS
- Amazon EMR
- Amazon FSx
- Amazon ElastiCache
- AWS Elastic Beanstalk
- AWS Glue
- Amazon MQ
- Amazon SageMaker AI
- Elastic Load Balancing
  - Penyeimbang Beban Aplikasi
  - Penyeimbang Beban Jaringan

Bagaimana fitur ini memengaruhi kuota yang ada

Kuota grup keamanan berlaku. Namun, untuk kuota 'Grup keamanan per antarmuka jaringan', jika peserta menggunakan grup milik dan bersama pada antarmuka jaringan Elastic (ENI), kuota minimum pemilik dan peserta berlaku.

Contoh untuk menunjukkan bagaimana kuota dipengaruhi oleh fitur ini:

- Kuota akun pemilik: 4 grup keamanan per antarmuka
- Kuota akun peserta: 5 grup keamanan per antarmuka.
- Pemilik berbagi grup SG-O1, SG-O2, SG-O3, SG-O4, SG-O5 dengan peserta. Peserta sudah memiliki grup mereka sendiri di VPC: SG-P1,, SG-P2, SG-P3 SG-P4, SG-P5.
- Jika peserta membuat ENI dan hanya menggunakan grup miliknya, mereka dapat mengaitkan semua 5 grup keamanan (SG-P1, SG-P2, SG-P3, SG-P4, SG-P5) karena itulah kuota mereka.
- Jika peserta membuat ENI dan menggunakan grup bersama di dalamnya, mereka hanya dapat mengaitkan hingga 4 grup. Dalam hal ini, kuota untuk ENI semacam itu adalah minimum kuota pemilik dan peserta. Kemungkinan konfigurasi yang valid akan terlihat seperti ini:
  - SG-O1, SG-P1, SG-P2, SG-P3
  - SG-O1, SG-O2, SG-O3, SG-O4

Berbagi grup keamanan

Bagian ini menjelaskan cara menggunakan Konsol Manajemen AWS dan AWS CLI untuk berbagi grup keamanan dengan akun lain di Organisasi Anda.

AWS Management Console

Untuk berbagi grup keamanan

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi kiri, pilih Grup keamanan.
3. Pilih grup keamanan untuk melihat detailnya.
4. Pilih tab Berbagi.
5. Pilih Bagikan grup keamanan.
6. Pilih Buat berbagi sumber daya. Akibatnya, AWS RAM konsol terbuka di mana Anda akan membuat berbagi sumber daya untuk grup keamanan.
7. Masukkan Nama untuk berbagi sumber daya.

8. Di bawah Sumber Daya - opsional, pilih Grup Keamanan.
9. Pilih grup keamanan. Grup keamanan tidak dapat menjadi grup keamanan default dan tidak dapat dikaitkan dengan VPC default.
10. Pilih Berikutnya.
11. Tinjau tindakan yang akan diizinkan untuk dilakukan oleh kepala sekolah dan pilih Ber ikutnya.
12. Di bawah Prinsip - opsional, pilih Izinkan berbagi hanya dalam organisasi Anda.
13. Di bawah Prinsi pal, pilih salah satu jenis utama berikut dan masukkan nomor yang sesuai:
    - AWS akun: Nomor rekening akun di Organisasi Anda.
    - Organisasi: ID AWS Organisasi.
    - Unit organisasi (OU): ID OU dalam Organisasi.
    - Peran IAM: ARN dari peran IAM. Akun yang membuat peran harus menjadi anggota Organisasi yang sama dengan akun yang membuat berbagi sumber daya ini.
    - Pengguna IAM: ARN pengguna IAM. Akun yang membuat pengguna harus menjadi anggota Organisasi yang sama dengan akun yang membuat berbagi sumber daya ini.
    - Prinsip layanan: Anda tidak dapat berbagi grup keamanan dengan prinsipal layanan.
14. Pilih Tambahkan.
15. Pilih Berikutnya.
16. Pilih Buat berbagi sumber daya.
17. Di bawah Sumber daya bersama, tunggu untuk melihat Status `Associated`. Jika ada kegagalan asosiasi grup keamanan, itu mungkin karena salah satu batasan yang tercantum di atas. Lihat detail grup keamanan dan tab Berbagi pada halaman detail untuk melihat pesan apa pun yang terkait dengan alasan grup keamanan mungkin tidak dapat dibagikan.
18. Kembali ke daftar grup keamanan konsol VPC.
19. Pilih grup keamanan yang Anda bagikan.
20. Pilih tab Berbagi. Sumber AWS RAM daya Anda harus terlihat di sana. Jika tidak, pembuatan berbagi sumber daya mungkin gagal dan Anda mungkin perlu membuatnya kembali.

Command line

Untuk berbagi grup keamanan

1. Anda harus terlebih dahulu membuat berbagi sumber daya untuk grup keamanan yang ingin Anda bagikan AWS RAM. Untuk langkah-langkah tentang cara membuat berbagi sumber daya dengan AWS RAM menggunakan AWS CLI, lihat Membuat berbagi sumber daya AWS RAM di Panduan AWS RAM Pengguna
2. Untuk melihat asosiasi berbagi sumber daya yang dibuat, gunakan asosiasi get- resource-share-.

Grup keamanan sekarang dibagikan. Anda dapat memilih grup keamanan saat meluncurkan instance EC2 di subnet bersama dalam VPC yang sama.

Berhenti berbagi grup keamanan

Bagian ini menjelaskan cara menggunakan Konsol Manajemen AWS dan AWS CLI menghentikan berbagi grup keamanan dengan akun lain di Organisasi Anda.

AWS Management Console

Menghentikan berbagi grup keamanan

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi kiri, pilih Grup keamanan.
3. Pilih grup keamanan untuk melihat detailnya.
4. Pilih tab Berbagi.
5. Pilih berbagi sumber daya grup keamanan dan pilih Ber henti berbagi.
6. Pilih Ya, berhenti berbagi.

Command line

Menghentikan berbagi grup keamanan

Hapus berbagi sumber daya dengan delete- resource-share.

Grup keamanan tidak lagi dibagikan. Setelah pemilik berhenti berbagi grup keamanan, aturan berikut berlaku:

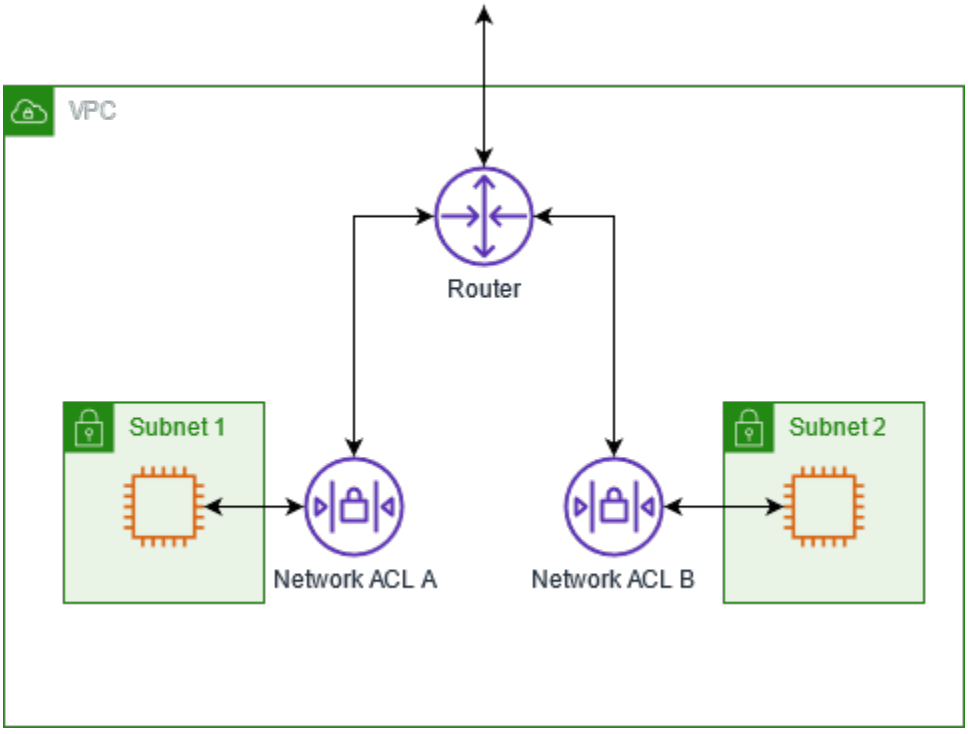
- Peserta yang ada Elastic Network Interfaces (ENI) terus mendapatkan pembaruan aturan grup keamanan apa pun yang dibuat untuk grup keamanan yang tidak dibagikan. Penghentian berbagi hanya mencegah peserta membuat asosiasi baru dengan grup yang tidak dibagikan.
- Peserta tidak dapat lagi mengaitkan grup keamanan yang tidak dibagikan dengan ENI apa pun yang mereka miliki.
- Peserta dapat menjelaskan dan menghapus ENI yang masih terkait dengan grup keamanan yang tidak dibagikan.
- Jika peserta masih memiliki ENI yang terkait dengan grup keamanan yang tidak dibagikan, pemilik tidak dapat menghapus grup keamanan yang tidak dibagikan. Pemilik hanya dapat menghapus grup keamanan setelah peserta memisahkan (menghapus) grup keamanan dari semua ENI mereka.
- Peserta tidak dapat meluncurkan instans EC2 baru menggunakan ENI yang terkait dengan grup keamanan yang tidak dibagikan.

Kontrol lalu lintas subnet dengan daftar kontrol akses jaringan

Daftar kontrol akses jaringan (ACL) memungkinkan atau menolak lalu lintas masuk atau keluar tertentu di tingkat subnet. Anda dapat menggunakan ACL jaringan default untuk VPC Anda, atau Anda dapat membuat ACL jaringan khusus untuk VPC Anda dengan aturan yang mirip dengan aturan grup keamanan Anda. ACL jaringan khusus menambahkan lapisan keamanan tambahan ke VPC Anda.

Tidak ada biaya tambahan untuk menggunakan ACL jaringan.

Diagram berikut menunjukkan VPC dengan dua subnet. Setiap subnet memiliki ACL jaringan. Ketika lalu lintas memasuki VPC (misalnya, dari VPC yang diintip, koneksi VPN, atau internet), router mengirimkan lalu lintas ke tujuannya. Jaringan ACL A menentukan lalu lintas mana yang ditujukan untuk subnet 1 yang diizinkan masuk ke subnet 1, dan lalu lintas mana yang ditujukan untuk lokasi di luar subnet 1 diizinkan meninggalkan subnet 1. Demikian pula, jaringan ACL B menentukan lalu lintas mana yang diizinkan masuk dan keluar dari subnet 2.



Untuk informasi tentang perbedaan antara grup keamanan dan ACL jaringan, lihatMembandingkan grup keamanan dan ACL jaringan.

Daftar Isi

- Dasar-dasar ACL jaringan
- Aturan ACL Jaringan
- ACL jaringan default untuk VPC
- ACL jaringan khusus untuk VPC Anda
- Path MTU Discovery dan ACL jaringan
- Membuat ACL jaringan untuk VPC anda
- Kelola asosiasi ACL jaringan untuk VPC Anda
- Menghapus ACL jaringan untuk VPC Anda
- Contoh: Kontrol akses ke instans dalam subnet

Dasar-dasar ACL jaringan

Berikut ini adalah hal-hal dasar yang perlu diketahui tentang ACL jaringan sebelum Anda mulai.

Asosiasi ACL jaringan

- Setiap subnet di VPC Anda harus dihubungkan dengan sebuah ACL jaringan. Jika Anda tidak secara eksplisit mengaitkan subnet dengan ACL jaringan, subnet secara otomatis dikaitkan dengan ACL jaringan default.
- Anda dapat membuat ACL jaringan khusus dan mengaitkannya dengan subnet untuk mengizinkan atau menolak lalu lintas masuk atau keluar tertentu di tingkat subnet.
- Anda dapat menghubungkan ACL jaringan dengan beberapa subnet. Namun, subnet hanya dapat dihubungkan ke satu ACL jaringan saja dalam satu waktu. Ketika Anda menghubungkan ACL jaringan dengan sebuah subnet, hubungan sebelumnya akan dihapus.

Aturan ACL Jaringan

- ACL jaringan memiliki aturan masuk dan aturan keluar. Ada ku ota (atau batasan) untuk jumlah aturan yang dapat Anda miliki per ACL jaringan. Setiap aturan dapat mengizinkan atau menolak lalu lintas. Setiap aturan memiliki angka dari 1 hingga 32766. Kami mengevaluasi aturan secara berurutan, dimulai dengan aturan bernomor terendah, ketika memutuskan apakah mengizinkan atau menolak lalu lintas. Jika lalu lintas cocok dengan aturan, aturan diterapkan dan kami tidak mengevaluasi aturan tambahan apa pun. Kami menyarankan Anda memulai dengan membuat aturan secara bertahap (misalnya, kenaikan 10 atau 100) sehingga Anda dapat menyisipkan aturan baru nanti, jika diperlukan.
- Kami mengevaluasi aturan ACL jaringan ketika lalu lintas masuk dan meninggalkan subnet, bukan seperti yang dirutekan dalam subnet.
- NACL tidak memiliki kewargan egaraan, yang berarti bahwa informasi tentang lalu lintas yang dikirim atau diterima sebelumnya tidak disimpan. Jika, misalnya, Anda membuat aturan NACL untuk mengizinkan lalu lintas masuk tertentu ke subnet, respons terhadap lalu lintas tersebut tidak diizinkan secara otomatis. Ini berbeda dengan cara kerja kelompok keamanan. Grup keamanan bersifat stateful, yang berarti bahwa informasi tentang lalu lintas yang dikirim atau diterima sebelumnya disimpan. Jika, misalnya, grup keamanan mengizinkan lalu lintas masuk ke instans EC2, respons secara otomatis diizinkan terlepas dari aturan grup keamanan keluar.

Batasan

- Ada kuota (juga dikenal sebagai batas) untuk ACL jaringan. Untuk informasi selengkapnya, lihat ACL jaringan.

- ACL jaringan tidak dapat memblokir permintaan DNS ke atau dari Route 53 Resolver (juga dikenal sebagai alamat IP VPC+2 atau DNS). AmazonProvided Untuk memfilter permintaan DNS melalui Route 53 Resolver, Anda dapat mengaktifkan Route 53 Resolver DNS Firewall.
- ACL jaringan tidak dapat memblokir lalu lintas ke Layanan Metadata Instance (IMDS). Untuk mengelola akses ke IMDS, lihat Meng onfigurasi opsi metadata instans di Panduan Pengguna Amazon EC2.
- ACL jaringan tidak menyaring lalu lintas yang ditujukan ke dan dari yang berikut:
  - Layanan Nama Domain Amazon (DNS)
  - Protokol Konfigurasi Host Dinamis (DHCP)
  - Metadata instans Amazon EC2
  - Titik akhir metadata tugas Amazon ECS
  - Aktivasi lisensi untuk instans Windows
  - Layanan Amazon Time Sync
  - Alamat IP cadangan yang digunakan oleh router VPC default

Aturan ACL Jaringan

Anda dapat menambahkan atau menghapus aturan dari ACL jaringan default, atau membuat ACL jaringan tambahan untuk VPC Anda. Ketika Anda menambahkan atau menghapus aturan dari ACL jaringan, perubahan secara otomatis diterapkan ke subnet yang terhubung dengannya.

Berikut ini adalah bagian-bagian dari aturan ACL jaringan:

- Nomor aturan. Aturan dievaluasi mulai dari aturan bernomor terendah. Setelah aturan cocok dengan lalu lintas, aturan tersebut langsung diterapkan terlepas dari apakah ada aturan bernomor lebih tinggi yang mungkin bertentangan dengan itu.
- Jenis. Jenis lalu lintas; misalnya, SSH. Anda juga dapat menentukan semua lalu lintas atau rentang kustom.
- Protokol. Anda dapat menetapkan protokol manapun yang memiliki nomor protokol standar. Untuk informasi selengkapnya, lihat Nomor Protokol. Jika Anda menetapkan ICMP sebagai protokol, Anda dapat menetapkan satu atau semua jenis dan kode ICMP.
- Rentang port. Listening port atau rentang port untuk lalu lintas. Misalnya, 80 untuk lalu lintas HTTP.
- Sumber. [Aturan masuk saja] Sumber lalu lintas (rentang CIDR).
- Tujuan. [Aturan keluar saja] Tujuan untuk lalu lintas (rentang CIDR).

- Allow/Deny. Apakah akan mengiz inkan atau menolak lalu lintas yang ditentukan.

Misalnya aturan, lihatthe section called “Contoh: Kontrol akses ke instans dalam subnet”.

Pertimbangan-pertimbangan

- Ada kuota (juga dikenal sebagai batas) untuk jumlah aturan per ACL jaringan. Untuk informasi selengkapnya, lihat Kuota Amazon VPC.
- Ketika Anda menambahkan atau menghapus aturan dari ACL, subnet yang terkait dengan ACL tunduk pada perubahan tersebut. Perubahan berlaku setelah beberapa saat.
- Jika Anda menambahkan aturan menggunakan alat baris perintah atau API Amazon EC2, rentang CIDR secara otomatis diubah ke bentuk kanonisnya. Misalnya, jika Anda menetapkan `100.68.0.18/18` untuk rentang CIDR, kami membuat aturan dengan rentang CIDR `100.68.0.0/18`.
- Anda mungkin ingin menambahkan aturan tolak dalam situasi di mana Anda harus membuka berbagai port, tetapi ada port tertentu dalam rentang yang ingin Anda tolak. Pastikan untuk memberikan aturan tolak angka yang lebih rendah daripada aturan yang memungkinkan jangkauan lalu lintas port yang lebih luas.
- Jika Anda menambahkan dan menghapus aturan dari ACL jaringan pada saat yang sama, berhati-hatilah. Jika Anda menghapus aturan masuk atau keluar dan kemudian menambahkan lebih banyak entri baru daripada yang diizinkan (lihatKuota Amazon VPC, entri yang dipilih untuk dihapus akan dihapus dan entri baru tidak ditambahkan. Hal ini dapat menyebabkan masalah konektivitas yang tidak terduga dan mencegah akses ke dan dari VPC Anda.

ACL jaringan default untuk VPC

Virtual Private Cloud (VPC) Anda secara otomatis dilengkapi dengan ACL jaringan default. ACL jaringan default dikonfigurasi untuk memungkinkan semua lalu lintas mengalir masuk dan keluar dari subnet yang terkait dengannya. Setiap ACL jaringan juga menyertakan aturan di mana nomor aturan adalah tanda bintang (*). Aturan ini memastikan bahwa jika paket tidak cocok dengan aturan bernomor lainnya, itu ditolak.

Anda dapat memodifikasi ACL jaringan default dengan menambahkan aturan atau menghapus aturan bernomor default. Anda tidak dapat menghapus aturan di mana nomor aturan adalah tanda bintang.

Aturan masuk default

Tabel berikut menunjukkan aturan inbound default untuk ACL jaringan default. Aturan untuk IPv6 ditambahkan hanya jika Anda membuat VPC dengan blok IPv6 CIDR terkait atau mengaitkan blok IPv6 CIDR dengan VPC. Namun, jika Anda telah mengubah aturan masuk dari ACL jaringan default, kami tidak menambahkan aturan yang mengizinkan semua lalu lintas IPv6 masuk saat Anda mengaitkan blok IPv6 dengan VPC.

Aturan #	Tipe	Protokol	Rentang port	Sumber	Allow/Deny
100	Semua lalu lintas IPv4	Semua	Semua	0.0.0. 0/0	IZINKAN
101	Semua lalu lintas IPv6	Semua	Semua	::/0	IZINKAN
*	Semua Lalu lintas	Semua	Semua	0.0.0. 0/0	DENY
*	Semua lalu lintas IPv6	Semua	Semua	::/0	TOLAK

Aturan keluar default

Tabel berikut menunjukkan aturan keluar default untuk ACL jaringan default. Aturan untuk IPv6 ditambahkan hanya jika Anda membuat VPC dengan blok IPv6 CIDR terkait atau mengaitkan blok IPv6 CIDR dengan VPC. Namun, jika Anda telah mengubah aturan keluar dari ACL jaringan default, kami tidak menambahkan aturan yang mengizinkan semua lalu lintas IPv6 keluar saat Anda mengaitkan blok IPv6 dengan VPC.

Aturan #	Tipe	Protokol	Rentang Port	Tujuan	Allow/Deny
100	Semua Lalu lintas	Semua	Semua	0.0.0. 0/0	IZINKAN
101	Semua lalu lintas IPv6	Semua	Semua	::/0	IZINKAN
*	Semua Lalu lintas	Semua	Semua	0.0.0. 0/0	DENY

Aturan #	Tipe	Protokol	Rentang Port	Tujuan	Allow/Deny
*	Semua lalu lintas IPv6	Semua	Semua	::/0	TOLAK

ACL jaringan khusus untuk VPC Anda

Anda dapat membuat ACL jaringan khusus dan mengaitkannya dengan subnet untuk mengizinkan atau menolak lalu lintas masuk atau keluar tertentu di tingkat subnet. Untuk informasi selengkapnya, lihat the section called “Buat ACL jaringan”.

Setiap ACL jaringan menyertakan aturan inbound default dan aturan keluar default yang nomor aturannya adalah tanda bintang (*). Aturan ini memastikan bahwa jika paket tidak cocok dengan aturan lain, itu ditolak.

Anda dapat memodifikasi ACL jaringan dengan menambahkan atau menghapus aturan. Anda tidak dapat menghapus aturan di mana nomor aturan adalah tanda bintang.

Untuk setiap aturan yang Anda tambahkan, harus ada aturan masuk atau keluar yang memungkinkan lalu lintas respons. Untuk informasi lebih lanjut tentang cara memilih rentang ephemeral port yang sesuai, lihat Ephemeral port.

Contoh aturan masuk

Tabel berikut menunjukkan contoh aturan inbound untuk ACL jaringan. Aturan untuk IPv6 ditambahkan hanya jika VPC memiliki blok IPv6 CIDR terkait. Lalu lintas IPv4 dan IPv6 dievaluasi secara terpisah. Oleh karena itu, tidak ada aturan untuk lalu lintas IPv4 yang berlaku untuk lalu lintas IPv6. Anda dapat menambahkan aturan IPv6 di samping aturan IPv4 yang sesuai, atau menambahkan aturan IPv6 setelah aturan IPv4 terakhir.

Saat paket datang ke subnet, kami mengevaluasinya terhadap aturan masuk ACL jaringan yang terkait dengan subnet, dimulai dengan aturan bernomor terendah. Misalnya, misalkan ada lalu lintas IPv4 yang ditujukan untuk port HTTPS (443). Paket tidak cocok dengan aturan 100 atau 105. Ini cocok dengan aturan 110, yang memungkinkan lalu lintas ke subnet. Jika paket telah ditujukan untuk port 139 (NetBIOS), itu tidak akan cocok dengan aturan bernomor mana pun, sehingga aturan* untuk lalu lintas IPv4 pada akhirnya menolak paket.

Aturan #	Tipe	Protokol	Rentang port	Sumber	Allow/ Deny	Komentar
100	HTTP	TCP	80	0.0.0. 0/0	IZINKAN	Mengizinkan lalu lintas HTTP masuk dari alamat IPv4 apa pun.
105	HTTP	TCP	80	::/0	IZINKAN	Mengizinkan lalu lintas HTTP masuk dari alamat IPv6 apa pun.
110	HTTPS	TCP	443	0.0.0. 0/0	IZINKAN	Mengizinkan lalu lintas HTTP masuk dari alamat IPv4 apa pun.
115	HTTPS	TCP	443	::/0	IZINKAN	Mengizinkan akses HTTPS masuk dari alamat IPv6 apa pun.
120	SSH	TCP	22	*192.0.2.0 /24*	IZINKAN	Mengizinkan lalu lintas SSH masuk dari rentang alamat IPv4 publik jaringan rumah Anda (melalui gateway internet).
140	TCP Kustom	TCP	*32768-655 35*	0.0.0. 0/0	IZINKAN	Memungkinkan lalu lintas IPv4 kembali masuk dari internet (untuk permintaan yang berasal dari subnet).
145	TCP Kustom	TCP	*32768-655 35*	::/0	IZINKAN	Memungkinkan lalu lintas IPv6 kembali

Aturan #	Tipe	Protokol	Rentang port	Sumber	Allow/ Deny	Komentar
						masuk dari internet (untuk permintaan yang berasal dari subnet).
*	Semua Lalu lintas	Semua	Semua	0.0.0. 0/0	DENY	Menolak semua lalu lintas IPv4 masuk yang belum ditangani oleh aturan sebelumnya (tidak dapat diubah).
*	Semua lalu lintas	Semua	Semua	::/0	TOLAK	Menolak semua lalu lintas jalur masuk IPv6 yang belum ditangani oleh aturan sebelumnya (tidak dapat dimodifikasi).

Contoh aturan keluar

Tabel berikut menunjukkan contoh aturan keluar untuk ACL jaringan kustom. Aturan untuk IPv6 ditambahkan hanya jika VPC memiliki blok IPv6 CIDR terkait. Lalu lintas IPv4 dan IPv6 dievaluasi secara terpisah. Oleh karena itu, tidak ada aturan untuk lalu lintas IPv4 yang berlaku untuk lalu lintas IPv6. Anda dapat menambahkan aturan IPv6 di samping aturan IPv4 yang sesuai, atau menambahkan aturan IPv6 setelah aturan IPv4 terakhir.

Aturan #	Tipe	Protokol	Rentang Port	Tujuan	Allow/ Deny	Komentar
100	HTTP	TCP	80	0.0.0. 0/0	IZINKAN	Mengizinkan lalu lintas HTTP IPv4 keluar dari subnet ke internet.

Aturan #	Tipe	Protokol	Rentang Port	Tujuan	Allow/ Deny	Komentar
105	HTTP	TCP	80	::/0	IZINKAN	Mengizinkan lalu lintas HTTP IPv6 keluar dari subnet ke internet.
110	HTTPS	TCP	443	0.0.0. 0/0	IZINKAN	Mengizinkan lalu lintas HTTPS IPv4 keluar dari subnet ke internet.
115	HTTPS	TCP	443	::/0	IZINKAN	Mengizinkan lalu lintas HTTPS IPv6 keluar dari subnet ke internet.
120	TCP Kustom	TCP	*1024-655 5*	*192.0.2.(/24*	IZINKAN	Memungkinkan respons keluar terhadap lalu lintas SSH dari jaringan rumah Anda.
140	TCP Kustom	TCP	*32768-65 35*	0.0.0. 0/0	IZINKAN	Memungkinkan respons IPv4 keluar ke klien di internet (misalnya, melayani halaman web).
145	TCP Kustom	TCP	*32768-65 35*	::/0	IZINKAN	Memungkinkan respons IPv6 keluar ke klien di internet (misalnya, melayani halaman web).

Aturan #	Tipe	Protokol	Rentang Port	Tujuan	Allow/ Deny	Komentar
*	Semua Lalu lintas	Semua	Semua	0.0.0. 0/0	DENY	Menolak semua lalu lintas IPv4 keluar yang belum ditangani oleh aturan sebelumnya.
*	Semua Lalu lintas	Semua	Semua	::/0	TOLAK	Menolak semua lalu lintas IPv6 keluar yang belum ditangani oleh aturan sebelumnya.

Ephemeral port

Contoh ACL jaringan di bagian sebelumnya menggunakan rentang ephemeral port 32768-65535. Namun, Anda mungkin ingin menggunakan rentang yang berbeda untuk ACL jaringan Anda tergantung pada jenis klien yang Anda gunakan atau yang berkomunikasi dengan Anda.

Klien yang menginisiasi permintaan memilih rentang ephemeral port. Rentang bervariasi tergantung pada sistem operasi klien.

- Banyak kernel Linux (termasuk kernel Amazon Linux) menggunakan port 32768-61000.
- Permintaan yang berasal dari Elastic Load Balancing menggunakan port 1024-65535.
- Sistem operasi Windows melalui Windows Server 2003 menggunakan port 1025-5000.
- Windows Server 2008 dan versi yang lebih baru menggunakan port 49152-65535.
- Gateway NAT menggunakan port 1024-65535.
- AWS Lambda fungsi menggunakan port 1024-65535.

Sebagai contoh, jika permintaan datang ke server web di VPC Anda dari klien Windows 10 di internet, ACL jaringan Anda harus memiliki aturan keluar untuk mengaktifkan lalu lintas yang ditujukan untuk port 49152-65535.

Jika instance di VPC Anda adalah klien yang memulai permintaan, ACL jaringan Anda harus memiliki aturan masuk untuk mengaktifkan lalu lintas yang ditujukan untuk port sementara khusus untuk sistem operasi instans.

Dalam prakteknya, untuk mencakup berbagai jenis klien yang mungkin menginisiasi lalu lintas untuk ke instans yang menghadap publik di VPC Anda, Anda dapat membuka ephemeral port 1024-65535. Namun, Anda juga dapat menambahkan aturan ke ACL untuk menolak lalu lintas pada setiap port yang berbahaya dalam rentang tersebut. Pastikan bahwa Anda menempatkan aturan Tolak sebelumnya dalam tabel daripada aturan Izinkan yang membuka berbagai macam ephemeral port.

ACL jaringan kustom dan lainnya AWS layanan

Jika Anda membuat ACL jaringan kustom, perhatikan bagaimana hal itu dapat memengaruhi sumber daya yang Anda buat menggunakan AWS layanan lain.

Dengan Elastic Load Balancing, jika subnet untuk instans backend Anda memiliki ACL jaringan di mana Anda telah menambahkan aturan Tolak untuk semua lalu lintas dengan sumber `0.0.0.0/0` atau CIDR subnet, penyeimbang beban Anda tidak dapat melakukan pemeriksaan kondisi pada instans.

Untuk informasi selengkapnya tentang aturan ACL jaringan yang direkomendasikan untuk penyeimbang beban dan instans backend Anda, lihat berikut ini:

- ACL Jaringan untuk Penyeimbang Beban Aplikasi
- ACL Jaringan untuk Penyeimbang Beban Jaringan
- ACL Jaringan untuk Penyeimbang Beban Klasik

Memecahkan masalah keterjangkauan

Reachability Analyzer adalah alat analisis konfigurasi statis. Gunakan Reachability Analyzer untuk menganalisis dan men-debug jangkauan jaringan antara dua sumber daya di VPC Anda. Reachability Analyzer menghasilkan detail hop-by-hop dari jalur virtual antara sumber daya ini ketika mereka dapat dijangkau, dan mengidentifikasi komponen pemblokiran sebaliknya. Misalnya, dapat mengidentifikasi aturan ACL jaringan yang hilang atau salah dikonfigurasi.

Untuk informasi selengkapnya, lihat Panduan Peng analisis Jangkauan.

Path MTU Discovery dan ACL jaringan

Path MTU Discovery digunakan untuk menentukan jalur MTU antara dua perangkat. Jalur MTU adalah ukuran paket maksimum yang didukung pada jalur antara host asal dan host penerima.

Untuk IPv4, ketika host mengirimkan paket yang lebih besar dari MTU host penerima atau perangkat di sepanjang jalur, host atau perangkat penerima menjatuhkan paket. Kemudian mengembalikan pesan ICMP berikut: `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set` (Tipe 3, Kode 4).

Ini menginstruksikan host transmisi untuk membagi muatan menjadi beberapa paket yang lebih kecil, dan kemudian mentrasmisikannya kembali.

Protokol IPv6 tidak mendukung fragmentasi dalam jaringan. Ketika host mengirim paket yang lebih besar dari MTU host penerima atau perangkat di sepanjang jalur, host atau perangkat penerima menjatuhkan paket. Kemudian mengembalikan pesan ICMP berikut: `ICMPv6 Packet Too Big (PTB)` (Tipe 2).

Ini menginstruksikan host transmisi untuk membagi muatan menjadi beberapa paket yang lebih kecil, dan kemudian mentrasmisikannya kembali.

Jika unit transmisi maksimum (MTU) antar host di subnet Anda berbeda, atau instans Anda berkomunikasi dengan rekan-rekan melalui internet, Anda harus menambahkan aturan ACL jaringan berikut, baik masuk maupun keluar. Hal ini memastikan bahwa Path MTU Discovery dapat berfungsi dengan benar dan mencegah kehilangan paket. Pilih Aturan ICMP Kustom untuk jenis tersebut dan Tujuan yang Tidak Dapat Dihubungi, fragmentasi yang diperlukan, dan bendera DF yang ditetapkan untuk rentang port tersebut (tipe 3, kode 4). Jika Anda menggunakan traceroute, tambahkan juga aturan berikut: pilih Aturan ICMP Kustom untuk jenis ini dan Waktu Terlampaui, Transit kedaluwarsa TTL untuk rentang port ini (tipe 11, kode 0). Untuk informasi selengkapnya, lihat Unit transmisi maksimum jaringan (MTU) untuk instans EC2 Anda di Panduan Pengguna Amazon EC2.

Membuat ACL jaringan untuk VPC anda

Tugas berikut menunjukkan cara membuat ACL jaringan, menambahkan aturan ke ACL jaringan, dan kemudian mengaitkan ACL jaringan dengan subnet.

Tugas

- Langkah 1: Buat ACL jaringan
- Langkah 2: Tambahkan aturan

- Langkah 3: Mengaitkan subnet dengan ACL jaringan
- (Opsional) Mengelola ACL jaringan menggunakan Firewall Manager

Langkah 1: Buat ACL jaringan

Anda dapat membuat ACL jaringan kustom untuk VPC Anda. Aturan awal untuk ACL jaringan khusus memblokir semua lalu lintas masuk dan keluar. ACL jaringan kustom baru Anda tidak terkait dengan subnet secara default dan harus secara eksplisit dikaitkan dengan subnet.

Untuk membuat ACL jaringan menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih ACL Jaringan.
3. Pilih Buat ACL jaringan.
4. (Opsional) Untuk Nama, masukkan nama untuk ACL jaringan Anda.
5. Untuk VPC, pilih VPC.
6. (Opsional) Untuk Tag , pilih Tam bah tag lalu masukkan kunci tag dan nilai tag.
7. Pilih Buat ACL jaringan.

Untuk membuat ACL jaringan menggunakan baris perintah

- create-network-acl (AWS CLI)
- New-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Langkah 2: Tambahkan aturan

Anda dapat menambahkan aturan yang mengizinkan atau menolak lalu lintas masuk atau keluar.

Kami memproses aturan secara berurutan, dimulai dengan aturan dengan angka terendah. Kami sarankan Anda membiarkan adanya selisih lebar di antara nomor aturan (seperti 100, 200, 300), daripada menggunakan nomor berurutan (101, 102, 103). Hal ini memudahkan penambahan aturan baru tanpa harus mengatur ulang nomor aturan yang ada.

Jika Anda menggunakan API Amazon EC2 atau alat baris perintah, Anda tidak dapat mengubah aturan. Anda hanya dapat menambahkan dan menghapus aturan. Jika Anda menggunakan konsol Amazon VPC, Anda dapat mengubah entri untuk aturan yang ada. Konsol tersebut menghapus

aturan yang ada dan menambahkan aturan baru untuk Anda. Jika Anda perlu mengubah urutan aturan di ACL, Anda harus menambahkan aturan baru dengan nomor aturan baru, dan kemudian menghapus aturan semula.

Untuk menambahkan aturan ke ACL jaringan menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih ACL Jaringan.
3. Pilih ACL jaringan.
4. Untuk menambahkan aturan masuk, lakukan hal berikut:
   a. Pilih tab Aturan masuk.
   b. Pilih Edit aturan masuk, Tambahkan aturan baru.
   c. Masukkan nomor aturan yang belum digunakan, jenis, protokol, rentang port, sumber, dan apakah akan mengizinkan atau menolak lalu lintas. Untuk beberapa jenis, kami mengisi protokol dan port untuk Anda. Jika Anda diminta untuk rentang port, masukkan nomor port atau rentang port (misalnya, 49152-65535).

      Untuk menggunakan protokol yang tidak terdaftar, pilih Protokol K ustom untuk jenisnya dan kemudian pilih protokol. Untuk informasi selengkapnya, lihat Nomor Protokol IANA.
   d. Pilih Simpan perubahan.
5. Untuk menambahkan aturan keluar, lakukan hal berikut:
   a. Pilih tab Aturan keluar.
   b. Pilih Edit aturan keluar, Tambahkan aturan baru.
   c. Masukkan nomor aturan yang belum digunakan, jenis, protokol, rentang port, sumber, dan apakah akan mengizinkan atau menolak lalu lintas. Untuk beberapa jenis, kami mengisi protokol dan port untuk Anda. Jika Anda diminta untuk rentang port, masukkan nomor port atau rentang port (misalnya, 49152-65535).

      Untuk menggunakan protokol yang tidak terdaftar, pilih Protokol K ustom untuk jenisnya dan kemudian pilih protokol. Untuk informasi selengkapnya, lihat Nomor Protokol IANA.
   d. Pilih Simpan perubahan.

