



Panduan Pengguna

Amazon Virtual Private Cloud



Amazon Virtual Private Cloud: Panduan Pengguna

Copyright © 2025 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 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
VPCs dan subnet	7
Default dan nondefault VPCs	7
Tabel rute	8
Mengakses internet	8
Mengakses jaringan perusahaan atau rumah	9
Connect VPCs dan jaringan	9
AWS jaringan global pribadi	10
Rencanakan VPC Anda	11
Mendaftar untuk Akun AWS	11
Memverifikasi izin	12
Tentukan rentang alamat IP Anda	12
Pilih Availability Zone	12
Rencanakan konektivitas internet Anda	13
Buat VPC Anda	13
Men-deploy aplikasi Anda	14
Penentuan alamat IP	15
IPv4 Alamat pribadi	16
IPv4 Alamat publik	16
IPv6 alamat	18
IPv6 Alamat publik	19
IPv6 Alamat pribadi	19
Gunakan Alamat IP Anda sendiri	21
Gunakan Manajer Alamat IP VPC Amazon	21
Blok VPC CIDR	22
IPv4 Blok VPC CIDR	22
Kelola blok IPv4 CIDR untuk VPC	23
IPv4 Pembatasan asosiasi blok CIDR	26
IPv6 Blok VPC CIDR	28

Blok CIDR subnet	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
Daftar prefiks yang dikelola konsumen	36
Daftar prefiks yang dikelola AWS	46
Optimalkan manajemen AWS infrastruktur dengan daftar awalan	48
AWS Rentang alamat IP	50
Unduh	51
Kontrol jalan keluar	52
Umpan geolokasi	52
Temukan rentang alamat	52
Sintaksis	59
Berlangganan notifikasi	64
IPv6 dukungan untuk VPC Anda	66
Tambahkan IPv6 dukungan untuk VPC Anda	67
Contoh VPC dual-stack	72
IPv6 dukungan pada AWS	73
Layanan yang mendukung IPv6	74
IPv6 Dukungan tambahan	82
Pelajari selengkapnya	82
Virtual private cloud	83
Dasar-dasar VPC	84
Rentang alamat IP VPC	84
Diagram VPC	84
Sumber daya VPC	85
Opsi konfigurasi VPC	86
Default VPCs	88
Komponen VPC default	88
Subnet default	91
Bekerja dengan VPC default dan subnet default	91
Buat VPC	96
Buat VPC plus sumber daya VPC lainnya	96

Buat VPC saja	98
Buat VPC menggunakan AWS CLI	100
Visualisasikan sumber daya di VPC Anda	105
Tambah atau hapus blok CIDR	106
Set opsi DHCP	109
Apa itu DHCP?	109
Konsep set opsi DHCP	110
Bekerja dengan set opsi DHCP	114
Atribut DNS	118
Memahami DNS Amazon	119
Lihat nama host DNS untuk instans Anda EC2	124
Melihat dan memperbarui atribut DNS untuk VPC Anda	125
Penggunaan Alamat Jaringan	126
Bagaimana NAU dihitung	127
Contoh NAU	128
Bagikan subnet VPC	129
Prasyarat subnet bersama	130
Bekerja dengan subnet bersama	130
Penagihan dan pengukuran untuk pemilik dan peserta	133
Tanggung jawab dan izin untuk pemilik dan peserta	133
AWS sumber daya dan subnet VPC bersama	136
Memperluas VPC ke Zona lain	138
Subnet di AWS Local Zones	138
Subnet di AWS Wavelength	144
Subnet di AWS Outposts	147
Hapus VPC Anda	148
Hapus menggunakan konsol	149
Hapus menggunakan CLI	150
Hasilkan IAc dari tindakan konsol	151
Subnet	153
Dasar-dasar subnet	153
Rentang alamat IP subnet	153
Jenis subnet	154
Diagram subnet	155
Perutean subnet	155
Pengaturan subnet	155

Keamanan subnet	156
Membuat subnet	157
Menambahkan atau menghapus blok IPv6 CIDR dari subnet Anda	159
Ubah atribut pengalamatan IP subnet Anda	159
Reservasi CIDR subnet	161
Bekerja dengan reservasi CIDR subnet menggunakan konsol	162
Bekerja dengan reservasi CIDR subnet menggunakan AWS CLI	162
Tabel rute	163
Konsep tabel rute	164
Tabel rute subnet	166
Tabel rute gateway	173
Prioritas rute	176
Opsi perutean contoh	178
Buat tabel rute dan rute	193
Mengelola tabel rute subnet	196
Ganti tabel rute utama	199
Kaitkan tabel rute dengan gateway	200
Mengganti atau memulihkan target untuk rute lokal	201
Perutean dinamis di VPC Anda	202
Memecahkan masalah keterjangkauan	232
Wisaya perutean Middlebox	232
Prasyarat wizard perutean Middlebox	233
Arahkan lalu lintas VPC ke alat keamanan	233
Pertimbangan wizard perutean Middlebox	236
Skenario Middlebox	236
Hapus subnet	246
Hubungkan VPC Anda	248
Gateway internet	249
Dasar-dasar gateway internet	250
Membuat gateway internet baru	253
Menghapus gateway internet	255
Gateway internet khusus egress	256
Dasar-dasar gateway internet egress-only	257
Tambahkan akses internet khusus egres ke subnet	258
Perangkat NAT	261
Gateway NAT	262

Instans NAT	310
Bandingkan perangkat NAT	322
Alamat IP elastis	325
Konsep dan aturan alamat IP Elastis	326
Mulai gunakan alamat IP Elastis	328
AWS Transit Gateway	337
AWS Virtual Private Network	338
Koneksi peering VPC	340
Pemantauan	342
Log Alur VPC	343
Dasar-dasar log alur	344
Catatan log alur	347
Contoh catatan log alur	358
Batasan log alur	367
Harga	370
Bekerja dengan log alur	370
Publikasikan ke CloudWatch Log	373
Terbitkan ke Amazon S3	382
Publikasikan ke Amazon Data Firehose	390
Kueri menggunakan Athena	398
Pemecahan Masalah	402
CloudWatch metrik	407
Metrik dan dimensi NAU	407
Mengaktifkan atau menonaktifkan pemantauan NAU	410
Contoh CloudWatch alarm NAU	411
Laporan penagihan dan penggunaan	412
Manajemen alamat IP	412
Titik akhir VPC	413
Transit gateway	414
Analisis jaringan	414
Mirroring lalu lintas	415
Kisi VPC	415
Sumber daya lintas akun/wilayah	416
Keamanan	417
Perlindungan data	418
Privasi lalu lintas antarjaringan	419

Manajemen identitas dan akses	419
Audiens	420
Mengautentikasi menggunakan identitas	420
Mengelola akses menggunakan kebijakan	424
Bagaimana cara Amazon VPC bekerja sama dengan IAM	426
Contoh kebijakan	431
Pemecahan Masalah	444
AWS kebijakan terkelola	446
Keamanan infrastruktur	449
Isolasi jaringan	450
Mengendalikan lalu lintas jaringan	450
Bandingkan grup keamanan dan jaringan ACLs	451
Grup keamanan	453
Dasar-dasar grup keamanan	455
Contoh grup keamanan	456
Aturan-aturan grup keamanan	457
Grup keamanan default	462
Membuat grup keamanan	464
Mengonfigurasi aturan grup keamanan	466
Menghapus grup keamanan	468
Mengaitkan grup keamanan dengan beberapa VPCs	469
Bagikan grup keamanan dengan AWS Organizations	472
Jaringan ACLs	478
Dasar-dasar ACL jaringan	479
Aturan ACL Jaringan	481
ACL jaringan default	482
Jaringan kustom ACLs	484
Path MTU Discovery	489
Buat ACL jaringan	490
Kelola asosiasi ACL jaringan	494
Menghapus ACL jaringan	497
Contoh: Kontrol akses ke instans dalam subnet	498
Ketahanan	501
Validasi kepatuhan	503
Memblokir akses publik ke VPCs dan subnet	504
Dasar-dasar VPC BPA	505

Menilai dampak VPC BPA dan memantau VPC BPA	511
Contoh lanjutan	516
Praktik terbaik	570
Gunakan dengan layanan lain	572
AWS PrivateLink	573
AWS Network Firewall	574
Route 53 Resolver DNS Firewall	576
Reachability Analyzer	577
Contoh	578
Lingkungan uji	579
Gambaran Umum	579
1. Buat VPC	581
2. Men-deploy aplikasi Anda	582
3. Uji konfigurasi Anda	583
4. Bersihkan	583
Server web dan basis data	583
Gambaran Umum	584
1. Buat VPC	588
2. Men-deploy aplikasi Anda	589
3. Uji konfigurasi Anda	589
4. Bersihkan	590
Server pribadi	590
Gambaran Umum	590
1. Buat VPC	593
2. Men-deploy aplikasi Anda	594
3. Uji konfigurasi Anda	594
4. Bersihkan	595
Tutorial	596
Memulai dengan Amazon VPC menggunakan AWS CLI	596
.....	596
Prasyarat	597
Buat VPC	597
Buat subnet	598
Konfigurasi konektivitas internet	600
Buat Gateway NAT	601
Konfigurasi pengaturan subnet	602

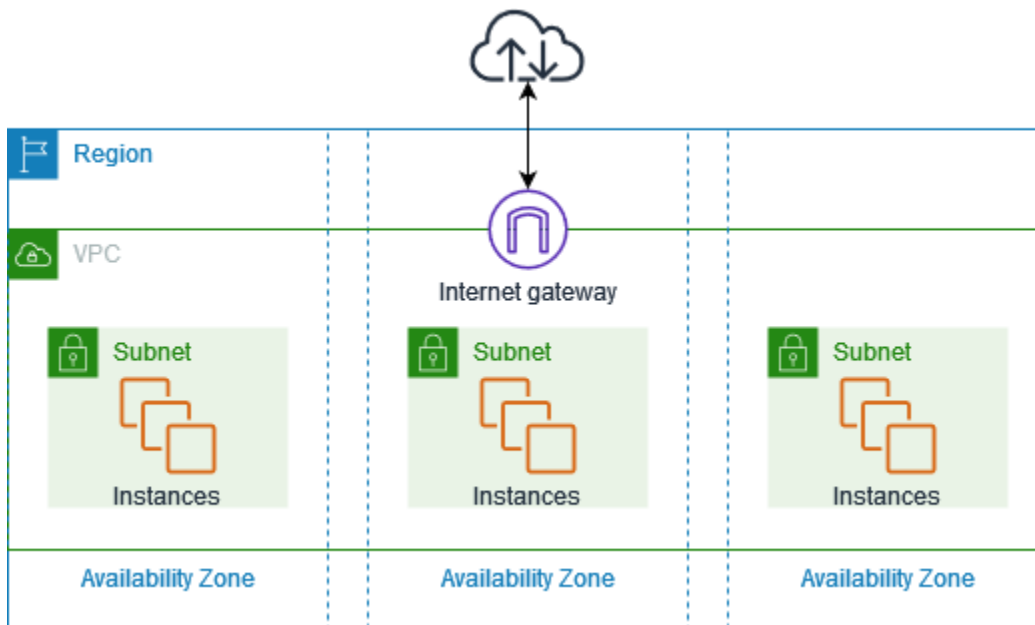
Buat grup keamanan	603
Verifikasi konfigurasi VPC	604
Menyebarkan contoh EC2	605
Pemecahan Masalah	607
Pembersihan sumber daya	608
Pergi ke produksi	609
Langkah selanjutnya	610
Buat VPC dengan subnet pribadi dan gateway NAT menggunakan AWS CLI	610
Prasyarat	597
Buat VPC dan subnet	612
Buat dan konfigurasi konektivitas internet	614
Buat gateway NAT	616
Buat titik akhir VPC untuk Amazon S3	617
Konfigurasi grup keamanan	618
Buat template peluncuran untuk EC2 instance	619
Buat penyeimbang beban dan grup target	621
Membuat grup Auto Scaling	622
Uji konfigurasi Anda	623
Pembersihan sumber daya	608
Langkah selanjutnya	610
Kuota	626
VPC dan subnet	626
DNS	627
Alamat IP elastis	627
Gerbang	627
Daftar prefiks yang dikelola konsumen	628
Jaringan ACLs	630
Antarmuka jaringan	630
Tabel rute	631
Server rute	632
Grup keamanan	634
Berbagi subnet VPC	635
Penggunaan Alamat Jaringan	635
EC2 Pelambatan API Amazon	636
Sumber daya kuota tambahan	636
Riwayat dokumen	638

..... dcxlix

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 tradisional 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 AWS 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 \(AWS VPN\)](#).

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 [Rencanakan 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:

- AWS Management Console— 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, pencermiran 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.

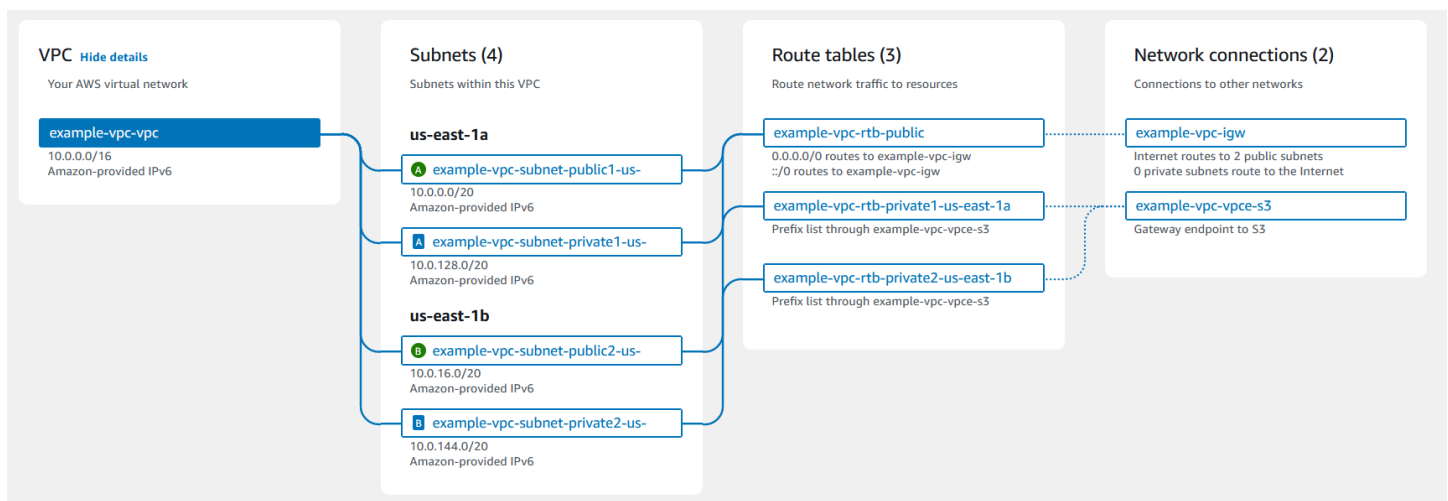
- Amazon AppStream 2.0
- [AWS Client VPN](#)

- 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 di jaringan virtual yang terisolasi secara logis yang telah Anda tentukan. Jaringan virtual ini sangat mirip dengan jaringan tradisional 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 Pratinjau yang ditampilkan saat Anda membuat VPC menggunakan AWS Management Console Untuk VPC yang ada, Anda dapat mengakses visualisasi ini di tab Peta [sumber](#) daya. Contoh ini menunjukkan sumber daya yang awalnya dipilih pada halaman Buat VPC saat Anda memilih untuk membuat VPC plus sumber daya jaringan lainnya. VPC ini dikonfigurasi dengan IPv4 CIDR dan CIDR yang disediakan Amazon IPv6, subnet dalam dua Availability Zones, tiga tabel rute, gateway internet, dan titik akhir gateway. Karena kami telah memilih gateway internet, visualisasi menunjukkan bahwa lalu lintas dari subnet publik dirutekan ke internet karena tabel rute yang sesuai mengirimkan lalu lintas ke gateway internet.



Konsep

- [VPCs dan subnet](#)
- [Default dan nondefault VPCs](#)
- [Tabel rute](#)
- [Mengakses internet](#)
- [Mengakses jaringan perusahaan atau rumah](#)
- [Connect VPCs dan jaringan](#)

- [AWS jaringan global pribadi](#)

VPCs dan subnet

Virtual private cloud (VPC) adalah jaringan 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 EC2 instans Amazon, ke subnet Anda. Anda dapat menghubungkan subnet ke internet, lainnya VPCs, dan pusat data Anda sendiri, dan mengarahkan lalu lintas ke dan dari subnet Anda menggunakan tabel rute.

Pelajari selengkapnya

- [Penentuan alamat IP](#)
- [Virtual private cloud](#)
- [Subnet](#)

Default dan nondefault VPCs

Jika akun Anda dibuat setelah 4 Desember 2013, ia dilengkapi dengan VPC default di setiap Wilayah. VPC default dikonfigurasi dan siap untuk Anda gunakan. Misalnya, ia memiliki subnet default di setiap Availability Zone di Region, 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 instance dengan alamat IP publik dan mengaktifkan resolusi DNS melalui server DNS yang disediakan Amazon (lihat). [Atribut DNS untuk VPC Anda](#) Oleh karena itu, EC2 instance 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 EC2 instance ke Wilayah itu, 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 “Default VPCs”](#)

- [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

- [Konfigurasi 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 instance yang Anda luncurkan ke subnet default memiliki IPv4 alamat pribadi dan IPv4 alamat publik. Instans ini dapat berkomunikasi dengan internet melalui gateway internet. Gateway internet memungkinkan instans Anda terhubung ke internet melalui tepi EC2 jaringan Amazon.

Secara default, setiap instance yang Anda luncurkan ke subnet nondefault memiliki IPv4 alamat pribadi, tetapi tidak ada IPv4 alamat publik, kecuali jika Anda secara khusus menetapkan satu saat peluncuran, atau Anda memodifikasi 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 IPv4 alamat pribadi ke satu IPv4 alamat publik. 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 IPv6 CIDR dengan VPC Anda dan IPv6 menetapkan alamat ke instans Anda, instans dapat terhubung ke internet melalui gateway internet IPv6 . Atau, instance dapat memulai koneksi keluar ke internet melalui IPv6 menggunakan gateway internet khusus egress. IPv6 lalu lintas terpisah dari IPv4 lalu lintas; tabel rute Anda harus menyertakan rute terpisah untuk IPv6 lalu lintas.

Pelajari selengkapnya

- [Aktifkan akses internet untuk VPC menggunakan gateway internet](#)
- [Aktifkan IPv6 lalu lintas keluar menggunakan gateway internet khusus egress-only](#)
- [Connect 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 IPsec AWS Site-to-Site VPN koneksi, menjadikan AWS Cloud sebagai perpanjangan 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 konfigurasi di sisi koneksi Site-to-Site VPN Anda.

Pelajari selengkapnya

- [AWS Site-to-Site VPN Panduan Pengguna](#)
- [Gerbang Transit VPC Amazon](#)

Connect VPCs dan jaringan

Anda dapat membuat koneksi peering VPC antara dua VPCs yang memungkinkan Anda untuk merutekan lalu lintas di antara mereka secara pribadi. Instans di kedua VPC tersebut dapat berkomunikasi satu sama lain seolah berada di jaringan yang sama.

Anda juga dapat membuat gateway transit dan menggunakannya untuk menghubungkan jaringan Anda VPCs dan lokal. Gateway transit bertindak sebagai router virtual Regional untuk lalu lintas yang mengalir di antara lampirannya, yang dapat mencakup VPCs, koneksi VPN, AWS Direct Connect gateway, dan koneksi peering gateway transit.

Pelajari selengkapnya

- [Panduan Peering VPC Amazon](#)
- [Gerbang Transit VPC Amazon](#)

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 (ISPs) serta ke tulang punggung jaringan global pribadi, yang memberikan peningkatan kinerja jaringan untuk lalu lintas lintas wilayah yang dikirim oleh pelanggan.

Paket yang berasal dari jaringan global pribadi dengan tujuan di jaringan global pribadi tetap berada di jaringan global pribadi dan tidak melintasi internet publik. Ini benar apakah tujuan adalah alamat IP pribadi atau alamat IP publik. Misalnya, jika EC2 instance dalam dua VPCs berkomunikasi menggunakan alamat IP publik, lalu lintas tetap berada di jaringan global pribadi. Tujuan dapat berada di Availability Zone yang sama, Availability Zone yang berbeda di Wilayah yang sama, atau Wilayah yang berbeda, kecuali untuk Wilayah Tiongkok.

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 packet-loss (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%.

Rencanakan VPC Anda

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

Tugas

- [Mendaftar untuk Akun AWS](#)
- [Memverifikasi izin](#)
- [Tentukan rentang alamat IP Anda](#)
- [Pilih Availability Zone](#)
- [Rencanakan konektivitas internet Anda](#)
- [Buat VPC Anda](#)
- [Men-deploy aplikasi Anda](#)

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka <https://portal.aws.amazon.com/billing/pendaftaran>.
2. Ikuti petunjuk online.

Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon atau pesan teks dan memasukkan kode verifikasi pada keypad telepon.

Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWS dibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan [tugas yang memerlukan akses pengguna root](#).

AWS mengirim Anda email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk <https://aws.amazon.com/ke/> dan memilih Akun Saya.

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 VPCs dan subnet, Anda dapat memilih rentang alamat IP mereka. Saat Anda menyebarkan sumber daya di subnet, seperti EC2 instance, mereka 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 alamat IP Anda Akun AWS dan VPCs. Pastikan bahwa rentang alamat IP untuk VPCs Anda tidak tumpang tindih dengan rentang alamat IP untuk jaringan Anda sendiri. Jika Anda memerlukan konektivitas antara beberapa VPCs, 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 Availability Zone

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

Lingkungan produksi

Untuk lingkungan produksi, kami menyarankan Anda memilih setidaknya dua Availability Zone dan menyebarkan AWS sumber daya Anda secara merata di setiap Availability Zone yang aktif.

Lingkungan pengembangan atau pengujian

Untuk lingkungan pengembangan atau pengujian, Anda dapat memilih untuk menghemat uang dengan menerapkan sumber daya Anda hanya dalam satu Availability Zone.

Rencanakan konektivitas internet Anda

Rencanakan untuk membagi setiap VPC menjadi subnet berdasarkan kebutuhan konektivitas Anda. Misalnya:

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

Jika aplikasi Anda akan menerima lalu lintas dari internet, VPC harus memiliki gateway internet. Melampirkan gateway internet ke VPC tidak secara otomatis membuat instance 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 instans 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 ke seluruh instans terdaftar di satu atau beberapa Availability Zone. Untuk informasi selengkapnya, lihat [Elastic Load Balancing](#). Untuk mengizinkan instance di subnet pribadi mengakses internet (misalnya, untuk mengunduh pembaruan) tanpa mengizinkan koneksi masuk yang tidak diminta dari internet, tambahkan gateway NAT publik di setiap Availability Zone 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 VPCs dan subnet yang Anda butuhkan, blok CIDR apa yang akan ditetapkan untuk Anda VPCs dan subnet, dan bagaimana menghubungkan VPC Anda ke internet, Anda siap untuk membuat VPC Anda. Jika Anda membuat VPC Anda menggunakan AWS

Management Console 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 Anda membuat VPC, Anda dapat menerapkan aplikasi Anda.

Lingkungan produksi

Untuk lingkungan produksi, Anda dapat menggunakan salah satu layanan berikut untuk menyebarkan server di beberapa Availability Zone, 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.

- [EC2 Auto Scaling Amazon](#)
- [EC2 Armada](#)
- [Amazon Elastic Container Service \(Amazon ECS\)](#)

Lingkungan pengembangan atau pengujian

Untuk lingkungan pengembangan atau pengujian, Anda dapat memilih untuk meluncurkan satu EC2 instance. Untuk informasi selengkapnya, lihat [Memulai Amazon EC2](#) di Panduan EC2 Pengguna Amazon.

Alamat IP untuk Anda VPCs dan subnet

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 mask jaringannya. Format alamat ini adalah sebagai berikut:

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

Untuk informasi lebih lanjut, lihat [Apa itu CIDR?](#)

Daftar Isi

- [IPv4 Alamat pribadi](#)
- [IPv4 Alamat publik](#)
- [IPv6 alamat](#)
- [Gunakan Alamat IP Anda sendiri](#)
- [Gunakan Manajer Alamat IP VPC Amazon](#)
- [Blok VPC CIDR](#)
- [Blok CIDR subnet](#)
- [Bandingkan IPv4 dan IPv6](#)
- [Mengkonsolidasikan dan mengelola blok CIDR jaringan dengan daftar awalan terkelola](#)

- [AWS Rentang alamat IP](#)
- [IPv6 dukungan untuk VPC Anda](#)
- [AWS layanan yang mendukung IPv6](#)

IPv4 Alamat pribadi

IPv4 Alamat pribadi (juga disebut sebagai alamat IP pribadi dalam topik ini) tidak dapat dijangkau melalui internet, dan dapat digunakan untuk komunikasi antara instance di VPC Anda. Saat Anda meluncurkan instance ke VPC, alamat IP pribadi utama dari rentang IPv4 alamat subnet ditetapkan ke antarmuka jaringan utama (misalnya, eth0) dari instance. 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 berbasis IP. Untuk informasi lebih lanjut, lihat [penamaan EC2 contoh](#). 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 EC2 Panduan Pengguna Amazon.

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 EC2 Pengguna Amazon.

Kami menyebut alamat IP pribadi sebagai alamat IP yang berada dalam kisaran IPv4 CIDR dari 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 AWS Direct Connect.

Kami tidak pernah mengiklankan rentang IPv4 alamat subnet ke internet.

IPv4 Alamat publik

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

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

 Note

AWS mengenakan biaya untuk semua IPv4 alamat publik, termasuk IPv4 alamat publik yang terkait dengan instans yang sedang berjalan dan alamat IP Elastis. Untuk informasi selengkapnya, lihat tab IPv4 Alamat 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 instans Anda setelah peluncuran dengan mengelola alamat IP yang terkait dengan antarmuka jaringan. Untuk informasi selengkapnya, lihat [Mengelola alamat IP](#) di Panduan EC2 Pengguna Amazon.

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 menetapkan yang baru. Untuk informasi selengkapnya, lihat [Alamat IP Publik](#) di Panduan EC2 Pengguna Amazon.

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 [Kaitkan alamat IP Elastis 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 publik yang berdekatan AWS dan menggunakannya untuk mengalokasikan IPv4 alamat IP Elastis berurutan ke sumber daya. AWS Menggunakan blok IPv4 alamat yang berdekatan dapat secara signifikan mengurangi overhead manajemen untuk daftar kontrol akses keamanan dan menyederhanakan alokasi dan pelacakan alamat IP untuk skala perusahaan. AWS Untuk informasi selengkapnya, lihat [Mengalokasikan alamat IP Elastis berurutan dari kumpulan IPAM di Panduan Pengguna Amazon VPC IPAM](#).

IPv6 alamat

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. IPv6 menyelesaikan masalah kelelahan IPv4 alamat dan memungkinkan Anda untuk menghubungkan lebih banyak perangkat ke internet. Transisi ini bertahap, tetapi seiring berkembangnya IPv6 adopsi, Anda dapat menyederhanakan jaringan Anda dan memanfaatkan kemampuan IPv6 canggih untuk konektivitas, kinerja, dan keamanan yang lebih baik.

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

Untuk informasi selengkapnya tentang layanan yang mendukung IPv6, lihat [AWS layanan yang mendukung IPv6](#).

Perhatikan bahwa beberapa IPv6 alamat disediakan oleh Internet Engineering Task Force. Untuk informasi selengkapnya tentang rentang IPv6 alamat yang dipesan, lihat [Registri Alamat IPv6 Tujuan Khusus IANA](#) dan [RFC4291](#)

Note

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

Daftar Isi

- [IPv6 Alamat publik](#)
- [IPv6 Alamat pribadi](#)

IPv6 Alamat publik

IPv6 Alamat yang disediakan Amazon selalu diiklankan di internet. Mereka unik secara global, dan karenanya dapat dijangkau melalui internet. Anda dapat mengontrol apakah sumber daya seperti EC2 instance dapat dijangkau menggunakan IPv6 alamatnya dengan mengontrol perutean untuk subnet Anda, atau dengan menggunakan grup keamanan dan jaringan. ACLs

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

- Buat IPAM dengan Amazon VPC IP Address Manager dan berikan rentang alamat IPv6 publik milik Amazon ke kumpulan alamat IPAM. Untuk informasi selengkapnya, lihat [Membuat IPv6 kumpulan](#) di Panduan Pengguna Amazon VPC IPAM.
- Jika Anda memiliki IPAM dan Anda memiliki jangkauan IPv6 alamat publik, bawalah beberapa atau semua rentang IPv6 alamat publik ke IPAM dan berikan rentang IPv6 alamat publik ke kumpulan alamat IPAM. Untuk informasi selengkapnya, lihat [Tutorial: Membawa alamat IP Anda ke IPAM](#) di Panduan Pengguna Amazon VPC IPAM.
- Jika Anda tidak memiliki IPAM tetapi Anda memiliki rentang IPv6 alamat publik, bawalah beberapa atau semua rentang IPv6 alamat publik ke AWS. Untuk informasi selengkapnya, lihat [Membawa alamat IP Anda sendiri \(BYOIP\) ke Amazon EC2](#) di EC2 Panduan Pengguna Amazon.

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

IPv6 Alamat pribadi

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

Anda dapat menggunakan IPv6 alamat pribadi jika Anda ingin jaringan pribadi Anda mendukung IPv6 dan Anda tidak berniat merutekan lalu lintas dari alamat ini ke Internet. Jika Anda ingin terhubung ke

internet dari sumber daya yang memiliki IPv6 alamat pribadi, Anda bisa, tetapi Anda harus merutekan lalu lintas melalui sumber daya di subnet lain dengan IPv6 alamat publik untuk melakukannya.

Ada dua jenis IPv6 alamat pribadi:

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

Perhatikan hal berikut:

- IPv6 Alamat pribadi hanya tersedia melalui [Amazon VPC IP Address Manager \(IPAM\)](#). IPAM menemukan sumber daya dengan alamat IPv6 ULA dan GUA dan memantau kumpulan untuk ruang alamat IPv6 ULA dan GUA yang tumpang tindih.
- Saat Anda menggunakan rentang IPv6 GUA pribadi, kami mengharuskan Anda menggunakan rentang IPv6 GUA yang dimiliki oleh Anda.
- IPv6 Alamat pribadi tidak dan tidak dapat diiklankan di internet oleh AWS. AWS tidak mengizinkan jalan keluar langsung ke internet publik dari IPv6 jangkauan pribadi bahkan jika ada gateway internet atau jalan keluar hanya gateway internet di VPC. IPv6Alamat pribadi secara otomatis dijatuhkan di tepi gateway internet memastikan bahwa mereka tidak dirutekan secara publik.
- AWS menyimpan 4 IPv6 alamat pribadi subnet pertama dan yang terakhir.
- Rentang yang valid untuk IPv6 ULA pribadi adalah /9 hingga /60 dimulai dengan fd80: :/9.
- Jika Anda memiliki jangkauan IPv6 GUA 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 rentang alamat IPv6 ULA dan GUA pribadi didukung (seperti di seluruh Direct Connect, peering VPC, gateway transit, atau koneksi VPN).
- [Anda dapat menggunakan IPv6 alamat pribadi dengan subnet VPC IPv6 -only dan dual-stack, penyeimbang beban elastis, dan titik akhir.AWS Global Accelerator](#)
- Tidak ada biaya untuk IPv6 alamat pribadi.

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

- Buat IPAM dengan Amazon VPC IP Address Manager dan berikan rentang ULA IPv6 pribadi ke kumpulan alamat IPAM. Untuk informasi selengkapnya, lihat [Membuat IPv6 kumpulan](#) di Panduan Pengguna Amazon VPC IPAM.
- Buat IPAM dengan Amazon VPC IP Address Manager dan sediakan rentang GUA IPv6 pribadi ke kumpulan alamat IPAM. Opsi untuk menggunakan rentang IPv6 GUA sebagai IPv6 alamat pribadi dinonaktifkan secara default dan harus diaktifkan pada IPAM Anda sebelum Anda dapat menggunakannya. Untuk informasi selengkapnya, lihat [Mengaktifkan penyediaan IPv6 GUA pribadi CIDRs](#) di Panduan Pengguna Amazon VPC IPAM.

Ketika Anda siap untuk menggunakan IPv6 alamat pribadi, Anda dapat mengalokasikan blok IPv6 CIDR pribadi dari kolam IPAM ke VPC Anda (lihat [Tambahkan 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 IPv4 alamat publik atau rentang IPv6 alamat Anda sendiri ke AWS akun Anda. 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 IPv4 alamat Anda, dan Anda dapat mengaitkan blok IPv6 CIDR dari kumpulan IPv6 alamat Anda dengan VPC.

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

Gunakan Manajer Alamat IP VPC Amazon

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 alamat IP CIDRs untuk VPCs menggunakan aturan bisnis tertentu.

Untuk informasi lebih lanjut, lihat [Apa itu IPAM?](#) di Panduan Pengguna Amazon VPC IPAM.

Blok VPC CIDR

Alamat IP untuk virtual private cloud (VPC) Anda direpresentasikan 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 [Alamat IP untuk Anda VPCs dan subnet](#).

Daftar Isi

- [IPv4 Blok VPC CIDR](#)
- [Kelola blok IPv4 CIDR untuk VPC](#)
- [IPv4 Pembatasan asosiasi blok CIDR](#)
- [IPv6 Blok VPC CIDR](#)

IPv4 Blok VPC CIDR

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

[Saat Anda membuat VPC, kami sarankan Anda menentukan blok CIDR dari rentang IPv4 alamat pribadi seperti yang ditentukan dalam RFC 1918.](#)

Rentang RFC 1918	Contoh Blok CIDR
10.0.0.0 - 10.255.255.255 (prefiks 10/8)	10.0.0.0/16
172.16.0.0 - 172.31.255.255 (prefiks 172.16/12)	172.31.0.0/16
192.168.0.0 - 192.168.255.255 (prefiks 192.168/16)	192.168.0.0/20

Important

Beberapa AWS layanan menggunakan rentang 172.17.0.0/16 CIDR. Layanan dapat mengalami konflik alamat IP jika rentang alamat IP sudah digunakan di mana saja di jaringan

Anda. Misalnya, AWS Cloud9 dan penggunaan Amazon SageMaker AI 172.17.0.0/16. Untuk menghindari konflik, jangan gunakan rentang ini saat membuat VPC Anda. Untuk informasi selengkapnya, lihat [Tidak dapat terhubung ke EC2 lingkungan karena alamat IP VPC digunakan oleh Docker](#) di AWS Cloud9 Panduan Pengguna.

Anda dapat membuat VPC dengan blok CIDR yang dapat dirutekan secara publik yang berada di luar rentang IPv4 alamat pribadi yang ditentukan dalam RFC 1918. Namun, untuk keperluan dokumentasi ini, kami menyebut alamat IP pribadi sebagai IPv4 alamat yang berada dalam kisaran CIDR VPC Anda.

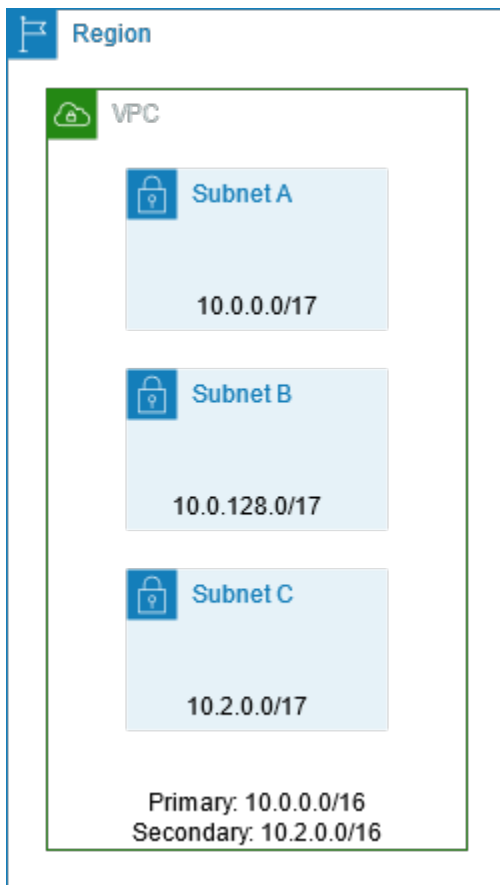
Saat Anda membuat VPC untuk digunakan dengan AWS layanan, periksa dokumentasi layanan untuk memverifikasi apakah ada persyaratan khusus untuk konfigurasinya.

Jika Anda membuat VPC 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.

Kelola blok IPv4 CIDR untuk VPC

Anda dapat mengaitkan blok IPv4 CIDR 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 CIDR VPC utama. Blok CIDR untuk Subnet C berasal dari blok CIDR VPC 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 batasan pada rentang IPv4 alamat yang dapat Anda gunakan. Untuk informasi selengkapnya, lihat [IPv4 Pembatasan asosiasi blok CIDR](#).
- 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 IPv4 CIDR 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 penerima 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 AWS Direct Connect untuk menyambung ke beberapa VPCs melalui gateway Direct Connect, gateway VPCs yang terkait dengan gateway Direct Connect tidak boleh memiliki blok CIDR yang tumpang tindih. Jika Anda menambahkan blok CIDR ke salah satu VPCs yang terkait dengan gateway Direct Connect, pastikan bahwa blok CIDR baru tidak tumpang tindih dengan blok CIDR yang ada dari VPC terkait lainnya. Untuk informasi selengkapnya, lihat [Gateway Direct Connect](#) di Panduan Pengguna AWS 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 VPC Amazon, pilih Your, pilih kotak centang untuk VPC VPCs Anda, dan pilih tab. CIDRs Untuk melihat CIDR utama menggunakan AWS CLI, gunakan [perintah deskripsi-vpcs](#) sebagai berikut. CIDR utama dikembalikan di tingkat `atasCidrBlock` element.

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

Berikut ini adalah output contoh.

```
10.0.0.0/16
```

IPv4 Pembatasan asosiasi blok CIDR

Tabel berikut memberikan gambaran umum tentang asosiasi blok CIDR VPC yang diizinkan dan dibatasi. Alasan pembatasan adalah bahwa beberapa AWS layanan menggunakan fitur cross-VPC dan cross-account yang memerlukan blok CIDR yang tidak bertentangan di sisi layanan. AWS

Rentang alamat IP	Asosiasi terbatas	Asosiasi yang diizinkan
10.0.0.0/8	Blok CIDR dari RFC 1918 lainnya rentang* (172.16.0.0/12 dan 192.168.0.0/16). Jika salah satu blok CIDR yang terkait dengan VPC berasal dari kisaran 10.0.0.0/15 (10.0.0.0 hingga 10.1.255.255), Anda tidak dapat menambahkan blok CIDR dari kisaran 10.0.0.0/16 (10.0.0.0 hingga 10.0.255.255). CIDR memblokir dari kisaran 198.19.0.0/16.	Blok CIDR lainnya dari rentang 10.0.0.0/8 antara netmask /16 dan /28 netmask yang tidak dibatasi. Setiap blok IPv4 CIDR yang dapat dirutekan secara publik (non-RFC 1918) antara netmask /16 dan /28 netmask atau blok CIDR antara /16 netmask dan /28 netmask dari kisaran 100.64.0.0/10.
169.254.0.0/16	Blok CIDR dari blok “tautan lokal” dicadangkan seperti yang dijelaskan	

Rentang alamat IP	Asosiasi terbatas	Asosiasi yang diizinkan
	n dalam RFC 5735 dan tidak dapat ditetapkan. VPCs	
172.16.0.0/12	Blok CIDR dari RFC 1918 lainnya rentang* (10.0.0.0/8 dan 192.168.0.0/16). CIDR memblokir dari kisaran 172.31.0.0/16. CIDR memblokir dari kisaran 198.19.0.0/16.	Blok CIDR lainnya dari rentang 172.16.0.0/12 antara netmask /16 dan /28 netmask yang tidak dibatasi. Setiap blok IPv4 CIDR yang dapat dirutekan secara publik (non-RFC 1918) antara netmask /16 dan /28 netmask atau blok CIDR antara /16 netmask dan /28 netmask dari kisaran 100.64.0.0/10.
192.168.0.0/16	Blok CIDR dari rentang RFC 1918* lainnya (10.0.0.0/8 dan 172.16.0.0/12). CIDR memblokir dari kisaran 198.19.0.0/16.	Blok CIDR lainnya dari rentang 192.168.0.0/16 antara netmask /16 dan /28 netmask. Setiap blok IPv4 CIDR yang dapat dirutekan secara publik (non-RFC 1918) antara netmask /16 dan /28 netmask atau blok CIDR dari rentang 100.64.0.0/10 antara netmask /16 dan /28 netmask.
198.19.0.0/16	Blok CIDR dari RFC 1918 rentang*.	Setiap blok IPv4 CIDR yang dapat dirutekan secara publik (non-RFC 1918) antara netmask /16 dan /28 netmask atau blok CIDR dari rentang 100.64.0.0/10 antara netmask /16 dan /28 netmask.

Rentang alamat IP	Asosiasi terbatas	Asosiasi yang diizinkan
Blok CIDR yang dapat dirutekan secara publik (non-RFC 1918), atau blok CIDR dari kisaran 100.64.0.0/10	Blok CIDR dari RFC 1918 rentang*. CIDR memblokir dari kisaran 198.19.0.0/16.	Blok IPv4 CIDR lain yang dapat dirutekan secara publik (non-RFC 1918) antara netmask /16 dan /28 netmask atau blok CIDR antara /16 netmask dan /28 netmask dari kisaran 100.64.0.0/10. Anda juga dapat mengaitkan CIDR di salah satu rentang RFC 1918, tetapi untuk melakukan ini Anda harus menambahkan CIDR itu terlebih dahulu saat Anda membuat VPC dan kemudian menambahkan CIDR non-RFC 1918.

* Rentang RFC 1918 adalah rentang IPv4 alamat pribadi yang ditentukan dalam [RFC](#) 1918.

IPv6 Blok VPC CIDR

Anda dapat mengaitkan satu blok IPv6 CIDR saat Anda membuat VPC baru atau Anda dapat mengaitkan hingga IPv6 lima blok CIDR /44 dari /60 hingga secara bertahap. /4 Anda dapat meminta blok IPv6 CIDR dari kumpulan IPv6 alamat 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 IPv6 blok 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”](#).

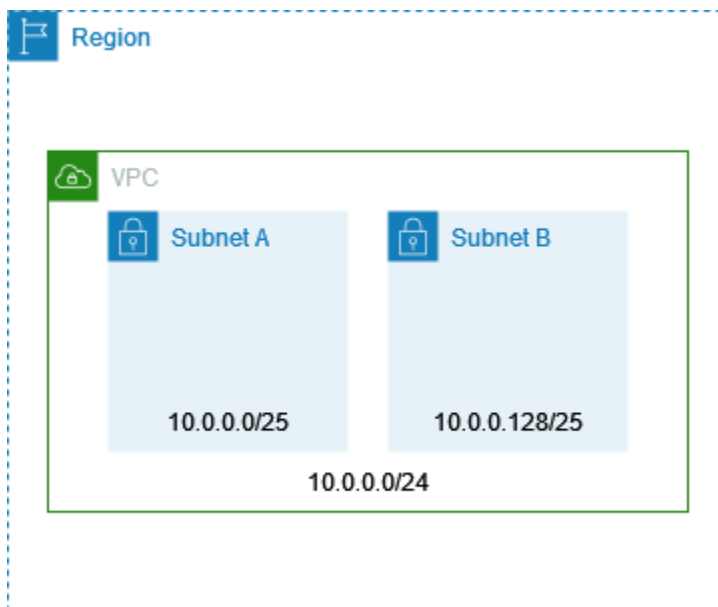
Misalnya, Anda membuat VPC dan menentukan bahwa Anda ingin mengaitkan IPv6 blok CIDR yang disediakan Amazon dengan VPC. Amazon menetapkan blok IPv6 CIDR berikut ke VPC Anda: 2001:db8:1234:1a00::/56 Anda tidak dapat memilih rentang alamat IP tersebut oleh Anda sendiri. Anda dapat membuat subnet dan mengaitkan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

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

Blok CIDR subnet

Alamat IP untuk subnet Anda direpresentasikan menggunakan notasi Classless Inter-Domain Routing (CIDR). Blok CIDR subnet bisa sama dengan blok CIDR untuk VPC (untuk membuat subnet tunggal di VPC), atau subset dari 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 mendukung 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 IPv4 dan IPv6 subnet blok CIDR. 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 IPv4 dan IPv6 CIDR yang akan 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 VPCs 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 oleh untuk penggunaan AWS masa depan.
- 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 IPv4 alamat untuk AWS menggunakan [BYOIP](#), Anda dapat menggunakan semua alamat IP dalam rentang tersebut, termasuk alamat pertama (alamat jaringan) dan alamat terakhir (alamat siaran).

Ukuran subnet untuk IPv6

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

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

Empat IPv6 alamat pertama dan IPv6 alamat terakhir di setiap blok CIDR subnet tidak tersedia untuk Anda gunakan, dan alamat tersebut tidak dapat ditetapkan ke sebuah EC2 instans. 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 untuk router VPC pada contoh di atas, IPv6 alamat berikut dicadangkan untuk router VPC default:

- IPv6 Alamat link-lokal dalam rentang FE80::/10 yang dihasilkan menggunakan EUI-64. Untuk informasi selengkapnya tentang alamat link-local, lihat Alamat [link-local](#).
- Alamat link-lokal IPv6 . FE80::ec2::1

Jika Anda perlu berkomunikasi dengan router VPC 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.
Pemilihan alamat	Anda dapat memilih blok IPv4 CIDR untuk VPC Anda atau Anda dapat	Anda dapat membawa blok IPv6 CIDR Anda sendiri AWS untuk VPC

Karakteristik	IPv4	IPv6
	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, 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 egress.
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 menggunakan 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 satu set dari satu atau lebih blok CIDR. Anda dapat menggunakan daftar prefiks untuk memudahkan pengkonfigurasiannya 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:

- Daftar prefiks yang dikelola konsumen — Serangkaian 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 terkelola - Set 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](#)
- [Daftar prefiks yang dikelola konsumen](#)
- [Daftar prefiks yang dikelola AWS](#)
- [Optimalkan manajemen AWS 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.

Daftar prefiks yang dikelola konsumen

Aturan berikut berlaku untuk daftar prefiks yang dikelola konsumen:

- Daftar awalan mendukung satu jenis pengalamatan IP saja (IPv4 atau IPv6). Anda tidak dapat menggabungkan IPv4 dan IPv6 CIDR blok dalam daftar awalan tunggal.
- 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 mengubah daftar awalan. Saat Anda menambah atau menghapus entri, kami membuat versi baru dari daftar awalan. Sumber daya yang mereferensikan awalan selalu menggunakan versi (terbaru) saat ini. 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 [Daftar prefiks yang dikelola konsumen](#).
- Daftar awalan yang dikelola pelanggan tersedia di semua [AWS Wilayah](#) komersial (termasuk GovCloud (AS) dan Wilayah Tiongkok).

Daftar prefiks yang dikelola AWS

Aturan berikut berlaku untuk daftar awalan AWS-managed:

- Anda tidak dapat membuat, memodifikasi, membagikan, atau menghapus daftar awalan yang AWS dikelola.
- Daftar awalan AWS-managed yang berbeda memiliki bobot yang berbeda saat Anda menggunakannya. Untuk informasi selengkapnya, lihat [AWS berat daftar awalan -terkelola](#).
- Anda tidak dapat melihat nomor versi dari daftar awalan AWS-managed.

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 untuk bekerja dengan daftar awalan.

Untuk melihat daftar tindakan VPC Amazon 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 p1-123456abcde123456. 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:region:account:prefix-list/p1-123456abcde123456"
  },
  {
    "Effect": "Allow",
    "Action": "ec2:DescribeManagedPrefixLists",
    "Resource": "*"
  }
]
```

Untuk informasi selengkapnya tentang bekerja dengan IAM di Amazon VPC, lihat [Identity and access management untuk Amazon VPC](#).

Daftar prefiks yang dikelola konsumen

Daftar awalan yang dikelola pelanggan memungkinkan Anda 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 mempromosikan konsistensi dan penggunaan kembali di seluruh lanskap Anda.

AWS

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 dapat mengaktifkan tim atau organisasi lain untuk memanfaatkan rentang alamat IP yang ditentukan dalam sumber daya mereka sendiri. Pendekatan kolaboratif ini mendorong pengalaman cloud yang lebih kohesif dan efisien, di mana manajemen alamat IP dibagikan dan disinkronkan.

Di bagian berikutnya, kami akan menyelami lebih dalam aspek praktis bekerja dengan daftar awalan yang dikelola pelanggan, termasuk step-by-step panduan untuk membuat, mengelola, dan berbagi rentang alamat IP Anda.

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](#)
- [Ubah 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 VPC Amazon 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 awalan mendukung IPv4 atau IPv6 entri.
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 AWS-terkelola.

Untuk melihat daftar prefiks menggunakan konsol

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>

2. Di panel navigasi, pilih Daftar Prefiks yang Dikelola.
3. Kolom Owner ID menunjukkan ID AWS akun pemilik daftar awalan. Untuk daftar awalan AWS-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, daftar awalan yang dibagikan dengan Anda, dan daftar awalan AWS-terkelola.

Untuk melihat entri untuk daftar prefiks menggunakan konsol ini

1. Buka konsol VPC Amazon 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 IDs dan pemilik sumber daya yang terkait dengan daftar awalan 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 AWS-managed.

Untuk melihat asosiasi daftar prefiks menggunakan konsol ini

1. Buka konsol VPC Amazon 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, lihat [Ubah 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

- Anda tidak dapat mengubah daftar awalan AWS-managed.
- Saat Anda menambah jumlah maksimum entri dalam daftar awalan, ukuran maksimum yang ditingkatkan diterapkan ke 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 VPC Amazon 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. 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.
6. Pilih Simpan daftar prefiks.

Untuk memodifikasi daftar awalan menggunakan AWS CLI

Gunakan perintah [modify-managed-prefix-list](#).

Ubah ukuran daftar awalan

Anda dapat mengubah ukuran daftar awalan dan memodifikasi jumlah maksimum entri untuk daftar awalan hingga 1000. Untuk informasi selengkapnya tentang kuota daftar awalan yang dikelola pelanggan, lihat. [Daftar prefiks yang dikelola konsumen](#)

Untuk mengubah ukuran daftar awalan menggunakan konsol

1. Buka konsol VPC Amazon 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 memuat entri dari versi sebelumnya.

Untuk memulihkan versi sebelumnya dari daftar prefiks menggunakan konsol ini

1. Buka konsol VPC Amazon 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, Pulihkan 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 VPC Amazon 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 membagikan daftar awalan dengan yang berikut:

- AWS Akun tertentu di dalam atau di luar organisasinya di AWS Organizations
- 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 entri, dan mereka dapat mereferensikan daftar awalan dalam sumber daya mereka. AWS

Untuk informasi selengkapnya AWS RAM, lihat [Panduan AWS RAM Pengguna](#). Untuk kuota informasi selengkapnya, lihat [Kuota layanan](#) di AWS RAM Panduan 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 AWS sumber IDs 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 sumber daya mereka. AWS 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

Daftar awalan berbagi dapat sangat berguna untuk organisasi dengan persyaratan jaringan yang kompleks atau mereka yang perlu mengoordinasikan penggunaan alamat IP di beberapa beban AWS 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 membagikan 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 AWS-managed.
- 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 pembagian sumber daya dan membagikan daftar prefiks menggunakan konsol AWS RAM

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 prefiks untuk pembagian sumber daya yang ada menggunakan konsol AWS RAM

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:

- [create-resource-share](#)
- [associate-resource-share](#)
- [update-resource-share](#)

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

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

Lihat [Memperbarui Pembagian Sumber Daya](#) di Panduan Pengguna.AWS RAM

Untuk membatalkan pembagian 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 VPC Amazon 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 merujuk daftar awalan bersama.

Untuk mengidentifikasi referensi ke daftar prefiks bersama menggunakan konsol Amazon VPC

1. Buka konsol VPC Amazon 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. Sumber IDs daya yang mereferensikan daftar awalan tercantum di 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](#).

Daftar prefiks yang dikelola AWS

AWS Daftar awalan terkelola 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 up-to-date dan dengan benar memperhitungkan alamat IP yang digunakan oleh AWS layanan yang Anda andalkan. Ini dapat membantu menyederhanakan tugas jaringan dan mengurangi overhead administratif dari memelihara daftar alamat IP secara manual.

Selain manfaat praktis, menggunakan daftar awalan terkelola juga sejalan 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. Ini bisa sangat penting untuk aplikasi misi kritis atau beban kerja dengan persyaratan kepatuhan yang ketat.

Daftar Isi

- [Daftar awalan AWS-terkelola yang tersedia](#)
- [AWS berat daftar awalan -terkelola](#)
- [Menggunakan daftar awalan AWS-managed](#)

Daftar awalan AWS-terkelola yang tersedia

Layanan berikut menyediakan daftar awalan AWS-managed.

Layanan AWS	Nama daftar awalan	Berat Badan
Amazon CloudFront	com.amazonaws.global.cloudfront.origin-facing	55
Amazon DynamoDB	com.amazonaws. <i>region</i> .dynamodb	1
Amazon EC2 Instans Connect	com.amazonaws. <i>region</i> .ec2-instance-connect	2

Layanan AWS	Nama daftar awalan	Berat Badan
	com.amazonaws. <i>region</i> .ipv6.ec2-instance-connect	2
AWS Ground Station	com.amazonaws.global.groundstation	5
Rute Amazon 53	com.amazonaws. <i>region</i> .ipv6.route53-healthchecks	25
	com.amazonaws. <i>region</i> .route53-healthchecks	25
Amazon S3	com.amazonaws. <i>region</i> .s3	1
Amazon S3 Express Satu Zona	com.amazonaws. <i>region</i> .s3express	6
Kisi VPC Amazon	com.amazonaws. <i>region</i> .vpc-kisi	10
	com.amazonaws. <i>region</i> .ipv6.vpc-kisi	10

Untuk melihat daftar awalan AWS-managed menggunakan konsol

1. Buka konsol VPC Amazon 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 daftar awalan AWS-managed menggunakan AWS CLI

Gunakan perintah [describe-managed-prefix-lists](#) sebagai berikut.

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

AWS berat daftar awalan -terkelola

Bobot daftar awalan yang AWS dikelola mengacu pada jumlah entri yang dibutuhkan dalam sumber daya.

Misalnya, berat daftar awalan CloudFront terkelola Amazon adalah 55. Inilah cara hal ini memengaruhi kuota VPC Amazon 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 dapat menambahkan daftar awalan ke tabel rute.

Menggunakan daftar awalan AWS-managed

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

Seperti daftar awalan yang dikelola pelanggan, Anda dapat menggunakan daftar awalan yang AWS dikelola dengan AWS sumber daya seperti grup keamanan dan tabel rute. Untuk informasi selengkapnya, lihat [Optimalkan manajemen AWS infrastruktur dengan daftar awalan](#).

Optimalkan manajemen AWS 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 VPC Amazon 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 awalan, pilih ID dari daftar awalan.
6. Pilih Simpan aturan.

Untuk mereferensikan daftar awalan dalam aturan grup keamanan menggunakan AWS CLI

Gunakan [authorize-security-group-ingress](#) dan [authorize-security-group-egress](#) perintah. 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 [Konfigurasi tabel rute](#).

Untuk menyebutkan daftar prefiks dalam tabel rute menggunakan konsol ini

1. Buka konsol VPC Amazon 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 stateful yang kompatibel dengan Suricata AWS Network Firewall, Anda dapat mereferensikan daftar awalan dari grup aturan. Untuk informasi selengkapnya, lihat [Mereferensikan daftar awalan Amazon VPC dan Membuat grup aturan stateful](#) di Panduan Pengembang AWS Network Firewall

Kontrol akses jaringan Grafana yang Dikelola Amazon

Anda dapat menentukan satu atau beberapa daftar awalan sebagai aturan masuk untuk permintaan ke ruang kerja Grafana Terkelola Amazon. Untuk informasi selengkapnya tentang kontrol akses jaringan ruang kerja Grafana, termasuk cara mereferensikan daftar awalan, lihat [Mengelola akses jaringan di](#) Panduan Pengguna Grafana Terkelola Amazon.

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 CIDRs yang sering Anda gunakan dalam daftar awalan dan mereferensikan daftar ini sebagai target rute di tabel rute gateway lokal Anda. Untuk informasi selengkapnya, lihat [Mengelola 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

- Kami mempublikasikan rentang alamat IP untuk layanan yang biasa digunakan pelanggan untuk melakukan pemfilteran jalan 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 membawa alamat IP Anda sendiri (BYOIP) tidak termasuk dalam file. `.json` Untuk informasi selengkapnya, lihat [Mengiklankan rentang alamat Anda AWS di Panduan EC2](#) Pengguna Amazon.

Beberapa layanan mempublikasikan rentang alamat mereka menggunakan AWS daftar awalan - managed. Untuk informasi selengkapnya, lihat [the section called “Daftar awalan AWS-terkelola yang tersedia”](#).

Daftar Isi

- [Unduh file JSON](#)
- [Kontrol jalan keluar](#)
- [Umpan geolokasi](#)
- [Temukan rentang alamat IP untuk Layanan AWS](#)
- [Sintaks untuk rentang alamat AWS IP JSON](#)
- [AWS Pemberitahuan rentang alamat IP](#)

Unduh file JSON

Untuk mempertahankan riwayat, simpan versi file JSON yang berurutan 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 ke file JSON, lihat [AWS Pemberitahuan rentang alamat IP](#).

Kontrol jalan keluar

Untuk memungkinkan sumber daya yang Anda buat dengan satu AWS layanan hanya mengakses AWS layanan lain, Anda dapat menggunakan informasi rentang alamat IP dalam file `ip-ranges.json` untuk melakukan pemfilteran jalan keluar. Pastikan bahwa aturan grup keamanan mengizinkan lalu lintas keluar ke blok CIDR dalam daftar AMAZON. Ada [kuota 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 EC2 dan menggunakan ruang alamat EC2 IP. Jika Anda memblokir lalu lintas ke ruang alamat EC2 IP, Anda memblokir lalu lintas ke EC2 non-layanan ini juga.

Umpan geolokasi

Rentang alamat IP di `ip-ranges.json` adalah oleh Wilayah AWS. Namun, Zona Lokal tidak berada di lokasi fisik yang sama dengan Wilayah induknya. Data geolokasi yang dipublikasikan [geo-ip-feeddi.csv](#) menyumbang Local Zones. Data mengikuti [RFC 8805](#).

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 memanfaatkan informasi tersebut untuk meningkatkan keamanan jaringan dan kontrol akses Anda. Dengan mengurai data terperinci yang terkandung dalam file JSON ini, Anda dapat dengan tepat mengidentifikasi rentang alamat IP yang terkait dengan spesifik Layanan AWS dan Wilayah.

Misalnya, Anda dapat menggunakan rentang alamat IP untuk mengonfigurasi kebijakan keamanan jaringan yang kuat, menyiapkan aturan firewall granular untuk mengizinkan atau menolak akses ke sumber daya tertentu AWS. 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 mengonfigurasi pemfilteran jalan keluar yang canggih pada infrastruktur jaringan Anda. Dengan memahami rentang alamat IP tujuan untuk yang berbeda Layanan AWS, Anda dapat mengatur kebijakan perutean atau memanfaatkan solusi keamanan jaringan tingkat lanjut seperti mengizinkan atau memblokir lalu lintas keluar secara selektif berdasarkan tujuan yang dimaksudkan. Kontrol jalan 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 up-to-date lokal sangat penting untuk memastikan Anda memiliki informasi yang paling akurat dan terkini. Dengan terus memanfaatkan konten file ini, Anda dapat secara efisien mengelola akses jaringan dan keamanan 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. [AWS Tools for Windows PowerShell](#) Termasuk cmdlet, [Get-AWSPublicIpAddressRange](#), yang dapat Anda gunakan untuk mengurai file JSON ini. Untuk informasi selengkapnya, lihat blog berikut: [Menanyakan Rentang Alamat IP Publik untuk AWS](#).

Untuk mendapatkan file JSON, lihat [the section called “Unduh”](#). Untuk informasi selengkapnya tentang sintaks file JSON, lihat [the section called “Sintaksis”](#)

Contoh

- [Dapatkan tanggal pembuatan file](#)
- [Dapatkan alamat IP untuk Wilayah tertentu](#)
- [Dapatkan semua IPv4 alamat](#)
- [Dapatkan semua IPv4 alamat untuk layanan tertentu](#)
- [Dapatkan semua IPv4 alamat untuk layanan tertentu di Wilayah tertentu](#)
- [Dapatkan semua IPv6 alamat](#)
- [Dapatkan semua IPv6 alamat 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 menyaring file JSON untuk alamat IP untuk Wilayah tertentu.

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 IPv4 alamat

Contoh berikut menyaring file JSON untuk IPv4 alamat.

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 IPv4 alamat untuk layanan tertentu

Contoh berikut menyaring file JSON untuk IPv4 alamat 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 IPv4 alamat untuk layanan tertentu di Wilayah tertentu

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

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 IPv6 alamat

Contoh berikut menyaring file JSON untuk IPv6 alamat.

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 IPv6 alamat untuk layanan tertentu

Contoh berikut menyaring file JSON untuk IPv6 alamat 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 menyaring 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 rentang alamat AWS IP JSON

AWS menerbitkan rentang alamat IP saat ini dalam format JSON. Untuk mendapatkan file JSON, lihat [the 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 format UTC YY-MM-DD-hh -mm-ss.

Tipe: String

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

prefiks

Awalan IP untuk rentang IPv4 alamat.

Jenis: Array

ipv6_prefixes

Awalan IP untuk rentang IPv6 alamat.

Jenis: Array

ip_prefix

Rentang IPv4 alamat publik, dalam notasi CIDR. Perhatikan bahwa AWS mungkin mengiklankan awalan dalam rentang yang lebih spesifik. Misalnya, prefiks 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 IPv6 alamat 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 Availability Zones atau Local Zones dari mana AWS mengiklankan alamat IP, atau GLOBAL. Lalu lintas untuk GLOBAL layanan dapat ditarik ke atau berasal dari beberapa (hingga semua) Availability Zone atau Local Zones tempat AWS mengiklankan alamat IP.

Tipe: String

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

region

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

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-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_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 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— [Mengkonfigurasi untuk media dan pensinyalan](#)
- CLOUDFRONT— [Lokasi dan rentang alamat IP server CloudFront edge](#)
- DYNAMODB— [Rentang alamat IP](#)
- EC2— [IPv4 Alamat publik](#)
- EC2_INSTANCE_CONNECT— [Prasyarat EC2 Instance Connect](#)
- GLOBALACCELERATOR— [Lokasi dan rentang alamat IP server tepi Global Accelerator](#)
- ROUTE53— [Rentang alamat IP dari server Amazon Route 53](#)
- ROUTE53_HEALTHCHECKS— [Rentang alamat IP dari server Amazon Route 53](#)
- ROUTE53_HEALTHCHECKS_PUBLISHING— [Rentang alamat IP dari server Amazon Route 53](#)
- WORKSPACES_GATEWAYS— [Server gateway PCo IP](#)

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 AURORA_DSQL .	21 Mei 2025

Deskripsi	Tanggal rilis
Menambahkan kode layanan IVS_REALTIME .	Juni 11, 2024
Menambahkan kode layanan MEDIA_PAC KAGE_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
Menambahkan kode layanan AMAZON_APPFLOW .	9 Juni 2020
Menambahkan dukungan untuk grup perbatasan jaringan.	7 April 2020
Menambahkan kode layanan WORKSPACE_S_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

Deskripsi	Tanggal rilis
Menambahkan kode layanan GLOBALACC ELERATOR .	20 Desember 2018
Menambahkan kode layanan AMAZON_C0 NNECT .	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 IPv6 alamat.	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 dari topik Amazon SNS bernama. `AmazonIpSpaceChanged` Untuk informasi selengkapnya tentang sintaks file JSON, lihat [the section called “Sintaksis”](#)

Muatan 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 pemberitahuan rentang alamat AWS IP

1. [Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home](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](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](#).

IPv6 dukungan untuk VPC Anda

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

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

Pertimbangan

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

Daftar Isi

- [Tambahkan IPv6 dukungan untuk VPC Anda](#)
- [Contoh konfigurasi VPC dual-stack](#)

Tambahkan IPv6 dukungan untuk VPC Anda

Tabel berikut memberikan ikhtisar proses IPv6 untuk mengaktifkan VPC Anda.

Daftar Isi

- [Langkah 1: Kaitkan blok IPv6 CIDR dengan VPC dan subnet Anda](#)
- [Langkah 2: Perbarui tabel rute VPC Anda](#)
- [Langkah 3: Perbarui aturan grup keamanan Anda](#)
- [Langkah 4: Tetapkan IPv6 alamat ke instans Anda](#)

Langkah	Catatan
Langkah 1: Kaitkan blok IPv6 CIDR dengan VPC dan subnet Anda	Kaitkan IPv6 blok CIDR yang disediakan Amazon atau BYOIP dengan VPC Anda dan dengan subnet Anda.
Langkah 2: Perbarui tabel rute VPC Anda	Perbarui tabel rute Anda untuk merutekan IPv6 lalu lintas Anda. Untuk subnet publik, buat rute yang merutekan semua IPv6 lalu lintas dari subnet ke gateway internet. Untuk subnet pribadi, buat rute yang merutekan semua IPv6 lalu lintas internet dari subnet ke gateway internet khusus egres.
Langkah 3: Perbarui aturan grup keamanan Anda	Perbarui aturan grup keamanan Anda untuk menyertakan aturan untuk IPv6 alamat. Ini memungkinkan IPv6 lalu lintas mengalir ke dan dari instans Anda. Jika Anda telah membuat aturan ACL jaringan khusus untuk mengontrol arus lalu lintas ke dan dari subnet Anda, Anda

Langkah	Catatan
	harus menyertakan aturan untuk IPv6 lalu lintas.
Langkah 4: Tetapkan IPv6 alamat ke instans Anda	Tetapkan IPv6 alamat ke instans Anda dari rentang IPv6 alamat subnet Anda.

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

Anda dapat mengaitkan blok IPv6 CIDR dengan VPC Anda, dan kemudian mengaitkan blok CIDR dari rentang tersebut /64 dengan setiap subnet.

Untuk mengaitkan blok IPv6 CIDR dengan VPC

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Your VPCs.
3. Pilih VPC Anda.
4. Pilih Tindakan, Edit CIDRs dan kemudian pilih Tambahkan IPv6 CIDR baru.
5. Pilih salah satu opsi berikut, lalu pilih Pilih CIDR:
 - Blok IPv6 CIDR yang disediakan Amazon - Gunakan IPv6 blok CIDR dari kumpulan alamat Amazon. IPv6 Untuk Grup Perbatasan Jaringan, pilih grup tempat AWS mengiklankan alamat IP.
 - [Blok CIDR yang dialokasikan IPAM — Gunakan blok IPv6 CIDR dari kolam IPAM IPv6](#). Pilih kolam IPAM dan blok IPv6 CIDR.
 - IPv6 CIDR yang dimiliki oleh saya - Gunakan blok IPv6 CIDR dari kumpulan IPv6 alamat Anda ([BYOIP](#)). Pilih kumpulan IPv6 alamat dan blok IPv6 CIDR.
6. Pilih Tutup.

Untuk mengaitkan blok IPv6 CIDR dengan subnet

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Pengguna.
3. Pilih subnet.
4. Pilih Actions, Edit IPv6 CIDRs dan kemudian pilih Add 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 [IPv6 Blok 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 agar memungkinkan IPv6 lalu lintas 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 instance (seperti instance database) untuk menggunakan gateway internet khusus egress untuk IPv6 lalu lintas, karena gateway NAT tidak mendukung. IPv6

Untuk memperbarui tabel rute untuk subnet publik

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Pengguna. Pilih subnet publik. Pada tab tabel Route, 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 untuk tujuan. Pilih ID gateway internet untuk Target.
5. Pilih Simpan perubahan.

Untuk memperbarui tabel rute untuk subnet pribadi

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

Untuk informasi selengkapnya, lihat [Aktifkan IPv6 lalu lintas keluar menggunakan gateway internet khusus egress-only](#).

3. Di panel navigasi, pilih Pengguna. Pilih subnet pribadi. Pada tab tabel Route, 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` untuk tujuan. Pilih ID gateway internet khusus egres 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 egres secara bersamaan. Jika Anda menerima pesan kesalahan yang menyatakan “Ada rute ipv6 yang ada dengan lompatan berikutnya sebagai Gateway internet” saat mengonfigurasi gateway internet khusus egres, Anda harus terlebih dahulu menghapus rute yang ada ke gateway internet sebelum menambahkan IPv6 rute ke gateway internet khusus egres.

Untuk informasi selengkapnya, lihat [Opsi perutean contoh](#).

Langkah 3: Perbarui aturan grup keamanan Anda

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

Untuk memperbarui aturan grup keamanan masuk

1. Buka konsol VPC Amazon 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 IPv4 lalu lintas, pilih Tambahkan aturan dan konfigurasi aturan untuk mengizinkan IPv6 lalu lintas yang sesuai. Misalnya, untuk menambahkan aturan yang memungkinkan semua lalu lintas HTTP berakhir IPv6, pilih HTTP untuk Jenis dan `::/0` Sumber.

5. Setelah selesai menambahkan aturan, pilih Simpan aturan.

Perbarui aturan grup keamanan keluar Anda

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 asli untuk grup keamanan Anda, aturan ini tidak ditambahkan secara otomatis, dan Anda harus menambahkan aturan keluar yang setara untuk IPv6 lalu lintas.

Memperbarui aturan ACL jaringan Anda

Saat 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 lalu lintas secara manual. IPv6 Untuk informasi selengkapnya, lihat [Menambahkan dan menghapus aturan](#).

Langkah 4: Tetapkan IPv6 alamat ke instans Anda

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

Setelah memverifikasi bahwa jenis instans mendukung IPv6, Anda dapat menetapkan IPv6 alamat ke instans menggunakan EC2 konsol Amazon. IPv6 Alamat ditetapkan ke antarmuka jaringan utama (misalnya, eth0) untuk contoh. Untuk informasi selengkapnya, lihat [Menetapkan IPv6 alamat ke instans](#) di Panduan EC2 Pengguna Amazon.

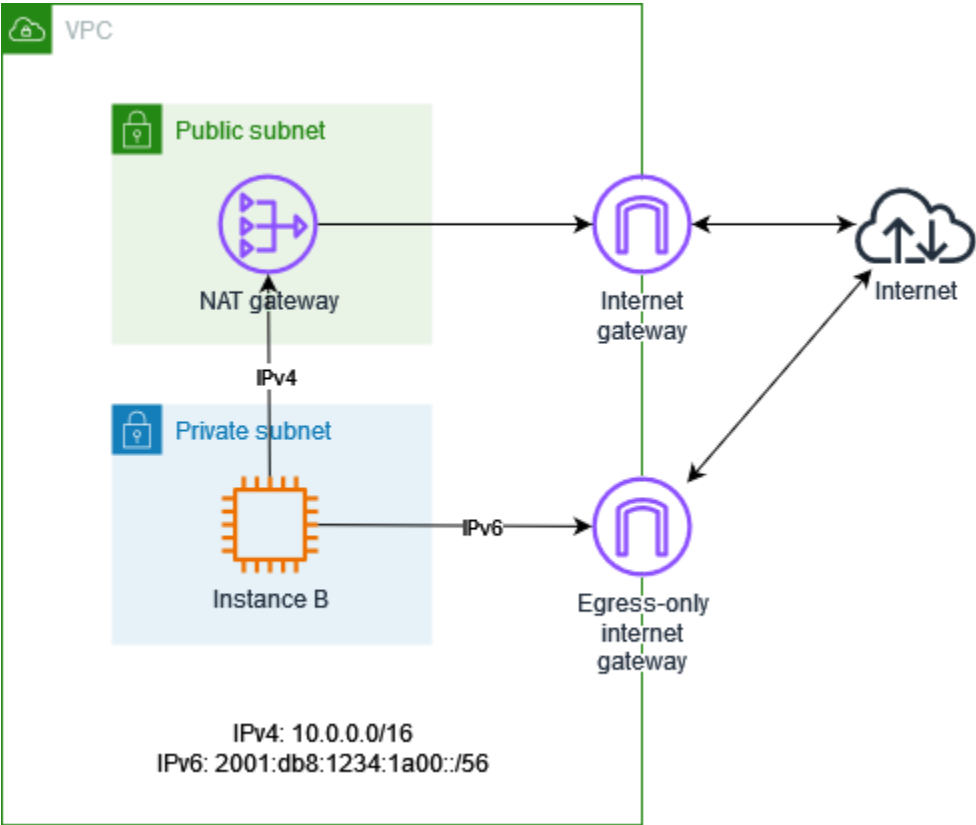
Anda dapat terhubung ke sebuah instance menggunakan IPv6 alamatnya. Untuk informasi selengkapnya, lihat [Connect ke instans Linux menggunakan klien SSH](#) di Panduan EC2 Pengguna Amazon.

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

Contoh konfigurasi VPC dual-stack

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

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



Tabel rute untuk subnet publik

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

Tujuan	Target
VPC IPv4 CIDR	lokal

Tujuan	Target
<i>VPC IPv6 CIDR</i>	lokal
0.0.0.0/0	<i>internet-gateway-id</i>
::/0	<i>internet-gateway-id</i>

Tabel rute untuk subnet pribadi

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

Tujuan	Target
<i>VPC IPv4 CIDR</i>	lokal
<i>VPC IPv6 CIDR</i>	lokal
0.0.0.0/0	<i>nat-gateway-id</i>
::/0	<i>egress-only-gateway-id</i>

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 menyertakan dukungan untuk konfigurasi tumpukan ganda (IPv4 dan IPv6) atau IPv6 hanya konfigurasi. 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, tumpukan ganda, atau IPv4 hanya. IPv6

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, IPv6 hanya dukungan, 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	Dukungan titik akhir publik IPv6	Dukungan IPv6 titik akhir pribadi 1
AWS Amplify	Ya	Tidak	Ya	
Amazon API Gateway	Ya	Tidak	Ya	Ya
AWS App Mesh	Ya	Ya	Ya	Tidak
AWS AppConfig	Ya	Tidak	Ya	Ya
AWS Application Discovery Service	Ya	Tidak	Ya	Ya
Pengontrol Pemulihan Aplikasi (ARC)	Ya	Tidak	Ya	
Amazon AppStream 2.0	Ya	Tidak	Tidak	Tidak
AWS AppSync ²	Sebagian	Tidak	Sebagian	Tidak
Amazon Athena	Ya	Tidak	Ya	Ya
Amazon Aurora	Ya	Tidak	Ya	Tidak
AWS B2B Pertukaran Data	Ya	Tidak	Ya	Ya

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Dukungan titik akhir publik IPv6	Dukungan IPv6 titik akhir pribadi 1
AWS Backup	Ya	Tidak	Ya	Ya
AWS Batch	Ya	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
Amazon Braket	Ya	Ya	Ya	Ya
AWS Certificate Manager	Ya	Tidak	Ya	Tidak
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	
AWS Cloud Control API	Ya	Tidak	Ya	Ya
Amazon CloudFront	Ya	Tidak	Tidak	
AWS CloudHSM	Ya	Tidak	Ya	Ya
AWS CloudTrail	Ya	Tidak	Ya	Ya
CloudWatch Log Amazon	Ya	Ya	Ya	Ya

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Dukungan titik akhir publik IPv6	Dukungan IPv6 titik akhir pribadi 1
Amazon CloudWatch Synthetics	Ya	Tidak	Ya	Ya
AWS Cloud Map	Ya	Ya	Ya	Ya
AWS Awan WAN	Ya	Tidak	Ya	Ya
AWS CodeArtifact	Ya	Tidak	Ya	Ya
Amazon Connect Customer Profiles	Ya	Tidak	Ya	Ya
Amazon CodeGuru Profiler	Ya	Tidak	Ya	Ya
AWS Cost Explorer	Ya	Tidak	Ya	Ya
Hub Optimisasi Biaya AWS	Ya	Tidak	Ya	Ya
AWS Elastic Beanstalk	Tidak	Tidak	Ya	Ya
Amazon Cognito	Ya	Tidak	Ya	
Amazon Data Firehose	Tidak	Tidak	Ya	Ya
Amazon Data Lifecycle Manager	Ya	Tidak	Ya	Ya
AWS Database Migration Service	Ya	Tidak	Tidak	Tidak
AWS Deadline Cloud	Ya	Tidak	Ya	Ya
Amazon Detective	Ya	Ya	Ya	
AWS Direct Connect	Ya	Ya	Tidak	

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Dukungan titik akhir publik IPv6	Dukungan IPv6 titik akhir pribadi 1
Amazon EBS langsung APIs	Ya	Tidak	Ya	Ya
Amazon EC2	Ya	Ya	Ya	Tidak
Amazon ECR	Ya	Tidak	Ya	Tidak
Amazon ECS	Ya	Tidak	Ya	Ya
Amazon EFS	Ya	Ya	Ya	
Amazon EKS	Sebagian	Sebagian	Ya	Ya
Penyeimbang Beban Elastis	Sebagian	Sebagian	Tidak	Tidak
Amazon ElastiCache	Ya	Ya	Tidak	Tidak
AWS Pesan Pengguna Akhir Sosial	Ya	Tidak	Ya	Tidak
Resolusi Entitas AWS	Ya	Tidak	Ya	Ya
AWS Fargate	Ya	Tidak	Tidak	Tidak
Amazon FSx	Tidak	Tidak	Ya	Ya
GameLift Aliran Amazon	Ya	Tidak	Ya	Tidak
AWS Global Accelerator	Ya	Tidak	Tidak	
AWS Glue	Ya	Tidak	Tidak	Ya
Grafana Dikelola Amazon 3	Ya	Tidak	Ya	Ya
AWS Ground Station ⁴	Ya	Tidak	Ya	Ya

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Dukungan titik akhir publik IPv6	Dukungan IPv6 titik akhir pribadi 1
AWS Identity and Access Management (IAM)	Ya	Ya	Ya	Ya
AWS Penganalisis Akses IAM	Ya	Tidak	Ya	Ya
Amazon Inspector	Ya	Ya	Ya	Ya
AWS IoT	Ya	Tidak	Ya	Tidak
AWS IoT FleetWise	Ya	Tidak	Ya	Ya
AWS IoT SiteWise	Ya	Tidak	Ya	Ya
AWS IoT TwinMaker	Ya	Tidak	Ya	Ya
AWS IoT Wireless	Ya	Tidak	Ya	Ya
AWS Key Management Service	Ya	Sebagian	Ya	Ya
Amazon Kinesis Data Streams	Ya	Tidak	Ya	Tidak
AWS Lake Formation	Tidak	Tidak	Tidak	Ya
AWS Lambda	Ya	Tidak	Ya	Ya
Amazon Lightsail	Ya	Ya	Ya	Ya
Amazon Macie	Ya	Tidak	Ya	Ya
AWS Mainframe Modernization	Ya	Tidak	Ya	Ya
AWS Network Firewall	Ya	Ya	Tidak	Tidak

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Dukungan titik akhir publik IPv6	Dukungan IPv6 titik akhir pribadi 1
AWS Network Manager	Ya	Tidak	Ya	Ya
OpenSearch Layanan Amazon	Ya	Tidak	Ya	Tidak
AWS Organizations	Ya	Tidak	Ya	Tidak
Amazon Personalize	Ya	Tidak	Ya	Ya
Amazon Pinpoint	Ya	Tidak	Ya	Tidak
Amazon Polly	Ya	Tidak	Ya	Ya
AWS Private Certificate Authority	Ya	Tidak	Ya	Ya
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	
Layanan Terkelola Amazon untuk Prometheus	Ya	Tidak	Ya	Ya
Amazon RDS	Ya	Tidak	Ya	Tidak
Keranjang Sampah	Ya	Tidak	Ya	Ya
AWS re:Post Privat	Ya	Tidak	Ya	Ya

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Dukungan titik akhir publik IPv6	Dukungan IPv6 titik akhir pribadi 1
AWS Resource Access Manager	Ya	Tidak	Ya	Ya
Penjelajah Sumber Daya AWS	Ya	Tidak	Ya	
AWS Resource Groups	Ya	Ya	Ya	Ya
AWS Resource Groups Tagging API	Ya	Ya	Ya	Ya
Amazon Route 53	Ya	Ya	Tidak	
Amazon S3	Ya	Tidak	Ya	Tidak
AWS Secrets Manager	Ya	Tidak	Ya	Tidak
Amazon Security Lake	Ya	Tidak	Ya	Ya
AWS Shield	Ya	Ya	Tidak	
Layanan Email Sederhana Amazon	Ya	Tidak	Ya	Ya
Amazon Simple Notification Service	Ya	Tidak	Ya	Tidak
Amazon Simple Queue Service	Ya	Tidak	Ya	Tidak
Layanan Alur Kerja Sederhana Amazon	Ya	Tidak	Ya	Ya
AWS Site-to-Site VPN	Ya	Tidak	Ya	Tidak
AWS Step Functions	Ya	Tidak	Ya	Ya

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Dukungan titik akhir publik IPv6	Dukungan IPv6 titik akhir pribadi ¹
Amazon Transcribe	Ya	Ya	Ya	Ya
AWS Transit Gateway	Ya	Tidak	Ya	Tidak
Amazon Translate	Ya	Ya	Ya	Ya
Izin Terverifikasi Amazon	Ya	Tidak	Ya	Ya
Amazon VPC	Ya	Ya	Ya	Tidak
AWS WAF	Ya	Ya	Tidak	
Amazon WorkSpaces	Ya	Tidak	Tidak	Tidak
AWS X-Ray	Ya	Tidak	Ya	Ya
EC2 Image Builder	Ya	Ya	Ya	Ya

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

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

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

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

IPv6 Dukungan tambahan

Komputasi

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

Jaringan dan Pengiriman Konten

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

Keamanan, Identitas, dan Kepatuhan

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

Pengelolaan dan Tata Kelola

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

Pelajari selengkapnya

- [IPv6 pada AWS](#)
- [Dual Stack dan IPv6 -only Arsitektur Referensi VPC Amazon](#) (PDF)

Konfigurasi cloud pribadi 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 tambahan VPCs bisa menguntungkan.

Membuat tambahan VPCs 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 VPCs 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) kustom VPCs 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](#)
- [Default VPCs](#)
- [Buat VPC](#)
- [Visualisasikan sumber daya di VPC Anda](#)
- [Tambahkan atau hapus blok CIDR dari VPC Anda](#)

- [Opsis 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 Wavelength, atau Pos Luar](#)
- [Hapus VPC Anda](#)
- [Hasilkan infrastructure-as-code 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

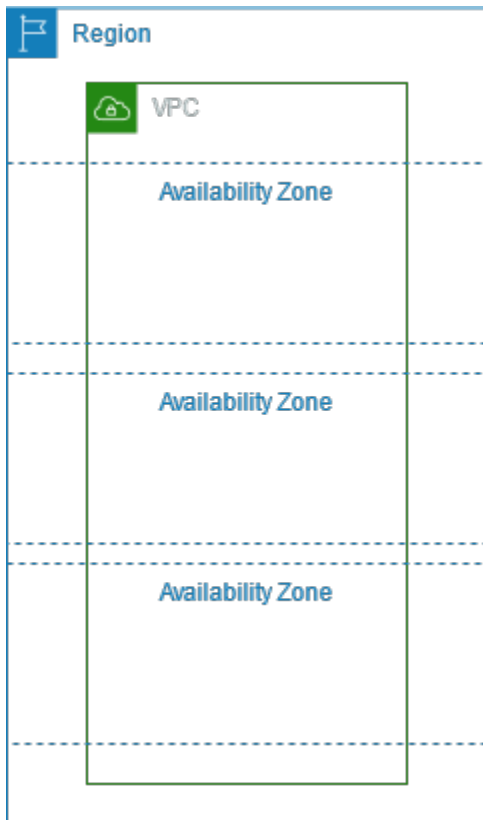
Saat Anda membuat VPC, Anda menentukan alamat IP-nya sebagai berikut:

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

Untuk informasi selengkapnya, lihat [Alamat IP untuk Anda VPCs dan subnet](#).

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:

- [Jaringan ACLs](#)
- [Tabel rute khusus](#)
- [Grup keamanan](#)
- [Gerbang internet](#)
- [Gateway NAT](#)

Opsis 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 AZs untuk mengoperasikan aplikasi produksi dan database yang lebih tersedia, toleran kesalahan, dan skalabel daripada yang mungkin dari satu pusat data. Jika Anda mempartisi aplikasi yang berjalan di subnet AZs, 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 [Alamat IP untuk Anda VPCs dan subnet](#).

Opsis DNS

Jika Anda memerlukan nama host IPv4 DNS publik untuk EC2 instance yang diluncurkan ke subnet Anda, Anda harus mengaktifkan kedua opsi DNS. Untuk informasi selengkapnya, lihat [Atribut DNS untuk VPC Anda](#).

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

gateway internet

Hubungkan 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 selengkapnya, 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 EC2 instance, 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 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

Default VPCs

Saat Anda mulai menggunakan Amazon VPC, Anda memiliki VPC default di setiap Wilayah. AWS VPC default dilengkapi dengan subnet publik di setiap Availability Zone, gateway internet, dan pengaturan untuk mengaktifkan resolusi DNS. Oleh karena itu, Anda dapat segera mulai meluncurkan EC2 instans Amazon 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 instance 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

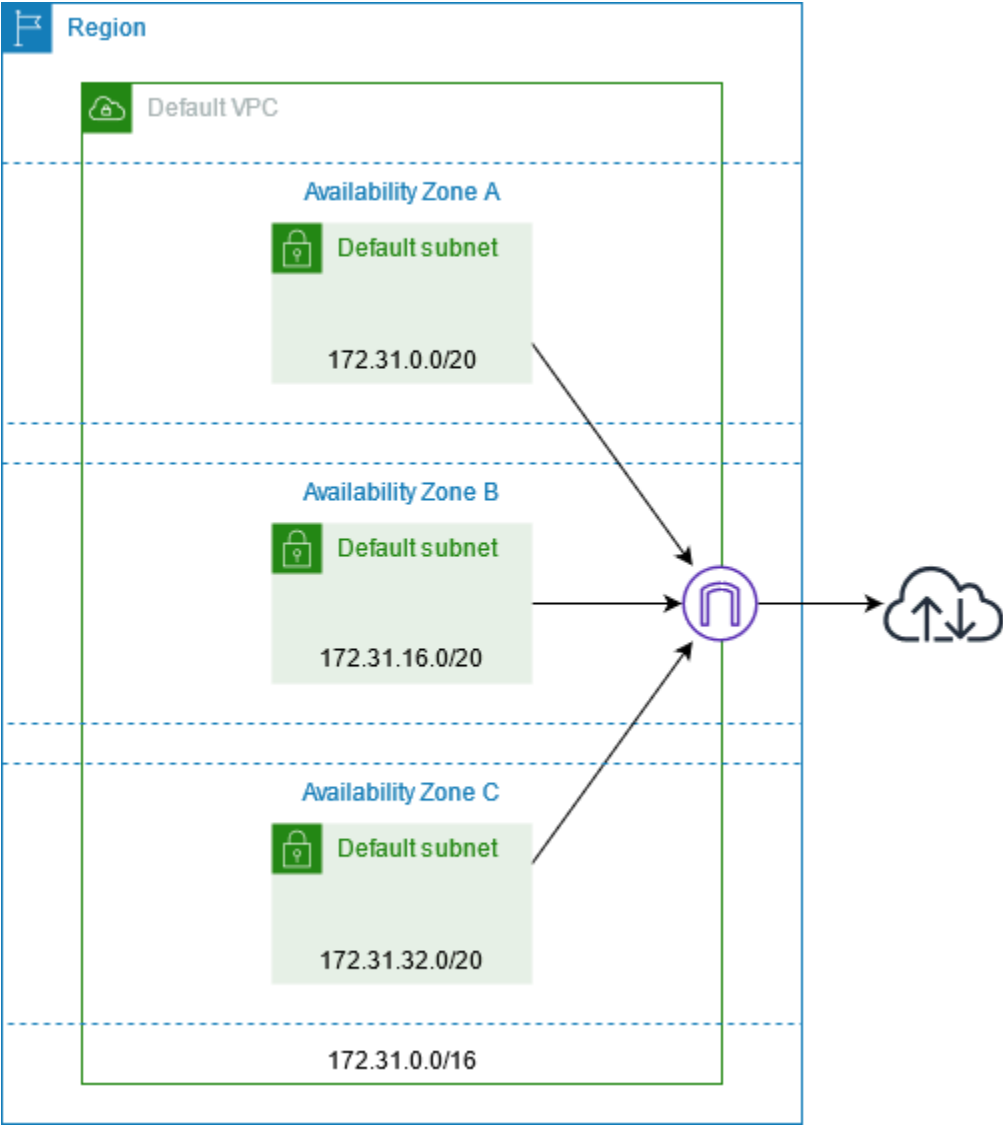
Ketika kita membuat VPC default, kita melakukan hal berikut untuk menyiapkannya untuk Anda:

- Buat VPC dengan ukuran /16 IPv4 CIDR block (). 172.31.0.0/16 Ini menyediakan hingga 65.536 alamat pribadi. IPv4
- 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 menelepon `CreateDefaultVpc`, 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, lihat. [Memblokir akses publik ke VPCs dan subnet](#)

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



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

Tujuan	Target
172.31.0.0/16	lokal
0.0.0.0/0	<i>internet_gateway_id</i>

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.
- Tambahkan lebih banyak blok IPv4 CIDR.
- Akses VPCs 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 karena Anda akan menggunakan subnet lainnya; tambahkan tabel rute khusus dan atur jaringan. ACLs Anda juga dapat menentukan subnet default tertentu ketika Anda meluncurkan sebuah EC2 instance.

Anda dapat secara opsional mengaitkan blok IPv6 CIDR 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 ke subnet privat dengan menghapus rute dari tujuan 0.0.0.0/0 ke gateway internet. Namun, jika Anda melakukan ini, tidak ada EC2 instance yang berjalan di subnet itu yang dapat mengakses internet.

Contoh yang Anda luncurkan ke subnet default menerima IPv4 alamat publik dan IPv4 alamat pribadi, dan nama host DNS publik dan pribadi. Instance yang Anda luncurkan ke subnet nondefault di VPC default tidak menerima IPv4 alamat 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 Availability Zone baru ke Region. 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 subnet default VPCs dan 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 VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Your VPCs.
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 VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Your VPCs.
3. Pilih Tindakan, Buat VPC Default.
4. Pilih Buat. Tutup layar konfirmasi.

Untuk membuat VPC default menggunakan baris perintah

Anda dapat menggunakan perintah [create-default-vpc](#) AWS CLI . 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-EC2DefaultVpcTools](#) for Windows atau tindakan [CreateDefaultVpc](#) Amazon EC2 API.

Membuat subnet default

Note

Anda tidak dapat membuat subnet default menggunakan AWS Management Console.

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 Availability Zone baru dan tidak secara otomatis membuat subnet default untuk zona tersebut di VPC default Anda.

Saat Anda membuat subnet default, subnet dibuat dengan blok /20 IPv4 CIDR ukuran di ruang bersebelahan berikutnya yang tersedia 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 membutuhkan lebih banyak ruang alamat, Anda dapat [menambahkan blok IPv4 CIDR ke VPC Anda](#).

Jika Anda telah mengaitkan blok IPv6 CIDR dengan VPC default Anda, subnet default baru tidak secara otomatis menerima IPv6 blok CIDR. Sebagai gantinya, Anda dapat mengaitkan blok IPv6 CIDR 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 [create-default-subnet](#) AWS CLI perintah dan tentukan Availability Zone 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](#) Tools for 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 VPCs satu saat Anda meluncurkan instance. Jika Anda tidak memiliki VPC lain, Anda harus membuat VPC dengan subnet di setidaknya satu Availability Zone. 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 Penyewaan. 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 gateway NAT](#).
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 hal berikut ini:
 - 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 Anda 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 konfigurasi 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 adalah 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 adalah 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-gateway](#) perintah 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 khusus untuk subnet publik Anda dengan menggunakan [create-route-table](#) perintah 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-table](#) perintah 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 egress 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 berikut create-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-table](#) perintah 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 egress 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-table](#) perintah 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-table](#) perintah 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-table](#) perintah 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-block](#) dan [disassociate-vpc-cidr-block](#) perintah.

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

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

Setiap Wilayah memiliki set opsi DHCP default. Setiap VPC menggunakan opsi DHCP default yang ditetapkan untuk Wilayahnya kecuali Anda membuat dan mengaitkan opsi DHCP khusus yang ditetapkan dengan VPC atau mengonfigurasi VPC tanpa set opsi DHCP.

Jika VPC Anda tidak memiliki set opsi DHCP yang dikonfigurasi:

- Untuk [EC2 contoh yang dibangun di Sistem Nitro](#), AWS mengkonfigurasi 169.254.169.253 sebagai server nama domain default.
- Untuk [EC2 contoh yang dibangun di Xen](#), tidak ada server nama domain yang dikonfigurasi dan, karena instance di VPC tidak memiliki akses ke server DNS, mereka tidak dapat mengakses internet.

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

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

Daftar Isi

- [Set opsi DHCP default](#)
- [Set opsi DHCP kustom](#)

Set opsi DHCP default

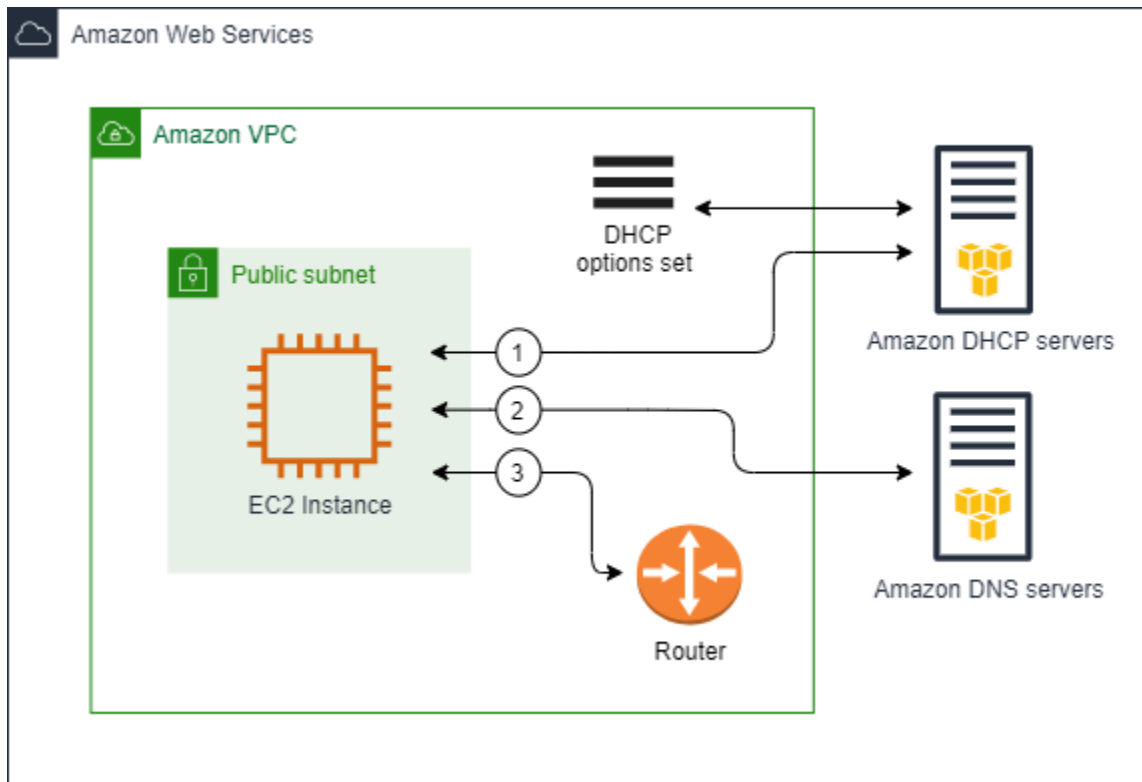
Set opsi DHCP default berisi pengaturan berikut:

- 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 EC2 instance, lihat nama [host EC2 instans Amazon](#).
- IPv6 Waktu Sewa Pilihan: Seberapa sering instance yang berjalan dengan yang IPv6 ditugaskan padanya melewati perpanjangan DHCPv6 sewa. Waktu sewa default adalah 140 detik. Perpanjangan sewa biasanya terjadi ketika setengah dari waktu sewa telah berlalu.

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

- Server NTP: Secara default, EC2 instance menggunakan [Layanan Sinkronisasi Waktu Amazon](#) untuk mengambil waktu.
- Server nama NetBIOS: Untuk EC2 contoh 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 EC2 contoh yang menjalankan Windows, ini adalah metode yang digunakan instance 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 Amazon DHCP kapan saja untuk mendapatkan sewa alamat IP mereka dan pengaturan jaringan tambahan.



Set opsi DHCP kustom

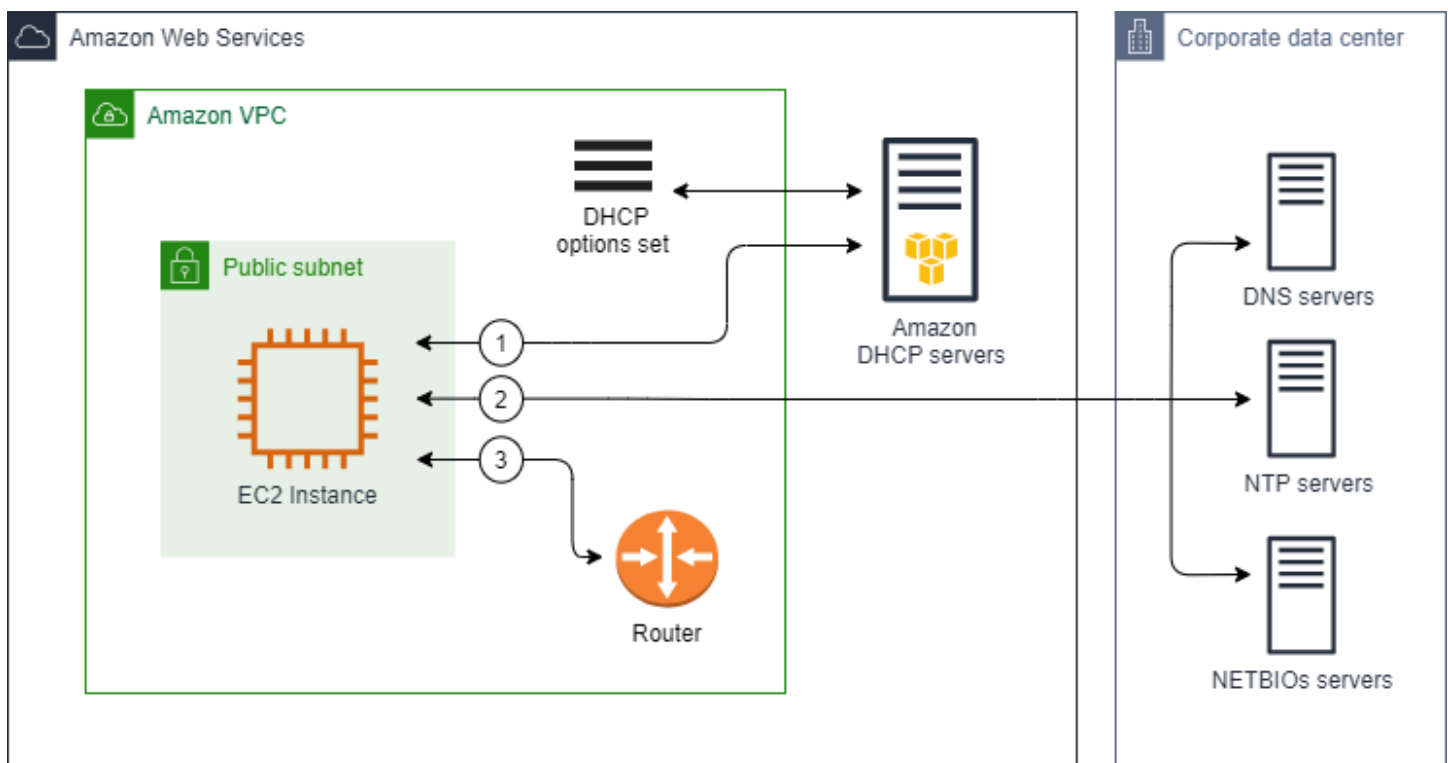
Anda dapat membuat opsi DHCP khusus yang disetel dengan pengaturan berikut, dan kemudian mengaitkannya dengan VPC:

- 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 Domain Name System (DNS).
- Server NTP: Server NTP yang menyediakan waktu untuk instance.
- Server nama NetBIOS: Untuk EC2 contoh 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 EC2 contoh yang menjalankan Windows, metode yang digunakan instance untuk menyelesaikan nama NetBIOS ke alamat IP.
- 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 4294967295 detik (sekitar 138 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.

Saat Anda menggunakan set opsi khusus, instance yang diluncurkan ke VPC Anda melakukan hal berikut, seperti yang ditunjukkan pada diagram: (1) gunakan pengaturan jaringan di set opsi DHCP khusus, (2) berinteraksi dengan DNS, NTP, dan server 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, lihat [the 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 melalui Sistem Nama Domain. 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 kendalikan 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 opsi DHCP yang ditetapkan 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 diatur untuk 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.

IPv4 Alamat publik memungkinkan komunikasi melalui internet, sementara IPv4 alamat pribadi memungkinkan komunikasi dalam jaringan instance. Untuk informasi selengkapnya, lihat [Alamat IP untuk Anda VPCs dan subnet](#).

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

Daftar Isi

- [Memahami DNS Amazon](#)
- [Lihat nama host DNS untuk instans Anda EC2](#)
- [Melihat dan memperbarui atribut DNS untuk VPC Anda](#)

Memahami DNS Amazon

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 penyelesai DNS ini terintegrasi secara native ke dalam setiap Availability Zone di AWS Wilayah Anda, memberikan solusi yang andal dan terukur untuk resolusi nama domain dalam Virtual Private Cloud (VPC) Anda. Di bagian ini Anda akan mempelajari tentang alamat IP server DNS Amazon, nama host DNS pribadi yang dapat diatasi, dan aturan yang mengatur penggunaannya.

Daftar Isi

- [Server Amazon DNS](#)
- [Aturan dan pertimbangan](#)
- [Nama host DNS untuk instance EC2](#)
- [Atribut DNS untuk VPC Anda](#)
- [Kuota DNS](#)
- [Zona host pribadi](#)

Server Amazon DNS

Route 53 Resolver (juga disebut “Amazon DNS server” atau “DNS”) adalah layanan AmazonProvided DNS Resolver yang dibangun ke dalam setiap Availability Zone di suatu Wilayah. AWS Route 53 Resolver terletak di 169.254.169.253 (IPv4), fd00:ec2::253 (IPv6), dan pada rentang IPV4 CIDR pribadi utama yang disediakan untuk VPC Anda ditambah dua. Misalnya, jika Anda memiliki VPC dengan CIDR 10.0.0.0/16 dan IPv4 CIDR dari 2001:db8::/32, Anda dapat IPv6 mencapai Route 53 Resolver di 169.254.169.253 (IPv4), (), fd00:ec2::253 atau (). IPv6 10.0.0.2 IPv4 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 subnet IPv6 -only, alamat IPv4 link-lokal (169.254.169.253) masih dapat dijangkau selama “DNS” adalah server nama dalam set opsi DHCP. AmazonProvided

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 IPv4 alamat publik dan atribut DNS VPC diaktifkan.

Format nama host DNS pribadi tergantung pada bagaimana Anda mengonfigurasi EC2 instance saat Anda meluncurkannya. Untuk informasi selengkapnya tentang jenis nama host DNS pribadi, lihat [jenis nama host EC2 instans Amazon 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 memfilter lalu lintas ke atau dari server DNS Amazon menggunakan jaringan ACLs 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 instance EC2

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

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

Nama IPv4 DNS pribadi

Nama host IPv4 DNS pribadi dari sebuah instans menyelesaikan ke alamat pribadinya. IPv4 Anda dapat menggunakan nama host IPv4 DNS pribadi untuk komunikasi antar instance di VPC yang sama atau terhubung. VPCs Untuk informasi selengkapnya, lihat [IPv4 Alamat pribadi](#) di Panduan EC2 Pengguna Amazon.

Nama IPv4 DNS publik

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

Untuk menyelesaikan nama IPv4 DNS publik ke IPv4 alamat 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 DNS berbasis RBN 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 subnet dual-stack dan -only. IPv6 Untuk informasi selengkapnya tentang RBN, lihat [jenis nama host EC2 instance](#) 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 diberi IPv4 alamat publik atau alamat IP Elastis saat pembuatan. Jika Anda mengaktifkan kedua atribut untuk VPC yang sebelumnya tidak mengaktifkan keduanya, instance yang sudah diluncurkan ke VPC tersebut akan menerima nama host DNS publik jika memiliki alamat publik atau alamat IP Elastis. IPv4

Untuk memeriksa apakah atribut ini diaktifkan untuk VPC Anda, lihat. [Melihat dan memperbarui atribut DNS untuk VPC Anda](#)

Atribut	Deskripsi
<code>enableDnsHostnames</code>	Menentukan apakah VPC mendukung penetapan nama host DNS publik ke instance dengan alamat IP publik. Default untuk atribut ini adalah <code>false</code> kecuali VPC adalah VPC default. Perhatikan Aturan dan pertimbangan untuk atribut ini di bawah ini.
<code>enableDnsSupport</code>	Menentukan apakah VPC mendukung resolusi DNS melalui server DNS yang disediakan Amazon.

Atribut	Deskripsi
	Jika atribut <code>init</code> <code>true</code>, kueri ke server DNS yang disediakan Amazon berhasil. Untuk informasi selengkapnya, lihat Server Amazon DNS. Default untuk atribut ini adalah <code>true</code>. Perhatikan Aturan 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.
 - Amazon Route 53 Resolver Server dapat menyelesaikan nama host DNS pribadi yang disediakan Amazon.
- Jika setidaknya salah satu atribut diatur ke `false`, berikut ini terjadi:
 - Instans dengan alamat IP publik tidak menerima nama host DNS publik yang sesuai.
 - Amazon Route 53 Resolver Tidak dapat menyelesaikan nama host DNS pribadi yang disediakan Amazon.
 - Instans-instans menerima nama host DNS pribadi kustom jika ada nama domain kustom di [kumpulan opsi DHCP](#). Jika Anda tidak menggunakan server Amazon Route 53 Resolver, server nama domain kustom Anda harus mengganti nama host yang sesuai.
- Jika Anda menggunakan nama domain DNS khusus yang ditentukan di zona host pribadi di Amazon Route 53, atau menggunakan DNS pribadi dengan titik akhir VPC antarmuka (AWS PrivateLink), Anda harus menyetel atribut dan ke. `enableDnsHostnames` `enableDnsSupport` `true`
- Amazon Route 53 Resolver [Dapat menyelesaikan nama host DNS pribadi ke IPv4 alamat pribadi untuk semua ruang alamat, termasuk di mana rentang IPv4 alamat VPC Anda berada di luar rentang IPv4 alamat pribadi yang ditentukan oleh RFC 1918](#). Namun, jika Anda membuat VPC sebelum Oktober 2016, VPC Amazon Route 53 Resolver tidak menyelesaikan nama host DNS pribadi jika rentang IPv4 alamat 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-lokal.](#) Batas ini mencakup agregat kueri DNS Route 53 Resolver, permintaan Layanan [Metadata Instans \(IMDS\)](#), permintaan [Amazon Time Service Network Time Protocol \(NTP\)](#), dan permintaan [Layanan Lisensi Windows](#) (untuk instance berbasis Microsoft Windows). Kuota ini tidak dapat dinaikkan jumlahnya.

Jumlah kueri DNS per detik yang didukung oleh Route 53 Resolver bervariasi menurut jenis kueri, ukuran respons, dan protokol yang digunakan. Untuk informasi selengkapnya dan rekomendasi untuk arsitektur DNS yang dapat diskalakan, lihat Panduan Teknis [AWS Hybrid DNS with Active Directory](#).

Jika Anda mencapai kuota, Resolver Route 53 menolak lalu lintas. Beberapa penyebab untuk mencapai kuota mungkin karena masalah pembatasan DNS, atau kueri metadata instance yang menggunakan antarmuka jaringan Route 53 Resolver. 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 instance, lihat [Mengambil metadata instans](#) di Panduan Pengguna Amazon EC2.

Zona host pribadi

Untuk mengakses sumber daya di VPC Anda menggunakan nama domain DNS kustom, seperti `example.com`, alih-alih menggunakan IPv4 alamat pribadi atau nama host DNS pribadi AWS yang disediakan, Anda dapat membuat zona host pribadi di Route 53. Zona host pribadi adalah wadah yang menyimpan informasi tentang bagaimana Anda ingin merutekan lalu lintas untuk domain dan subdomainnya dalam satu atau lebih VPCs 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 Anda menggunakan nama DNS pribadi kustom mereka dari sisi lain koneksi VPN.

Important

Jika Anda menggunakan nama domain DNS kustom yang ditentukan di zona yang dihosting pribadi di Amazon Route 53, Anda harus menyetel `enableDnsSupport` atribut `enableDnsHostnames` dan atribut `true`.

Lihat nama host DNS untuk instans Anda EC2

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

Bidang DNS Publik (IPv4) dan DNS Pribadi tersedia saat opsi DNS diaktifkan untuk VPC yang terkait dengan instance. 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 EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Di panel navigasi, pilih Instans.
3. Pilih Instans Anda dari daftar.
4. Di panel detail, bidang DNS Publik (IPv4) dan DNS Pribadi menampilkan nama host DNS, jika berlaku.

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 EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Di panel navigasi, pilih Antarmuka Jaringan.
3. Pilih antarmuka jaringan dari daftar.
4. Di panel detail, bidang Private DNS (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 mulus 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. Di panel navigasi, pilih Your VPCs.
3. Pilih kotak centang untuk VPC.
4. Tinjau informasi dalam Detail. Dalam contoh ini, nama host DNS dan resolusi DNS diaktifkan.

Details	CIDRs	Flow logs	Tags
Details			
VPC ID  vpc-e03dd489	State  Available	DNS hostnames Enabled	DNS resolution Enabled

5. Untuk memperbarui pengaturan ini, pilih Tindakan dan kemudian 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

Network Address Usage (NAU) adalah metrik yang diterapkan pada 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 yang diintip. VPCs Jika VPC diintip dengan yang lain VPCs di Wilayah yang sama, VPCs gabungan dapat memiliki hingga 128.000 unit NAU secara default. Anda dapat meminta kenaikan kuota hingga 512.000. VPCs yang diintip di berbagai Wilayah tidak berkontribusi pada batas ini.

Anda dapat menggunakan NAU dengan cara-cara berikut:

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

- Setelah membuat VPC, gunakan Amazon CloudWatch untuk memantau penggunaan VPC NAU agar tidak tumbuh melampaui batas kuota NAU. Untuk informasi selengkapnya, lihat [the section called “CloudWatch metrik”](#).

Bagaimana NAU dihitung

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

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 pribadi atau publik IPv4 dan setiap IPv6 alamat yang ditetapkan ke antarmuka jaringan untuk sebuah EC2 instance di VPC	1
Antarmuka jaringan tambahan yang dilampirkan ke sebuah instance EC2	1
Awalan ditetapkan ke antarmuka jaringan	1
Network Load Balancer untuk AZ	6
Load Balancer Gerbang untuk AZ	6
Titik akhir VPC untuk AZ	6
Lampiran gerbang transit	6
Fungsi Lambda	6
Gateway NAT	6
Target pemasangan EFS	6
Antarmuka EFA (EFA dengan perangkat ENA) atau antarmuka khusus EFA	1

Sumber Daya	Unit NAU
Pod Amazon EKS	1

Contoh NAU

Contoh berikut menunjukkan cara menghitung NAU.

Contoh 1 - Dua VPCs terhubung menggunakan VPC peering

Peered VPCs di Wilayah yang sama berkontribusi pada kuota NAU gabungan.

- VPC 1
 - 50 Network Load Balancer dalam 2 subnet di Availability Zone terpisah - 600 unit NAU
 - 5.000 instance (masing-masing dengan IPv4 alamat dan IPv6 alamat) dalam satu subnet dan 5.000 instance (masing-masing dengan IPv4 alamat dan IPv6 alamat) di subnet lain - 20.000 unit
 - 100 fungsi Lambda - 600 unit NAU
- VPC 2
 - 50 Network Load Balancer dalam 2 subnet di Availability Zone terpisah - 600 unit NAU
 - 5.000 instance (masing-masing dengan IPv4 alamat dan IPv6 alamat) dalam satu subnet dan 5.000 instance (masing-masing dengan IPv4 alamat dan IPv6 alamat) di subnet lain - 20.000 unit
 - 100 fungsi Lambda - 600 unit NAU
- Jumlah total pengintip NAU: 42.400 unit
- Kuota NAU peering default: 128.000 unit

Contoh 2 - Dua VPCs terhubung menggunakan gateway transit

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

- VPC 1
 - 50 Network Load Balancer dalam 2 subnet di Availability Zone terpisah - 600 unit NAU
 - 5.000 instance (masing-masing dengan IPv4 alamat dan IPv6 alamat) dalam satu subnet dan 5.000 instance (masing-masing dengan IPv4 alamat dan IPv6 alamat) di subnet lain - 20.000 unit
 - 100 fungsi Lambda - 600 unit NAU

- VPC 2
 - 50 Network Load Balancer dalam 2 subnet di Availability Zone terpisah - 600 unit NAU
 - 5.000 instance (masing-masing dengan IPv4 alamat dan IPv6 alamat) dalam satu subnet dan 5.000 instance (masing-masing dengan IPv4 alamat dan IPv6 alamat) di subnet lain - 20.000 unit
 - 100 fungsi Lambda - 600 unit NAU
- Total jumlah NAU per VPC: 21.200 unit
- Kuota NAU default per VPC: 64.000 unit

Bagikan subnet VPC Anda dengan akun lain

Berbagi subnet VPC memungkinkan beberapa orang Akun AWS untuk membuat sumber daya aplikasinya, seperti EC2 instans Amazon, database Amazon Relational Database Service (RDS), cluster Amazon Redshift, dan fungsi, ke dalam cloud pribadi virtual yang dikelola secara terpusat (). AWS Lambda VPCs Dalam model ini, akun yang memiliki VPC (pemilik) berbagi satu atau lebih subnet dengan akun lain (peserta) yang termasuk dalam organisasi yang sama dari. 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 membagikan subnet VPC Anda untuk memanfaatkan perutean implisit dalam VPC untuk aplikasi yang memerlukan tingkat interkoneksi tinggi dan berada dalam batas kepercayaan yang sama. Ini mengurangi jumlah VPCs yang Anda buat dan kelola, saat menggunakan akun terpisah untuk penagihan dan kontrol akses. Anda dapat menyederhanakan topologi jaringan dengan menghubungkan subnet VPC Amazon 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 [Mengaktifkan berbagi sumber daya AWS Organizations di dalam](#) Panduan AWS RAM Pengguna.
- Anda harus membuat pembagian sumber daya. Anda dapat menentukan subnet yang akan dibagikan saat Anda membuat pembagian sumber daya, atau menambahkan subnet ke pembagian 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 Organizations. 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

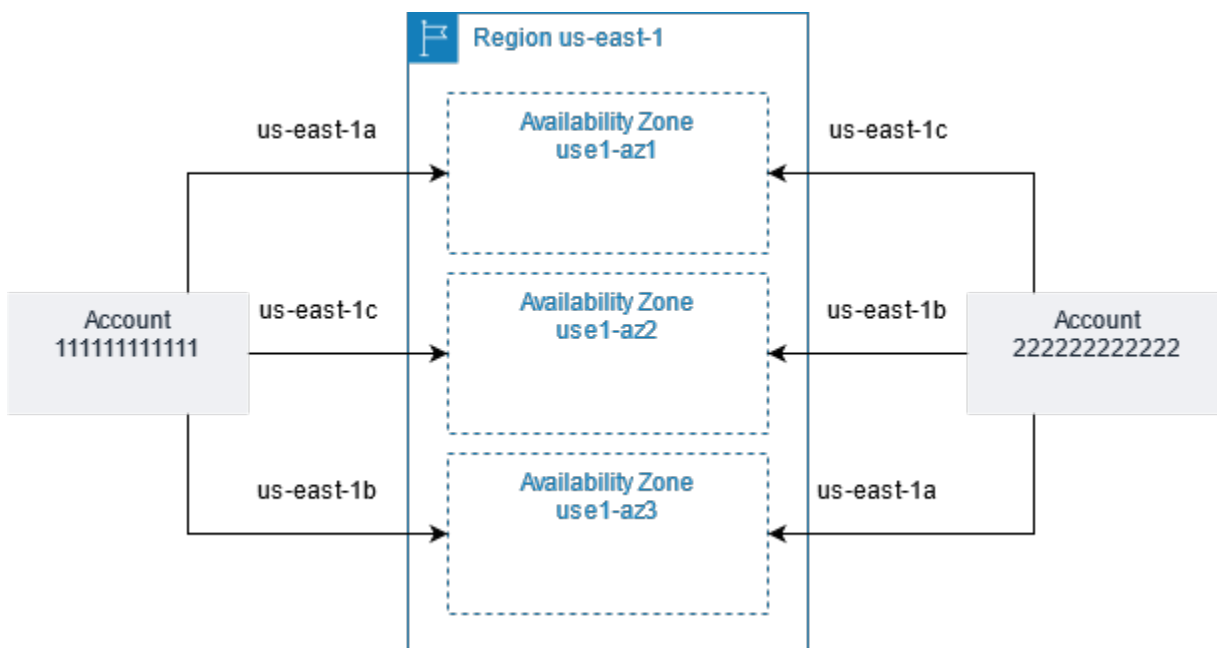
Gunakan [create-resource-share](#) dan [associate-resource-share](#) perintah.

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, Availability Zone `us-east-1a` untuk AWS akun Anda mungkin tidak memiliki lokasi yang sama dengan AWS akun lain. `us-east-1a`

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

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 EC2 instans Amazon, database Amazon Relational Database Service, cluster Amazon Redshift, dan fungsi. AWS Lambda Peserta juga membayar biaya transfer data yang terkait dengan transfer data Inter-availability Zone serta transfer data melalui koneksi peering VPC, lintas gateway internet, dan lintas gateway. AWS Direct Connect
- Pemilik VPC membayar biaya per jam (jika berlaku), pemrosesan data, dan biaya transfer data di seluruh gateway NAT, gateway pribadi virtual, gateway transit, dan titik akhir VPC. AWS PrivateLink Selain itu, IPv4 alamat publik yang digunakan bersama VPCs ditagih ke pemilik VPC. Untuk informasi selengkapnya tentang harga IPv4 alamat publik, lihat tab IPv4 Alamat Publik di halaman [harga Amazon VPC](#).
- Transfer data dalam Availability Zone yang sama (yang diidentifikasi secara unik menggunakan AZ-ID) bebas terlepas dari kepemilikan akun sumber daya yang berkomunikasi.

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, jaringan ACLs, koneksi peering, titik akhir gateway, titik akhir antarmuka, Amazon Route 53 Resolver titik akhir, 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 di 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 alur log untuk antarmuka jaringan yang mereka miliki di subnet VPC bersama.
- Peserta tidak dapat membuat, menghapus, atau menjelaskan log aliran 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 aliran untuk antarmuka jaringan yang tidak mereka miliki di subnet VPC bersama.
- Pemilik VPC dapat membuat, menghapus, dan menjelaskan flow log untuk subnet VPC bersama.
- Pemilik VPC tidak dapat menjelaskan atau menghapus log alur yang dibuat oleh peserta.

Gateway internet dan gateway internet khusus jalan keluar

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

Gateway NAT

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

Daftar kontrol akses jaringan (NACLs)

- Peserta tidak dapat membuat, menghapus, atau mengganti NACLs di subnet VPC bersama. Peserta dapat menjelaskan NACLs dibuat oleh pemilik VPC dalam 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 dalam 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 dalam kelompok keamanan yang mereka miliki yaitu kelompok keamanan referensi milik peserta lain atau pemilik VPC sebagai berikut: nomor akun/ security-group-id
- Peserta tidak dapat meluncurkan instance menggunakan grup keamanan default untuk VPC karena milik pemilik.
- [Peserta tidak dapat meluncurkan instance menggunakan grup keamanan non-default yang dimiliki oleh pemilik VPC atau peserta lain kecuali grup keamanan dibagikan dengan mereka.](#)
- Pemilik VPC dapat menggambarkan 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 instance menggunakan grup keamanan yang dibuat oleh peserta.

Subnet

- Peserta tidak dapat memodifikasi subnet bersama atau atribut terkait mereka. Hanya pemilik VPC yang bisa. Peserta dapat mendeskripsikan subnet dalam subnet VPC bersama.
- Pemilik VPC dapat berbagi subnet hanya dengan akun lain atau unit organisasi yang berada di organisasi yang sama dari Organizations. AWS Pemilik VPC tidak dapat berbagi subnet yang ada di VPC default.

Transit gateway

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

VPCs

- Peserta tidak dapat memodifikasi VPCs atau atribut terkait mereka. Hanya pemilik VPC yang bisa. Peserta dapat menjelaskan VPCs, attributes mereka, dan set opsi DHCP.
- Tag dan tag VPC untuk sumber daya dalam VPC bersama tidak dibagikan dengan peserta.
- Peserta dapat mengasosiasikan grup keamanan mereka sendiri dengan VPC bersama. Hal ini memungkinkan peserta untuk menggunakan grup keamanan dengan antarmuka jaringan Elastis yang mereka miliki di VPC bersama.

AWS sumber daya dan subnet VPC bersama

Sumber daya Layanan AWS dukungan berikut dalam 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](#)
- Penyeimbang Beban Elastis

- [Penyeimbang Beban Aplikasi](#)
- [Penyeimbang Beban Gateway](#)
- [Penyeimbang Beban Jaringan](#)
- [Amazon EMR](#)
- [AWS Glue](#)
- AWS Lambda
- Amazon MQ menjalankan Apache MQ (bukan MQ Kelinci)
- Amazon MSK
- AWS Network Manager
 - [AWS Awan WAN](#)
 - [Penganalisis Akses Jaringan](#)
 - [Reachability Analyzer](#)
- OpenSearch Layanan Amazon
- [AWS PrivateLink](#)[†]
- [Amazon Relational Database Service \(RDS\)](#)
- [Amazon Redshift](#)
- [Rute Amazon 53](#)
- [AWS Transit Gateway](#)
- [Akses Terverifikasi AWS](#)
- Amazon VPC
 - [Mengintip](#)
 - [Pencerminan Lalu Lintas](#)
- [Kisi VPC Amazon](#)

[†] Anda dapat terhubung ke semua AWS layanan yang mendukung PrivateLink menggunakan 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 mencakup semua layanan yang mendukung peluncuran sumber daya dalam 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 Wavelength, atau Pos Luar

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 membawa AWS layanan asli, infrastruktur, dan model operasi ke hampir semua pusat data, ruang co-lokasi, atau fasilitas lokal.
- Wavelength Zone memungkinkan developer membangun aplikasi yang menghadirkan latensi sangat rendah ke perangkat 5G dan pengguna akhir. Wavelength menyebarkan layanan komputasi dan penyimpanan AWS standar ke tepi jaringan 5G operator telekomunikasi.

AWS beroperasi state-of-the-art, pusat data yang 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.

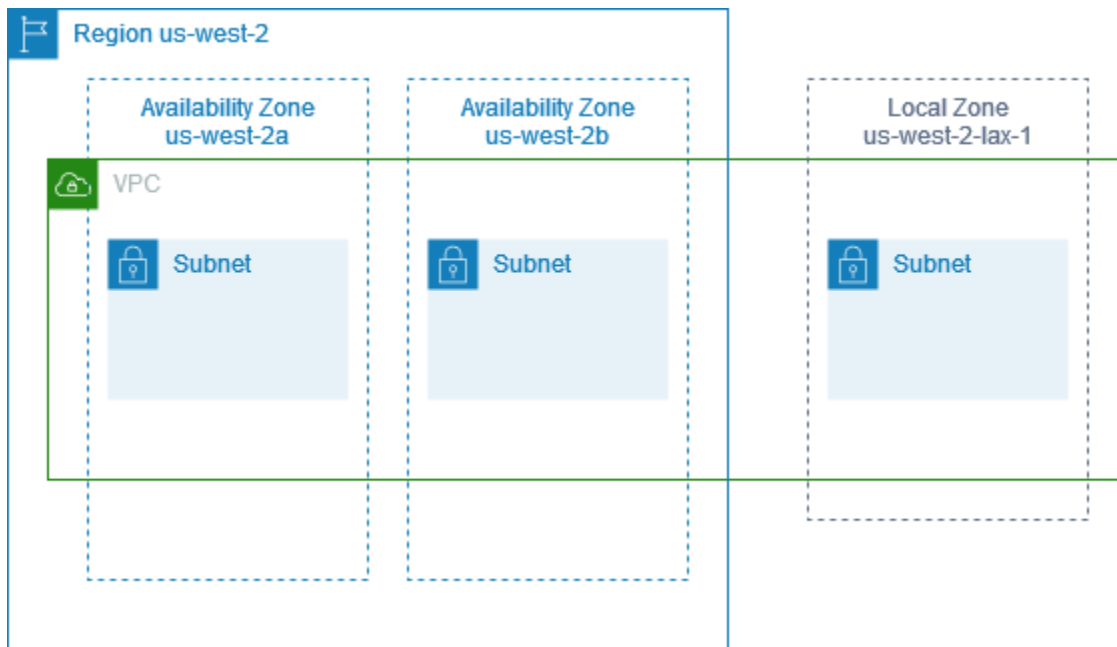
Subnet di AWS Local Zones

AWS Local Zones memungkinkan Anda untuk menempatkan sumber daya lebih dekat dengan pengguna Anda, dan terhubung dengan mulus ke berbagai layanan di AWS Wilayah, menggunakan perangkat familiar APIs dan alat. Saat Anda membuat subnet di Zona Lokal, VPC Anda diperluas ke Zona Lokal tersebut.

Untuk menggunakan Zona Lokal, Anda menggunakan proses berikut:

- Pilih 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 Availability Zone dan Local Zone.



Saat membuat VPC, Anda dapat memilih untuk menetapkan satu set alamat IP publik yang disediakan Amazon 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 Local Zone akan langsung menuju internet atau ke points-of-presence (PoPs) tanpa melintasi Wilayah induk Local Zone, memungkinkan akses ke komputasi latensi rendah. Untuk daftar lengkap Local Zones dan Wilayah induknya yang sesuai, lihat [Available Local Zones](#) di Panduan Pengguna AWS Local Zones.

Aturan berikut berlaku untuk Local Zones:

- Subnet Zona Lokal mengikuti aturan perutean yang sama dengan subnet Availability Zone, termasuk tabel rute, grup keamanan, dan jaringan. ACLs
- 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 IP yang IPv6 disediakan Amazon dan mengaitkannya dengan grup perbatasan jaringan untuk VPC baru atau yang sudah ada. Untuk

daftar Local Zones yang mendukung IPv6, lihat [Pertimbangan](#) di Panduan Pengguna AWS Local Zones

- Anda tidak dapat membuat titik akhir VPC di subnet Zona Lokal.

Untuk informasi selengkapnya tentang bekerja dengan Local Zones, lihat [Panduan Pengguna AWS Local Zones](#).

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 AWS Direct Connect lokasi di Wilayah. Pusat data lokal memiliki AWS Direct Connect koneksi ke AWS Direct Connect lokasi.

Note

Lalu lintas yang ditujukan untuk subnet di Zona Lokal menggunakan Direct Connect tidak melakukan perjalanan 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 pada halaman detail subnet di Amazon Virtual Private Cloud Console, atau menggunakan perintah deskripsi-subnet.](#)

Untuk informasi tentang cara membuat virtual private gateway, lihat [Membuat gateway target](#) di Panduan Pengguna AWS Site-to-Site VPN .

- Koneksi Direct Connect. Untuk kinerja latensi terbaik, AWS merekomendasikan agar Anda menggunakan lokasi Direct Connect yang paling dekat dengan Zona Lokal tempat Anda akan memperluas subnet Anda.

Untuk informasi tentang memerintahkan koneksi, lihat [Koneksi silang](#) dalam Panduan Pengguna AWS Direct Connect .

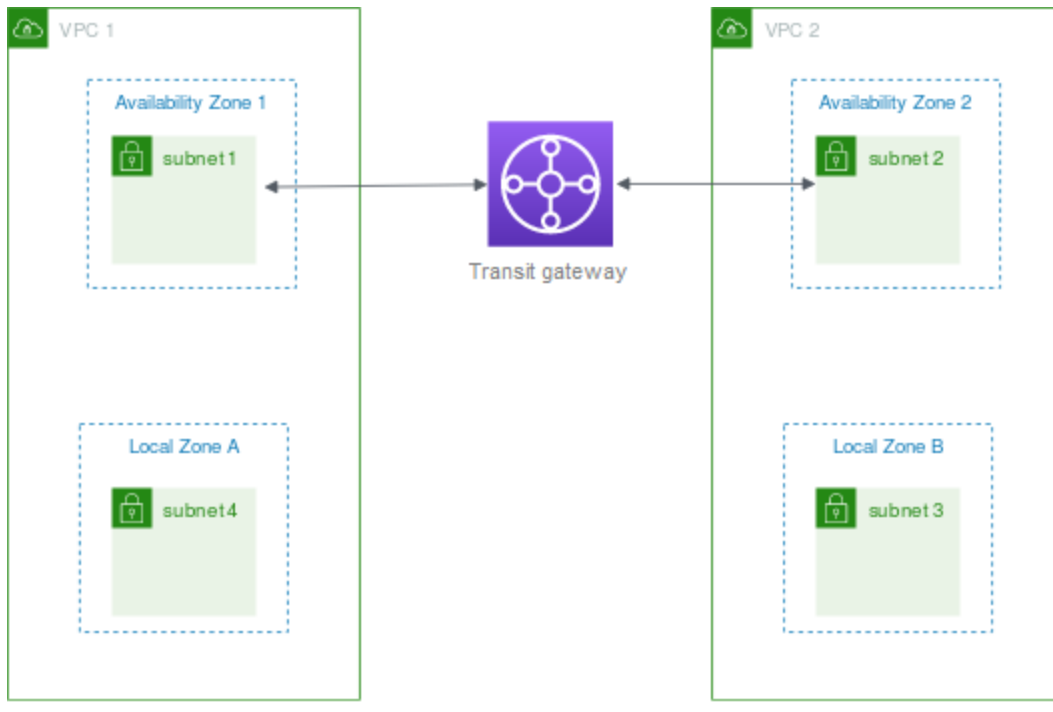
- Sebuah gateway Direct Connect. Untuk informasi tentang cara membuat gateway Direct Connect, lihat [Membuat gateway Direct Connect](#) di Panduan Pengguna AWS Direct Connect .
- Pengaitan virtual private gateway untuk menghubungkan VPC ke gateway Direct Connect. Untuk informasi tentang cara membuat pengaitan virtual private gateway, lihat [Mengaitkan dan memisahkan virtual private gateway](#) di Panduan Pengguna AWS Direct Connect .
- Antarmuka virtual pribadi pada koneksi dari AWS 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 AWS 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 mengkonfigurasi jaringan Anda sehingga subnet di Zona Lokal terhubung ke gateway transit melalui Availability Zone induk. Buat subnet di Local Zones dan subnet di Availability Zones induk. Hubungkan subnet di Availability Zones induk ke gateway transit, lalu buat rute di tabel rute untuk setiap VPC yang merutekan lalu lintas yang ditujukan untuk CIDR VPC 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:

- 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 Gateway Transit VPC Amazon](#).
- Lampiran gateway transit untuk setiap VPC menggunakan Availability Zone induk. Untuk informasi selengkapnya, lihat [Membuat lampiran gateway transit ke VPC di Gateway Transit VPC Amazon](#).
- Sebuah tabel rute transit gateway yang terkait dengan transit gateway attachment. Untuk informasi selengkapnya, lihat [Tabel rute gateway transit](#) di Amazon VPC Transit Gateways.
- Untuk setiap VPC, entri dalam tabel rute subnet subnet dari subnet Zona Lokal yang memiliki CIDR VPC lain 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
<i>VPC 1 CIDR</i>	<i>local</i>
<i>VPC 2 CIDR</i>	<i>vpc1-attachment-network-interface-id</i>

Berikut ini adalah contoh tabel rute untuk VPC 2.

Tujuan	Target
<i>VPC 2 CIDR</i>	<i>local</i>
<i>VPC 1 CIDR</i>	<i>vpc2-attachment-network-interface-id</i>

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

CIDR	Lampiran	Jenis rute
<i>VPC 1 CIDR</i>	<i>Attachment for VPC 1</i>	diperbanyak
<i>VPC 2 CIDR</i>	<i>Attachment for VPC 2</i>	diperbanyak

Subnet 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 virtual private cloud (VPC) ke satu atau beberapa Wavelength Zone, dan kemudian menggunakan sumber daya AWS seperti EC2 instans Amazon untuk menjalankan aplikasi yang memerlukan latensi ultra-rendah dan terhubung ke di Wilayah. Layanan AWS

Untuk menggunakan Wavelength Zones, Anda harus terlebih dahulu memilih Zona tersebut. Selanjutnya, membuat subnet di Zona Wavelength. Anda dapat membuat EC2 instans Amazon, volume Amazon EBS, dan subnet VPC Amazon serta gateway operator di Zona Wavelength. Anda juga dapat menggunakan layanan yang mengatur atau bekerja dengan EC2, EBS, dan VPC, seperti Amazon EC2 Auto Scaling, Amazon EKS cluster, Amazon ECS cluster, Amazon Systems Manager, Amazon EC2 , dan. CloudWatch AWS CloudTrail AWS CloudFormation Layanan di Wavelength adalah bagian dari VPC yang terhubung melalui koneksi bandwidth tinggi yang andal ke Wilayah untuk AWS 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.
- Saat Anda meluncurkan EC2 instance di subnet di Wavelength Zone, 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 Wavelength Zones memiliki komponen jaringan yang sama dengan subnet di Availability Zones, IPv4 termasuk alamat, set opsi DHCP, dan jaringan. ACLs

- Anda tidak dapat membuat lampiran gateway transit ke subnet di Wavelength Zone. Sebagai gantinya, buat lampiran melalui subnet di Availability Zone induk, lalu rutekan lalu lintas ke tujuan yang diinginkan melalui gateway transit. Sebagai contoh, lihat bagian berikut.

Pertimbangan untuk beberapa Wavelength

EC2 instance yang berada di Zona Wavelength yang berbeda di VPC yang sama tidak diizinkan untuk berkomunikasi satu sama lain. Jika Anda membutuhkan komunikasi Wavelength Zone to Wavelength Zone, rekomendasikan agar Anda menggunakan beberapa AWS , satu untuk setiap Wavelength Zone. VPCs Anda dapat menggunakan gateway transit untuk menghubungkan VPCs. Konfigurasi ini memungkinkan komunikasi antar instans di Wavelength Zones.

Rute lalu lintas Wavelength Zone ke Wavelength Zone melalui Wilayah. AWS 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:

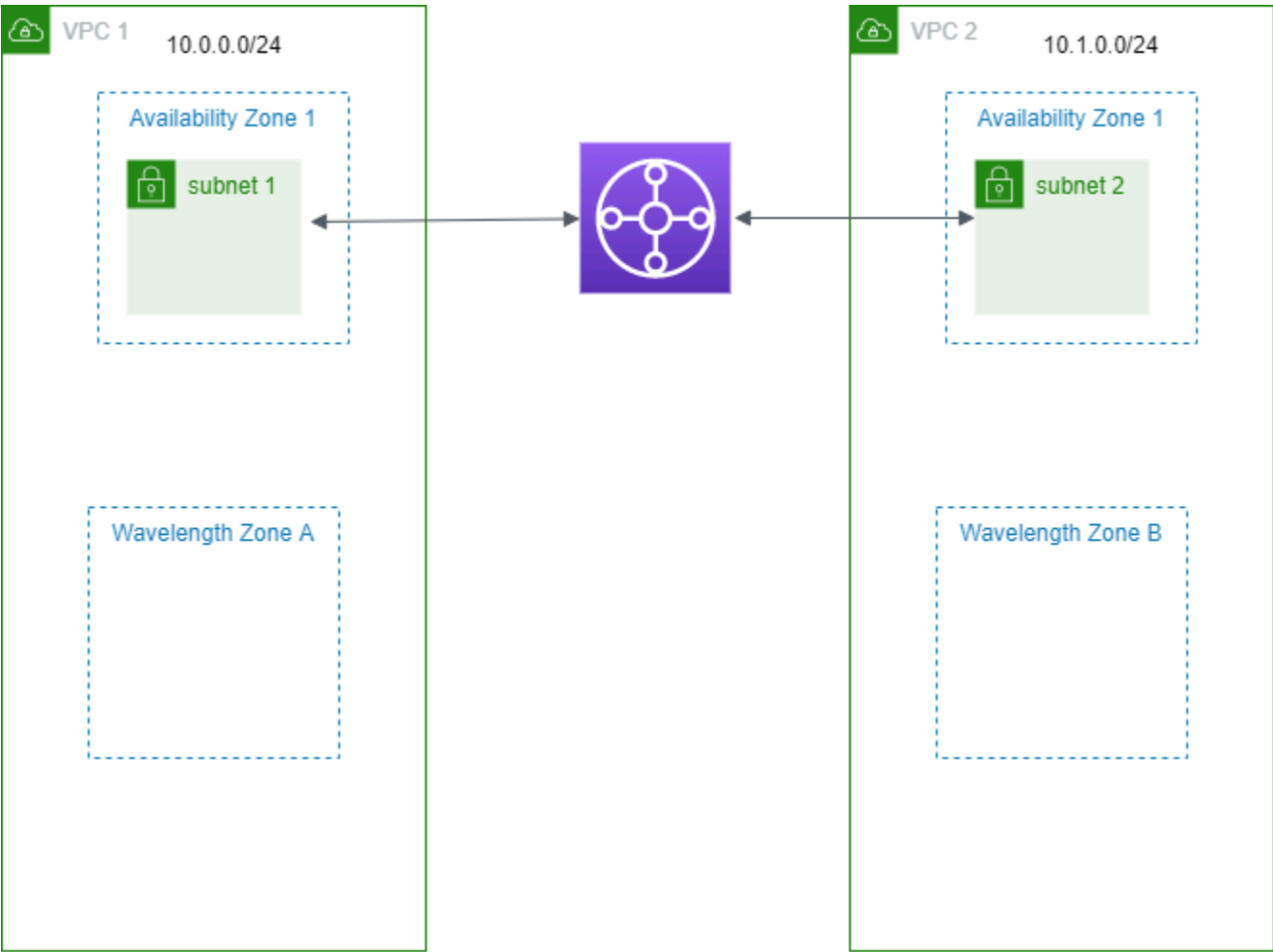
- Untuk setiap Zona Wavelength, subnet di Availability Zone yang merupakan Availability Zone induk untuk Zona Wavelength. Misalnya, Anda membuat subnet 1 dan subnet 2. Untuk informasi tentang membuat subnet, lihat [the section called “Membuat subnet”](#). Gunakan [describe-availability-zones](#) perintah untuk menemukan zona induk.
- Transit gateway. Gerbang transit menghubungkan VPCs. 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 Availability Zone induk dari Wavelength Zone. Untuk informasi selengkapnya, lihat [Lampiran gateway transit ke VPC](#) di Panduan Gerbang Transit VPC Amazon.
- 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-222222222222222222

Misalnya, tabel rute untuk VPC 2 memiliki entri berikut:

Tujuan	Target
10.0.0.0/24	tgw-222222222222222222



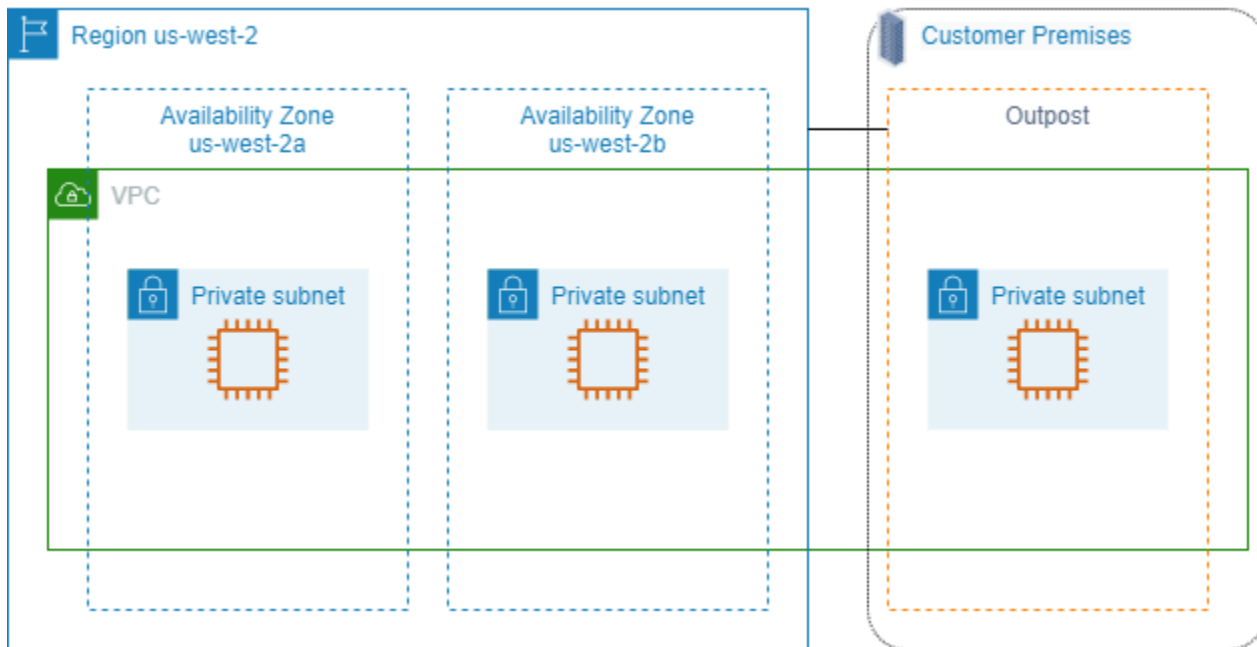
Subnet di AWS Outposts

AWS Outposts menawarkan infrastruktur, layanan APIs, dan alat AWS perangkat keras yang sama untuk membangun dan menjalankan aplikasi Anda di tempat 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 Availability Zone di suatu Wilayah. AWS Setelah Anda menghubungkan Outpost Anda ke Wilayah induknya, Anda dapat memperluas VPC apa pun di Wilayah ke Pos Luar Anda dengan membuat subnet untuk Outpost di VPC tersebut.

Aturan berikut berlaku untuk AWS Outposts:

- Subnet harus berada di satu lokasi Outpost.
- Anda membuat subnet untuk Outpost dengan menentukan Amazon Resource Name (ARN) dari Outpost saat Anda membuat subnet.
- Outposts rack - Gateway lokal menangani konektivitas jaringan antara VPC dan jaringan lokal. Untuk informasi selengkapnya, lihat [Gateway lokal](#) di rak Panduan AWS Outposts Pengguna untuk Outposts.
- Server Outposts - 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 Outposts.
- Secara default, setiap subnet yang Anda buat di VPC, termasuk subnet untuk Outposts Anda, secara implisit terkait dengan tabel rute utama untuk VPC. Atau, Anda dapat secara eksplisit mengaitkan tabel rute kustom dengan subnet di VPC Anda dan memiliki gateway lokal sebagai target lompatan berikutnya 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 VPC Amazon 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-group](#) perintah.

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

2. Hapus setiap ACL jaringan dengan menggunakan [delete-network-acl](#) perintah.