Untuk menambahkan aturan ke ACL jaringan menggunakan baris perintah

- create-network-acl-entry (AWS CLI)
- New-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Untuk mengganti aturan dalam ACL jaringan menggunakan baris perintah

- mengganti-acl jaringan (AWS CLI)
- Set-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Untuk menghapus aturan dari ACL jaringan menggunakan baris perintah

- delete-network-acl-entry (AWS CLI)
- Remove-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Langkah 3: Mengaitkan subnet dengan ACL jaringan

Untuk menerapkan aturan ACL jaringan untuk subnet tertentu, Anda harus mengaitkan subnet tersebut dengan ACL jaringan. Anda dapat menghubungkan ACL jaringan dengan beberapa subnet. Namun, suatu subnet dapat dikaitkan dengan hanya satu ACL jaringan. Setiap subnet yang tidak terkait dengan ACL tertentu dikaitkan dengan ACL jaringan default secara default.

Untuk mengaitkan subnet dengan ACL jaringan

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih ACL Jaringan, dan kemudian pilih ACL jaringan.
3. Di panel rincian, pada tab Pengaitan Subnet, pilih Edit. Pilih kotak centang Pengaitan untuk mengaitkan subnet dengan ACL jaringan, dan kemudian pilih Simpan.

(Opsional) Mengelola ACL jaringan menggunakan Firewall Manager

AWS Firewall Manager menyederhanakan tugas administrasi dan pemeliharaan ACL jaringan Anda di beberapa akun dan subnet. Anda dapat menggunakan Firewall Manager untuk memantau akun dan subnet di organisasi Anda dan untuk secara otomatis menerapkan konfigurasi ACL jaringan yang telah Anda tetapkan. Firewall Manager sangat berguna ketika Anda ingin melindungi seluruh

organisasi Anda, atau jika Anda sering menambahkan subnet baru yang ingin Anda lindungi secara otomatis dari akun administrator pusat.

Dengan kebijakan ACL jaringan Firewall Manager, menggunakan akun administrator tunggal, Anda dapat mengonfigurasi, memantau, dan mengelola kumpulan aturan minimum yang ingin Anda tetapkan dalam ACL jaringan yang Anda gunakan di seluruh organisasi. Anda menentukan akun dan subnet mana di organisasi Anda yang berada dalam cakupan kebijakan Firewall Manager. Firewall Manager melaporkan status kepatuhan ACL jaringan untuk subnet dalam cakupan, dan Anda dapat mengonfigurasi Firewall Manager untuk mengotomatiskan remediasi ACL jaringan yang tidak sesuai.

Untuk informasi selengkapnya, lihat sumber daya berikut di Panduan AWS Firewall Manager Pengembang:

- AWS Firewall Manager prasyarat
- Menyiapkan AWS Firewall Manager kebijakan ACL jaringan
- Menggunakan kebijakan ACL jaringan dengan Firewall Manager

Kelola asosiasi ACL jaringan untuk VPC Anda

Setiap subnet dikaitkan dengan satu jaringan ACL. Ketika Anda pertama kali membuat subnet, itu dikaitkan dengan ACL jaringan default untuk VPC. Anda dapat membuat ACL jaringan khusus dan mengaitkannya dengan satu atau lebih subnet, menggantikan asosiasi ACL jaringan sebelumnya.

Tugas

- Jelaskan asosiasi ACL jaringan Anda
- Mengubah subnet yang terkait dengan ACL jaringan
- Mengubah ACL jaringan yang terkait dengan subnet

Jelaskan asosiasi ACL jaringan Anda

Anda dapat menjelaskan ACL jaringan yang terkait dengan subnet dan Anda juga dapat menjelaskan subnet mana yang terkait dengan ACL jaringan.

Untuk mendeskripsikan ACL jaringan yang terkait dengan subnet menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Pengguna.

3. Pilih subnet.
4. Pilih tab Network ACL.

Untuk menggambarkan jaringan ACL yang terkait dengan subnet menggunakan AWS CLI

Gunakan perintah describe-network-acls berikut untuk mencantumkan ACL jaringan yang terkait dengan subnet yang ditentukan.

```
aws ec2 describe-network-acls --filters Name=association.subnet-
id,Values=subnet-0d2d1b81e0bc9c6d4 --query NetworkAcls[*].NetworkAclId
```

Berikut ini adalah output contoh.

```
[
    "acl-03701d1f82d8c3fd6"
]
```

Untuk menjelaskan subnet yang terkait dengan ACL jaringan menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih ACL Jaringan.
3. Pilih ACL jaringan.
4. Pilih tab A sosiasi subnet.

Untuk menggambarkan subnet yang terkait dengan ACL jaringan menggunakan AWS CLI

Gunakan perintah describe-network-acls berikut untuk mencantumkan subnet yang terkait dengan ACL jaringan tertentu.

```
aws ec2 describe-network-acls --network-acl-ids acl-060415a18fcc9afde --query
 NetworkAcls[*].Associations[].SubnetId
```

Berikut ini adalah output contoh.

```
[
    "subnet-0d2d1b81e0bc9c6d4",
    "subnet-0e990c67809773b19",
    "subnet-0eb17d85f5dfd33b1",
```

```
    "subnet-0e01d500780bb7468"
]
```

Mengubah subnet yang terkait dengan ACL jaringan

Anda dapat melepaskan ACL jaringan dari subnet. Setelah Anda melepaskan subnet dari ACL jaringan kustom, kami secara otomatis mengaitkannya dengan ACL jaringan default untuk VPC. Perubahan mulai berlaku setelah periode waktu yang singkat.

Untuk mengubah subnet yang terkait dengan ACL jaringan

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih ACL Jaringan.
3. Pilih ACL jaringan.
4. Pilih T indakan, Edit asosiasi subnet.
5. Hapus subnet dari subnet yang dipilih.
6. Pilih Simpan perubahan.

Mengubah ACL jaringan yang terkait dengan subnet

Anda dapat mengubah ACL jaringan yang terkait dengan suatu subnet. Misalnya, ketika Anda membuat subnet, pada awalnya dikaitkan dengan ACL jaringan default untuk VPC. Jika Anda membuat ACL jaringan kustom, Anda menerapkan aturan ACL jaringan dengan mengaitkan ACL jaringan dengan satu atau lebih subnet.

Setelah Anda mengubah ACL jaringan untuk subnet, perubahan akan berlaku setelah periode waktu yang singkat.

Untuk mengubah ACL jaringan yang terkait dengan subnet

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Pengguna.
3. Pilih subnet.
4. Pilih T indakan, Edit asosiasi ACL jaringan.
5. Untuk ID ACL Jaringan, pilih ACL jaringan yang akan diasosiasikan dengan subnet, dan tinjau aturan masuk dan keluar untuk ACL jaringan yang dipilih.
6. Pilih Simpan.

Untuk mengganti asosiasi ACL jaringan menggunakan baris perintah

- replace-network-acl-association (AWS CLI)
- Set-EC2NetworkAclAssociation (AWS Tools for Windows PowerShell)

Menghapus ACL jaringan untuk VPC Anda

Ketika Anda selesai dengan ACL jaringan, Anda dapat menghapusnya. Anda tidak dapat menghapus ACL jaringan jika ada subnet yang terkait dengannya. Anda tidak dapat menghapus ACL jaringan default.

Untuk menghapus asosiasi subnet dari ACL jaringan menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih ACL Jaringan. Kol om Terkait dengan menunjukkan jumlah subnet yang terkait dengan setiap ACL jaringan. Kolom ini adalah - jika tidak ada subnet terkait.
3. Pilih ACL jaringan.
4. Pilih T indakan, Edit asosiasi subnet.
5. Hapus asosiasi subnet.
6. Pilih Simpan perubahan.

Untuk menggambarkan ACL jaringan Anda, termasuk asosiasi, menggunakan baris perintah

- describe-network-acls (AWS CLI)
- Get-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Untuk mengganti asosiasi ACL jaringan menggunakan baris perintah

- replace-network-acl-association (AWS CLI)
- Set-EC2NetworkAclAssociation (AWS Tools for Windows PowerShell)

Untuk menghapus ACL jaringan menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih ACL Jaringan.

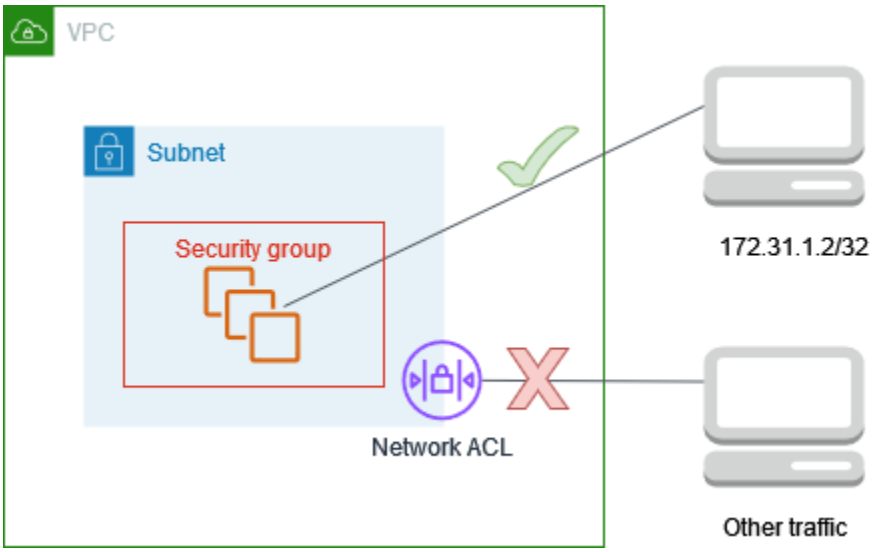
3. Pilih ACL jaringan.
4. Pilih T ind akan, Hapus ACL jaringan.
5. Saat diminta konfirmasi, masukkan **`delete`**, lalu pilih Hapus.

Untuk menghapus ACL jaringan menggunakan baris perintah

- delete-network-acl (AWS CLI)
- Remove-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Contoh: Kontrol akses ke instans dalam subnet

Dalam contoh ini, instance di subnet dapat berkomunikasi satu sama lain, dan dapat diakses dari komputer jarak jauh tepercaya untuk melakukan tugas administratif. Komputer jarak jauh mungkin merupakan komputer di jaringan lokal Anda, seperti yang ditunjukkan dalam diagram, atau mungkin contoh di subnet atau VPC yang berbeda. Aturan ACL jaringan untuk subnet, dan aturan grup keamanan untuk instance, memungkinkan akses dari alamat IP komputer jarak jauh Anda. Semua lalu lintas lain dari internet atau jaringan lain ditolak.



Menggunakan ACL jaringan memberi Anda fleksibilitas untuk mengubah grup keamanan atau aturan grup keamanan untuk instans Anda sambil mengandalkan ACL jaringan sebagai lapisan pertahanan cadangan.

Misalnya, jika Anda secara tidak sengaja memperbarui grup keamanan untuk mengizinkan akses SSH masuk dari mana saja, ACL jaringan masih membatasi akses hanya ke rentang alamat IP komputer jarak jauh. ACL jaringan menolak lalu lintas SSH masuk dari alamat IP lainnya.

Aturan ACL Jaringan

Berikut ini adalah contoh aturan inbound untuk ACL jaringan yang terkait dengan subnet. Aturan ini berlaku untuk semua instance di subnet.

Aturan #	Tipe	Protokol	Rentang port	Sumber	Allow/Deny	Komentar
100	SSH	TCP	22	*172.31.1.2/32*	IZINKAN	Izinkan lalu lintas masuk dari komputer jarak jauh.
*	Semua Lalu lintas	Semua	Semua	0.0.0. 0/0	DENY	Tolak semua lalu lintas masuk lainnya.

Berikut ini adalah contoh aturan keluar untuk ACL jaringan yang terkait dengan subnet. ACL jaringan bersifat stateless. Oleh karena itu, Anda harus menyertakan aturan yang memungkinkan respons terhadap lalu lintas masuk.

Aturan #	Tipe	Protokol	Rentang Port	Tujuan	Allow/Deny	Komentar
100	TCP Kustom	TCP	1024-65535	*172.31.1.2/32*	IZINKAN	Mengizinkan respon keluar ke komputer jarak jauh.
*	Semua lalu lintas	Semua	Semua	0.0.0. 0/0	DENY	Menolak semua lalu lintas

Aturan #	Tipe	Protokol	Rentang Port	Tujuan	Allow/Deny	Komentar
						keluar lainnya.

Aturan grup keamanan

Berikut ini adalah contoh aturan masuk untuk grup keamanan yang terkait dengan instance. Aturan ini berlaku untuk semua instance yang terkait dengan grup keamanan. Pengguna dengan kunci pribadi untuk pasangan kunci yang terkait dengan instance dapat terhubung ke instance dari komputer jarak jauh menggunakan SSH.

Tipe protokol	Protokol	Rentang port	Sumber	Komentar
Semua lalu lintas	Semua	Semua	*sg-1234567890abcdef0*	Izinkan komunikasi antara instance yang terkait dengan grup keamanan ini.
SSH	TCP	22	*172.31.1.2/32*	Izinkan akses SSH masuk dari komputer jarak jauh.

Berikut ini adalah contoh aturan terikat keluar untuk grup keamanan yang terkait dengan instance. Grup keamanan bersifat stateful. Oleh karena itu, Anda tidak memerlukan aturan yang memungkinkan respons terhadap lalu lintas masuk.

Jenis protokol	Protokol	Rentang Port	Tujuan	Komentar
Semua lalu lintas	Semua	Semua	*sg-1234567890abcdef0*	Izinkan komunikasi antara instance

Jenis protokol	Protokol	Rentang Port	Tujuan	Komentar
				yang terkait dengan grup keamanan ini.

Perbedaan antara ACL jaringan dan grup keamanan

Tabel berikut merangkum perbedaan dasar antara ACL jaringan dan grup keamanan.

Karakteristik	ACL jaringan	Grup keamanan
Tingkat operasi	Tingkat subnet	Tingkat instans
Lingkup	Berlaku untuk semua instance di subnet terkait	Berlaku untuk semua instans yang terkait dengan grup keamanan
Jenis aturan	Izinkan dan tolak aturan	Izinkan aturan saja
Evaluasi aturan	Mengevaluasi aturan dalam urutan menaik hingga kecocokan untuk lalu lintas ditemukan	Mengevaluasi semua aturan sebelum memutuskan apakah akan mengizinkan lalu lintas
Kembali lalu lintas	Harus diizinkan secara eksplisit (tanpa kewarganegaraan)	Diizinkan secara otomatis (stateful)

Ketahanan di Amazon Virtual Private Cloud

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Zona Ketersediaan. Wilayah AWS menyediakan beberapa Zona Ketersediaan yang terpisah secara fisik dan terisolasi, yang terhubung menggunakan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Wilayah AWS adalah blok bangunan utama, masing-masing mewakili lokasi geografis yang berbeda yang menampung beberapa Zona Ketersediaan yang terpisah secara fisik dan terisolasi. Zona

Ketersediaan ini terhubung melalui struktur jaringan latensi rendah, throughput tinggi, dan sangat redundan, memungkinkan komunikasi dan transfer data yang mulus di antara keduanya.

Arsitektur Availability Zones adalah pembeda utama, karena dirancang agar jauh lebih kuat dan toleran terhadap kesalahan daripada pengaturan pusat data tunggal atau ganda tradisional. Dengan mendistribusikan sumber daya di beberapa Zona Ketersediaan dalam Wilayah, aplikasi dan database dapat direkayasa untuk secara otomatis gagal di antara zona tanpa gangguan pada layanan. Tingkat redundansi dan ketersediaan tinggi ini merupakan persyaratan penting untuk beban kerja kritis misi dan memungkinkan organisasi untuk membangun solusi cloud-native yang tangguh.

Selain itu, skala dan jangkauan global AWS infrastruktur memberdayakan pelanggan untuk menerapkan aplikasi mereka lebih dekat ke pengguna akhir, mengurangi latensi dan meningkatkan pengalaman pengguna secara keseluruhan. Ketersediaan beberapa Wilayah di seluruh dunia juga memungkinkan kedaulatan dan kepatuhan data yang efektif, karena pelanggan dapat menyimpan dan memproses data dalam batas-batas geografis yang diperlukan oleh peraturan dan kebutuhan bisnis spesifik mereka.

Dengan menggunakan infrastruktur AWS global, organisasi dapat merancang lingkungan cloud mereka agar sangat tersedia, toleran terhadap kesalahan, dan dapat diskalakan, dengan fleksibilitas untuk beradaptasi dengan perubahan persyaratan dan kebutuhan bisnis yang berkembang. Fondasi yang kuat ini adalah pendorong utama untuk keberhasilan implementasi aplikasi dan layanan berbasis cloud modern.

Untuk informasi selengkapnya tentang Wilayah AWS dan Zona Ketersediaan, lihat Infrastruktur AWS Global.

Anda dapat mengonfigurasi VPC Anda untuk memenuhi persyaratan ketahanan untuk beban kerja Anda. Untuk informasi selengkapnya, lihat berikut ini:

- Memahami pola ketahanan dan pertukaran (Blog Arsitektur)AWS
- Rencanakan topologi jaringan Anda (AWS Well-Architected Framework)
- Opsi Konektivitas Cloud Pribadi Virtual Amazon (AWS Whitepapers)

Validasi kepatuhan untuk Amazon Virtual Private Cloud

Pengalaman AWS pendaftaran baru kami tidak dirancang untuk beban kerja yang diatur. Jika Anda menggunakan pengalaman AWS pendaftaran baru kami, tetapi ingin menggunakannya AWS untuk

beban kerja yang diatur, Anda dapat mendaftar untuk AWS (lanjutan) atau mengaktifkan fitur lanjutan untuk lingkungan Anda AWS .

Untuk mengetahui apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup berdasarkan Program Kepatuhan dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program Kep AWS atuhan Program Jaminan .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. Untuk informasi selengkapnya tentang tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS, lihat Dokumentasi AWS Keamanan.

Blokir akses publik ke VPC dan subnet

VPC Block Public Access (BPA) adalah fitur keamanan terpusat yang secara otoritatif mencegah akses internet publik ke sumber daya VPC di seluruh akun. AWS Ini memastikan kepatuhan dengan persyaratan keamanan sambil memberikan fleksibilitas untuk pengecualian tertentu dan kemampuan audit.

Fitur VPC BPA memiliki mode berikut:

- Dua Arah: Semua lalu lintas ke dan dari gateway internet dan gateway internet khusus keluar di Wilayah ini (kecuali untuk VPC dan subnet yang dikecualikan) diblokir.
- Ingress-only: Semua lalu lintas internet ke VPC di Wilayah ini (kecuali untuk VPC atau subnet yang dikecualikan) diblokir. Hanya lalu lintas ke dan dari gateway NAT dan gateway internet khusus keluar yang diizinkan karena gateway ini hanya memungkinkan koneksi keluar untuk dibuat.

Anda juga dapat membuat “pengecualian” untuk fitur ini untuk lalu lintas yang tidak ingin Anda blokir. Pengecualian adalah mode yang dapat diterapkan ke satu VPC atau subnet yang membebaskannya dari mode BPA VPC akun dan akan memungkinkan akses dua arah atau hanya keluar.

Pengecualian dapat memiliki salah satu mode berikut:

- Dua arah: Semua lalu lintas internet ke dan dari VPC dan subnet yang dikecualikan diizinkan.

- Egress-only: Lalu lintas internet keluar dari VPC dan subnet yang dikecualikan diperbolehkan. Lalu lintas internet masuk ke VPC dan subnet yang dikecualikan diblokir. Ini hanya berlaku ketika VPC BPA diatur ke Dua Arah.

Daftar Isi

- Dasar-dasar VPC BPA
- Menilai dampak VPC BPA dan memantau VPC BPA
- Contoh lanjutan

Dasar-dasar VPC BPA

Bagian ini mencakup detail penting tentang VPC BPA, termasuk layanan mana yang mendukungnya dan bagaimana Anda dapat bekerja dengannya.

Daftar Isi

- Ketersediaan wilayah
- AWS dampak layanan dan dukungan
- Batasan BPA VPC
- Kontrol akses ke VPC BPA dengan kebijakan IAM
- Aktifkan mode dua arah VPC BPA untuk akun Anda
- Ubah mode VPC BPA ke input saja
- Membuat dan menghapus pengecualian
- Aktifkan VPC BPA di tingkat Organisasi

Ketersediaan wilayah

VPC BPA tersedia di semua Wilayah komersial termasuk GovCloud dan Wil AWS ayah China.

Dalam panduan ini, Anda juga akan menemukan informasi tentang menggunakan Network Access Analyzer dan Reachability Analyzer dengan VPC BPA. Perhatikan bahwa Network Access Analyzer dan Reachability Analyzer tidak tersedia di semua Wilayah komersial. Untuk informasi tentang ketersediaan regional Network Access Analyzer dan Reachability Analyzer, lihat Keter batasan dalam Panduan Penganalisis Akses Jaringan dan Per timbangan dalam Panduan Penganalisis Jang kauan.

AWS dampak layanan dan dukungan

Sumber daya dan layanan berikut mendukung VPC BPA dan lalu lintas ke layanan dan sumber daya ini dipengaruhi oleh VPC BPA:

- Gateway Internet: Semua lalu lintas masuk dan keluar diblokir.
- Egress-only gateway internet: Semua lalu lintas keluar diblokir. Egress-only Gateway internet tidak mengizinkan lalu lintas masuk.
- Gateway Load Balancer (GWLB): Semua lalu lintas masuk dan keluar diblokir kecuali subnet yang berisi titik akhir GWLB dikecualikan.
- NAT gateway: Semua lalu lintas masuk dan keluar diblokir. Gerbang NAT memerlukan gateway internet untuk konektivitas internet.
- Internet-facing Network Load Balancer: Semua lalu lintas masuk dan keluar diblokir. Internet-facing Network Load Balancers memerlukan gateway internet untuk konektivitas internet.
- Internet-facing Penyeimbang Beban Aplikasi: Semua lalu lintas masuk dan keluar diblokir. Internet-facing Application Load Balancers memerlukan gateway internet untuk konektivitas internet.
- Amazon CloudFront VPC Origins: Semua lalu lintas masuk dan keluar diblokir.
- Direct Connect: Semua lalu lintas masuk dan keluar yang menggunakan antarmuka virtual publik (IPv4 publik atau alamat IPv6 unicast global) diblokir. Lalu lintas ini menggunakan gateway internet (atau gateway internet khusus keluar) untuk konektivitas.
- AWS Aksel erator Global: Lalu lintas masuk ke VPC diblokir, terlepas dari apakah target dapat diakses dari internet atau tidak.
- AWS Network Firewall: Semua lalu lintas masuk dan keluar diblokir kecuali subnet yang berisi titik akhir firewall dikecualikan.
- AWS Wavelength gateway operator: Semua lalu lintas masuk dan keluar diblokir.

Lalu lintas yang terkait dengan konektivitas pribadi, seperti lalu lintas untuk layanan dan sumber daya berikut, tidak diblokir atau terpengaruh oleh BPA VPC:

- AWS Client VPN
- AWS CloudWAN
- AWS Outposts gerbang lokal
- AWS Site-to-Site VPN
- Gateway transit

- Akses Terverifikasi AWS

Important

- Jika Anda merutekan lalu lintas masuk dan keluar melalui alat (seperti alat keamanan atau pemantauan pihak ketiga) yang berjalan pada instans EC2 di subnet menggunakan Perutean Ingress VPC, Anda harus mengecualikan subnet beban kerja dari VPC Block Public Access. Subnet beban kerja adalah subnet yang berisi instance yang lalu lintasnya dialihkan melalui alat. Subnet yang berisi alat tidak perlu dikecualikan.
- Lalu lintas yang dikirim secara pribadi dari sumber daya di VPC Anda ke layanan lain yang berjalan di VPC Anda, seperti Route 53 Resolver, diizinkan bahkan ketika VPC BPA dihidupkan karena tidak melewati gateway internet di VPC Anda. Ada kemungkinan bahwa layanan ini dapat membuat permintaan ke sumber daya di luar VPC atas nama Anda, misalnya, untuk menyelesaikan kueri DNS, dan dapat mengekspos informasi tentang aktivitas sumber daya dalam VPC Anda jika tidak dikurangi melalui kontrol keamanan lainnya.
- Jika Anda memiliki penyeimbang beban yang menghadap ke internet dan membuat pengecualian BPA VPC hanya untuk salah satu subnetnya, penyeimbang beban masih dapat menerima lalu lintas publik di subnet yang dikecualikan dan merutekan secara pribadi ke target di subnet yang tidak dikecualikan. Untuk memastikan VPC BPA sepenuhnya memblokir akses publik ke target Anda, pastikan tidak ada subnet penyeimbang beban yang dikecualikan.

Batasan BPA VPC

Mode masuk khusus VPC BPA tidak didukung di Zona Lokal (LZ) di mana gateway NAT dan gateway internet khusus keluar tidak diizinkan.

Kontrol akses ke VPC BPA dengan kebijakan IAM

Untuk contoh kebijakan IAM yang allow/deny mengakses fitur VPC BPA, lihat. Blokir akses publik ke VPC dan subnet

Aktifkan mode dua arah VPC BPA untuk akun Anda

Mode dua arah VPC BPA memblokir semua lalu lintas ke dan dari gateway internet dan gateway internet khusus keluar di Wilayah ini (kecuali untuk VPC dan subnet yang dikecualikan). Untuk informasi selengkapnya tentang pengecualian, lihatMembuat dan menghapus pengecualian.

Important

Kami sangat menyarankan Anda meninjau secara menyeluruh beban kerja yang memerlukan akses Internet sebelum mengaktifkan VPC BPA di akun produksi Anda.

Note

- Untuk mengaktifkan VPC BPA pada VPC dan subnet di akun Anda, Anda harus memiliki VPC dan subnet.
- Jika saat ini Anda berbagi subnet VPC dengan akun lain, mode BPA VPC yang diberlakukan oleh pemilik subnet juga berlaku untuk lalu lintas peserta, tetapi peserta tidak dapat mengontrol pengaturan BPA VPC yang memengaruhi subnet bersama.

Konsol Manajemen AWS

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi kiri, pilih Peng aturan.
3. Pilih Edit pengaturan akses publik.
4. Pilih Aktifkan blokir akses publik dan Dua arah, lalu pilih S impan perubahan.
5. Tunggu Status berubah menjadi Aktif. Mungkin perlu beberapa menit agar pengaturan VPC BPA berlaku dan status diperbarui.

Mode dua arah VPC BPA sekarang aktif.

AWS CLI

1. Nyalakan VPC BPA:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-
gateway-block-mode block-bidirectional
```

Mungkin perlu beberapa menit agar pengaturan VPC BPA berlaku dan status diperbarui.

2. Lihat status VPC BPA:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

Ubah mode VPC BPA ke input saja

Mode masuk VPC BPA hanya memblokir semua lalu lintas internet ke VPC di Wilayah ini (kecuali untuk VPC atau subnet yang dikecualikan). Hanya lalu lintas ke dan dari gateway NAT dan gateway internet khusus keluar yang diizinkan karena gateway ini hanya memungkinkan koneksi keluar untuk dibuat.

Konsol Manajemen AWS

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi kiri, pilih Peng aturan.
3. Pilih Edit pengaturan akses publik.
4. Ubah arah ke Ingress-only.
5. Simpan perubahan dan tunggu status diperbarui. Mungkin perlu beberapa menit agar pengaturan VPC BPA berlaku dan status diperbarui.

AWS CLI

1. Ubah arah blok VPC BPA:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-
gateway-block-mode block-ingress
```

Mungkin perlu beberapa menit agar pengaturan VPC BPA berlaku dan status diperbarui.

2. Lihat status VPC BPA:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

Membuat dan menghapus pengecualian

Pengecualian VPC BPA adalah mode yang dapat diterapkan ke satu VPC atau subnet yang membebaskannya dari mode BPA VPC akun dan akan memungkinkan akses dua arah atau hanya keluar. Anda dapat membuat pengecualian VPC BPA untuk VPC dan subnet bahkan ketika VPC BPA tidak diaktifkan di akun untuk memastikan bahwa tidak ada gangguan lalu lintas pada pengecualian saat VPC BPA diaktifkan. Pengecualian untuk VPC secara otomatis berlaku untuk semua subnet di VPC.

Anda dapat membuat maksimal 50 pengecualian. Untuk informasi tentang meminta kenaikan batas, lihat pengecualian VPC BPA per akun di. Kuota Amazon VPC

Konsol Manajemen AWS

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi kiri, pilih Peng aturan.
3. Di tab Blokir akses publik, di bawah Pengecualian, lakukan salah satu hal berikut:
   - Untuk menghapus pengecualian, pilih pengecualian, lalu pilih Tindakan > H apus pengecualian.
   - Untuk membuat pengecualian, pilih Buat pengecualian dan lanjutkan dengan langkah selanjutnya.
4. Pilih arah blok:
   - Dua arah: Memungkinkan semua lalu lintas internet ke dan dari VPC dan subnet yang dikecualikan.
   - Egress-only: Memungkinkan lalu lintas internet keluar dari VPC dan subnet yang dikecualikan. Memblokir lalu lintas internet masuk ke VPC dan subnet yang dikecualikan. Pengaturan ini berlaku saat VPC BPA disetel ke Dua Arah.
5. Pilih VPC atau subnet.
6. Pilih Buat pengecualian.
7. Tunggu status Pengecualian berubah menjadi Aktif. Anda mungkin perlu menyegarkan tabel pengecualian untuk melihat perubahan.

Pengecualian telah dibuat.

AWS CLI

1. Ubah pengecualian izinkan arah:

```
aws ec2 --region us-east-2 create-vpc-block-public-access-exclusion --subnet-
id subnet-id --internet-gateway-exclusion-mode allow-bidirectional
```

2. Butuh waktu untuk memperbarui status pengecualian. Untuk melihat status pengecualian:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-exclusions --
exclusion-ids exclusion-id
```

Aktifkan VPC BPA di tingkat Organisasi

Jika Anda menggunakan AWS Organisasi untuk mengelola akun di organisasi Anda, Anda dapat menggunakan kebijakan deklaratif Organisasi untuk menerapkan BPA VPC pada akun di AWS organisasi. Untuk informasi selengkapnya tentang kebijakan deklaratif VPC BPA, lihat Kebijakan deklaratif yang didukung di Panduan Pengguna Organisasi AWS .

> **Note**
>
> - Anda dapat menggunakan kebijakan deklaratif VPC BPA untuk mengonfigurasi apakah pengecualian diizinkan, tetapi Anda tidak dapat membuat pengecualian dengan kebijakan tersebut. Untuk membuat pengecualian, Anda masih harus membuatnya di akun yang memiliki VPC. Untuk informasi selengkapnya tentang membuat pengecualian VPC BPA, lihat. Membuat dan menghapus pengecualian
> - Jika kebijakan deklaratif VPC BPA diaktifkan, di B lokir setelan akses publik, Anda akan melihat Dikel ola oleh Kebijakan Deklaratif dan Anda tidak akan dapat mengubah setelan BPA VPC di tingkat akun.

Menilai dampak VPC BPA dan memantau VPC BPA

Bagian ini berisi informasi tentang Anda dapat menilai dampak VPC BPA sebelum Anda menyalakannya dan bagaimana Anda memantau apakah lalu lintas diblokir setelah Anda menyalakannya.

Daftar Isi

- Menilai dampak VPC BPA menggunakan Network Access Analyzer
- Pantau dampak BPA VPC dengan log aliran
- Lacak penghapusan pengecualian dengan CloudTrail
- Verifikasi konektivitas diblokir dengan Reachability Analyzer

Menilai dampak VPC BPA menggunakan Network Access Analyzer

Di bagian ini, Anda akan menggunakan Network Access Analyzer untuk melihat sumber daya di akun Anda yang menggunakan gateway internet sebelum Anda mengaktifkan VPC BPA dan memblokir akses. Gunakan analisis ini untuk memahami dampak dari mengaktifkan VPC BPA di akun Anda dan memblokir lalu lintas.

> **Note**
>
> - Network Access Analyzer tidak mendukung IPv6; jadi Anda tidak akan dapat menggunakannya untuk melihat potensi dampak VPC BPA pada lalu lintas IPv6 keluar gateway internet khusus keluar.
> - Anda dikenakan biaya untuk analisis yang Anda lakukan dengan Network Access Analyzer. Untuk informasi selengkapnya, lihat Harga di Panduan Penganalisis Akses Jaringan.
> - Untuk informasi tentang ketersediaan regional Network Access Analyzer, lihat Bat asan di Panduan Peng analisis Akses Jaringan.

Konsol Manajemen AWS

1. Buka konsol AWS Network Insights dihttps://console.aws.amazon.com/networkinsights/.
2. Pilih Network Access Analyzer.
3. Pilih Buat Lingkup Akses Jaringan.
4. Pilih Men ilai dampak Akses Publik Blok VPC dan pilih Ber ikutnya.
5. Template sudah dikonfigurasi untuk menganalisis lalu lintas ke dan dari gateway internet di akun Anda. Anda dapat melihat ini di bawah Sumber dan Tujuan.
6. Pilih Berikutnya.
7. Pilih Buat Lingkup Akses Jaringan.
8. Pilih ruang lingkup yang baru saja Anda buat dan pilih Analisis.

9. Tunggu analisis selesai.
10. Lihat temuan analisis. Setiap baris di bawah Temuan menunjukkan jalur jaringan yang dapat diambil paket dalam jaringan ke atau dari gateway internet di akun Anda. Dalam hal ini, jika Anda mengaktifkan VPC BPA dan tidak ada VPC dan/atau subnet yang muncul dalam temuan ini dikonfigurasi sebagai pengecualian VPC BPA, lalu lintas ke VPC dan subnet tersebut akan dibatasi.
11. Analisis setiap temuan untuk memahami dampak VPC BPA pada sumber daya di VPC Anda.

Analisis dampak selesai.

AWS CLI

1. Buat cakupan akses jaringan:

```
aws ec2 create-network-insights-access-scope --region us-east-2 --match-paths
 "Source={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
 "Destination={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
```

2. Mulai analisis lingkup:

```
aws ec2 start-network-insights-access-scope-analysis  --region us-east-2 --
network-insights-access-scope-id nis-id
```

3. Dapatkan hasil analisis:

```
aws ec2 get-network-insights-access-scope-analysis-findings  --region us-east-2
 --network-insights-access-scope-analysis-id nisa-0aa383a1938f94cd1 --max-items
 1
```

   Hasilnya menunjukkan lalu lintas ke dan dari gateway internet di semua VPC di akun Anda. Hasilnya disusun sebagai “temuan”. “FindingId“:" AnalysisFinding-1 "menunjukkan bahwa ini adalah temuan pertama dalam analisis. Perhatikan bahwa ada beberapa temuan dan masing-masing menunjukkan aliran lalu lintas yang akan terpengaruh dengan mengaktifkan VPC BPA. Temuan pertama akan menunjukkan bahwa lalu lintas dimulai di gateway internet (” SequenceNumber “: 1), diteruskan ke NACL (” SequenceNumber “: 2) ke grup keamanan (” SequenceNumber “: 3) dan berakhir pada instance (” SequenceNumber “: 4).
4. Analisis temuan untuk memahami dampak VPC BPA pada sumber daya di VPC Anda.

Analisis dampak selesai.

Pantau dampak BPA VPC dengan log aliran

VPC Flow Logs adalah fitur yang memungkinkan Anda menangkap informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan Elastic di VPC Anda. Anda dapat menggunakan fitur ini untuk memantau lalu lintas yang diblokir oleh VPC BPA agar tidak mencapai antarmuka jaringan instans Anda.

Buat log alur untuk VPC Anda menggunakan langkah-langkah diBekerja dengan log alur.

Saat Anda membuat log alur, pastikan Anda menggunakan format kustom yang menyertakan bidang`reject-reason`.

Saat Anda melihat log alur, jika lalu lintas ke ENI ditolak karena VPC BPA, Anda akan melihat `reject-reason` dari dalam entr BPA i log alur.

Selain batasan standar untuk log aliran VPC, perhatikan batasan berikut khusus untuk VPC BPA:

- Log aliran untuk VPC BPA tidak menyertakan catatan yang dile wati.
- Log alur untuk VPC BPA tidak disertakan `bytes` meskipun Anda menyertakan `bytes` bidang tersebut dalam log alur Anda.

Lacak penghapusan pengecualian dengan CloudTrail

Bagian ini menjelaskan cara Anda dapat menggunakan AWS CloudTrail untuk memantau dan melacak penghapusan pengecualian VPC BPA.

Konsol Manajemen AWS

Anda dapat melihat pengecualian yang dihapus di CloudTrail riwayat acara dengan mencari Jenis sumber daya > `AWS::EC2::VPCBlockPublicAccessExclusion` di AWS CloudTrail konsol dihttps://console.aws.amazon.com/cloudtrailv2/.

AWS CLI

Anda dapat menggunakan `lookup-events` perintah untuk melihat peristiwa yang terkait dengan menghapus pengecualian:

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceType,AttributeValue=AWS::EC2::VPCBlockPublicAccessExclusion
```

Verifikasi konektivitas diblokir dengan Reachability Analyzer

VPC Reachability Analyzer dapat digunakan untuk mengevaluasi apakah jalur jaringan tertentu dapat dicapai dengan konfigurasi jaringan Anda, termasuk pengaturan VPC BPA.

Untuk informasi tentang ketersediaan regional Reachability Analyzer, lihat Per timbangan dalam Panduan Penganalisis Jang kauan.

Konsol Manajemen AWS

1. Buka konsol AWS Network Insights dihttps://console.aws.amazon.com/networkinsights/home#ReachabilityAnalyzer.
2. Pilih Buat dan analisis jalur.
3. Untuk Jenis Sumber, pilih Internet Gateway dan pilih gateway internet yang ingin Anda blokir lalu lintas dari drop down Sumber.
4. Untuk Ti pe Tujuan, pilih Instans dan pilih instans yang ingin Anda blokir lalu lintas dari dropdown Tujuan.
5. Pilih Buat dan analisis jalur.
6. Tunggu analisis selesai. Ini bisa memakan waktu beberapa menit.
7. Setelah selesai, Anda akan melihat bahwa Status Jangkauan Tidak dapat dijangkau dan detail Jalur menunjukkan bahwa `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` itulah penyebab masalah jangkauan ini.

AWS CLI

1. Buat jalur jaringan menggunakan ID Internet Gateway yang ingin Anda blokir lalu lintas dari (sumber) dan ID instance yang ingin Anda blokir lalu lintas ke (tujuan):

   ```
   aws ec2 --region us-east-2 create-network-insights-path --source igw-id --
   destination instance-id --protocol TCP
   ```

2. Mulai analisis pada jalur jaringan:

```
aws ec2 --region us-east-2 start-network-insights-analysis --network-insights-
path-id nip-id
```

3. Ambil hasil analisis:

```
aws ec2 --region us-east-2 describe-network-insights-analyses --network-
insights-analysis-ids nia-id
```

4. Verifikasi `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` bahwa itu `ExplanationCode` karena kurangnya jangkauan.

Contoh lanjutan

Bagian ini berisi contoh lanjutan yang akan membantu Anda memahami cara kerja fitur Akses Publik Blok VPC dalam berbagai skenario. Setiap skenario dibangun dari skenario sebelumnya, jadi penting untuk menyelesaikan langkah-langkah secara berurutan.

> **Important**
>
> Jangan menelusuri contoh ini di akun produksi. Kami sangat menyarankan Anda meninjau secara menyeluruh beban kerja yang memerlukan akses Internet sebelum mengaktifkan VPC BPA di akun produksi Anda.

> **Note**
>
> Untuk memahami sepenuhnya fitur VPC BPA, Anda memerlukan sumber daya tertentu di akun Anda. Di bagian ini, kami menyediakan CloudFormation template yang dapat Anda gunakan untuk menyediakan sumber daya yang Anda butuhkan untuk memahami sepenuhnya cara kerja fitur ini. Ada biaya yang terkait dengan sumber daya yang Anda sediakan dengan CloudFormation template dan analisis yang Anda lakukan dengan Network Access Analyzer dan Reachability Analyzer. Jika Anda menggunakan template di bagian ini, pastikan Anda menyelesaikan langkah-langkah Pembersihan setelah Anda selesai dengan contoh ini.

Daftar Isi

- Menyebarkan CloudFormation template (opsional)
- Lihat dampak VPC BPA dengan Network Access Analyzer
- Skenario 1 - Sambungkan ke instans tanpa VPC BPA diaktifkan
- Skenario 2 - Aktifkan VPC BPA dalam mode Dua Arah
- Skenario 3 - Ubah VPC BPA ke mode Ingress-only
- Skenario 4 - Buat pengecualian
- Skenario 5 - Ubah mode pengecualian
- Skenario 6 - Ubah mode VPC BPA
- Pembersihan

Menyebarkan CloudFormation template (opsional)

Untuk menunjukkan cara kerja fitur ini, Anda memerlukan VPC, subnet, instance, dan sumber daya lainnya. Untuk mempermudah menyelesaikan demonstrasi ini, kami telah menyediakan CloudFormation template di bawah ini yang dapat Anda gunakan untuk dengan cepat memutar sumber daya yang diperlukan untuk skenario dalam demo ini. Langkah ini opsional dan Anda mungkin ingin melihat diagram di Skenario di bagian ini.

> **Note**
>
> - Ada biaya yang terkait dengan sumber daya yang Anda buat di bagian ini dengan CloudFormation template, seperti biaya gateway NAT dan alamat IPv4 publik. Untuk menghindari biaya berlebih, pastikan Anda menyelesaikan langkah-langkah Pembersihan untuk menghapus semua sumber daya yang dibuat untuk tujuan contoh ini.
> - CloudFormation Template ini membuat sumber daya dasar yang diperlukan untuk VPC BPA tetapi tidak mengaktifkan fitur VPC BPA itu sendiri. Sumber daya yang digunakan di sini dimaksudkan untuk membantu Anda memahami dan menguji fungsionalitas VPC BPA setelah Anda memilih untuk mengaktifkannya secara terpisah.

Template membuat sumber daya berikut di akun Anda:

- Egress-only gerbang internet
- gateway internet
- Gateway NAT

- Dua subnet publik
- Satu subnet pribadi
- Dua instans EC2 dengan alamat IPv4 publik dan pribadi
- Satu instance EC2 dengan alamat IPv6 dan alamat IPv4 pribadi
- Satu instance EC2 dengan alamat IPv4 pribadi saja
- Grup keamanan dengan lalu lintas masuk SSH dan ICMP diizinkan dan SEMUA lalu lintas keluar diizinkan
- Log aliran VPC
- Satu titik akhir Instans EC2 Connect di Subnet B

Salin template di bawah ini dan simpan ke file.yaml.

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Creates a VPC with public and private subnets, NAT gateway, and EC2
 instances for VPC BPA.

Parameters:
  InstanceAMI:
    Description: ID of the Amazone Machine Image (AMI) to use with the instances
 launched by this template
    Type: AWS::EC2::Image::Id
  InstanceType:
    Description: EC2 Instance type to use with the instances launched by this template
    Type: String
    Default: t2.micro

Resources:

  # VPC
  VPCBPA:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: 10.0.0.0/16
      EnableDnsHostnames: true
      EnableDnsSupport: true
      InstanceTenancy: default
      Tags:
        - Key: Name
          Value: VPC BPA
```

```
# VPC IPv6 CIDR
VPCBPAIpv6CidrBlock:
  Type: AWS::EC2::VPCCidrBlock
  Properties:
    VpcId: !Ref VPCBPA
    AmazonProvidedIpv6CidrBlock: true

# EC2 Key Pair
VPCBPAKeyPair:
  Type: AWS::EC2::KeyPair
  Properties:
    KeyName: vpc-bpa-key

# Internet Gateway
VPCBPAInternetGateway:
  Type: AWS::EC2::InternetGateway
  Properties:
    Tags:
      - Key: Name
        Value: VPC BPA Internet Gateway

VPCBPAInternetGatewayAttachment:
  Type: AWS::EC2::VPCGatewayAttachment
  Properties:
    VpcId: !Ref VPCBPA
    InternetGatewayId: !Ref VPCBPAInternetGateway

# Egress-Only Internet Gateway
VPCBPAEgressOnlyInternetGateway:
  Type: AWS::EC2::EgressOnlyInternetGateway
  Properties:
    VpcId: !Ref VPCBPA

# Subnets
VPCBPAPublicSubnetA:
  Type: AWS::EC2::Subnet
  Properties:
    VpcId: !Ref VPCBPA
    CidrBlock: 10.0.1.0/24
    MapPublicIpOnLaunch: true
    Tags:
      - Key: Name
        Value: VPC BPA Public Subnet A
```

```
  VPCBPAPublicSubnetB:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPCBPA
      CidrBlock: 10.0.2.0/24
      MapPublicIpOnLaunch: true
      Tags:
        - Key: Name
          Value: VPC BPA Public Subnet B

  VPCBPAPrivateSubnetC:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPCBPA
      CidrBlock: 10.0.3.0/24
      MapPublicIpOnLaunch: false
      Ipv6CidrBlock: !Select [0, !GetAtt VPCBPA.Ipv6CidrBlocks]
      AssignIpv6AddressOnCreation: true
      Tags:
        - Key: Name
          Value: VPC BPA Private Subnet C

  # NAT Gateway
  VPCBPANATGateway:
    Type: AWS::EC2::NatGateway
    Properties:
      AllocationId: !GetAtt VPCBPANATGatewayEIP.AllocationId
      SubnetId: !Ref VPCBPAPublicSubnetB
      Tags:
        - Key: Name
          Value: VPC BPA NAT Gateway

  VPCBPANATGatewayEIP:
    Type: AWS::EC2::EIP
    Properties:
      Domain: vpc
      Tags:
        - Key: Name
          Value: VPC BPA NAT Gateway EIP

  # Route Tables
  VPCBPAPublicRouteTable:
    Type: AWS::EC2::RouteTable
```

```
    Properties:
      VpcId: !Ref VPCBPA
      Tags:
        - Key: Name
          Value: VPC BPA Public Route Table

  VPCBPAPublicRoute:
    Type: AWS::EC2::Route
    DependsOn: VPCBPAInternetGatewayAttachment
    Properties:
      RouteTableId: !Ref VPCBPAPublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref VPCBPAInternetGateway

  VPCBPAPublicSubnetARouteTableAssoc:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      SubnetId: !Ref VPCBPAPublicSubnetA
      RouteTableId: !Ref VPCBPAPublicRouteTable

  VPCBPAPublicSubnetBRouteTableAssoc:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      SubnetId: !Ref VPCBPAPublicSubnetB
      RouteTableId: !Ref VPCBPAPublicRouteTable

  VPCBPAPrivateRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref VPCBPA
      Tags:
        - Key: Name
          Value: VPC BPA Private Route Table

  VPCBPAPrivateRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref VPCBPAPrivateRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      NatGatewayId: !Ref VPCBPANATGateway

  VPCBPAPrivateSubnetCRoute:
    Type: AWS::EC2::Route
    Properties:
```

```
      RouteTableId: !Ref VPCBPAPrivateRouteTable
      DestinationIpv6CidrBlock: ::/0
      EgressOnlyInternetGatewayId: !Ref VPCBPAEgressOnlyInternetGateway

  VPCBPAPrivateSubnetCRouteTableAssociation:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      SubnetId: !Ref VPCBPAPrivateSubnetC
      RouteTableId: !Ref VPCBPAPrivateRouteTable

  # EC2 Instances Security Group
  VPCBPAInstancesSecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupName: VPC BPA Instances Security Group
      GroupDescription: Allow SSH and ICMP access
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 22
          ToPort: 22
          CidrIp: 0.0.0.0/0
        - IpProtocol: icmp
          FromPort: -1
          ToPort: -1
          CidrIp: 0.0.0.0/0
      VpcId: !Ref VPCBPA
      Tags:
        - Key: Name
          Value: VPC BPA Instances Security Group

  # EC2 Instances
  VPCBPAInstanceA:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: !Ref InstanceAMI
      InstanceType: t2.micro
      KeyName: !Ref VPCBPAKeyPair
      SubnetId: !Ref VPCBPAPublicSubnetA
      SecurityGroupIds:
        - !Ref VPCBPAInstancesSecurityGroup
      Tags:
        - Key: Name
          Value: VPC BPA Instance A
```

```
  VPCBPAInstanceB:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: !Ref InstanceAMI
      InstanceType: !Ref InstanceType
      KeyName: !Ref VPCBPAKeyPair
      SubnetId: !Ref VPCBPAPublicSubnetB
      SecurityGroupIds:
        - !Ref VPCBPAInstancesSecurityGroup
      Tags:
        - Key: Name
          Value: VPC BPA Instance B

  VPCBPAInstanceC:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: !Ref InstanceAMI
      InstanceType: !Ref InstanceType
      KeyName: !Ref VPCBPAKeyPair
      SubnetId: !Ref VPCBPAPrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCBPAInstancesSecurityGroup
      Tags:
        - Key: Name
          Value: VPC BPA Instance C

  VPCBPAInstanceD:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: !Ref InstanceAMI
      InstanceType: !Ref InstanceType
      KeyName: !Ref VPCBPAKeyPair
      NetworkInterfaces:
        - DeviceIndex: '0'
          GroupSet:
            - !Ref VPCBPAInstancesSecurityGroup
          SubnetId: !Ref VPCBPAPrivateSubnetC
          Ipv6AddressCount: 1
      Tags:
        - Key: Name
          Value: VPC BPA Instance D

  # Flow Logs IAM Role
  VPCBPAFlowLogRole:
```

```
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service: vpc-flow-logs.amazonaws.com
            Action: 'sts:AssumeRole'
      Tags:
        - Key: Name
          Value: VPC BPA Flow Logs Role

  VPCBPAFlowLogPolicy:
    Type: AWS::IAM::Policy
    Properties:
      PolicyName: VPC-BPA-FlowLogsPolicy
      PolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Action:
              - 'logs:CreateLogGroup'
              - 'logs:CreateLogStream'
              - 'logs:PutLogEvents'
              - 'logs:DescribeLogGroups'
              - 'logs:DescribeLogStreams'
            Resource: '*'
      Roles:
        - !Ref VPCBPAFlowLogRole

  # Flow Logs
  VPCBPAFlowLog:
    Type: AWS::EC2::FlowLog
    Properties:
      ResourceId: !Ref VPCBPA
      ResourceType: VPC
      TrafficType: ALL
      LogDestinationType: cloud-watch-logs
      LogGroupName: /aws/vpc-flow-logs/VPC-BPA
      DeliverLogsPermissionArn: !GetAtt VPCBPAFlowLogRole.Arn
      LogFormat: '${version} ${account-id} ${interface-id} ${srcaddr} ${dstaddr}
 ${srcport} ${dstport} ${protocol} ${packets} ${bytes} ${start} ${end} ${action} ${log-
status} ${vpc-id} ${subnet-id} ${instance-id} ${tcp-flags} ${type} ${pkt-srcaddr}
```

```
 ${pkt-dstaddr} ${region} ${az-id} ${sublocation-type} ${sublocation-id} ${pkt-src-aws-
service} ${pkt-dst-aws-service} ${flow-direction} ${traffic-path} ${reject-reason}'
      Tags:
        - Key: Name
          Value: VPC BPA Flow Logs

  # EC2 Instance Connect Endpoint
  VPCBPAEC2InstanceConnectEndpoint:
    Type: AWS::EC2::InstanceConnectEndpoint
    Properties:
      SecurityGroupIds:
        - !Ref VPCBPAInstancesSecurityGroup
      SubnetId: !Ref VPCBPAPublicSubnetB

Outputs:
  VPCBPAVPCId:
    Description: A reference to the created VPC
    Value: !Ref VPCBPA
    Export:
      Name: vpc-id

  VPCBPAPublicSubnetAId:
    Description: The ID of the public subnet A
    Value: !Ref VPCBPAPublicSubnetA

  VPCBPAPublicSubnetAName:
    Description: The name of the public subnet A
    Value: VPC BPA Public Subnet A

  VPCBPAPublicSubnetBId:
    Description: The ID of the public subnet B
    Value: !Ref VPCBPAPublicSubnetB

  VPCBPAPublicSubnetBName:
    Description: The name of the public subnet B
    Value: VPC BPA Public Subnet B

  VPCBPAPrivateSubnetCId:
    Description: The ID of the private subnet C
    Value: !Ref VPCBPAPrivateSubnetC

  VPCBPAPrivateSubnetCName:
    Description: The name of the private subnet C
    Value: VPC BPA Private Subnet C
```

```
VPCBPAInstanceAId:
  Description: The ID of instance A
  Value: !Ref VPCBPAInstanceA

VPCBPAInstanceBId:
  Description: The ID of instance B
  Value: !Ref VPCBPAInstanceB

VPCBPAInstanceCId:
  Description: The ID of instance C
  Value: !Ref VPCBPAInstanceC

VPCBPAInstanceDId:
  Description: The ID of instance D
  Value: !Ref VPCBPAInstanceD
```

Konsol Manajemen AWS

1. Buka CloudFormation konsol dihttps://console.aws.amazon.com/cloudformation/.
2. Pilih Buat tumpukan dan unggah file template.yaml.
3. Ikuti langkah-langkah untuk meluncurkan template. Anda harus memasukkan ID gambar dan jenis instance (seperti t2.micro). Anda juga harus mengizinkan CloudFormation untuk membuat peran IAM untuk pembuatan log alur dan izin untuk CloudWatch masuk.
4. Setelah Anda meluncurkan tumpukan, lihat tab Acara untuk melihat kemajuan dan memastikan bahwa tumpukan selesai sebelum Anda melanjutkan.

AWS CLI

1. Jalankan perintah berikut untuk membuat CloudFormation tumpukan:

```
aws cloudformation create-stack --stack-name VPC-BPA-stack --template-body
 file://sampletemplate.yaml --capabilities CAPABILITY_IAM --region us-east-2
```

Output:

```
{
    "StackId": "arn:aws:cloudformation:us-east-2:470889052923:stack/VPC-BPA-
stack/8a7a2cc0-8001-11ef-b196-06386a84b72f"
```

```
}
```

2. Lihat kemajuan dan pastikan bahwa tumpukan selesai sebelum Anda melanjutkan:

```
aws cloudformation describe-stack-events --stack-name VPC-BPA-stack --region us-east-2
```

Lihat dampak VPC BPA dengan Network Access Analyzer

Di bagian ini, Anda akan menggunakan Network Access Analyzer untuk melihat sumber daya di akun Anda yang menggunakan gateway internet. Gunakan analisis ini untuk memahami dampak dari mengaktifkan VPC BPA di akun Anda dan memblokir lalu lintas.

Untuk informasi tentang ketersediaan regional Network Access Analyzer, lihat Bat asan di Panduan Peng analisis Akses Jaringan.

Konsol Manajemen AWS

1. Buka konsol AWS Network Insights dihttps://console.aws.amazon.com/networkinsights/.
2. Pilih Network Access Analyzer.
3. Pilih Buat Lingkup Akses Jaringan.
4. Pilih Men ilai dampak Akses Publik Blok VPC dan pilih Ber ikutnya.
5. Template sudah dikonfigurasi untuk menganalisis lalu lintas ke dan dari gateway internet di akun Anda. Anda dapat melihat ini di bawah Sumber dan Tujuan.
6. Pilih Berikutnya.
7. Pilih Buat Lingkup Akses Jaringan.
8. Pilih ruang lingkup yang baru saja Anda buat dan pilih Analisis.
9. Tunggu analisis selesai.
10. Lihat temuan analisis. Setiap baris di bawah Temuan menunjukkan jalur jaringan yang dapat diambil paket dalam jaringan ke atau dari gateway internet di akun Anda. Dalam hal ini, jika Anda mengaktifkan VPC BPA dan tidak ada VPC dan/atau subnet yang muncul dalam temuan ini dikonfigurasi sebagai pengecualian VPC BPA, lalu lintas ke VPC dan subnet tersebut akan dibatasi.
11. Analisis setiap temuan untuk memahami dampak VPC BPA pada sumber daya di VPC Anda.

Analisis dampak selesai.

AWS CLI

1. Buat cakupan akses jaringan:

```
aws ec2 create-network-insights-access-scope --match-paths
 "Source={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
 "Destination={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
 --region us-east-2
```

Output:

```
{
  "NetworkInsightsAccessScope": {
    "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
    "NetworkInsightsAccessScopeArn": "arn:aws:ec2:us-
east-2:470889052923:network-insights-access-scope/nis-04cad3c4b3a1d5e3e",
    "CreatedDate": "2024-09-30T15:55:53.171000+00:00",
    "UpdatedDate": "2024-09-30T15:55:53.171000+00:00"
  },
  "NetworkInsightsAccessScopeContent": {
    "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
    "MatchPaths": [
      {
        "Source": {
          "ResourceStatement": {
            "ResourceTypes": [
              "AWS::EC2::InternetGateway"
            ]
          }
        }
      },
      {
        "Destination": {
          "ResourceStatement": {
            "ResourceTypes": [
              "AWS::EC2::InternetGateway"
            ]
          }
        }
      }
    ]
  }
```

```
}
```

2. Mulai analisis lingkup:

```
aws ec2 start-network-insights-access-scope-analysis --network-insights-access-
scope-id nis-04cad3c4b3a1d5e3e --region us-east-2
```

Output:

```
{
  "NetworkInsightsAccessScopeAnalysis": {
    "NetworkInsightsAccessScopeAnalysisId": "nisa-0aa383a1938f94cd1",
    "NetworkInsightsAccessScopeAnalysisArn": "arn:aws:ec2:us-
east-2:470889052923:network-insights-access-scope-analysis/
nisa-0aa383a1938f94cd",
    "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
    "Status": "running",
    "StartDate": "2024-09-30T15:56:59.109000+00:00",
    "AnalyzedEniCount": 0
  }
}
```

3. Dapatkan hasil analisis:

```
aws ec2 get-network-insights-access-scope-analysis-findings --network-insights-
access-scope-analysis-id nisa-0aa383a1938f94cd1 --region us-east-2 --max-items 1
```

Output:

```
{
  "AnalysisFindings": [
    {
      "NetworkInsightsAccessScopeAnalysisId": "nisa-0aa383a1938f94cd1",
      "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
      "FindingId": "AnalysisFinding-1",
      "FindingComponents": [
        {
          "SequenceNumber": 1,
          "Component": {
            "Id": "igw-04a5344b4e30486f1",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:internet-gateway/
igw-04a5344b4e30486f1",
```

```
            "Name": "VPC BPA Internet Gateway"
          },
          "OutboundHeader": {
            "DestinationAddresses": [
              "10.0.1.85/32"
            ]
          },
          "InboundHeader": {
            "DestinationAddresses": [
              "10.0.1.85/32"
            ],
            "DestinationPortRanges": [
              {
                "From": 22,
                "To": 22
              }
            ],
            "Protocol": "6",
            "SourceAddresses": [
              "0.0.0.0/5",
              "100.0.0.0/10",
              "96.0.0.0/6"
            ],
            "SourcePortRanges": [
              {
                "From": 0,
                "To": 65535
              }
            ]
          },
          "Vpc": {
            "Id": "vpc-0762547ec48b6888d",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:vpc/
vpc-0762547ec48b6888d",
            "Name": "VPC BPA"
          }
        },
        {
          "SequenceNumber": 2,
          "AclRule": {
            "Cidr": "0.0.0.0/0",
            "Egress": false,
            "Protocol": "all",
            "RuleAction": "allow",
```

```
            "RuleNumber": 100
          },
          "Component": {
            "Id": "acl-06194fc3a4a03040b",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:network-acl/
acl-06194fc3a4a03040b"
          }
        },
        {
          "SequenceNumber": 3,
          "Component": {
            "Id": "sg-093dde06415d03924",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:security-group/
sg-093dde06415d03924",
            "Name": "VPC BPA Instances Security Group"
          },
          "SecurityGroupRule": {
            "Cidr": "0.0.0.0/0",
            "Direction": "ingress",
            "PortRange": {
              "From": 22,
              "To": 22
            },
            "Protocol": "tcp"
          }
        },
        {
          "SequenceNumber": 4,
          "AttachedTo": {
            "Id": "i-058db34f9a0997895",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:instance/
i-058db34f9a0997895",
            "Name": "VPC BPA Instance A"
          },
          "Component": {
            "Id": "eni-0fa23f2766f03b286",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:network-interface/
eni-0fa23f2766f03b286"
          },
          "InboundHeader": {
            "DestinationAddresses": [
              "10.0.1.85/32"
            ],
            "DestinationPortRanges": [
```

```
              {
                "From": 22,
                "To": 22
              }
            ],
            "Protocol": "6",
            "SourceAddresses": [
              "0.0.0.0/5",
              "100.0.0.0/10",
              "96.0.0.0/6"
            ],
            "SourcePortRanges": [
              {
                "From": 0,
                "To": 65535
              }
            ]
          },
          "Subnet": {
            "Id": "subnet-035d235a762eeed04",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:subnet/
subnet-035d235a762eeed04",
            "Name": "VPC BPA Public Subnet A"
          },
          "Vpc": {
            "Id": "vpc-0762547ec48b6888d",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:vpc/
vpc-0762547ec48b6888d",
            "Name": "VPC BPA"
          }
        }
      ]
    }
  ],
  "AnalysisStatus": "succeeded",
  "NetworkInsightsAccessScopeAnalysisId": "nisa-0aa383a1938f94cd1",
  "NextToken":
 "eyJOZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxfQ=="
}
```


Hasilnya menunjukkan lalu lintas ke dan dari gateway internet di semua VPC di akun Anda. Hasilnya disusun sebagai “temuan”. “FindingId“:" AnalysisFinding-1 "menunjukkan bahwa ini adalah temuan pertama dalam analisis. Perhatikan bahwa ada beberapa temuan dan

masing-masing menunjukkan aliran lalu lintas yang akan terpengaruh dengan mengaktifkan VPC BPA. Temuan pertama akan menunjukkan bahwa lalu lintas dimulai di gateway internet (” SequenceNumber “: 1), diteruskan ke NACL (” SequenceNumber “: 2) ke grup keamanan (” SequenceNumber “: 3) dan berakhir pada instance (” SequenceNumber “: 4).

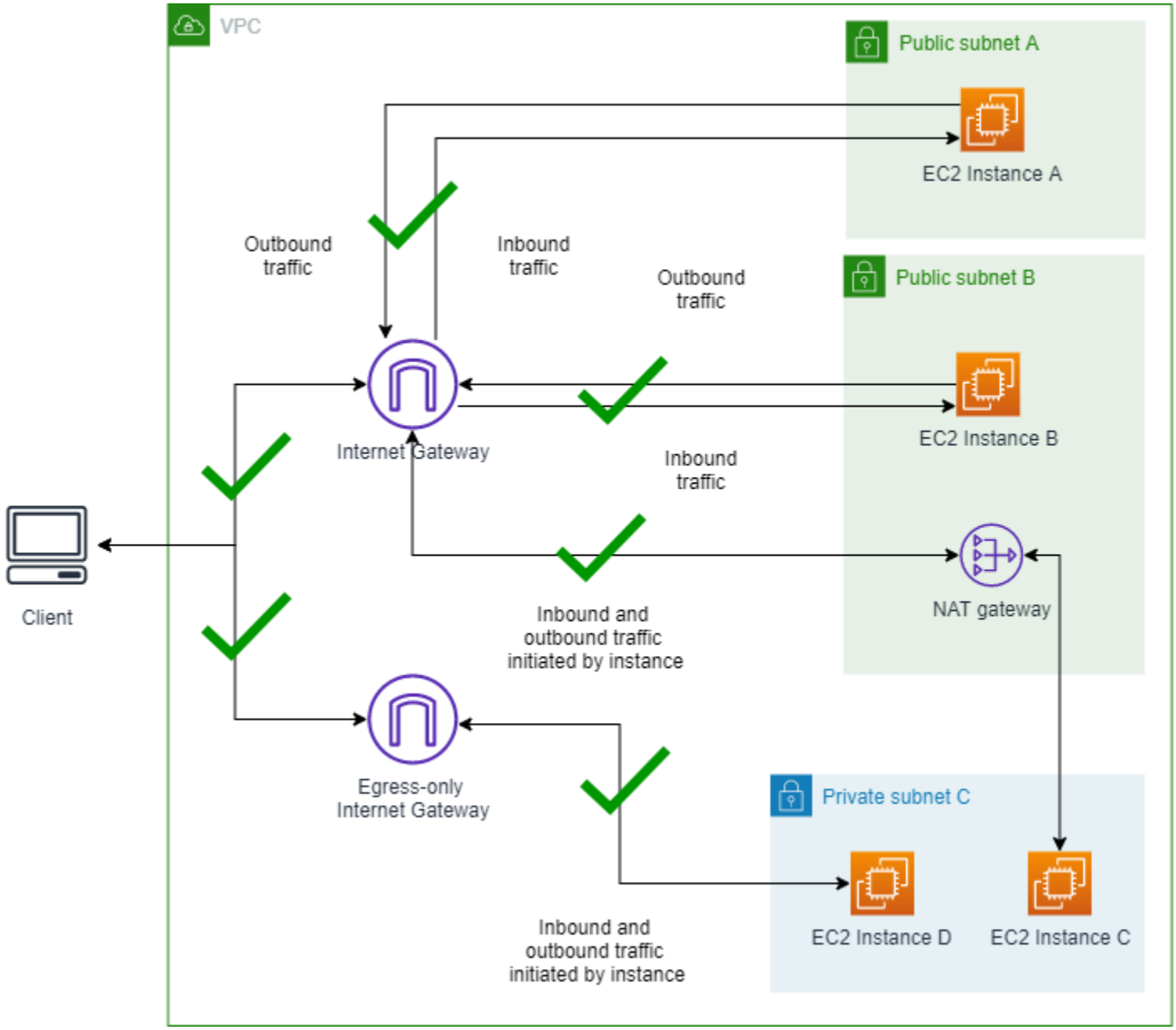
4. Analisis temuan untuk memahami dampak VPC BPA pada sumber daya di VPC Anda.

Analisis dampak selesai.

Skenario 1 - Sambungkan ke instans tanpa VPC BPA diaktifkan

Pada bagian ini, instans EC2 di subnet publik A dan B dapat dijangkau dari internet melalui gateway internet, yang memungkinkan lalu lintas masuk dan keluar. Instans C dan D di subnet pribadi dapat memulai lalu lintas keluar melalui gateway NAT atau gateway internet khusus keluar, tetapi tidak dapat dijangkau langsung dari internet. Pengaturan ini menyediakan akses internet ke beberapa sumber daya sambil melindungi yang lain. Tujuan dari pengaturan ini adalah untuk menetapkan baseline dan memastikan bahwa, sebelum Anda mengaktifkan VPC BPA, semua instans dapat dicapai, Anda akan terhubung ke semua instance dan melakukan ping ke alamat IP publik.

Diagram VPC tanpa VPC BPA dihidupkan:



1.1 Hubungkan ke instance

Lengkapi bagian ini untuk menyambung ke instans Anda dengan VPC BPA dimatikan untuk memastikan Anda dapat terhubung tanpa masalah. Semua instance yang dibuat dengan CloudFormation contoh ini memiliki nama seperti, “Instans BPA VPC A”.

Konsol Manajemen AWS

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Buka detail Instance A.

3. Sambungkan ke instans A menggunakan opsi EC2 Instance Connect > Connect menggunakan EC2 Instance Connect Endpoint.
4. Pilih Hubungkan. Setelah Anda berhasil terhubung ke instance, ping www.amazon.com untuk memverifikasi bahwa Anda dapat mengirim permintaan keluar ke internet.
5. Gunakan metode yang sama yang Anda gunakan untuk menyambung ke instance A untuk terhubung ke instans B, C, dan D. Dari setiap instance, ping www.amazon.com untuk memverifikasi bahwa Anda dapat mengirim permintaan keluar ke internet.

AWS CLI

1. Ping Instance A menggunakan alamat IPv4 publik untuk memeriksa lalu lintas masuk:

```
ping 18.225.8.244
```

Output:

```
Pinging 18.225.8.244 with 32 bytes of data:

Reply from 18.225.8.244: bytes=32 time=51ms TTL=110
Reply from 18.225.8.244: bytes=32 time=61ms TTL=110
```

Perhatikan bahwa ping berhasil dan lalu lintas tidak diblokir.

2. Gunakan alamat IPv4 pribadi untuk menghubungkan dan memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~._.   _/
/ /
```

```
/m/'
Last login: Fri Sep 27 18:27:57 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING www-amazon-com.customer.fastly.net (18.65.233.187) 56(84) bytes of data.
64 bytes from 18.65.233.187 (18.65.233.187): icmp_seq=15 ttl=58 time=2.06 ms
64 bytes from 18.65.233.187 (18.65.233.187): icmp_seq=16 ttl=58 time=2.26 ms
```

Perhatikan bahwa ping berhasil dan lalu lintas tidak diblokir.

3. Ping Instance B menggunakan alamat IPv4 publik untuk memeriksa lalu lintas masuk:

```
ping 3.18.106.198
```

Output:

```
Pinging 3.18.106.198 with 32 bytes of data:
Reply from 3.18.106.198: bytes=32 time=83ms TTL=110
Reply from 3.18.106.198: bytes=32 time=54ms TTL=110
```

Perhatikan bahwa ping berhasil dan lalu lintas tidak diblokir.

4. Gunakan alamat IPv4 pribadi untuk menghubungkan dan memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id  i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.
Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
/ /
/m/'
Last login: Fri Sep 27 18:12:27 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

```
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=249 time=1.55 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=249 time=1.67 ms
```

Perhatikan bahwa ping berhasil dan lalu lintas tidak diblokir.

5. Hubungkan ke Instance C. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian melakukan ping ke IP publik dari instance untuk memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.
Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
/ /
/m/'
Last login: Thu Sep 19 20:31:26 2024 from 10.0.2.86
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=248 time=1.75 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=248 time=1.97 ms
64 bytes from server-3-160-24-26.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=3 ttl=248 time=1.08 ms
```

Perhatikan bahwa ping berhasil dan lalu lintas tidak diblokir.

6. Hubungkan ke Instance D. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian melakukan ping ke IP publik dari instance untuk memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Output:

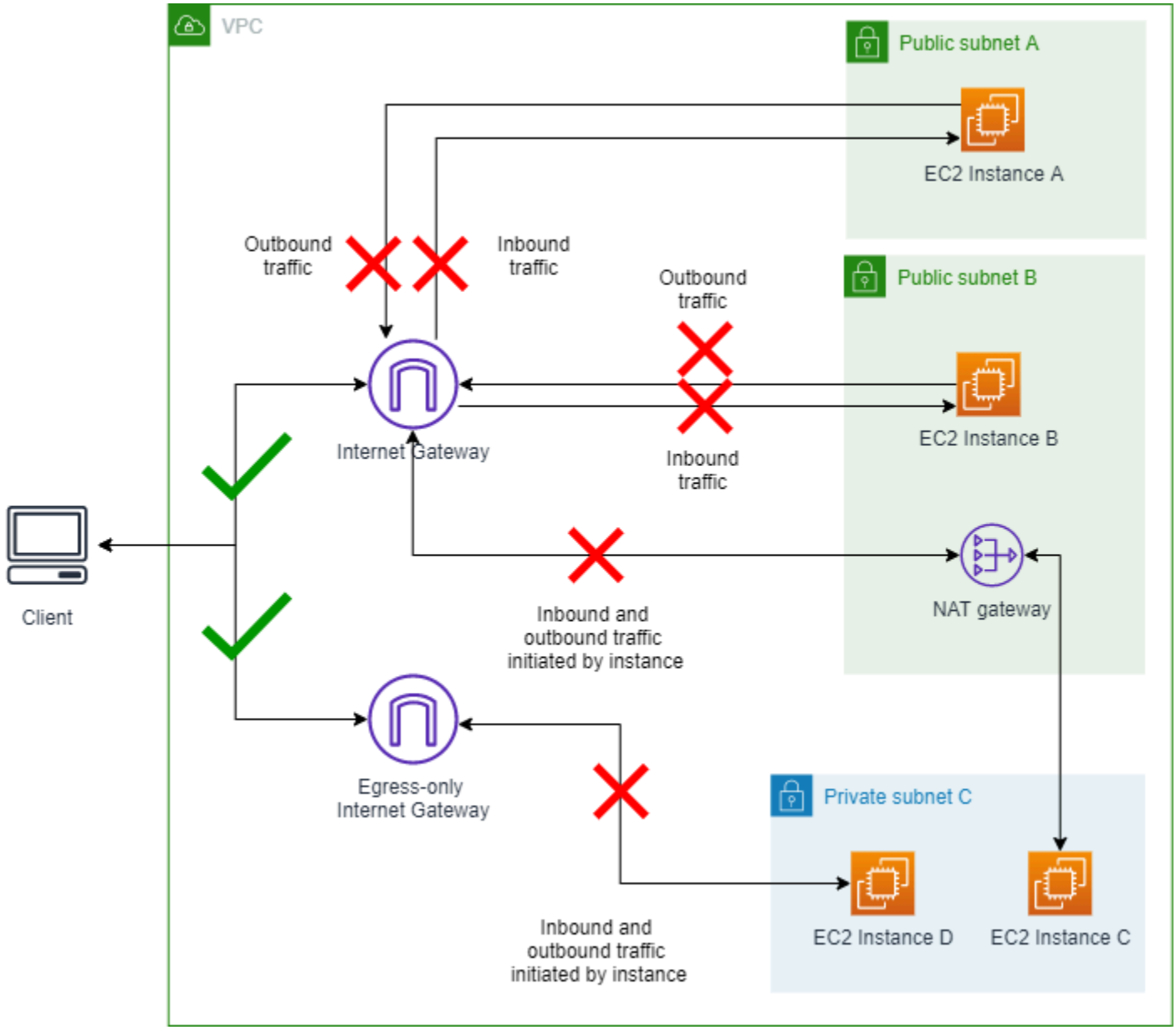
```
The authenticity of host '10.0.3.59 can't be established.
ECDSA key fingerprint is SHA256:c4naBCqbC61/cExDyccEproNU+1HHSpMSzl2J6cOtIZA8g.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.3.59' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ _/
_/m/'
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:ee00:7:49a5:5fd4:b121
 (2600:9000:25f3:ee00:7:49a5:5fd4:b121)) 56 data bytes
64 bytes from 2600:9000:25f3:ee00:7:49a5:5fd4:b121
 (2600:9000:25f3:ee00:7:49a5:5fd4:b121): icmp_seq=1 ttl=58 time=1.19 ms
64 bytes from 2600:9000:25f3:ee00:7:49a5:5fd4:b121
 (2600:9000:25f3:ee00:7:49a5:5fd4:b121): icmp_seq=2 ttl=58 time=1.38 ms
```

Perhatikan bahwa ping berhasil dan lalu lintas tidak diblokir.

Skenario 2 - Aktifkan VPC BPA dalam mode Dua Arah

Di bagian ini Anda akan mengaktifkan VPC BPA dan memblokir lalu lintas ke dan dari gateway internet di akun Anda.

Diagram yang menunjukkan mode dua arah VPC BPA dihidupkan:



2.1 Aktifkan mode dua arah VPC BPA

Lengkapi bagian ini untuk mengaktifkan VPC BPA. Mode dua arah VPC BPA memblokir semua lalu lintas ke dan dari gateway internet dan gateway internet khusus keluar di Wilayah ini (kecuali untuk VPC dan subnet yang dikecualikan).

Konsol Manajemen AWS

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi kiri, pilih Peng aturan.
3. Pilih Edit pengaturan akses publik.

4. Pilih Aktifkan blokir akses publik dan Dua arah, lalu pilih S impan perubahan.
5. Tunggu Status berubah menjadi Aktif. Mungkin perlu beberapa menit agar pengaturan VPC BPA berlaku dan status diperbarui.

VPC BPA sekarang aktif.

AWS CLI

1. Gunakan perintah modify-vpc-block-public-access-options untuk mengaktifkan VPC BPA:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-
gateway-block-mode block-bidirectional
```

   Mungkin perlu beberapa menit agar pengaturan VPC BPA berlaku dan status diperbarui.
2. Lihat status VPC BPA:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

2.2 Hubungkan ke instance

Lengkapi bagian ini untuk menyambung ke instans Anda.