```
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-table](#) perintah.

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

5. Lepaskan gateway internet Anda dari VPC Anda dengan menggunakan [detach-internet-gateway](#) perintah.

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

6. Hapus gateway internet Anda dengan menggunakan [delete-internet-gateway](#) perintah.

```
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 ewgw-id
```

8. Hapus VPC Anda dengan menggunakan perintah [delete-vpc](#).

```
aws ec2 delete-vpc --vpc-id vpc-id
```

Hasilkan infrastructure-as-code 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 pilihan Anda infrastructure-as-code (IaC) untuk tindakan yang Anda inginkan. Karena alur kerja konsol memastikan nilai parameter yang Anda tentukan valid bersama-sama, kode yang Anda hasilkan dengan menggunakan Console-to-Code memiliki nilai parameter yang kompatibel. Anda dapat menggunakan kode sebagai titik awal, dan kemudian menyesuaikannya untuk membuatnya siap produksi untuk kasus penggunaan spesifik Anda.

Misalnya, dengan Console-to-Code Anda dapat merekam diri sendiri menggunakan konsol VPC untuk membuat subnet, grup keamanan, tabel perutean khusus NACLs, dan gateway internet dan menghasilkan kode dalam format JSON. AWS CloudFormation Kemudian, Anda dapat menyalin kode itu dan menyesuaikannya untuk digunakan dalam AWS 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 YAMB

Untuk informasi selengkapnya dan petunjuk tentang cara menggunakan Console-to-Code, lihat [Mengotomatisasi AWS layanan dengan Pengembang Amazon Q 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 EC2 instance, dalam 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](#)
- [Konfigurasi 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:

- IPv4 hanya — Subnet memiliki blok IPv4 CIDR tetapi tidak memiliki blok IPv6 CIDR. Sumber daya dalam subnet IPv4 -only harus berkomunikasi. IPv4
- Dual stack — Subnet memiliki blok IPv4 CIDR dan blok IPv6 CIDR. VPC harus memiliki blok CIDR dan blok IPv4 CIDR. IPv6 Sumber daya dalam subnet dual-stack dapat berkomunikasi berulang kali. IPv4 IPv6
- IPv6 hanya — Subnet memiliki blok IPv6 CIDR tetapi tidak memiliki blok IPv4 CIDR. VPC harus memiliki blok IPv6 CIDR. Sumber daya dalam subnet IPv6 -only harus berkomunikasi. IPv6

Note

Sumber daya dalam subnet IPv6 -only diberi alamat IPv4 link-lokal dari blok CIDR. 169.254.0.0/16 Alamat ini digunakan untuk berkomunikasi dengan layanan yang hanya tersedia di VPC. Sebagai contoh, lihat [Alamat tautan-lokal](#) di EC2 Panduan Pengguna Amazon.

Untuk informasi selengkapnya, lihat [Alamat IP untuk Anda VPCs dan subnet](#).

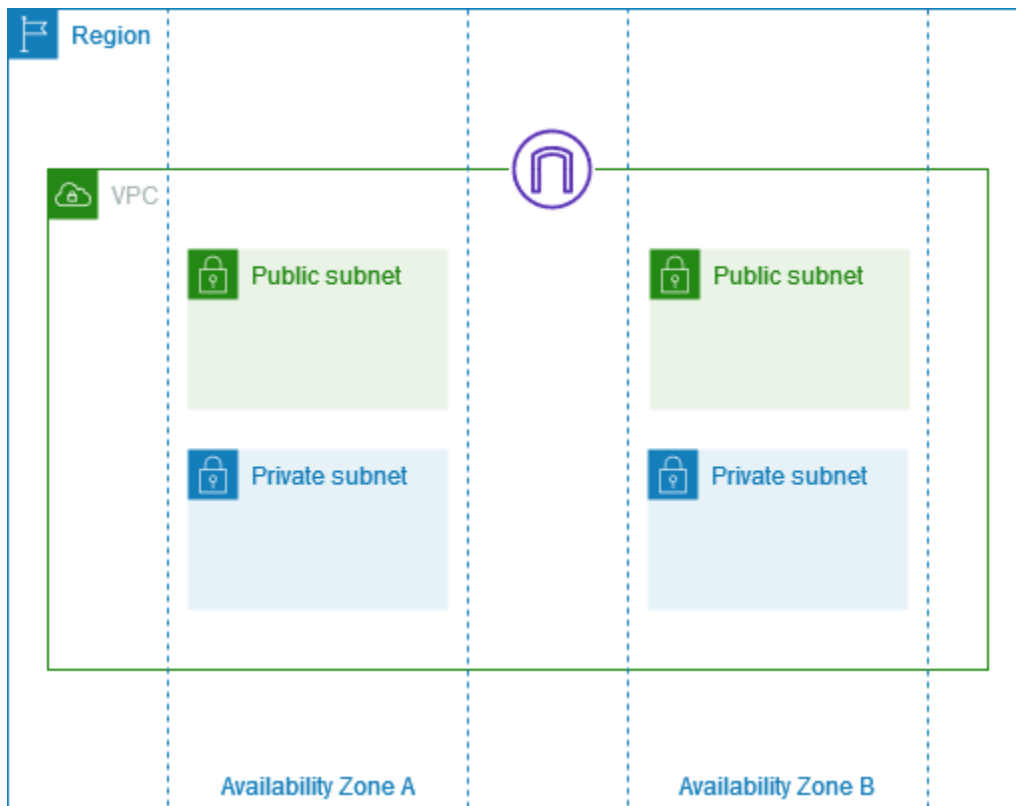
Jenis subnet

Jenis subnet ditentukan oleh bagaimana Anda mengkonfigurasi routing untuk subnet Anda. Misalnya:

- 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.
- Subnet khusus VPN — 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 [Konfigurasi tabel rute](#).

Pengaturan subnet

Semua subnet memiliki atribut yang dapat dimodifikasi yang menentukan apakah antarmuka jaringan yang dibuat di subnet tersebut diberi IPv4 alamat 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:

- Pengaturan IP tetapkan otomatis: Memungkinkan Anda mengonfigurasi pengaturan IP penetapan otomatis untuk secara otomatis meminta publik IPv4 atau IPv6 alamat untuk antarmuka jaringan baru di subnet ini.
- Pengaturan Nama Berbasis Sumber Daya (RBN): Memungkinkan Anda menentukan jenis nama host untuk EC2 instance di subnet ini dan mengonfigurasi bagaimana kueri catatan DNS A dan AAAA ditangani. Untuk informasi selengkapnya, lihat [jenis nama host EC2 instans Amazon](#) di Panduan EC2 Pengguna Amazon.

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 EC2 instance, 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 EC2 instance. Jaringan ACLs memungkinkan atau menolak lalu lintas masuk dan keluar di tingkat subnet. Dalam kebanyakan kasus, kelompok keamanan dapat memenuhi kebutuhan Anda. Namun, Anda dapat menggunakan jaringan ACLs jika Anda menginginkan lapisan keamanan tambahan. Untuk informasi selengkapnya, lihat [the section called “Bandingkan grup keamanan dan jaringan ACLs”](#).

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 jaringan khusus ACLs 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 [Mencatat lalu lintas IP menggunakan VPC Flow Logs](#).

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 [Alamat IP untuk Anda VPCs dan subnet](#).
- 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 VPC Amazon 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 selanjutnya

Setelah Anda membuat subnet, Anda dapat mengkonfigurasinya sebagai berikut:

- Konfigurasi 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 [Konfigurasi 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. Untuk informasi selengkapnya, lihat [???](#).

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 Amazon VPC 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 ke `false`, 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 menetakannya 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. Pilihan 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. Ketika Anda menyimpan beberapa rentang CIDR dalam VPC yang sama, rentang CIDR tersebut 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.

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-reservation](#) untuk 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-reservations](#) untuk melihat detail reservasi CIDR subnet.

```
aws ec2 get-subnet-cidr-reservations --subnet-id subnet-05ee9fb78EXAMPLE
```

Menghapus reservasi CIDR subnet

Anda dapat menggunakan [delete-subnet-cidr-reservation](#) untuk menghapus reservasi CIDR subnet.

```
aws ec2 delete-subnet-cidr-reservation --subnet-cidr-reservation-id scr-044f977c4eEXAMPLE
```

Konfigurasi tabel rute

Tabel rute berfungsi sebagai pengontrol lalu lintas untuk virtual private cloud (VPC) Anda. 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 jaringan lain VPCs atau 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 diarahkan ke target berdasarkan alamat IP tujuannya. Tabel rute memungkinkan Anda membuat arsitektur jaringan kompleks yang mencakup subnet publik, subnet pribadi, subnet khusus VPN, dan subnet terisolasi.

Daftar Isi

- [Konsep tabel rute](#)
- [Tabel rute subnet](#)
- [Tabel rute gateway](#)
- [Bagaimana prioritas rute bekerja](#)
- [Opsi perutean contoh](#)
- [Buat tabel rute untuk VPC Anda](#)
- [Mengelola 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 dinamis di VPC Anda menggunakan VPC Route Server](#)
- [Memecahkan masalah keterjangkauan di VPC Anda](#)

Konsep tabel rute

Berikut ini adalah konsep kunci untuk tabel rute:

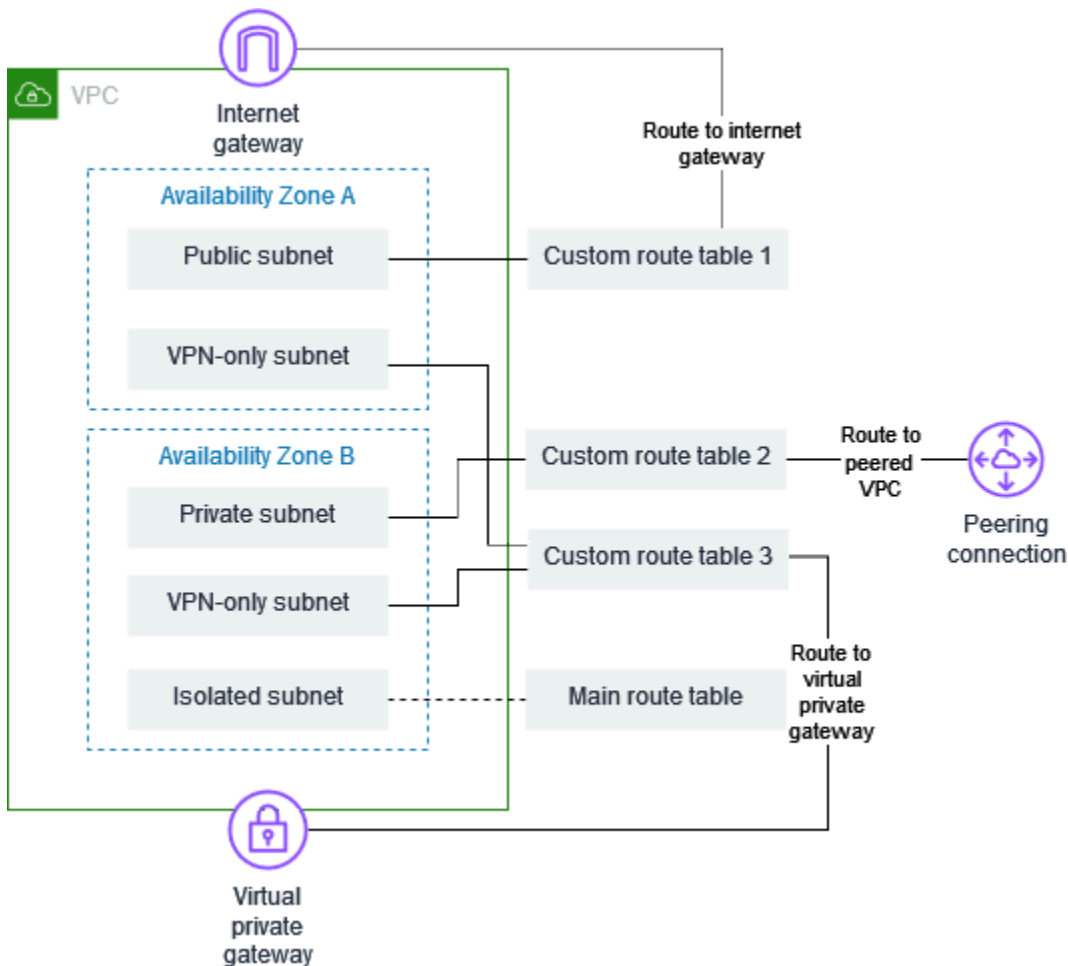
- Tabel rute utama—Tabel rute yang secara otomatis bawaan di VPC Anda. Tabel rute utama mengendalikan perutean untuk semua subnet yang tidak secara eksplisit dikaitkan dengan tabel rute lainnya.
- Tabel rute kustom—Tabel rute yang Anda buat untuk VPC Anda.
- Tujuan—Kisaran alamat IP di mana Anda menginginkan 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 keduanya IPv4 dan IPV6 alamat, 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 VPN](#) di Panduan Pengguna Site-to-Site 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 gerbang transit —Tabel rute yang terkait dengan gateway transit. Untuk informasi selengkapnya, lihat [Tabel rute gateway transit](#) di Amazon VPC Transit Gateways.
- Tabel rute gateway lokal—Tabel rute yang dikaitkan dengan gateway lokal Outposts. Untuk informasi selengkapnya, lihat [Gateway lokal](#) di AWS Outposts Panduan 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 Availability Zone A. Tabel rute kustom 2 memiliki rute ke VPC peered, dan dikaitkan dengan subnet pribadi di Availability Zone B. Tabel rute kustom 3 memiliki rute ke gateway pribadi virtual, dan dikaitkan dengan subnet khusus VPN di kedua Availability Zones.



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 adalah `0.0.0.0/0`, yang mewakili semua IPv4 alamat. Targetnya adalah gateway internet yang melekat pada VPC Anda.

Tujuan	Target
0.0.0.0/0	<i>igw-id</i>

Blok CIDR untuk IPv4 dan IPv6 diperlakukan secara terpisah. Misalnya, rute dengan CIDR tujuan `0.0.0.0/0` tidak secara otomatis menyertakan semua IPv6 alamat. Anda harus membuat rute dengan CIDR tujuan `::/0` untuk semua IPv6 alamat.

Jika Anda sering mereferensikan kumpulan blok CIDR yang sama di seluruh AWS sumber daya Anda, Anda dapat membuat [daftar awalan yang dikelola pelanggan](#) untuk mengelompokkannya 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 IPv4 CIDR, tabel rute Anda berisi rute lokal untuk setiap IPv4 blok CIDR. Jika Anda telah mengaitkan blok IPv6 CIDR dengan VPC Anda, tabel rute Anda berisi rute lokal untuk IPv6 blok CIDR. Anda dapat [mengganti atau mengembalikan](#) target setiap rute lokal sesuai kebutuhan.

Aturan dan pertimbangan

- Anda dapat menambahkan rute ke tabel rute Anda yang lebih spesifik daripada rute lokal. Tujuan harus cocok dengan seluruh IPv4 atau IPv6 CIDR blok 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 IPv4 alamat 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 EC2 instance, seperti Layanan Metadata Instans (IMDS) dan server DNS Amazon. Anda dapat menggunakan blok CIDR yang lebih besar dari tetapi tumpang tindih 169.254.168.0/22, tetapi paket yang ditujukan untuk alamat di 169.254.168.0/22 tidak akan diteruskan.

- Anda tidak dapat menambahkan rute ke IPv6 alamat yang sama persis atau subset dari rentang berikut: fd00:ec2: :/32. Rentang ini berada dalam ruang alamat lokal unik (ULA) dan dicadangkan untuk digunakan oleh AWS layanan. Misalnya, Amazon EC2 menggunakan alamat dalam rentang ini untuk layanan yang hanya dapat diakses dari EC2 instance, seperti Layanan Metadata Instans (IMDS) dan server DNS Amazon. 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 perutean untuk VPC Anda. Untuk informasi selengkapnya, lihat [the section called “Perutean untuk perangkat middlebox”](#).

Contoh

Dalam contoh berikut, misalkan VPC memiliki blok CIDR dan blok IPv4 CIDR. IPv6 IPv4 dan IPv6 lalu lintas 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-aabbccdde1122334

- IPv4 lalu lintas yang akan diarahkan dalam VPC (10.0.0.0/16) dicakup oleh rute. Local
- IPv6 lalu lintas yang akan diarahkan dalam VPC (2001:db 8:1234:1 a00: :/56) dicakup oleh rute. Local
- Rute untuk 172.31.0.0/16 mengirimkan lalu lintas ke koneksi peering.

- Rute untuk semua IPv4 lalu lintas (0.0.0.0/0) mengirimkan lalu lintas ke gateway internet. Oleh karena itu, semua IPv4 lalu lintas, kecuali untuk lalu lintas dalam VPC dan ke koneksi peering, diarahkan ke gateway internet.
- Rute untuk semua IPv6 lalu lintas (:: /0) mengirimkan lalu lintas ke gateway internet khusus egres. Oleh karena itu, semua IPv6 lalu lintas, kecuali lalu lintas di dalam VPC, dialihkan ke gateway internet khusus egres.

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 Route di konsol VPC Amazon, 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](#) dan 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](#) dan 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.

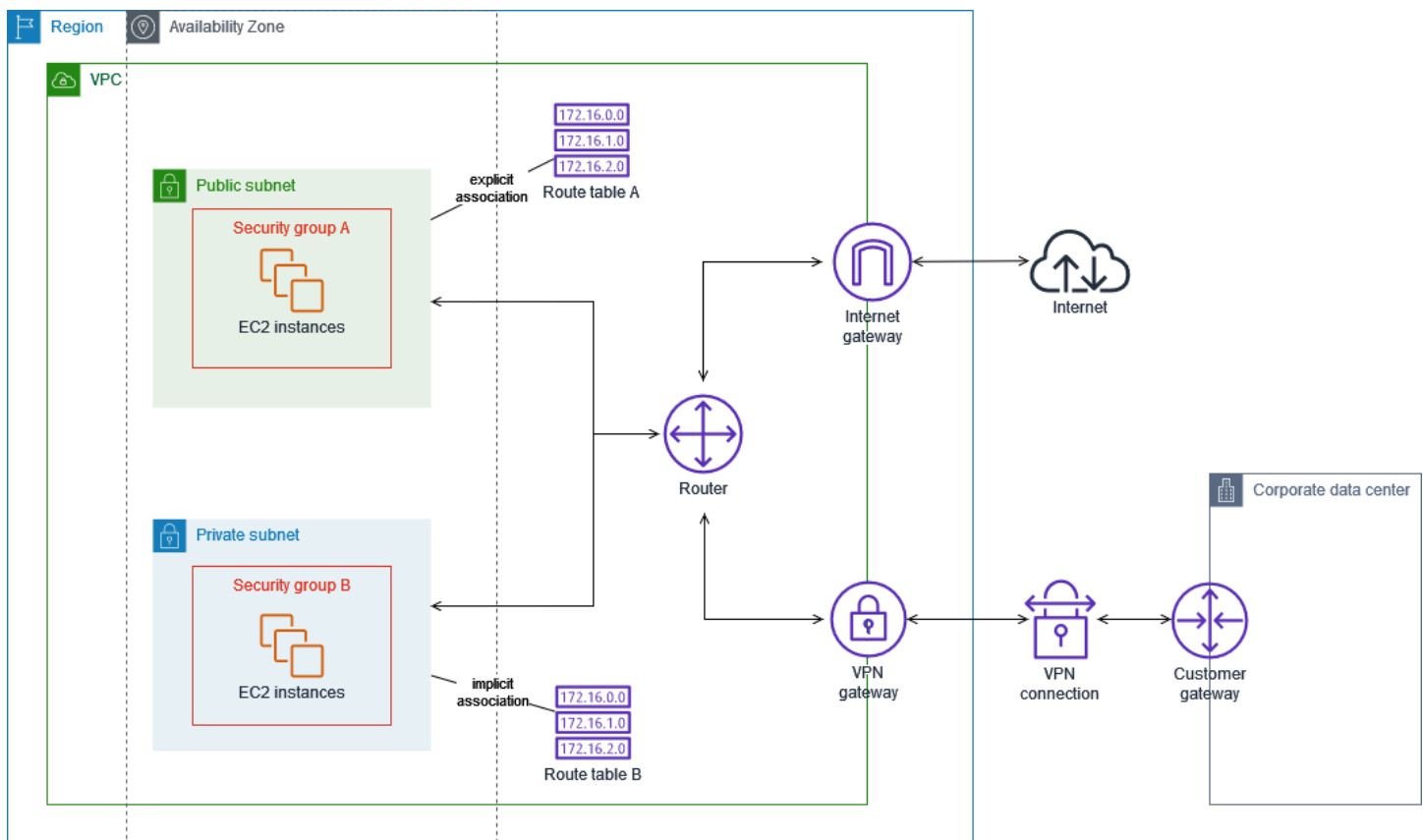
Pengaitan tabel rute subnet

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 VPCs terkait dengan Outposts dapat memiliki jenis target tambahan dari gateway lokal. Ini adalah satu-satunya perbedaan perutean dari subnet non-Outposts.

Contoh 1: pengaitan subnet implisit dan eksplisit

Diagram berikut menunjukkan perutean untuk VPC dengan gateway internet, virtual private gateway, subnet publik, dan subnet VPN saja.



Route table A adalah tabel rute kustom 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
<i>VPC CIDR</i>	Lokal:
0.0.0.0/0	<i>igw-id</i>

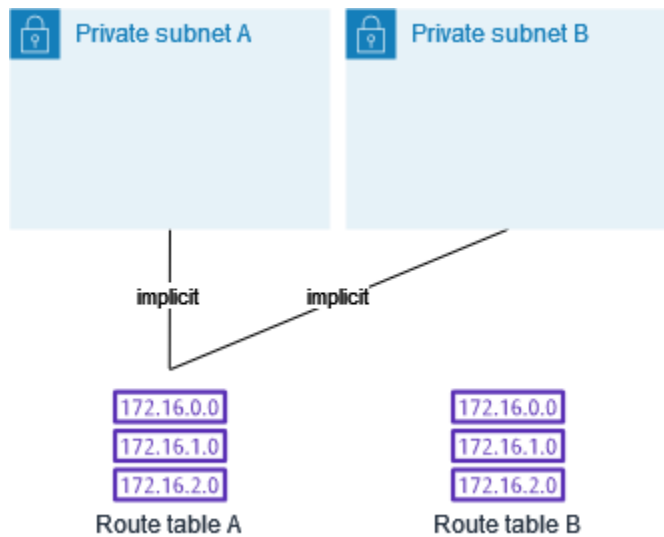
Tabel rute B adalah tabel rute utama. Ini secara implisit terkait dengan subnet pribadi. Ini memiliki rute yang mengirimkan semua lalu lintas ke gateway pribadi virtual, tetapi tidak ada rute ke gateway internet, yang membuat subnet menjadi subnet khusus VPN. Jika Anda membuat subnet lain di VPC ini dan tidak mengaitkan tabel rute khusus, subnet juga akan secara implisit dikaitkan dengan tabel rute ini karena ini adalah tabel rute utama.

Tujuan	Target
<i>VPC CIDR</i>	Lokal:
0.0.0.0/0	<i>vgw-id</i>

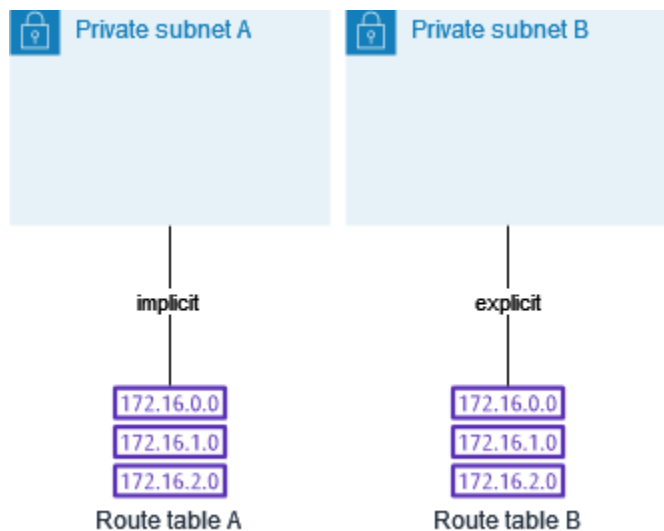
Contoh 2: Mengganti tabel rute utama

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.