Konsol Manajemen AWS

1. Ping alamat IPv4 publik Instance A dan Instance B seperti yang Anda lakukan dalam Skenario 1. Perhatikan bahwa lalu lintas diblokir.
2. Sambungkan ke instans A menggunakan opsi EC2 Instance Connect > Connect menggunakan EC2 Instance Connect Endpoint seperti yang Anda lakukan di Skenario 1. Pastikan Anda menggunakan opsi endpoint.
3. Pilih Hubungkan. Setelah Anda berhasil terhubung ke instance, ping www.amazon.com. Perhatikan bahwa semua lalu lintas keluar diblokir.
4. Gunakan metode yang sama yang Anda gunakan untuk menyambung ke instance A untuk terhubung ke instance B, C, dan D, menguji permintaan keluar ke internet. Perhatikan bahwa semua lalu lintas keluar diblokir.

AWS CLI

1. Ping Instance A menggunakan alamat IPv4 publik untuk memeriksa lalu lintas masuk:

```
ping 18.225.8.244
```

Output:

```
Pinging 18.225.8.244 with 32 bytes of data:

Request timed out.
```

Perhatikan bahwa ping gagal dan lalu lintas diblokir.

2. Gunakan alamat IPv4 pribadi untuk menghubungkan dan memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Output:

```
The authenticity of host '10.0.1.85' can't be established.
ECDSA key fingerprint is SHA256:3zo/gSss+HAZ+7eTyWlOB/Ke04IM+hadjsoLJeRTWBk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.1.85' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~._.   _/
/ /
/m/'
Last login: Fri Sep 27 14:16:53 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Perhatikan bahwa ping gagal dan lalu lintas diblokir.

3. Ping Instance B menggunakan alamat IPv4 publik untuk memeriksa lalu lintas masuk:

```
ping 3.18.106.198
```

Output:

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Perhatikan bahwa ping gagal dan lalu lintas diblokir.

4. Gunakan alamat IPv4 pribadi untuk menghubungkan dan memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id  i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

Output:

```
The authenticity of host '10.0.2.98' can't be established.
ECDSA key fingerprint is SHA256:0IjXKKyVlDthcCfI0IPIJMUiItAOLYKRNLGTYURnFXo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.98' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
/ /
/m/'
Last login: Fri Sep 27 14:18:16 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Perhatikan bahwa ping gagal dan lalu lintas diblokir.

5. Hubungkan ke Instance C. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian melakukan ping ke IP publik dari instance untuk memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
/ /
/m/'
Last login: Tue Sep 24 15:17:56 2024 from 10.0.2.86
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Perhatikan bahwa ping gagal dan lalu lintas diblokir.

6. Hubungkan ke Instance D. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian melakukan ping ke IP publik dari instance untuk memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ _/
_/m/'
Last login: Fri Sep 27 16:42:01 2024 from 3.16.146.5
```

```
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:8200:7:49a5:5fd4:b121
 (2600:9000:25f3:8200:7:49a5:5fd4:b121)) 56 data bytes
```

Perhatikan bahwa ping gagal dan lalu lintas diblokir.

2.3 Opsional: Verifikasi konektivitas diblokir dengan Reachability Analyzer

VPC Reachability Analyzer dapat digunakan untuk memahami apakah jalur jaringan tertentu dapat dicapai dengan konfigurasi jaringan Anda, termasuk pengaturan VPC BPA. Dalam contoh ini Anda akan menganalisis jalur jaringan yang sama yang dicoba sebelumnya untuk mengonfirmasi bahwa VPC BPA adalah alasan mengapa konektivitas gagal.

Konsol Manajemen AWS

1. Buka konsol Network Insights dihttps://console.aws.amazon.com/networkinsights/home#ReachabilityAnalyzer.
2. Pilih Buat dan analisis jalur.
3. Untuk Jenis Sumber, pilih Internet Gateway dan pilih gateway internet dengan tag VPC BPA Internet Gateway dari dropdown Sumber.
4. Untuk Tipe Tujuan, pilih Instans dan pilih instance yang ditandai dengan Instans BPA VPC A dari dropdown Tujuan.
5. Pilih Buat dan analisis jalur.
6. Tunggu analisis selesai. Ini bisa memakan waktu beberapa menit.
7. Setelah selesai, Anda akan melihat bahwa Status J angkauan Tidak dapat dij angkau dan detail Jalur menunjukkan bahwa `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` itulah penyebabnya.

AWS CLI

1. Buat jalur jaringan menggunakan ID gateway internet dengan tag VPC BPA Internet Gateway dan ID instance yang diberi tag VPC BPA Instance A:

```
aws ec2 --region us-east-2 create-network-insights-path --source igw-id --
destination instance-id --protocol TCP
```

2. Mulai analisis pada jalur jaringan:

```
aws ec2 --region us-east-2 start-network-insights-analysis --network-insights-
path-id nip-id
```

3. Ambil hasil analisis:

```
aws ec2 --region us-east-2 describe-network-insights-analyses --network-
insights-analysis-ids nia-id
```

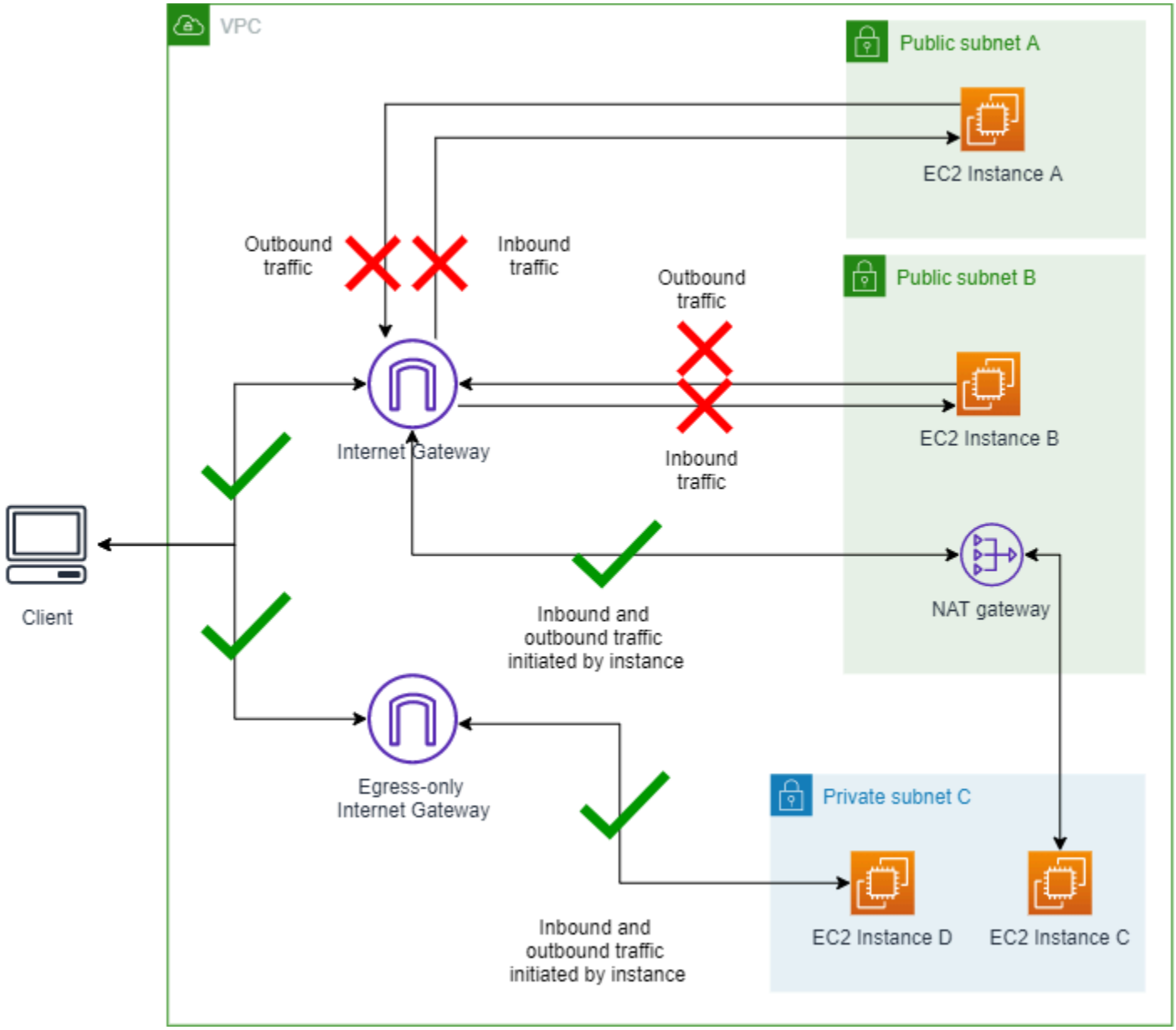
4. Verifikasi `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` bahwa itu `ExplanationCode` karena kurangnya jangkauan.

Perhatikan bahwa Anda juga bisaPantau dampak BPA VPC dengan log aliran.

Skenario 3 - Ubah VPC BPA ke mode Ingress-only

Di bagian ini Anda akan mengubah arah lalu lintas VPC BPA dan hanya mengizinkan lalu lintas yang menggunakan gateway NAT atau gateway internet khusus keluar. Instans EC2 A dan B di subnet publik tidak dapat dijangkau dari internet karena BPA memblokir lalu lintas masuk melalui Internet Gateway. Instans C dan D di subnet pribadi akan tetap dapat memulai lalu lintas keluar melalui gateway NAT dan gateway internet khusus keluar, dan oleh karena itu masih dapat mencapai internet.

Diagram Ingress-only mode VPC BPA dihidupkan:



3.1 Ubah mode ke input saja

Lengkapi bagian ini untuk mengubah mode.

Konsol Manajemen AWS

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi kiri, pilih Peng aturan.
3. Di tab Blokir akses publik, pilih Edit pengaturan akses publik.
4. Ubah pengaturan akses publik di konsol VPC dan ubah arah ke Ingress-only.

5. Simpan perubahan dan tunggu status diperbarui. Mungkin perlu beberapa menit agar pengaturan VPC BPA berlaku dan status diperbarui.

AWS CLI

1. Ubah mode VPC BPA:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-
gateway-block-mode block-ingress
```

   Mungkin perlu beberapa menit agar pengaturan VPC BPA berlaku dan status diperbarui.

2. Lihat status VPC BPA:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

3.2 Hubungkan ke instance

Lengkapi bagian ini untuk terhubung ke instance.

Konsol Manajemen AWS

1. Ping alamat IPv4 publik Instance A dan Instance B seperti yang Anda lakukan dalam Skenario 1. Perhatikan bahwa lalu lintas diblokir.
2. Hubungkan ke Instans A dan B menggunakan koneksi instans EC2 seperti yang Anda lakukan di Skenario 1 dan ping www.amazon.com darinya. Perhatikan bahwa Anda tidak dapat melakukan ping ke situs publik di internet dari Instance A atau B dan lalu lintas diblokir.
3. Hubungkan ke Instans C dan D menggunakan koneksi instans EC2 seperti yang Anda lakukan di Skenario 1 dan ping www.amazon.com darinya. Perhatikan bahwa Anda dapat melakukan ping ke situs publik di internet dari Instance C atau D dan lalu lintas diperbolehkan.

AWS CLI

1. Ping Instance A menggunakan alamat IPv4 publik untuk memeriksa lalu lintas masuk:

```
ping 18.225.8.244
```

Output:

```
Pinging 18.225.8.244 with 32 bytes of data:

Request timed out.
```

Perhatikan bahwa ping gagal dan lalu lintas diblokir.

2. Gunakan alamat IPv4 pribadi untuk menghubungkan dan memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Output:

```
The authenticity of host '10.0.1.85' can't be established.
ECDSA key fingerprint is SHA256:3zo/gSss+HAZ+7eTyWlOB/Ke04IM+hadjsoLJeRTWBk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.1.85' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~._.   _/
/ /
/m/'
Last login: Fri Sep 27 14:16:53 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Perhatikan bahwa ping gagal dan lalu lintas diblokir.

3. Ping Instance B menggunakan alamat IPv4 publik untuk memeriksa lalu lintas masuk:

```
ping 3.18.106.198
```

Output:

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Perhatikan bahwa ping gagal dan lalu lintas diblokir.

4. Gunakan alamat IPv4 pribadi untuk menghubungkan dan memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

Output:

```
The authenticity of host '10.0.2.98 ' can't be established.
ECDSA key fingerprint is SHA256:0IjXKKyVlDthcCfI0IPIJMUiItAOLYKRNLGTYURnFXo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.98' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ /
/m/'
Last login: Fri Sep 27 14:18:16 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Perhatikan bahwa ping gagal dan lalu lintas diblokir.

5. Hubungkan ke Instance C. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian melakukan ping ke IP publik dari instance untuk memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'

Last login: Tue Sep 24 15:28:09 2024 from 10.0.2.86

[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com

PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.

64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=248 time=1.84 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=248 time=1.40 ms
```

Perhatikan bahwa ping berhasil dan lalu lintas tidak diblokir.

6. Hubungkan ke Instance D. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian melakukan ping ke IP publik dari instance untuk memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
```

```
        _/ _/
      _/m/'
Last login: Fri Sep 27 16:48:38 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:5800:7:49a5:5fd4:b121
 (2600:9000:25f3:5800:7:49a5:5fd4:b121)) 56 data bytes
64 bytes from 2600:9000:25f3:5800:7:49a5:5fd4:b121
 (2600:9000:25f3:5800:7:49a5:5fd4:b121): icmp_seq=14 ttl=58 time=1.47 ms
64 bytes from 2600:9000:25f3:5800:7:49a5:5fd4:b121
 (2600:9000:25f3:5800:7:49a5:5fd4:b121): icmp_seq=16 ttl=58 time=1.59 ms
```

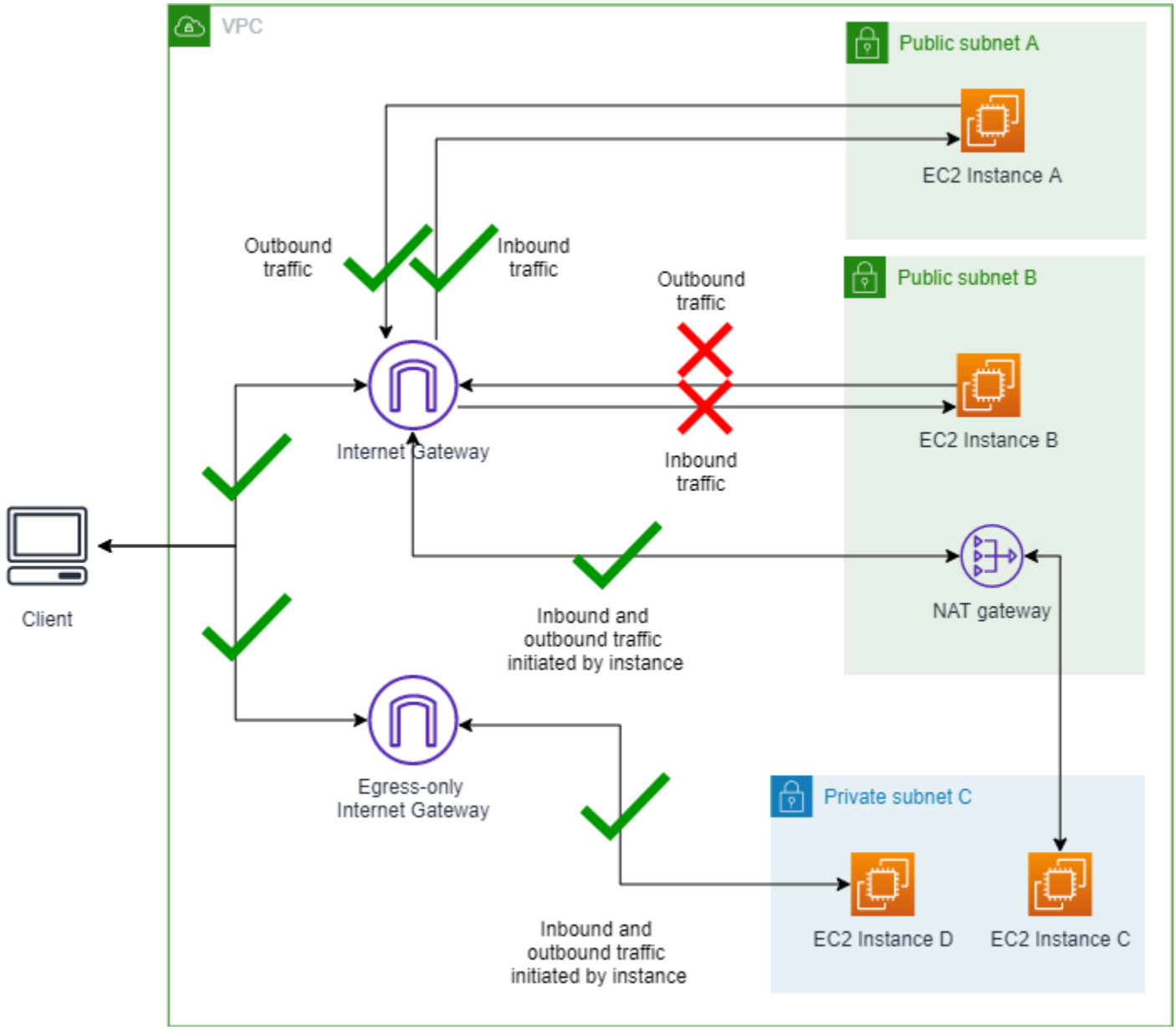
Perhatikan bahwa ping berhasil dan lalu lintas tidak diblokir.

Skenario 4 - Buat pengecualian

Di bagian ini, Anda akan membuat pengecualian. VPC BPA kemudian hanya akan memblokir lalu lintas di subnet tanpa pengecualian. Pengecualian VPC BPA adalah mode yang dapat diterapkan ke satu VPC atau subnet yang membebaskannya dari mode BPA VPC akun dan akan memungkinkan akses dua arah atau hanya keluar. Anda dapat membuat pengecualian VPC BPA untuk VPC dan subnet bahkan ketika VPC BPA tidak diaktifkan di akun untuk memastikan bahwa tidak ada gangguan lalu lintas pada pengecualian saat VPC BPA diaktifkan.

Dalam contoh ini, kita akan membuat pengecualian untuk Subnet A untuk menunjukkan bagaimana lalu lintas ke pengecualian dipengaruhi oleh BPA VPC.

Diagram Ingress-only mode VPC BPA dihidupkan dan pengecualian Subnet A dengan mode Dua Arah dihidupkan:



4.1 Buat pengecualian untuk Subnet A

Lengkapi bagian ini untuk membuat pengecualian. Pengecualian VPC BPA adalah mode yang dapat diterapkan ke satu VPC atau subnet yang membebaskannya dari mode BPA VPC akun dan akan memungkinkan akses dua arah atau hanya keluar. Anda dapat membuat pengecualian VPC BPA untuk VPC dan subnet bahkan ketika VPC BPA tidak diaktifkan di akun untuk memastikan bahwa tidak ada gangguan lalu lintas pada pengecualian saat VPC BPA diaktifkan.

Konsol Manajemen AWS

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.

2. Di panel navigasi kiri, pilih Peng aturan.
3. Di tab Blokir akses publik, di bawah Peng ecualian, pilih Buat pengecualian.
4. Pilih VPC BPA Public Subnet A, pastikan bahwa izinkan arah Dua Arah dipilih, dan pilih Buat pengecualian.
5. Tunggu status Pengecualian berubah menjadi Aktif. Anda mungkin perlu menyegarkan tabel pengecualian untuk melihat perubahan.

Pengecualian telah dibuat.

AWS CLI

1. Ubah pengecualian izinkan arah:

```
aws ec2 --region us-east-2 create-vpc-block-public-access-exclusion --subnet-
id subnet-id --internet-gateway-exclusion-mode allow-bidirectional
```

2. Butuh waktu untuk memperbarui status pengecualian. Untuk melihat status pengecualian:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-exclusions --
exclusion-ids exclusion-id
```

4.2 Hubungkan ke instans

Lengkapi bagian ini untuk terhubung ke instance.

Konsol Manajemen AWS

1. Ping alamat IPv4 publik Instance A. Perhatikan bahwa lalu lintas diperbolehkan.
2. Ping alamat IPv4 publik Instance B. Perhatikan bahwa lalu lintas diblokir.
3. Hubungkan ke Instans A menggunakan koneksi instans EC2 seperti yang Anda lakukan di Skenario 1 dan ping www.amazon.com. Perhatikan bahwa Anda dapat melakukan ping ke situs publik di internet dari Instance A. Lalu lintas diperbolehkan.
4. Hubungkan ke Instans B menggunakan koneksi instans EC2 seperti yang Anda lakukan di Skenario 1 dan ping www.amazon.com darinya. Perhatikan bahwa Anda tidak dapat melakukan ping ke situs publik di internet dari Instance B. Lalu lintas diblokir.

5. Hubungkan ke Instans C dan D menggunakan koneksi instans EC2 seperti yang Anda lakukan di Skenario 1 dan ping www.amazon.com darinya. Perhatikan bahwa Anda dapat melakukan ping ke situs publik di internet dari Instance C atau D. Lalu lintas diperbolehkan.

AWS CLI

1. Ping Instance A menggunakan alamat IPv4 publik untuk memeriksa lalu lintas masuk:

```
ping 18.225.8.244
```

Output:

```
Pinging 18.225.8.244 with 32 bytes of data:

Reply from 18.225.8.244: bytes=32 time=51ms TTL=110
Reply from 18.225.8.244: bytes=32 time=61ms TTL=110
```

Perhatikan bahwa ping berhasil dan lalu lintas tidak diblokir.

2. Gunakan alamat IPv4 pribadi untuk menghubungkan dan memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~._.   _/
/ /
/m/'
Last login: Fri Sep 27 17:58:12 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=249 time=1.03 ms
```

```
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=249 time=1.72 ms
```

Perhatikan bahwa ping berhasil dan lalu lintas tidak diblokir.

3. Ping Instance B menggunakan alamat IPv4 publik untuk memeriksa lalu lintas masuk:

```
ping 3.18.106.198
```

Output:

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Perhatikan bahwa ping gagal dan lalu lintas diblokir.

4. Gunakan alamat IPv4 pribadi untuk menghubungkan dan memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ /
/m/'
Last login: Fri Sep 27 18:12:03 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Perhatikan bahwa ping gagal dan lalu lintas diblokir.

5. Hubungkan ke Instance C. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian melakukan ping ke IP publik dari instance untuk memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Output

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ /
/m/'

Last login: Tue Sep 24 15:28:09 2024 from 10.0.2.86

[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com

PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.

64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=248 time=1.84 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=248 time=1.40 ms
```

Perhatikan bahwa ping berhasil dan lalu lintas tidak diblokir.

6. Hubungkan ke Instance D. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian melakukan ping ke IP publik dari instance untuk memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Output

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
```

```
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:00:52 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING
 www.amazon.com(g2600-141f-4000-059a-0000-0000-0000-3bd4.deploy.static.akamaitechnologie
 (2600:141f:4000:59a::3bd4)) 56 data bytes
64 bytes from
 g2600-141f-4000-059a-0000-0000-0000-3bd4.deploy.static.akamaitechnologies.com
 (2600:141f:4000:59a::3bd4): icmp_seq=1 ttl=48 time=15.9 ms
64 bytes from
 g2600-141f-4000-059a-0000-0000-0000-3bd4.deploy.static.akamaitechnologies.com
 (2600:141f:4000:59a::3bd4): icmp_seq=2 ttl=48 time=15.8 ms
```

Perhatikan bahwa ping berhasil dan lalu lintas tidak diblokir.

4.3 Opsional: Verifikasi konektivitas dengan Reachability Analyzer

Menggunakan jalur jaringan yang sama yang dibuat di Reachability Analyzer di Skenario 2, Anda sekarang dapat menjalankan analisis baru dan mengonfirmasi bahwa jalur dapat dijangkau sekarang karena pengecualian telah dibuat untuk Subnet Publik A.

Untuk informasi tentang ketersediaan regional Reachability Analyzer, lihat Per timbangan dalam Panduan Penganalisis Jang kauan.

Konsol Manajemen AWS

1. Dari Jalur Jaringan yang Anda buat sebelumnya di konsol Network Insights, pilih Re-run analisis.
2. Tunggu analisis selesai. Mungkin butuh beberapa menit.
3. Konfirmasikan bahwa jalur sekarang dapat dijangkau.

AWS CLI

1. Menggunakan ID jalur jaringan yang dibuat sebelumnya, mulailah analisis baru:

```
aws ec2 --region us-east-2 start-network-insights-analysis --network-insights-path-id nip-id
```

2. Ambil hasil analisis:

```
aws ec2 --region us-east-2 describe-network-insights-analyses --network-insights-analysis-ids nia-id
```

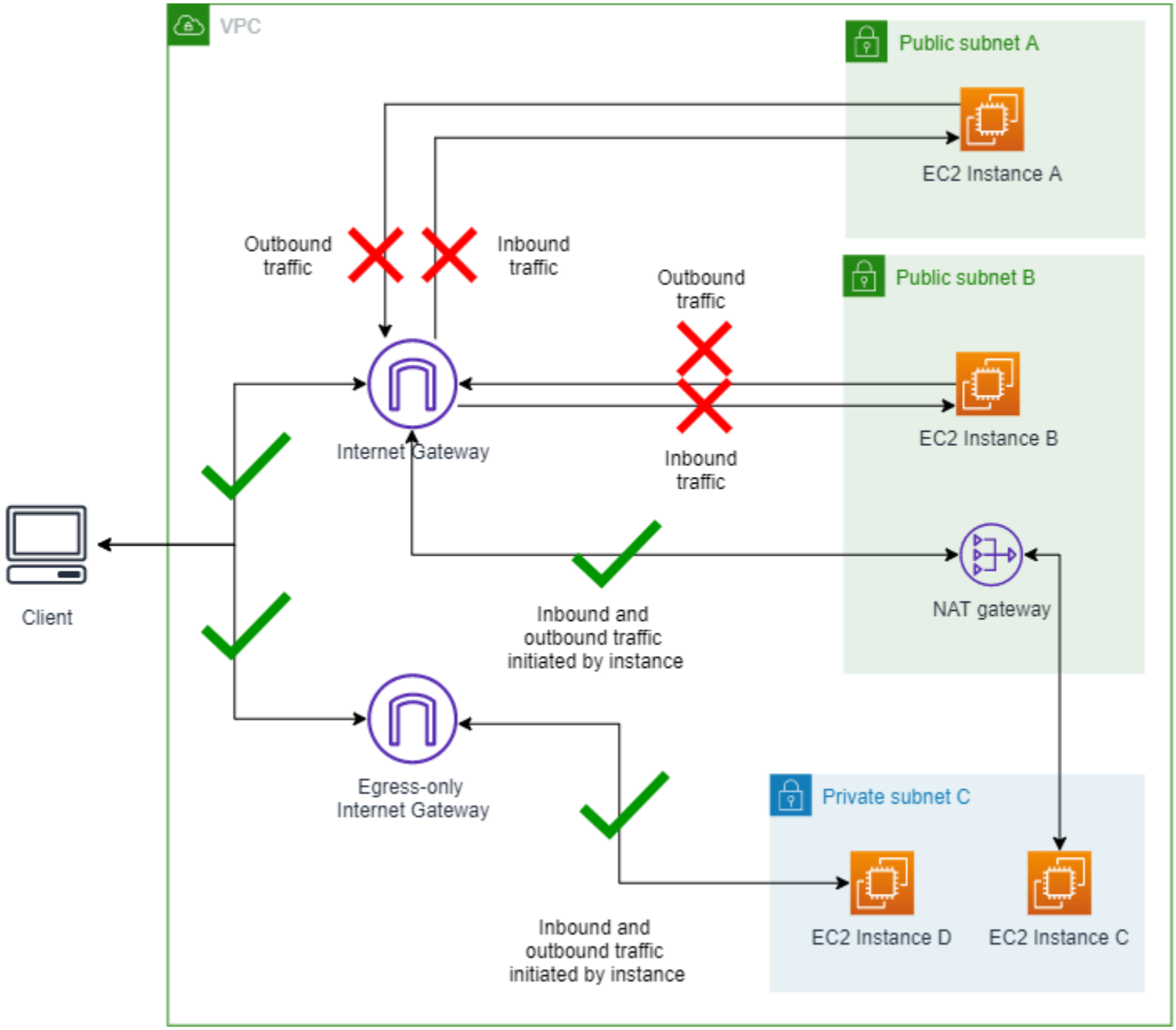
3. Konfirmasikan bahwa kode `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` penjelasan tidak lagi ada.

Skenario 5 - Ubah mode pengecualian

Di bagian ini Anda akan mengubah arah lalu lintas izinkan pada pengecualian untuk melihat bagaimana pengaruhnya terhadap VPC BPA.

> **Note**
>
> Dalam skenario ini, Anda akan mengubah mode pengecualian menjadi Egress-only. Perhatikan bahwa ketika Anda melakukan ini, Egress-only pengecualian pada Subnet A tidak mengizinkan lalu lintas keluar, yang berlawanan dengan intuisi karena Anda mengharapkannya mengizinkan lalu lintas keluar. Namun, karena BPA tingkat akun adalah Ingress-only, peng Egress-only ecualian diabaikan, dan perutean Subnet A ke gateway internet dibatasi oleh VPC BPA, memblokir lalu lintas keluar. Untuk mengaktifkan lalu lintas keluar di Subnet A, Anda harus mengalihkan VPC BPA ke mode Dua Arah.

Diagram Ingress-only mode VPC BPA dihidupkan dan pengecualian Subnet A dengan mode khusus keluar diaktifkan:



5.1 Ubah pengecualian izinkan arah ke pintu keluar saja

Lengkapi bagian ini untuk mengubah arah izin pengecualian.

Konsol Manajemen AWS

1. Edit pengecualian yang Anda buat di Skenario 4 dan ubah arah izinkan ke Egress-only.
2. Pilih Simpan perubahan.
3. Tunggu status Pengecualian berubah menjadi Aktif. Mungkin perlu beberapa menit agar pengaturan VPC BPA berlaku dan status diperbarui. Anda mungkin perlu menyegarkan tabel pengecualian untuk melihat perubahan.

AWS CLI

1. Ubah pengecualian izinkan arah:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-exclusion --exclusion-
id exclusion-id --internet-gateway-exclusion-mode allow-egress
```

   Mungkin perlu beberapa menit agar pengaturan VPC BPA berlaku dan status diperbarui.

2. Butuh waktu untuk memperbarui status pengecualian. Untuk melihat status pengecualian:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-exclusion
```

5.2 Sambungkan ke instans

Lengkapi bagian ini untuk terhubung ke instance.

Konsol Manajemen AWS

1. Ping alamat IPv4 publik Instance A dan B. Perhatikan bahwa lalu lintas diblokir.
2. Hubungkan ke Instans A dan B menggunakan koneksi instans EC2 seperti yang Anda lakukan di Skenario 1 dan ping www.amazon.com. Perhatikan bahwa Anda tidak dapat melakukan ping ke situs publik di internet dari Instance A atau B. Lalu lintas diblokir.
3. Hubungkan ke Instans C dan D menggunakan koneksi instans EC2 seperti yang Anda lakukan di Skenario 1 dan ping www.amazon.com darinya. Perhatikan bahwa Anda dapat melakukan ping ke situs publik di internet dari Instance C atau D. Lalu lintas diperbolehkan.

AWS CLI

1. Ping Instance A menggunakan alamat IPv4 publik untuk memeriksa lalu lintas masuk:

```
ping 18.225.8.244
```

   Output:

```
Pinging 18.225.8.244 with 32 bytes of data:
Request timed out.
```

Perhatikan bahwa ping gagal dan lalu lintas diblokir.

2. Gunakan alamat IPv4 pribadi untuk menghubungkan dan memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:09:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Perhatikan bahwa ping gagal dan lalu lintas diblokir.

3. Ping Instance B menggunakan alamat IPv4 publik untuk memeriksa lalu lintas masuk:

```
ping 3.18.106.198
```

Output:

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Perhatikan bahwa ping gagal dan lalu lintas diblokir.

4. Gunakan alamat IPv4 pribadi untuk menghubungkan dan memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:09:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Perhatikan bahwa ping gagal dan lalu lintas diblokir.

5. Hubungkan ke Instance C. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian melakukan ping ke IP publik dari instance untuk memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:00:31 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:a600:7:49a5:5fd4:b121
 (2600:9000:25f3:a600:7:49a5:5fd4:b121)) 56 data bytes
```

```
64 bytes from 2600:9000:25f3:a600:7:49a5:5fd4:b121
 (2600:9000:25f3:a600:7:49a5:5fd4:b121): icmp_seq=1 ttl=58 time=1.51 ms
64 bytes from 2600:9000:25f3:a600:7:49a5:5fd4:b121
 (2600:9000:25f3:a600:7:49a5:5fd4:b121): icmp_seq=2 ttl=58 time=1.49 ms
```

Perhatikan bahwa ping berhasil dan lalu lintas tidak diblokir.

6. Hubungkan ke Instance D. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian melakukan ping ke IP publik dari instance untuk memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Output:

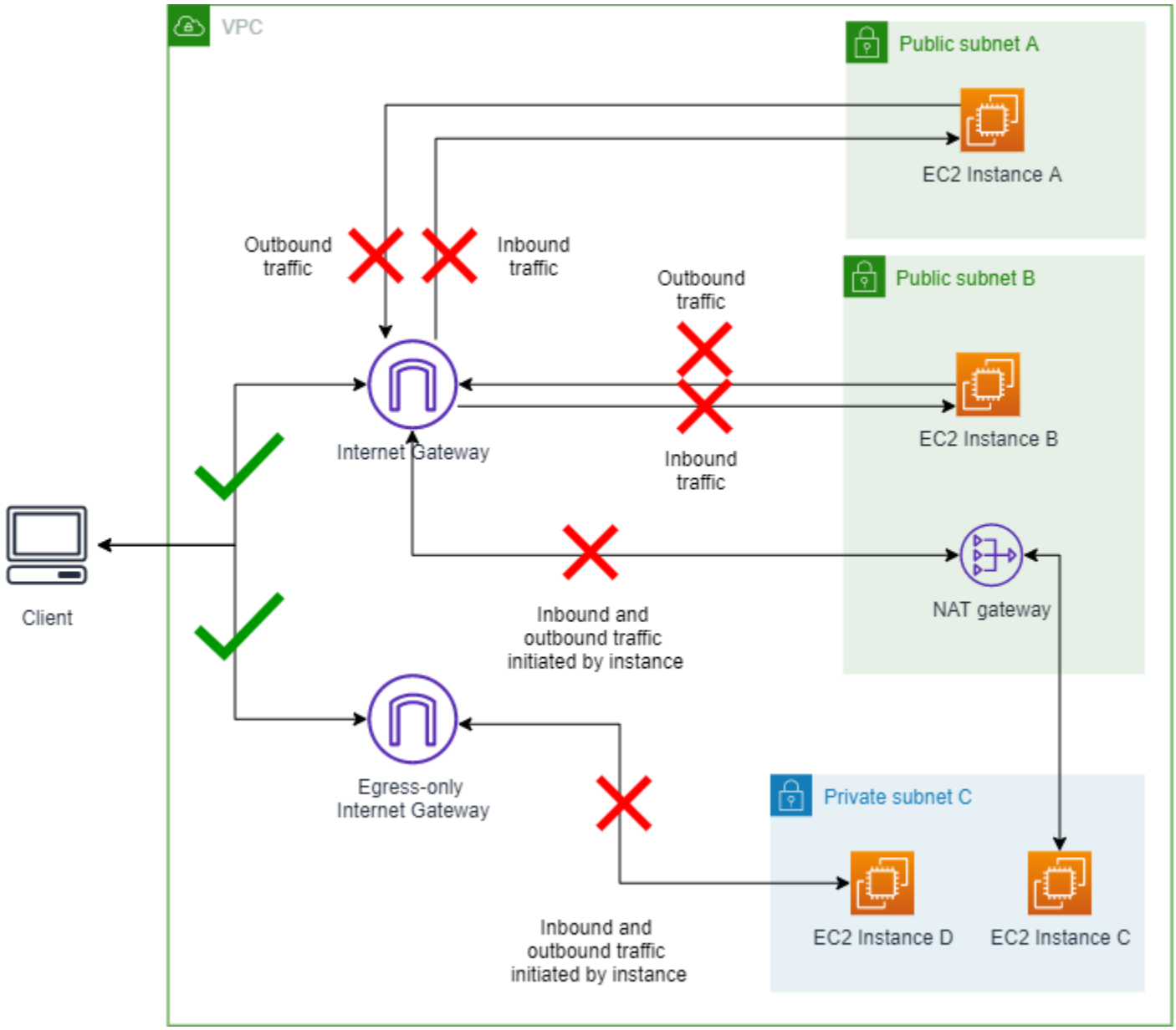
```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:13:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2606:2cc0::374 (2606:2cc0::374)) 56 data bytes
64 bytes from 2606:2cc0::374 (2606:2cc0::374): icmp_seq=1 ttl=58 time=1.21 ms
64 bytes from 2606:2cc0::374 (2606:2cc0::374): icmp_seq=2 ttl=58 time=1.51 ms
```

Perhatikan bahwa ping berhasil dan lalu lintas tidak diblokir.

Skenario 6 - Ubah mode VPC BPA

Di bagian ini Anda akan mengubah arah blok VPC BPA untuk melihat bagaimana pengaruhnya terhadap lalu lintas. Dalam skenario ini, VPC BPA yang diaktifkan dalam mode dua arah memblokir semua lalu lintas seperti dalam Skenario 1. Kecuali pengecualian memiliki akses ke gateway NAT atau gateway internet khusus keluar, lalu lintas diblokir.

Diagram mode VPC BPA Dua Arah dihidupkan dan pengecualian Subnet A dengan mode khusus keluar diaktifkan:



6.1 Ubah VPC BPA ke mode dua arah

Lengkapi bagian ini untuk mengubah mode VPC BPA.

Konsol Manajemen AWS

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi kiri, pilih Peng aturan.
3. Pilih Edit pengaturan akses publik.

4. Ubah arah blok ke Dua Arah lalu pilih S impan perubahan.
5. Tunggu Status berubah menjadi Aktif. Mungkin perlu beberapa menit agar pengaturan VPC BPA berlaku dan status diperbarui.

AWS CLI

1. Ubah arah blok VPC BPA:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-
gateway-block-mode block-bidirectional
```

   Mungkin perlu beberapa menit agar pengaturan VPC BPA berlaku dan status diperbarui.
2. Lihat status VPC BPA:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

6.2 Hubungkan ke instance

Lengkapi bagian ini untuk terhubung ke instance.

Konsol Manajemen AWS

1. Ping alamat IPv4 publik Instance A dan B. Perhatikan bahwa lalu lintas diblokir.
2. Hubungkan ke Instans A dan B menggunakan koneksi instans EC2 seperti yang Anda lakukan di Skenario 1 dan ping www.amazon.com. Perhatikan bahwa Anda tidak dapat melakukan ping ke situs publik di internet dari Instance A atau B. Lalu lintas diblokir.
3. Hubungkan ke Instans C dan D menggunakan koneksi instans EC2 seperti yang Anda lakukan di Skenario 1 dan ping www.amazon.com darinya. Perhatikan bahwa Anda tidak dapat melakukan ping ke situs publik di internet dari Instance C atau D. Lalu lintas diblokir.

AWS CLI

1. Ping Instance A menggunakan alamat IPv4 publik untuk memeriksa lalu lintas masuk:

```
ping 18.225.8.244
```

Output:

```
Pinging 18.225.8.244 with 32 bytes of data:
Request timed out.
```

Perhatikan bahwa ping gagal dan lalu lintas diblokir.

2. Gunakan alamat IPv4 pribadi untuk menghubungkan dan memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:17:44 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Perhatikan bahwa ping gagal dan lalu lintas diblokir.

3. Ping Instance A menggunakan alamat IPv4 publik untuk memeriksa lalu lintas masuk:

```
ping 3.18.106.198
```

Output:

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Perhatikan bahwa ping gagal dan lalu lintas diblokir.

4. Gunakan alamat IPv4 pribadi untuk menghubungkan dan memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:09:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Perhatikan bahwa ping gagal dan lalu lintas diblokir.

5. Hubungkan ke Instance C. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian melakukan ping ke IP publik dari instance untuk memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
```

```
      _/m/'
Last login: Fri Sep 27 18:19:45 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:6200:7:49a5:5fd4:b121
 (2600:9000:25f3:6200:7:49a5:5fd4:b121)) 56 data bytes
```

Perhatikan bahwa ping gagal dan lalu lintas diblokir.

6. Hubungkan ke Instance D. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian melakukan ping ke IP publik dari instance untuk memeriksa lalu lintas keluar:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Output:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:20:58 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:b400:7:49a5:5fd4:b121
 (2600:9000:25f3:b400:7:49a5:5fd4:b121)) 56 data bytes
```

Perhatikan bahwa ping gagal dan lalu lintas diblokir.

Pembersihan

Di bagian ini Anda akan menghapus semua sumber daya yang telah Anda buat untuk contoh lanjutan ini. Penting untuk membersihkan sumber daya untuk menghindari biaya tambahan berlebih untuk sumber daya yang dibuat di akun Anda.

Hapus sumber CloudFormation daya

Lengkapi bagian ini untuk menghapus sumber daya yang Anda buat dengan CloudFormation template.

Konsol Manajemen AWS

1. Buka CloudFormation konsol dihttps://console.aws.amazon.com/cloudformation/.
2. Pilih tumpukan VPC BPA.
3. Pilih Hapus.
4. Setelah Anda mulai menghapus tumpukan, lihat tab Acara untuk melihat kemajuan dan memastikan bahwa tumpukan dihapus. Anda mungkin harus memaksa menghapus tumpukan agar dapat dihapus sepenuhnya.

AWS CLI

1. Hapus tum CloudFormation pukan. Anda mungkin harus memaksa menghapus tumpukan agar dapat dihapus sepenuhnya.

```
aws cloudformation delete-stack --stack-name VPC-BPA-stack --region us-east-2
```

2. Lihat kemajuan dan pastikan tumpukan dihapus.

```
aws cloudformation describe-stack-events --stack-name VPC-BPA-stack --region us-east-2
```

Lacak penghapusan pengecualian menggunakan CloudTrail

Lengkapi bagian ini untuk melacak penghapusan pengecualian menggunakan AWS CloudTrail. CloudTrail entri muncul saat Anda menghapus pengecualian.

Konsol Manajemen AWS

Anda dapat melihat pengecualian yang dihapus di ri CloudTrail wayat acara dengan mencari Jenis sumber daya > AWS: :EC2:: VPCBlockPublicAccessExclusion di konsol di AWS CloudTrail . https://console.aws.amazon.com/cloudtrailv2/

AWS CLI

Anda dapat menggunakan perintah lookup-events untuk melihat peristiwa yang terkait dengan menghapus pengecualian:

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceType,AttributeValue=AWS::EC2::VPCBlockPublicAccessExclusion
```

Contoh lanjutan sudah lengkap.

Praktik terbaik keamanan untuk VPC Anda

Praktik terbaik berikut adalah pedoman umum dan tidak mewakili solusi keamanan yang lengkap. Karena praktik terbaik ini mungkin tidak sesuai atau cukup untuk lingkungan Anda, anggap sebagai pertimbangan yang membantu dan bukan sebagai resep.

- Saat Anda menambahkan subnet ke VPC untuk meng-host aplikasi Anda, buat subnet tersebut di beberapa Zona Ketersediaan. Zona Ketersediaan adalah satu atau lebih pusat data diskrit dengan daya redundan, jaringan, dan konektivitas di suatu Wil AWS ayah. Menggunakan beberapa Zona Ketersediaan membuat aplikasi produksi Anda sangat tersedia, toleran terhadap kesalahan, dan dapat diskalakan.
- Gunakan grup keamanan untuk mengontrol lalu lintas ke instans EC2 di subnet Anda. Untuk informasi selengkapnya, lihat Grup keamanan.
- Gunakan ACL jaringan untuk mengontrol lalu lintas masuk dan keluar di tingkat subnet. Untuk informasi selengkapnya, lihat Kontrol lalu lintas subnet dengan daftar kontrol akses jaringan.
- Kelola akses ke AWS sumber daya di VPC Anda menggunakan federasi identitas AWS Identity and Access Management (IAM), pengguna, dan peran. Untuk informasi selengkapnya, lihat Identity and access management untuk Amazon VPC.
- Gunakan Log Aliran VPC untuk memantau lalu lintas IP yang menuju dan dari VPC, subnet, atau antarmuka jaringan. Untuk informasi selengkapnya, lihat Log Alur VPC.
- Gunakan Network Access Analyzer untuk mengidentifikasi akses jaringan yang tidak diinginkan ke sumber daya di VPC kami. Untuk informasi selengkapnya, lihat Panduan Penganalisis Akses Jaringan.
- Gunakan AWS Network Firewall untuk memantau dan melindungi VPC Anda dengan menyaring lalu lintas masuk dan keluar. Untuk informasi lebih lanjut, lihat AWS Network Firewall Panduan.

- Gunakan Amazon GuardDuty untuk mendeteksi potensi ancaman terhadap akun, wadah, beban kerja, dan data di AWS lingkungan Anda. Deteksi ancaman dasar mencakup pemantauan log aliran VPC yang terkait dengan instans Amazon EC2 Anda. Untuk informasi selengkapnya, lihat Log Aliran VPC di Panduan GuardDuty Pengguna Amazon.

Untuk jawaban atas pertanyaan umum terkait keamanan VPC, lihat Keamanan dan Penyaringan di FAQ Amazon VPC.

Gunakan Amazon VPC dengan yang lain Layanan AWS

Amazon Virtual Private Cloud (VPC) adalah AWS layanan dasar yang menyediakan lingkungan jaringan yang aman dan dapat disesuaikan untuk infrastruktur cloud Anda. Selain membuat dan mengelola VPC Anda sendiri, Anda dapat menggunakan integrasi antara VPC dan AWS layanan lain untuk membangun solusi komprehensif yang disesuaikan dengan kebutuhan spesifik Anda.

Anda dapat menghubungkan VPC Anda ke berbagai AWS layanan menggunakan AWS PrivateLink. Ini memungkinkan konektivitas pribadi antara VPC Anda dan AWS layanan yang didukung atau aplikasi lokal, menjaga lalu lintas jaringan di dalam AWS jaringan dan menghindari paparan ke internet publik. Ini sangat berguna untuk mempertahankan batas keamanan yang ketat dan persyaratan kepatuhan.

Untuk lebih memperkuat keamanan VPC Anda, Anda dapat menggunakan AWS Network Firewall. Layanan firewall terkelola ini memungkinkan Anda untuk menentukan dan menerapkan kebijakan keamanan tingkat jaringan, memfilter lalu lintas utara-selatan dan timur-barat dalam VPC Anda. Dengan memasangkan Network Firewall dengan VPC Anda, Anda dapat meningkatkan strategi pertahanan dan melindungi sumber daya cloud Anda dari akses tidak sah atau aktivitas berbahaya.

Selain itu, Anda dapat memfilter lalu lintas DNS dalam VPC Anda menggunakan Route 53 Resolver DNS Firewall. Kemampuan ini memungkinkan Anda membuat aturan pemfilteran DNS khusus untuk mengontrol domain mana yang dapat diselesaikan oleh sumber daya VPC Anda, memberikan lapisan keamanan dan penegakan kepatuhan tambahan.

Jika Anda mengalami masalah keterjangkauan antara sumber daya dalam VPC atau terhubung ke VPC Anda, Anda dapat menggunakan Reachability Analyzer. Reachability Analyzer melakukan tes konektivitas virtual, memberikan informasi jalur hop-by-hop terperinci dan mengidentifikasi komponen pemblokiran apa pun. Alat pemecahan masalah ini dapat dengan cepat membantu Anda mengidentifikasi dan menyelesaikan masalah konektivitas jaringan.

Dengan mengintegrasikan AWS layanan pelengkap ini dengan VPC Anda, Anda dapat membangun solusi cloud yang kuat, aman, dan tangguh yang memenuhi kebutuhan bisnis dan arsitektur unik Anda.

Daftar Isi

- Hubungkan VPC Anda ke layanan menggunakan AWS PrivateLink
- Filter lalu lintas jaringan menggunakan AWS Network Firewall

- Filter lalu lintas DNS menggunakan Route 53 Resolver DNS Firewall
- Memecahkan masalah keterjangkauan menggunakan Reachability Analyzer

Hubungkan VPC Anda ke layanan menggunakan AWS PrivateLink

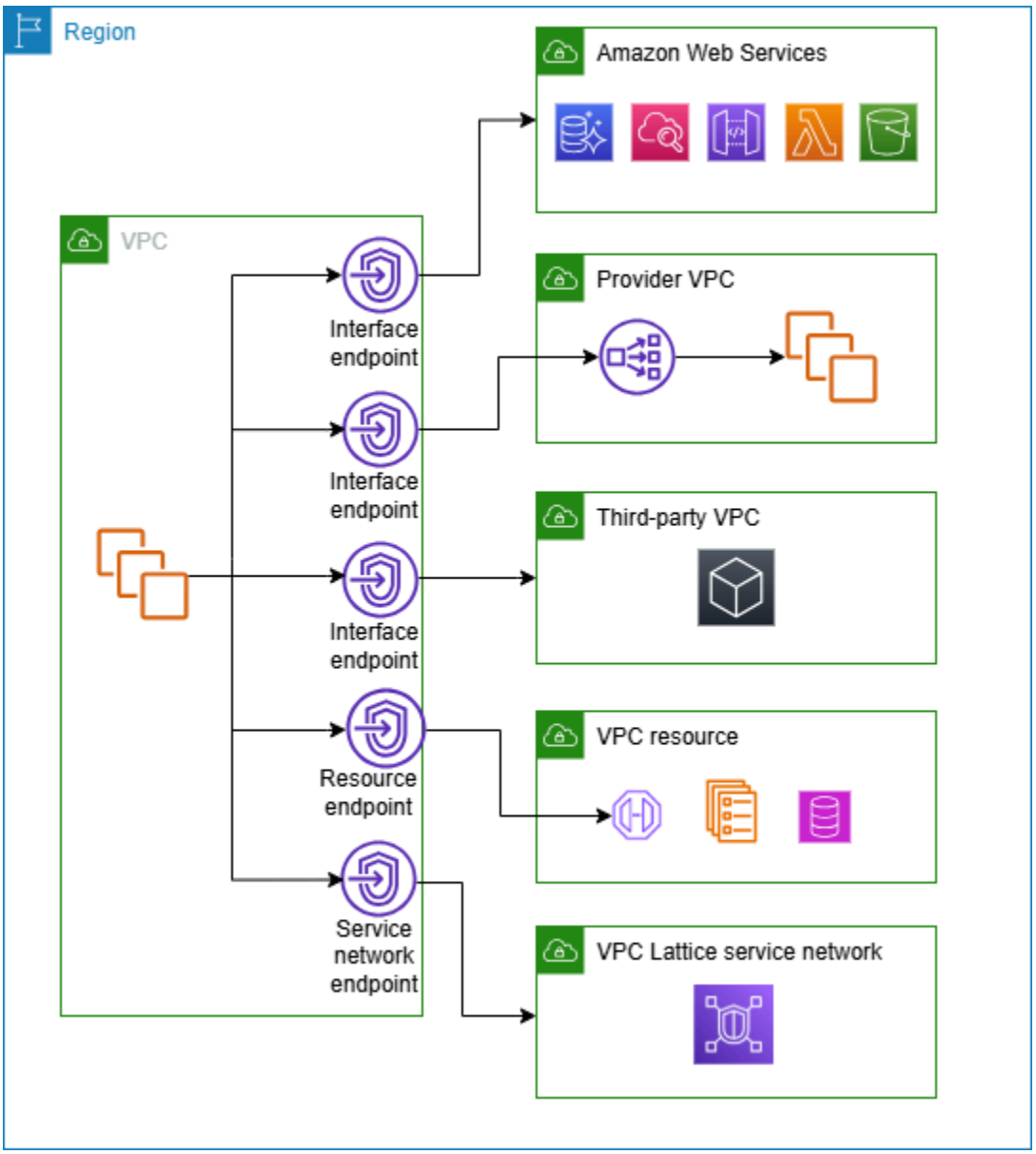
AWS PrivateLink membangun konektivitas pribadi antara cloud pribadi virtual (VPC) dan layanan yang didukung Layanan AWS, yang dihosting oleh layanan lain Akun AWS yang didukung AWS Marketplace , dan sumber daya yang didukung. Anda tidak perlu menggunakan gateway internet, perangkat NAT, Direct Connect koneksi, atau AWS Site-to-Site VPN koneksi untuk berkomunikasi dengan layanan atau sumber daya.

Untuk menggunakan AWS PrivateLink, buat titik akhir VPC di subnet mana pun yang Anda butuhkan untuk mengakses layanan atau sumber daya. Ini menciptakan antarmuka jaringan elastis di subnet tertentu yang berfungsi sebagai titik masuk untuk lalu lintas yang ditujukan ke layanan atau sumber daya.

Anda juga dapat membuat layanan titik akhir VPC Anda sendiri, didukung oleh AWS PrivateLink dan memungkinkan AWS pelanggan lain untuk mengakses layanan Anda. PrivateLink memungkinkan pembuatan titik akhir API pribadi, memungkinkan organisasi untuk mengekspos layanan mereka sendiri dengan aman kepada AWS pelanggan lain. Ini memberdayakan bisnis untuk memonetisasi kemampuan internal mereka, menumbuhkan ekosistem kolaboratif, dan mempertahankan kontrol atas bagaimana layanan mereka diakses dan dikonsumsi.

Salah satu manfaat utama penggunaan AWS PrivateLink adalah kemampuan untuk membangun konektivitas pribadi yang aman tanpa perlu konstruksi jaringan tradisional seperti gateway internet, perangkat NAT, atau koneksi VPN. Ini membantu menyederhanakan arsitektur jaringan, mengurangi permukaan serangan, dan meningkatkan keamanan secara keseluruhan dengan menjaga lalu lintas data terbatas di dalam AWS jaringan.

Diagram berikut menunjukkan kasus penggunaan umum untuk AWS PrivateLink. VPC memiliki beberapa instans EC2 dalam subnet pribadi yang memiliki akses ke sumber daya melalui lima titik akhir VPC. Ada tiga titik akhir VPC antarmuka, satu titik akhir VPC sumber daya, dan satu titik akhir VPC jaringan layanan.



Lihat informasi yang lebih lengkap di AWS PrivateLink.

Filter lalu lintas jaringan menggunakan AWS Network Firewall

Anda dapat memfilter lalu lintas jaringan di perimeter VPC Anda menggunakan. AWS Network Firewall Network Firewall adalah stateful, dikelola, jaringan firewall dan deteksi intrusi dan layanan pencegahan. Lihat informasi selengkapnya di Panduan Developer AWS Network Firewall.

Anda menerapkan Network Firewall dengan AWS sumber daya berikut.

Sumber daya Network Firewall	Deskripsi
firewall	Firewall menghubungkan perilaku penyaringan lalu lintas jaringan kebijakan firewall ke VPC yang ingin Anda lindungi. Konfigurasi firewall mencakup spesifikasi untuk Availability Zone dan subnet tempat endpoint firewall ditempatkan. Ini juga mendefinisikan pengaturan tingkat tinggi seperti konfigurasi logging firewall dan penandaan pada sumber daya firewall. AWS Untuk informasi selengkapnya, lihat Firewall di AWS Network Firewall.
Kebijakan Firewall	Kebijakan firewall mendefinisikan perilaku pemantauan dan perlindun gan untuk firewall. Rincian perilaku didefinisikan dalam grup aturan yang Anda tambahkan ke kebijakan Anda, dan di beberapa pengatura n default kebijakan. Untuk menggunakan kebijakan firewall, Anda mengaitkannya dengan satu atau lebih firewall. Untuk informasi selengkapnya, lihat Kebijakan Firewall di AWS Network Firewall.
Grup aturan	Grup aturan adalah seperangkat kriteria yang dapat digunakan kembali untuk memeriksa dan menangani lalu lintas jaringan. Anda menambahkan satu atau lebih grup aturan kebijakan firewall sebagai bagian dari konfigurasi kebijakan Anda. Anda dapat menentukan grup aturan stateless untuk memeriksa setiap paket jaringan dalam isolasi. Grup aturan stateless serupa dalam perilaku dan digunakan untuk daftar ACLs kontrol akses jaringan Amazon VPC (). Anda juga dapat menentukan grup aturan stateful untuk memeriksa paket dalam konteks arus lalu lintas mereka. Grup aturan stateful serupa dalam hal perilaku dan manfaat untuk grup keamanan Amazon VPC. Untuk informasi selengkapnya, lihat Grup aturan di AWS Network Firewall.

Anda juga dapat menggunakan AWS Firewall Manager untuk mengonfigurasi dan mengelola sumber daya Firewall Jaringan secara terpusat di seluruh akun dan aplikasi Anda. AWS Organizations Anda

dapat mengelola firewall untuk beberapa akun menggunakan satu akun di Firewall Manager. Untuk informasi selengkapnya, lihat AWS Firewall Managerdi AWS WAF AWS Firewall Manager, dan Panduan AWS Shield Advanced Pengembang.

Filter lalu lintas DNS menggunakan Route 53 Resolver DNS Firewall

Dengan DNS Firewall, Anda menentukan aturan pemfilteran nama domain dalam grup aturan yang Anda kaitkan dengan Anda. VPCs Anda dapat menentukan daftar nama domain untuk mengizinkan atau memblokir, dan Anda dapat menyesuaikan respon untuk kueri DNS yang Anda blokir. Untuk informasi selengkapnya, lihat Dokumentasi Route 53 Resolver DNS Firewall.

Anda menerapkan DNS Firewall dengan AWS sumber daya berikut.

Sumber daya DNS Firewall	Deskripsi
Grup aturan DNS Firewall	Grup aturan DNS Firewall sekumpulan aturan DNS Firewall yang diberi nama dan dapat digunakan kembali untuk menyaring kueri DNS. Anda mengisi grup aturan dengan aturan pemfilteran, lalu mengaitkan grup aturan dengan satu atau lebih dari VPCs Amazon VPC. Ketika Anda mengaitkan grup aturan dengan VPC, Anda mengaktifkan penyaringan DNS Firewall untuk VPC. Kemudian, ketika Resolver menerima kueri DNS untuk VPC yang memiliki grup aturan yang terkait dengannya, Resolver meneruskan kueri tersebut ke DNS Firewall untuk disaring. Setiap aturan dalam grup aturan menentukan satu daftar domain dan tindakan yang akan dilakukan terhadap kueri DNS yang domainnya sesuai dengan spesifikasi domain dalam daftar. Anda dapat mengizink an, memblokir, atau memperingatkan adanya kueri yang cocok. Anda juga dapat menentukan respon kustom untuk kueri yang diblokir. Untuk informasi lebih lanjut, lihat: Grup aturan dan aturan dalam Route 53 Resolver DNS Firewall.
Daftar domain	Daftar domain adalah seperangkat spesifikasi domain yang dapat digunakan kembali yang Anda gunakan dalam aturan DNS Firewall, di dalam grup aturan.

Sumber daya DNS Firewall	Deskripsi
	Untuk informasi selengkapnya, lihat Daftar domain dalam Route 53 Resolver DNS Firewall.

Anda juga dapat menggunakan AWS Firewall Manager untuk mengonfigurasi dan mengelola sumber daya DNS Firewall secara terpusat di seluruh akun dan organisasi Anda. AWS Organizations Anda dapat mengelola firewall untuk beberapa akun menggunakan satu akun di Firewall Manager. Untuk informasi selengkapnya, lihat AWS Firewall Managerdi AWS WAF AWS Firewall Manager, dan Panduan AWS Shield Advanced Pengembang.

Memecahkan masalah keterjangkauan menggunakan Reachability Analyzer

Reachability Analyzer adalah alat analisis konfigurasi statis. Gunakan Reachability Analyzer untuk menganalisis dan men-debug jangkauan jaringan antara dua sumber daya di VPC Anda. Reachability Analyzer menghasilkan detail hop-by-hop dari jalur virtual antara sumber daya ini ketika mereka dapat dijangkau, dan mengidentifikasi komponen pemblokiran sebaliknya.

Anda dapat menggunakan Reachability Analyzer untuk menganalisis keterjangkauan antara sumber daya berikut:

- Contoh
- Gateway internet
- Antarmuka jaringan
- Transit gateway
- Lampiran gateway transit
- Layanan VPC endpoint
- Titik akhir VPC
- Koneksi peering VPC
- Gerbang VPN

Untuk informasi selengkapnya, lihat Panduan Peng analisis Jangkauan.

Contoh VPC

Amazon Virtual Private Cloud (VPC) adalah blok bangunan mendasar dalam AWS ekosistem, memungkinkan Anda untuk menyediakan jaringan virtual terisolasi yang disesuaikan dengan kebutuhan spesifik Anda. Dengan membuat dan mengelola sendiri VPCs, Anda mendapatkan kontrol penuh atas lingkungan jaringan, termasuk kemampuan untuk menentukan rentang alamat IP, subnet, tabel routing, dan opsi konektivitas.

Bagian ini berisi tiga contoh konfigurasi untuk virtual private cloud (VPCs) Anda, masing-masing dirancang untuk mengatasi serangkaian persyaratan yang berbeda:

- VPC untuk lingkungan pengujian: Konfigurasi ini menunjukkan cara membuat VPC yang dapat Anda gunakan sebagai lingkungan pengembangan atau pengujian.
- VPC untuk server Web dan database: Konfigurasi ini menunjukkan cara membuat VPC yang dapat Anda gunakan untuk arsitektur resilent di lingkungan produksi.
- VPC dengan server di subnet pribadi dan NAT: Dalam konfigurasi yang lebih canggih ini, semua EC2 instance disediakan dalam subnet pribadi, dengan gateway NAT yang memfasilitasi akses internet keluar yang aman. Ini adalah contoh di mana Anda perlu membatasi konektivitas internet langsung ke sumber daya Anda sambil tetap memungkinkan komunikasi keluar yang diperlukan.

Dengan memberikan contoh konfigurasi VPC ini, kami berharap dapat menggambarkan fleksibilitas dan opsi penyesuaian yang tersedia saat merancang lingkungan jaringan cloud Anda. Pengaturan VPC spesifik yang Anda pilih harus didasarkan pada arsitektur aplikasi Anda, persyaratan keamanan, dan tujuan bisnis secara keseluruhan. Merencanakan infrastruktur VPC dengan cermat dapat membantu Anda membuat jaringan virtual yang kuat, terukur, dan aman yang mendukung pertumbuhan dan evolusi beban kerja berbasis cloud Anda.

Contoh

- Contoh: VPC untuk lingkungan pengujian
- Contoh: VPC untuk server web dan database
- Contoh: VPC dengan server di subnet pribadi dan NAT

Contoh terkait

- Untuk menghubungkan satu sama lain, lihat konfigurasi peering VPC di Panduan Peering VPC Amazon. VPCs

- Untuk menghubungkan jaringan Anda VPCs ke jaringan Anda sendiri, lihat skenario Site-to-Site VPN di Panduan AWS Site-to-Site VPN Pengguna.
- Untuk menghubungkan Anda VPCs satu sama lain dan ke jaringan Anda sendiri, lihat Contoh skenario gateway transit di Gateway Transit VPC Amazon.

Sumber daya tambahan

- Memahami pola ketahanan dan trade-off (Blog Arsitektur)AWS
- Rencanakan topologi jaringan Anda (AWS Well-Architected Framework)
- Opsi Konektivitas Amazon Virtual Private Cloud (AWS Whitepaper)

Contoh: VPC untuk lingkungan pengujian

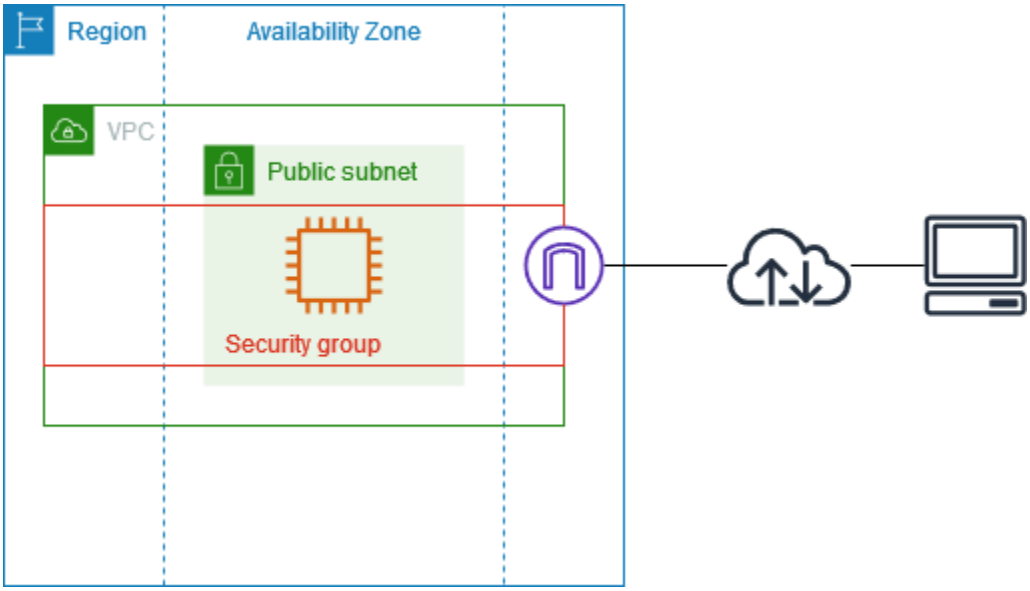
Contoh ini menunjukkan cara membuat VPC yang dapat Anda gunakan sebagai lingkungan pengembangan atau pengujian. Karena VPC ini tidak dimaksudkan untuk digunakan dalam produksi, Anda tidak perlu menyebarkan server Anda di beberapa Availability Zone. Untuk menjaga biaya dan kompleksitas tetap rendah, Anda dapat menerapkan server Anda dalam satu Availability Zone.

Daftar Isi

- Ikhtisar
- 1. Buat VPC
- 2. Men-deploy aplikasi Anda
- 3. Uji konfigurasi Anda
- 4. Bersihkan

Ikhtisar

Diagram berikut memberikan gambaran umum tentang sumber daya yang termasuk dalam contoh ini. VPC memiliki subnet publik dalam satu Availability Zone dan gateway internet. Server adalah instance EC2 yang berjalan di subnet publik. Grup keamanan misalnya memungkinkan lalu lintas SSH dari komputer Anda sendiri, ditambah lalu lintas lain yang secara khusus diperlukan untuk kegiatan pengembangan atau pengujian Anda.



Perutean

Saat Anda membuat VPC ini dengan menggunakan konsol VPC Amazon, kami membuat tabel rute untuk subnet publik dengan rute lokal dan rute ke gateway internet. Berikut ini adalah contoh tabel rute dengan rute untuk keduanya IPv4 dan IPv6. Jika Anda membuat subnet IPv4 -only alih-alih subnet tumpukan ganda, tabel rute Anda hanya memiliki rute. IPv4

Destinasi	Target
10.0.0.0/16	lokal
2001:db8:1234:1a00::/56	lokal
0.0.0.0/0	*igw-id*
::/0	*igw-id*

Keamanan

Untuk konfigurasi contoh ini, Anda harus membuat grup keamanan untuk instans Anda yang memungkinkan lalu lintas yang dibutuhkan aplikasi Anda. Misalnya, Anda mungkin perlu menambahkan aturan yang memungkinkan lalu lintas SSH dari komputer atau lalu lintas HTTP dari jaringan Anda.

Berikut ini adalah contoh aturan masuk untuk grup keamanan, dengan aturan untuk keduanya IPv4 dan IPv6. Jika Anda membuat subnet IPv4 -only alih-alih subnet tumpukan ganda, Anda hanya perlu aturan untuk. IPv4

Sumber	Protokol	Rentang Port	Deskripsi
0.0.0.0/0	TCP	80	Memungkinkan akses HTTP masuk dari semua alamat IPv4
::/0	TCP	80	Memungkinkan akses HTTP masuk dari semua alamat IPv6
0.0.0.0/0	TCP	443	Memungkinkan akses HTTPS masuk dari semua alamat IPv4
::/0	TCP	443	Memungkinkan akses HTTPS masuk dari semua alamat IPv6
Public IPv4 address range of your network	TCP	22	(Opsional) Memungkinkan akses SSH masuk dari alamat IPv4 IP di jaringan Anda
IPv6 address range of your network	TCP	22	(Opsional) Memungkinkan akses SSH masuk dari alamat IPv6 IP di jaringan Anda
Public IPv4 address range of your network	TCP	3389	(Opsional) Memungkinkan akses RDP masuk dari alamat IPv4 IP di jaringan Anda
IPv6 address range of your network	TCP	3389	(Opsional) Memungkinkan akses RDP masuk dari alamat IPv6 IP di jaringan Anda

1. Buat VPC

Gunakan prosedur berikut untuk membuat VPC dengan subnet publik dalam satu Availability Zone. Konfigurasi ini cocok untuk lingkungan pengembangan atau pengujian.

Untuk membuat VPC

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di dasbor, pilih Buat VPC.
3. Agar Sumber Daya dapat dibuat, pilih VPC dan lainnya.
4. Konfigurasikan VPC
    a. Untuk Pembuatan otomatis tanda nama, masukkan nama untuk VPC.
    b. Untuk blok IPv4 CIDR, Anda dapat menyimpan saran default, atau sebagai alternatif Anda dapat memasukkan blok CIDR yang diperlukan oleh aplikasi atau jaringan Anda. Untuk informasi selengkapnya, lihat the section called “Blok VPC CIDR”.
    c. (Opsional) Jika aplikasi Anda berkomunikasi dengan menggunakan IPv6 alamat, pilih blok CIDR, blok IPv6 CIDR yang disediakan Amazon IPv6 .
5. Konfigurasikan subnet
    a. Untuk Jumlah Availability Zone, pilih 1. Anda dapat mempertahankan Availability Zone default, atau sebagai alternatif Anda dapat memperluas Kustomisasi AZs dan memilih Availability Zone.
    b. Untuk Jumlah subnet publik, pilih 1.
    c. Untuk Jumlah subnet pribadi, pilih 0.
    d. Anda dapat menyimpan blok CIDR default untuk subnet publik, atau sebagai alternatif Anda dapat memperluas Kustomisasi blok CIDR subnet dan memasukkan blok CIDR. Untuk informasi selengkapnya, lihat the section called “Blok subnet CIDR”.
6. Untuk gateway NAT, pertahankan nilai default, None.
7. Untuk titik akhir VPC, pilih Tidak Ada. Titik akhir VPC gateway untuk S3 hanya digunakan untuk mengakses Amazon S3 dari subnet pribadi.
8. Untuk opsi DNS, tetap pilih kedua opsi. Akibatnya, instans Anda akan menerima nama host DNS publik yang sesuai dengan alamat IP publiknya.
9. Pilih Buat VPC.

2. Men-deploy aplikasi Anda

Ada berbagai cara untuk menerapkan instans EC2. Contoh:

- Wisaya instans peluncuran Amazon EC2

- Amazon EC2 Auto Scaling
- AWS CloudFormation
- Amazon Elastic Container Service (Amazon ECS)

Setelah menerapkan instans EC2, Anda dapat terhubung ke instans, menginstal perangkat lunak yang Anda butuhkan untuk aplikasi Anda, dan kemudian membuat gambar untuk penggunaan di masa mendatang. Untuk informasi selengkapnya, lihat Membuat AMI di Panduan Pengguna Amazon EC2. Atau, Anda dapat menggunakan EC2 Image Builder untuk membuat dan mengelola Amazon Machine Image (AMI).

3. Uji konfigurasi Anda

Setelah Anda selesai menerapkan aplikasi Anda, Anda dapat mengujinya. Jika Anda tidak dapat terhubung ke instans EC2 Anda, atau jika aplikasi Anda tidak dapat mengirim atau menerima lalu lintas yang Anda harapkan, Anda dapat menggunakan Reachability Analyzer untuk membantu Anda memecahkan masalah. Misalnya, Reachability Analyzer dapat mengidentifikasi masalah konfigurasi dengan tabel rute atau grup keamanan Anda. Untuk informasi selengkapnya, lihat Panduan Reachability Analyzer.

4. Bersihkan

Setelah selesai dengan konfigurasi ini, Anda dapat menghapusnya. Sebelum Anda dapat menghapus VPC, Anda harus menghentikan instance Anda. Lihat informasi yang lebih lengkap di the section called “Hapus VPC Anda”.

Contoh: VPC untuk server web dan database

Contoh ini menunjukkan cara membuat VPC yang dapat Anda gunakan untuk arsitektur dua tingkat di lingkungan produksi. Untuk meningkatkan ketahanan, Anda menerapkan server di dua Availability Zone.

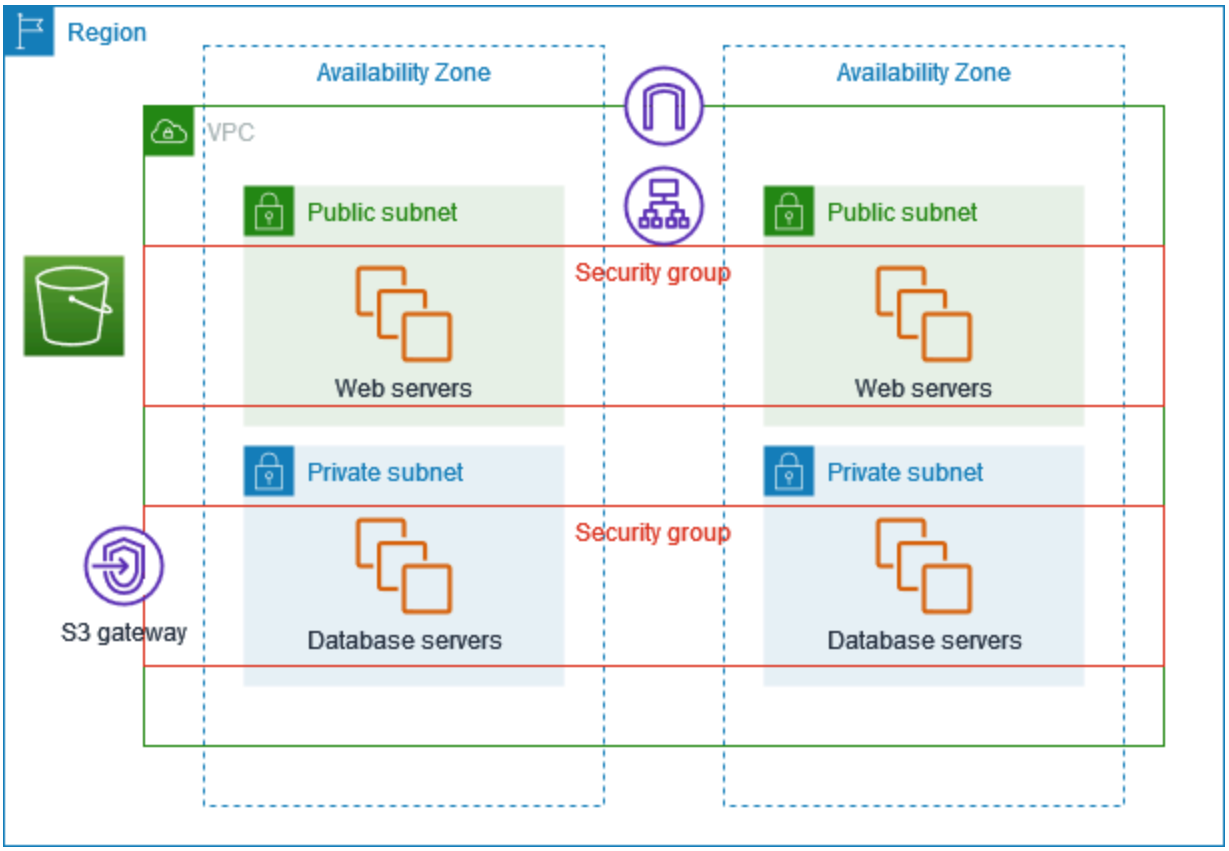
Daftar Isi

- Ikhtisar
- 1. Buat VPC
- 2. Men-deploy aplikasi Anda
- 3. Uji konfigurasi Anda

- 4. Bersihkan

Ikhtisar

Diagram berikut memberikan gambaran umum tentang sumber daya yang termasuk dalam contoh ini. VPC memiliki subnet publik dan subnet pribadi di dua Availability Zone. Server web berjalan di subnet publik dan menerima lalu lintas dari klien melalui penyeimbang beban. Grup keamanan untuk server web memungkinkan lalu lintas dari penyeimbang beban. Server database berjalan di subnet pribadi dan menerima lalu lintas dari server web. Grup keamanan untuk server database memungkinkan lalu lintas dari server web. Server database dapat terhubung ke Amazon S3 dengan menggunakan titik akhir VPC gateway.



Perutean

Saat Anda membuat VPC ini dengan menggunakan konsol VPC Amazon, kami membuat tabel rute untuk subnet publik dengan rute dan rute lokal ke gateway internet, dan tabel rute untuk setiap subnet pribadi dengan rute lokal dan rute ke titik akhir VPC gateway.

Berikut ini adalah contoh tabel rute untuk subnet publik, dengan rute untuk keduanya IPv4 dan IPv6. Jika Anda membuat subnet IPv4 -only alih-alih subnet tumpukan ganda, tabel rute Anda hanya memiliki rute. IPv4

Tujuan	Target
10.0.0.0/16	lokal
2001:db8:1234:1a00::/56	lokal
0.0.0.0/0	*igw-id*
::/0	*igw-id*

Berikut ini adalah contoh tabel rute untuk subnet pribadi, dengan rute lokal untuk keduanya IPv4 dan IPv6. Jika Anda membuat subnet IPv4 -only, tabel rute Anda hanya memiliki rute. IPv4 Rute terakhir mengirimkan lalu lintas yang ditujukan untuk Amazon S3 ke titik akhir VPC gateway.

Tujuan	Target
10.0.0.0/16	lokal
2001:db8:1234:1a00::/56	lokal
s3-prefix-list-id	*s3-gateway-id*

Keamanan

Untuk konfigurasi contoh ini, Anda membuat grup keamanan untuk penyeimbang beban, grup keamanan untuk server web, dan grup keamanan untuk server database.

Load balancer

Grup keamanan untuk Application Load Balancer atau Network Load Balancer Anda harus mengizinkan lalu lintas masuk dari klien pada port pendengar penyeimbang beban. Untuk menerima lalu lintas dari mana saja di internet, tentukan 0.0.0.0/0 sebagai sumbernya. Grup keamanan penyeimbang beban juga harus mengizinkan lalu lintas keluar dari penyeimbang beban ke instance target pada port pendengar instans dan port pemeriksaan kesehatan.

Server web

Aturan grup keamanan berikut memungkinkan server web menerima lalu lintas HTTP dan HTTPS dari penyeimbang beban. Anda dapat secara opsional mengizinkan server web untuk menerima lalu lintas SSH atau RDP dari jaringan Anda. Server web dapat mengirim lalu lintas SQL atau MySQL ke server database Anda.

Sumber	Protokol	Rentang Port	Deskripsi
ID of the security group for the load balancer	TCP	80	Memungkinkan akses HTTP masuk dari penyeimbang beban
ID of the security group for the load balancer	TCP	443	Memungkinkan akses HTTPS masuk dari penyeimbang beban
Public IPv4 address range of your network	TCP	22	(Opsional) Memungkinkan akses SSH masuk dari alamat IPv4 IP di jaringan Anda
IPv6 address range of your network	TCP	22	(Opsional) Memungkinkan akses SSH masuk dari alamat IPv6 IP di jaringan Anda
Public IPv4 address range of your network	TCP	3389	(Opsional) Memungkinkan akses RDP masuk dari alamat IPv4 IP di jaringan Anda
IPv6 address range of your network	TCP	3389	(Opsional) Memungkinkan akses RDP masuk dari alamat IPv6 IP di jaringan Anda

Tujuan	Protokol	Rentang Port	Deskripsi
ID of the security group for instances running	TCP	1433	Memungkinkan akses Microsoft SQL Server keluar ke server database

Tujuan	Protokol	Rentang Port	Deskripsi
Microsoft SQL Server			
ID of the security group for instances running MySQL	TCP	3306	Memungkinkan akses MySQL keluar ke server database

Server basis data

Aturan grup keamanan berikut memungkinkan server database menerima permintaan baca dan tulis dari server web.

Sumber	Protokol	Rentang Port	Komentar
ID of the web server security group	TCP	1433	Memungkinkan akses Microsoft SQL Server masuk dari server web
ID of the web server security group	TCP	3306	Memungkinkan akses MySQL Server masuk dari server web

Tujuan	Protokol	Rentang Port	Komentar
0.0.0.0/0	TCP	80	Memungkinkan akses HTTP keluar ke internet melalui IPv4
0.0.0.0/0	TCP	443	Memungkinkan akses HTTPS keluar ke internet melalui IPv4

Untuk informasi selengkapnya tentang grup keamanan untuk instans DB Amazon RDS, lihat Mengendalikan akses dengan grup keamanan di Panduan Pengguna Amazon RDS.

1. Buat VPC

Gunakan prosedur berikut untuk membuat VPC dengan subnet publik dan subnet pribadi di dua Availability Zones.

Untuk membuat VPC

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di dasbor, pilih Buat VPC.
3. Agar Sumber Daya dapat dibuat, pilih VPC dan lainnya.
4. Konfigurasikan VPC:
    a. Biarkan pembuatan otomatis tag Nama dipilih untuk membuat tag Nama untuk sumber daya VPC atau hapus untuk menyediakan tag Nama Anda sendiri untuk sumber daya VPC.
    b. Untuk blok IPv4 CIDR, Anda dapat menyimpan saran default, atau sebagai alternatif Anda dapat memasukkan blok CIDR yang diperlukan oleh aplikasi atau jaringan Anda. Untuk informasi selengkapnya, lihat the section called “Blok VPC CIDR”.
    c. (Opsional) Jika aplikasi Anda berkomunikasi dengan menggunakan IPv6 alamat, pilih blok CIDR, blok IPv6 CIDR yang disediakan Amazon IPv6 .
    d. Pilih opsi Sewa. Opsi ini menentukan apakah EC2 instance yang Anda luncurkan ke VPC akan berjalan pada perangkat keras yang dibagikan dengan perangkat keras lain Akun AWS atau pada perangkat keras yang didedikasikan untuk penggunaan Anda saja. Jika Anda memilih penyewaan VPC yang `Default` akan menjadi EC2 , instance yang diluncurkan ke VPC ini akan menggunakan atribut penyewaan yang ditentukan saat Anda meluncurkan instance. Untuk informasi selengkapnya, lihat Meluncurkan instance menggunakan parameter yang ditentukan di Panduan EC2 Pengguna Amazon. Jika Anda memilih penyewaan VPC, instans akan selalu berjalan sebagai Instans Khusus pada perangkat keras yang didedikasikan untuk Anda gunakan. `Dedicated`
5. Konfigurasikan subnet:
    a. Untuk Jumlah Availability Zone, pilih 2, sehingga Anda dapat meluncurkan instans di dua Availability Zone untuk meningkatkan ketahanan.
    b. Untuk Jumlah subnet publik, pilih 2.
    c. Untuk Jumlah subnet pribadi, pilih 2.

   d. Anda dapat menyimpan blok CIDR default untuk subnet, atau sebagai alternatif Anda dapat memperluas Kustomisasi subnet blok CIDR dan memasukkan blok CIDR. Untuk informasi selengkapnya, lihat the section called “Blok subnet CIDR”.
6. Untuk gateway NAT, pertahankan nilai default, None.
7. Untuk titik akhir VPC, pertahankan nilai default, S3 Gateway. Meskipun tidak ada efek kecuali Anda mengakses bucket S3, tidak ada biaya untuk mengaktifkan titik akhir VPC ini.
8. Untuk opsi DNS, tetap pilih kedua opsi. Akibatnya, server web Anda akan menerima nama host DNS publik yang sesuai dengan alamat IP publik mereka.
9. Pilih Buat VPC.

2. Men-deploy aplikasi Anda

Idealnya, Anda telah menguji server web dan server database Anda di lingkungan pengembangan atau pengujian, dan membuat skrip atau gambar yang akan Anda gunakan untuk menyebarkan aplikasi Anda dalam produksi.

Anda dapat menggunakan EC2 instance untuk server web Anda. Ada berbagai cara untuk menyebarkan EC2 instance. Contoh:

- Wisaya instans EC2 peluncuran Amazon
- AWS CloudFormation
- Amazon Elastic Container Service (Amazon ECS)

Untuk meningkatkan ketersediaan, Anda dapat menggunakan Amazon EC2 Auto Scaling untuk menyebarkan server di beberapa Availability Zone dan mempertahankan kapasitas server minimum yang diperlukan oleh aplikasi Anda.

Anda dapat menggunakan Elastic Load Balancing untuk mendistribusikan lalu lintas secara merata di seluruh server Anda. Anda dapat melampirkan penyeimbang beban Anda ke grup Auto Scaling.

Anda dapat menggunakan EC2 instance untuk server database Anda, atau salah satu jenis database kami yang dibuat khusus. Untuk informasi selengkapnya, lihat Database tentang AWS: Cara memilih.

3. Uji konfigurasi Anda

Setelah Anda selesai menerapkan aplikasi Anda, Anda dapat mengujinya. Jika aplikasi Anda tidak dapat mengirim atau menerima lalu lintas yang Anda harapkan, Anda dapat menggunakan

Reachability Analyzer untuk membantu Anda memecahkan masalah. Misalnya, Reachability Analyzer dapat mengidentifikasi masalah konfigurasi dengan tabel rute atau grup keamanan Anda. Untuk informasi selengkapnya, lihat Panduan Reachability Analyzer.

4. Bersihkan

Setelah selesai dengan konfigurasi ini, Anda dapat menghapusnya. Sebelum Anda dapat menghapus VPC, Anda harus menghentikan instans Anda dan menghapus penyeimbang beban. Lihat informasi yang lebih lengkap di the section called “Hapus VPC Anda”.

Contoh: VPC dengan server di subnet pribadi dan NAT

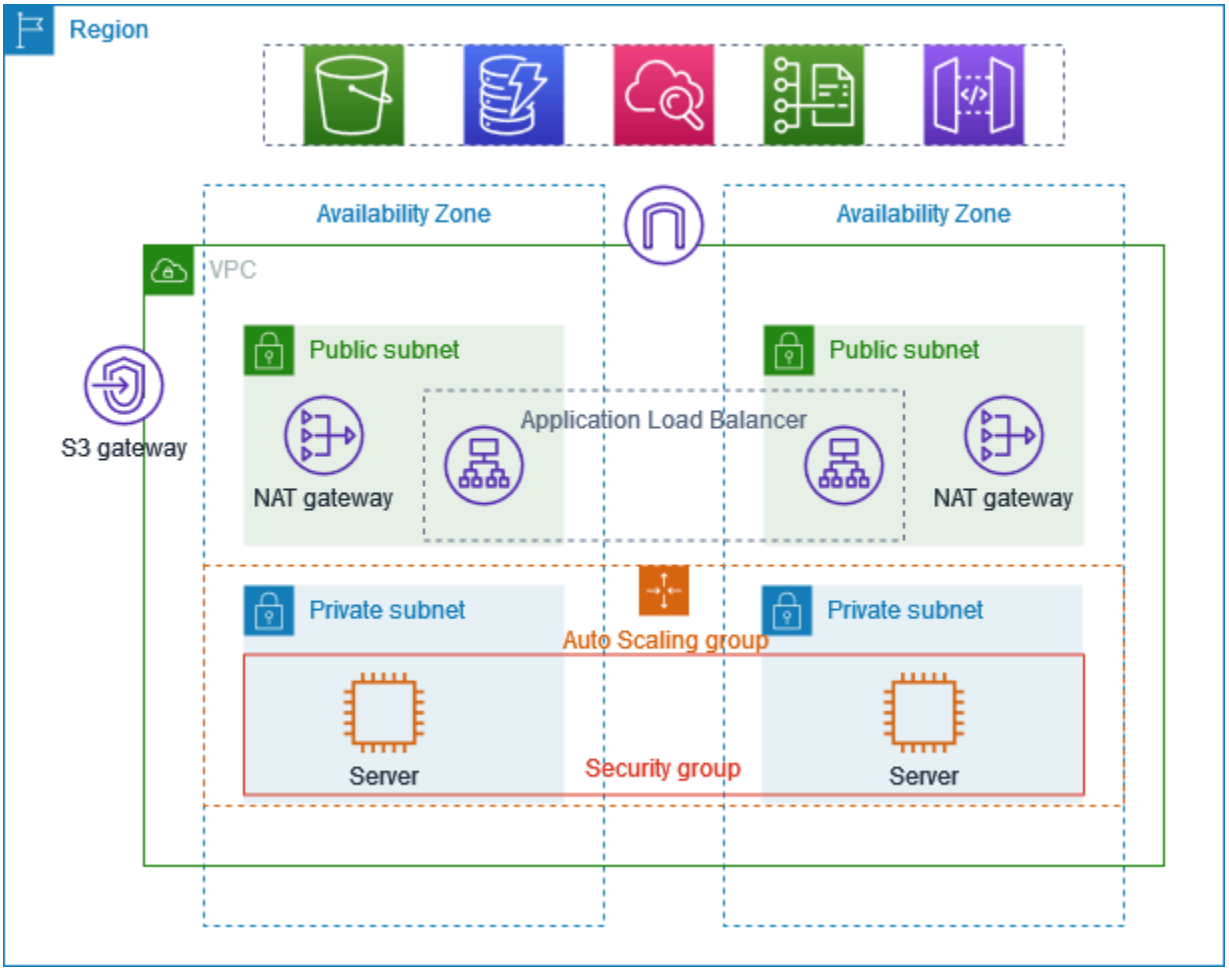
Contoh ini menunjukkan cara membuat VPC yang dapat Anda gunakan untuk server di lingkungan produksi. Untuk meningkatkan ketahanan, Anda menyebarkan server di dua Availability Zone, dengan menggunakan grup Auto Scaling dan Application Load Balancer. Untuk keamanan tambahan, Anda menyebarkan server di subnet pribadi. Server menerima permintaan melalui penyeimbang beban. Server dapat terhubung ke internet dengan menggunakan NAT gateway. Untuk meningkatkan ketahanan, Anda menyebarkan gateway NAT di kedua Availability Zone.

Daftar Isi

- Gambaran umum
- 1. Buat VPC
- 2. Men-deploy aplikasi Anda
- 3. Uji konfigurasi Anda
- 4. Bersihkan

Gambaran umum

Diagram berikut memberikan ikhtisar sumber daya yang disertakan dalam contoh ini. VPC memiliki subnet publik dan subnet pribadi di dua Zona Ketersediaan. Setiap subnet publik berisi gateway NAT dan node penyeimbang beban. Server berjalan di subnet pribadi, diluncurkan dan dihentikan dengan menggunakan grup Auto Scaling, dan menerima lalu lintas dari penyeimbang beban. Server dapat terhubung ke internet dengan menggunakan NAT gateway. Server dapat terhubung ke Amazon S3 dengan menggunakan titik akhir VPC gateway.



Perutean

Saat Anda membuat VPC ini dengan menggunakan konsol Amazon VPC, kami membuat tabel rute untuk subnet publik dengan rute lokal dan rute ke gateway internet. Kami juga membuat tabel rute untuk subnet pribadi dengan rute lokal, dan rute ke gateway NAT, gateway internet khusus egress, dan titik akhir VPC gateway.

Berikut ini adalah contoh tabel rute untuk subnet publik, dengan rute untuk IPv4 dan IPv6. Jika Anda membuat IPv4-only subnet alih-alih subnet tumpukan ganda, tabel rute Anda hanya menyertakan rute IPv4.

Tujuan	Target
10.0.0.0/16	lokal
2001:db8:1234:1a00::/56	lokal

Tujuan	Target
0.0.0. 0/0	*igw-id*
::/0	*igw-id*

Berikut ini adalah contoh tabel rute untuk salah satu subnet pribadi, dengan rute untuk IPv4 dan IPv6. Jika Anda membuat IPv4-only subnet, tabel rute hanya menyertakan rute IPv4. Rute terakhir mengirimkan lalu lintas yang ditujukan untuk Amazon S3 ke titik akhir VPC gateway.

Tujuan	Target
10.0.0.0/16	lokal
2001:db8:1234:1a00::/56	lokal
0.0.0. 0/0	*nat-gateway-id*
::/0	*eigw-id*
s3-prefix-list-id	*s3-gateway-id*

Keamanan

Berikut ini adalah contoh aturan yang mungkin Anda buat untuk grup keamanan yang Anda kaitkan dengan server Anda. Grup keamanan harus mengizinkan lalu lintas dari penyeimbang beban melalui port dan protokol pendengar. Itu juga harus memungkinkan lalu lintas pemeriksaan kesehatan.

Sumber	Protokol	Rentang Port	Komentar
ID of the load balancer security group	*listener protocol*	*listener port*	Memungkinkan lalu lintas masuk dari penyeimbang beban pada port pendengar
ID of the load balancer security group	*health check protocol*	*health check port*	Memungkinkan lalu lintas pemeriksaan kesehatan masuk dari penyeimbang beban

1. Buat VPC

Gunakan prosedur berikut untuk membuat VPC dengan subnet publik dan subnet pribadi di dua Zona Ketersediaan, dan gateway NAT di setiap Zona Ketersediaan.

Untuk membuat VPC

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada dasbor, pilih Buat VPC.
3. Untuk Sumber Daya yang akan dibuat, pilih VPC dan lainnya.
4. Konfigurasikan VPC
   a. Untuk Pembuatan otomatis tanda nama, masukkan nama untuk VPC.
   b. Untuk blok IPv4 CIDR, Anda dapat menyimpan saran default, atau sebagai alternatif Anda dapat memasukkan blok CIDR yang diperlukan oleh aplikasi atau jaringan Anda.
   c. Jika aplikasi Anda berkomunikasi dengan menggunakan alamat IPv6, pilih blok IPv6 CIDR, blok Amazon-provided IPv6 CIDR.
5. Konfigurasikan subnet
   a. Untuk Jumlah Zona Ketersediaan, pilih 2, sehingga Anda dapat meluncurkan instans di beberapa Zona Ketersediaan untuk meningkatkan ketahanan.
   b. Untuk Jumlah subnet publik, pilih 2.
   c. Untuk Jumlah subnet pribadi, pilih 2.
   d. Anda dapat menyimpan blok CIDR default untuk subnet publik, atau sebagai alternatif Anda dapat memperluas Ku stomisasi blok CIDR subnet dan memasukkan blok CIDR. Untuk informasi selengkapnya, lihat the section called “Blok subnet CIDR”.
6. Untuk gateway NAT, pilih 1 per AZ untuk meningkatkan ketahanan.
7. Jika aplikasi Anda berkomunikasi menggunakan alamat IPv6, untuk gateway internet Egress saja, pilih Ya.
8. Untuk titik akhir VPC, jika instans Anda harus mengakses bucket S3, pertahankan default S3 Gateway. Jika tidak, instans di subnet pribadi Anda tidak dapat mengakses Amazon S3. Tidak ada biaya untuk opsi ini, jadi Anda dapat mempertahankan default jika Anda mungkin menggunakan bucket S3 di masa mendatang. Jika Anda memilih Tidak Ada, Anda selalu dapat menambahkan titik akhir VPC gateway nanti.
9. Untuk opsi DNS, hapus Aktifkan nama host DNS.

10. Pilih Buat VPC.

2. Men-deploy aplikasi Anda

Idealnya, Anda telah selesai menguji server Anda di lingkungan pengembangan atau pengujian, dan membuat skrip atau gambar yang akan Anda gunakan untuk menerapkan aplikasi Anda dalam produksi.

Anda dapat menggunakan Amazon EC2 Auto Scaling untuk menyebarkan server di beberapa Zona Ketersediaan dan mempertahankan kapasitas server minimum yang diperlukan oleh aplikasi Anda.

Untuk meluncurkan instans dengan menggunakan grup Penskalaan Otomatis

1. Buat template peluncuran untuk menentukan informasi konfigurasi yang diperlukan untuk meluncurkan instans EC2 Anda dengan menggunakan Amazon EC2 Auto Scaling. Untuk petunjuk langkah demi langkah, lihat Membuat template peluncuran untuk grup Penskalaan Otomatis Anda di Panduan Pengguna Penskalaan Otomatis Amazon EC2.
2. Buat grup Penskalaan Otomatis, yang merupakan kumpulan instans EC2 dengan ukuran minimum, maksimum, dan yang diinginkan. Untuk petunjuk langkah demi langkah, lihat Membuat grup Penskalaan Otomatis menggunakan template peluncuran di Panduan Pengguna Penskalaan Otomatis Amazon EC2.
3. Buat penyeimbang beban, yang mendistribusikan lalu lintas secara merata di seluruh instans dalam grup Penskalaan Otomatis Anda, dan lampirkan penyeimbang beban ke grup Penskalaan Otomatis Anda. Untuk informasi selengkapnya, lihat Panduan Pengguna Elastic Load Balancing dan Gunakan Elastic Load Balancing di Panduan Pengguna Penskalaan Otomatis Amazon EC2.

3. Uji konfigurasi Anda

Setelah selesai menerapkan aplikasi Anda, Anda dapat mengujinya. Jika aplikasi Anda tidak dapat mengirim atau menerima lalu lintas yang Anda harapkan, Anda dapat menggunakan Reachability Analyzer untuk membantu memecahkan masalah. Misalnya, Reachability Analyzer dapat mengidentifikasi masalah konfigurasi dengan tabel rute atau grup keamanan Anda. Untuk informasi selengkapnya, lihat Panduan Peng analisis Jangkauan.

4. Bersihkan

Ketika Anda selesai dengan konfigurasi ini, Anda dapat menghapusnya. Sebelum Anda dapat menghapus VPC, Anda harus menghapus grup Auto Scaling, menghentikan instans Anda, menghapus gateway NAT, dan menghapus penyeimbang beban. Lihat informasi yang lebih lengkap di the section called “Hapus VPC Anda”.

Tutorial VPC

Amazon Virtual Private Cloud (VPC) adalah fondasi infrastruktur jaringan Anda. AWS Sementara AWS Management Console menyediakan antarmuka yang ramah pengguna, AWS Command Line Interface (CLI) menawarkan fleksibilitas dan kemampuan otomatisasi yang lebih besar untuk membuat dan mengelola sumber daya VPC Anda.

Panduan ini menyajikan dua skenario penyebaran VPC penting:

- Pengaturan VPC dasar dengan subnet publik, ideal untuk aplikasi web sederhana
- Konfigurasi VPC canggih dengan subnet pribadi dan publik menggunakan gateway NAT, cocok untuk aplikasi multi-tier

Dengan mengikuti tutorial ini, Anda akan belajar cara:

- Buat VPCs dengan konfigurasi subnet yang berbeda
- Mengatur gateway internet dan NAT
- Konfigurasikan tabel rute dan grup keamanan
- Gunakan AWS CLI perintah untuk mengelola infrastruktur jaringan Anda
- Menerapkan praktik terbaik AWS jaringan

Mari mulai membangun infrastruktur AWS jaringan Anda menggunakan baris perintah.

Tutorial

- Memulai dengan Amazon VPC menggunakan CLI AWS
- Buat VPC dengan subnet pribadi dan gateway NAT menggunakan AWS CLI

Memulai dengan Amazon VPC menggunakan CLI AWS

Tutorial ini memandu Anda melalui pembuatan Virtual Private Cloud (VPC) menggunakan AWS Command Line Interface ().AWS CLI Anda akan belajar cara mengatur VPC dengan subnet publik dan pribadi, mengonfigurasi konektivitas internet, dan menyebarkan EC2 instance untuk mendemonstrasikan arsitektur aplikasi web yang umum.

Prasyarat

Sebelum Anda memulai tutorial ini, pastikan Anda memiliki yang berikut:

1. The AWS CLI. Jika Anda perlu menginstalnya, ikuti panduan AWS CLI instalasi.
2. Konfigurasikan Anda AWS CLI dengan kredensi yang sesuai. Jalankan `aws configure` jika Anda belum menyiapkan kredensional Anda.
3. Pemahaman dasar tentang konsep jaringan.
4. Identity and access management untuk Amazon VPCuntuk membuat dan mengelola sumber daya VPC di akun Anda AWS .

Pertimbangan Biaya

Tutorial ini menciptakan AWS sumber daya yang mungkin menimbulkan biaya di akun Anda. Biaya utama berasal dari NAT Gateway ($0,045 per jam ditambah biaya pemrosesan data) dan EC2 instance (t2.micro, masing-masing sekitar $0,0116 per jam). Jika Anda menyelesaikan tutorial ini dalam satu jam dan kemudian membersihkan semua sumber daya, total biaya akan menjadi sekitar $0,07. Untuk optimalisasi biaya di lingkungan pengembangan, pertimbangkan untuk menggunakan Instans NAT alih-alih Gateway NAT, yang dapat mengurangi biaya secara signifikan.

Mari kita verifikasi bahwa Anda AWS CLI telah dikonfigurasi dengan benar sebelum melanjutkan.

```
aws configure list
```

Anda akan melihat kunci AWS akses, kunci rahasia, dan wilayah default Anda. Juga, verifikasi bahwa Anda memiliki izin yang diperlukan untuk membuat sumber daya VPC.

```
aws sts get-caller-identity
```

Perintah ini menampilkan ID AWS akun, ID pengguna, dan ARN, yang mengonfirmasi bahwa kredensialnya valid.

Buat VPC

Virtual Private Cloud (VPC) adalah jaringan virtual yang didedikasikan untuk akun Anda. AWS Di bagian ini, Anda akan membuat VPC dengan blok CIDR 10.0.0.0/16, yang menyediakan hingga 65.536 alamat IP.

Buat VPC

Perintah berikut membuat VPC baru dan memberinya tag nama.

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --tag-specifications
 'ResourceType=vpc,Tags=[{Key=Name,Value=MyVPC}]'
```

Catat ID VPC di output. Anda akan membutuhkannya untuk perintah berikutnya. Untuk tujuan tutorial ini, kita akan menggunakan “vpc-0123456789abcdef0" sebagai contoh VPC ID. Ganti ini dengan ID VPC Anda yang sebenarnya di semua perintah.

Aktifkan dukungan DNS dan nama host

Secara default, resolusi DNS dan nama host DNS dinonaktifkan di VPC baru. Aktifkan fitur-fitur ini untuk memungkinkan instance di VPC Anda menyelesaikan nama domain.

```
aws ec2 modify-vpc-attribute --vpc-id vpc-0123456789abcdef0 --enable-dns-support
aws ec2 modify-vpc-attribute --vpc-id vpc-0123456789abcdef0 --enable-dns-hostnames
```

Perintah ini tidak menghasilkan output jika berhasil. VPC Anda sekarang memiliki dukungan DNS dan resolusi nama host diaktifkan.

Buat subnet

Subnet adalah segmen dari rentang alamat IP VPC di mana Anda dapat menempatkan kelompok sumber daya yang terisolasi. Di bagian ini, Anda akan membuat subnet publik dan pribadi di dua Availability Zone untuk ketersediaan tinggi.

Dapatkan Availability Zone yang tersedia

Pertama, ambil Availability Zones yang tersedia di wilayah Anda.

```
aws ec2 describe-availability-zones
```

Untuk tutorial ini, kita akan menggunakan dua Availability Zones pertama. Perhatikan nama mereka dari output (misalnya, “us-east-1a” dan “us-east-1b”).

Buat subnet publik

Subnet publik digunakan untuk sumber daya yang perlu diakses dari internet, seperti server web.

```
aws ec2 create-subnet \
  --vpc-id vpc-0123456789abcdef0 \
  --cidr-block 10.0.0.0/24 \
  --availability-zone us-east-1a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Public-Subnet-AZ1}]'
```

Perhatikan subnet ID dari output. Untuk tutorial ini, kita akan menggunakan “subnet-0123456789abcdef0" sebagai contoh untuk subnet publik pertama.

```
aws ec2 create-subnet \
  --vpc-id vpc-0123456789abcdef0 \
  --cidr-block 10.0.1.0/24 \
  --availability-zone us-east-1b \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Public-Subnet-AZ2}]'
```

Perhatikan subnet ID dari output. Untuk tutorial ini, kita akan menggunakan “subnet-0123456789abcdef1" sebagai contoh untuk subnet publik kedua.

Buat subnet pribadi

Subnet pribadi digunakan untuk sumber daya yang seharusnya tidak dapat diakses langsung dari internet, seperti database.

```
aws ec2 create-subnet \
  --vpc-id vpc-0123456789abcdef0 \
  --cidr-block 10.0.2.0/24 \
  --availability-zone us-east-1a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Private-Subnet-AZ1}]'
```

Perhatikan subnet ID dari output. Untuk tutorial ini, kita akan menggunakan “subnet-0123456789abcdef2" sebagai contoh untuk subnet pribadi pertama.

```
aws ec2 create-subnet \
  --vpc-id vpc-0123456789abcdef0 \
  --cidr-block 10.0.3.0/24 \
  --availability-zone us-east-1b \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Private-Subnet-AZ2}]'
```

Perhatikan subnet ID dari output. Untuk tutorial ini, kita akan menggunakan “subnet-0123456789abcdef3" sebagai contoh untuk subnet pribadi kedua.

Anda sekarang memiliki empat subnet: dua subnet publik dan dua subnet pribadi, didistribusikan di dua Availability Zone.

Tip: Saat merencanakan blok CIDR Anda, pastikan blok tersebut tidak tumpang tindih dengan jaringan yang ada. Untuk lingkungan produksi, alokasikan alamat IP yang cukup untuk pertumbuhan masa depan sambil menjaga subnet berukuran cukup untuk keamanan dan manajemen.

Konfigurasikan konektivitas internet

Untuk memungkinkan sumber daya di VPC Anda berkomunikasi dengan internet, Anda perlu membuat dan melampirkan Internet Gateway. Di bagian ini, Anda akan mengatur konektivitas internet untuk VPC Anda.

Buat Internet Gateway

Internet Gateway memungkinkan komunikasi antara VPC Anda dan internet.

```
aws ec2 create-internet-gateway \
  --tag-specifications 'ResourceType=internet-gateway,Tags=[{Key=Name,Value=MyIGW}]'
```

Perhatikan ID Internet Gateway dari output. Untuk tutorial ini, kita akan menggunakan “igw-0123456789abcdef0" sebagai contoh.

Lampirkan Internet Gateway ke VPC Anda

Setelah membuat Internet Gateway, lampirkan ke VPC Anda.

```
aws ec2 attach-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --vpc-id
 vpc-0123456789abcdef0
```

Buat dan konfigurasikan tabel rute

Tabel rute berisi aturan (rute) yang menentukan ke mana lalu lintas jaringan diarahkan. Pertama, buat tabel rute untuk subnet publik Anda.

```
aws ec2 create-route-table \
  --vpc-id vpc-0123456789abcdef0 \
  --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=Public-RT}]'
```

Perhatikan ID tabel rute dari output. Untuk tutorial ini, kita akan menggunakan “rtb-0123456789abcdef0" sebagai contoh untuk tabel rute umum.