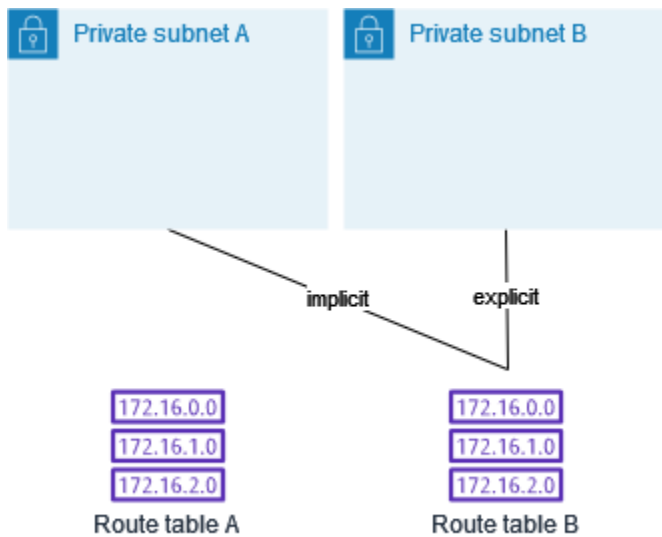
Diagram berikut menunjukkan dua subnet dan dua tabel rute. Subnet A secara implisit dikaitkan dengan tabel rute A, tabel rute utama. Subnet B secara implisit terkait dengan tabel rute A. Tabel rute B, tabel rute khusus, tidak terkait dengan subnet mana pun.



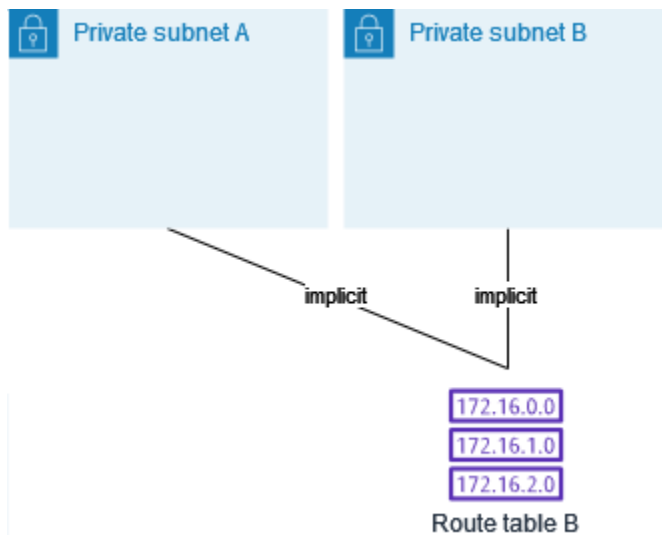
Untuk mengganti tabel rute utama, mulailah dengan membuat asosiasi eksplisit antara subnet B dan tabel rute B. Tabel rute uji B.



Setelah Anda menguji tabel rute B, jadikan tabel rute utama. Subnet B masih memiliki asosiasi 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 subnet mana pun.



(Opsional) Jika Anda memisahkan subnet B dari tabel rute B, masih ada hubungan implisit antara subnet B dan tabel rute B. Jika Anda tidak lagi membutuhkan 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 mencegah 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 [Load Balancer 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 [Load Balancer Gateway](#)
- Antarmuka jaringan untuk alat middlebox

Ketika target adalah titik akhir Penyeimbang Beban Gateway atau antarmuka jaringan, tujuan berikut diperbolehkan:

- Seluruh IPv4 atau IPv6 CIDR blok VPC Anda. Dalam kasus ini, Anda ganti target rute lokal default.
- Seluruh IPv4 atau IPv6 CIDR blok 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	<i>eni-id</i>

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	<i>eni-id</i>

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 “Ops perutean contoh”](#).
- Anda tidak dapat menentukan daftar prefiks sebagai tujuan.
- Anda tidak dapat menggunakan tabel rute gateway untuk mengendalikan atau mencegah 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 itu. Lalu lintas yang ditujukan untuk alamat MAC dari antarmuka jaringan lain di subnet menggunakan perutean data link (lapisan 2) alih-alih jaringan (lapisan 3) sehingga aturan tidak berlaku untuk lalu lintas ini.
- Tidak semua Local Zones mendukung asosiasi tepi dengan gateway pribadi virtual. Untuk informasi selengkapnya tentang zona yang tersedia, lihat [Pertimbangan](#) di Panduan Pengguna AWS Local Zones.

Bagaimana prioritas rute bekerja

Secara umum, kami mengarahkan lalu lintas menggunakan rute paling spesifik yang cocok dengan lalu lintas. Ini dikenal sebagai kecocokan 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 pengintipan VPC dan koneksi gateway internet)
3. [Rute daftar awalan](#)
4. [Rute yang diperbanyak](#)
 - a. Rute Direct Connect BGP (rute dinamis)
 - b. Rute statis VPN
 - c. Rute VPN BGP (rute dinamis) (seperti gateway pribadi virtual)

Pertandingan awalan terpanjang

Rute ke IPv4 dan IPv6 alamat atau blok CIDR tidak tergantung satu sama lain. Kami menggunakan rute paling spesifik yang cocok dengan IPv4 lalu lintas atau lalu IPv6 lintas untuk menentukan cara merutekan lalu lintas.

Contoh tabel rute subnet berikut memiliki rute untuk lalu lintas IPv4 internet (`0.0.0.0/0`) yang menunjuk ke gateway internet, dan rute untuk `172.31.0.0/16` IPv4 lalu lintas 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
<code>10.0.0.0/16</code>	lokal
<code>172.31.0.0/16</code>	<code>pcx-11223344556677889</code>
<code>0.0.0.0/0</code>	<code>igw-12345678901234567</code>

Prioritas rute untuk rute statis dan dinamis yang disebar

Jika Anda telah melampirkan gateway pribadi virtual ke VPC Anda dan mengaktifkan propagasi rute pada tabel rute subnet Anda, rute yang mewakili koneksi Site-to-Site VPN Anda secara otomatis muncul sebagai rute yang disebar di tabel rute Anda.

Jika tujuan rute yang disebar identik dengan tujuan rute statis, rute statis akan 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 disebar ke gateway pribadi virtual. Kedua rute memiliki tujuan `172.31.0.0/24`. Karena rute statis ke gateway internet diprioritaskan, semua lalu lintas yang `172.31.0.0/24` ditujukan untuk diarahkan ke gateway internet.

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 Anda berisi rute propagasi 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 rute tersebut adalah rute yang disebar, 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](#)
- [Routing ke gateway AWS Outposts 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 melakukan ini, buat dan lampirkan gateway internet ke VPC Anda, lalu tambahkan rute dengan tujuan `0.0.0.0/0` untuk IPv4 lalu lintas atau `::/0` IPv6 lalu lintas, dan target ID gateway internet (`igw-xxxxxxxxxxxxxxxxxx`).

Tujuan	Target
0.0.0.0/0	<i>igw-id</i>
::/0	<i>igw-id</i>

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 merutekan lalu lintas IPv4 internet (`0.0.0.0/0`) ke perangkat NAT.

Tujuan	Target
0.0.0.0/0	<i>nat-gateway-id</i>

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-xxxxxxx, daftar awalan yang berisi rentang alamat IP untuk Amazon S3 di Wilayah tertentu) dirutekan ke titik akhir VPC gateway, dan lalu lintas 10.25.0.0/16 dirutekan 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	<i>nat-gateway-id</i>
pl- <i>xxxxxxx</i>	<i>vpce-id</i>
10.25.0.0/16	<i>pcx-id</i>

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-xxxxxxxxxxxxxxxxxxxx).

Tujuan	Target
10.0.0.0/16	<i>vgw-id</i>

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 IPv6 lalu lintas. Namun, kami mendukung IPv6 lalu lintas yang diarahkan melalui gateway pribadi virtual ke AWS Direct Connect koneksi. Untuk informasi selengkapnya, silakan lihat [Panduan Pengguna AWS Direct Connect](#).

Routing ke gateway AWS Outposts lokal

Bagian ini menjelaskan konfigurasi tabel routing untuk routing ke gateway lokal. AWS Outposts

Daftar Isi

- [Aktifkan lalu lintas antara subnet Outpost dan jaringan lokal Anda](#)
- [Aktifkan lalu lintas antar subnet di VPC yang sama di Outposts](#)

Aktifkan lalu lintas antara subnet Outpost dan jaringan lokal Anda

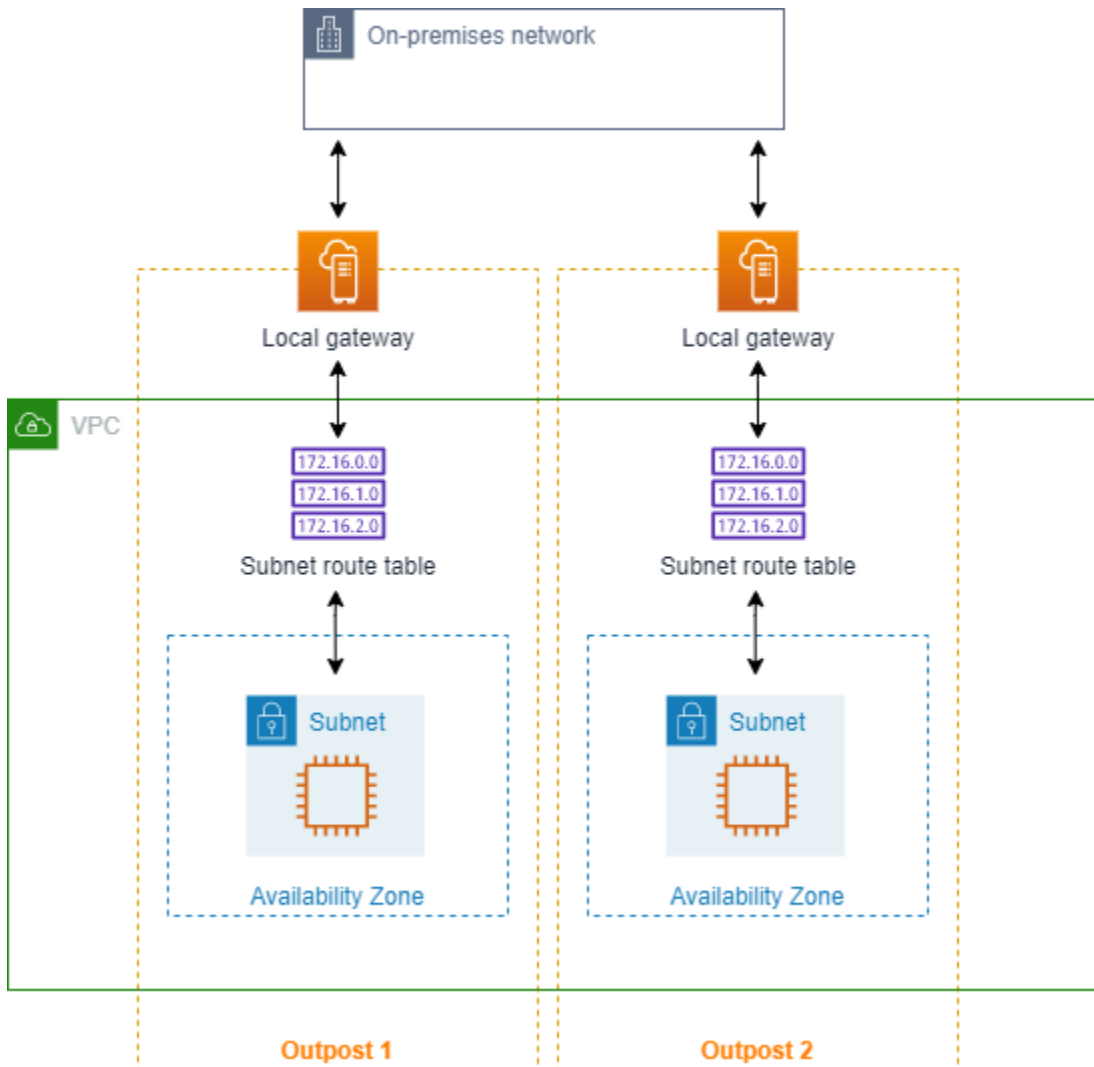
Subnet yang VPCs terkait dengan AWS Outposts dapat memiliki jenis target tambahan dari gateway lokal. Pertimbangkan kasus di mana Anda ingin memiliki lalu lintas rute gateway lokal dengan alamat tujuan 192.168.10.0/24 ke jaringan pelanggan. Untuk melakukannya, tambahkan rute berikut dengan jaringan tujuan dan target gateway lokal (*lgw-xxxx*).

Tujuan	Target
192.168.10.0/24	<i>lgw-id</i>

Aktifkan lalu lintas antar subnet di VPC yang sama di Outposts

Anda dapat menjalin komunikasi antara subnet yang berada di VPC yang sama di berbagai Outposts menggunakan gateway lokal Outpost dan jaringan lokal Anda.

Anda dapat menggunakan fitur ini untuk membangun arsitektur yang mirip dengan arsitektur Multi-availability Zone (AZ) untuk aplikasi on-premise Anda yang berjalan di rak Outposts dengan membangun konektivitas antara rak Outposts yang ditambahkan ke yang berbeda. AZs



Untuk mengaktifkan fitur ini, tambahkan rute ke tabel rute subnet rak Outpost Anda yang lebih spesifik daripada rute lokal di tabel rute tersebut dan memiliki tipe target gateway lokal. Tujuan rute harus sesuai dengan seluruh IPv4 blok 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 on-premise 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 dalam subnet Outpost. Anda tidak dapat menggunakan grup keamanan IDs.
- Rak Outposts yang ada mungkin memerlukan pembaruan untuk mengaktifkan dukungan komunikasi intra-VPC di beberapa Outposts. Jika fitur ini tidak berfungsi untuk Anda, [hubungi AWS Support](#).

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	<i>lgw-1-id</i>

Entri untuk tabel rute subnet Outpost 2 adalah sebagai berikut:

Tujuan	Target
10.0.0.0/16	Lokal
10.0.1.0/24	<i>lgw-2-id</i>

Perutean ke koneksi peering VPC

Koneksi peering VPC adalah koneksi jaringan antara dua VPCs yang memungkinkan Anda untuk merutekan lalu lintas di antara mereka menggunakan alamat pribadi. IPv4 Instans-instans di VPC yang manapun dapat berkomunikasi satu sama lain seolah-olah mereka berada di jaringan yang sama.

Untuk mengaktifkan perutean lalu lintas antara VPCs koneksi peering VPC, Anda harus menambahkan rute ke satu atau lebih tabel rute subnet Anda yang menunjuk 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) antara dua VPCs, 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 antara VPCs dan mengizinkan akses ke seluruh blok IPv4 CIDR dari salah satu VPC, 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 mendukung IPv6 komunikasi antar instans di VPCs, jika instans VPCs dan instans diaktifkan untuk komunikasi. IPv6 Untuk mengaktifkan perutean IPv6 lalu lintas antara VPCs, Anda harus menambahkan rute ke tabel rute Anda yang menunjuk ke koneksi peering VPC untuk mengakses semua atau sebagian blok CIDR dari IPv6 VPC rekan.

Misalnya, menggunakan koneksi peering VPC yang sama (pcx-11223344556677889) di atas, asumsikan VPCs memiliki informasi berikut:

- VPC A: Blok IPv6 CIDR adalah 2001:db8:1234:1a00::/56
- VPC B: Blok IPv6 CIDR adalah 2001:db8:5678:2b00::/56

Untuk mengaktifkan IPv6 komunikasi 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 (p1-**xxxxxxxx**), dan target dengan ID titik akhir (vpce-**xxxxxxxxxxxxxxxxxxxx**). 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. Sebuah gateway internet egress-only digunakan untuk IPv6 lalu lintas saja. Untuk mengonfigurasi perutean untuk gateway internet khusus egress, tambahkan rute di tabel rute subnet pribadi yang merutekan lalu lintas IPv6 internet (: : /0) ke gateway internet khusus egress.

Tujuan	Target
::/0	<i>eigw-id</i>

Untuk informasi selengkapnya, lihat [Aktifkan IPv6 lalu lintas keluar menggunakan gateway internet khusus egress-only](#).

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 VPCs yang melekat pada gateway transit. 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 VPCs, dengan informasi berikut:

- VPC A: 10.1.0.0/16, ID lampiran tgw-attach-111111111111111111
- VPC B: 10.2.0.0/16, ID lampiran tgw-attach-222222222222222222

Untuk mengaktifkan lalu lintas antara VPCs dan mengizinkan akses ke gateway transit, tabel rute VPC A dikonfigurasi sebagai berikut.

Tujuan	Target
10.1.0.0/16	Lokal
10.0.0.0/8	<i>tgw-id</i>

Berikut ini adalah contoh entri tabel rute Transit Gateway untuk pelampiran VPC.

Tujuan	Target
10.1.0.0/16	tgw-attach-111111111111111111
10.2.0.0/16	tgw-attach-222222222222222222

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 perutean untuk VPC Anda. Berikut ini adalah kemungkinan kasus penggunaan:

- Mencegat 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 perutean 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”](#).
- Lalu lintas langsung antara dua subnet ke alat middlebox. Anda dapat melakukannya dengan membuat rute untuk satu tabel rute subnet yang cocok dengan subnet CIDR dari subnet lainnya dan menentukan titik akhir Gateway Load Balancer, gateway NAT, titik akhir Network Firewall, atau antarmuka jaringan untuk alat sebagai target. Atau, untuk mengarahkan semua lalu lintas dari subnet ke subnet lainnya, 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. Alat ini digunakan sebagai EC2 instans Amazon di subnet di VPC Anda, dan diwakili oleh elastic network interface (network interface) 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 disebar. 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 AWS 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 routing middlebox, lihat. [Skenario Middlebox](#)

Daftar Isi

- [Pertimbangan perangkat](#)
- [Merutekan lalu lintas antara gateway dan alat](#)
- [Merutekan lalu lintas antar-subnet ke alat](#)

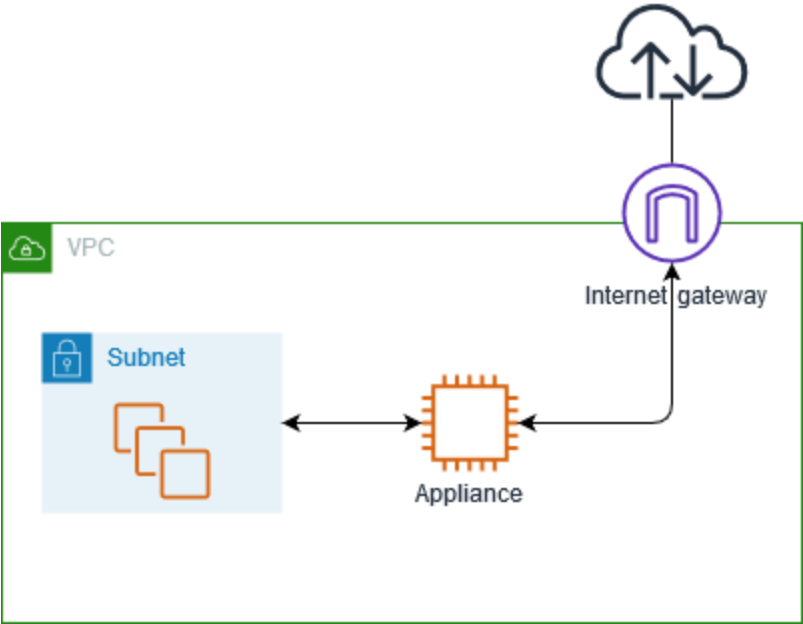
Pertimbangan perangkat

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 pemeriksaan pada alat. Untuk informasi selengkapnya, lihat [Mengubah Pemeriksaan Sumber atau Tujuan](#) di Panduan EC2 Pengguna Amazon.
- 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 Anda yang lebih spesifik daripada rute lokal. Anda dapat menggunakan rute yang lebih spesifik untuk mengarahkan lalu lintas antar subnet dalam VPC (lalu lintas Timur-Barat) ke alat middlebox. Tujuan rute harus cocok dengan seluruh IPv4 atau IPv6 CIDR blok subnet di VPC Anda.
- Untuk mencegah IPv6 lalu lintas, pastikan VPC, subnet, dan alat Anda mendukung. IPv6

Merutekan 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 IPv4 lalu lintas yang ditujukan untuk subnet ke antarmuka jaringan untuk alat. Rute ini lebih spesifik daripada rute lokal.

Tujuan	Target
<i>VPC CIDR</i>	Lokal:
<i>Subnet CIDR</i>	<i>Appliance network interface ID</i>

Atau, Anda dapat mengganti target untuk rute lokal dengan antarmuka jaringan alat. Anda dapat melakukan ini untuk memastikan bahwa semua lalu lintas secara otomatis diarahkan ke alat, termasuk lalu lintas yang ditujukan untuk subnet yang Anda tambahkan ke VPC di masa mendatang.

Tujuan	Target
<i>VPC CIDR</i>	<i>Appliance network interface ID</i>

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 IPv4 alamat) untuk tujuan.

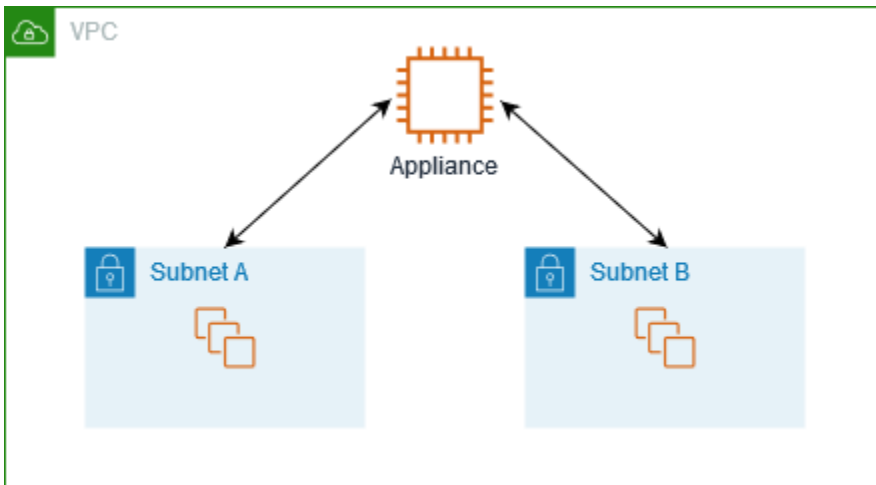
Tujuan	Target
<i>VPC CIDR</i>	Lokal:
<code>0.0.0.0/0</code>	<i>Appliance network interface ID</i>

Kemudian, dalam tabel rute yang terkait dengan subnet alat, tambahkan rute yang mengirim lalu lintas kembali ke gateway internet atau gateway pribadi virtual.

Tujuan	Target
<i>VPC CIDR</i>	Lokal:
<code>0.0.0.0/0</code>	<i>igw-id</i>

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 antar subnet dialihkan melalui alat.



Grup keamanan

Saat Anda merutekan lalu lintas antar instance di subnet yang berbeda melalui perangkat middlebox, grup keamanan untuk kedua instance harus mengizinkan lalu lintas mengalir di antara instance. 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
<i>VPC CIDR</i>	Lokal:
<i>Subnet B CIDR</i>	<i>Appliance network interface ID</i>

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
<i>VPC CIDR</i>	Lokal:
<i>Subnet A CIDR</i>	<i>Appliance network interface ID</i>

Atau, Anda dapat mengganti target untuk rute lokal dengan antarmuka jaringan alat. Anda dapat melakukan ini untuk memastikan bahwa semua lalu lintas secara otomatis diarahkan ke alat, termasuk lalu lintas yang ditujukan untuk subnet yang Anda tambahkan ke VPC di masa mendatang.

Tujuan	Target
<i>VPC CIDR</i>	<i>Appliance network interface ID</i>

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 mengelompokkannya 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. VPCs 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	<i>tgw-id</i>

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 Load Balancer Gateway, mengonfigurasi layanan [titik akhir Load Balancer Gateway](#), dan kemudian membuat [titik akhir Load Balancer Gateway 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 belakang Load Balancer Gateway, lihat [the 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 Load Balancer Gateway, tambahkan rute berikut.

Tujuan	Target
10.0.1.0/24	<i>vpc-endpoint-id</i>

Saat menggunakan titik akhir Load Balancer Gateway 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-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](#)
- [Kaitkan 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](#).

Kaitkan 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 untuk dikaitkan dengan tabel rute.
5. Pilih Simpan pengaitan.

Untuk mengaitkan atau memisahkan subnet dengan tabel rute menggunakan AWS CLI

- [associate-route-table](#)
- [disassociate-route-table](#)

Mengelola tabel rute subnet

Gunakan prosedur berikut untuk mengelola perutean 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 rutanya. Untuk menentukan apakah asosiasi ke tabel rute utama, dan jika asosiasi itu eksplisit, lihat [Tentukan 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 terkait dengan tabel rute. Subnet di bawah Subnet tanpa asosiasi eksplisit termasuk dalam VPC yang sama dengan tabel rute, tetapi tidak terkait dengan tabel rute apa pun, sehingga 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 Asosiasi tepi.

Untuk mendeskripsikan satu atau beberapa 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

- 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, satu alamat IP, atau ID daftar awalan. Untuk Target, pilih jenis sumber daya lalu 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 Hapus.
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 VPN](#) di Panduan Pengguna Site-to-Site 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

- [enable-vgw-route-propagation](#)
- [disable-vgw-route-propagation](#)

Ubah tabel rute untuk subnet

Anda dapat mengubah pengaitan tabel rute untuk subnet.

Ketika Anda mengubah tabel rute, koneksi yang ada di subnet diiadakan 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 Route, 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 VPC Amazon di. <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Tabel rute, lalu pilih tabel rute utama yang baru.
3. Pilih Tindakan, Atur 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 VPC Amazon di. <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Tabel rute, lalu pilih tabel rute.
3. Dari tab Asosiasi 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 memisahkan gateway dengan tabel rute menggunakan konsol

1. Buka konsol VPC Amazon 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 batal 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 VPC Amazon 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 VPC Amazon 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 dinamis di VPC Anda menggunakan VPC Route Server

Amazon VPC Route Server menyederhanakan perutean untuk lalu lintas antara beban kerja yang digunakan dalam VPC dan gateway internetnya. Dengan fitur ini, VPC Route Server secara dinamis memperbarui VPC dan tabel rute gateway internet dengan pilihan IPv4 atau IPv6 rute Anda untuk mencapai toleransi kesalahan perutean untuk beban kerja tersebut. Ini memungkinkan Anda untuk secara otomatis mengalihkan lalu lintas dalam VPC, yang meningkatkan pengelolaan perutean 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 dalam tabel rute gateway transit, gunakan [Transit Gateway Connect](#).

Kuota

Untuk kuota yang terkait dengan Amazon VPC Route Server, [lihat Kuota server rute](#).

Penetapan Harga

Untuk informasi tentang biaya yang terkait dengan Amazon VPC Route Server, lihat tab [VPC Route Server](#) di halaman harga Amazon VPC.

Daftar Isi

- [Terminologi](#)
- [Cara kerja Server Rute VPC Amazon](#)
- [Rute server peer logging](#)
- [Mulai tutorial](#)

Terminologi

Istilah-istilah berikut digunakan dalam panduan ini:

- FIB: [Forwarding Information Base \(FIB\)](#) berfungsi sebagai tabel penerusan untuk rute apa yang telah ditentukan oleh server rute adalah rute jalur terbaik di RIB setelah mengevaluasi semua informasi dan kebijakan perutean 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-rekan BGP. RIB terus diperbarui saat informasi perutean baru diterima atau rute yang ada berubah. Ini memastikan bahwa server rute selalu memiliki pandangan terkini dari topologi jaringan dan dapat membuat keputusan routing yang optimal.
- Server rute: Komponen server rute memperbarui tabel rute VPC dan gateway internet Anda dengan IPv6 rute IPv4 atau di Basis Informasi Penerusan (FIB) Anda. Server rute mewakili satu FIB 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 memfasilitasi koneksi [BGP \(Border Gateway Protocol\)](#) antara server rute Anda dan rekan BGP Anda.
- Route server peer: 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 sebuah instance). EC2 Perangkat harus memenuhi persyaratan ini:
 - Memiliki elastic network interface di VPC
 - Support BGP (Border Gateway Protocol)
 - Dapat memulai sesi BGP
- Propagasi server rute: Saat diaktifkan, propagasi server rute menginstal rute di FIB pada tabel rute yang telah Anda tentukan. Dukungan server rute IPv4 dan propagasi IPv6 rute.

Cara kerja Server Rute VPC Amazon

Bagian ini menjelaskan cara kerja Amazon VPC Route Server dan membantu Anda memahami cara kerjanya mencapai toleransi kesalahan perutean untuk beban kerja Anda yang berjalan di subnet.

Daftar Isi

- [Gambaran Umum](#)
- [Diagram](#)

Gambaran Umum

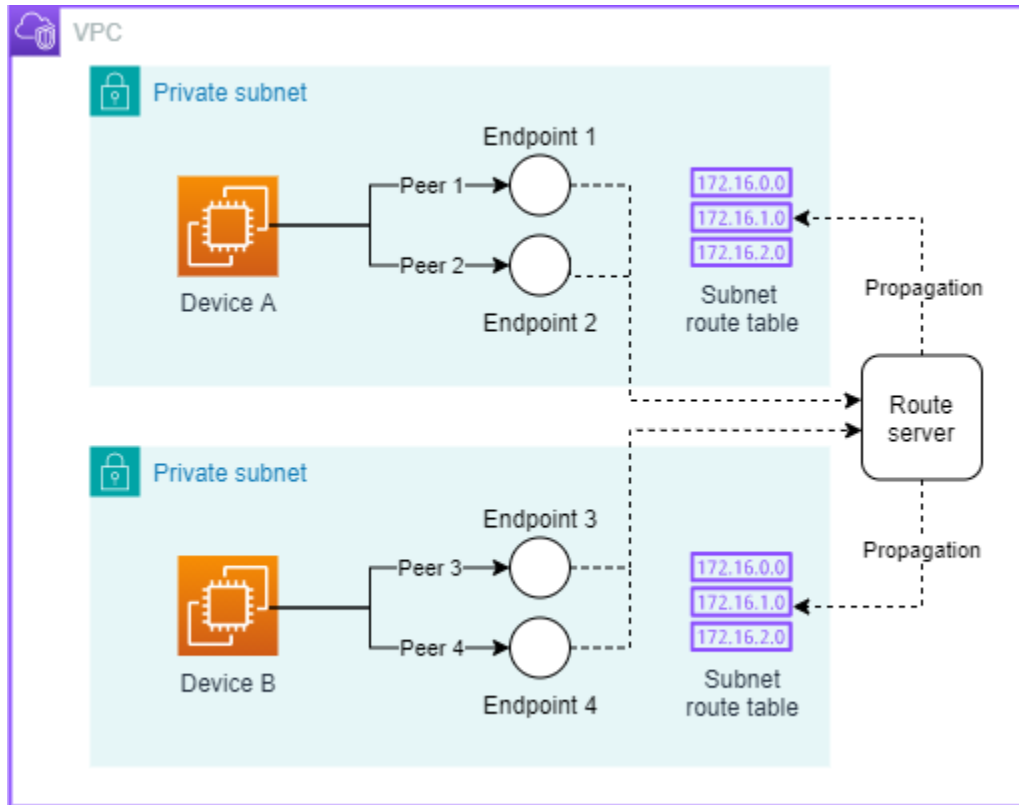
Cara kerja Server Rute VPC Amazon:

1. Anda mengonfigurasi perangkat jaringan (seperti firewall yang berjalan pada EC2 instance di VPC) untuk menggunakan Amazon VPC Route Server.
2. Perangkat jaringan gagal.
3. Titik akhir server rute mendeteksi kegagalan melalui [BFD \(Deteksi Penerusan Dua Arah\)](#) yang dikonfigurasi pada rekan server rute.
4. Titik akhir server rute memperbarui server rute untuk menarik rute di [Basis Informasi Perutean \(RIB\)](#) di mana perangkat yang gagal adalah lompatan berikutnya.
5. Server rute menghitung [Forwarding Information Base \(FIB\) dari RIB](#), memilih rute terbaik yang tersedia.
6. Server rute memperbarui tabel rute yang dikonfigurasi dengan rute dari FIB.

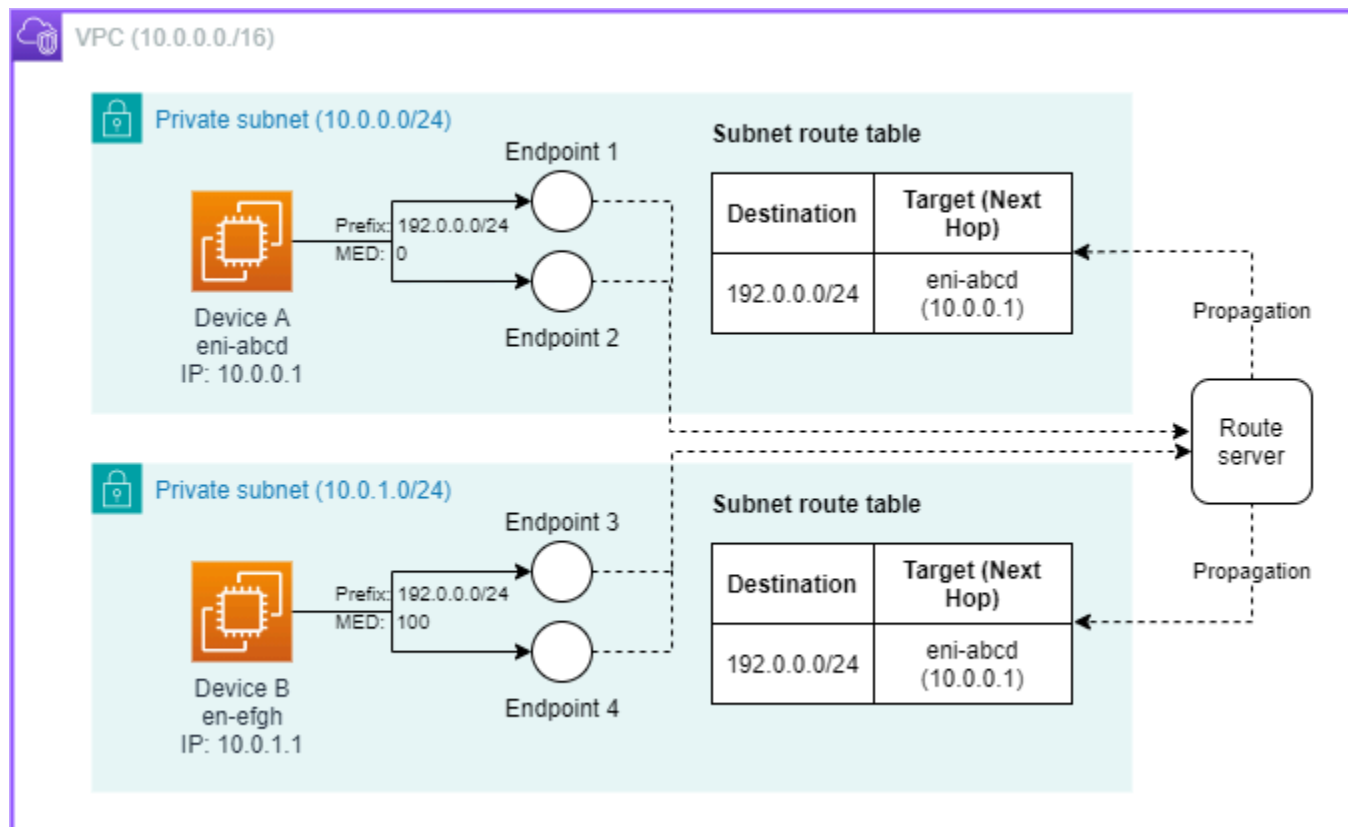
7. Semua lalu lintas baru diteruskan ke perangkat siaga.

Diagram

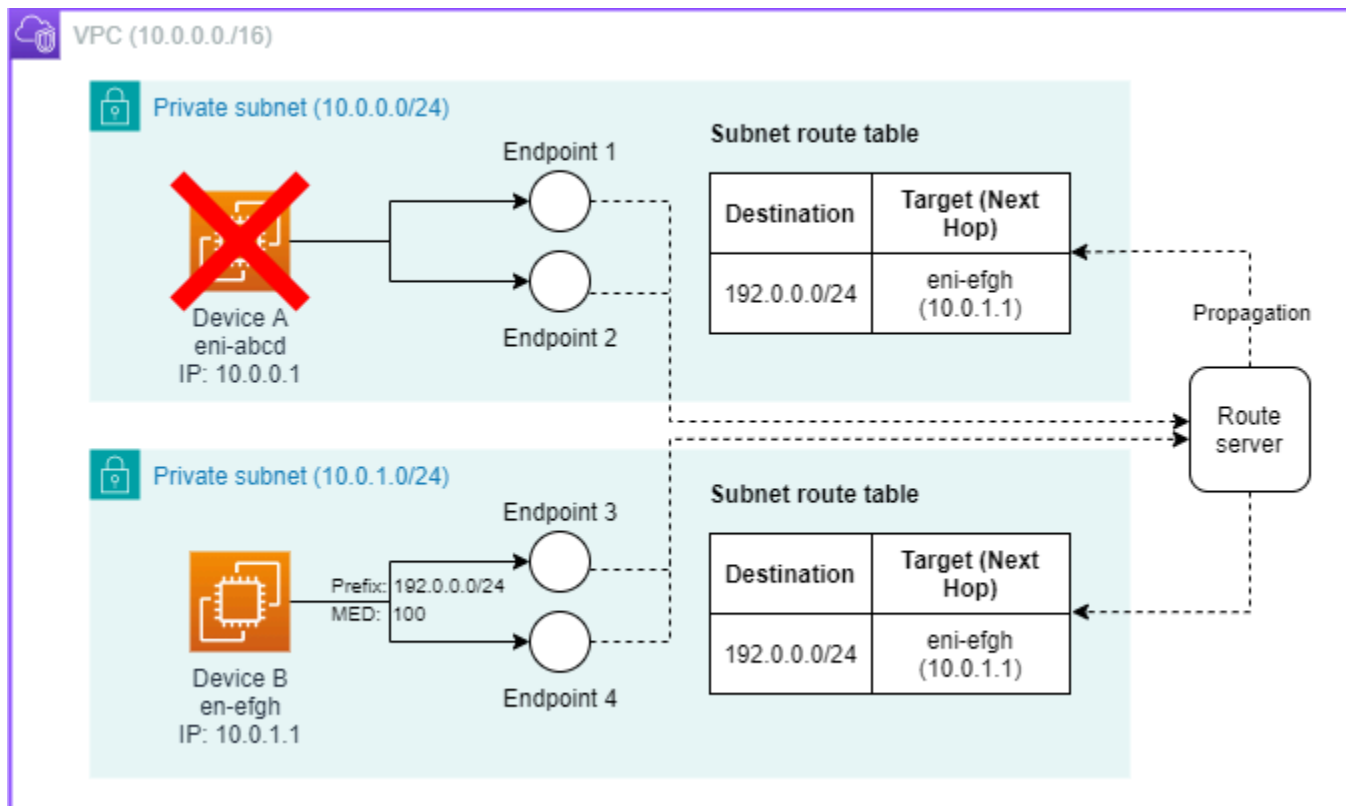
Berikut ini adalah contoh diagram server rute VPC dengan titik akhir server rute yang dikonfigurasi untuk perangkat dalam dua subnet.



Dimulai dengan contoh di atas sebagai garis dasar, 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 MED (Multi-Exit 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 itu di tabel rute subnet dengan antarmuka jaringan Perangkat A sebagai “lompatan berikutnya”. Akibatnya, setiap lalu lintas dalam subnet dengan IP tujuan dalam kisaran 192.0.0.0/24 dikirim ke Perangkat A. Perangkat A kemudian memproses lalu lintas dan mengirimkannya ke depan. Lalu lintas dalam 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 ini-abcd (10.0.0.1) sebagai lompatan berikutnya.



Contoh terakhir di bawah ini menunjukkan bagaimana server rute 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) turun, server rute memperbarui tabel rute subnet, dan lalu lintas ke 192.0.0.0/24 dirutekan ke Perangkat B eni-efgh (10.0.1.1) sebagai lompatan berikutnya.



Route server peer logging

Gunakan peer logging VPC Route Server saat Anda perlu:

- Memantau kesehatan sesi BGP dan BFD
- Memecahkan masalah koneksi
- Tinjau perubahan sesi historis
- Lacak status jaringan

Harga

- CloudWatch: Biaya konsumsi data dan arsip untuk log vended berlaku saat Anda mempublikasikan log peer server rute ke Log. CloudWatch
- S3: Biaya konsumsi data dan arsip untuk log vended berlaku saat Anda mempublikasikan log peer server rute ke Amazon S3.
- Data Firehose: Biaya konsumsi dan pengiriman standar berlaku.

Vending logs adalah log dari AWS layanan tertentu yang tersedia dengan harga berjenjang volume dan dikirimkan ke CloudWatch Log, Amazon S3, atau Amazon Data Firehose. Untuk informasi selengkapnya, buka [CloudWatchHarga Amazon](#), pilih Log dan temukan Log Terjual.

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:

- `resource_arn`Ini adalah ARN untuk peer server rute.
- `event_timestamp`Ini adalah stempel waktu acara.
- `type`Peristiwa log yang kami hasilkan (RouteStatus,BGPStatus,BFDStatus).
- `status`Bidang adalah pembaruan status.
 - Untuk pesan RouteStatus tipe
 - ADVERTISED(rute diiklankan oleh rekan)
 - UPDATED(rute yang ada diperbarui oleh rekan)
 - WITHDRAWN(rute ditarik oleh rekan)

- Untuk BFDStatus dan BGPStatus update
 - UP, DOWN.
- messageBidang 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 VPC Amazon di. <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, di bawah Virtual private cloud, pilih Route server.
3. Pada halaman Route server, pilih Route server peer.
4. Pilih tab Pengiriman log.
5. Pilih Tambahkan pengiriman log.
6. Pilih tujuan dan konfigurasi pengaturan:
 - CloudWatch Log Amazon
 - Jenis log: Jenis log untuk 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-peers).
 - Pemilihan 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
 - Cross account - Mengirim log ke AWS akun yang berbeda
 - Jenis log: Jenis log untuk 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

- Pemilihan bidang: Bidang data untuk disertakan dalam log Anda.
- Akhiran: Akhir ditambahkan ke nama file log (contoh: .log, .txt).
- Kompatibel dengan HIVE: Saat diaktifkan, mengatur log dalam struktur folder yang berfungsi dengan alat berbasis HIVE untuk pencarian yang lebih mudah dengan layanan seperti Amazon Athena.
- Pembatas bidang: Saat menggunakan format Teks, ini adalah karakter yang memisahkan bidang.
- Di akun saat ini
 - Jenis log: Jenis log untuk 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.
 - Pemilihan bidang: Bidang data untuk disertakan dalam log Anda.
 - Akhiran: Akhir ditambahkan ke nama file log (contoh: .log, .txt).
 - Kompatibel dengan HIVE: Saat diaktifkan, mengatur log dalam struktur folder yang berfungsi dengan alat berbasis HIVE untuk pencarian yang lebih mudah.
 - Pembatas bidang: Saat menggunakan format Teks, ini adalah karakter yang memisahkan bidang.
- Amazon Data Firehose
 - Lintas akun
 - Jenis log: Jenis log untuk dikirimkan. Satu-satunya jenis log yang didukung adalah EVENT_LOGS.
 - Tujuan pengiriman ARN: Nama Sumber Daya Amazon dari aliran pengiriman Firehose di akun lain. AWS
 - Pemilihan bidang: Bidang data untuk disertakan dalam log Anda.
 - Pembatas bidang: Saat menggunakan format Teks, ini adalah karakter yang memisahkan bidang.
 - Di akun saat ini
 - Jenis log: Jenis log untuk dikirimkan. Satu-satunya jenis log yang didukung adalah EVENT_LOGS.
 - Aliran tujuan pengiriman: Aliran pengiriman Firehose di akun Anda tempat log akan dikirim. Aliran harus menggunakan tipe sumber "Direct Put".

- Pemilihan 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 menautkan ke dokumentasi Referensi AWS CLI. 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 perutean dinamis di VPC Anda. Anda akan belajar cara membuat dan mengkonfigurasi semua komponen yang diperlukan, membuat peering BGP, dan memverifikasi operasi yang benar. Tutorial ini mencakup semuanya mulai dari penyiapan IAM awal hingga pengujian dan pembersihan.

Sebelum memulai tutorial ini, pastikan Anda memiliki:

- Akses administratif ke AWS akun Anda
- VPC dengan setidaknya dua subnet di mana Anda ingin mengaktifkan perutean dinamis
- Perangkat jaringan (seperti firewall yang berjalan pada EC2 instance) yang mendukung BGP dan dapat berfungsi sebagai perangkat peer server rute
- Keakraban dasar dengan konsep dan jaringan BGP AWS

Langkah-langkah dapat diselesaikan menggunakan AWS Management Console atau AWS CLI. Kedua metode disediakan untuk setiap langkah.

Perkiraan waktu untuk menyelesaikan: 15-30 menit

Langkah-langkah

- [Langkah 1: Konfigurasi izin Peran IAM yang diperlukan](#)
- [Langkah 2: Buat server rute](#)
- [Langkah 3: Kaitkan server rute dengan VPC](#)
- [Langkah 4: Buat titik akhir server rute](#)
- [Langkah 5: Aktifkan propagasi server rute](#)

- [Langkah 6: Buat rekan 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 tentang izin 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 IPv6 rute IPv4 atau di Basis Informasi Penerusan (FIB) Anda. Server rute mewakili satu FIB dan Routing Information Base (RIB).

AWS Management Console

Untuk membuat server rute

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, di bawah Virtual private cloud, pilih Route server.
3. Pada halaman Route server, pilih Buat server rute.
4. Pada halaman Buat server rute, konfigurasi pengaturan berikut:
 - Untuk Nama, masukkan nama untuk server rute Anda (mis., "my-route-server-01"). Nama harus 255 karakter atau kurang panjangnya.
 - Untuk Amazon Side ASN, masukkan nilai BGP ASN. Nilai ini harus berada di kisaran 1-4294967295. Sebaiknya gunakan ASN pribadi dalam rentang 64512—65534 (ASN 16-bit) atau 4200000000—4294967294 (ASN 32-bit).
 - Untuk rute Persista, pilih Aktifkan atau Nonaktifkan. 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 ketika semua sesi BGP berakhir
 - Jika Anda mengaktifkan rute tetap, untuk durasi Bertahan, 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 rutenya sebelum server rute melanjutkan fungsionalitas 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, alihkan sakelar Aktifkan notifikasi SNS. Mengaktifkan pemberitahuan SNS tetap ada 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 tanda.
6. Tinjau pengaturan Anda dan pilih Buat server rute.
7. Tunggu server rute dibuat. Setelah selesai, Anda akan diarahkan ke halaman server Route, di mana Anda dapat melihat server rute baru Anda terdaftar dengan status Tersedia.

Command line

Gunakan prosedur berikut untuk membuat server rute baru untuk mengelola perutean dinamis di VPC.

Untuk `--amazon-side-asn`, masukkan nilai BGP ASN. Nilai ini harus berada di kisaran 1-4294967295. Sebaiknya gunakan ASN pribadi dalam rentang 64512—65534 (ASN 16-bit) 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"
  }
}
```

Detail pemberitahuan SNS

Tabel berikut menunjukkan detail tentang pesan yang akan dikirim oleh Amazon VPC Route Server menggunakan Amazon SNS:

Bidang standar		Atribut pesan (Metadata)			
Pesan	Ketika itu dikirim	stempel waktu	EventCode	routeServ erEndpointId	affectedR outeServe rPeerIds
Route Server Endpoint [ENDPOINT ID] sekarang sedang menjalani pemeliharaan. Sesi BFD dan BGP mungkin terpengaruh.	Pemeliharaan titik akhir server rute	Format: 2025-02-17T 15:55:00 Z	ROUTE_SER VER_ENDPO INT_MAINT ENANCE	ID titik akhir yang terpengaruh	Daftar rekan yang terkena dampak IDs
Pesan	Ketika itu dikirim	stempel waktu	EventCode	routeServ erPeerId	newBgpSta tus

Bidang standar		Atribut pesan (Metadata)			
BGP untuk Route Server Peer [PEER ID] sekarang [UP/DOWN].	Perubahan status BGP rekan server rute	Format: 2025-02-17T 15:55:00 Z	ROUTE_SERVER_PEER_BGP_STATUS_CHANGE	ID rekan yang terpengaruh	NAIK atau TURUN
Pesan	Ketika itu dikirim	stempel waktu	EventCode	routeServerPeerId	newBfdStatus
BFD untuk Route Server Peer [PEER ID] sekarang [UP/DOWN].	Perubahan status BFD rekan server rute	Format: 2025-02-17T 15:55:00 Z	ROUTE_SERVER_PEER_BFD_STATUS_CHANGE	ID rekan yang terpengaruh	NAIK atau TURUN

Langkah 3: Kaitkan 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.
- 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 keadaannya (seperti asosiasi dan terkait).
- Asosiasi dapat dihapus (dipisahkan) jika Anda tidak lagi ingin server rute beroperasi di VPC itu.

AWS Management Console

Kaitkan server rute dengan VPC

1. Buka konsol VPC Amazon di. <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, di bawah Virtual private cloud, pilih Route server.
3. Pilih server rute yang ingin Anda kaitkan dengan VPC.
4. Pada tab Asosiasi, pilih Server rute asosiasi.
5. Dalam kotak dialog Server rute asosiasi:
 - Bidang ID server Route 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 Terkait pada tab Asosiasi.

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 memfasilitasi koneksi [BGP \(Border Gateway Protocol\)](#) antara server rute Anda dan rekan BGP Anda.

Titik akhir server rute adalah “titik kontak” tempat 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 perutean 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 VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, di bawah Virtual private cloud, pilih Route server.

3. Pilih server rute yang ingin Anda buat titik akhir.
4. Di panel bawah, pilih tab Route server endpoints.
5. Pilih Buat titik akhir server rute.
6. Pada halaman Create route server endpoint, konfigurasi pengaturan berikut:
 - Untuk Nama, masukkan nama deskriptif untuk titik akhir Anda.
 - Untuk server Route, konfirmasi 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 hingga 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 Route untuk server rute Anda.
13. Verifikasi bahwa Anda melihat dua titik akhir yang 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. Dukungan server rute IPv4 dan propagasi IPv6 rute.

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 kunci dari 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
 - Menjaga konsistensi rute di seluruh tabel rute yang ditentukan
 - Memperbarui rute secara dinamis saat kondisi jaringan berubah
- Status
 - Dapat diaktifkan (rute sedang disebar)
 - Dapat dinonaktifkan (rute tidak disebar)

AWS Management Console

Untuk mengaktifkan propagasi server rute

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Pilih server rute yang ingin Anda aktifkan propagasi.
3. Pilih tab Propagations di panel rincian server rute.
4. Pilih Aktifkan propagasi.
5. Dalam dialog Aktifkan propagasi:
 - ID server Route akan diisi sebelumnya.
 - Di bawah tabel Route, pilih tabel rute tujuan dari menu tarik-turun untuk rute yang baru disebar.
6. Pilih Aktifkan propagasi untuk mengonfirmasi.
7. Tunggu status propagasi berubah menjadi Tersedia di daftar Propagasi.
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 hingga 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 rekan 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 sebuah EC2 instance). Perangkat harus memenuhi persyaratan ini:

- Memiliki elastic network interface di VPC
- Support BGP (Border Gateway Protocol)
- Dapat memulai sesi BGP

 Note

Kami menyarankan Anda membuat satu rute server peer per titik akhir server rute untuk redundansi.

AWS Management Console

Untuk membuat peer server rute

1. Buka konsol VPC Amazon di. <https://console.aws.amazon.com/vpc/>
2. Di jalur navigasi, pilih VPC > Route server peer > Create route server peer.
3. Di bawah Detail, konfigurasi hal berikut:
 - 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 rekan: Masukkan IPv4 alamat 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)
 - Deteksi 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 nilai kunci. Tag membantu mengidentifikasi dan melacak AWS sumber daya.
4. Tinjau pengaturan Anda dan pilih Buat rekan 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 hingga 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, konfigurasi 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 VPC Route Server berfungsi dengan memverifikasi bahwa tabel rute berisi rute terbaik yang disebarkan oleh server rute.

Langkah 8: Pembersihan

Bagian bangunan dari tutorial selesai. Selesaikan langkah-langkah di bagian ini untuk menghapus komponen VPC Route Server yang Anda buat.

7.1: Tarik iklan BGP di perangkat

Penarikan 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 VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Pilih server rute yang ingin Anda nonaktifkan propagasi.
3. Pilih Tindakan > Ubah server rute.
4. Pilih tab Propagations di panel rincian server rute.
5. Pilih propagasi yang ingin Anda nonaktifkan dan kemudian pilih Nonaktifkan propagasi.
6. Di kotak dialog, pilih Nonaktifkan 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 rekan-rekan server rute.

AWS Management Console

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di jalur navigasi, pilih Route server > Route server peer.
3. Pilih peer server rute.
4. Pilih Tindakan > Hapus rekan 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 VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Pilih server rute yang ingin Anda hapus titik akhir.
3. Pilih Rute titik akhir server.
4. Pilih endpoint dan pilih Actions > Delete route server endpoint.
5. Masukkan hapus dan pilih Hapus.

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: Pisahkan server rute dari VPC

Gunakan prosedur berikut untuk memisahkan server rute dari VPC.

AWS Management Console

1. Buka konsol VPC Amazon di. <https://console.aws.amazon.com/vpc/>
2. Pilih server rute yang ingin Anda pisahkan.
3. Pilih Asosiasi.
4. Pilih Pisahkan server rute.
5. Konfirmasikan perubahan yang akan dilakukan dan pilih Disassociate route server.

Command line

1. Putuskan server rute dari VPC:

```
aws ec2 disassociate-route-server --route-server-id rs-1 --vpc-id vpc-1
```

2. Konfirmasikan disosiasi:

```
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 VPC Amazon di. <https://console.aws.amazon.com/vpc/>
2. Pilih server rute yang akan dihapus.
3. Pilih Tindakan > Hapus server rute.
4. Masukkan hapus dan pilih Hapus.

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 hop-by-hop menghasilkan rincian 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 konfigurasi.

Untuk informasi selengkapnya, lihat Panduan [Reachability Analyzer](#).

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, EC2 instance Amazon 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

Ulasan [the 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 routing middlebox tersedia di file. Amazon Virtual Private Cloud Console

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 Amazon VPC 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 mengubah rute middlebox menggunakan wizard perutean middlebox

1. Buka konsol Amazon VPC 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 rutanya 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 pemeriksaan sumber/tujuan pada perangkat. Untuk informasi selengkapnya, lihat [Mengubah Pemeriksaan Sumber atau Tujuan](#) di Panduan EC2 Pengguna Amazon.
- 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 untuk menyesuaikan dan mengontrol perutean lalu lintas dalam jaringan virtual Anda. Salah satu fitur tersebut adalah wizard perutean middlebox, yang memungkinkan kontrol halus atas jalur perutean lalu lintas yang masuk atau keluar dari VPC Anda.

Jika Anda perlu mengarahkan 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 yang diperlukan (hop) untuk mengarahkan lalu lintas yang ditentukan sesuai kebutuhan, menghilangkan upaya manual yang diperlukan untuk mengatur konfigurasi perutean yang kompleks.