Tambahkan rute ke Internet Gateway di tabel rute umum.

```
aws ec2 create-route --route-table-id rtb-0123456789abcdef0 --destination-cidr-block
 0.0.0.0/0 --gateway-id igw-0123456789abcdef0
```

Kaitkan subnet publik dengan tabel rute umum.

```
aws ec2 associate-route-table --route-table-id rtb-0123456789abcdef0 --subnet-id
 subnet-0123456789abcdef0
aws ec2 associate-route-table --route-table-id rtb-0123456789abcdef0 --subnet-id
 subnet-0123456789abcdef1
```

Sekarang, buat tabel rute untuk subnet pribadi Anda.

```
aws ec2 create-route-table \
  --vpc-id vpc-0123456789abcdef0 \
  --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=Private-RT}]'
```

Perhatikan ID tabel rute dari output. Untuk tutorial ini, kita akan menggunakan “rtb-0123456789abcdef1" sebagai contoh untuk tabel rute pribadi.

Kaitkan subnet pribadi dengan tabel rute pribadi.

```
aws ec2 associate-route-table --route-table-id rtb-0123456789abcdef1 --subnet-id
 subnet-0123456789abcdef2
aws ec2 associate-route-table --route-table-id rtb-0123456789abcdef1 --subnet-id
 subnet-0123456789abcdef3
```

Buat Gateway NAT

NAT Gateway memungkinkan instance di subnet pribadi untuk memulai lalu lintas keluar ke internet sambil mencegah lalu lintas masuk dari internet. Ini penting untuk contoh yang perlu mengunduh pembaruan atau mengakses layanan eksternal.

Alokasikan IP Elastis

Pertama, alokasikan alamat IP Elastis untuk NAT Gateway Anda.

```
aws ec2 allocate-address --domain vpc
```

Perhatikan ID Alokasi dari output. Untuk tutorial ini, kita akan menggunakan “eipalloc-0123456789abcdef0" sebagai contoh.

Buat NAT Gateway

Buat Gateway NAT di salah satu subnet publik Anda menggunakan IP Elastis yang dialokasikan.

```
aws ec2 create-nat-gateway \
  --subnet-id subnet-0123456789abcdef0 \
  --allocation-id eipalloc-0123456789abcdef0 \
  --tag-specifications 'ResourceType=natgateway,Tags=[{Key=Name,Value=MyNATGateway}]'
```

Perhatikan ID Gateway NAT dari output. Untuk tutorial ini, kita akan menggunakan “nat-0123456789abcdef0" sebagai contoh.

Tunggu NAT Gateway tersedia sebelum melanjutkan.

```
aws ec2 wait nat-gateway-available --nat-gateway-ids nat-0123456789abcdef0
```

Tambahkan rute ke NAT Gateway

Tambahkan rute ke NAT Gateway di tabel rute pribadi untuk memungkinkan instance di subnet pribadi mengakses internet.

```
aws ec2 create-route --route-table-id rtb-0123456789abcdef1 --destination-cidr-block
 0.0.0.0/0 --nat-gateway-id nat-0123456789abcdef0
```

Catatan: Untuk lingkungan produksi, pertimbangkan untuk membuat Gateway NAT di setiap Availability Zone di mana Anda memiliki subnet pribadi untuk menghilangkan satu titik kegagalan.

Konfigurasikan pengaturan subnet

Konfigurasikan subnet publik Anda untuk secara otomatis menetapkan alamat IP publik ke instance yang diluncurkan di dalamnya.

```
aws ec2 modify-subnet-attribute --subnet-id subnet-0123456789abcdef0 --map-public-ip-
on-launch
aws ec2 modify-subnet-attribute --subnet-id subnet-0123456789abcdef1 --map-public-ip-
on-launch
```

Ini memastikan bahwa instance yang diluncurkan di subnet publik Anda menerima alamat IP publik secara default, membuatnya dapat diakses dari internet.

Buat grup keamanan

Grup keamanan bertindak sebagai firewall virtual untuk instans Anda untuk mengontrol lalu lintas masuk dan keluar. Di bagian ini, Anda akan membuat grup keamanan untuk server web dan server database.

Buat grup keamanan untuk server web

```
aws ec2 create-security-group \
  --group-name WebServerSG \
  --description "Security group for web servers" \
  --vpc-id vpc-0123456789abcdef0
```

Perhatikan ID grup keamanan dari output. Untuk tutorial ini, kita akan menggunakan “sg-0123456789abcdef0" sebagai contoh untuk grup keamanan server web.

Izinkan lalu lintas HTTP dan HTTPS ke server web Anda.

```
aws ec2 authorize-security-group-ingress --group-id sg-0123456789abcdef0 --protocol tcp
 --port 80 --cidr 0.0.0.0/0
aws ec2 authorize-security-group-ingress --group-id sg-0123456789abcdef0 --protocol tcp
 --port 443 --cidr 0.0.0.0/0
```

Catatan: Untuk lingkungan produksi, batasi lalu lintas masuk ke rentang IP tertentu daripada mengizinkan lalu lintas dari 0.0.0.0/0 (alamat IP apa pun).

Membuat grup keamanan untuk server database

```
aws ec2 create-security-group \
  --group-name DBServerSG \
  --description "Security group for database servers" \
  --vpc-id vpc-0123456789abcdef0
```

Perhatikan ID grup keamanan dari output. Untuk tutorial ini, kita akan menggunakan “sg-0123456789abcdef1" sebagai contoh untuk grup keamanan server database.

Izinkan MySQL/Aurora lalu lintas dari server web saja.

```
aws ec2 authorize-security-group-ingress --group-id sg-0123456789abcdef1 --protocol tcp
 --port 3306 --source-group sg-0123456789abcdef0
```

Konfigurasi ini memastikan bahwa hanya instance dalam grup keamanan server web yang dapat terhubung ke server database Anda pada port 3306, mengikuti prinsip hak istimewa paling sedikit.

Verifikasi konfigurasi VPC Anda

Setelah membuat semua komponen yang diperlukan, verifikasi konfigurasi VPC Anda untuk memastikan semuanya diatur dengan benar.

Periksa VPC Anda

```
aws ec2 describe-vpcs --vpc-id vpc-0123456789abcdef0
```

Periksa subnet Anda

```
aws ec2 describe-subnets --filters "Name=vpc-id,Values=vpc-0123456789abcdef0"
```

Periksa tabel rute Anda

```
aws ec2 describe-route-tables --filters "Name=vpc-id,Values=vpc-0123456789abcdef0"
```

Periksa Internet Gateway Anda

```
aws ec2 describe-internet-gateways --filters "Name=attachment.vpc-
id,Values=vpc-0123456789abcdef0"
```

Periksa NAT Gateway Anda

```
aws ec2 describe-nat-gateways --filter "Name=vpc-id,Values=vpc-0123456789abcdef0"
```

Periksa grup keamanan Anda

```
aws ec2 describe-security-groups --filters "Name=vpc-id,Values=vpc-0123456789abcdef0"
```

Perintah ini memberikan informasi terperinci tentang setiap komponen VPC Anda, memungkinkan Anda memverifikasi bahwa semuanya dikonfigurasi dengan benar.

Menyebarkan contoh EC2

Sekarang setelah Anda membuat infrastruktur VPC, Anda dapat menerapkan EC2 instance untuk menunjukkan cara kerja arsitektur. Anda akan meluncurkan server web di subnet publik dan server database di subnet pribadi.

Buat key pair untuk akses SSH

Pertama, buat key pair untuk terhubung dengan aman ke instans Anda:

```
aws ec2 create-key-pair --key-name vpc-tutorial-key --query 'KeyMaterial' --output text
 > vpc-tutorial-key.pem
chmod 400 vpc-tutorial-key.pem
```

Perintah ini membuat key pair baru dan menyimpan kunci pribadi ke file dengan izin terbatas.

Temukan Amazon Linux 2 AMI terbaru

Temukan AMI Amazon Linux 2 terbaru yang akan digunakan untuk instans Anda:

```
aws ec2 describe-images --owners amazon \
  --filters "Name=name,Values=amzn2-ami-hvm-*-x86_64-gp2" "Name=state,Values=available"
 \
  --query "sort_by(Images, &CreationDate)[-1].ImageId" --output text
```

Perhatikan ID AMI dari output. Untuk tutorial ini, kita akan menggunakan “ami-0123456789abcdef0" sebagai contoh.

Luncurkan server web di subnet publik

Sekarang, luncurkan EC2 instance di subnet publik untuk berfungsi sebagai server web:

```
aws ec2 run-instances \
  --image-id ami-0123456789abcdef0 \
  --count 1 \
  --instance-type t2.micro \
  --key-name vpc-tutorial-key \
  --security-group-ids sg-0123456789abcdef0 \
  --subnet-id subnet-0123456789abcdef0 \
  --associate-public-ip-address \
  --user-data '#!/bin/bash
               yum update -y
               yum install -y httpd
```

```
                systemctl start httpd
                systemctl enable httpd
                echo "<h1>Hello from $(hostname -f)</h1>" > /var/www/html/index.html' \
  --tag-specifications 'ResourceType=instance,Tags=[{Key=Name,Value=WebServer}]'
```

Perhatikan ID instance dari output. Untuk tutorial ini, kita akan menggunakan “i-0123456789abcdef0" sebagai contoh untuk instance server web.

Luncurkan server database di subnet pribadi

Selanjutnya, luncurkan EC2 instance di subnet pribadi untuk berfungsi sebagai server database:

```
aws ec2 run-instances \
  --image-id ami-0123456789abcdef0 \
  --count 1 \
  --instance-type t2.micro \
  --key-name vpc-tutorial-key \
  --security-group-ids sg-0123456789abcdef1 \
  --subnet-id subnet-0123456789abcdef2 \
  --user-data '#!/bin/bash
                yum update -y
                yum install -y mariadb-server
                systemctl start mariadb
                systemctl enable mariadb' \
  --tag-specifications 'ResourceType=instance,Tags=[{Key=Name,Value=DBServer}]'
```

Perhatikan ID instance dari output. Untuk tutorial ini, kita akan menggunakan “i-0123456789abcdef1" sebagai contoh untuk instance server database.

Akses server web Anda

Setelah instance server web Anda berjalan, Anda dapat mengaksesnya menggunakan alamat IP publiknya:

```
aws ec2 describe-instances \
  --instance-ids i-0123456789abcdef0 \
  --query 'Reservations[0].Instances[0].PublicIpAddress' \
  --output text
```

Perintah ini akan menampilkan alamat IP publik server web Anda. Untuk tutorial ini, kita akan menggunakan “203.0.113.10" sebagai contoh.

Anda sekarang dapat membuka URL ini di browser web Anda: http://203.0.113.10

Connect ke instans Anda menggunakan SSH

Untuk terhubung ke server web Anda:

```
ssh -i vpc-tutorial-key.pem ec2-user@203.0.113.10
```

Untuk terhubung ke server database Anda, Anda perlu SSH ke server web Anda terlebih dahulu dan kemudian ke server database Anda:

```
# Get the private IP of the database server
aws ec2 describe-instances \
  --instance-ids i-0123456789abcdef1 \
  --query 'Reservations[0].Instances[0].PrivateIpAddress' \
  --output text
```

Perintah ini akan menampilkan alamat IP pribadi server database Anda. Untuk tutorial ini, kita akan menggunakan “10.0.2.10" sebagai contoh.

```
# First SSH to web server, then to database server
ssh -i vpc-tutorial-key.pem -A ec2-user@203.0.113.10
ssh ec2-user@10.0.2.10
```

Ini menunjukkan arsitektur jaringan yang Anda buat: server web dapat diakses publik, sedangkan server database hanya dapat diakses dari dalam VPC.

Pemecahan masalah

Berikut adalah beberapa masalah umum yang mungkin Anda temui saat membuat VPC dan cara mengatasinya:

Blok CIDR Tumpang tindih

Jika Anda menerima kesalahan tentang tumpang tindih blok CIDR, pastikan bahwa blok CIDR untuk VPC dan subnet Anda tidak tumpang tindih dengan subnet yang ada atau di akun Anda. VPCs

Kesalahan Izin

Jika Anda menemukan kesalahan izin, verifikasi bahwa pengguna atau peran IAM Anda memiliki izin yang diperlukan untuk membuat dan mengelola sumber daya VPC. Anda mungkin perlu melampirkan `AmazonVPCFullAccess` kebijakan atau membuat kebijakan khusus dengan izin yang diperlukan.

Batas Sumber Daya

AWS akun memiliki batasan default pada jumlah VPCs, subnet, dan sumber daya lain yang dapat Anda buat. Jika Anda mencapai batas ini, Anda dapat meminta peningkatan melalui AWS Support Center.

Kegagalan Ketergantungan Selama Pembersihan

Saat membersihkan sumber daya, Anda mungkin mengalami kesalahan ketergantungan jika mencoba menghapus sumber daya dalam urutan yang salah. Selalu hapus sumber daya dalam urutan pembuatan terbalik, dimulai dengan sumber daya yang paling bergantung.

Pembersihan sumber daya

Setelah selesai menggunakan VPC, Anda dapat membersihkan sumber daya untuk menghindari biaya. Hapus sumber daya dalam urutan terbalik pembuatan untuk menangani dependensi dengan benar.

Mengakhiri instance EC2

```
aws ec2 terminate-instances --instance-ids i-0123456789abcdef0 i-0123456789abcdef1
aws ec2 wait instance-terminated --instance-ids i-0123456789abcdef0 i-0123456789abcdef1
```

Hapus key pair

```
aws ec2 delete-key-pair --key-name vpc-tutorial-key
rm vpc-tutorial-key.pem
```

Hapus Gateway NAT

```
aws ec2 delete-nat-gateway --nat-gateway-id nat-0123456789abcdef0
aws ec2 wait nat-gateway-deleted --nat-gateway-ids nat-0123456789abcdef0
```

Lepaskan IP Elastis

```
aws ec2 release-address --allocation-id eipalloc-0123456789abcdef0
```

Hapus grup keamanan

```
aws ec2 delete-security-group --group-id sg-0123456789abcdef1
aws ec2 delete-security-group --group-id sg-0123456789abcdef0
```

Hapus tabel rute

Pertama, temukan asosiasi tabel rute IDs:

```
aws ec2 describe-route-tables --route-table-id rtb-0123456789abcdef0
aws ec2 describe-route-tables --route-table-id rtb-0123456789abcdef1
```

Kemudian lepaskan tabel rute dari subnet (ganti asosiasi IDs dengan yang dari output Anda):

```
aws ec2 disassociate-route-table --association-id rtbassoc-0123456789abcdef0
aws ec2 disassociate-route-table --association-id rtbassoc-0123456789abcdef1
aws ec2 disassociate-route-table --association-id rtbassoc-0123456789abcdef2
aws ec2 disassociate-route-table --association-id rtbassoc-0123456789abcdef3
```

Kemudian hapus tabel rute:

```
aws ec2 delete-route-table --route-table-id rtb-0123456789abcdef1
aws ec2 delete-route-table --route-table-id rtb-0123456789abcdef0
```

Lepaskan dan hapus Internet Gateway

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --vpc-id
 vpc-0123456789abcdef0
aws ec2 delete-internet-gateway --internet-gateway-id igw-0123456789abcdef0
```

Hapus subnet

```
aws ec2 delete-subnet --subnet-id subnet-0123456789abcdef0
aws ec2 delete-subnet --subnet-id subnet-0123456789abcdef1
aws ec2 delete-subnet --subnet-id subnet-0123456789abcdef2
aws ec2 delete-subnet --subnet-id subnet-0123456789abcdef3
```

Hapus VPC

```
aws ec2 delete-vpc --vpc-id vpc-0123456789abcdef0
```

Pergi ke produksi

Tutorial ini dirancang untuk membantu Anda mempelajari cara membuat VPC menggunakan. AWS CLI Untuk lingkungan produksi, pertimbangkan praktik terbaik keamanan dan arsitektur berikut:

1. Aturan Grup Keamanan: Batasi lalu lintas masuk ke rentang IP tertentu daripada mengizinkan lalu lintas dari 0.0.0.0/0.
2. Ketersediaan Tinggi: Terapkan Gateway NAT di setiap Availability Zone di mana Anda memiliki subnet pribadi untuk menghilangkan satu titik kegagalan.
3. Jaringan ACLs: Menerapkan Jaringan ACLs sebagai lapisan keamanan tambahan di luar kelompok keamanan.
4. VPC Flow Logs: Aktifkan VPC Flow Logs untuk memantau dan menganalisis pola lalu lintas jaringan.
5. Resource Tagging: Menerapkan strategi penandaan yang komprehensif untuk manajemen sumber daya yang lebih baik.

Untuk informasi lebih lanjut tentang membangun arsitektur siap produksi, lihat Kerangka Kerja AWS Well-Architected dan Praktik Terbaik Keamanan.AWS

Langkah selanjutnya

Sekarang setelah Anda membuat VPC dengan subnet publik dan pribadi, Anda dapat:

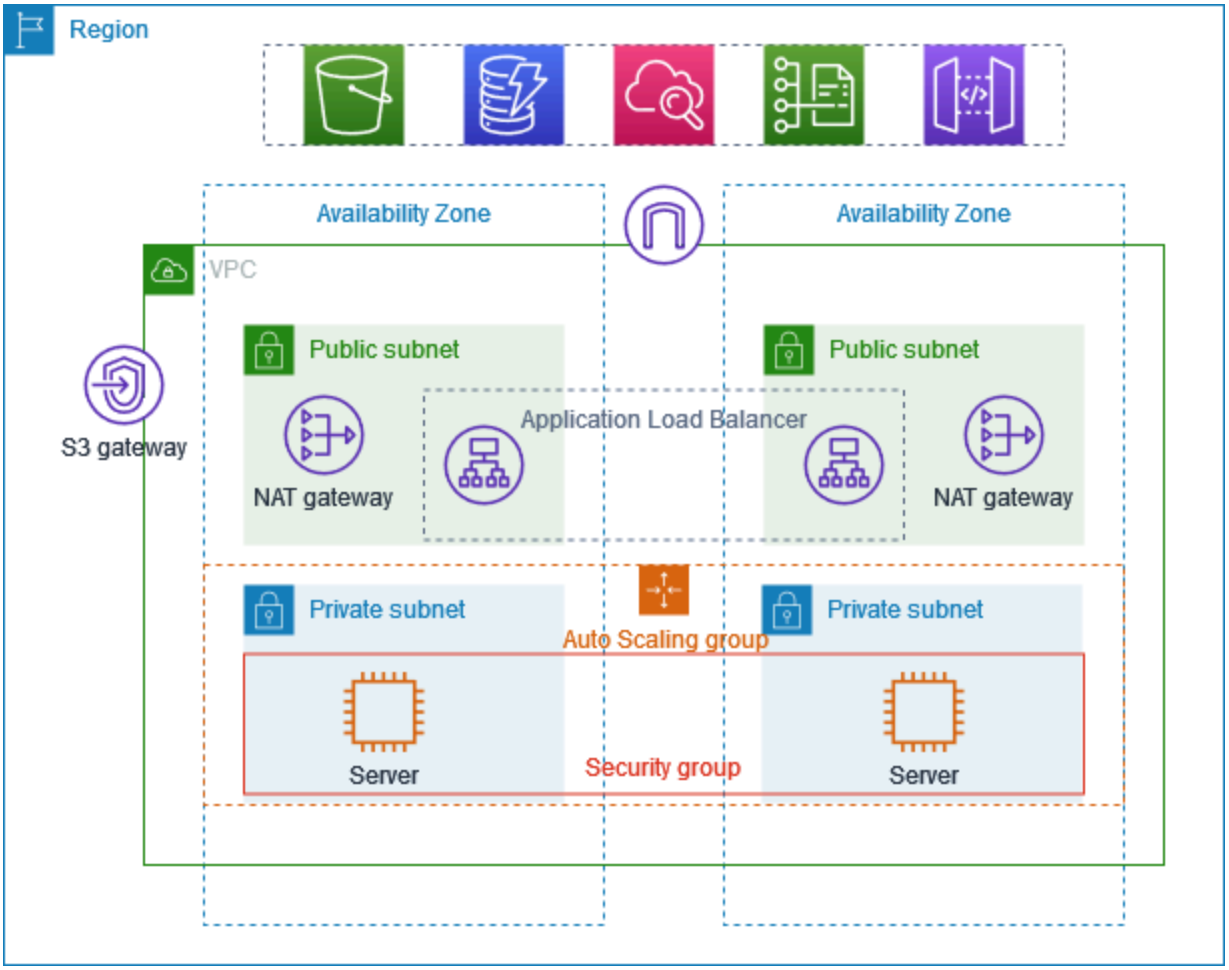
1. Luncurkan EC2 instance di subnet publik atau pribadi Anda.
2. Menyebarkan penyeimbang beban untuk mendistribusikan lalu lintas di beberapa instance.
3. Siapkan grup Auto Scaling untuk ketersediaan dan skalabilitas tinggi.
4. Konfigurasikan database RDS di subnet pribadi Anda.
5. Menerapkan VPC peering untuk terhubung dengan yang lain. VPCs
6. Siapkan koneksi VPN untuk menghubungkan VPC Anda dengan jaringan lokal Anda.

Buat VPC dengan subnet pribadi dan gateway NAT menggunakan AWS CLI

Tutorial ini menunjukkan cara membuat VPC yang dapat Anda gunakan untuk server di lingkungan produksi menggunakan. AWS CLI Untuk meningkatkan ketahanan, Anda akan menerapkan server di dua Availability Zone, menggunakan grup Auto Scaling dan Application Load Balancer. Untuk keamanan tambahan, Anda akan menyebarkan server di subnet pribadi. Server akan menerima permintaan melalui penyeimbang beban dan dapat terhubung ke internet menggunakan gateway

NAT. Untuk meningkatkan ketahanan, Anda akan menerapkan gateway NAT di setiap Availability Zone.

Diagram berikut memberikan gambaran umum tentang sumber daya yang termasuk dalam tutorial ini. VPC memiliki subnet publik dan subnet pribadi di dua Availability Zone. Setiap subnet publik berisi gateway NAT dan node penyeimbang beban. Server berjalan di subnet pribadi, diluncurkan dan dihentikan dengan menggunakan grup Auto Scaling, dan menerima lalu lintas dari penyeimbang beban. Server dapat terhubung ke internet dengan menggunakan gateway NAT. Server dapat terhubung ke Amazon S3 dengan menggunakan titik akhir VPC gateway.



Prasyarat

Sebelum Anda memulai tutorial ini, Anda perlu:

- AWS CLI Diinstal dan dikonfigurasi dengan izin untuk membuat sumber daya VPC EC2 , instance, penyeimbang beban, dan grup Auto Scaling. Untuk informasi tentang menginstal AWS CLI, lihat Menginstal atau memperbarui versi terbaru AWS CLI.

- Pengetahuan dasar tentang konsep VPC, termasuk subnet, tabel rute, dan gateway internet.
- Prosesor JSON `jq` baris perintah diinstal. Ini digunakan untuk mengurai output AWS CLI perintah. Untuk informasi tentang menginstal jq, lihat Download jq.
- Kuota layanan yang memadai untuk sumber daya yang akan Anda buat, termasuk:
- Setidaknya 2 alamat IP Elastis yang tersedia
- Setidaknya 2 gateway NAT
- Setidaknya 1 VPC
- Setidaknya 4 subnet
- Setidaknya 1 Application Load Balancer

Perkiraan biaya: Sumber daya yang dibuat dalam tutorial ini akan dikenakan biaya di AWS akun Anda: Gateway NAT: ~ $0,045 per jam, ditambah biaya pemrosesan data Alamat IP elastis: Gratis bila dikaitkan dengan instance yang sedang berjalan, ~ $0,005 per jam bila tidak terkait instans: Bervariasi berdasarkan jenis EC2 instans (t3.micro digunakan dalam tutorial ini) Application Load Balancer: ~ $0,0225 per jam, ditambah biaya pemrosesan data

Buat VPC dan subnet

Pertama, Anda akan membuat VPC dengan blok CIDR 10.0.0.0/16, yang menyediakan hingga 65.536 alamat IP pribadi.

```
# Create a VPC with CIDR block 10.0.0.0/16
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --tag-specifications
 'ResourceType=vpc,Tags=[{Key=Name,Value=ProductionVPC}]'
```

Perintah tersebut mengembalikan output serupa dengan berikut ini:

```
{
    "Vpc": {
        "CidrBlock": "10.0.0.0/16",
        "DhcpOptionsId": "dopt-abcd1234",
        "State": "pending",
        "VpcId": "vpc-abcd1234",
        "OwnerId": "123456789012",
        "InstanceTenancy": "default",
        "Ipv6CidrBlockAssociationSet": [],
```

```
        "CidrBlockAssociationSet": [
            {
                "AssociationId": "vpc-cidr-assoc-abcd1234",
                "CidrBlock": "10.0.0.0/16",
                "CidrBlockState": {
                    "State": "associated"
                }
            }
        ],
        "IsDefault": false,
        "Tags": [
            {
                "Key": "Name",
                "Value": "ProductionVPC"
            }
        ]
    }
}
```

Perhatikan ID VPC dari output (misalnya,`vpc-abcd1234`). Anda akan menggunakan ID ini dalam perintah berikutnya.

Selanjutnya, Anda akan mengidentifikasi dua Availability Zone di wilayah Anda untuk membuat arsitektur tangguh.

```
# Get available Availability Zones
aws ec2 describe-availability-zones --query 'AvailabilityZones[0:2].ZoneName' --output
 text
```

Perintah tersebut mengembalikan output serupa dengan berikut ini:

```
us-east-1a us-east-1b
```

Sekarang, buat empat subnet: dua subnet publik untuk load balancer dan gateway NAT, dan dua subnet pribadi untuk server aplikasi Anda. Ganti `vpc-abcd1234` dengan ID VPC Anda yang sebenarnya, dan `us-east-1a` dan `us-east-1b` dengan Availability Zone Anda yang sebenarnya.

```
# Create public subnet in first AZ
aws ec2 create-subnet \
  --vpc-id vpc-abcd1234 \
  --cidr-block 10.0.0.0/24 \
```

```
  --availability-zone us-east-1a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=PublicSubnet1}]'

# Create private subnet in first AZ
aws ec2 create-subnet \
  --vpc-id vpc-abcd1234 \
  --cidr-block 10.0.1.0/24 \
  --availability-zone us-east-1a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=PrivateSubnet1}]'

# Create public subnet in second AZ
aws ec2 create-subnet \
  --vpc-id vpc-abcd1234 \
  --cidr-block 10.0.2.0/24 \
  --availability-zone us-east-1b \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=PublicSubnet2}]'

# Create private subnet in second AZ
aws ec2 create-subnet \
  --vpc-id vpc-abcd1234 \
  --cidr-block 10.0.3.0/24 \
  --availability-zone us-east-1b \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=PrivateSubnet2}]'
```

Setiap perintah mengembalikan output yang berisi subnet ID. Perhatikan ini IDs untuk digunakan dalam perintah berikutnya:

- Subnet Publik 1: `subnet-abcd1234`
- Subnet Pribadi 1: `subnet-abcd5678`
- Subnet Publik 2: `subnet-efgh1234`
- Subnet Pribadi 2: `subnet-efgh5678`

Buat dan konfigurasikan konektivitas internet

Di bagian ini, Anda akan membuat gateway internet untuk memungkinkan komunikasi antara VPC dan internet, dan melampirkannya ke VPC Anda.

```
# Create an Internet Gateway
aws ec2 create-internet-gateway --tag-specifications 'ResourceType=internet-
gateway,Tags=[{Key=Name,Value=ProductionIGW}]'
```

Perintah mengembalikan output yang berisi ID Internet Gateway. Perhatikan ID ini (misalnya,`igw-abcd1234`).

Lampirkan Internet Gateway ke VPC Anda. Ganti `igw-abcd1234` dengan ID Internet Gateway Anda yang sebenarnya dan `vpc-abcd1234` dengan ID VPC Anda yang sebenarnya.

```
# Attach the Internet Gateway to the VPC
aws ec2 attach-internet-gateway --internet-gateway-id igw-abcd1234 --vpc-id vpc-
abcd1234
```

Selanjutnya, buat tabel rute untuk subnet publik dan pribadi Anda. Ganti `vpc-abcd1234` dengan ID VPC Anda yang sebenarnya.

```
# Create a route table for public subnets
aws ec2 create-route-table --vpc-id vpc-abcd1234 --tag-specifications
 'ResourceType=route-table,Tags=[{Key=Name,Value=PublicRouteTable}]'

# Create route table for private subnet in first AZ
aws ec2 create-route-table --vpc-id vpc-abcd1234 --tag-specifications
 'ResourceType=route-table,Tags=[{Key=Name,Value=PrivateRouteTable1}]'

# Create route table for private subnet in second AZ
aws ec2 create-route-table --vpc-id vpc-abcd1234 --tag-specifications
 'ResourceType=route-table,Tags=[{Key=Name,Value=PrivateRouteTable2}]'
```

Setiap perintah mengembalikan output yang berisi ID tabel rute. Perhatikan ini IDs:

- Tabel Rute Umum: `rtb-abcd1234`
- Tabel Rute Pribadi 1: `rtb-efgh1234`
- Tabel Rute Pribadi 2: `rtb-ijkl1234`

Tambahkan rute ke Internet Gateway di tabel rute publik untuk mengaktifkan akses internet. Ganti `rtb-abcd1234` dengan ID tabel rute publik Anda yang sebenarnya dan `igw-abcd1234` dengan ID Internet Gateway Anda yang sebenarnya.

```
# Add a route to the Internet Gateway
aws ec2 create-route --route-table-id rtb-abcd1234 --destination-cidr-block 0.0.0.0/0
 --gateway-id igw-abcd1234
```

Kaitkan subnet dengan tabel rute masing-masing. Ganti tabel rute IDs dan subnet IDs dengan yang sebenarnya IDs.

```
# Associate public subnets with the public route table
aws ec2 associate-route-table --route-table-id rtb-abcd1234 --subnet-id subnet-abcd1234
aws ec2 associate-route-table --route-table-id rtb-abcd1234 --subnet-id subnet-efgh1234

# Associate private subnets with their respective route tables
aws ec2 associate-route-table --route-table-id rtb-efgh1234 --subnet-id subnet-abcd5678
aws ec2 associate-route-table --route-table-id rtb-ijkl1234 --subnet-id subnet-efgh5678
```

Buat gateway NAT

Gateway NAT memungkinkan instance di subnet pribadi untuk terhubung ke internet atau AWS layanan lain, tetapi mencegah internet memulai koneksi dengan instans tersebut. Pertama, alokasikan alamat IP Elastis untuk gateway NAT Anda.

```
# Allocate Elastic IP for NAT Gateway in first AZ
aws ec2 allocate-address --domain vpc --tag-specifications 'ResourceType=elastic-
ip,Tags=[{Key=Name,Value=NAT1-EIP}]'

# Allocate Elastic IP for NAT Gateway in second AZ
aws ec2 allocate-address --domain vpc --tag-specifications 'ResourceType=elastic-
ip,Tags=[{Key=Name,Value=NAT2-EIP}]'
```

Setiap perintah mengembalikan output yang berisi ID alokasi. Perhatikan ini IDs:

- ID Alokasi EIP 1: `eipalloc-abcd1234`
- ID Alokasi EIP 2: `eipalloc-efgh1234`

Buat Gateway NAT di setiap subnet publik. Ganti subnet IDs dan alokasi IDs dengan yang sebenarnya. IDs

```
# Create NAT Gateway in public subnet of first AZ
aws ec2 create-nat-gateway \
  --subnet-id subnet-abcd1234 \
  --allocation-id eipalloc-abcd1234 \
  --tag-specifications 'ResourceType=natgateway,Tags=[{Key=Name,Value=NAT-Gateway1}]'
```

```
# Create NAT Gateway in public subnet of second AZ
aws ec2 create-nat-gateway \
  --subnet-id subnet-efgh1234 \
  --allocation-id eipalloc-efgh1234 \
  --tag-specifications 'ResourceType=natgateway,Tags=[{Key=Name,Value=NAT-Gateway2}]'
```

Setiap perintah mengembalikan output yang berisi NAT Gateway ID. Perhatikan ini IDs:

- Gerbang NAT 1: `nat-abcd1234`
- Gerbang NAT 2: `nat-efgh1234`

NAT Gateways membutuhkan waktu beberapa menit untuk penyediaan. Tunggu sampai tersedia sebelum melanjutkan. Ganti NAT Gateway IDs dengan yang sebenarnya IDs.

```
# Wait for NAT Gateways to be available
aws ec2 wait nat-gateway-available --nat-gateway-ids nat-abcd1234
aws ec2 wait nat-gateway-available --nat-gateway-ids nat-efgh1234
```

Tambahkan rute ke Gateway NAT di tabel rute pribadi untuk mengaktifkan akses internet untuk instance di subnet pribadi. Ganti tabel rute IDs dan NAT Gateway IDs dengan yang sebenarnya IDs.

```
# Add route to NAT Gateway 1 in private route table 1
aws ec2 create-route \
  --route-table-id rtb-efgh1234 \
  --destination-cidr-block 0.0.0.0/0 \
  --nat-gateway-id nat-abcd1234

# Add route to NAT Gateway 2 in private route table 2
aws ec2 create-route \
  --route-table-id rtb-ijkl1234 \
  --destination-cidr-block 0.0.0.0/0 \
  --nat-gateway-id nat-efgh1234
```

Buat titik akhir VPC untuk Amazon S3

Titik akhir VPC untuk Amazon S3 memungkinkan instance di subnet pribadi Anda mengakses S3 tanpa melalui NAT Gateway, yang mengurangi biaya transfer data dan memberikan kinerja jaringan yang lebih baik. Ganti `vpc-abcd1234` dengan ID VPC Anda yang sebenarnya dan tabel rute IDs dengan yang sebenarnya. IDs

```
# Get the prefix list ID for S3 in your region
S3_PREFIX_LIST_ID=$(aws ec2 describe-prefix-lists --filters "Name=prefix-
list-name,Values=com.amazonaws.$(aws configure get region).s3" --query
 'PrefixLists[0].PrefixListId' --output text)

# Create the VPC endpoint for S3
aws ec2 create-vpc-endpoint \
  --vpc-id vpc-abcd1234 \
  --service-name com.amazonaws.$(aws configure get region).s3 \
  --route-table-ids rtb-efgh1234 rtb-ijkl1234 \
  --tag-specifications 'ResourceType=vpc-endpoint,Tags=[{Key=Name,Value=S3-Endpoint}]'
```

Perintah mengembalikan output yang berisi ID titik akhir VPC. Perhatikan ID ini (misalnya,`vpce-abcd1234`).

Konfigurasikan grup keamanan

Grup keamanan bertindak sebagai firewall virtual untuk instans Anda untuk mengontrol lalu lintas masuk dan keluar. Buat grup keamanan untuk penyeimbang beban yang memungkinkan lalu lintas HTTP masuk dari mana saja. Ganti `vpc-abcd1234` dengan ID VPC Anda yang sebenarnya.

```
# Create security group for the load balancer
aws ec2 create-security-group \
  --group-name LoadBalancerSG \
  --description "Security group for the load balancer" \
  --vpc-id vpc-abcd1234 \
  --tag-specifications 'ResourceType=security-
group,Tags=[{Key=Name,Value=LoadBalancerSG}]'
```

Perintah mengembalikan output yang berisi ID grup keamanan. Perhatikan ID ini (misalnya,`sg-abcd1234`).

Izinkan lalu lintas HTTP masuk ke penyeimbang beban. Ganti `sg-abcd1234` dengan ID grup keamanan penyeimbang beban Anda yang sebenarnya.

```
# Allow inbound HTTP traffic from anywhere
aws ec2 authorize-security-group-ingress \
  --group-id sg-abcd1234 \
  --protocol tcp \
  --port 80 \
```

```
  --cidr 0.0.0.0/0
```

Buat grup keamanan untuk server aplikasi yang memungkinkan lalu lintas masuk hanya dari penyeimbang beban. Ganti `vpc-abcd1234` dengan ID VPC Anda yang sebenarnya.

```
# Create security group for the application servers
aws ec2 create-security-group \
  --group-name AppServerSG \
  --description "Security group for the application servers" \
  --vpc-id vpc-abcd1234 \
  --tag-specifications 'ResourceType=security-
group,Tags=[{Key=Name,Value=AppServerSG}]'
```

Perintah mengembalikan output yang berisi ID grup keamanan. Perhatikan ID ini (misalnya,`sg-efgh1234`).

Izinkan lalu lintas HTTP masuk dari grup keamanan penyeimbang beban ke server aplikasi. Ganti `sg-efgh1234` dengan ID grup keamanan server aplikasi Anda yang sebenarnya dan `sg-abcd1234` dengan ID grup keamanan penyeimbang beban Anda yang sebenarnya.