Wizard routing middlebox mendukung beberapa skenario berbeda. Misalnya, Anda dapat menggunakannya untuk memeriksa lalu lintas yang ditujukan untuk subnet tertentu, mengkonfigurasi 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 lanjutan, mengaktifkan pemantauan jaringan terpusat, atau mengoptimalkan kinerja aplikasi berbasis cloud Anda.

Contoh berikut menjelaskan skenario untuk wizard routing middlebox.

Daftar Isi

- [Periksa lalu lintas yang ditujukan untuk subnet](#)
- [Konfigurasi perutean dan inspeksi lalu lintas middlebox di VPC](#)
- [Periksa lalu lintas antar subnet](#)

Periksa lalu lintas yang ditujukan untuk subnet

Pertimbangkan skenario di mana Anda memiliki lalu lintas yang 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 sebuah instance. EC2 Alat firewall harus diinstal dan dikonfigurasi pada EC2 instance di subnet terpisah dari subnet B di VPC Anda, katakanlah subnet C. Anda kemudian dapat menggunakan wizard routing middlebox untuk mengkonfigurasi rute untuk lalu lintas antara subnet B dan gateway internet.

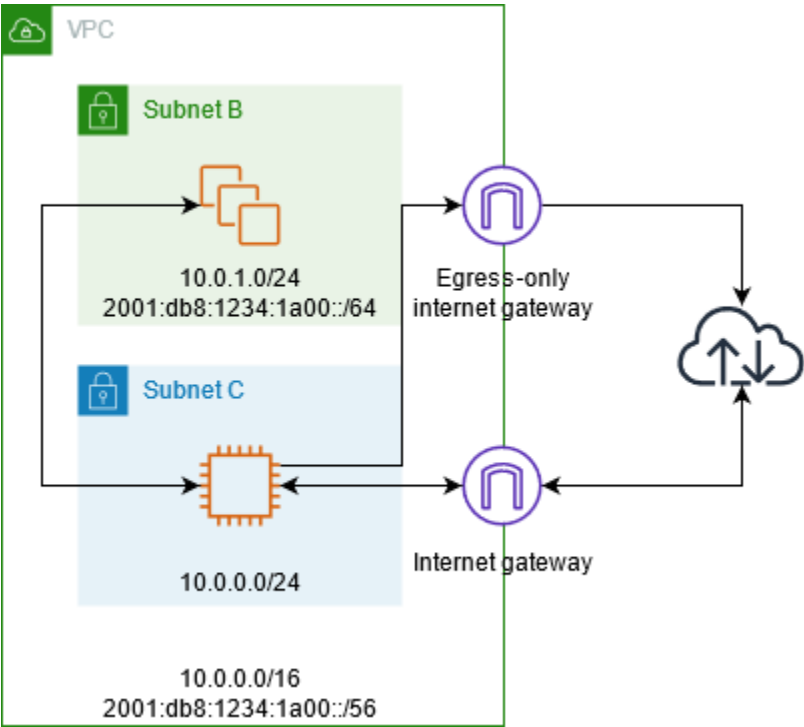
Wizard routing middlebox, secara otomatis melakukan operasi berikut:

- 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 perutean middlebox), tabel rute C dengan subnet C (Middlebox di wizard perutean middlebox), dan tabel rute B dengan subnet B (Tujuan di wizard perutean middlebox).
- 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 sumber daya gateway dan subnet Anda. Jika sumber daya Anda sudah secara eksplisit dikaitkan 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 routing 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
<i>10.0.1.0/24</i>	<i>appliance-eni</i>	Rute IPv4 lalu lintas yang ditujukan untuk subnet B ke middlebox
<i>2001:db8:1234:1a00::/56</i>	Lokal:	Rute lokal untuk IPv6
<i>2001:db8:1234:1a00::/64</i>	<i>appliance-eni</i>	Rute IPv6 lalu lintas yang ditujukan untuk subnet B ke middlebox

Ada hubungan tepi antara gateway internet dan VPC.

Saat Anda menggunakan wizard perutean middlebox, ini mengaitkan tag berikut dengan tabel rute:

- Kuncinya adalah “Asal” dan nilainya adalah “Middlebox wizard”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-02-18T 22:25:49.137 Z”)

Tabel rute subnet tujuan

Tambahkan rute berikut ke tabel rute untuk subnet tujuan (subnet B dalam diagram contoh).

Tujuan	Target	Tujuan
<i>10.0.0.0/16</i>	Lokal:	Rute lokal untuk IPv4
0.0.0.0/0	<i>appliance-eni</i>	Rute IPv4 lalu lintas yang ditujukan untuk internet ke middlebox
<i>2001:db8:1234:1a00::/56</i>	Lokal:	Rute lokal untuk IPv6
::/0	<i>appliance-eni</i>	Rute IPv6 lalu lintas yang ditujukan untuk internet ke middlebox

Ada asosiasi subnet dengan subnet middlebox.

Saat Anda menggunakan wizard perutean middlebox, ini mengaitkan tag berikut dengan tabel rute:

- Kuncinya adalah “Asal” dan nilainya adalah “Middlebox wizard”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-02-18T 22:25:49.137 Z”)

Tabel rute subnet Middlebox

Tambahkan rute berikut ke tabel rute untuk subnet middlebox (subnet C dalam diagram contoh).

Tujuan	Target	Tujuan
<i>10.0.0.0/16</i>	Lokal:	Rute lokal untuk IPv4
0.0.0.0/0	<i>igw-id</i>	Rutekan IPv4 lalu lintas ke gateway internet
<i>2001:db8:1234:1a00::/56</i>	Lokal:	Rute lokal untuk IPv6
::/0	<i>eigw-id</i>	Rutekan IPv6 lalu lintas ke gateway internet khusus egres

Ada asosiasi subnet dengan subnet tujuan.

Saat Anda menggunakan wizard perutean middlebox, ini mengaitkan tag berikut dengan tabel rute:

- Kuncinya adalah “Asal” dan nilainya adalah “Middlebox wizard”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-02-18T 22:25:49.137 Z”)

Konfigurasi perutean dan inspeksi lalu lintas middlebox 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 Load Balancer Gateway. Pemilik VPC konsumen layanan membuat titik akhir Load Balancer Gateway di subnet di VPC mereka (diwakili oleh antarmuka jaringan titik akhir). Semua lalu lintas yang memasuki VPC melalui gateway internet pertama kali dirutekan ke titik akhir Gateway

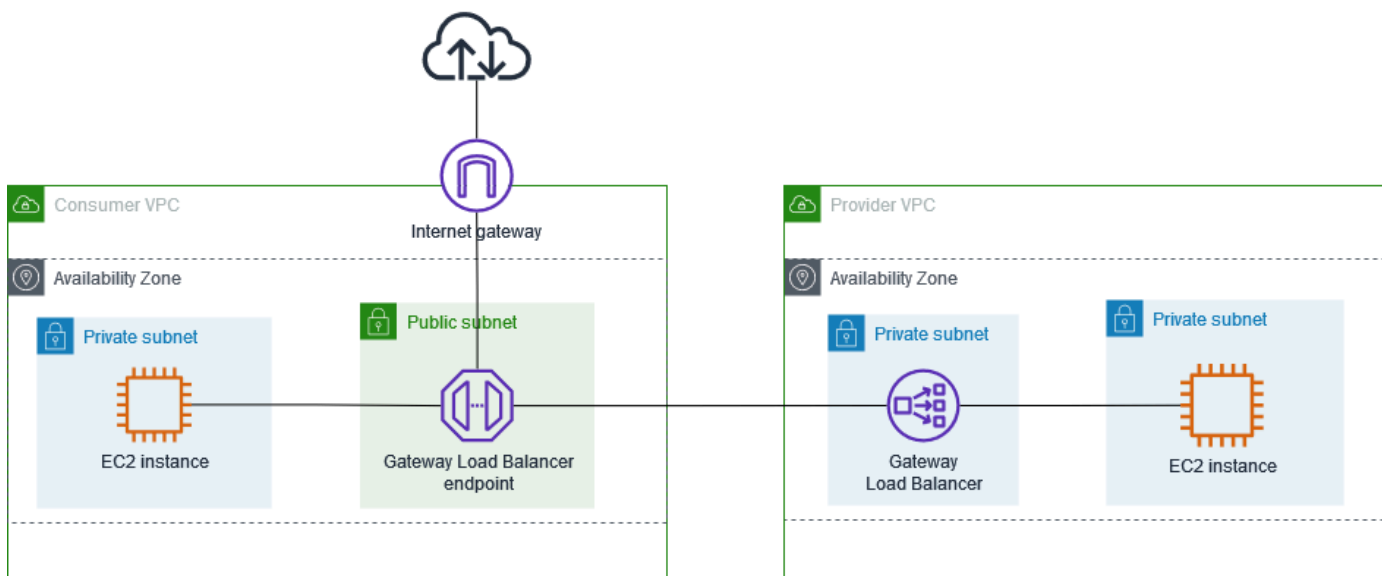
Load Balancer untuk diperiksa sebelum dialihkan ke subnet aplikasi. Demikian pula, semua lalu lintas yang meninggalkan subnet aplikasi pertama kali dirutekan ke titik akhir Gateway Load Balancer untuk diperiksa sebelum dialihkan ke internet.

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 sumber daya gateway dan subnet Anda. Jika sumber daya Anda sudah secara eksplisit dikaitkan 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 routing 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
<i>Consumer VPC CIDR</i>	Lokal:	Rute lokal
<i>Application subnet CIDR</i>	<i>endpoint-id</i>	Rutekan lalu lintas yang ditujukan untuk subnet aplikasi ke titik akhir Load Balancer Gateway

Ada asosiasi tepi dengan gateway.

Saat Anda menggunakan wizard perutean middlebox, ini mengaitkan tag berikut dengan tabel rute:

- Kuncinya adalah “Asal” dan nilainya adalah “Middlebox wizard”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-02-18T 22:25:49.137 Z”)

Tabel rute subnet aplikasi

Tabel rute untuk subnet aplikasi memiliki rute berikut.

Tujuan	Target	Tujuan
<i>Consumer VPC CIDR</i>	Lokal:	Rute lokal
0.0.0.0/0	<i>endpoint-id</i>	Rutekan lalu lintas dari server aplikasi ke titik akhir Gateway Load Balancer sebelum dialihkan ke internet

Saat Anda menggunakan wizard perutean middlebox, ini mengaitkan tag berikut dengan tabel rute:

- Kuncinya adalah “Asal” dan nilainya adalah “Middlebox wizard”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-02-18T 22:25:49.137 Z”)

Tabel rute subnet penyedia

Tabel rute untuk subnet penyedia memiliki rute berikut.

Tujuan	Target	Tujuan
<i>Provider VPC CIDR</i>	Lokal:	Rute lokal. Memastikan bahwa lalu lintas yang berasal dari internet dialihkan ke server aplikasi
0.0.0.0/0	<i>igw-id</i>	Rutekan semua lalu lintas ke gateway internet

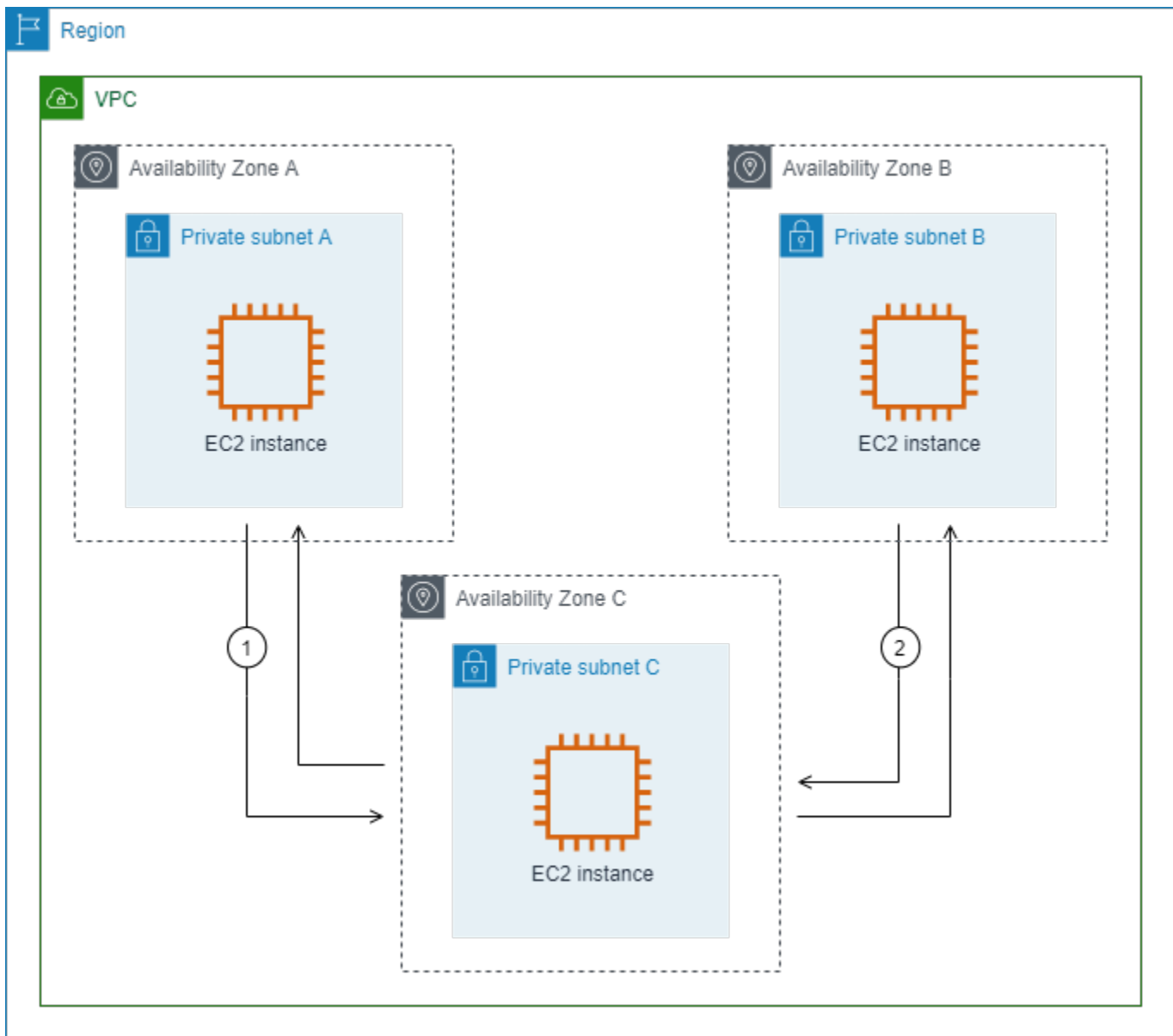
Saat Anda menggunakan wizard perutean middlebox, ini mengaitkan tag berikut dengan tabel rute:

- Kuncinya adalah “Asal” dan nilainya adalah “Middlebox wizard”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-02-18T22:25:49.137 Z”)

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. Konfigurasi dan instal alat firewall pada EC2 instance di subnet terpisah di VPC Anda.

Diagram berikut menunjukkan alat firewall yang dipasang pada sebuah EC2 instance 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 VPC dan subnet 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 sumber daya gateway dan subnet Anda. Jika sumber daya Anda sudah secara eksplisit dikaitkan 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 routing 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
<i>VPC CIDR</i>	Lokal:	Rute lokal
<i>Subnet B CIDR</i>	<i>appliance-eni</i>	Rute lalu lintas yang ditujukan untuk subnet B ke middlebox

Saat Anda menggunakan wizard perutean middlebox, ini mengaitkan tag berikut dengan tabel rute:

- Kuncinya adalah “Asal” dan nilainya adalah “Middlebox wizard”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-02-18T22:25:49.137 Z”)

Tabel rute khusus untuk subnet B

Tabel rute untuk subnet B memiliki rute berikut.

Tujuan	Target	Tujuan
<i>VPC CIDR</i>	Lokal:	Rute lokal

Tujuan	Target	Tujuan
<i>Subnet A CIDR</i>	<i>appliance-eni</i>	Rute lalu lintas yang ditujukan untuk subnet A ke middlebox

Saat Anda menggunakan wizard perutean middlebox, ini mengaitkan tag berikut dengan tabel rute:

- Kuncinya adalah “Asal” dan nilainya adalah “Middlebox wizard”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-02-18T22:25:49.137 Z”)

Tabel rute utama

Subnet C menggunakan tabel rute utama. Tabel rute utama memiliki rute berikut.

Tujuan	Target	Tujuan
<i>VPC CIDR</i>	Lokal:	Rute lokal

Saat Anda menggunakan wizard perutean middlebox, ini mengaitkan tag berikut dengan tabel rute:

- Kuncinya adalah “Asal” dan nilainya adalah “Middlebox wizard”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-02-18T22:25:49.137 Z”)

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

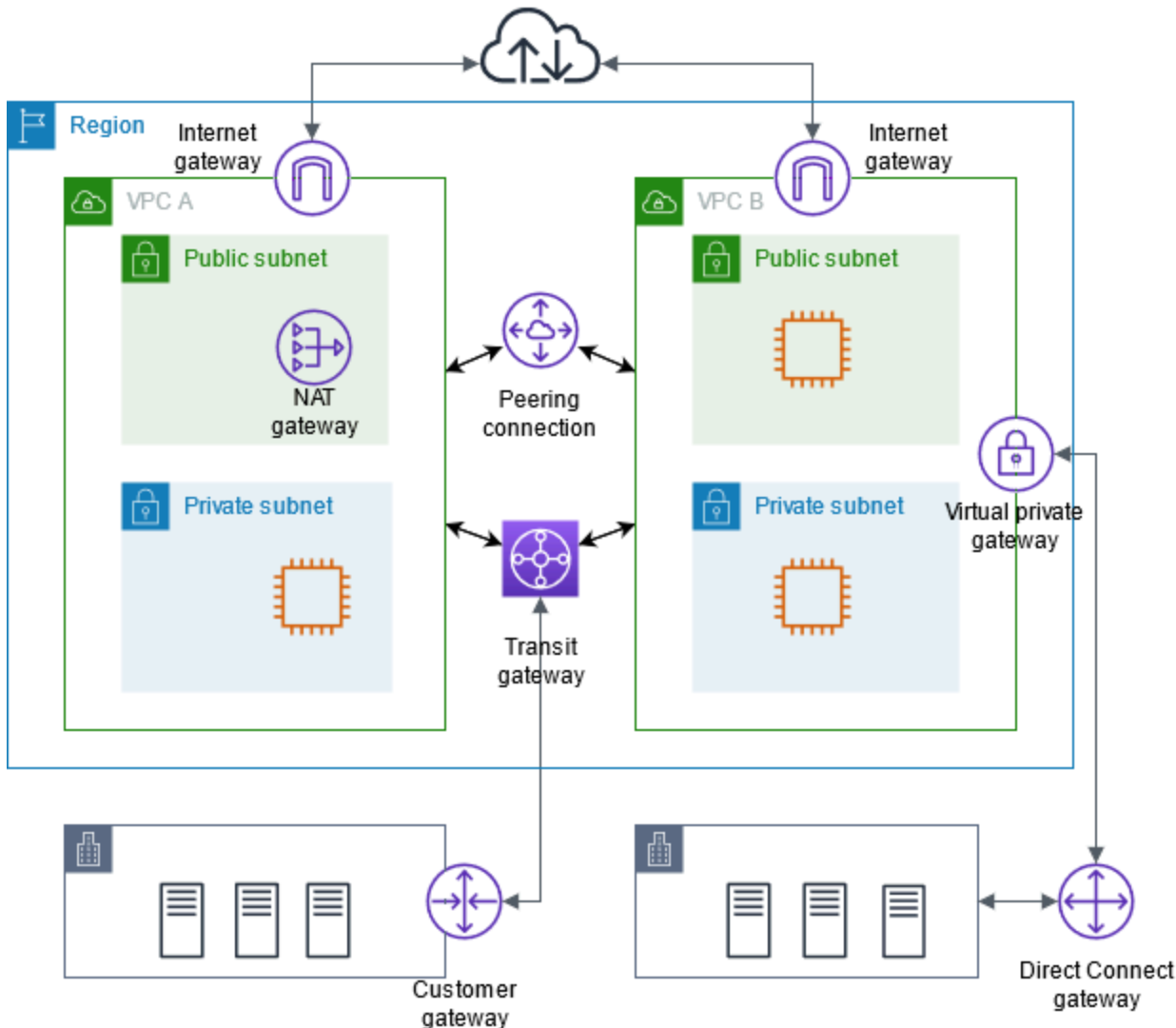
1. Buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Mengakhiri semua instans di subnet. Untuk informasi selengkapnya, lihat [Menghentikan instans Anda](#) di Panduan EC2 Pengguna Amazon.
3. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>
4. Di panel navigasi, pilih 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 jaringan lain VPCs, internet, atau jaringan lokal Anda.



Anda dapat menghubungkan virtual private cloud (VPC) ke jaringan lain, seperti jaringan lain VPCs, internet, atau jaringan lokal Anda.

Diagram menunjukkan beberapa opsi konektivitas ini. VPC A terhubung ke internet melalui gateway internet, dan EC2 instance 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 EC2 instance 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 AWS 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 VPCs 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 memfasilitasi aliran data yang efisien antara berbagai komponen lanskap TI terdistribusi, baik di dalam cloud maupun di tempat.

AWS menyediakan berbagai alat dan fitur untuk mengaktifkan koneksi VPC ini, termasuk gateway internet, gateway NAT, peering VPC, gateway transit, dan. AWS Direct Connect Dengan memanfaatkan kemampuan ini, organisasi dapat menciptakan lingkungan cloud yang aman dan terintegrasi yang terintegrasi secara mulus dengan infrastruktur TI yang ada.

Anda dapat menghubungkan virtual private cloud (VPC) Anda ke jaringan lain. Misalnya, lainnya VPCs, internet, atau jaringan lokal Anda.

Untuk informasi selengkapnya, lihat [Ops Konektivitas Amazon Virtual Private Cloud](#).

Daftar Isi

- [Aktifkan akses internet untuk VPC menggunakan gateway internet](#)
- [Aktifkan IPv6 lalu lintas keluar menggunakan gateway internet khusus egress-only](#)
- [Connect ke internet atau jaringan lain menggunakan perangkat NAT](#)
- [Kaitkan alamat IP Elastis dengan sumber daya di VPC Anda](#)
- [Hubungkan VPC Anda ke jaringan lain VPCs dan menggunakan gateway transit](#)
- [Hubungkan VPC Anda ke jaringan jarak jauh menggunakan AWS Virtual Private Network](#)
- [Connect VPCs menggunakan VPC peering](#)

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 IPv4 dan IPv6 lalu lintas. Gateway internet tidak menimbulkan risiko ketersediaan atau kendala bandwidth pada lalu lintas jaringan Anda.

Gateway internet memungkinkan sumber daya di subnet publik Anda (seperti EC2 instance) untuk terhubung ke internet jika sumber daya memiliki IPv4 alamat publik atau alamat IPv6. Demikian pula, sumber daya di internet dapat memulai koneksi ke sumber daya di subnet Anda menggunakan IPv4 alamat atau IPv6 alamat publik. Misalnya, gateway internet memungkinkan Anda untuk terhubung ke sebuah EC2 instans dalam AWS menggunakan komputer lokal Anda.

Gateway internet menyediakan target dalam tabel rute VPC Anda untuk lalu lintas yang dapat dirutekan internet. Untuk penggunaan komunikasi 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 EC2 contoh yang menggunakan gateway internet. Untuk informasi selengkapnya, lihat [Harga EC2 Sesuai Permintaan Amazon](#).

Daftar Isi

- [Dasar-dasar gateway internet](#)
- [Tambahkan akses internet ke subnet](#)
- [Menghapus gateway internet](#)

Dasar-dasar gateway internet

Untuk menggunakan gateway internet, Anda harus melampirkannya ke VPC dan mengonfigurasi perutean.

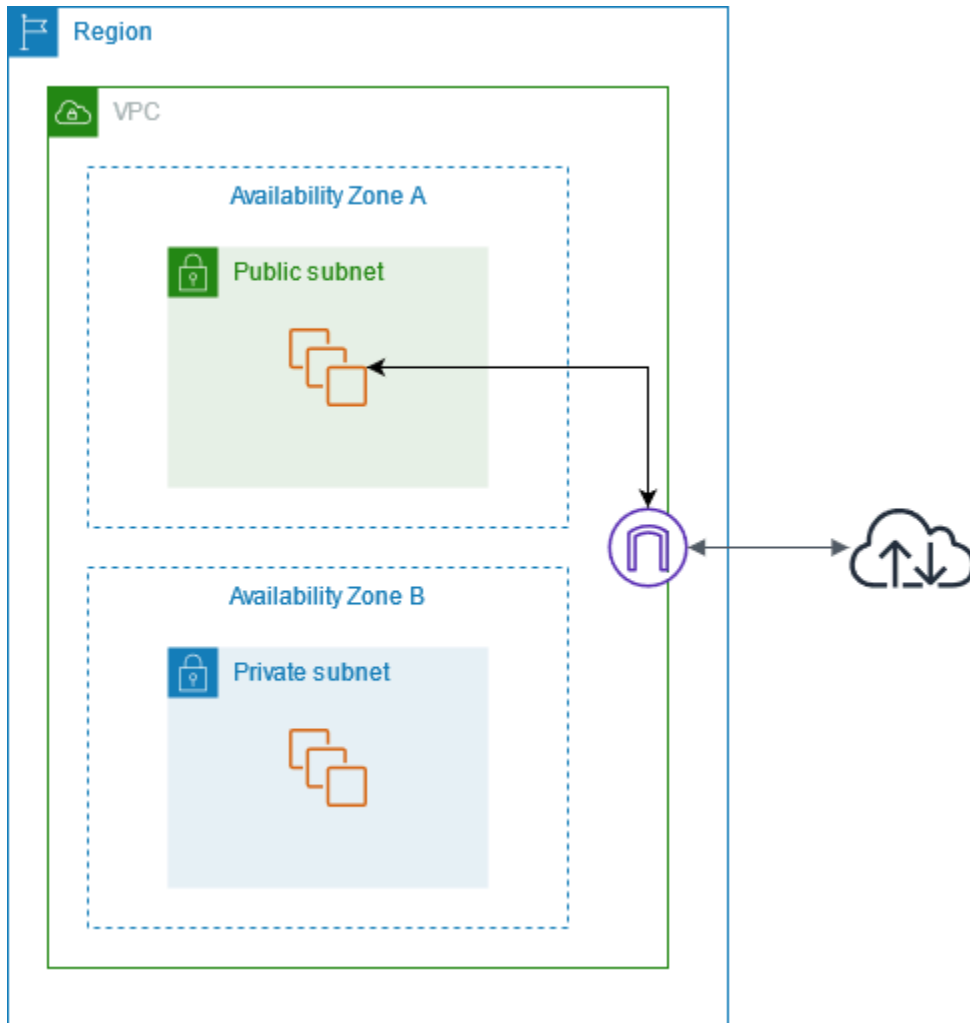
Konfigurasi perutean

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.

Dalam tabel rute subnet publik Anda, Anda dapat menentukan rute untuk gateway internet ke semua tujuan yang tidak secara eksplisit diketahui ke tabel rute (0.0.0.0/0 untuk atau ::/0 untuk). IPv4 IPv6 Atau, Anda dapat menjangkau rute ke rentang alamat IP yang lebih sempit; misalnya, alamat publik titik akhir publik IPv4 perusahaan Anda di luar AWS, atau alamat IP Elastis dari EC2 instans Amazon lainnya di luar VPC Anda.

Diagram gerbang internet

Dalam diagram berikut, subnet di Availability Zone A adalah subnet publik karena tabel rutenya memiliki rute yang mengirimkan semua IPv4 lalu lintas internet terikat ke gateway internet. Contoh 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 rutenya 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 IPv4, instans Anda harus memiliki IPv4 alamat publik. Anda dapat mengonfigurasi VPC Anda untuk secara otomatis menetapkan IPv4 alamat publik ke instans Anda, atau Anda dapat menetapkan alamat IP Elastis ke instans Anda. Instans Anda hanya mengenal ruang alamat IP pribadi (internal) yang terdefinisi di dalam VPC dan subnet. Gateway internet secara logis menyediakan one-to-one NAT atas nama instans Anda, sehingga ketika lalu lintas meninggalkan subnet VPC Anda dan masuk ke internet, bidang alamat

balasan diatur ke alamat IPv4 publik atau alamat IP Elastis dari instans Anda, dan bukan alamat IP pribadinya. Sebaliknya, lalu lintas yang ditujukan untuk IPv4 alamat publik atau alamat IP Elastis dari instans Anda memiliki alamat tujuannya diterjemahkan ke IPv4 alamat pribadi instans sebelum lalu lintas dikirim ke VPC.

Untuk mengaktifkan komunikasi melalui internet IPv6, VPC dan subnet Anda harus memiliki blok IPv6 CIDR terkait, dan instans Anda harus diberi IPv6 alamat dari kisaran subnet. IPv6 alamat secara global unik, dan oleh karena itu publik secara default.

Akses internet untuk default dan nondefault VPCs

Tabel berikut memberikan gambaran umum apakah VPC Anda secara otomatis dilengkapi dengan komponen yang diperlukan untuk akses internet melalui atau. IPv4 IPv6

Komponen	VPC Default	VPC Nondefault
gateway internet	Ya	Tidak
Tabel rute dengan rute ke gateway internet untuk IPv4 lalu lintas (0.0.0.0/0)	Ya	Tidak
Tabel rute dengan rute ke gateway internet untuk IPv6 lalu lintas (:: /0)	Tidak	Tidak
IPv4 Alamat publik secara otomatis ditetapkan ke instance yang diluncurkan ke subnet	Ya (subnet default)	Tidak ada (subnet nondefault)
IPv6 alamat secara otomatis ditetapkan ke instance diluncurkan ke subnet	Tidak (subnet default)	Tidak (subnet nondefault)

Tambahkan 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, EC2 instans Anda harus memiliki publik IPv4 atau IPv6 alamat, dan grup keamanan untuk instans Anda harus mengizinkan lalu lintas tertentu ke dan dari internet.

Atau, untuk memberikan instans Anda dengan akses internet tanpa memberi mereka 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 gateway Internet.
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 Lampirkan ke VPC dari spanduk di bagian atas layar, pilih VPC yang tersedia, lalu pilih Lampirkan 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 gateway Internet.
3. Pilih kotak centang untuk gateway internet.
4. Untuk melampirkannya, pilih Tindakan, Lampirkan ke VPC, pilih VPC yang tersedia, dan pilih Lampirkan gateway internet.
5. Untuk melepaskannya, pilih Tindakan, Lepaskan dari VPC dan pilih Lepaskan gateway internet. Saat diminta konfirmasi, pilih Lepaskan 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 dan kemudian pilih Tambah 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 gateway Internet.
3. Pilih kotak centang untuk gateway internet.
4. Untuk melampirkannya, pilih Tindakan, Lampirkan ke VPC, pilih VPC yang tersedia, dan pilih Lampirkan gateway internet.
5. Untuk melepaskannya, pilih Tindakan, Lepaskan dari VPC dan pilih Lepaskan gateway internet. Saat diminta konfirmasi, pilih Lepaskan gateway internet.

Untuk mendeskripsikan 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 gateway Internet.
3. Pilih kotak centang untuk gateway internet.
4. Pilih Tindakan, Hapus gateway internet.
5. Saat diminta konfirmasi, masukkan **delete**, lalu pilih Hapus gateway internet.

Untuk menghapus gateway internet menggunakan baris perintah

- [delete-internet-gateway](#) (AWS CLI)
- [Remove-EC2InternetGateway](#) (AWS Tools for Windows PowerShell)

Aktifkan IPv6 lalu lintas keluar menggunakan gateway internet khusus egress-only

Gateway internet khusus egres adalah komponen VPC yang diskalakan secara horizontal, berlebihan, dan sangat tersedia yang memungkinkan komunikasi keluar IPv6 dari instance di VPC Anda ke internet, dan mencegah internet memulai koneksi dengan instans Anda. IPv6

Gateway internet khusus egres hanya untuk digunakan dengan IPv6 lalu lintas. Untuk mengaktifkan komunikasi internet outbound only IPv4, gunakan gateway NAT sebagai gantinya. Untuk informasi selengkapnya, lihat [Gateway NAT](#).

Harga

Tidak ada biaya untuk gateway internet khusus egres, tetapi ada biaya transfer data untuk EC2 contoh yang menggunakan gateway internet. Untuk informasi selengkapnya, lihat [Harga EC2 Sesuai Permintaan Amazon](#).

Daftar Isi

- [Dasar-dasar gateway internet egress-only](#)
- [Tambahkan akses internet khusus egres ke subnet](#)

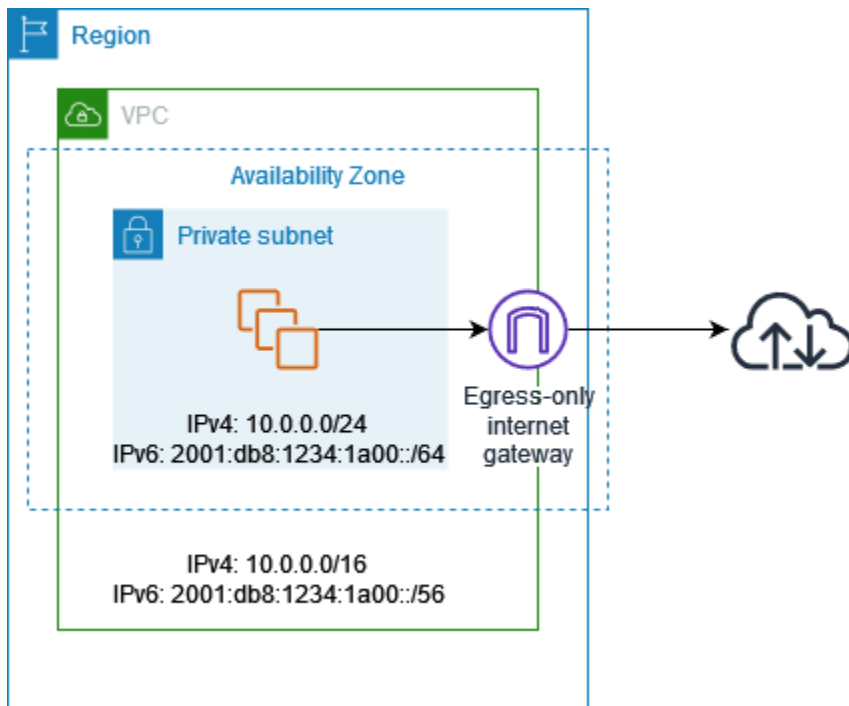
Dasar-dasar gateway internet egress-only

IPv6 alamat bersifat unik secara global, dan oleh karena itu 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 egress-only. Untuk melakukan ini, buat gateway internet khusus egres di VPC Anda, lalu tambahkan rute ke tabel rute Anda yang mengarahkan semua IPv6 lalu lintas (: : /0) atau rentang IPv6 alamat tertentu ke gateway internet khusus egress. IPv6 lalu lintas di subnet yang terkait dengan tabel rute dirutekan ke gateway internet khusus egres.

Sebuah gateway internet egress-only stateful: ia meneruskan lalu lintas dari instance di subnet ke internet atau AWS layanan lain, dan kemudian mengirim respon kembali ke instance.

Anda tidak dapat mengaitkan grup keamanan dengan gateway internet khusus egres untuk mengontrol lalu lintas yang diizinkan untuk mencapai atau meninggalkan gateway internet khusus egres. 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 keduanya IPv4 dan blok IPv6 CIDR, dan subnet keduanya IPv4 dan blok CIDR. IPv6 VPC memiliki gateway internet khusus egress-only.



Berikut ini adalah contoh tabel rute yang terkait dengan subnet. Ada rute yang mengirimkan semua IPv6 lalu lintas terikat internet (:: /0) ke gateway internet khusus egress.

Tujuan	Target
10.0.0.0/16	Lokal
2001:db 8:1234:1 a00: /64	Lokal:
::/0	<i>eigw-id</i>

Tambahkan akses internet khusus egres ke subnet

Tugas-tugas berikut menjelaskan cara membuat gateway internet egress-only (outbound) untuk subnet pribadi Anda dan untuk mengkonfigurasi 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 VPC Amazon 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 Hapus 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 VPC Amazon 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 [Konfigurasi 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 VPC Amazon 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 di halaman ini menggunakan baris perintah.

Buat gateway internet egress-only

- [create-egress-only-internet-pintu gerbang](#) ()AWS CLI
- [New-EC2EgressOnlyInternetGateway](#) (AWS Tools for Windows PowerShell)

Jelaskan gateway internet egress-only

- [describe-egress-only-internet-gateway](#) ()AWS CLI
- [Get-EC2EgressOnlyInternetGatewayList](#) (AWS Tools for Windows PowerShell)

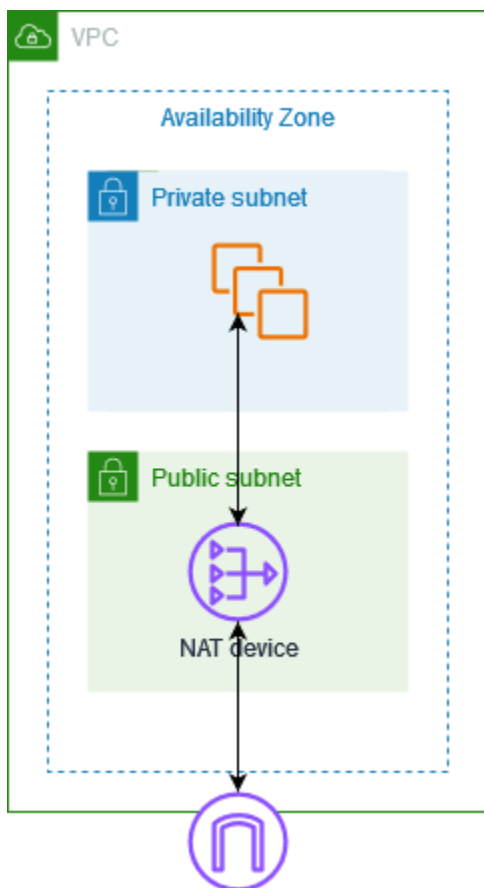
Hapus gateway internet egress-only

- [delete-egress-only-internet-pintu gerbang](#) ()AWS CLI
- [Remove-EC2EgressOnlyInternetGateway](#) (AWS Tools for Windows PowerShell)

Connect ke internet atau jaringan lain menggunakan perangkat NAT

Anda dapat menggunakan perangkat NAT untuk memungkinkan sumber daya di subnet pribadi terhubung ke internet, jaringan lain VPCs, atau 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 EC2 instance di subnet pribadi untuk terhubung ke internet melalui gateway internet. Perangkat NAT menggantikan IPv4 alamat sumber instance dengan alamat perangkat NAT. Saat mengirim lalu lintas respons ke instance, perangkat NAT menerjemahkan alamat kembali ke alamat sumber asli. IPv4



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 sebuah EC2 instance, 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 instance 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 - (Default) Instans dalam 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 elastis dengan gateway NAT pada saat dibuat. Anda merutekan lalu lintas dari gateway NAT ke gateway internet untuk VPC. Atau, Anda dapat menggunakan gateway NAT publik untuk terhubung ke jaringan lain VPCs atau lokal Anda. Dalam hal ini, Anda merutekan lalu lintas dari gateway NAT melalui transit gateway atau virtual private gateway.
- Private — Instans dalam subnet pribadi dapat terhubung ke jaringan lain VPCs atau lokal Anda melalui gateway NAT pribadi, tetapi instans tidak dapat menerima koneksi masuk yang tidak diminta dari jaringan lain atau di tempat. VPCs Anda dapat merutekan lalu lintas dari gateway NAT melalui transit gateway atau virtual private gateway. Anda tidak dapat mengaitkan alamat IP elastis

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 adalah untuk digunakan dengan IPv4 atau IPv6 lalu lintas (menggunakan [DNS64 dan NAT64](#)). [Pilihan lain untuk mengaktifkan komunikasi internet outbound saja IPv6 adalah menggunakan gateway internet khusus egres.](#)

Gateway NAT pribadi dan publik memetakan IPv4 alamat pribadi sumber instance ke IPv4 alamat pribadi gateway NAT, tetapi dalam kasus gateway NAT publik, gateway internet kemudian memetakan IPv4 alamat pribadi gateway NAT publik ke alamat IP Elastis 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.

Important

Koneksi harus selalu dimulai dari dalam VPC yang berisi NAT Gateway.

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 berasal 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 berasal dari alamat IP pribadi gateway NAT publik. Gateway NAT publik hanya akan menggunakan EIP sebagai alamat IP sumber ketika digunakan bersama dengan gateway internet di VPC yang sama.

Gateway NAT mendukung lalu lintas dengan unit transmisi maksimum (MTU) 8500. Untuk informasi selengkapnya, lihat [Dasar gateway NAT](#).

Daftar Isi

- [Dasar gateway NAT](#)
- [Bekerja dengan gateway NAT](#)
- [Kasus penggunaan gateway NAT](#)
- [DNS64 dan NAT64](#)
- [Pantau gateway NAT dengan Amazon CloudWatch](#)

- [Memecahkan masalah gateway NAT](#)
- [Harga untuk gateway NAT](#)

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 [Kuota Amazon VPC](#).

Jika Anda memiliki sumber daya di beberapa Availability Zone dan mereka berbagi satu gateway NAT, dan jika Availability Zone gateway NAT down, sumber daya di Availability Zone lainnya kehilangan akses internet. Untuk meningkatkan ketahanan, buat gateway NAT di setiap Availability Zone, dan konfigurasi routing Anda untuk memastikan bahwa resource 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.
- Gateway NAT didukung untuk IPv4 atau lalu lintas. IPv6 Untuk IPv6 lalu lintas, gateway NAT berkinerja NAT64. Dengan menggunakan ini bersama dengan DNS64 (tersedia di resolver Route 53), IPv6 beban kerja Anda di subnet di Amazon VPC dapat berkomunikasi dengan sumber daya. IPv4 Layanan ini dapat hadir dalam 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.
- Gateway NAT dapat memproses satu juta paket per detik dan secara otomatis menskalakan hingga sepuluh juta paket per detik. Di luar batas ini, gateway NAT akan menjatuhkan paket. Untuk mencegah kehilangan paket, pisahkan sumber daya Anda menjadi beberapa subnet dan buat gateway NAT terpisah untuk setiap subnet.
- Setiap IPv4 alamat dapat mendukung hingga 55.000 koneksi simultan ke setiap tujuan unik. Tujuan unik diidentifikasi oleh kombinasi unik dari alamat IP tujuan, port tujuan, dan protokol (TCP/UDP/ICMP). Anda dapat meningkatkan batas ini dengan mengaitkan hingga 8 IPv4 alamat ke gateway NAT Anda (1 IPv4 alamat utama dan 7 alamat sekunder). IPv4 Anda dibatasi untuk mengaitkan 2 alamat IP Elastis 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 memilih IPv4 alamat pribadi untuk ditetapkan ke gateway NAT atau menentukannya secara otomatis dari rentang IPv4 alamat subnet. IPv4 Alamat pribadi yang ditetapkan tetap ada sampai Anda menghapus gateway NAT pribadi. Anda tidak dapat melepaskan IPv4 alamat pribadi dan Anda tidak dapat melampirkan IPv4 alamat pribadi tambahan.
- Anda tidak dapat mengaitkan grup keamanan dengan gateway NAT. Anda dapat mengaitkan grup keamanan ke instans Anda untuk mengontrol lalu lintas masuk dan keluar.
- 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 [Kontrol lalu lintas subnet dengan daftar kontrol akses jaringan](#).
- Gateway NAT menerima antarmuka jaringan. Anda dapat memilih IPv4 alamat pribadi untuk ditetapkan ke antarmuka atau secara otomatis ditetapkan dari rentang IPv4 alamat subnet. Anda dapat melihat antarmuka jaringan untuk gateway NAT menggunakan EC2 konsol Amazon. Untuk informasi selengkapnya, lihat [Menampilkan detail tentang antarmuka jaringan](#). Anda tidak dapat mengubah atribut antarmuka jaringan ini.
- Anda tidak dapat merutekan lalu lintas ke gateway NAT melalui koneksi peering VPC.
- 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.
- Gateway NAT mendukung lalu lintas dengan unit transmisi maksimum (MTU) 8500, tetapi penting untuk dicatat 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 EC2 instance Anda tidak boleh melebihi 1500 byte. Untuk informasi selengkapnya tentang memeriksa dan menyetel MTU pada instans, lihat [Memeriksa dan mengatur MTU pada instans Linux Anda](#) di EC2 Panduan Pengguna Amazon.
 - Gateway NAT mendukung Path MTU Discovery (PMTUD) melalui paket FRAG_NEEDED dan ICMPv4 paket Packet Too Big (PTB). ICMPv6

- Gateway NAT memberlakukan penjepitan Ukuran Segmen Maksimum (MSS) untuk semua paket. Untuk informasi selengkapnya, 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, mendeskripsikan, 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 kehabisan jumlah yang EIPs dialokasikan ke akun Anda. Untuk informasi lebih lanjut tentang kuota EIP dan cara menyesuaikannya, lihat [Alamat IP elastis](#)
- Anda dapat menetapkan hingga 8 IPv4 alamat pribadi ke gateway NAT pribadi Anda. Batas ini tidak dapat disesuaikan.
- Anda dibatasi untuk mengaitkan 2 alamat IP Elastis 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 gateway NAT.
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 Publik default untuk membuat gateway NAT publik atau pilih Private untuk membuat gateway NAT pribadi. Untuk informasi lebih lanjut tentang perbedaan antara gateway NAT publik dan pribadi, lihat [Gateway NAT](#).
7. Jika Anda memilih Publik, lakukan hal berikut; jika tidak, lewati ke langkah 8:
 1. Pilih ID alokasi IP Elastis untuk menetapkan EIP ke gateway NAT atau pilih Alokasikan IP Elastis untuk mengalokasikan EIP secara otomatis untuk gateway NAT publik. Anda dibatasi untuk mengaitkan 2 alamat IP Elastis 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 EIP ke gateway NAT publik, grup perbatasan jaringan EIP harus cocok dengan grup perbatasan jaringan 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 EIP dengan melihat detail alamat EIP. Untuk informasi selengkapnya tentang grup perbatasan jaringan dan EIPs, lihat [1. Alokasikan sebuah alamat IP Elastis](#).

2. (Opsional) Pilih Pengaturan tambahan dan, di bawah Alamat IP pribadi - opsional, masukkan IPv4 alamat pribadi untuk gateway NAT. Jika Anda tidak memasukkan alamat, secara otomatis AWS akan menetapkan IPv4 alamat pribadi ke gateway NAT Anda secara acak dari subnet tempat gateway NAT Anda berada.
3. Lewati ke langkah 11.
8. Jika Anda memilih Pribadi, untuk Pengaturan tambahan, Metode penetapan IPv4 alamat pribadi, pilih salah satu dari berikut ini:

- Tetapkan otomatis: AWS memilih IPv4 alamat pribadi utama untuk gateway NAT. Untuk Jumlah IPv4 alamat pribadi yang ditetapkan secara otomatis, Anda dapat secara opsional menentukan jumlah IPv4 alamat pribadi sekunder untuk gateway NAT. AWS memilih alamat IP ini secara acak dari subnet untuk gateway NAT Anda.
 - Kustom: Untuk IPv4 alamat pribadi Primer, pilih IPv4 alamat pribadi utama untuk gateway NAT. Untuk IPv4 alamat pribadi sekunder, Anda dapat secara opsional menentukan hingga 7 IPv4 alamat pribadi sekunder untuk gateway NAT.
9. Jika Anda memilih Kustom di Langkah 8, lewati langkah ini. Jika Anda memilih Tetapkan otomatis, di bawah Jumlah alamat IP pribadi yang ditetapkan secara otomatis, pilih jumlah IPv4 alamat sekunder yang ingin Anda AWS tetapkan ke gateway NAT pribadi ini. Anda dapat memilih hingga 7 IPv4 alamat.

 Note

IPv4 Alamat 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). IPv4 Alamat 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 Tetapkan otomatis di Langkah 9, lewati langkah ini. Jika Anda memilih Custom, lakukan hal berikut:
1. Di bawah IPv4 Alamat pribadi utama, masukkan IPv4 alamat pribadi.
 2. Di bawah IPv4 Alamat pribadi sekunder, masukkan hingga 7 IPv4 alamat 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 tanda.
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 IPv4 alamat dapat mendukung hingga 55.000 koneksi simultan ke setiap tujuan unik. Tujuan unik diidentifikasi oleh kombinasi unik dari alamat IP tujuan, port tujuan, dan protokol (TCP/UDP/ICMP). Anda dapat meningkatkan batas ini dengan mengaitkan hingga 8 IPv4 alamat ke gateway NAT Anda (1 IPv4 alamat utama dan 7 alamat sekunder). IPv4 Anda dibatasi untuk mengaitkan 2 alamat IP Elastis 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 [CloudWatchmetrik gateway NAT ErrorPortAllocation](#) dan [PacketsDropCount](#) untuk menentukan apakah gateway NAT Anda menghasilkan kesalahan alokasi port atau menjatuhkan paket. Untuk mengatasi masalah ini, tambahkan IPv4 alamat sekunder ke gateway NAT Anda.

Pertimbangan

- Anda dapat menambahkan IPv4 alamat pribadi sekunder saat membuat gateway NAT pribadi atau setelah Anda membuat gateway NAT menggunakan prosedur di bagian ini. Anda dapat menambahkan alamat EIP sekunder ke gateway NAT publik hanya setelah Anda membuat gateway NAT dengan menggunakan prosedur di bagian ini.
- Gateway NAT Anda dapat memiliki hingga 8 IPv4 alamat yang terkait dengannya (1 IPv4 alamat utama dan 7 IPv4 alamat sekunder). Anda dapat menetapkan hingga 8 IPv4 alamat pribadi ke gateway NAT pribadi Anda. Anda dibatasi untuk mengaitkan 2 alamat IP Elastis 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 IPv4 alamat sekunder

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih gateway NAT.
3. Pilih gateway NAT yang asosiasi IPv4 alamat sekundernya ingin Anda edit.
4. Pilih Tindakan, lalu pilih Edit asosiasi alamat IP sekunder.
5. Jika Anda mengedit asosiasi IPv4 alamat sekunder dari gateway NAT pribadi, di bawah Tindakan, pilih Tetapkan IPv4 alamat baru atau Batalkan penetapan alamat yang ada. IPv4 Jika Anda mengedit asosiasi IPv4 alamat sekunder dari gateway NAT publik, di bawah Tindakan, pilih Kaitkan IPv4 alamat baru atau Putuskan alamat yang ada IPv4 .
6. Lakukan salah satu tindakan berikut:

- Jika Anda memilih untuk menetapkan atau mengaitkan IPv4 alamat baru, lakukan hal berikut:
 1. Langkah ini diperlukan. Anda harus memilih IPv4 alamat pribadi. Pilih metode IPv4 penetapan alamat pribadi:
 - Tetapkan AWS otomatis: secara otomatis memilih IPv4 alamat pribadi utama dan Anda memilih apakah Anda ingin menetapkan AWS hingga 7 IPv4 alamat pribadi sekunder untuk ditetapkan ke gateway NAT. AWS secara otomatis memilih dan menetapkan untuk Anda secara acak dari subnet tempat gateway NAT Anda berada.
 - Kustom: Pilih IPv4 alamat pribadi utama dan hingga 7 IPv4 alamat pribadi sekunder untuk ditetapkan ke gateway NAT.
 2. Di bawah ID alokasi IP elastis, pilih EIP untuk ditambahkan sebagai alamat sekunder IPv4 . Langkah ini diperlukan. Anda harus memilih EIP bersama dengan IPv4 alamat pribadi. Jika Anda memilih Kustom untuk metode penetapan alamat IP Pribadi, Anda juga harus memasukkan IPv4 alamat pribadi untuk setiap EIP yang Anda tambahkan.

 Important

Saat Anda menetapkan EIP sekunder ke gateway NAT publik, grup perbatasan jaringan EIP harus cocok dengan grup perbatasan jaringan Availability Zone (AZ) tempat gateway NAT publik berada. Jika tidak sama, EIP akan gagal untuk menetapkan. Anda dapat melihat grup perbatasan jaringan untuk AZ subnet dengan melihat detail subnet. Demikian pula, Anda dapat melihat grup perbatasan jaringan EIP dengan melihat detail alamat EIP. Untuk informasi selengkapnya tentang grup perbatasan jaringan dan EIPs, 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 EIPs per Wilayah. Untuk informasi selengkapnya, lihat [Alamat IP elastis](#).

- Jika Anda memilih untuk membatalkan penetapan atau memisahkan IPv4 alamat baru, lengkapi yang berikut ini:
 1. Di bawah Alamat IP sekunder yang ada untuk membatalkan penetapan, pilih alamat IP sekunder yang ingin Anda batalkan.
 2. (opsional) Di bawah durasi pengurusan 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 [Menandai EC2 sumber daya Amazon Anda](#) di Panduan EC2 Pengguna Amazon.

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 gateway NAT.
3. Pilih gateway NAT yang ingin Anda tag dan pilih Tindakan. Kemudian pilih Kelola tag.
4. Pilih Tambahkan tag baru, dan tentukan Kunci dan Nilai untuk tag. Anda dapat menambahkan hingga 50 tanda.
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 gateway NAT.
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 di halaman ini menggunakan baris perintah.

Tetapkan IPv4 alamat pribadi ke gateway NAT pribadi

- [assign-private-nat-gateway-alamat](#) (AWS CLI)
- [Register-EC2PrivateNatGatewayAddress](#) (AWS Tools for Windows PowerShell)

Kaitkan alamat IP Elastis (EIPs) dan IPv4 alamat pribadi dengan gateway NAT publik

- [associate-nat-gateway-address](#) (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

- [describe-nat-gateways](#) (AWS CLI)
- [Get-EC2NatGateway](#) (AWS Tools for Windows PowerShell)

Putuskan alamat IP Elastis sekunder (EIPs) dari gateway NAT publik

- [disassociate-nat-gateway-address](#) (AWS CLI)
- [Unregister-EC2NatGatewayAddress](#) (AWS Tools for Windows PowerShell)

Menandai gateway NAT

- [create-tags](#) (AWS CLI)
- [New-EC2Tag](#) (AWS Tools for Windows PowerShell)

Batalan penetapan IPv4 alamat sekunder dari gateway NAT pribadi

- [unassign-private-nat-gateway-alamat](#) ()AWS CLI
- [Unregister-EC2PrivateNatGatewayAddress](#) (AWS Tools for Windows PowerShell)

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 diizinkan](#)
- [Aktifkan komunikasi antara jaringan yang tumpang tindih](#)

Mengakses internet dari subnet privat

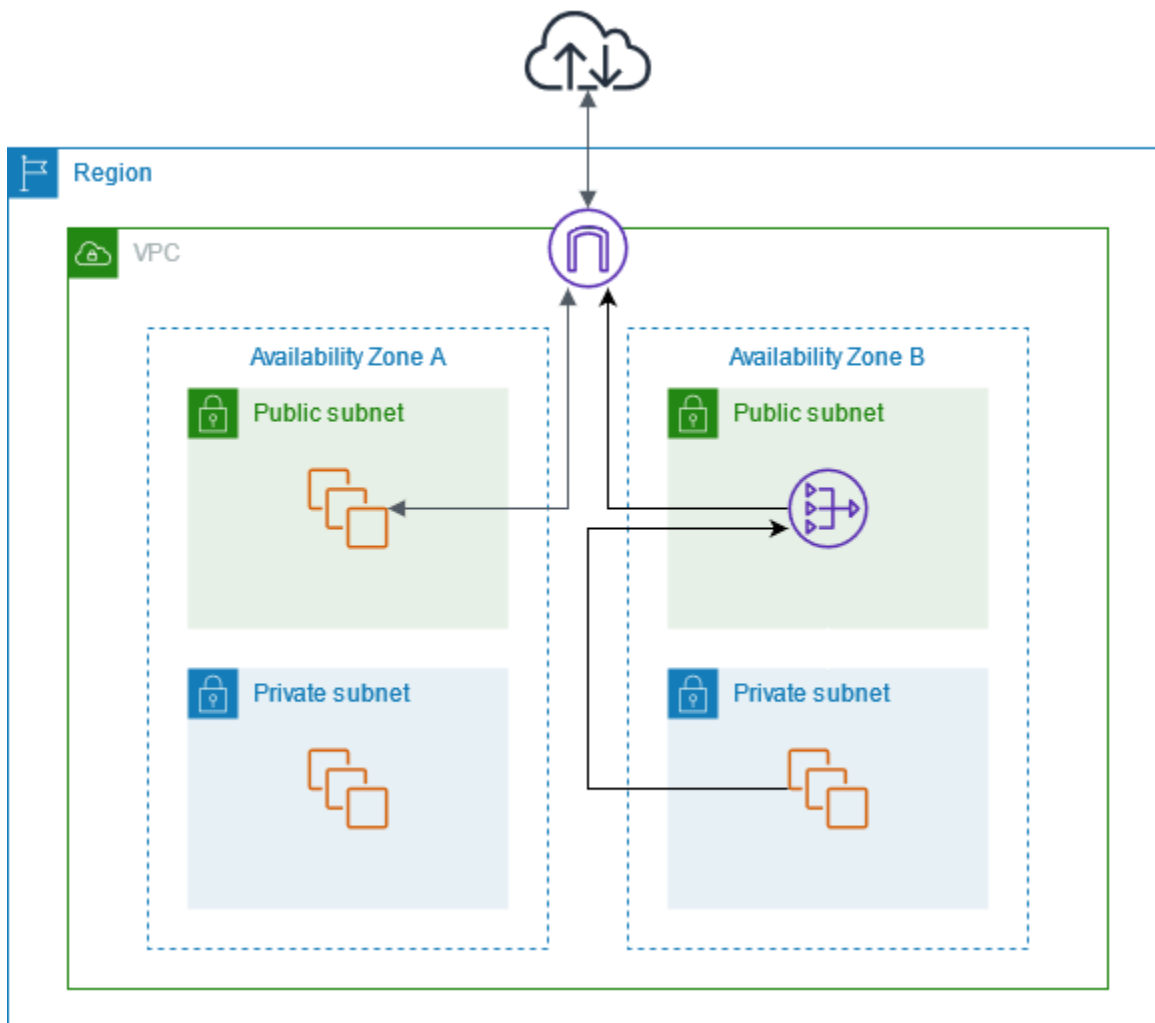
Anda dapat menggunakan gateway NAT publik untuk mengaktifkan instance di subnet pribadi untuk mengirim lalu lintas keluar ke internet, sekaligus mencegah internet membuat koneksi ke instans.

Daftar Isi

- [Gambaran Umum](#)
- [Perutean](#)
- [Uji gateway NAT publik](#)

Gambaran Umum

Diagram berikut menggambarkan kasus penggunaan ini. Ada dua Availability Zone, dengan dua subnet di setiap Availability Zone. 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. Gateway NAT pribadi dan publik memetakan IPv4 alamat pribadi sumber instance ke alamat pribadi gateway NAT pribadi IPv4, tetapi dalam kasus gateway NAT publik, gateway internet kemudian memetakan IPv4 alamat pribadi gateway NAT publik ke alamat IP Elastis 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, lihat [the 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 instance di subnet untuk berkomunikasi dengan instance lain di VPC menggunakan alamat IP pribadi. Entri kedua mengirimkan semua lalu lintas subnet lainnya ke gateway internet, yang memungkinkan instance di subnet untuk mengakses internet.

Tujuan	Target
<i>VPC CIDR</i>	lokal
0.0.0.0/0	<i>internet-gateway-id</i>

Berikut ini adalah tabel rute yang terkait dengan subnet pribadi di Availability Zone A. Entri adalah rute lokal, yang memungkinkan instance di subnet untuk berkomunikasi dengan instance lain di VPC menggunakan alamat IP pribadi. Contoh di subnet ini tidak memiliki akses ke internet.

Tujuan	Target
<i>VPC CIDR</i>	lokal

Berikut ini adalah tabel rute yang terkait dengan subnet publik di Availability Zone B. Entri pertama adalah rute lokal, yang 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 internet, yang memungkinkan gateway NAT di subnet untuk mengakses internet.

Tujuan	Target
<i>VPC CIDR</i>	lokal
0.0.0.0/0	<i>internet-gateway-id</i>

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
<i>VPC CIDR</i>	lokal
0.0.0.0/0	<i>nat-gateway-id</i>

Untuk informasi selengkapnya, lihat [the section called “Mengelola 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 menjadi alamat IP elastis 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 launch wizard, pastikan bahwa Anda memilih Amazon Linux AMI, dan menetapkan alamat IP publik untuk

- instans Anda. Pastikan bahwa aturan grup keamanan Anda mengizinkan lalu lintas SSH masuk dari rentang alamat IP untuk jaringan on-premise Anda, dan lalu lintas SSH keluar ke rentang alamat IP dari subnet privat Anda (Anda juga dapat menggunakan `0.0.0.0/0` untuk lalu lintas SSH masuk dan keluar untuk tes 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: [Memulai OpenSSH](#) untuk Windows. Kemudian tambahkan kunci Anda ke agen otentikasi. Untuk informasi selengkapnya, lihat [Autentikasi berbasis kunci 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 menggunakan PuTTYgen](#) di Panduan EC2 Pengguna Amazon.
3. Mulai Pageant, klik kanan ikon Pageant pada taskbar (mungkin tersembunyi), dan pilih Tambah 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 [Connect to Linux Anda 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 EC2 Pengguna Amazon.

Akses jaringan Anda menggunakan alamat IP yang diizinkan

Anda dapat menggunakan gateway NAT pribadi untuk mengaktifkan komunikasi dari jaringan lokal Anda VPCs ke jaringan lokal menggunakan kumpulan alamat yang diizinkan. Alih-alih menetapkan setiap instans alamat IP terpisah dari rentang alamat IP yang terdaftar yang diizinkan, Anda dapat merutekan lalu lintas dari subnet yang ditujukan untuk jaringan lokal melalui gateway NAT pribadi dengan alamat IP dari rentang alamat IP yang terdaftar yang diizinkan.

Daftar Isi

- [Gambaran Umum](#)
- [Sumber daya](#)
- [Perutean](#)

Gambaran Umum

Diagram berikut menunjukkan bagaimana instance dapat mengakses sumber daya lokal. AWS VPN Lalu lintas dari instans dirutekan ke gateway pribadi virtual, melalui koneksi VPN, ke gateway pelanggan, dan kemudian ke tujuan di jaringan lokal. Namun, misalkan tujuan memungkinkan 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.

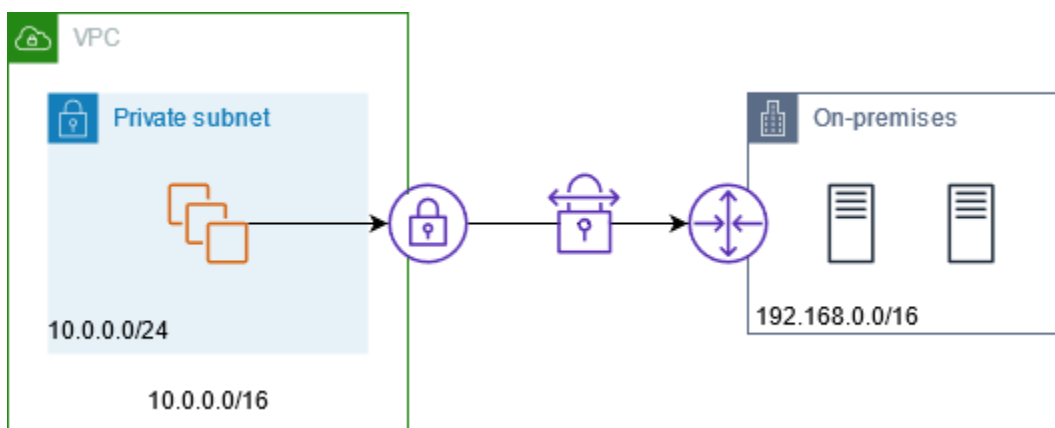
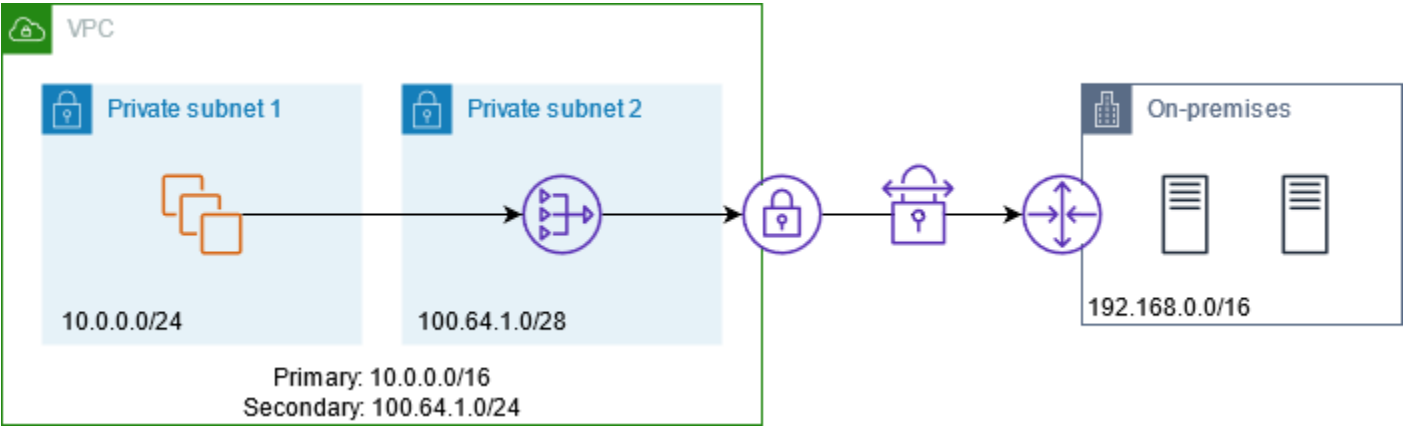


Diagram berikut menunjukkan komponen kunci konfigurasi untuk skenario ini. VPC memiliki rentang alamat IP asli ditambah rentang alamat IP yang diizinkan. VPC memiliki subnet dari rentang alamat IP yang diizinkan dengan gateway NAT pribadi. Lalu lintas dari instans yang ditujukan untuk jaringan lokal dikirim ke gateway NAT sebelum dirutekan ke koneksi VPN. Jaringan lokal menerima lalu lintas dari instans 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 instance 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 CIDR VPC. 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

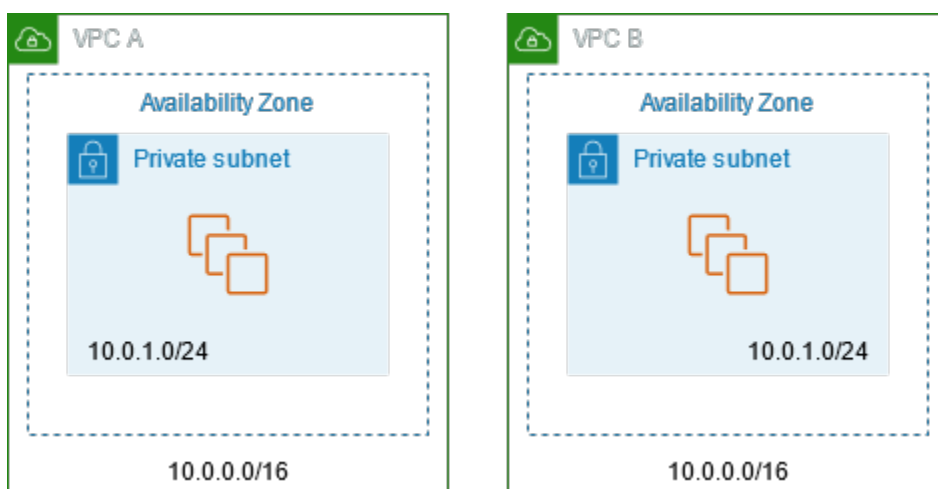
Tujuan	Target
<i>100.64.1.0/24</i>	lokal
<i>192.168.0.0/16</i>	<i>nat-gateway-id</i>

Berikut ini adalah tabel rute yang terkait dengan subnet kedua. Ada rute lokal untuk setiap CIDR VPC. 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
<i>10.0.0.0/16</i>	lokal
<i>100.64.1.0/24</i>	lokal
<i>192.168.0.0/16</i>	<i>vgw-id</i>

Aktifkan komunikasi antara jaringan yang tumpang tindih

Anda dapat menggunakan gateway NAT pribadi untuk mengaktifkan komunikasi antar jaringan bahkan jika mereka memiliki rentang CIDR yang tumpang tindih. Misalnya, misalkan instance di VPC A perlu mengakses layanan yang disediakan oleh instance di VPC B.



Daftar Isi

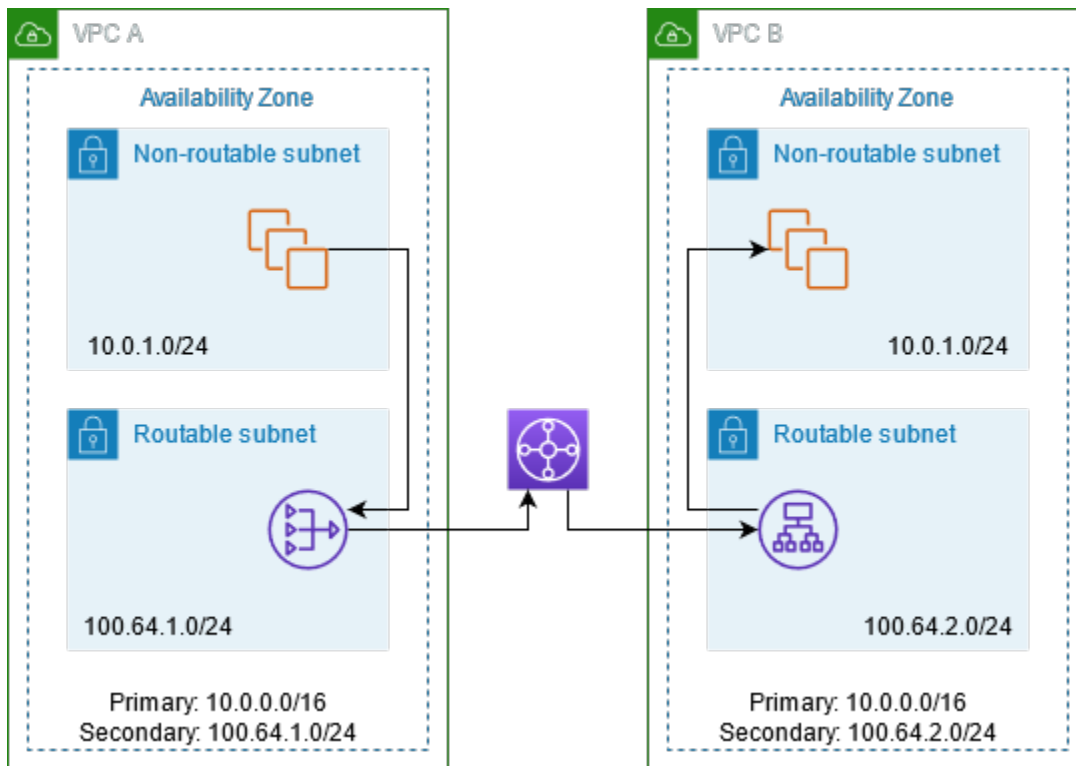
- [Gambaran Umum](#)
- [Sumber daya](#)
- [Perutean](#)

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 dirutekan) dan mana yang tidak (rentang alamat yang dapat dirutekan). Tim manajemen IP mengalokasikan rentang alamat dari kumpulan rentang alamat yang dapat dirutekan hingga proyek berdasarkan permintaan.

Setiap VPC memiliki rentang alamat IP aslinya, yang tidak dapat dirutekan, ditambah rentang alamat IP yang dapat dirutekan yang ditetapkan oleh tim manajemen IP. VPC A memiliki subnet dari jangkauan routable dengan gateway NAT pribadi. Gateway NAT pribadi mendapatkan alamat IP-nya dari subnetnya. VPC B memiliki subnet dari rentang routable dengan Application Load Balancer. Application Load Balancer mendapatkan alamat IP dari subnetnya.

Lalu lintas dari instance di subnet VPC A yang tidak dapat dirutekan yang ditujukan untuk instance di subnet VPC B yang tidak dapat dirutekan dikirim melalui gateway NAT pribadi dan kemudian dirutekan 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 dari 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 penyeimbang beban menggunakan alamat gateway NAT pribadi sebagai tujuannya. Lalu lintas respons dikirim ke gateway transit dan kemudian dirutekan ke gateway NAT pribadi, yang menerjemahkan tujuan ke instance di subnet VPC A yang tidak dapat dirutekan.



Sumber daya

Buat atau perbarui sumber daya sebagai berikut:

- Kaitkan rentang alamat IP routable yang ditetapkan dengan masing-masing VPCs.
- 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 routable, 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 VPCs. 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 yang tidak dapat dirutekan di VPC A untuk mengirim semua lalu lintas yang ditujukan untuk rentang alamat VPC B yang dapat dirutekan ke gateway NAT pribadi. Perbarui tabel rute subnet yang dapat dirutekan di VPC A untuk mengirim semua lalu lintas yang ditujukan untuk rentang alamat VPC B yang dapat dirutekan ke gateway transit.
- Perbarui tabel rute subnet yang dapat dirutekan di VPC B untuk mengirim semua lalu lintas yang ditujukan untuk rentang alamat VPC A yang dapat dirutekan ke gateway transit.

Perutean

Berikut ini adalah tabel rute untuk subnet non-routable di VPC A.

Tujuan	Target
<i>10.0.0.0/16</i>	lokal
<i>100.64.1.0/24</i>	lokal
<i>100.64.2.0/24</i>	<i>nat-gateway-id</i>

Berikut ini adalah tabel rute untuk subnet routable di VPC A.

Tujuan	Target
<i>10.0.0.0/16</i>	lokal
<i>100.64.1.0/24</i>	lokal
<i>100.64.2.0/24</i>	<i>transit-gateway-id</i>

Berikut ini adalah tabel rute untuk subnet non-routable di VPC B.

Tujuan	Target
<i>10.0.0.0/16</i>	lokal
<i>100.64.2.0/24</i>	lokal

Berikut ini adalah tabel rute untuk subnet routable di VPC B.

Tujuan	Target
<i>10.0.0.0/16</i>	lokal
<i>100.64.2.0/24</i>	lokal

Tujuan	Target
<i>100.64.1.0/24</i>	<i>transit-gateway-id</i>

Berikut ini adalah tabel rute transit gateway.

CIDR	Lampiran	Jenis rute
<i>100.64.1.0/24</i>	<i>Attachment for VPC A</i>	Statis
<i>100.64.2.0/24</i>	<i>Attachment for VPC B</i>	Statis

DNS64 dan NAT64

Gateway NAT mendukung terjemahan alamat jaringan dari IPv6 ke IPv4, yang dikenal sebagai. NAT64 NAT64 membantu IPv6 AWS sumber daya Anda berkomunikasi dengan IPv4 sumber daya dalam 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 Anda sendiri. DNS64

Daftar Isi

- [Apa itu DNS64?](#)
- [Apa itu NAT64?](#)
- [Konfigurasi DNS64 dan NAT64](#)

Apa itu DNS64?

Beban kerja IPv6 -only Anda yang berjalan hanya VPCs dapat mengirim dan menerima paket IPv6 jaringan. Tanpa DNS64, kueri DNS untuk layanan IPv4 -only akan menghasilkan alamat IPv4 tujuan sebagai respons dan layanan IPv6 -only Anda tidak dapat berkomunikasi dengannya. Untuk menjembatani kesenjangan komunikasi ini, Anda dapat mengaktifkan DNS64 subnet dan itu berlaku untuk semua AWS sumber daya dalam subnet itu. Dengan DNS64, Amazon Route 53 Resolver mencari data DNS untuk layanan yang Anda kueri dan melakukan salah satu hal berikut:

- Jika catatan berisi IPv6 alamat, ia mengembalikan catatan asli dan koneksi dibuat tanpa terjemahan apa pun IPv6.

- Jika tidak ada IPv6 alamat yang terkait dengan tujuan dalam catatan DNS, Route 53 Resolver mensintesisnya dengan mendahului /96 awalan terkenal, yang didefinisikan dalam RFC6052 (64:ff9b::/96), ke alamat dalam catatan. IPv4 Layanan IPv6 -only Anda mengirimkan paket jaringan ke alamat yang disintesis IPv6. Anda kemudian perlu merutekan lalu lintas ini melalui gateway NAT, yang melakukan terjemahan yang diperlukan pada lalu lintas untuk memungkinkan IPv6 layanan di subnet Anda mengakses IPv4 layanan di luar subnet itu.

Anda dapat mengaktifkan atau menonaktifkan DNS64 pada subnet menggunakan menggunakan AWS CLI atau dengan konsol VPC dengan memilih subnet dan memilih Actions > Edit pengaturan subnet. [modify-subnet-attribute](#)

Apa itu NAT64?

NAT64 memungkinkan layanan IPv6 -only Anda di Amazon VPCs untuk berkomunikasi dengan layanan IPv4 -only dalam VPC yang sama (dalam subnet yang berbeda) atau terhubung VPCs, di jaringan lokal Anda, atau melalui internet.

NAT64 secara otomatis tersedia di gateway NAT Anda yang ada atau di gateway NAT baru yang Anda buat. Ini bukan fitur yang Anda aktifkan atau nonaktifkan. Subnet tempat gateway NAT berada tidak perlu menjadi subnet tumpukan ganda agar dapat berfungsi. NAT64

Setelah Anda mengaktifkan DNS64, jika layanan IPv6 -only Anda mengirim paket jaringan ke IPv6 alamat yang disintesis melalui gateway NAT, hal berikut terjadi:

- Dari 64:ff9b::/96 awalan, gateway NAT mengakui bahwa tujuan asli adalah IPv4 dan menerjemahkan IPv6 paket ke dengan mengganti: IPv4
 - Sumber IPv6 dengan IP pribadinya sendiri yang diterjemahkan ke alamat IP Elastis oleh gateway internet.
 - Tujuan IPv6 ke IPv4 dengan memotong awalan. 64:ff9b::/96
- Gateway NAT mengirimkan IPv4 paket yang diterjemahkan ke tujuan melalui gateway internet, gateway pribadi virtual, atau gateway transit dan memulai koneksi.
- Host IPv4 -only mengirim kembali paket IPv4 respon. Setelah koneksi dibuat, gateway NAT menerima IPv4 paket respons dari host eksternal.
- IPv4 Paket respon ditujukan untuk gateway NAT, yang menerima paket dan de-NATs mereka dengan mengganti IP (IP tujuan) dengan alamat host dan prepending kembali ke IPv6 64:ff9b::/96 alamat sumber. IPv4 Paket kemudian mengalir ke host mengikuti rute lokal.

Dengan cara ini, gateway NAT memungkinkan beban kerja IPv6 -only Anda di subnet untuk berkomunikasi dengan layanan IPv4 -only di luar subnet.

Konfigurasi DNS64 dan NAT64

Ikuti langkah-langkah di bagian ini untuk mengonfigurasi DNS64 dan NAT64 mengaktifkan komunikasi dengan layanan IPv4 -only.

Daftar Isi

- [Aktifkan komunikasi dengan layanan IPv4 -only di internet dengan CLI AWS](#)
- [Aktifkan komunikasi dengan layanan IPv4 -only di lingkungan lokal](#)

Aktifkan komunikasi dengan layanan IPv4 -only di internet dengan CLI AWS

Jika Anda memiliki subnet dengan beban kerja IPv6 -only yang perlu berkomunikasi dengan layanan IPv4 -only di luar subnet, contoh ini menunjukkan kepada Anda cara mengaktifkan layanan -only ini untuk berkomunikasi dengan IPv4 layanan IPv6 -only di internet.

Anda harus terlebih dahulu mengonfigurasi gateway NAT di subnet publik (terpisah dari subnet yang berisi beban kerja IPv6 -only). 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 layanan IPv6 -only ini untuk terhubung dengan layanan IPv4 -only di internet:

1. Tambahkan tiga rute berikut ke tabel rute subnet yang berisi beban kerja IPv6 -only:
 - IPv4 rute (jika ada) menunjuk ke gateway NAT.
 - `64:ff9b::/96` rute yang menunjuk ke gateway NAT. Ini akan memungkinkan lalu lintas dari beban kerja IPv6 -only Anda yang ditujukan untuk layanan IPv4 -only yang akan dirutekan melalui gateway NAT.
 - IPv6 `:::/0` rute yang menunjuk ke gateway internet khusus egress (atau gateway internet).

Perhatikan bahwa menunjuk `:::/0` ke gateway internet akan memungkinkan IPv6 host eksternal (di luar VPC) untuk memulai koneksi. 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 DNS64 kemampuan 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 membangun koneksi stateful dengan keduanya IPv4 dan IPv6 layanan di internet. Konfigurasi grup keamanan Anda dan NACLs dengan tepat untuk memungkinkan lalu lintas keluar dan masuk ke lalu lintas. 64:ff9b::/96

Aktifkan komunikasi dengan layanan IPv4 -only 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 keluar Route 53 Resolver di VPC dan menetapkan alamat yang IPv4 Anda inginkan Route 53 Resolver untuk meneruskan kueri. Untuk penyelesai DNS lokal Anda, ini adalah alamat IP tempat kueri DNS berasal dan, oleh karena itu, harus berupa alamat. IPv4
- Anda membuat satu atau beberapa aturan yang menentukan nama domain kueri DNS yang ingin diteruskan Route 53 Resolver ke resolver lokal Anda. Anda juga menentukan IPv4 alamat resolver lokal.
- Sekarang setelah Anda menyiapkan titik akhir keluar Route 53 Resolver, Anda harus mengaktifkan DNS64 pada subnet yang berisi beban kerja IPv6 -only Anda dan merutekan data apa pun yang ditujukan untuk jaringan lokal Anda melalui gateway NAT.

Cara DNS64 kerja untuk tujuan IPv4 -only di jaringan lokal:

1. Anda menetapkan IPv4 alamat ke titik akhir keluar Route 53 Resolver di VPC Anda.

2. Kueri DNS dari IPv6 layanan Anda menuju ke Route 53 Resolver over. IPv6 Route 53 Resolver mencocokkan kueri dengan aturan penerusan dan mendapatkan IPv4 alamat untuk resolver lokal Anda.
3. Route 53 Resolver mengkonversi paket query dari IPv6 ke IPv4 dan meneruskannya ke endpoint keluar. Setiap alamat IP titik akhir mewakili satu ENI yang meneruskan permintaan ke IPv4 alamat lokal resolver DNS Anda.
4. Penyelesai lokal mengirimkan paket respons IPv4 kembali melalui titik akhir keluar ke Route 53 Resolver.
5. Dengan asumsi kueri dibuat dari subnet DNS64 yang diaktifkan, Route 53 Resolver melakukan dua hal:
 - a. Memeriksa isi paket respons. Jika ada IPv6 alamat dalam catatan, itu menyimpan konten apa adanya, tetapi jika hanya berisi IPv4 catatan. Ini mensintesis IPv6 catatan juga dengan mendahului `64:ff9b::/96` alamat. IPv4
 - b. Mengepak ulang konten dan mengirimkannya ke layanan di IPv6 VPC Anda.

Pantau gateway NAT dengan Amazon CloudWatch

Anda dapat memantau gateway NAT Anda menggunakan CloudWatch, yang mengumpulkan informasi dari gateway NAT Anda dan membuat metrik mendekati waktu nyata yang dapat dibaca. 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 untuk memantau operasinya dengan cermat dan memecahkan masalah apa pun dengan cepat.

Metrik gateway NAT 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 kemacetan apa pun. CloudWatch mengirimkan data metrik ini pada interval 1 menit, memberi Anda gambaran terperinci tentang perilaku up-to-the-minute gateway NAT Anda.

Selain itu, CloudWatch simpan data metrik gateway NAT ini untuk jangka waktu 15 bulan, 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 memanfaatkan 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 metrik gateway CloudWatch NAT](#)
- [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: Jumlah Statistik: Statistik yang paling berguna adalahMax.
BytesInFromDestination	Jumlah byte yang diterima oleh gateway NAT dari tujuan. Jika nilai untuk BytesOutToSource kurang dari nilai untukBytesInFromDestina tion , mungkin ada kehilangan data selama pemrosesan gateway NAT, atau lalu lintas diblokir secara aktif oleh gateway NAT.

Metrik	Deskripsi
	Unit: Bit Statistik: Statistik yang paling berguna adalah Sum.
BytesInFromSource	Jumlah byte yang diterima oleh gateway NAT dari klien di VPC Anda. Jika nilai untuk BytesOutToDestination kurang dari nilai untuk BytesInFromSource, mungkin ada kehilangan data selama pemrosesan gateway NAT. Unit: Bit Statistik: Statistik yang paling berguna adalah Sum.
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 untuk BytesInFromSource, mungkin ada kehilangan data selama pemrosesan gateway NAT. Unit: Bit Statistik: Statistik yang paling berguna adalah Sum.

Metrik	Deskripsi
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 untuk BytesInFromDestination, mungkin ada kehilangan data selama pemrosesan gateway NAT, atau lalu lintas diblokir secara aktif oleh gateway NAT. Unit: Bit Statistik: Statistik yang paling berguna adalah Sum.
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 adalah Sum.

Metrik	Deskripsi
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.
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: Jumlah Statistik: Statistik yang paling berguna adalahSum.

Metrik	Deskripsi
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, ini 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: $\text{PacketsDropCount} / (\text{PacketsInFromSource} + \text{PacketsInFromDestination}) * 100$. Jika nilai ini melebihi 0,01 persen dari total lalu lintas di gateway NAT, mungkin ada masalah dengan layanan Amazon VPC. Gunakan dasbor kesehatan AWS layanan untuk mengidentifikasi masalah apa pun dengan layanan yang mungkin menyebabkan gateway NAT menjatuhkan paket. Unit: Jumlah Statistik: Statistik yang paling berguna adalah Sum.
PacketsInFromDestination	Jumlah paket yang diterima oleh gateway NAT dari tujuan. Jika nilai untuk PacketsOutToSource kurang dari nilai untuk PacketsInFromDestination, mungkin ada kehilangan data selama pemrosesan gateway NAT, atau lalu lintas diblokir secara aktif oleh gateway NAT. Unit: Jumlah Statistik: Statistik yang paling berguna adalah Sum.

Metrik	Deskripsi
PacketsInFromSource	Jumlah paket yang diterima oleh gateway NAT dari klien di VPC Anda. Jika nilai untuk PacketsOutToDestination kurang dari nilai untuk PacketsInFromSource, mungkin ada kehilangan data selama pemrosesan gateway NAT. Unit: Jumlah Statistik: Statistik yang paling berguna adalah Sum.
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 untuk PacketsInFromSource, mungkin ada kehilangan data selama pemrosesan gateway NAT. Unit: Jumlah Statistik: Statistik yang paling berguna adalah Sum.

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 untuk PacketsInFromDestination, mungkin ada kehilangan data selama pemrosesan gateway NAT, atau lalu lintas diblokir secara aktif oleh gateway NAT. Unit: Jumlah Statistik: Statistik yang paling berguna adalah Sum.
PeakBytesPerSecond	Metrik ini melaporkan rata-rata 10 detik byte per detik tertinggi dalam satu menit tertentu. Unit: Jumlah Statistik: Statistik yang paling berguna adalah Maximum.
PeakPacketsPerSecond	Metrik ini menghitung laju paket rata-rata (paket diproses per detik) setiap 10 detik selama 60 detik dan kemudian melaporkan maksimum enam tingkat (tingkat paket rata-rata tertinggi). Unit: Jumlah Statistik: Statistik yang paling berguna adalah Maximum.

Untuk mem-filter data metrik, gunakan dimensi berikut.

Dimensi	Deskripsi
NatGatewayId	Filter data metrik berdasarkan ID gateway NAT.

Lihat metrik gateway CloudWatch NAT

Metrik gateway NAT dikirim ke CloudWatch interval 1 menit. Metrik dikelompokkan terlebih dahulu 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 konsol CloudWatch

1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Pada panel navigasi, silakan pilih Metrik, Semua metrik.
3. Pilih namespace NATGatewaymetrik.
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 NATGatewaymetrik dan kemudian pilih dimensi metrik. Saat Anda masuk ke metrik, pilih kotak centang di sebelah BytesOutToDestinationmetrik untuk gateway NAT, lalu pilih Pilih metrik.
6. Konfigurasi alarm sebagai berikut, lalu pilih Next (Selanjutnya):
 - Untuk Statistik pilih Jumlah.
 - Untuk Periode, pilih 15 menit.
 - Untuk Kapan pun, pilih Greater/Equal dan masukkan 5000000 untuk ambang batas.
7. Untuk Pemberitahuan, 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 Berikutnya.
9. Setelah selesai mengonfigurasi 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 NATGatewaymetrik dan kemudian pilih dimensi metrik. Saat Anda masuk ke metrik, pilih kotak centang di sebelah ErrorPortAllocationmetrik untuk gateway NAT, lalu pilih Pilih metrik.
6. Konfigurasi alarm sebagai berikut, lalu pilih Next (Selanjutnya):
 - Untuk Statistik, pilih Maksimum.

- Untuk Periode, pilih 5 menit.
 - Untuk Kapan pun, pilih Lebih Besar dan masukkan 0 untuk ambang batas.
 - Untuk konfigurasi tambahan, Datapoint ke alarm, masukkan 3.
7. Untuk Pemberitahuan, 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 Berikutnya.
 9. Setelah selesai mengonfigurasi 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. Untuk membuat alamat IP gratis di subnet Anda, Anda dapat menghapus antarmuka jaringan yang tidak terpakai, atau mengakhiri instans yang tidak Anda butuhkan.

Kesalahan ditampilkan	Penyebab	Solusi
Jaringan vpc-xxxxxxx 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 Tambahkan akses internet ke subnet .
Alamat IP Elastis eipalloc-xxxxxxx 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 memerlukan 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 Elastis .

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 [Mencatat lalu lintas IP menggunakan VPC Flow Logs](#).

- 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 hal berikut ini:

- 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 gateway NAT

Ketika Anda menyediakan gateway NAT, Anda dikenakan biaya untuk setiap jam bahwa gateway NAT Anda tersedia dan setiap gigabyte data yang diproses. 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 Availability Zone, pastikan sumber daya berada di Availability Zone yang sama dengan gateway NAT. Atau, buat gateway NAT di setiap Availability Zone dengan sumber daya.
- Jika sebagian besar lalu lintas melalui gateway NAT Anda adalah ke 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 lebih lanjut tentang potensi penghematan biaya, lihat [AWS PrivateLink harga](#).

Instans NAT

Sebuah contoh NAT menyediakan terjemahan alamat jaringan (NAT). Anda dapat menggunakan instans NAT untuk memungkinkan sumber daya di subnet pribadi berkomunikasi dengan tujuan di luar virtual private cloud (VPC), seperti internet atau jaringan lokal. Sumber daya di subnet pribadi dapat memulai IPv4 lalu lintas keluar ke internet, tetapi mereka tidak dapat menerima lalu lintas masuk yang dimulai di internet.

Important

NAT AMI dibangun di atas versi terakhir 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 sudah ada, AWS sarankan Anda [bermigrasi ke gateway NAT](#). Gateway NAT menyediakan 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 dalam [the section called “3. Buat NAT AMI”](#)

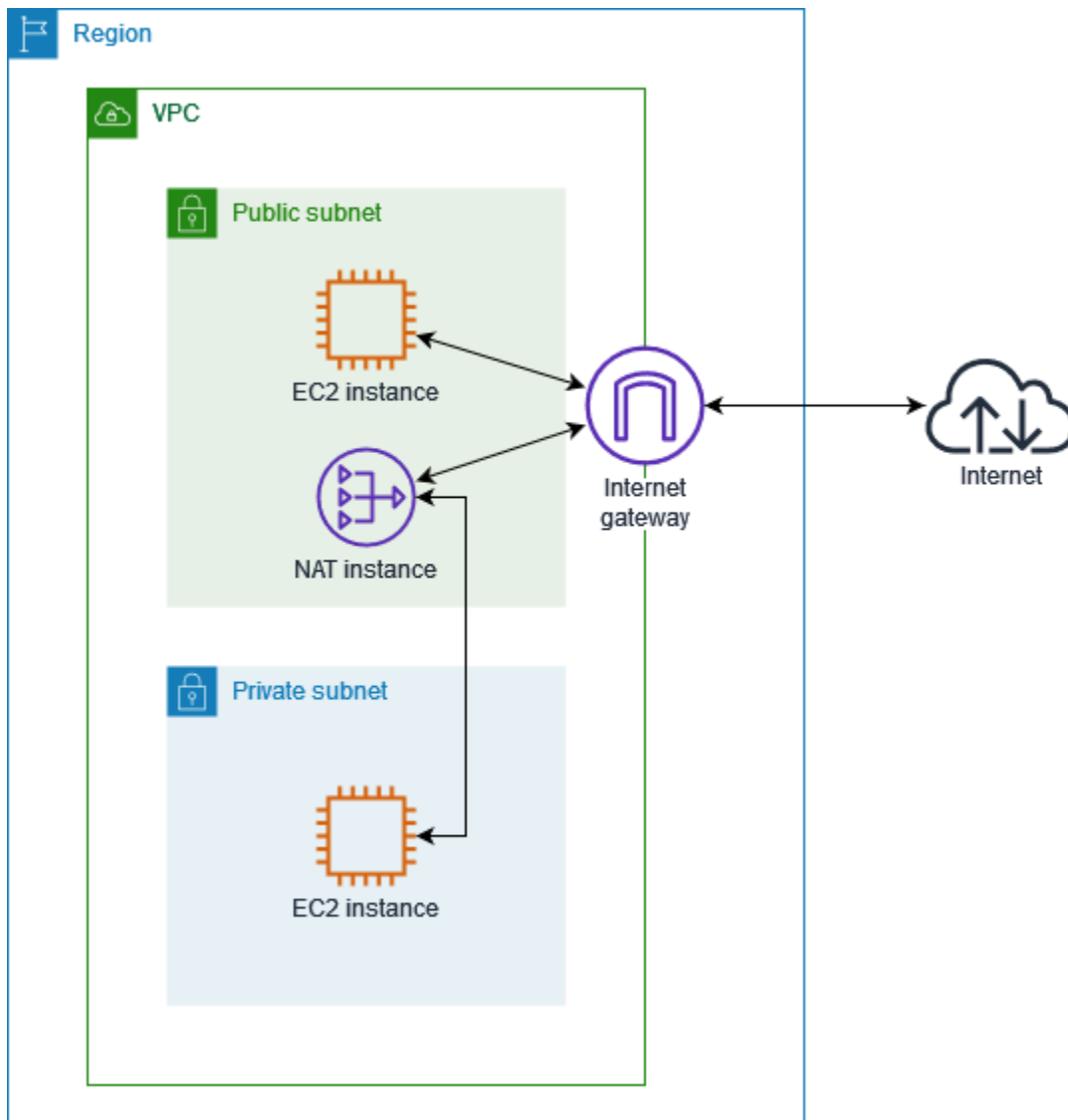
Daftar Isi

- [Dasar-dasar instans NAT](#)
- [Memungkinkan 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 dalam subnet publik (subnet yang memiliki tabel rute dengan rute ke gateway internet), dan harus memiliki alamat IP publik atau alamat IP Elastis.



Untuk memulai instans NAT, buat NAT AMI, buat grup keamanan untuk instans NAT, dan luncurkan instance NAT ke VPC Anda.

Kuota instans NAT Anda tergantung pada kuota instans Anda untuk Wilayah. Untuk informasi selengkapnya, lihat [kuota EC2 layanan Amazon](#) di. Referensi Umum AWS

Memungkinkan 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. [Buat VPC untuk instance NAT](#)

- [2. Buat grup keamanan untuk instance NAT](#)
- [3. Buat NAT AMI](#)
- [4. Luncurkan instance NAT](#)
- [5. Nonaktifkan pemeriksaan sumber/tujuan](#)
- [6. Perbarui tabel rute](#)
- [7. Uji instans NAT Anda](#)

1. Buat 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. Agar Sumber Daya dapat 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 Availability Zone, pilih 1 atau 2, tergantung kebutuhan Anda.
 - b. Untuk Jumlah subnet publik, pastikan Anda memiliki satu subnet publik per Availability Zone.
 - c. Untuk Jumlah subnet pribadi, pastikan Anda memiliki satu subnet pribadi per Availability Zone.
6. Pilih Buat VPC.

2. Buat grup keamanan untuk instance NAT

Buat grup keamanan dengan aturan yang dijelaskan dalam tabel berikut. Aturan ini memungkinkan instans NAT Anda menerima lalu lintas 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 yang direkomendasikan masuk.

Sumber	Protokol	Rentang Port	Komentar
<i>Private subnet CIDR</i>	TCP	80	Izinkan lalu lintas HTTP masuk dari server di subnet privat
<i>Private subnet CIDR</i>	TCP	443	Izinkan lalu lintas HTTPS masuk dari server di subnet privat
<i>Public IP address range of your network</i>	TCP	22	Izinkan akses SSH masuk ke instans 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. Di 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 instans 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 sebuah EC2 instance. Anda harus membuat NAT AMI dan kemudian meluncurkan instans NAT Anda menggunakan NAT AMI Anda.

Jika Anda berencana untuk 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 instance reboot.

Untuk membuat NAT AMI untuk Amazon Linux

1. Luncurkan EC2 instance yang menjalankan AL2 023 atau Amazon Linux 2. Pastikan untuk menentukan grup keamanan yang Anda buat untuk instance NAT.
2. Connect 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 sedemikian rupa sehingga tetap ada setelah reboot:
 - a. Menggunakan editor teks, seperti nano atau vim, 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 perhatikan nama antarmuka jaringan utama. Anda akan memerlukan informasi ini untuk langkah selanjutnya.

```
netstat -i
```

Dalam contoh output berikut, `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 EC2 instance. Untuk informasi selengkapnya, lihat [Membuat AMI Linux dari instans](#) di Panduan EC2 Pengguna Amazon.

4. Luncurkan instance NAT

Gunakan prosedur berikut untuk meluncurkan instans NAT menggunakan VPC, grup keamanan, dan NAT AMI yang Anda buat.

Untuk meluncurkan instance NAT

1. Buka EC2 konsol Amazon 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 Browse more AMIs, My AMIs).
5. Untuk tipe Instance, pilih jenis instans yang menyediakan sumber daya komputasi, memori, dan penyimpanan yang dibutuhkan instans NAT Anda.
6. Untuk Key pair, pilih key pair yang ada atau pilih Create new key pair.
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 Auto-assign IP publik, pilih Aktifkan. Atau, setelah Anda meluncurkan instance NAT, alokasikan alamat IP Elastis dan tetapkan ke instance NAT.
 - e. Untuk Firewall, pilih Pilih grup keamanan yang ada, lalu pilih grup keamanan yang Anda buat.
8. Pilih Luncurkan instans. Pilih ID instance untuk membuka halaman detail instance. Tunggu status instance berubah menjadi Running dan agar pemeriksaan status berhasil.
9. Nonaktifkan pemeriksaan sumber/tujuan untuk instance NAT (lihat). [5. Nonaktifkan pemeriksaan sumber/tujuan](#)
10. Perbarui tabel rute untuk mengirim lalu lintas ke instance NAT (lihat [6. Perbarui tabel rute](#)).

5. Nonaktifkan pemeriksaan sumber/tujuan

Setiap EC2 instance melakukan source/destination checks by default. This means that the instance must be the source or destination of any traffic it sends or receives. However, a NAT instance must be able to send and receive traffic when the source or destination is not itself. Therefore, you must disable source/destination pemeriksaan pada instance NAT.

Untuk menonaktifkan pemeriksaan sumber/tujuan

1. Buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Di panel navigasi, pilih Instans.
3. Pilih contoh NAT.
4. Pilih Tindakan, Jaringan, Ubah pemeriksaan sumber/tujuan.
5. Untuk pemeriksaan sumber/tujuan, 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 Tindakan, Ubah pemeriksaan sumber/tujuan, 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 dan kemudian pilih Tambah rute.
5. Masukkan 0.0.0.0/0 untuk Destination dan ID instance dari instance NAT untuk Target.
6. Pilih Simpan perubahan.

Untuk informasi selengkapnya, lihat [Konfigurasi tabel rute](#).

7. Uji instans NAT Anda

Setelah Anda meluncurkan instans NAT dan menyelesaikan langkah-langkah konfigurasi di atas, Anda dapat menguji apakah sebuah instance di subnet pribadi Anda dapat mengakses internet melalui instance NAT dengan menggunakan instance NAT sebagai server bastion.

Tugas

- [Langkah 1: Perbarui grup keamanan instans NAT](#)
- [Langkah 2: Luncurkan instance pengujian di subnet pribadi](#)
- [Langkah 3: Ping situs web berkemampuan ICMP](#)
- [Langkah 4: Membersihkan](#)

Langkah 1: Perbarui grup keamanan instans NAT

Untuk mengizinkan instance di subnet pribadi Anda mengirim lalu lintas ping ke instans NAT, tambahkan aturan untuk mengizinkan lalu lintas ICMP masuk dan keluar. Untuk memungkinkan instance NAT berfungsi sebagai server bastion, tambahkan aturan untuk mengizinkan lalu lintas SSH keluar ke subnet pribadi.

Untuk memperbarui grup keamanan instans NAT Anda

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>
2. Di 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 Jenis. Pilih Custom for Source 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 Custom for Destination dan masukkan rentang alamat IP subnet pribadi Anda.
8. Pilih Tambahkan aturan. Pilih Semua ICMP - IPv4 untuk Jenis. Pilih Di Mana Saja - IPv4 untuk Tujuan. Pilih Simpan aturan.

Langkah 2: Luncurkan instance pengujian di subnet pribadi

Luncurkan sebuah instans ke subnet privat Anda. Anda harus mengizinkan akses SSH dari instance NAT, dan Anda harus menggunakan key pair yang sama dengan yang Anda gunakan untuk instance NAT.

Untuk meluncurkan instance pengujian di subnet pribadi

1. Buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Pada dasbor, pilih Luncurkan instans.
3. Pilih subnet pribadi Anda.
4. Jangan menetapkan alamat IP publik untuk contoh ini.
5. Pastikan bahwa grup keamanan untuk contoh ini memungkinkan akses SSH masuk dari instans NAT Anda, atau dari rentang alamat IP subnet publik Anda, dan lalu lintas ICMP keluar.
6. Pilih key pair yang sama yang Anda gunakan untuk instance NAT.

Langkah 3: Ping situs web berkemampuan ICMP

Untuk memverifikasi bahwa instance pengujian di subnet pribadi Anda dapat menggunakan instance NAT Anda untuk berkomunikasi dengan internet, jalankan perintah. ping

Untuk menguji koneksi internet dari instans pribadi Anda

1. Dari komputer lokal Anda, konfigurasi 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, klik kanan ikon Pageant di taskbar (mungkin disembunyikan), dan pilih Add Key. Pilih file.ppk yang Anda buat, masukkan frasa sandi jika diperlukan, dan pilih Buka.

2. Dari komputer lokal Anda, sambungkan ke instans NAT Anda.

Linux and macOS

```
ssh -A ec2-user@nat-instance-public-ip-address
```

Windows

Connect ke instans NAT Anda menggunakan PuTTY. Untuk Auth, Anda harus memilih Izinkan 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 instans 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 rutenya 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 instans NAT Anda, sambungkan ke instans 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 instans 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.
- Verifikasi bahwa grup keamanan untuk instans NAT Anda memungkinkan lalu lintas ICMP masuk dari subnet pribadi Anda. Jika tidak, instans NAT Anda tidak dapat menerima ping perintah dari instance pribadi Anda.
- Verifikasi bahwa Anda menonaktifkan pemeriksaan sumber/tujuan untuk instans NAT Anda. Untuk informasi selengkapnya, lihat [5. Nonaktifkan pemeriksaan sumber/tujuan](#).
- Verifikasi bahwa 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 instance sehingga Anda tidak lagi ditagih untuk itu. Untuk informasi selengkapnya, lihat [Menghentikan instans Anda](#) di Panduan EC2 Pengguna Amazon.

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.
Kinerja	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 menentukan tipe atau ukurannya.	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.
Jaringan ACLs	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 instans 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, dan kemudian mengganti rute yang ada di tabel rute Anda yang menunjuk ke instance NAT dengan rute yang menunjuk ke gateway NAT. Untuk menggunakan alamat IP Elastis yang sama untuk gateway NAT yang saat ini Anda gunakan untuk instans NAT Anda, Anda harus terlebih dahulu memisahkan alamat IP Elastis dari instans NAT Anda dan kemudian mengaitkannya dengan gateway NAT Anda 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.

Kaitkan alamat IP Elastis dengan sumber daya di VPC Anda

Alamat IP Elastis adalah IPv4 alamat publik statis yang dirancang khusus untuk sifat dinamis komputasi awan. Fitur ini memungkinkan Anda untuk mengaitkan alamat IP Elastis dengan instans atau antarmuka jaringan apa pun dalam Virtual Private Cloud (VPC) apa pun di akun Anda. AWS Dengan memanfaatkan 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 instans. Jika sebuah instans mengalami pemadaman yang tidak terduga atau perlu diganti, Anda dapat memetakan ulang alamat IP Elastis 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 waktu henti dan memberikan pengalaman pengguna yang unggul.

Selain itu, alamat IP Elastic menawarkan fleksibilitas dalam cara Anda mengelola sumber daya jaringan Anda. Anda dapat mengasosiasikan dan memisahkan alamat-alamat ini secara terprogram sesuai kebutuhan, memungkinkan Anda mengarahkan lalu lintas ke berbagai contoh berdasarkan kebutuhan bisnis Anda yang berkembang. Alokasi dinamis alamat IP publik ini memberdayakan Anda untuk beradaptasi dengan perubahan permintaan, skala infrastruktur Anda, dan menerapkan arsitektur inovatif tanpa kendala penetapan IP statis.

Selain 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 AWS-host Anda. Dengan mengaitkan alamat IP publik yang persisten, Anda dapat membuktikan konfigurasi jaringan Anda di masa depan dan menghindari kebutuhan untuk memperbarui referensi eksternal ketika instance yang mendasarinya diganti atau diskalakan.

Daftar Isi

- [Konsep dan aturan alamat IP Elastis](#)
- [Mulai gunakan alamat IP Elastis](#)

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 Elastis Anda tetap dialokasikan ke AWS akun Anda sampai Anda melepaskannya secara eksplisit.

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 EC2 Pengguna Amazon.

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 Elastis dengan antarmuka jaringan utama instans Anda, IPv4 alamat publiknya saat ini (jika ada) dilepaskan ke kumpulan alamat IP publik. Jika Anda memisahkan alamat IP Elastis, antarmuka jaringan utama secara otomatis diberi IPv4 alamat 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 [Connect ke internet atau jaringan lain menggunakan perangkat NAT](#).

- Alamat IP elastis untuk IPv6 tidak didukung.
- 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, silakan lihat [Grup keamanan](#) dan [Jaringan ACLs](#).
- 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 [Membawa alamat IP Anda sendiri \(BYOIP\)](#) di EC2 Panduan Pengguna Amazon.
- IPv4 Alamat publik mendukung tag alokasi biaya. Jika Anda menerapkan tag ke alamat IP Elastis, Anda dapat menggunakan tag tersebut untuk melacak biaya IPv4 alamat publik 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 pengguna](#) di Panduan Pengguna AWS Billing. 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 IPv4 alamat publik (termasuk IPv4 alamat publik yang ditetapkan ke EC2 instans dan alamat IP Elastis) yang terkait dengan elastic network interface, Anda dapat melihat biaya yang terkait dengan IPv4 alamat publik di Cost Explorer dengan memilih Usage type > Public IPv4 InUseAddress (Hrs).
- Jika alamat IP Elastic yang ditandai tidak terkait dengan ENI atau dikaitkan dengan sumber daya yang dihentikan (seperti EC2 instance yang dihentikan), itu dianggap sebagai alamat idle IPv4. Anda dapat melihat biaya yang terkait dengan IPv4 alamat idle di Cost Explorer dengan memilih Usage type > Public IPv4 IdleAddress (Hrs).

Untuk informasi selengkapnya tentang Cost Explorer, lihat [Menganalisis biaya Anda AWS Cost Explorer](#) di 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 alamat IP Elastis, lihat [IPv4 Alamat publik di Harga VPC Amazon](#).

Mulai gunakan alamat IP Elastis

Bagian berikut menjelaskan bagaimana Anda dapat mulai menggunakan alamat IP Elastis.

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 Elastic IPs.
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 Availability Zones (AZs), Local Zones, atau Wavelength Zones AWS yang mengiklankan alamat IP publik. Local Zones dan Wavelength Zones mungkin memiliki grup perbatasan jaringan yang berbeda dari AZs di Wilayah untuk memastikan latensi minimum atau jarak fisik antara jaringan dan pelanggan yang mengakses sumber AWS 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 Zona Lokal atau Aktifkan Zona Wavelength](#)), Anda dapat memilih grup perbatasan jaringan untuk, Local Zones, atau Wavelength Zones. 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 EC2 konsol untuk melihat grup perbatasan jaringan tempat Availability Zone, Local Zones, atau Wavelength Zones 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 Zones, ketika Anda mengalokasikan EIP, grup perbatasan jaringan yang mewakili semua untuk Wilayah (us-west-2 seperti) 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 wilayah tempat Anda berada.

5. Untuk kumpulan IPv4 alamat Publik pilih salah satu dari berikut ini:

- Kumpulan alamat IP Amazon —Jika Anda ingin IPv4 alamat dialokasikan dari kumpulan alamat IP Amazon.
- Kumpulan IPv4 alamat publik saya —Jika Anda ingin mengalokasikan IPv4 alamat dari kumpulan alamat IP yang telah Anda bawa ke akun Anda AWS. Opsi ini dinonaktifkan jika Anda tidak memiliki kumpulan alamat IP.
- Kumpulan IPv4 alamat milik pelanggan —Jika Anda ingin mengalokasikan IPv4 alamat dari kumpulan yang dibuat dari jaringan lokal untuk digunakan dengan Outpost. Opsi ini hanya tersedia jika Anda memiliki Outpost.

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 tanda] Pilih Hapus di sebelah kanan Kunci dan Nilai tanda.

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 panel navigasi, pilih Elastic IPs.
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 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 panel navigasi, pilih Elastic IPs.
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 Anda dan NACLs.
- **Administrasi keamanan terpusat** — Gunakan akun AWS keamanan terpusat untuk melacak dan mentransfer alamat IP Elastis yang telah diperiksa untuk kepatuhan keamanan.
- **Pemulihan bencana** - Gunakan transfer alamat IP Elastis untuk memetakan ulang beban kerja internet yang dihadapi publik dengan cepat IPs selama acara 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 Elastis dari Akun AWS (akun sumber) apa pun ke AWS akun lain di AWS Wilayah 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 itu, akun sumber dapat melihat transfer yang tertunda (misalnya di AWS konsol atau dengan menggunakan [describe-address-transfers](#) AWS CLI perintah). Setelah tujuh hari, transfer berakhir dan kepemilikan alamat IP Elastis kembali ke akun sumber.
- Transfer yang diterima dapat dilihat oleh akun sumber (misalnya di AWS konsol atau dengan menggunakan [describe-address-transfers](#) AWS CLI perintah) selama 14 hari setelah transfer diterima.