```
# Allow inbound HTTP traffic from the load balancer security group
aws ec2 authorize-security-group-ingress \
  --group-id sg-efgh1234 \
  --protocol tcp \
  --port 80 \
  --source-group sg-abcd1234
```

Buat template peluncuran untuk EC2 instance

Template peluncuran berisi informasi konfigurasi untuk meluncurkan instance, seperti ID AMI, tipe instans, dan grup keamanan. Pertama, buat skrip data pengguna yang akan dieksekusi saat instance diluncurkan.

```
cat > user-data.sh << 'EOF'
#!/bin/bash
yum update -y
yum install -y httpd
systemctl start httpd
systemctl enable httpd
echo "<h1>Hello from $(hostname -f) in $(curl -s http://169.254.169.254/latest/meta-
data/placement/availability-zone)</h1>" > /var/www/html/index.html
```

```
EOF
```

Encode script data pengguna di base64.

```
USER_DATA=$(base64 -w 0 user-data.sh)
```

Dapatkan ID AMI Amazon Linux 2 terbaru.

```
# Get the latest Amazon Linux 2 AMI ID
aws ec2 describe-images --owners amazon --filters "Name=name,Values=amzn2-ami-hvm-
*-x86_64-gp2" "Name=state,Values=available" --query 'sort_by(Images, &CreationDate)
[-1].ImageId' --output text
```

Buat template peluncuran dengan ID AMI, tipe instans, grup keamanan, dan data pengguna. Ganti `sg-efgh1234` dengan ID grup keamanan server aplikasi Anda yang sebenarnya `$AMI_ID` dan dan `$USER_DATA` dengan nilai yang diperoleh dari perintah sebelumnya.

```
# Create a launch template
aws ec2 create-launch-template \
  --launch-template-name AppServerTemplate \
  --version-description "Initial version" \
  --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=Name,Value=AppServerTemplate}]' \
  --launch-template-data '{
    "NetworkInterfaces": [{
      "DeviceIndex": 0,
      "Groups": ["sg-efgh1234"],
      "DeleteOnTermination": true
    }],
    "ImageId": "ami-abcd1234",
    "InstanceType": "t3.micro",
    "UserData":
 "IyEvYmluL2Jhc2gKeXVtIHVwZGF0ZSAteQp5dW0gaW5zdGFsbCAteSBodHRwZApzeXN0ZW1jdGwgc3RhcnQgaHR0cGQKc
+SGVsbG8gZnJvbSAkKGhvc3RuYW1lIC1mKSBpbiAkKGN1cmwgLXMgaHR0cDovLzE2OS4yNTQuMTY5LjI1NC9sYXRlc3QvbW
    "TagSpecifications": [{
      "ResourceType": "instance",
      "Tags": [{
        "Key": "Name",
        "Value": "AppServer"
      }]
    }]
```

```
  }'
```

Buat penyeimbang beban dan grup target

Grup target merutekan permintaan ke target terdaftar, seperti EC2 instance, menggunakan protokol dan port yang Anda tentukan. Buat grup target untuk server aplikasi Anda. Ganti `vpc-abcd1234` dengan ID VPC Anda yang sebenarnya.

```
# Create a target group
aws elbv2 create-target-group \
  --name AppTargetGroup \
  --protocol HTTP \
  --port 80 \
  --vpc-id vpc-abcd1234 \
  --target-type instance \
  --health-check-protocol HTTP \
  --health-check-path / \
  --health-check-port traffic-port
```

Perintah mengembalikan output yang berisi kelompok target ARN. Perhatikan ARN ini (misalnya,`arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/AppTargetGroup/abcd1234`).

Buat Application Load Balancer di subnet publik. Ganti subnet IDs dan ID grup keamanan dengan ID Anda yang sebenarnya IDs.

```
# Create a load balancer
aws elbv2 create-load-balancer \
  --name AppLoadBalancer \
  --subnets subnet-abcd1234 subnet-efgh1234 \
  --security-groups sg-abcd1234 \
  --tags Key=Name,Value=AppLoadBalancer
```

Perintah mengembalikan output yang berisi ARN penyeimbang beban. Perhatikan ARN ini (misalnya,`arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/app/AppLoadBalancer/abcd1234`).

Tunggu penyeimbang beban aktif sebelum melanjutkan. Ganti `arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/app/AppLoadBalancer/abcd1234` dengan ARN penyeimbang beban Anda yang sebenarnya.

```
# Wait for load balancer to be active
aws elbv2 wait load-balancer-available \
  --load-balancer-arns arn:aws:elasticloadbalancing:us-
east-1:123456789012:loadbalancer/app/AppLoadBalancer/abcd1234
```

Buat pendengar untuk penyeimbang beban yang meneruskan lalu lintas HTTP ke grup target. Ganti ARN penyeimbang beban dan ARN grup target dengan ARN Anda yang sebenarnya. ARNs

```
# Create a listener
aws elbv2 create-listener \
  --load-balancer-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/
app/AppLoadBalancer/abcd1234 \
  --protocol HTTP \
  --port 80 \
  --default-actions Type=forward,TargetGroupArn=arn:aws:elasticloadbalancing:us-
east-1:123456789012:targetgroup/AppTargetGroup/abcd1234
```

Membuat grup Auto Scaling

Grup Auto Scaling berisi kumpulan EC2 instance yang diperlakukan sebagai pengelompokan logis untuk tujuan penskalaan dan manajemen otomatis. Buat grup Auto Scaling yang menggunakan template peluncuran dan menempatkan instance di subnet pribadi. Ganti subnet IDs dan kelompok sasaran ARN dengan ARN aktual IDs dan ARN Anda.

```
# Create an Auto Scaling group
aws autoscaling create-auto-scaling-group \
  --auto-scaling-group-name AppAutoScalingGroup \
  --launch-template LaunchTemplateName=AppServerTemplate,Version='$Latest' \
  --min-size 2 \
  --max-size 4 \
  --desired-capacity 2 \
  --vpc-zone-identifier "subnet-abcd5678,subnet-efgh5678" \
  --target-group-arns arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/
AppTargetGroup/abcd1234 \
  --health-check-type ELB \
  --health-check-grace-period 300 \
  --tags Key=Name,Value=AppServer,PropagateAtLaunch=true
```

Uji konfigurasi Anda

Setelah grup Auto Scaling meluncurkan instans dan mereka lulus pemeriksaan kesehatan, Anda dapat menguji penyeimbang beban Anda. Dapatkan nama DNS dari penyeimbang beban. Ganti ARN penyeimbang beban dengan ARN Anda yang sebenarnya.

```
# Get the DNS name of the load balancer
aws elbv2 describe-load-balancers \
  --load-balancer-arns arn:aws:elasticloadbalancing:us-
east-1:123456789012:loadbalancer/app/AppLoadBalancer/abcd1234 \
  --query "LoadBalancers[0].DNSName" \
  --output text
```

Gunakan curl untuk menguji aplikasi dengan nama penyeimbang beban.

```
curl http://LoadBalancerName
```

Jika Anda me-refresh halaman beberapa kali, Anda akan melihat tanggapan dari berbagai instance di Availability Zone yang berbeda.

Pembersihan sumber daya

Setelah selesai dengan tutorial ini, Anda harus menghapus semua sumber daya untuk menghindari biaya yang dikenakan. Ganti semua IDs dengan sumber daya Anda yang sebenarnya IDs.

```
# Delete the Auto Scaling group
aws autoscaling delete-auto-scaling-group \
  --auto-scaling-group-name AppAutoScalingGroup \
  --force-delete

# Wait for the Auto Scaling group to be deleted
sleep 60

# Delete the load balancer
aws elbv2 delete-load-balancer \
  --load-balancer-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/
app/AppLoadBalancer/abcd1234

# Wait for the load balancer to be deleted
sleep 30

# Delete the target group
```

```
aws elbv2 delete-target-group \
  --target-group-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/
AppTargetGroup/abcd1234

# Delete the launch template
aws ec2 delete-launch-template \
  --launch-template-name AppServerTemplate

# Delete the NAT Gateways
aws ec2 delete-nat-gateway --nat-gateway-id nat-abcd1234
aws ec2 delete-nat-gateway --nat-gateway-id nat-efgh1234

# Wait for the NAT Gateways to be deleted
sleep 90

# Release the Elastic IPs
aws ec2 release-address --allocation-id eipalloc-abcd1234
aws ec2 release-address --allocation-id eipalloc-efgh1234

# Delete the VPC endpoint
aws ec2 delete-vpc-endpoints --vpc-endpoint-ids vpce-abcd1234

# Wait for security group dependencies to clear
sleep 30

# Delete the security groups
aws ec2 delete-security-group --group-id sg-efgh1234
aws ec2 delete-security-group --group-id sg-abcd1234

# Detach the Internet Gateway
aws ec2 detach-internet-gateway --internet-gateway-id igw-abcd1234 --vpc-id vpc-
abcd1234

# Delete the Internet Gateway
aws ec2 delete-internet-gateway --internet-gateway-id igw-abcd1234

# Delete the route tables
aws ec2 delete-route-table --route-table-id rtb-efgh1234
aws ec2 delete-route-table --route-table-id rtb-ijkl1234
aws ec2 delete-route-table --route-table-id rtb-abcd1234

# Delete the subnets
aws ec2 delete-subnet --subnet-id subnet-abcd1234
aws ec2 delete-subnet --subnet-id subnet-efgh1234
```

```
aws ec2 delete-subnet --subnet-id subnet-abcd5678
aws ec2 delete-subnet --subnet-id subnet-efgh5678

# Delete the VPC
aws ec2 delete-vpc --vpc-id vpc-abcd1234
```

Langkah berikutnya

Sekarang setelah Anda membuat VPC dengan subnet pribadi dan gateway NAT, Anda mungkin ingin menjelajahi topik terkait ini:

- Praktik terbaik keamanan untuk VPC Anda
- Pencatatan lalu lintas IP menggunakan Log Aliran VPC
- Kebijakan penskalaan grup Auto Scaling
- Pemeriksaan kesehatan kelompok sasaran penyeimbang beban

Kuota Amazon VPC

Tabel berikut mencantumkan kuota, sebelumnya disebut sebagai batas, untuk sumber daya Amazon VPC untuk AWS akun Anda. Kecuali dinyatakan lain, kuota ini adalah per Wilayah.

Jika Anda meminta penambahan kuota yang berlaku per sumber daya, kami meningkatkan kuota untuk semua sumber daya di Wilayah.

VPC dan subnet

Nama	Default	Dapat disesuaikan	Komentar
VPC per Wilayah	5	Ya	Penambahan kuota ini menambah kuota pada gateway internet per Wilayah dengan jumlah yang sama. Anda dapat meningkatkan batas ini sehingga Anda dapat memiliki ratusan VPC per Wilayah.
Subnet per VPC	200	Ya	
Blok CIDR IPv4 per VPC	5	Ya (hingga 50)	Blok CIDR primer ini dan semua blok CIDR sekunder dihitung terhadap kuota ini.
blok CIDR IPv6 per VPC	5	Ya (hingga 50)	Jumlah CIDR yang dapat Anda alokasikan ke satu VPC.
Pengecualian Akses Publik Blok VPC per akun per Wilayah	50	Ya. Untuk meminta kenaikan, lihat Mem inta peningkatan kuota layanan	Jumlah pengecualian VPC BPA yang dapat Anda buat di akun.

Nama	Default	Dapat disesuaikan	Komentar
		di Panduan Pengguna AWS Dukungan.	

DNS

Setiap instance EC2 dapat mengirim 1024 paket per detik per antarmuka jaringan ke Route 53 Resolver (khususnya alamat.2, seperti 10.0.0.2 dan 169.254.169.253). Kuota ini tidak dapat dinaikkan jumlahnya. Jumlah kueri DNS per detik yang didukung oleh Route 53 Resolver bervariasi berdasarkan jenis kueri, ukuran respons, dan protokol yang digunakan. Untuk informasi selengkapnya dan rekomendasi untuk arsitektur DNS yang dapat diskalakan, lihat Panduan AWS Teknis DNS Hybrid dengan Active Directory.

Alamat IP elastis

Nama	Default	Dapat disesuaikan	Komentar
Alamat IP Elastis per Wilayah	5	Ya	Kuota ini berlaku untuk Akun AWS VPC individu dan VPC bersama.
Alamat IP elastis per gateway NAT publik	2	Ya	Anda dapat meminta kenaikan kuota hingga 8.

Gateway

Nama	Default	Dapat disesuaikan	Komentar
Egress-only gateway internet per Wilayah	5	Ya	Untuk menambah kuota ini, tingkatkan kuota VPC per Wilayah.

Nama	Default	Dapat disesuaikan	Komentar
			Anda dapat melampirkan hanya satu gateway internet egress untuk satu VPC pada suatu waktu.
Gateway internet per Wilayah	5	Ya	Untuk menambah kuota ini, tingkatkan kuota VPC per Wilayah. Anda dapat melampirkan hanya satu gateway internet untuk satu VPC pada suatu waktu.
NAT gateway per Availability Zone	5	Ya	Gerbang NAT hanya diperhitungkan dalam kuota Anda di negara `pending` bagian`active`,, dan`deleting`.
Kuota alamat IP pribadi per gateway NAT	8	Ya	
Gateway operator per VPC	1	Tidak	

Customer-managed daftar awalan

Meskipun kuota default untuk daftar awalan yang dikelola pelanggan dapat disesuaikan, Anda tidak dapat meminta peningkatan menggunakan konsol Kuota Layanan. Anda harus membuka kasus dukungan. Lihat Meminta peningkatan kuota layanan di Panduan Pengguna AWS Dukungan.

Nama	Default	Dapat disesuaikan	Komentar
Daftar prefiks per Wilayah	100	Ya	
Versi per daftar prefiks	1.000	Ya	Jika daftar prefiks memiliki 1.000 versi yang disimpan dan Anda menambahkan

Nama	Default	Dapat disesuaikan	Komentar
			versi baru, versi tertua akan dihapus agar versi baru dapat ditambahkan.
Jumlah maksimum entri per daftar prefiks	1.000	Ya	Anda dapat mengubah ukuran daftar awalan yang dikelola pelanggan hingga 1000. Untuk informasi selengkapnya, lihat Mengubah ukuran daftar awalan. Ketika Anda menyebutkan daftar prefiks di suatu sumber daya, jumlah maksimum entri untuk daftar prefiks tersebut dihitung berdasarkan kuota untuk jumlah entri untuk sumber daya tersebut. Sebagai contoh, jika Anda membuat daftar prefiks dengan maksimum 20 entri dan Anda sebutkan daftar prefiks tersebut dalam aturan grup keamanan, ini dianggap sebagai 20 aturan grup keamanan.
Referensi ke daftar prefiks per jenis sumber daya	10,000	Ya	Kuota ini berlaku per jenis sumber daya yang dapat merujuk ke daftar prefiks. Misalnya, Anda dapat memiliki 10.000 referensi ke daftar awalan di semua grup keamanan Anda ditambah 10.000 referensi ke daftar awalan di semua tabel rute subnet Anda. Jika Anda membagikan daftar awalan dengan AWS akun lain, referensi akun lain ke daftar awalan Anda diperhitungkan dalam kuota Anda.

ACL jaringan

Nama	Default	Dapat disesuaikan	Komentar
ACL jaringan per VPC	200	Ya	Anda dapat mengaitkan satu jaringan ACL untuk satu atau lebih subnet di VPC.
Aturan per jaringan ACL	20	Ya	Kuota ini menentukan jumlah maksimum aturan masuk dan jumlah maksimum aturan keluar. Kuota ini dapat ditingkatkan hingga maksimum 40 aturan masuk dan 40 aturan keluar (untuk total 80 aturan), tetapi kinerja jaringan mungkin terpengaruh.

Antarmuka jaringan

Nama	Default	Dapat disesuaikan	Komentar
Antarmuka jaringan per instans	Bervariasi tergantung tipe instans	Tidak	Untuk informasi selengkapnya, lihat Antarmuka jaringan per tipe instans.
Antarmuka jaringan per Wilayah	5000	Ya	Kuota ini berlaku untuk Akun AWS VPC individu dan VPC bersama. Batas ini diberlakukan per Availability Zone (AZ). Jika, misalnya, antarmuka jaringan berada di tiga AZ, setiap AZ akan

Nama	Default	Dapat disesuaikan	Komentar
			memiliki batas 5.000 dan Wilayah akan memiliki batas 15.000.

Tabel rute

Nama	Default	Dapat disesuaikan	Komentar
Tabel rute per VPC	200	Ya	Tabel rute utama dihitung terhadap kuota ini. Perhatikan bahwa jika Anda meminta kenaikan kuota untuk tabel rute, Anda mungkin juga ingin meminta kenaikan kuota untuk subnet. Sementara tabel rute dapat dibagikan dengan beberapa subnet, subnet hanya dapat dikaitkan dengan tabel rute tunggal.
Rute per tabel rute (rute yang tidak disebarkan)	500	Ya	Anda dapat menambah kuota ini hingga maksimum 1.000; namun, performa jaringan mungkin terkena dampaknya. Kuota ini diberlakukan secara terpisah untuk rute IPv4 dan rute IPv6. Jika Anda memiliki lebih dari 125 rute, kami sarankan Anda memberikan nomor halaman panggilan untuk menggambarkan tabel rute Anda untuk performa yang lebih baik.
Rute yang disebarkan per tabel rute	100	Tidak	Jika Anda memerlukan prefiks tambahan, iklankan rute default.

Server rute

Nama	Default	Dapat disesuaikan	Komentar
Rute server per VPC	5	Ya. Untuk meminta kenaikan, lihat Meminta peningkatan kuota layanan di Panduan Pengguna AWS Dukungan.	
Titik akhir server rute per server rute	10	Ya. Untuk meminta kenaikan, lihat Meminta peningkatan kuota layanan di Panduan Pengguna AWS Dukungan.	

Nama	Default	Dapat disesuaikan	Komentar
Sesi peering per antarmuka jaringan	20	Ya. Untuk meminta kenaikan, lihat Meminta peningkatan kuota layanan di Panduan Pengguna AWS Dukungan.	
Titik akhir server rute per server rute dan subnet	2	Tidak	Anda hanya dapat memiliki dua titik akhir di subnet yang sama untuk server rute yang sama untuk redundansi.
Rute per peer server rute	100	Tidak	Ini adalah jumlah rute yang dapat diiklankan secara dinamis melalui peer server rute
Rute per server rute	100	Tidak	Ini adalah jumlah rute yang dapat diinstal di Forwarding Information Base (FIB) dari server rute.

Grup keamanan

Nama	Default	Dapat disesuaikan	Komentar
Grup keamanan VPC per Wilayah	2500	Ya	Kuota ini berlaku untuk Akun AWS VPC individu dan VPC bersama. Jika Anda menambah kuota ini hingga lebih dari 5.000 grup keamanan di Wilayah, kami sarankan agar Anda melakukan pemberian nomor panggilan untuk menjelaskan grup keamanan Anda agar memiliki performa yang lebih baik.
Aturan masuk atau keluar per grup keamanan	60	Ya	Kuota ini diberlakukan secara terpisah untuk aturan masuk dan keluar. Untuk akun dengan kuota default 60 aturan, grup keamanan dapat memiliki 60 aturan masuk dan 60 aturan keluar. Selain itu, kuota ini diberlakukan secara terpisah untuk aturan IPv4 dan aturan IPv6. Untuk akun dengan kuota default 60 aturan, grup keamanan dapat memiliki 60 aturan masuk untuk lalu lintas IPv4 dan 60 aturan masuk untuk lalu lintas IPv6. Untuk informasi selengkapnya, lihat the section called “Ukuran grup keamanan”. Perubahan kuota berlaku untuk aturan masuk dan keluar. Kuota ini yang dikalikan dengan kuota untuk grup keamanan per antarmuka jaringan tidak dapat lebih dari 1.000.

Nama	Default	Dapat disesuaikan	Komentar
Grup keamanan per antarmuka jaringan	5	Ya (hingga 16)	Kuota ini dikalikan dengan kuota aturan per grup keamanan tidak boleh melebihi 1.000. Untuk mengurangi kuota grup keamanan per antarmuka jaringan di bawah nilai default 5, lihat Meminta peningkatan kuota layanan di Panduan Pengguna AWS Dukungan. Anda menggunakan proses yang sama untuk meminta penurunan seperti yang Anda lakukan untuk meminta kenaikan.

Berbagi subnet VPC

Semua kuota VPC standar berlaku untuk subnet VPC bersama.

Nama	Default	Dapat disesuaikan	Komentar
Akun peserta per VPC	100	Ya	Jumlah maksimum akun peserta berbeda yang dapat dibagikan dengan subnet dalam VPC. Ini adalah kuota per VPC dan berlaku di semua subnet yang dibagikan dalam suatu VPC. Pemilik VPC dapat melihat antarmuka jaringan dan grup keamanan yang dilekatkan pada sumber daya peserta.
Subnet yang dapat dibagikan dengan suatu akun	100	Ya	Ini adalah jumlah maksimum subnet yang dapat dibagikan dengan AWS akun.

Penggunaan Alamat Jaringan

Penggunaan Alamat Jaringan (NAU) terdiri dari alamat IP, antarmuka jaringan, dan CIDR dalam daftar awalan terkelola. NAU adalah metrik yang diterapkan ke sumber daya dalam VPC untuk membantu Anda merencanakan dan memantau ukuran VPC Anda. Untuk informasi selengkapnya, lihat Penggunaan Alamat Jaringan.

Sumber daya yang membentuk hitungan NAU memiliki kuota layanan masing-masing. Bahkan jika VPC memiliki kapasitas NAU yang tersedia, Anda tidak akan dapat meluncurkan sumber daya ke VPC jika sumber daya telah melebihi kuota layanannya.

Nama	Default	Dapat disesuaikan	Komentar
Penggunaan Alamat Jaringan	64,000	Ya (hingga 256.000)	Jumlah maksimum unit NAU per VPC.
Penggunaan Alamat Jaringan Peered	128.000	Ya (hingga 512.000)	Jumlah maksimum unit NAU untuk VPC dan semua VPC yang diintip intra-wilayahnya. VPC yang diintip di berbagai Wilayah tidak berkontribusi pada jumlah ini.

Amazon EC2 API throttling

Untuk informasi tentang pelambatan Amazon EC2, lihat Meminta pel ambatan di Panduan Pengembang Amazon EC2.

Sumber daya kuota tambahan

Untuk informasi selengkapnya, lihat berikut ini:

- AWS Client VPN kuota dalam Panduan AWS Client VPN Administrator
- Kuota Direct Connect dalam Panduan Pengguna AWS Direct Connect

- Kuota Peering di Panduan Peering Amazon VPC
- PrivateLink kuota dalam AWS PrivateLink Panduan
- Site-to-Site Kuota VPN di Panduan AWS Site-to-Site VPN Pengguna
- Kuota Pencerminan Lalu Lintas di Panduan Pencer minan Lalu Lintas Amazon VPC
- Kuota gateway transit di Panduan Gateway Transit Amazon VPC

Riwayat dokumen

Tabel berikut menjelaskan perubahan penting dalam setiap rilis Panduan Pengguna Amazon VPC.

Perubahan	Deskripsi	Tanggal
Kontrol enkripsi VPC	Anda sekarang dapat menerapkan enkripsi dalam transit untuk lalu lintas jaringan dalam VPC Anda menggunakan kontrol enkripsi VPC. Fitur ini menyediakan penegakan kebijakan enkripsi terpusat dan kemampuan pemantauan.	November 21, 2025
Gerbang NAT regional untuk ekspansi multi-AZ otomatis	Anda sekarang dapat menggunakan gateway NAT regional yang secara otomatis memperluas di seluruh Availability Zone berdasarkan jejak beban kerja Anda. Gerbang NAT regional menyediakan pengaturan yang disederhanakan, keamanan yang ditingkatkan, dan ketersediaan tinggi otomatis tanpa intervensi manual.	November 19, 2025
Merutekan lalu lintas VPC masuk ke alamat IP publik	Anda sekarang dapat mengonfigurasi aturan perutean lanjutan untuk mengarahkan lalu lintas masuk dari internet ke alamat IP publik tertentu dalam VPC Anda, memungkinkan kontrol yang lebih terperinci atas	Agustus 13, 2025

	arus lalu lintas dan keputusan routing untuk skenario masuk.	
Perutean dinamis di VPC Anda menggunakan Amazon VPC Route Server	Amazon VPC Route Server menyederhanakan routing untuk lalu lintas antara beban kerja yang digunakan dalam VPC dan gateway internetn ya. Dengan fitur ini, VPC Route Server secara dinamis memperbarui tabel rute VPC dan gateway dengan rute IPv4 atau IPv6 pilihan Anda untuk mencapai toleransi kesalahan routing untuk beban kerja tersebut. Ini memungkinkan Anda untuk mengubah rute lalu lintas secara otomatis dalam VPC, yang meningkat kan pengelolaan routing VPC dan interoperabilitas dengan beban kerja pihak ketiga.	Maret 31, 2025
AWS pembaruan kebijakan terkelola	Amazon VPC memperbarui AmazonVPCFullAccess dan AmazonVPCReadOnlyAccess mengelola kebijakan.	Desember 9, 2024
Dukungan kebijakan deklaratif untuk VPC BPA	Jika Anda menggunakan AWS Organisasi untuk mengelola akun di organisasi Anda, Anda dapat menggunakan kebijakan deklaratif untuk menerapka n BPA VPC pada akun di organisasi.	Desember 1, 2024

VPC Blok Akses Publik (BPA)	VPC Block Public Access (BPA) memungkinkan Anda memblokir sumber daya di VPC dan subnet yang Anda miliki di Wilayah agar tidak mencapai atau dijangkau dari internet melalui gateway internet dan gateway internet khusus keluar.	November 19, 2024
Grup Keamanan Bersama	Fitur ini memungkinkan Anda untuk berbagi grup keamanan dengan akun AWS Organisasi lainnya.	Oktober 30, 2024
Asosiasi VPC Grup Keamanan	Fitur ini memungkinkan Anda untuk mengaitkan grup keamanan dengan beberapa VPC di Wilayah yang sama.	Oktober 30, 2024
Dukungan MTU gateway NAT	Gerbang NAT mendukung lalu lintas dengan unit transmisi maksimum (MTU) 8500.	September 10, 2024
Pengalamatan IPv6 pribadi	Informasi tentang pengalamatan IPv6 pribadi ditambahkan. Alamat IPv6 pribadi hanya tersedia di Amazon VPC IP Address Manager.	Agustus 8, 2024
Waktu sewa yang disukai IPv6	Anda sekarang dapat memilih seberapa sering instance yang berjalan dengan IPv6 yang ditetapkan untuk itu melewati pembaruan sewa DHCPv6.	Februari 20, 2024

Tinjauan dan perbaikan struktur panduan	Struktur panduan ditinjau dan perbaikan dilakukan untuk meningkatkan pengalaman pelanggan terkait dengan menemukan info untuk skenario tertentu.	Februari 20, 2024
AWS pembaruan kebijakan terkelola	Amazon VPC memperbarui AmazonVPCFullAccess dan AmazonVPCReadOnlyAccess mengelola kebijakan.	Februari 8, 2024
AWS pembaruan kebijakan terkelola	Amazon VPC memperbarui kebijakan terkel AmazonVPC CrossAccountNetworkInterfaceOperations ola.	25 September 2023
EC2-Classic tidak digunakan lagi	Dengan EC2-Classic, instans EC2 berjalan dalam satu jaringan datar yang dibagikan dengan pelanggan lain. Amazon VPC menggantikan EC2-Classic. Dengan Amazon VPC, instans Anda berjalan di cloud pribadi virtual (VPC) yang secara logis terisolasi dengan Anda. Akun AWS	31 Juli 2023

Tambahkan alamat IPv4 sekunder ke gateway NAT	Anda dapat menambahkan alamat IPv4 pribadi sekunder ke gateway NAT publik dan pribadi. Alamat IPv4 sekunder meningkatkan jumlah port yang tersedia, dan oleh karena itu mereka meningkatkan batas jumlah koneksi bersamaan yang dapat dibuat oleh beban kerja Anda menggunakan gateway NAT.	31 Januari 2023
Menyelaraskan dengan praktik terbaik IAM	Memperbarui panduan untuk menyelaraskan dengan praktik terbaik IAM. Untuk informasi lebih lanjut, lihat Praktik terbaik keamanan di IAM.	4 Januari 2023
Pilih alamat IP pribadi dari gateway NAT Anda	Saat Anda membuat gateway NAT, Anda sekarang dapat memilih untuk memilih alamat IP pribadi yang ditetapkan ke gateway NAT. Sebelumnya, alamat IP pribadi secara otomatis ditetapkan dari rentang alamat IP subnet.	17 November 2022
Konfigurasi router gateway default IPv6	Tiga alamat IPv6 sekarang dicadangkan untuk digunakan oleh router VPC default.	11 November 2022
Mentransfer alamat IP Elastis	Anda sekarang dapat mentransfer alamat IP Elastic dari satu AWS akun ke akun lainnya.	31 Oktober 2022

Metrik Penggunaan Alamat Jaringan	Anda dapat mengaktifkan metrik Penggunaan Alamat Jaringan untuk VPC Anda untuk membantu Anda merencanakan dan memantau ukuran VPC Anda.	4 Oktober 2022
Publikasikan Log Alur ke Amazon Data Firehose	Anda dapat menentukan aliran pengiriman Amazon Data Firehose sebagai tujuan untuk data log aliran.	8 September 2022
Bandwidth gateway NAT	Gerbang NAT sekarang mendukung bandwidth hingga 100 Gbps (peningkatan dari 45 Gbps) dan dapat memproses hingga 10 juta paket per detik (naik dari empat juta paket).	15 Juni 2022
Beberapa blok IPv6 CIDR	Anda dapat mengaitkan hingga lima blok IPv6 CIDR ke VPC.	12 Mei 2022
Reorganisasi	Reorganisasi umum Panduan Pengguna Amazon Virtual Private Cloud ini.	Januari 2, 2022
Gerbang NAT IPv6 ke IPv4	NAT gateway mendukung terjemahan alamat jaringan dari IPv6 ke IPv4, yang dikenal sebagai NAT64.	24 November 2021
IPv6-only subnet dalam VPC	Anda dapat membuat IPv6-only subnet tempat Anda dapat meluncurkan instans IPv6-only EC2.	23 November 2021

Opsi pengiriman VPC Flow Logs ke Amazon S3	Anda dapat menentukan format file log Apache Parquet, partisi per jam, dan Hive-compatible awalan S3.	13 Oktober 2021
Tampilan Global Amazon EC2	Amazon EC2 Global View memungkinkan Anda melihat VPC, subnet, instans, grup keamanan, dan volume di beberapa Wil AWS ayah dalam satu konsol.	1 September 2021
Rute yang lebih spesifik	Anda dapat menambahkan rute ke tabel rute yang lebih spesifik daripada rute lokal. Anda dapat menggunakan rute yang lebih spesifik untuk mengarahkan lalu lintas antar subnet dalam VPC (East-West lalu lintas) ke alat middlebox. Anda dapat mengatur tujuan rute agar sesuai dengan seluruh blok IPv4 atau IPv6 CIDR dari subnet di VPC Anda.	Agustus 30, 2021
ID sumber daya dan dukungan penandaan untuk aturan grup keamanan	Anda dapat merujuk ke aturan grup keamanan berdasarkan ID sumber daya. Anda dapat menambahkan tanda ke aturan grup keamanan.	7 Juli 2021

Gerbang NAT pribadi	Anda dapat menggunakan gateway NAT pribadi untuk komunikasi pribadi outbound-only antar VPC atau antara VPC dan jaringan on-premise Anda.	10 Juni 2021
Tandai saat membuat	Anda dapat menambahkan tag ketika Anda membuat VPC, opsi DHCP, gateway internet, gateway egress-only, ACL jaringan, dan grup keamanan.	30 Juni 2020
Daftar awalan terkelola	Anda dapat membuat dan mengelola satu set blok CIDR di daftar prefiks.	29 Juni 2020
Peningkatan log aliran	Bidang log alur baru tersedia, dan Anda dapat menentuka n format khusus untuk log alur yang dipublikasikan ke CloudWatch Log.	4 Mei 2020
Dukungan penandaan untuk log aliran	Anda dapat menambahkan tag ke log alur Anda.	16 Maret 2020
Tandai pada pembuatan gateway NAT	Anda dapat menambahkan tag saat membuat gateway NAT.	9 Maret 2020
Interval agregasi maksimum untuk log aliran	Anda dapat menentukan jangka waktu maksimum selama alur terjadi dan teragregasi ke dalam catatan log alur.	4 Februari 2020

Konfigurasi grup perbatasan jaringan	Anda dapat mengonfigurasi grup perbatasan jaringan untuk VPC Anda dari konsol Amazon VPC.	22 Januari 2020
Tabel rute gateway	Anda dapat mengaitkan tabel rute dengan gateway dan rute masuk lalu lintas VPC rute inbound ke antarmuka jaringan tertentu di VPC Anda.	3 Desember 2019
Peningkatan log aliran	Anda dapat menentukan format kustom untuk log alur Anda dan memilih bidang mana yang akan dikembalikan dalam catatan log alur.	11 September 2019
Berbagi VPC	Anda dapat berbagi subnet yang berada di VPC yang sama dengan beberapa akun di organisasi yang sama AWS .	27 November 2018
Buat subnet default	Anda dapat membuat sebuah subnet default di sebuah Availability Zone yang tidak memiliki subnet.	9 November 2017
Dukungan penandaan untuk gateway NAT	Anda dapat menandai gateway NAT.	7 September 2017
CloudWatch Metrik Amazon untuk gateway NAT	Anda dapat melihat CloudWatch metrik untuk gateway NAT Anda.	7 September 2017
Deskripsi aturan grup keamanan	Anda dapat menambahk an deskripsi ke aturan grup keamanan.	31 Agustus 2017

Blok CIDR IPv4 sekunder untuk VPC Anda	Anda dapat menambahkan beberapa blok CIDR IPv4 untuk VPC Anda.	29 Agustus 2017
Pulihkan alamat IP elastis	Jika Anda merilis alamat IP Elastis Anda, Anda dapat memulihkannya.	11 Agustus 2017
Buat VPC default	Anda dapat membuat VPC default baru jika Anda menghapus VPC default yang ada.	27 Juli 2017
Dukungan IPv6	Anda dapat mengaitkan sebuah blok CIDR IPv6 dengan VPC Anda dan menetapkan alamat IPv6 ke sumber daya di VPC Anda.	1 Desember 2016
Dukungan resolusi DNS untuk rentang alamat IP non-RFC 1918	Server DNS Amazon sekarang dapat mengubah nama host DNS pribadi ke alamat IP pribadi untuk semua ruang alamat.	24 Oktober 2016
Gerbang NAT	Anda dapat membuat gateway NAT di subnet publik dan mengaktifkan instans di subnet pribadi untuk memulai lalu lintas outbound ke internet atau layanan AWS lainnya.	17 Desember 2015
Log aliran VPC	Anda dapat membuat log alur untuk menangkap informasi tentang lalu lintas IP ke dan dari antarmuka jaringan di VPC Anda.	10 Juni 2015

ClassicLink	Anda dapat menggunakannya ClassicLink untuk menautkan EC2-Classic instance Anda ke VPC di akun Anda. Anda dapat mengaitkan grup keamanan VPC dengan EC2-Classic instans, mengaktif kan komunikasi antara EC2-Classic instans dan instans di VPC menggunakan alamat IP pribadi.	7 Januari 2015
Gunakan zona pribadi yang dihosting	Anda dapat mengakses sumber daya di VPC Anda menggunakan nama domain DNS kustom yang Anda tetapkan di zona host pribadi di Route 53.	5 November 2014
Ubah atribut pengalamatan IP publik subnet	Anda dapat mengubah atribut penetapan alamat IP publik dari subnet Anda untuk mengetahui apakah instans yang diluncurkan ke subnet tersebut harus menerima alamat IP publik atau tidak.	21 Juni 2014
Menetapkan alamat IP publik	Anda dapat menetapkan alamat IP publik ke sebuah instans selama peluncuran.	20 Agustus 2013
Mengaktifkan nama host DNS dan menonaktifkan resolusi DNS	Anda dapat memodifikasi VPC default dan menonaktifkan resolusi DNS dan mengaktif kan nama host DNS.	11 Maret 2013

VPC Dimana-mana	Menambahkan dukungan untuk VPC di lima Wil AWS ayah, VPC di beberapa Zona Ketersediaan, beberapa VPC per AWS akun, dan beberapa koneksi VPN per VPC.	3 Agustus 2011
Instans Khusus	Instans Khusus adalah instans Amazon EC2 yang diluncurk an dalam VPC Anda yang menjalankan perangkat keras yang didedikasikan untuk satu pelanggan.	27 Maret 2011

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.