- AWS tidak memberi tahu akun transfer tentang permintaan transfer alamat IP Elastis 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 Elastis yang dialokasikan dari kumpulan IPv4 alamat publik yang Anda bawa ke kumpulan Akun AWS alamat Bring Your Own IP (BYOIP).
- Jika Anda mencoba mentransfer alamat IP Elastis yang memiliki catatan DNS terbalik yang terkait dengannya, Anda dapat memulai proses transfer, tetapi akun transfer tidak akan 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 IP milik pelanggan](#) di Panduan Pengguna AWS Outposts .
- 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 Elastic IPs.
4. Pilih satu atau beberapa alamat IP elastis untuk mengaktifkan transfer dan pilih Tindakan, Aktifkan transfer.
5. Jika Anda mentransfer beberapa alamat IP Elastis, Anda akan melihat opsi Tipe transfer. Pilih salah satu opsi berikut:
 - Pilih Akun tunggal jika Anda mentransfer alamat IP Elastis ke satu AWS akun.
 - Pilih Beberapa akun jika Anda mentransfer alamat IP Elastis ke beberapa AWS akun.
6. Di bawah Transfer ID akun, masukkan AWS akun yang ingin Anda transfer alamat IP Elastis. IDs

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 Elastic IPs.
4. Dalam daftar sumber daya Elastic IPs, 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 itu, akun sumber dapat melihat transfer yang tertunda (misalnya di AWS konsol atau dengan menggunakan [describe-address-transfers](#) AWS CLI perintah). 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 EC2 Pengguna Amazon untuk petunjuk tentang cara meningkatkan batas.

- **InvalidTransfer. AddressCustomPtrSet:** Jika Anda atau seseorang di organisasi Anda telah mengonfigurasi alamat IP Elastis yang Anda coba transfer untuk menggunakan pencarian DNS terbalik, akun sumber dapat mengaktifkan transfer untuk alamat IP Elastis, tetapi 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 [Menghapus catatan DNS terbalik](#) di Panduan EC2 Pengguna Amazon.
- **InvalidTransfer. AddressAssociated:** Jika alamat IP Elastis dikaitkan dengan ENI atau EC2 instans, akun sumber dapat mengaktifkan transfer untuk alamat IP Elastis, 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 [Memutuskan alamat IP Elastis](#) di Panduan EC2 Pengguna Amazon.

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 Elastic IPs.
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 instans. 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 panel navigasi, pilih Elastic IPs.
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 Elastis 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 Elastis dengan menggunakan Amazon EC2 API atau alat baris perintah.

Untuk memulihkan alamat IP Elastis 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

- [accept-address-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

- [describe-address-transfers](#) (AWS CLI)
- [Get-EC2AddressTransfer](#) (AWS Tools for Windows PowerShell)

Nonaktifkan transfer alamat IP Elastis

- [disable-address-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

- [enable-address-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 jaringan lain VPCs dan menggunakan gateway transit

Anda dapat menghubungkan virtual private cloud (VPC) dan jaringan lokal menggunakan gateway transit, yang bertindak sebagai hub pusat, merutekan lalu lintas antara, koneksi VPN VPCs, dan koneksi. AWS Direct Connect

Salah satu manfaat utama menggunakan gateway transit adalah kemampuan untuk memusatkan dan menyederhanakan pengelolaan konektivitas antara jaringan Anda VPCs dan jaringan lokal. Daripada mengonfigurasi beberapa koneksi VPN atau tautan Direct Connect, Anda dapat memanfaatkan 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 sewaktu-waktu, jadi penting untuk merujuk ke halaman AWS Transit Gateway harga saat ini untuk up-to-date informasi terbanyak. Dengan memahami model harga untuk gateway transit, Anda dapat merencanakan dan menganggarkan dengan lebih baik untuk biaya berkelanjutan yang terkait dengan layanan AWS jaringan ini. Hal ini, dikombinasikan dengan efisiensi operasional dan manfaat konektivitas, menjadikan gateway transit pilihan menarik bagi organisasi yang ingin membangun solusi cloud hybrid yang terukur 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 AWS Site-to-Site VPN koneksi Anda VPCs AWS Direct Connect, dan.
Terisolasi VPCs	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.
Terisolasi VPCs 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.

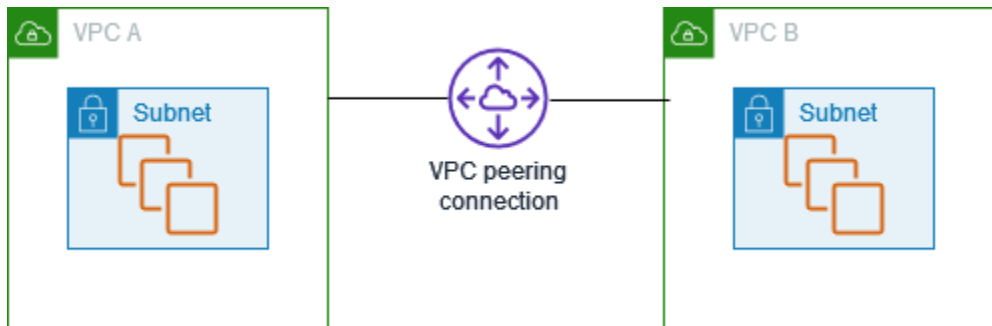
Opsi koneksi VPN	Deskripsi
AWS Site-to-Site VPN	Anda dapat membuat koneksi IPsec VPN antara VPC Anda dan jaringan jarak jauh Anda. Di AWS sisi koneksi Site-to-Site VPN, gateway pribadi virtual atau gateway transit menyediakan dua titik akhir VPN (terowongan) untuk failover otomatis. Anda mengonfigurasi 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 mengaktifkan 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 menjalankan 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 AWS 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 AWS Direct Connect?](#) dalam AWS Direct Connect User Guide.

Connect VPCs menggunakan VPC peering

Koneksi peering VPC adalah fitur jaringan yang memungkinkan komunikasi yang aman dan langsung antara dua awan pribadi virtual (VPCs) dalam infrastruktur. AWS Koneksi pribadi ini memungkinkan sumber daya di peered VPCs 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 memanfaatkan infrastruktur VPC yang ada untuk membangun koneksi ini, tanpa memerlukan 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 terhubung di VPCs berbagai AWS akun 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 dari koneksi juga memastikan bahwa semua lalu lintas data antara peered VPCs tetap berada dalam AWS jaringan, tanpa pernah melintasi internet publik.

Kasus penggunaan untuk koneksi peering VPC sangat luas. Organizations dapat memanfaatkan fitur ini untuk memungkinkan komunikasi yang aman antara berbagai tingkatan aplikasi (seperti server web dan server database), memfasilitasi berbagi sumber daya antara beberapa tim atau unit bisnis, atau bahkan mengaktifkan arsitektur cloud hybrid dengan menghubungkan jaringan lokal ke jaringan mereka. AWS VPCs

Koneksi peering VPC adalah koneksi jaringan antara dua VPCs yang memungkinkan Anda untuk mengarahkan lalu lintas di antara mereka secara pribadi. Sumber daya di peered VPCs dapat berkomunikasi satu sama lain seolah-olah mereka berada dalam jaringan yang sama. Anda dapat membuat koneksi peering VPC antara Anda sendiri VPCs, dengan VPC di tempat lain, Akun AWS atau dengan VPC di Wilayah yang berbeda. AWS Lalu lintas antar peered VPCs 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 EC2 instans Amazon 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 EC2 API Amazon menggunakan AWS CloudTrail](#) dalam Panduan EC2 Pengguna Amazon.

Mencatat lalu lintas IP menggunakan VPC Flow Logs

Log Alur VPC adalah 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 Log, 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 aliran, 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 VPCs. Untuk informasi tentang log aliran untuk gateway transit yang diperkenalkan di versi 6, lihat [Mencatat lalu lintas jaringan menggunakan Log Aliran Gateway Transit Transit di Panduan Pengguna Gateway Transit VPC Amazon](#).

Daftar Isi

- [Dasar-dasar log alur](#)
- [Catatan log alur](#)
- [Contoh catatan log alur](#)
- [Batasan log alur](#)
- [Harga](#)
- [Bekerja dengan log alur](#)
- [Publikasikan log aliran ke CloudWatch Log](#)
- [Terbitkan log alur ke Amazon S3](#)
- [Publikasikan log alur ke Amazon Data Firehose](#)
- [Log alur kueri menggunakan Amazon Athena](#)
- [Mengatasi masalah Log Alur VPC](#)

Dasar-dasar log alur

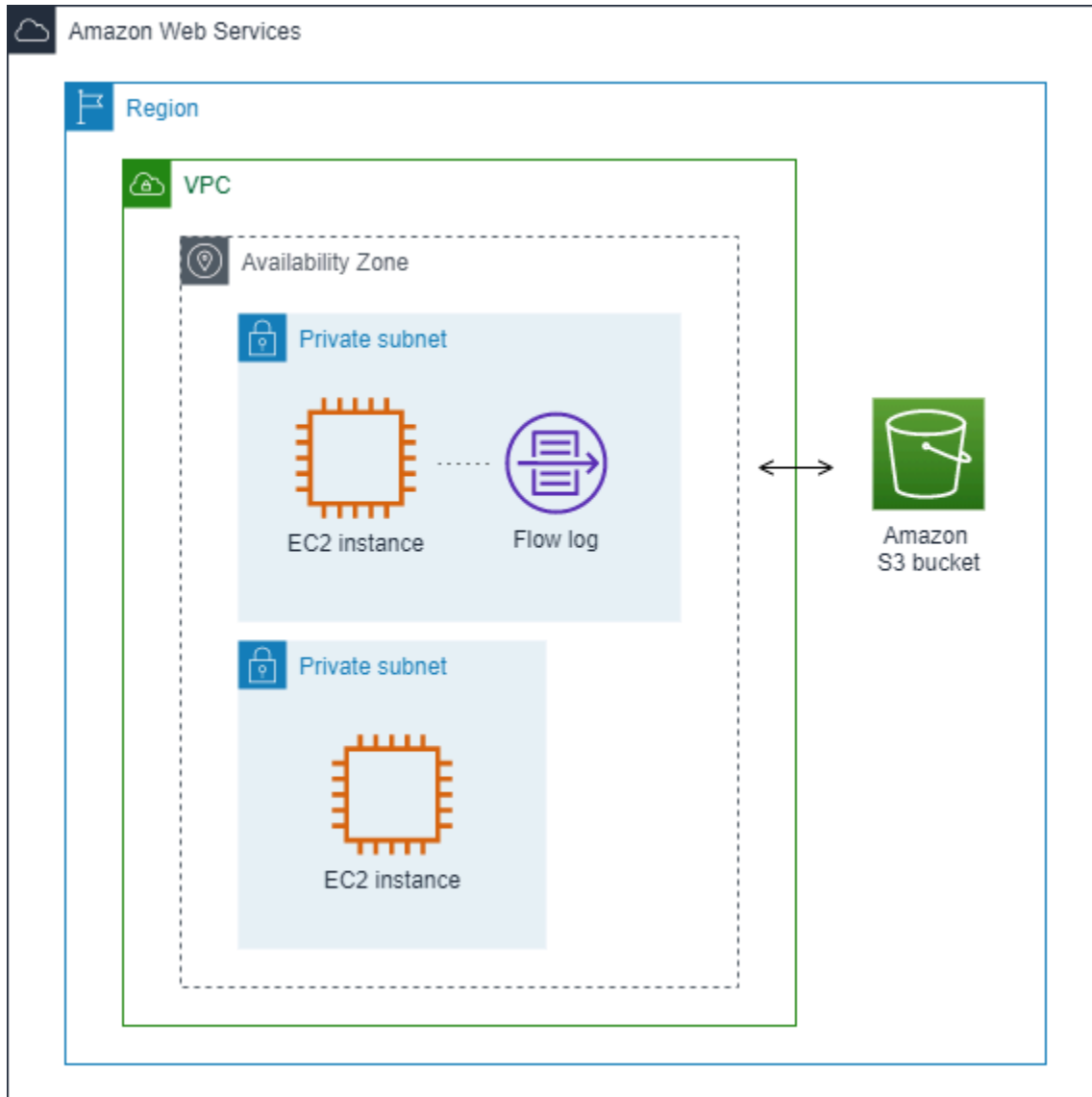
Anda dapat membuat log alur untuk VPC, subnet, atau antarmuka jaringan. Jika Anda membuat log alur untuk subnet atau VPC, setiap antarmuka jaringan di subnet atau VPC dipantau.

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](#).

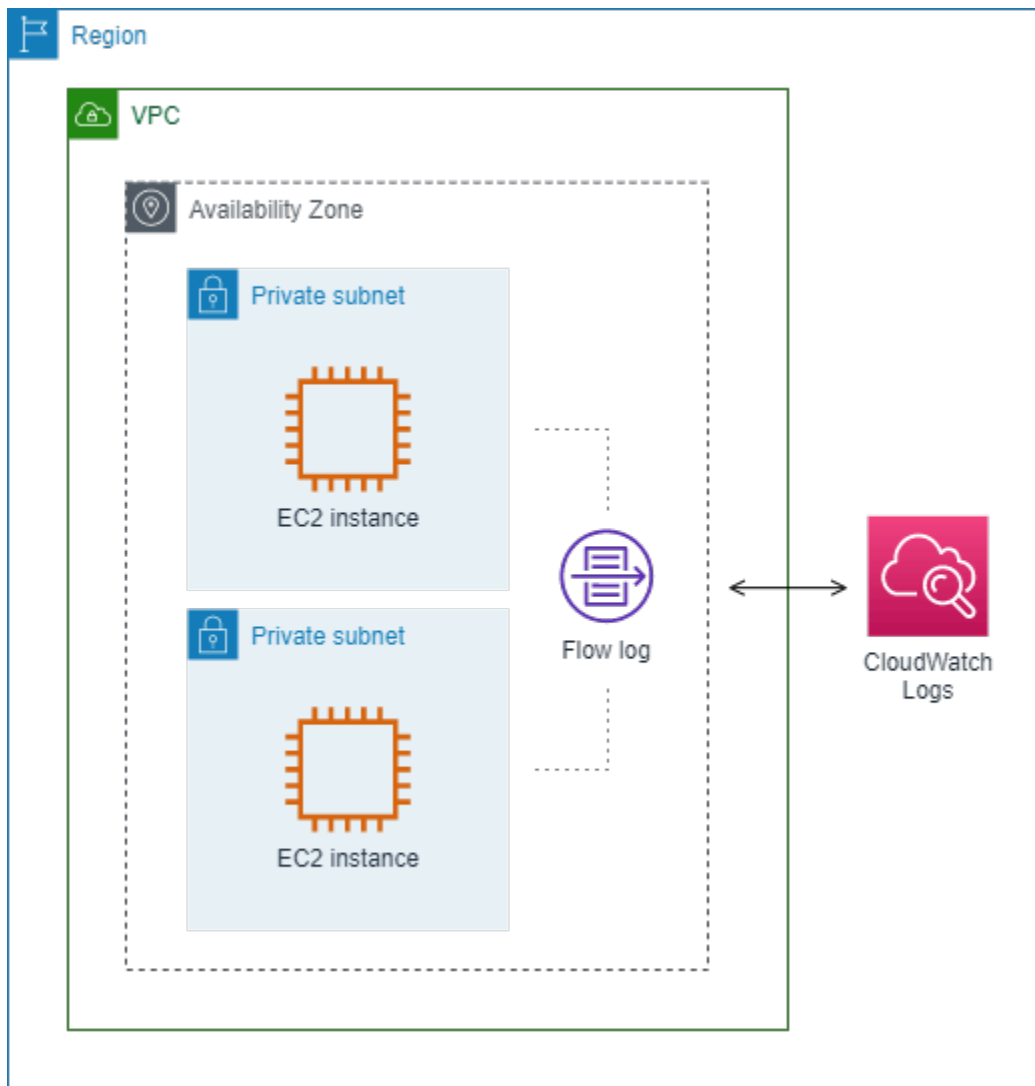
Untuk membuat log alur, Anda menentukan:

- 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 EC2 instance di subnet pribadi dan menerbitkan catatan log alur ke bucket Amazon S3.



Dalam contoh berikut, log alur menangkap semua lalu lintas untuk subnet dan menerbitkan catatan log aliran ke Amazon Logs. CloudWatch Flow log menangkap lalu lintas untuk semua antarmuka jaringan di subnet.



Setelah Anda membuat log alur, dibutuhkan 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 Anda setelah Anda membuat log aliran untuk subnet atau VPC Anda, kami membuat aliran log (untuk CloudWatch Log) atau objek file log (untuk Amazon S3) untuk antarmuka jaringan baru segera setelah ada lalu lintas jaringan untuk antarmuka jaringan.

Anda dapat membuat log alur untuk antarmuka jaringan yang dibuat oleh layanan AWS lainnya, seperti:

- Penyeimbang Beban Elastis
- Amazon RDS
- Amazon ElastiCache

- Amazon Redshift
- Amazon WorkSpaces
- Gateway NAT
- Transit gateway

Terlepas dari jenis antarmuka jaringan, Anda harus menggunakan EC2 konsol Amazon atau Amazon EC2 API untuk membuat log aliran 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 aliran menonaktifkan layanan log aliran untuk sumber daya, sehingga tidak ada catatan log aliran baru yang dibuat atau diterbitkan. Menghapus log aliran tidak menghapus data log aliran yang ada. Setelah Anda menghapus log aliran, Anda dapat menghapus data log aliran langsung dari tujuan ketika Anda selesai dengan itu. 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 terpasang ke [instans berbasis Nitro](#), 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 Log atau Amazon S3. Layanan flow log 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 memungkinkan 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 memublikasikan data log alur ke Amazon S3, tipe data untuk bidang bergantung pada format log alur. Jika formatnya adalah teks biasa, semua bidang bertipeSTRING. Jika formatnya Parquet, lihat tabel untuk tipe 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. Tipe data parquet: 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, rekaman mungkin unknown ditampilkan untuk bidang ini. Jenis data parquet: STRING	2
interface-id	ID antarmuka jaringan yang lalu lintasnya dicatat. Jenis data parquet: STRING	2
srcaddr	Untuk lalu lintas masuk, ini adalah alamat IP dari sumber lalu lintas. Untuk lalu lintas keluar, ini adalah IPv4 alamat pribadi atau IPv6 alamat antarmuka jaringan yang mengirimkan lalu lintas. Lihat juga pkt-srcaddr. Jenis data parquet: STRING	2
dstaddr	Alamat tujuan untuk lalu lintas keluar, IPv4 atau IPv6 alamat antarmuka jaringan untuk lalu lintas masuk pada antarmuka	2

Bidang	Deskripsi	Versi
	jaringan. IPv4 Alamat antarmuka jaringan selalu IPv4 alamat pribadinya. Lihat juga pkt-dstaddr. Jenis data paket: STRING	
srcport	Port sumber lalu lintas. Tipe data paket: INT_32	2
dstport	Port tujuan lalu lintas. Tipe data paket: INT_32	2
protocol	Nomor protokol IANA lalu lintas. Untuk informasi selengkapnya, lihat Nomor Protokol Internet yang Ditugaskan. Tipe data paket: INT_32	2
packets	Jumlah paket yang ditransfer selama aliran. Tipe data paket: INT_64	2
bytes	Jumlah byte yang ditransfer selama aliran. Tipe data paket: INT_64	2
start	Waktu, dalam detik Unix, ketika paket pertama aliran diterima dalam interval agregasi. Ini mungkin sampai 60 detik setelah paket ditransmisikan atau diterima pada antarmuka jaringan. Tipe data paket: INT_64	2
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 paket: INT_64	2

Bidang	Deskripsi	Versi
action	Tindakan yang terkait dengan lalu lintas: • ACCEPTLalu lintas diterima. • REJECTLalu lintas ditolak. Misalnya, lalu lintas tidak diizinkan oleh kelompok keamanan atau jaringan ACLs, atau paket tiba setelah koneksi ditutup. Jenis 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 Ini mungkin disebabkan oleh kendala AWS kapasitas internal atau kesalahan internal. Jika Anda menggunakan AWS Cost Explorer untuk melihat muatan 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. Jenis data parket: STRING	2
vpc-id	ID VPC yang berisi antarmuka jaringan yang lalu lintasnya dicatat. Jenis data parket: STRING	3

Bidang	Deskripsi	Versi
subnet-id	ID subnet yang berisi antarmuka jaringan yang lalu lintasnya dicatat. Jenis data parquet: 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, antarmuka untuk NAT gateway. Jenis data parquet: 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 direkam, nilai flag TCP adalah 0. Misalnya, karena tcp-flags tidak mendukung pencatatan bendera ACK atau PSH, catatan untuk lalu lintas dengan flag yang tidak didukung ini akan menghasilkan nilai tcp-flags 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 bendera yang didukung dan ECE tidak, nilai bendera TCP adalah 2. Jika karena alasan tertentu kombinasi bendera tidak valid dan nilainya tidak dapat dihitung, nilainya adalah '-'. Jika tidak ada bendera yang dikirim, nilai bendera TCP adalah 0. Bendera TCP dapat OR-ed selama interval agregasi. Untuk koneksi pendek, bendera mungkin diatur pada baris yang sama dalam catatan log alur, misalnya, 19 untuk SYN-ACK dan FIN, dan 3 untuk SYN dan FIN. Sebagai contoh, lihat Urutan bendera TCP. Untuk informasi umum tentang bendera TCP (seperti arti bendera seperti FIN, SYN, dan ACK), lihat Struktur segmen TCP di Wikipedia. Tipe data paket: INT_32	3
type	Jenis lalu lintas. Nilai yang mungkin adalah: IPv4 IPv6 EFA. Untuk informasi selengkapnya, lihat Adaptor Elastic Fabric. Jenis data paket: 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 aliran lalu lintas, dan alamat IP sumber asal dari lalu lintas. Misalnya, saat lalu lintas mengalir melalui antarmuka jaringan NAT gateway, atau di mana alamat IP dari pod di Amazon EKS berbeda dari alamat IP dari antarmuka jaringan dari simpul instans di mana pod berjalan (untuk komunikasi dalam VPC). Jenis data parquet: 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 aliran lalu lintas, dan alamat IP tujuan akhir dari lalu lintas. Misalnya, saat lalu lintas mengalir antarmuka jaringan untuk NAT gateway, atau di mana alamat IP dari pod di Amazon EKS berbeda dari alamat IP dari antarmuka jaringan dari simpul instans di mana pod berjalan (untuk komunikasi dalam VPC). Jenis data parquet: STRING	3
region	Wilayah yang berisi antarmuka jaringan yang lalu lintasnya dicatat. Jenis data parquet: 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 parquet: 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 parquet: 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 parquet: STRING	4
pkt-src-aws-service	Nama subset dari Rentang alamat IP untuk bidang pkt-srcaddr, jika alamat IP sumber adalah untuk layanan AWS. Jika alamat IP sumber termasuk dalam rentang yang 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_REALTIME KINESIS_VIDEO_STREAMS MEDIA_PACKAGE_V2 ROUTE53 ROUTE53_HEALTHCHECKS ROUTE53_HEALTHCHECKS_PUBLISHING ROUTE53_RESOLVER S3 WORKSPACES_GATEWAYS Jenis data parquet: STRING	5
pkt-dst-aws-service	Nama subset alamat IP berkisar untuk pkt-dstaddr bidang, jika alamat IP tujuan adalah untuk AWS layanan. Untuk daftar kemungkinan nilai, lihat bidang pkt-src-aws-service. Jenis data parquet: STRING	5

Bidang	Deskripsi	Versi
flow-direction	Arah aliran sehubungan dengan antarmuka di mana lalu lintas ditangkap. Kemungkinan nilai adalah: ingress egress. Jenis data paret: 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 sumber daya yang membuat antarmuka jaringan di VPC • 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 gateway lokal • 7 — Melalui VPC endpoint gateway (instans berbasis Nitro saja) • 8 — Melalui gateway internet (instans berbasis Nitro saja) Tipe data paret: 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 menyertakan bidang ini dalam langganan Anda, Anda memerlukan izin untuk menelepon ecs:ListClusters. Jenis data paret: STRING	7
ecs-cluster-name	Nama cluster ECS jika lalu lintas berasal dari tugas ECS yang sedang berjalan. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerlukan izin untuk menelepon ecs:ListClusters. Jenis data paret: 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 sebuah instance. EC2 Jika penyedia kapasitas adalah AWS Fargate, bidang ini akan menjadi '-'. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerlukan izin untuk menelepon ecs: ListClusters dan ecs: ListContainerInstances Jenis data parquet: STRING	7
ecs-container-instance-id	ID instance kontainer ECS jika lalu lintas berasal dari tugas ECS yang sedang berjalan pada sebuah EC2 instance. Jika penyedia kapasitas adalah AWS Fargate, bidang ini akan menjadi '-'. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerlukan izin untuk menelepon ecs: ListClusters dan ecs: ListContainerInstances Jenis data parquet: STRING	7
ecs-container-id	ID runtime Docker kontainer jika lalu lintas berasal dari tugas ECS yang sedang berjalan. Jika ada satu atau lebih kontainer dalam tugas ECS, ini akan menjadi ID runtime docker dari kontainer pertama. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerlukan izin untuk menelepon ecs:ListClusters. Jenis data parquet: STRING	7
ecs-second-container-id	ID runtime Docker kontainer jika lalu lintas berasal dari tugas ECS yang sedang berjalan. Jika ada lebih dari satu kontainer dalam tugas ECS, ini akan menjadi ID runtime Docker dari kontainer kedua. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerlukan izin untuk menelepon ecs:ListClusters. Jenis data parquet: STRING	7

Bidang	Deskripsi	Versi
ecs-service-name	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 menelepon ecs: ListClusters dan ecs: ListServices Jenis data parquet: 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 Jenis data parquet: STRING	7
ecs-task-arn	ARN dari tugas ECS jika lalu lintas berasal dari tugas ECS yang sedang berjalan. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerlukan izin untuk menelepon ecs: ListClusters dan ecs: ListTasks Jenis data parquet: STRING	7
ecs-task-id	ID tugas ECS jika lalu lintas berasal dari tugas ECS yang sedang berjalan. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerlukan izin untuk menelepon ecs: ListClusters dan ecs: ListTasks Jenis data parquet: STRING	7
tolak-alasan	Alasan Mengapa Lalu Lintas Ditolak Nilai yang mungkin: BPA. Mengembalikan '-' untuk alasan penolakan lainnya. Untuk informasi selengkapnya tentang VPC Block Public Access (BPA), lihat. Memblokir akses publik ke VPCs dan subnet Jenis data parquet: STRING	8

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](#)
- [IPv6 lalu lintas](#)
- [Urutan bendera TCP](#)
- [Lalu lintas melalui gateway NAT](#)
- [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
```

VPC Flow Logs melewati catatan ketika 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](#) Ini mungkin disebabkan oleh kendala AWS kapasitas internal atau kesalahan internal. Jika Anda menggunakan AWS Cost Explorer untuk melihat muatan 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, jaringan tidak ACLs memiliki kewarganegaraan, oleh karena itu tanggapan 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 jaringan ACLs tanpa kewarganegaraan, ping respons dijatuhkan dan tidak mencapai komputer di 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.

IPv6 lalu lintas

Berikut ini adalah contoh catatan log alur default. Dalam contoh, lalu lintas SSH (port 22) dari IPv6 alamat 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 aliran 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
```

tcp-flagsBidang dalam contoh di bagian ini diwakili oleh second-to-last nilai 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 bendera TCP, lihat. [Bidang 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 dikirim dari server untuk 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. Klien mengirim bendera FIN (1) ke server untuk koneksi pada port 43418. Server mengirim FIN ke klien 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
```

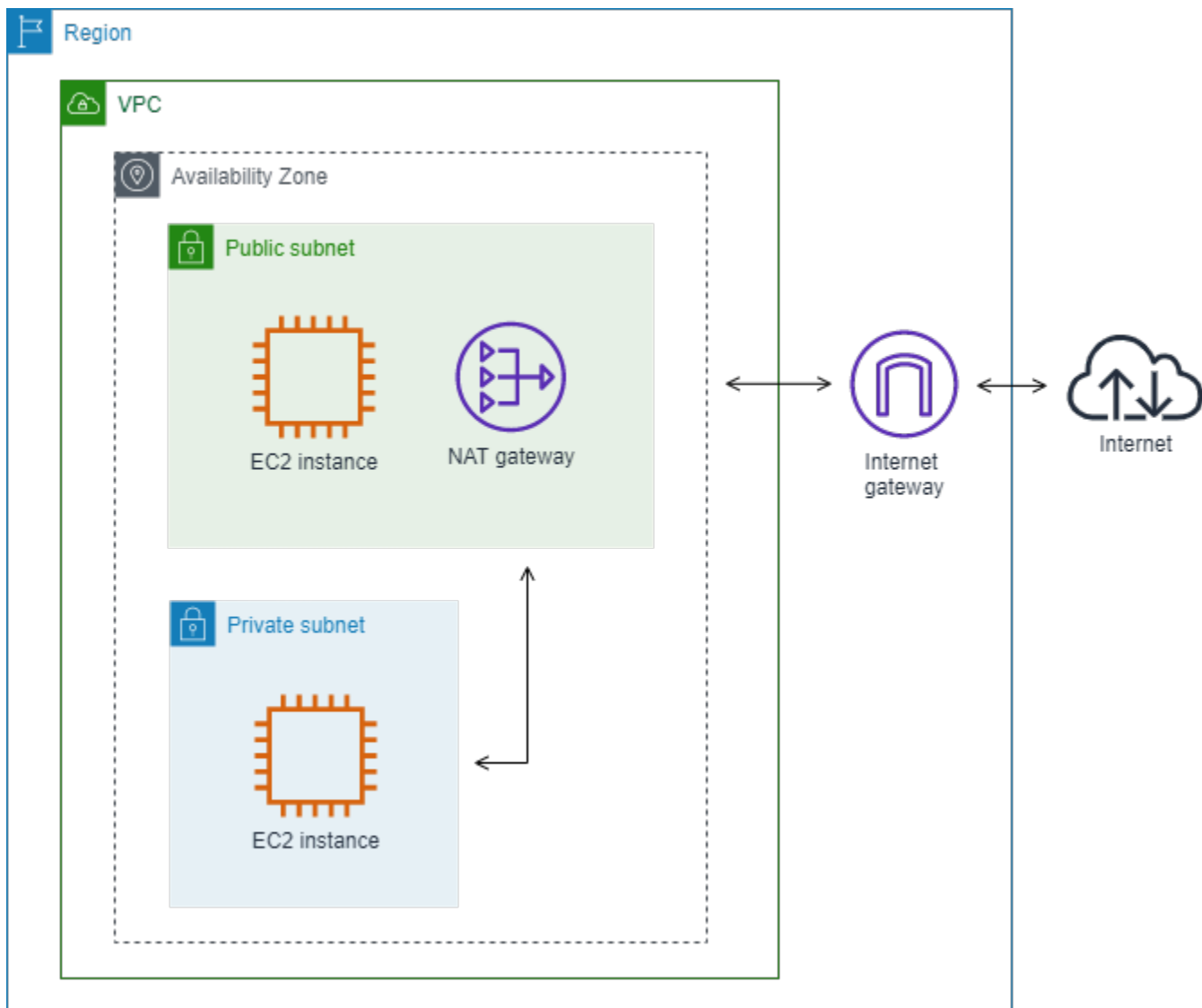
Untuk koneksi singkat (misalnya, beberapa detik) yang dibuka dan ditutup dalam interval agregasi tunggal, bendera mungkin ditetapkan pada baris yang sama dalam catatan log alur untuk lalu lintas dalam arah yang sama. Pada contoh berikut, koneksi dibuat dan selesai dalam interval agregasi yang sama. Pada 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 bendera TCP adalah 19, yang menunjukkan bahwa ada pesan SYN-ACK dan FIN yang 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

Dalam contoh ini, sebuah instans di subnet privat mengakses internet melalui gateway NAT yang ada di subnet publik.



Log alur kustom berikut untuk antarmuka jaringan gateway NAT menangkap bidang-bidang berikut dalam urutan berikut.

```
instance-id interface-id srcaddr dstaddr pkt-srcaddr pkt-dstaddr
```

Log alur menunjukkan aliran lalu lintas dari alamat IP instans (10.0.1.5) melalui antarmuka jaringan gateway NAT ke host di internet (203.0.113.5). Antarmuka jaringan NAT gateway adalah antarmuka jaringan yang dikelola peminta, oleh karena itu catatan log alur menampilkan simbol '-' untuk bidang instance-id. Baris berikut menunjukkan lalu lintas dari instans sumber ke antarmuka jaringan gateway NAT. Nilai-nilai untuk bidang dstaddr dan pkt-dstaddr berbeda. Bidang dstaddr menampilkan alamat IP privat antarmuka jaringan gateway NAT, dan bidang pkt-dstaddr 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 ke host target di internet, dan lalu lintas respon 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 respon dari antarmuka jaringan NAT gateway ke instans sumber. Nilai-nilai untuk bidang srcaddr dan pkt-srcaddr berbeda. Bidang srcaddr menampilkan alamat IP privat antarmuka jaringan gateway NAT, dan bidang pkt-srcaddr menampilkan alamat IP host di internet.

```
- eni-1235b8ca123456789 10.0.0.220 10.0.1.5 203.0.113.5 10.0.1.5
```

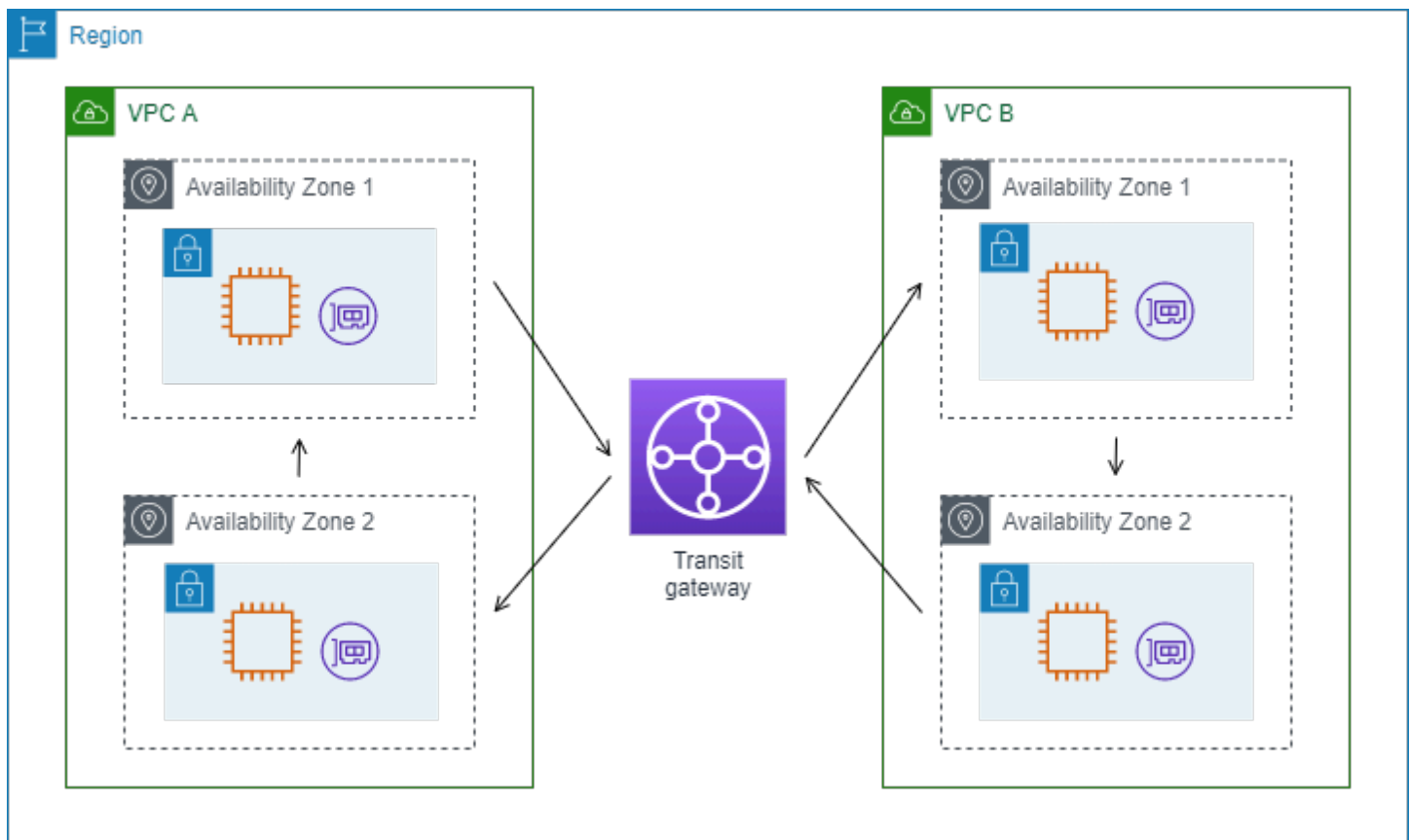
Anda membuat log alur kustom lain menggunakan set bidang di atas. Anda membuat log alur untuk antarmuka jaringan untuk instans di subnet privat. Dalam hal ini, bidang instance-id mengembalikan ID instans yang terkait dengan antarmuka jaringan, dan tidak ada perbedaan antara bidang dstaddr dan bidang pkt-dstaddr dan bidang srcaddr dan bidang pkt-srcaddr. Tidak seperti antarmuka jaringan untuk gateway NAT, 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 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 elastic network interface ID (dalam contoh ini, katakanlah IDnya adalah eni-11111111111111111111) dan meninggalkan VPC B menggunakan yang lain (misalnya eni-2222222222222222222).



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-3333333333333333 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbbb
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-3333333333333333 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbbb
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-1111111111111111, antarmuka jaringan yang dikelola peminta untuk transit gateway di subnet subnet-11111111aaaaaaaa. 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-1111111111111111 123456789010 vpc-abcdefab012345678 subnet-11111111aaaaaaaa -
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-2222222222222222, antarmuka jaringan yang dikelola peminta untuk transit gateway di subnet subnet-22222222bbbbbbbbbb. Bidang dstaddr menampilkan alamat IP privat antarmuka jaringan transit gateway, dan bidang pkt-dstaddr menampilkan alamat IP klien di VPC A.

```
3 eni-2222222222222222 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbbb -
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. Sebuah EC2 instance 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 Anda membuat log aliran, 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 VPCs yang diintegrasikan dengan VPC Anda kecuali VPC rekan ada di akun Anda.
- Setelah membuat log aliran, Anda tidak dapat mengubah konfigurasinya atau format catatan log aliran. 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 IPv4 alamat dan lalu lintas dikirim ke IPv4 alamat pribadi sekunder, log alur menampilkan IPv4 alamat pribadi utama di `dstaddr` bidang. 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 aliran menampilkan IPv4 alamat pribadi utama di `dstaddr` lapangan. 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, ketika catatan log adalah untuk aliran keluar, log aliran menampilkan IPv4 alamat pribadi utama di `srcaddr` lapangan. 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.
- Saat antarmuka jaringan Anda terpasang ke [Instans berbasis Nitro](#), interval agregasi selalu 1 menit atau kurang, terlepas dari interval agregasi maksimum yang ditentukan.

- Untuk `pkt-srcaddr` dan `pkt-dstaddr` bidang, jika lapisan perantara mengaktifkan Pelestarian alamat IP Klien, bidang ini dapat menampilkan IP Klien yang diawetkan, bukan alamat IP dari lapisan perantara.
- Beberapa catatan log aliran dapat dilewati selama interval agregasi (lihat log-status di). [Bidang yang tersedia](#) Ini mungkin disebabkan oleh kendala AWS kapasitas internal atau kesalahan internal. Jika Anda menggunakan AWS Cost Explorer untuk melihat muatan 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 termasuk catatan yang dilewati.](#)
 - Log aliran untuk VPC BPA tidak termasuk [bytes](#) bahkan jika Anda menyertakan bytes bidang dalam log aliran Anda.

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 akan melihat lalu lintas target cermin lalu lintas saja.
- 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 Address Resolution Protocol (ARP)

Batasan khusus untuk bidang ECS yang tersedia di versi 7:

- Untuk membuat langganan log alur dengan bidang ECS, akun Anda harus berisi setidaknya satu cluster ECS.
- Bidang ECS tidak dihitung jika tugas ECS yang mendasarinya tidak dimiliki oleh pemilik langganan log aliran. Misalnya, jika Anda berbagi subnet (SubnetA) dengan akun lain (AccountB), dan

kemudian Anda membuat langganan log aliran untuk SubnetA, jika AccountB meluncurkan tugas ECS di subnet bersama, langganan Anda akan menerima log lalu lintas dari tugas ECS yang diluncurkan oleh AccountB tetapi bidang ECS untuk log ini tidak akan 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 akan menjadi '-' untuk lalu lintas IP non-ECS. Misalnya, Anda memiliki subnet (subnet-000000) dan Anda membuat langganan log aliran untuk subnet ini dengan bidang ECS (). f1-00000000 Disubnet-000000, Anda meluncurkan EC2 instance (i-00000000) 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-00000000 dan menghasilkan lalu lintas IP, langganan log aliran Anda f1-00000000 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-00000000 terkait, bidang ini akan memiliki nilai '-'.
- ecs-container-id dan ecs-second-container-id dipesan saat layanan VPC Flow Logs menerimanya dari aliran peristiwa 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 STOPPED saat tugas masih berjalan, kontainer dapat 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 1) ketika kami menerima lalu lintas IP untuk antarmuka jaringan yang mendasarinya dan 2) ketika 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 1) ketika 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 2) ketika kami menerima acara ECS yang berisi metadata untuk tugas ECS Anda untuk menunjukkan tugas Anda tidak lagi berjalan.
- Hanya tugas ECS yang diluncurkan dalam [mode aws vpc jaringan](#) yang didukung.

Harga

Biaya konsumsi data dan arsip untuk log vended berlaku saat Anda mempublikasikan log aliran. Untuk informasi selengkapnya tentang harga saat menerbitkan log penjual, buka [CloudWatch Harga Amazon](#), pilih Log, dan temukan Log Terjual.

Untuk melacak biaya dari log alur penerbitan, Anda dapat menerapkan tag alokasi biaya ke sumber daya tujuan Anda. Setelah itu, laporan alokasi AWS biaya Anda mencakup penggunaan dan biaya yang dikumpulkan 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
- [Tandai grup log di CloudWatch Log Amazon](#) di Panduan Pengguna CloudWatch Log Amazon
- [Menggunakan tag bucket S3 alokasi biaya](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon
- [Menandai Aliran Pengiriman Anda](#) di Panduan Pengembang Amazon Data Firehose

Bekerja dengan log alur

Anda dapat bekerja dengan flow log menggunakan konsol untuk Amazon EC2 dan Amazon VPC.

Tugas

- [1. Kontrol penggunaan flow log dengan IAM](#)
- [2. Membuat log alur](#)
- [3. Tandai log aliran](#)
- [4. Menghapus log alur](#)
- [Ikhtisar baris perintah](#)

1. Kontrol penggunaan flow log 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, mendeskripsikan, dan menghapus log aliran.

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 aliran untuk VPCs, subnet, atau antarmuka jaringan Anda. Saat Anda membuat log aliran, Anda harus menentukan tujuan untuk log aliran. Untuk informasi selengkapnya, lihat berikut ini:

- [the section called “Buat log alur yang diterbitkan ke CloudWatch Log”](#)
- [the section called “Membuat log alur yang menerbitkan ke Amazon S3”](#)
- [the section called “Membuat log alur yang memublikasikan ke Amazon Data Firehose”](#)

3. Tandai log aliran

Anda dapat menambahkan atau menghapus tag untuk log aliran kapan saja.

Untuk mengelola tag untuk log alur

1. Lakukan salah satu tindakan berikut:

- Buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>. Di panel navigasi, pilih Antarmuka Jaringan. Pilih kotak centang untuk antarmuka jaringan.
- Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>. Di panel navigasi, pilih Your VPCs. Pilih kotak centang untuk VPC.
- Buka konsol VPC Amazon 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 Simpan.

4. Menghapus log alur

Anda dapat menghapus log aliran kapan saja. Setelah Anda menghapus log aliran, diperlukan beberapa menit untuk berhenti mengumpulkan data.

Menghapus log aliran tidak menghapus data log dari tujuan atau mengubah sumber daya tujuan. Anda harus menghapus data log aliran yang ada langsung dari tujuan, dan membersihkan sumber daya tujuan, menggunakan konsol untuk layanan tujuan.

Untuk menghapus log aliran

1. Lakukan salah satu tindakan berikut:

- Buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>. Di panel navigasi, pilih Antarmuka Jaringan. Pilih kotak centang untuk antarmuka jaringan.
- Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>. Di panel navigasi, pilih Your VPCs. Pilih kotak centang untuk VPC.
- Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>. Di panel navigasi, pilih Pengguna. Pilih kotak centang untuk subnet.

2. Pilih Log Aliran.

3. Pilih Tindakan, Hapus log aliran.

4. Saat diminta konfirmasi, ketik **delete** lalu pilih Hapus.

Ikhtisar baris perintah

Anda dapat melakukan tugas yang dijelaskan di 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)

Tandai log aliran

- [buat-tag dan hapus-tag](#) ()AWS CLI
- [New-EC2Tag](#) dan [Remove-EC2Tag](#) AWS Tools for Windows PowerShell

Menghapus log alur

- [delete-flow-logs](#) (AWS CLI)
- [Remove-EC2FlowLog](#) (AWS Tools for Windows PowerShell)

Publikasikan log aliran ke CloudWatch Log

Log aliran dapat mempublikasikan data log aliran langsung ke Amazon CloudWatch. Amazon CloudWatch adalah layanan pemantauan dan observabilitas 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 potensi masalah. Dengan CloudWatch, Anda dapat mengatur alarm, memvisualisasikan log dan metrik, dan bereaksi secara otomatis

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 memublikasikan 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 aliran. Bidang ingestionTime menunjukkan tanggal dan waktu ketika catatan log aliran diterima oleh Log. CloudWatch Stempel waktu ini lebih lambat dari waktu akhir yang ditangkap dalam catatan log alur.

Untuk informasi selengkapnya tentang CloudWatch Log, lihat [Log yang dikirim ke CloudWatch Log](#) di Panduan Pengguna CloudWatch Log Amazon.

Harga

Biaya konsumsi data dan arsip untuk log vendes berlaku saat Anda memublikasikan log aliran ke Log. CloudWatch Untuk informasi selengkapnya, buka [CloudWatch Harga Amazon](#), pilih Log dan temukan Log Terjual.

Daftar Isi

- [Peran IAM untuk menerbitkan log alur ke CloudWatch Log](#)
- [Buat log alur yang diterbitkan 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 CloudWatch Log

Peran IAM yang terkait dengan log alur Anda harus memiliki izin yang cukup untuk memublikasikan log aliran ke grup log yang ditentukan di CloudWatch Log. Peran IAM harus menjadi 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 flow logs 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 sumber ARN adalah ARN log aliran. 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"
  }
}
```

Buat peran IAM untuk log aliran

Anda dapat memperbarui peran yang ada seperti yang 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. Pilih JSON.
 - b. Ganti isi jendela ini dengan kebijakan izin di awal bagian ini.
 - c. Pilih Berikutnya.
 - d. Masukkan nama untuk kebijakan Anda serta deskripsi dan tag opsional, lalu pilih Buat kebijakan.
5. Di panel navigasi, pilih Peran.
6. Pilih Buat peran.
7. Untuk jenis entitas Tepercaya, pilih Kebijakan kepercayaan khusus. Untuk kebijakan kepercayaan kustom, ganti "Principal": {}, dengan yang berikut ini, lalu pilih Berikutnya.

```
"Principal": {
```

```
"Service": "vpc-flow-logs.amazonaws.com"
},
```

8. Pada halaman Tambahkan izin, pilih kotak centang untuk kebijakan yang Anda buat sebelumnya dalam prosedur ini, lalu pilih Berikutnya.
9. Masukkan nama untuk peran Anda dan berikan deskripsi secara opsional.
10. Pilih Buat peran.

Buat log alur yang diterbitkan ke CloudWatch Log

Anda dapat membuat log aliran untuk VPCs, subnet, atau antarmuka jaringan Anda. Jika Anda melakukan langkah-langkah ini sebagai pengguna menggunakan peran IAM tertentu, pastikan peran tersebut memiliki izin untuk menggunakan tindakan tersebut: `iam:PassRole`.

Prasyarat

Verifikasi bahwa prinsipal IAM yang Anda gunakan untuk membuat permintaan memiliki izin untuk memanggil tindakan. `iam:PassRole`

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["iam:PassRole"],
      "Resource": "arn:aws:iam::account-id:role/flow-log-role-name"
    }
  ]
}
```

Untuk membuat log aliran menggunakan konsol

1. Lakukan salah satu tindakan berikut:
 - Buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>. Di panel navigasi, pilih Antarmuka Jaringan. Pilih kotak centang untuk antarmuka jaringan.

- Buka konsol VPC Amazon di. <https://console.aws.amazon.com/vpc/> Di panel navigasi, pilih Your VPCs. Pilih kotak centang untuk VPC.
 - Buka konsol VPC Amazon di. <https://console.aws.amazon.com/vpc/> Di panel navigasi, pilih Pengguna. Pilih kotak centang untuk subnet.
2. Pilih Tindakan, 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 memublikasikan CloudWatch log ke Log atau memilih 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 aliran yang menangkap semua lalu lintas yang diterima untuk subnet yang ditentukan. Log aliran dikirim ke grup log yang ditentukan. `--deliver-logs-`

`permission-arn` Parameter menentukan peran IAM yang diperlukan untuk mempublikasikan 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 Log. Setelah Anda membuat log alur, mungkin perlu beberapa menit agar dapat 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 aliran Anda untuk membuka halaman detailnya.
4. Pilih nama aliran log yang berisi catatan log aliran. 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)
- [Dapatkan- CWLLog Acara](#) (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 Log

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 aliran 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 Pengguna CloudWatch Log Amazon.

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 yang akan diuji, pilih aliran log untuk antarmuka jaringan Anda. (Opsional)
Untuk melihat baris data log yang cocok dengan pola filter, pilih Pola uji.
6. Saat Anda siap, pilih Berikutnya.
7. Masukkan nama filter, namespace metrik, dan nama metrik. Tetapkan nilai metrik ke 1. Setelah selesai, pilih Berikutnya dan kemudian 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. Konfigurasi 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 Periode, pilih 1 jam.
 - Untuk Kapan TimeSinceLastActive pun... , pilih Greater/Equal dan masukkan 10 untuk ambang batas.
 - Untuk konfigurasi Tambahan, Datapoint ke alarm, biarkan default 1.
12. Pilih Berikutnya.
13. Untuk Pemberitahuan, 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 Berikutnya.
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 (Layanan Penyimpanan Sederhana) 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 flow log, lihat [Membuat bucket di Panduan Pengguna Amazon S3](#).

Untuk informasi selengkapnya tentang cara merampingkan konsumsi log aliran VPC, pemrosesan log aliran, dan visualisasi log aliran, [lihat Pencatatan Terpusat](#) dengan di Perpustakaan Solusi. OpenSearch AWS

Untuk informasi selengkapnya tentang CloudWatch Log, lihat [Log yang dikirim ke Amazon S3](#) di Panduan Pengguna Amazon CloudWatch Logs.

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 Terjual.

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.
- Parquet - 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 berkas log

Anda dapat secara opsional menentukan opsi berikut.

- Awalan S3 yang kompatibel dengan HIVE - Aktifkan awalan yang kompatibel dengan HIVE alih-alih mengimpor partisi ke alat yang kompatibel dengan HIVE Anda. Sebelum Anda menjalankan kueri, 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 ember S3 file log

File log disimpan ke bucket Amazon S3 yang ditentukan menggunakan struktur folder yang didasarkan pada opsi ID, Wilayah, tanggal pembuatan, dan tujuan log alur.

Secara default, file dikirim ke lokasi berikut.

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/
```

Jika Anda mengaktifkan awalan S3 yang kompatibel dengan HIVE, file akan 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 partisi yang kompatibel dengan HIVE dan mempartisi log aliran 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 berkas log

Nama file log didasarkan pada ID log aliran, 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 serta `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.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryWrite",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "my-s3-arn/*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": account_id,
          "s3:x-amz-acl": "bucket-owner-full-control"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:logs:region:account_id:*"
        }
      }
    },
    {
      "Sid": "AWSLogDeliveryAclCheck",
      "Effect": "Allow",
      "Principal": {
```

```

        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": "s3:GetBucketAcl",
    "Resource": "arn:aws:s3:::bucket_name",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": account_id
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:logs:region:account_id:*"
        }
    }
}
]
}

```

ARN yang Anda tentukan *my-s3-arn* bergantung pada apakah Anda menggunakan awalan S3 yang kompatibel dengan HIVE.

- Awalan default

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/account_id/*
```

- Awalan S3 yang kompatibel dengan HIVE

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/aws-account-id=account_id/*
```

Merupakan praktik terbaik untuk memberikan izin ini kepada prinsipal layanan pengiriman log alih-alih individu Akun AWS ARNs. 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 aliran dan sumber ARN adalah ARN wildcard (*) 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; itu akan tetap mengirimkan log aliran VPC meskipun tidak dapat mengonfirmasi bahwa bucket S3 ada dan lokasinya. Namun, akan ada AccessDenied kesalahan untuk panggilan ke HeadBucket dalam CloudTrail log Anda.

Kebijakan kunci yang diperlukan untuk digunakan dengan SSE-KMS

Anda dapat melindungi data di bucket Amazon S3 dengan mengaktifkan Enkripsi Sisi Server dengan Amazon S3-Managed Keys (SSE-S3) atau Enkripsi Sisi Server dengan Kunci KMS (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 ARN kunci yang dikelola pelanggan. Jika Anda menggunakan ID kunci, Anda dapat mengalami [LogDestination tidak terkirim](#) kesalahan saat membuat log aliran. Selain itu, Anda harus memperbarui kebijakan kunci untuk kunci terkelola pelanggan Anda sehingga akun pengiriman log dapat menulis ke bucket S3 Anda. Untuk informasi selengkapnya tentang kebijakan kunci yang diperlukan untuk digunakan dengan SSE-KMS, lihat [enkripsi sisi server bucket Amazon S3 di Panduan Pengguna Log](#) Amazon CloudWatch.

Izin file berkas log Amazon S3

Selain kebijakan bucket yang diperlukan, Amazon S3 menggunakan daftar kontrol akses (ACLs) untuk mengelola akses ke file 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 aliran untuk antarmuka jaringan, subnet, dan file. VPCs

Prasyarat

Prinsipal IAM yang membuat log alur harus menggunakan peran IAM yang memiliki izin berikut, yang diperlukan untuk mempublikasikan log alur ke bucket Amazon S3 tujuan.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
{
  "Effect": "Allow",
  "Action": [
    "logs:CreateLogDelivery",
    "logs>DeleteLogDelivery"
  ],
  "Resource": "*"
}
```

Untuk membuat log aliran menggunakan konsol

1. Lakukan salah satu tindakan berikut:

- Buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>. Di panel navigasi, pilih Antarmuka Jaringan. Pilih kotak centang untuk antarmuka jaringan.
- Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>. Di panel navigasi, pilih Your VPCs. Pilih kotak centang untuk VPC.
- Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>. Di panel navigasi, pilih Pengguna. Pilih kotak centang untuk subnet.

2. Pilih Tindakan, Buat log alur.

3. Untuk Filter, tentukan jenis data lalu lintas IP ke log.

- Terima - Log hanya lalu lintas yang diterima.
- Tolak — Log hanya lalu lintas yang ditolak.
- Semua — Log diterima dan ditolak lalu lintas.

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 aliran.
 - 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.
 - Parquet - 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 awalan S3 yang kompatibel dengan HIVE, pilih awalan S3 yang kompatibel dengan HIVE, Aktifkan.
11. (Opsional) Untuk mempartisi log aliran Anda per jam, pilih Setiap 1 jam (60 menit).
12. (Opsional) Untuk menambahkan tag ke log aliran, pilih Tambahkan tag baru dan tentukan kunci dan nilai tag.
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 aliran 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 dapat 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//AWSLogsaccount_id/vpcflowlogs////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 terkelola penuh yang mengumpulkan, mengubah, dan mengirimkan aliran data real-time ke berbagai AWS penyimpanan data dan layanan analitik. Ini menangani konsumsi 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 dapat menjadi

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 intensif sumber daya.

Dengan mengintegrasikan Firehose dengan log aliran VPC, Anda dapat mengirimkan data ini ke tujuan pilihan Anda, seperti Amazon S3, Amazon Redshift, atau Amazon OpenSearch Service. Firehose akan menskalakan untuk menangani konsumsi, transformasi, dan pengiriman log aliran VPC Anda, sehingga 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-fitur seperti transformasi data, kompresi, dan enkripsi, yang dapat meningkatkan efisiensi dan keamanan pipeline 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 memublikasikan 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 Terjual.

Daftar Isi

- [Peran IAM untuk pengiriman lintas akun](#)
- [Membuat log alur yang memublikasikan ke Amazon Data Firehose](#)

Peran IAM untuk pengiriman lintas akun

Saat memublikasikan ke Amazon Data Firehose, Anda dapat memilih aliran pengiriman yang berada di akun yang sama dengan sumber daya yang akan dipantau (akun sumber), atau di akun lain (akun tujuan). Untuk mengaktifkan pengiriman lintas akun log alur 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 perannya 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 diteruskan hanya ke layanan pengiriman log, dan hanya saat memantau sumber daya yang ditentukan. Saat Anda membuat kebijakan, tentukan VPCs, 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::source-account:role/mySourceRole",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "delivery.logs.amazonaws.com"
        },
        "StringLike": {
          "iam:AssociatedResourceARN": [
            "arn:aws:ec2:region:source-account:vpc/vpc-00112233344556677"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs>ListLogDeliveries",
        "logs:GetLogDelivery"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
```

```
"Resource": "arn:aws:iam::destination-account:role/  
AWSLogDeliveryFirehoseCrossAccountRole"  
}  
]  
}
```

Pastikan bahwa 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. Pilih JSON.
 - b. Ganti isi jendela ini dengan kebijakan izin di awal bagian ini.
 - c. Pilih Berikutnya.

- d. Masukkan nama untuk kebijakan Anda serta deskripsi dan tag opsional, lalu pilih Buat kebijakan.
5. Di panel navigasi, pilih Peran.
6. Pilih Buat peran.
7. Untuk jenis entitas Tepercaya, pilih Kebijakan kepercayaan khusus. Untuk kebijakan kepercayaan kustom, ganti "Principal": {}, dengan yang berikut ini, yang menentukan layanan pengiriman log. Pilih Berikutnya.

```
"Principal": {  
  "Service": "delivery.logs.amazonaws.com"  
},
```

8. Pada halaman Tambahkan izin, pilih kotak centang untuk kebijakan yang Anda buat sebelumnya dalam prosedur ini, lalu pilih Berikutnya.
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::source-account: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. Pilih JSON.
 - 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 jenis entitas Tepercaya, pilih Kebijakan kepercayaan khusus. Untuk kebijakan kepercayaan khusus, ganti `"Principal": {}`, dengan yang berikut, yang menentukan peran akun sumber. Pilih Berikutnya.

```
"Principal": {  
  "AWS": "arn:aws:iam::source-account:role/mySourceRole"  
},
```

8. Pada halaman Tambahkan izin, pilih kotak centang untuk kebijakan yang Anda buat sebelumnya dalam prosedur ini, lalu pilih Berikutnya.
9. Masukkan nama untuk peran Anda dan berikan deskripsi secara opsional.
10. Pilih Buat peran.

Membuat log alur yang memublikasikan ke Amazon Data Firehose

Anda dapat membuat log aliran untuk VPCs, subnet, atau antarmuka jaringan Anda.

Prasyarat

- Buat aliran pengiriman Amazon Data Firehose tujuan. Gunakan Direct Put sebagai sumbernya. Untuk informasi selengkapnya, lihat [Membuat aliran pengiriman Amazon Data Firehose](#).
- Jika Anda memublikasikan log alur ke akun lain, buat peran IAM yang diperlukan, seperti yang dijelaskan dalam [the 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 EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>. Di panel navigasi, pilih Antarmuka Jaringan. Pilih kotak centang untuk antarmuka jaringan.
 - Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>. Di panel navigasi, pilih Your VPCs. Pilih kotak centang untuk VPC.
 - Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>. Di panel navigasi, pilih Pengguna. Pilih kotak centang untuk subnet.
2. Pilih Tindakan, Buat log alur.
3. Untuk Filter, tentukan jenis lalu lintas ke log.
 - Terima - Log hanya lalu lintas yang diterima
 - Tolak - Log hanya lalu lintas yang ditolak
 - Semua — Log diterima dan ditolak lalu lintas

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 untuk dipantau berada di akun yang sama.
 - Kirim ke Amazon Data Firehose di akun yang berbeda — Aliran pengiriman dan sumber daya untuk dipantau berada 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 Siapkan izin untuk membuka konsol IAM dan membuat peran layanan.
8. Untuk format catatan Log, tentukan format untuk catatan log aliran.
 - 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 Tambahkan tag untuk menerapkan tag ke log aliran.
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 aliran 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 yang ditentukan dan mengirimkan log aliran 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 membuat log aliran, Anda bisa mendapatkan data log aliran dari tujuan yang Anda konfigurasikan 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 cloud pribadi virtual Anda (VPCs) yang merupakan pembicara teratas atau mengidentifikasi alamat IP dengan koneksi TCP yang paling banyak ditolak.

Opsi

- Anda dapat merampingkan dan mengotomatiskan integrasi log aliran VPC Anda dengan Athena dengan membuat CloudFormation template yang membuat AWS sumber daya yang diperlukan dan kueri yang telah ditentukan sebelumnya yang dapat Anda jalankan 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](#)
- [Menghasilkan CloudFormation template menggunakan AWS CLI](#)
- [Menjalankan kueri yang sudah ditentukan sebelumnya](#)

Hasilkan CloudFormation template menggunakan konsol

Setelah log aliran pertama dikirim ke bucket S3 Anda, Anda dapat berintegrasi dengan Athena dengan CloudFormation membuat 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 tertentu yang telah ditentukan sebelumnya yang ingin Anda jalankan.

Untuk menghasilkan templat menggunakan konsol

1. Lakukan salah satu tindakan berikut:
 - Buka konsol Amazon VPC. Di panel navigasi, pilih Your VPCs dan kemudian pilih VPC Anda.
 - Buka konsol Amazon VPC. Di panel navigasi, pilih Subnet, lalu pilih subnet Anda.
 - Buka EC2 konsol Amazon. 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 berakhir, CloudFormation template akan 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 template.
7. Dalam pesan sukses, pilih Buat CloudFormation tumpukan untuk membuka wizard Create Stack di AWS 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 database adalah `flow-logs-subscription-idvpcflowlogsathenadatabase< >`.
- Athena workgroup. Nama workgroup adalah `< flow-log-subscription-id>< >< start-date >< partition-load-frequencyend-date >workgroup`
- Sebuah tabel Athena dipartisi yang sesuai dengan catatan log alur Anda. Nama tabel adalah `< flow-log-subscription-id>< >< start-date partition-load-frequency>< 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.

Menghasilkan CloudFormation template menggunakan AWS CLI

Setelah log aliran pertama dikirim ke bucket S3 Anda, Anda dapat membuat dan menggunakan CloudFormation template untuk berintegrasi dengan Athena.

Gunakan perintah [get-flow-logs-integration-template](#) berikut untuk menghasilkan CloudFormation template.

```
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 bermakna tentang lalu lintas di jaringan Anda dengan cepat. AWS 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 standar 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 pertanyaan bernama Athena. Kueri yang telah ditentukan sebelumnya yang disediakan saat Anda membuat templat bergantung pada bidang yang merupakan bagian dari format catatan log untuk log aliran. Oleh karena itu, template mungkin tidak berisi semua kueri yang telah ditentukan ini.

- `VpcFlowLogsAcceptedTrafficKoneksi TCP` yang diizinkan berdasarkan grup keamanan dan jaringan ACLs Anda.
- `VpcFlowLogsAdminPortTraffic10` alamat IP teratas dengan lalu lintas terbanyak, seperti yang dicatat oleh aplikasi yang melayani permintaan pada port administratif.
- `VpcFlowLogsIPv4Lalu Lintas` — Total byte IPv4 lalu lintas yang direkam.
- `VpcFlowLogsIPv6Lalu Lintas` — Total byte IPv6 lalu lintas yang direkam.
- `VpcFlowLogsRejectedTCPTrafficKoneksi TCP` yang ditolak berdasarkan grup keamanan atau jaringan ACLs Anda.
- `VpcFlowLogsRejectedTraffic`— Lalu lintas yang ditolak berdasarkan grup atau jaringan keamanan Anda ACLs.
- `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`— IDs Dari 50 contoh dengan lalu lintas terbanyak yang tercatat.
- `VpcFlowLogsTopTalkingSubnets`— IDs 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 tercatat.
- `VpcFlowLogsTotalBytesTransferredPacketLevel`— 50 pasang alamat IP sumber dan tujuan tingkat paket dengan byte terbanyak yang tercatat.
- `VpcFlowLogsTrafficFrmSrcAddr`— Lalu lintas yang direkam untuk alamat IP sumber tertentu.
- `VpcFlowLogsTrafficToDstAddr`— Lalu lintas yang direkam untuk alamat IP tujuan tertentu.

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](#)
- ['LogDestinationNotFoundException' atau 'Akses Ditolak untuk kesalahan LogDestination '](#)
- [Melebihi batas kebijakan bucket Amazon S3](#)
- [LogDestination tidak terkirim](#)
- [Aliran log ukuran data 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 aliran ke grup CloudWatch log Log atau [SkipData entri mungkin ada](#).

Solusi

Periksa tab Flow logs untuk VPC, subnet, atau antarmuka jaringan. Perhatikan bahwa Anda tidak dapat menjelaskan log aliran untuk VPC atau subnet yang dibagikan dengan Anda, tetapi Anda dapat menjelaskan log aliran untuk antarmuka jaringan yang Anda buat di VPC atau subnet yang dibagikan dengan Anda. Jika ada kesalahan, mereka muncul di kolom Status. Atau, gunakan [describe-flow-logs](#) perintah, dan periksa nilai yang dikembalikan di `DeliverLogsErrorMessage` lapangan.

Berikut ini adalah kemungkinan nilai kesalahan untuk status:

- `Rate limited`: Kesalahan ini dapat terjadi jika pelambatan CloudWatch Log telah diterapkan — ketika jumlah catatan log aliran untuk antarmuka jaringan lebih tinggi dari jumlah maksimum catatan yang dapat dipublikasikan dalam jangka waktu tertentu. Kesalahan ini juga dapat terjadi jika Anda telah mencapai kuota untuk jumlah grup CloudWatch 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 mempublikasikan catatan log alur ke grup log CloudWatch

- 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 CloudWatch Log](#).

- `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 aliran, dan VPC Amazon atau EC2 konsol Amazon menampilkan log aliran 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 aliran masih dibuat. Dalam beberapa kasus, ini bisa memakan waktu sepuluh menit atau lebih setelah Anda membuat log aliran untuk grup log yang akan dibuat, dan untuk data yang akan ditampilkan.
- Belum ada lalu lintas yang dicatat untuk antarmuka jaringan Anda. Grup log di CloudWatch Log hanya dibuat saat lalu lintas direkam.

Solusi

Tunggu beberapa menit untuk membuat grup log, atau mencatat lalu lintas.

'LogDestinationNotFoundException' atau 'Akses Ditolak untuk kesalahan LogDestination '

Masalah

Anda mendapatkan `LogDestinationNotFoundException` kesalahan `Access Denied for LogDestination` atau kesalahan saat membuat log aliran.

Kemungkinan penyebab

- Saat membuat log alur yang memublikasikan data ke bucket Amazon S3, kesalahan ini menunjukkan bahwa bucket S3 yang ditentukan tidak dapat ditemukan atau kebijakan bucket tidak mengizinkan log dikirimkan 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 memublikasikan ke Amazon S3, pastikan 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 gunakan ID akun dan nama bucket yang benar di ARN.
- Saat memublikasikan 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 ARN kunci KMS. Ubah jenis enkripsi S3 default dari ID kunci KMS ke ARN kunci KMS. Untuk informasi selengkapnya, lihat [Mengonfigurasi enkripsi default](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Aliran log ukuran data tidak sesuai dengan data penagihan

Masalah

Ukuran data total log aliran 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](#) penjelasan tentang 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/EC2Namespace 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 • Setiap 24 jam. Dimensi • Nama:Per-VPC Metrics, Nilai: ID VPC.

AWS/UsageNamespace 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

Metrik	Deskripsi
	• 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 • 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

Metrik	Deskripsi
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 hal berikut ini:
 - 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
<i>region</i> -PublicIP	Waktu IPv4 alamat publik digunakan oleh sumber daya.	Jam	Per-detik

Kode	Deskripsi	Unit	Granularitas
<code>v4:InUseAddress</code>			
<i>region</i> - <code>PublicIP v4:IdleAddress</code>	Waktu dimana IPv4 alamat publik tidak digunakan oleh sumber daya.	Jam	Per-detik
<i>region</i> - <code>PublicIP v4:ContiguousBlock</code>	Penggunaan IPv4 alamat publik di blok IPv4 bersebelahan yang disediakan Amazon.	Jam	Per Jam
<i>region</i> - <code>IPAddressesManager- IP-Hours</code>	Waktu alamat IP dikelola oleh IPAM Advanced Tier.	Jam	Per Jam

Titik akhir VPC

Kode	Deskripsi	Unit	Granularitas
<i>region</i> - <code>VpcEndpoint-Hours</code>	Waktu dimana titik akhir VPC antarmuka disediakan.	Jam	Per Jam
<i>region</i> - <code>VpcEndpoint-Bytes</code>	Data diproses oleh titik akhir VPC antarmuka.	GB	Per Jam
<i>region</i> - <code>VpcEndpoint-GWLBE-Hours</code>	Waktu dimana titik akhir Load Balancer Gateway disediakan.	Jam	Per Jam

Kode	Deskripsi	Unit	Granularitas
<i>region</i> -VpcEndpoint-GWLBE-Bytes	Data diproses oleh titik akhir Load Balancer Gateway.	GB	Per Jam

Transit gateway

Kode	Deskripsi	Unit	Granularitas
<i>region</i> -TransitGateway-Hours	Penggunaan lampiran gateway transit.	Jam	Per Jam
<i>region</i> -TransitGateway-Bytes	Data diproses oleh gateway transit.	GB	Per Jam
<i>region</i> -TGW-Multicast-Consumer-Bytes	Data yang diproses oleh instance penerima multicast.	GB	Per Jam

Analisis jaringan

Kode	Deskripsi	Unit	Granularitas
<i>region</i> -Analysis-Runs	Jumlah jalur jaringan yang dianalisis oleh Reachability Analyzer.	Hitungan	Per analisis

Kode	Deskripsi	Unit	Granularitas
<i>region</i> -NetworkInterface-Assessment	Jumlah antarmuka jaringan yang dianalisis oleh Network Access Analyzer.	Hitungan	Per penilaian

Mirroring lalu lintas

Kode	Deskripsi	Unit	Granularitas
<i>region</i> -ENI-Mirror	Waktu antarmuka jaringan dikonfigurasi untuk pencerminan lalu lintas.	Jam	Per Jam

Kisi VPC

Kode	Deskripsi	Unit	Granularitas
<i>region</i> -VPC Lattice-Service-Hourly	Waktu berjalan untuk layanan VPC Lattice.	Jam	Per Jam
<i>region</i> -VPC Lattice-DataProcessing-Bytes	Data diproses oleh layanan VPC Lattice.	GB	Per Jam
<i>region</i> -VPC Lattice-RequestCount-Free	Permintaan HTTP gratis dan koneksi TCP.	Hitungan	Per Jam

Kode	Deskripsi	Unit	Granularitas
<i>region</i> -VpcLattice-Service-Network-Resource-Hours	Waktu berjalan untuk jaringan layanan VPC Lattice.	Jam	Per Jam

Sumber daya lintas akun/wilayah

Kode	Deskripsi	Unit	Granularitas
<i>region</i> -VpcResource-Provider-Bytes	Data yang ditransfer dari sumber penyedia di seluruh akun atau Wilayah.	GB	Per Jam
<i>region</i> -VpcResource-Consumer-Bytes	Data yang ditransfer oleh sumber daya konsumen di seluruh akun atau Wilayah.	GB	Per Jam

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 antara Anda AWS dan Anda. [Model tanggung jawab bersama](#) menjelaskan hal ini sebagai keamanan dari 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. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari [Program AWS Kepatuhan](#). Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon Virtual Private Cloud, lihat [AWS Layanan dalam Lingkup menurut AWS Layanan Program Kepatuhan](#).
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup 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 VPC Amazon Anda.

Daftar Isi

- [Pastikan perlindungan data di Amazon Virtual Private Cloud](#)
- [Identity and access management untuk Amazon VPC](#)
- [Keamanan infrastruktur di Amazon VPC](#)
- [Kontrol lalu lintas ke AWS sumber daya Anda 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](#)
- [Memblokir akses publik ke VPCs dan subnet](#)

- [Praktik terbaik keamanan untuk VPC Anda](#)

Pastikan perlindungan data di Amazon Virtual Private Cloud

[Model tanggung jawab AWS bersama 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. Lihat informasi yang lebih lengkap tentang privasi data dalam [Pertanyaan Umum Privasi Data](#). Lihat informasi tentang perlindungan data di Eropa di pos blog [Model Tanggung Jawab Bersama dan GDPR AWS](#) di Blog Keamanan AWS .

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 penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat [Bekerja dengan CloudTrail jejak](#) di AWS CloudTrail Panduan 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 SDKs 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.

Pastikan privasi lalu lintas internetwork 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 memungkinkan lalu lintas masuk dan keluar tertentu di tingkat sumber daya (seperti EC2 instance). 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](#).
- **Network Access Control List (ACL):** Jaringan ACLs mengizinkan 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 CloudWatch Log atau Amazon S3, dan ini dapat membantu Anda mendiagnosis aturan ACL grup dan jaringan keamanan yang terlalu ketat atau terlalu permisif. Untuk informasi selengkapnya, lihat [Mencatat lalu lintas IP menggunakan VPC Flow Logs](#).
- **Pencerminan lalu lintas:** Anda dapat menyalin lalu lintas jaringan dari elastic network interface dari EC2 instance Amazon. Anda kemudian dapat mengirim lalu lintas ke peralatan out-of-band keamanan dan pemantauan. Untuk informasi lebih lanjut, lihat [Panduan Mirroring Lalu Lintas](#).

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](#)

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 kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensial yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat [Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS](#).

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensial Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Guna mengetahui informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat [AWS Signature Version 4 untuk permintaan API](#) dalam Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat [Autentikasi multi-faktor](#) dalam Panduan Pengguna AWS IAM Identity Center dan [Autentikasi multi-faktor AWS di IAM](#) dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat [Tugas yang memerlukan kredensial pengguna root](#) dalam Panduan Pengguna IAM.

Pengguna dan grup IAM

[Pengguna IAM](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial

sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat [Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang](#) dalam Panduan Pengguna IAM.

[Grup IAM](#) adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat meminta kelompok untuk menyebutkan IAMAdmins dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat [Kasus penggunaan untuk pengguna IAM](#) dalam Panduan Pengguna IAM.

Peran IAM

[Peran IAM](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Untuk mengambil peran IAM sementara AWS Management Console, Anda dapat [beralih dari pengguna ke peran IAM \(konsol\)](#). Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat [Metode untuk mengambil peran](#) dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat [Buat peran untuk penyedia identitas pihak ketiga](#) dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat [Set izin](#) dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.

- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
- Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat [Sesi akses maju](#).
- Peran layanan – Peran layanan adalah [peran IAM](#) yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS](#) dalam Panduan pengguna IAM.
- Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS permintaan API. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensi

sementara. Untuk informasi selengkapnya, lihat [Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di Panduan Pengguna IAM](#).

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat [Gambaran umum kebijakan JSON](#) dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan](#) dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan

terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat [Pilih antara kebijakan yang dikelola dan kebijakan inline](#) dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah 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. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan prinsipal](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACLs)

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung. ACLs Untuk mempelajari selengkapnya ACLs, lihat [Ringkasan daftar kontrol akses \(ACL\)](#) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh

batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat [Batasan izin untuk entitas IAM](#) dalam Panduan Pengguna IAM.

- Kebijakan kontrol layanan (SCPs) — SCPs adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organizations dan SCPs, lihat [Kebijakan kontrol layanan](#) di Panduan AWS Organizations Pengguna.
- Kebijakan kontrol sumber daya (RCPs) — RCPs adalah kebijakan JSON yang dapat Anda gunakan untuk menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda tanpa memperbarui kebijakan IAM yang dilampirkan ke setiap sumber daya yang Anda miliki. RCP membatasi izin untuk sumber daya di akun anggota dan dapat memengaruhi izin efektif untuk identitas, termasuk Pengguna root akun AWS, terlepas dari apakah itu milik organisasi Anda. Untuk informasi selengkapnya tentang Organizations dan RCPs, termasuk daftar dukungan Layanan AWS tersebut RCPs, lihat [Kebijakan kontrol sumber daya \(RCPs\)](#) di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. 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 saat 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 layanan AWS lainnya dengan IAM, [AWS lihat 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 mendukung 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. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Amazon VPC membagikan namespace API-nya dengan Amazon. EC2 Tindakan kebijakan di Amazon VPC menggunakan prefiks berikut ini sebelum tindakan: `ec2:`. Misalnya, untuk memberikan izin kepada pengguna untuk membuat VPC menggunakan operasi `CreateVpc` API, Anda memberikan akses ke tindakan tersebut `ec2::CreateVpc`. 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 VPC Amazon, 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. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan [Amazon Resource Name \(ARN\)](#). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, 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 VPCs di Wilayah tertentu yang termasuk dalam 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 Amazon EC2 API melibatkan banyak sumber daya. Untuk menentukan beberapa sumber daya dalam satu pernyataan, pisahkan ARNs dengan koma.

```
"Resource": [  
    "resource1",  
    "resource2"  
]
```

Untuk melihat daftar jenis sumber daya Amazon VPC dan jenisnya ARNs, 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. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen Condition (atau blok Condition) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen Condition bersifat opsional. 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.

Jika Anda menentukan beberapa elemen Condition dalam sebuah pernyataan, atau beberapa kunci dalam elemen Condition tunggal, maka AWS akan mengevaluasinya menggunakan operasi AND logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan OR operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tanda yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat [Elemen kebijakan IAM: variabel dan tanda](#) dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat [kunci konteks kondisi AWS global](#) di Panduan Pengguna IAM.

Semua EC2 tindakan Amazon mendukung kunci `aws:RequestedRegion` dan `ec2:Region` kondisi. 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 yang dapat Anda gunakan kunci kondisi, lihat [Tindakan yang ditentukan oleh Amazon EC2](#).

kebijakan berbasis sumber daya Amazon VPC

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya Amazon VPC dan dengan syarat 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 prinsipal 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 dalam [elemen kondisi](#) kebijakan menggunakan kunci kondisi. Untuk informasi selengkapnya, lihat [Memberikan izin untuk menandai sumber daya selama pembuatan](#) di Panduan EC2 Pengguna Amazon.

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 khusus.

Gunakan kredensial sementara

Anda dapat menggunakan kredensial sementara untuk masuk dengan gabungan, menjalankan IAM role, atau menjalankan peran lintas akun. Anda memperoleh kredensial keamanan sementara dengan memanggil operasi AWS STS API seperti [AssumeRole](#) atau [GetFederationToken](#).

Amazon VPC men-support penggunaan kredensial sementara.

Peran terkait layanan

[Peran terkait AWS layanan](#) memungkinkan layanan mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Peran terkait layanan muncul di akun IAM Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat tetapi tidak dapat menyunting izin untuk peran terkait layanan.

[Transit Gateway](#) men-support peran yang terkait 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 membuat log alur, Anda harus memilih peran yang memungkinkan layanan flow CloudWatch logs mengakses Log. Untuk informasi selengkapnya, lihat [the section called “Peran IAM untuk menerbitkan log alur ke CloudWatch Log”](#).

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 AWS Management Console, 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](#)
- [Memblokir akses publik ke VPCs dan subnet](#)
- [Contoh kebijakan Amazon VPC tambahan](#)

Praktik terbaik kebijakan

Kebijakan berbasis identitas 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:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola 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 ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS 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 mengharuskan pengguna IAM atau pengguna root di Anda, 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 VPC Amazon di AWS akun Anda. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana dimaksud 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 membuat panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang cocok dengan operasi API yang perlu dilakukan peran.

Buat sebuah VPC dengan subnet publik

Contoh berikut memungkinkan peran untuk membuat VPCs, subnet, tabel rute, dan gateway internet. Peran juga dapat melampirkan gateway internet ke VPC dan membuat rute dalam tabel rute. `ec2:ModifyVpcAttribute` tindakan 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 VPC Amazon.

Modifikasi dan hapus sumber daya VPC

Anda mungkin ingin mengontrol sumber daya VPC yang dapat dimodifikasi atau dihapus oleh peran. Misalnya, kebijakan berikut memungkinkan peran untuk bekerja dengan dan menghapus tabel rute yang memiliki tagPurpose=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 memungkinkan peran untuk mengelola grup keamanan. Pernyataan pertama memungkinkan peran untuk menghapus grup keamanan apa pun dengan tag `Stack=test` dan 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 kelompok 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 tersebut 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:region:account-id:security-group/*",
    "Condition": {
      "ArnEquals": {

```

```

        "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/vpc-id"
    }
}
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeTags"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:ModifySecurityGroupRules"
    ],
    "Resource": "arn:aws:ec2:region:account-id:security-group-rule/*"
}
]
}

```

Luncurkan instans ke dalam subnet tertentu

Kebijakan berikut memberikan izin peran untuk meluncurkan instance ke subnet tertentu dan menggunakan grup keamanan tertentu dalam permintaan. Kebijakan melakukan ini dengan menentukan ARN untuk subnet dan ARN untuk kelompok 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 tersebut 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:region:image/ami-*",
    "arn:aws:ec2:region:account:instance/*",
    "arn:aws:ec2:region:account:subnet/subnet-id",
    "arn:aws:ec2:region:account:network-interface/*",
    "arn:aws:ec2:region:account:volume/*",
    "arn:aws:ec2:region:account:key-pair/*",
    "arn:aws:ec2:region:account:security-group/sg-id"
  ]
}]
}

```

Meluncurkan instans ke VPC tertentu

Kebijakan berikut memberikan izin peran untuk meluncurkan instance 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 instance hanya menggunakan AMIs yang memiliki tag `"department=dev"`.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:region:account-id:subnet/*",
    "Condition": {
      "ArnEquals": {
        "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/vpc-id"
      }
    }
  ]
},
{

```

```

    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:region::image/ami-*",
    "Condition": {
      "StringEquals": {
        "ec2:ResourceTag/department": "dev"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region:account:instance/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region:account:network-interface/*",
      "arn:aws:ec2:region:account:key-pair/*",
      "arn:aws:ec2:region:account:security-group/*"
    ]
  }
]
}

```

Memblokir akses publik ke VPCs dan subnet

Contoh kebijakan berikut memberikan izin peran untuk bekerja dengan [fitur VPC Block Public Access \(BPA\)](#) untuk memblokir akses publik ke sumber daya dan subnet. VPCs

Contoh 1 - Izinkan akses hanya-baca ke pengaturan seluruh akun VPC BPA dan pengecualian VPC BPA.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VPCBPAPublicAccess",
      "Action": [
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeVpcBlockPublicAccessExclusions"
      ]
    }
  ]
}

```

```

    ],
    "Effect": "Allow",
    "Resource": "*"
  }
]
}

```

Contoh 2 - Izinkan akses baca dan tulis penuh ke pengaturan seluruh akun VPC BPA dan pengecualian VPC BPA.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VPCBPFullAccess",
      "Action": [
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeVpcBlockPublicAccessExclusions",
        "ec2:ModifyVpcBlockPublicAccessOptions",
        "ec2:CreateVpcBlockPublicAccessExclusion",
        "ec2:ModifyVpcBlockPublicAccessExclusion",
        "ec2>DeleteVpcBlockPublicAccessExclusion"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}

```

Contoh 3 - Izinkan akses ke semua EC2 APIs kecuali memodifikasi pengaturan VPC BPA dan membuat pengecualian.

```

{
  "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 \(AWS PrivateLink\)](#)
- [Pengintip 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 di luar AWS akun saya untuk mengakses sumber daya VPC Amazon saya](#)

Saya tidak berwenang untuk melakukan tindakan di Amazon VPC

Jika AWS Management Console memberitahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, maka Anda harus menghubungi administrator Anda untuk 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 termasuk dalam 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 diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Amazon VPC.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut 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 di luar AWS akun saya untuk mengakses sumber daya VPC Amazon 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 (ACLs), 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 Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat [Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki](#) di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat [Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga](#) dalam 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 bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS 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 AWS terkelola saat 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 terkelola: VPCFull Akses Amazon

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 [Amazon VPCFull Access](#) di Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: Amazon VPCRead OnlyAccess

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 [Amazon VPCRead OnlyAccess](#) di Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: Amazon VPCCross AccountNetworkInterfaceOperations

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 [Amazon VPCCross AccountNetworkInterfaceOperations](#) di Referensi Kebijakan AWS Terkelola.

Amazon VPC memperbarui kebijakan terkelola AWS

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Amazon VPC sejak layanan ini mulai melacak perubahan ini pada Maret 2021.

Perubahan	Deskripsi	Tanggal
the section called “VPCFullAccesses Amazon” — Perbaruan ke kebijakan yang sudah ada	MenambahkanAssociateSecurityGroupVpc, DescribeSecurityGroupVpcAssociations, dan DisassociateSecuri	Desember 9, 2024

Perubahan	Deskripsi	Tanggal
	tyGroupVpc tindakan, yang memungkinkan Anda untuk mengaitkan, memisahkan, dan melihat asosiasi grup keamanan dengan VPCs.	
the section called “Amazon VPCRead OnlyAccess” – Pembaruan ke kebijakan yang ada	Menambahkan DescribeSecurityGroupVpcAssociations tindakan, yang memungkinkan Anda untuk melihat asosiasi grup keamanan dengan VPCs.	Desember 9, 2024
the section called “VPCFullAccesses Amazon” – Pembaruan ke kebijakan yang ada	Menambahkan GetSecurityGroupsForVpc tindakan, yang memungkinkan Anda mendapatkan grup keamanan yang dapat digunakan di VPC Anda.	Februari 8, 2024
the section called “Amazon VPCRead OnlyAccess” – Pembaruan ke kebijakan yang ada	Menambahkan GetSecurityGroupsForVpc tindakan, yang memungkinkan Anda mendapatkan grup keamanan yang dapat digunakan di VPC Anda.	Februari 8, 2024
the section called “Amazon VPCCross AccountNetworkInterfaceOperations” – Pembaruan ke kebijakan yang ada	Ditambahkan AssignIpv6Addresses dan UnassignIpv6Addresses tindakan, yang memungkinkan Anda untuk mengelola IPv6 alamat yang terkait dengan antarmuka jaringan.	25 September 2023

Perubahan	Deskripsi	Tanggal
the section called “Amazon VPCRead OnlyAccess” – Pembaruan ke kebijakan yang ada	Menambahkan DescribeSecurityGroupRules tindakan, yang memungkinkan Anda untuk melihat aturan grup keamanan .	2 Agustus 2021
the section called “VPCFullAccesses Amazon” – Pembaruan ke kebijakan yang ada	Menambahkan DescribeSecurityGroupRules dan ModifySecurityGroupRules tindakan, yang memungkinkan Anda untuk melihat dan memodifikasi aturan grup keamanan .	2 Agustus 2021
the section called “VPCFullAccesses Amazon” – Pembaruan ke kebijakan yang ada	Menambahkan tindakan untuk gateway operator, IPv6 kolam renang, gateway lokal, dan tabel rute gateway lokal.	23 Juni 2021
the section called “Amazon VPCRead OnlyAccess” – Pembaruan ke kebijakan yang ada	Menambahkan tindakan untuk gateway operator, IPv6 kolam renang, gateway lokal, dan tabel rute gateway lokal.	23 Juni 2021

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 [Keamanan AWS Cloud](#). Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat [Perlindungan Infrastruktur dalam Kerangka Kerja](#) yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan 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.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal IAM. Atau, Anda bisa menggunakan [AWS Security Token Service](#) (AWS STS) untuk membuat kredensial keamanan sementara untuk menandatangani permintaan.

Isolasi jaringan

Virtual Private Cloud (VPC) adalah jaringan virtual di area Anda sendiri yang terisolasi secara logis di AWS Cloud. Gunakan terpisah VPCs untuk mengisolasi 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 instans tersebut tidak dapat diakses secara langsung dari internet.

Anda dapat menggunakan [AWS PrivateLink](#) untuk mengaktifkan sumber daya di VPC Anda untuk terhubung Layanan AWS menggunakan alamat IP pribadi, seolah-olah layanan tersebut di-host 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 EC2 contoh:

- Gunakan [grup keamanan](#) sebagai mekanisme utama untuk mengontrol akses jaringan ke Anda VPCs. Bila perlu, gunakan [jaringan ACLs untuk menyediakan kontrol jaringan](#) butir kasar tanpa kewarganegaraan. Grup keamanan lebih fleksibel daripada jaringan ACLs, karena kemampuan mereka untuk melakukan penyaringan paket stateful dan membuat aturan yang merujuk pada kelompok keamanan lainnya. Jaringan ACLs dapat efektif sebagai kontrol sekunder (misalnya, untuk menolak subset tertentu dari lalu lintas) atau sebagai rel penjaga subnet tingkat tinggi. Juga,

karena jaringan ACLs berlaku untuk seluruh subnet, mereka dapat digunakan seolah-olah defense-in-depth sebuah 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.
- Konfigurasi [tabel rute](#) subnet dengan rute jaringan minimum untuk mendukung persyaratan konektivitas Anda.
- Pertimbangkan untuk menggunakan grup keamanan tambahan atau antarmuka jaringan untuk mengontrol dan mengaudit lalu lintas manajemen EC2 instans Amazon secara terpisah dari lalu lintas aplikasi biasa. Oleh karena itu, Anda dapat menerapkan kebijakan IAM khusus untuk kontrol perubahan, sehingga lebih mudah untuk mengaudit perubahan aturan grup keamanan atau skrip verifikasi aturan otomatis. Beberapa antarmuka jaringan juga menyediakan opsi tambahan untuk mengontrol lalu lintas jaringan, termasuk kemampuan untuk membuat kebijakan perutean berbasis host atau memanfaatkan aturan perutean subnet VPC yang berbeda berdasarkan antarmuka jaringan yang ditetapkan ke subnet.
- Gunakan AWS Virtual Private Network atau AWS Direct Connect untuk membuat koneksi pribadi dari jaringan jarak jauh Anda ke jaringan Anda VPCs. Untuk informasi selengkapnya, lihat [Network-to-Amazon opsi konektivitas VPC](#).
- Gunakan [Log Aliran VPC](#) untuk memantau lalu lintas yang menjangkau instans Anda.
- Gunakan [AWS Security Hub](#) untuk memeriksa aksesibilitas jaringan yang tidak disengaja pada instans Anda.
- Gunakan [AWS Network Firewall](#) untuk melindungi subnet di VPC Anda dari ancaman jaringan umum.

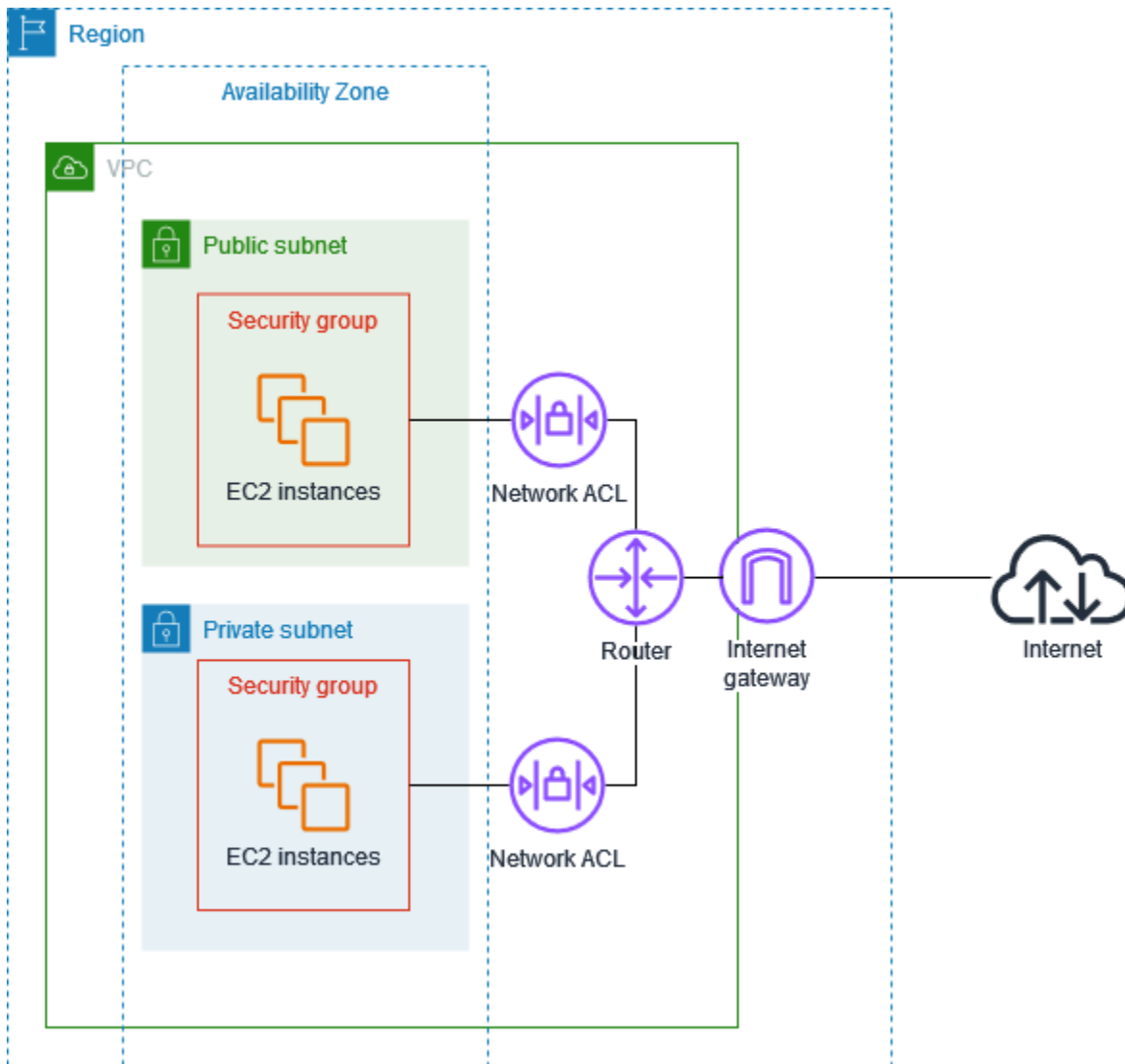
Bandingkan grup keamanan dan jaringan ACLs

Tabel berikut merangkum perbedaan dasar antara kelompok keamanan dan jaringan ACLs.

Karakteristik	Grup keamanan	ACL jaringan
Tingkat operasi	Tingkat instans	Tingkat subnet
Cakupan	Berlaku untuk semua instance yang terkait dengan grup keamanan	Berlaku untuk semua instance di subnet terkait

Karakteristik	Grup keamanan	ACL jaringan
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 sampai kecocokan untuk lalu lintas ditemukan
Kembalikan lalu lintas	Diizinkan secara otomatis (stateful)	Harus diizinkan secara eksplisit (tanpa kewarganegaraan)

Diagram berikut menggambarkan lapisan keamanan yang disediakan oleh kelompok keamanan dan jaringan ACLs. 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 jaringan ACLs sebagai lapisan pertahanan tambahan. Untuk informasi selengkapnya, lihat [Contoh: Kontrol akses ke instans dalam subnet](#).

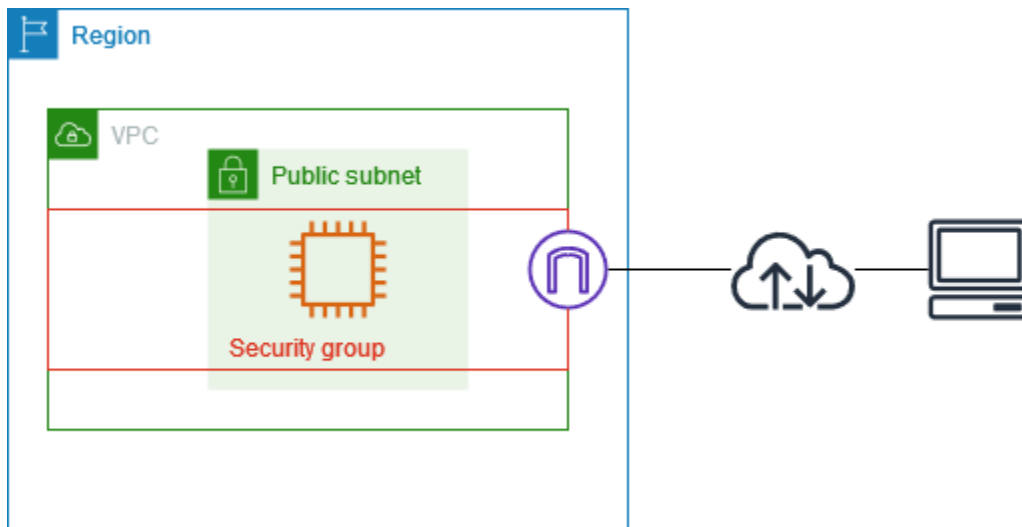
Kontrol lalu lintas ke AWS sumber daya Anda menggunakan grup keamanan

Grup keamanan mengontrol lalu lintas yang diizinkan untuk mencapai dan meninggalkan sumber daya yang terkait dengannya. Misalnya, setelah Anda mengaitkan grup keamanan dengan EC2 instans, grup ini mengontrol lalu lintas masuk dan keluar untuk instance tersebut.

Saat Anda membuat VPC, VPC 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 sebuah EC2 instance. 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 memungkinkan lalu lintas ICMP ke instance dari jaringan Anda, maka Anda dapat melakukan ping instance dari komputer Anda. Jika grup keamanan tidak berisi aturan yang memungkinkan lalu lintas SSH, maka Anda tidak dapat terhubung ke instance Anda menggunakan SSH.



Daftar Isi

- [Dasar-dasar grup keamanan](#)
- [Contoh grup keamanan](#)
- [Aturan-aturan grup keamanan](#)
- [Grup keamanan default untuk Anda VPCs](#)
- [Buat grup keamanan untuk VPC Anda](#)
- [Mengonfigurasi aturan grup keamanan](#)
- [Menghapus grup keamanan](#)
- [Mengaitkan grup keamanan dengan beberapa VPCs](#)
- [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 VPCs lainnya jika menggunakan fitur [Asosiasi VPC Grup Keamanan](#) untuk mengaitkan grup keamanan dengan grup keamanan VPCs lainnya 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, A-Z, 0-9, spasi, dan . _ - / () # , @ [] + = & ; { } ! \$ * .
 - Ketika nama berisi spasi tambahan, kami 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 instans, lalu lintas respons untuk permintaan tersebut diizinkan untuk mencapai instance terlepas dari aturan grup keamanan masuk. Tanggapan terhadap lalu lintas masuk yang diizinkan diizinkan untuk meninggalkan instance, terlepas dari aturan keluar.
- Grup keamanan tidak memfilter lalu lintas yang ditujukan ke dan dari yang berikut ini:
 - Layanan Nama Domain Amazon (DNS)
 - Protokol Konfigurasi Host Dinamis (DHCP)
 - EC2 Metadata contoh Amazon
 - Titik akhir metadata tugas Amazon ECS
 - Aktivasi lisensi untuk instance 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](#).

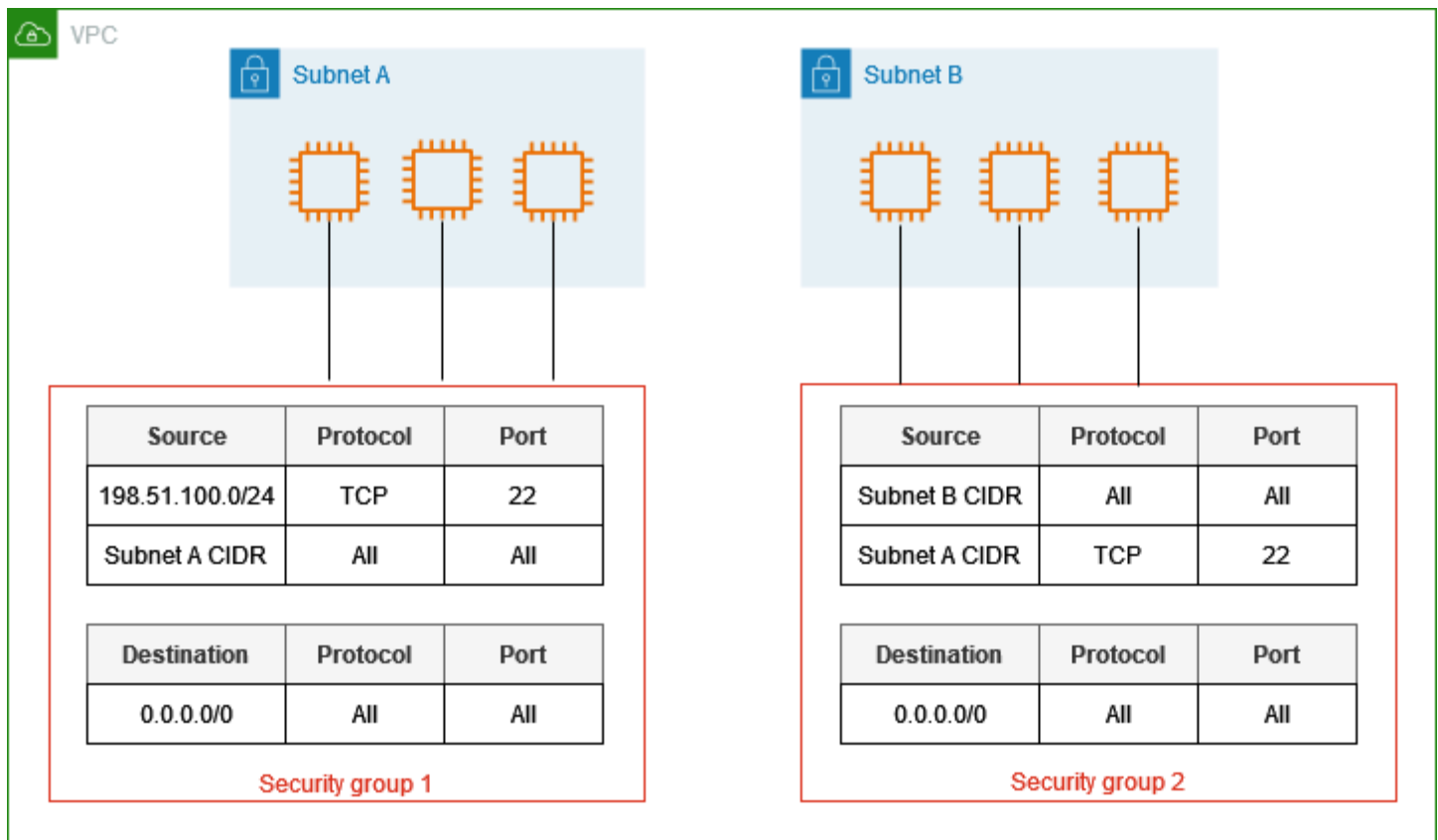
Praktik terbaik

- 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 Anda menambahkan aturan masuk untuk port 22 (SSH) atau 3389 (RDP) sehingga Anda dapat mengakses EC2 instans Anda, 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 dibatasi pada sumber atau tujuan yang membutuhkannya.
- Pertimbangkan untuk membuat jaringan ACLs dengan aturan yang mirip dengan grup keamanan Anda, untuk menambahkan lapisan keamanan tambahan ke VPC Anda. Untuk informasi selengkapnya tentang perbedaan antara grup keamanan dan jaringan ACLs, lihat [Bandingkan grup keamanan dan jaringan ACLs](#).

Contoh grup keamanan

Diagram berikut menunjukkan VPC dengan dua kelompok keamanan dan dua subnet. Instans di subnet A memiliki persyaratan konektivitas yang sama, sehingga terkait dengan grup keamanan 1. Instans di subnet B memiliki persyaratan konektivitas yang sama, sehingga terkait dengan grup keamanan 2. Aturan grup keamanan mengizinkan lalu lintas sebagai berikut:

- Aturan masuk pertama dalam grup keamanan 1 memungkinkan lalu lintas SSH ke instance di subnet A dari rentang alamat yang ditentukan (misalnya, rentang di jaringan Anda sendiri).
- Aturan inbound kedua dalam grup keamanan 1 memungkinkan instance di subnet A untuk berkomunikasi satu sama lain menggunakan protokol dan port apa pun.
- Aturan inbound pertama dalam kelompok keamanan 2 memungkinkan instance di subnet B untuk berkomunikasi satu sama lain menggunakan protokol dan port apa pun.
- Aturan inbound kedua dalam 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-aturan grup keamanan

Aturan grup keamanan mengontrol lalu lintas masuk yang diizinkan untuk mencapai sumber daya yang terkait dengan grup keamanan. Aturan-atruran 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 kelompok 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, ia 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 diperbolehkan.
- 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 Anda secara otomatis diterapkan 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 EC2 Pengguna Amazon.
- Saat Anda membuat aturan grup keamanan, AWS menetapkan ID unik ke 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 Resolver Route 53, 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 Resolver Route 53, 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. Misalnya, gunakan tipe 8 untuk ICMP Echo Request atau ketik 128 untuk ICMPv6 Echo Request. Untuk informasi selengkapnya, lihat [Aturan 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 IPv4 alamat. Anda harus menggunakan panjang awalan /32. Sebagai contoh, 203.0.113.1/32.
 - Satu IPv6 alamat. Anda harus menggunakan panjang awalan /128. Sebagai contoh, 2001:db8:1234:1a00::123/128.
 - Berbagai IPv4 alamat, dalam notasi blok CIDR. Misalnya, 203.0.113.0/24.
 - Berbagai IPv6 alamat, dalam notasi blok CIDR. Sebagai contoh, 2001:db8:1234:1a00::/64.
 - ID daftar awalan. Sebagai contoh, p1-1234abc1234abc123. Untuk informasi selengkapnya, lihat [Daftar prefiks terkelola](#).
 - ID grup keamanan. Sebagai contoh, sg-1234567890abcdef0. Untuk informasi selengkapnya, lihat [the section called “Referensi kelompok 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 diperbolehkan adalah a-z, A-Z, 0-9, spasi, dan . _ - : / () # , @ [] + = ; { } ! \$ * .

Sebagai contoh, lihat [Aturan grup keamanan untuk kasus penggunaan yang berbeda](#) di Panduan EC2 Pengguna Amazon.

Referensi kelompok keamanan

Saat Anda menentukan grup keamanan sebagai sumber atau tujuan aturan, aturan akan memengaruhi semua instance yang terkait dengan grup keamanan. Instance 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
<i>sg-0abcdef1234567890</i>	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 hubungan mengintip antara VPCs yang terkait dengan kelompok keamanan.
 - Ada gerbang transit antara VPCs yang terkait dengan kelompok keamanan.
- Anda dapat mereferensikan grup keamanan dalam aturan keluar jika salah satu dari berikut ini benar:
 - Grup keamanan dikaitkan dengan VPC yang sama.
 - Ada hubungan mengintip antara VPCs yang terkait dengan kelompok keamanan.
- Tidak ada aturan dari grup keamanan yang direferensikan ditambahkan ke grup keamanan yang mereferensikannya.
- Untuk aturan masuk, EC2 instance yang terkait dengan grup keamanan dapat menerima lalu lintas masuk dari alamat IP pribadi dari EC2 instance yang terkait dengan grup keamanan yang direferensikan.
- Untuk aturan keluar, EC2 instance yang terkait dengan grup keamanan dapat mengirim lalu lintas keluar ke alamat IP pribadi dari EC2 instance yang terkait dengan grup keamanan yang direferensikan.

Batasan

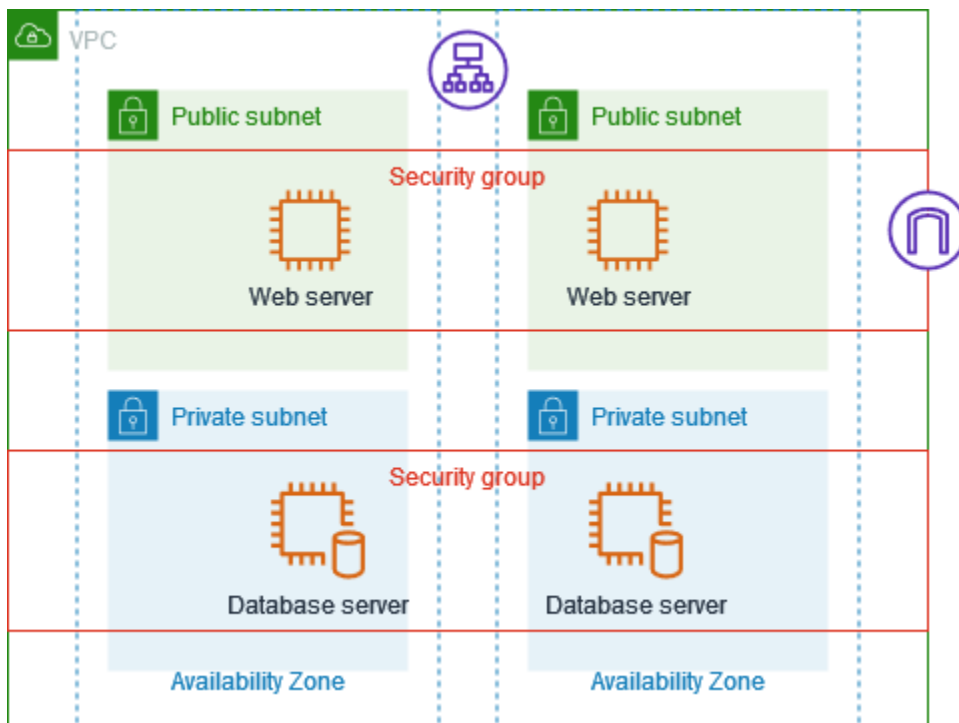
Jika Anda mengonfigurasi rute untuk meneruskan lalu lintas antara dua instans di subnet yang berbeda melalui perangkat middlebox, Anda harus memastikan bahwa grup keamanan untuk kedua instans tersebut mengizinkan lalu lintas mengalir di antara instans. Grup keamanan untuk setiap instance harus mereferensikan 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 Zones, 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 penyeimbang beban untuk memungkinkan 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 diperhitungkan terhadap jumlah maksimum aturan yang dapat Anda miliki per grup keamanan.

- Aturan yang mereferensikan blok CIDR dihitung sebagai satu aturan.
- Aturan yang merujuk kelompok keamanan lain dianggap sebagai satu aturan, tidak peduli ukuran kelompok 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 20 aturan.
- Aturan yang mereferensikan daftar awalan AWS-managed 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 “Daftar awalan AWS-terkelola yang tersedia”](#).

Aturan grup keamanan yang kedaluwarsa

Jika VPC Anda memiliki koneksi peering VPC dengan VPC lain, atau jika VPC menggunakan VPC yang dibagikan oleh akun lain, aturan grup keamanan di VPC Anda dapat mereferensikan grup keamanan di VPC rekan atau VPC bersama tersebut. Hal ini memungkinkan sumber daya yang terkait dengan kelompok keamanan yang direferensikan dan yang terkait dengan kelompok keamanan referensi untuk berkomunikasi satu sama lain. Untuk informasi selengkapnya, lihat [Memperbarui grup keamanan Anda untuk mereferensikan grup keamanan rekan di Panduan Peering VPC Amazon](#).

Jika Anda memiliki aturan grup keamanan yang mereferensikan grup keamanan di VPC rekan atau VPC bersama dan grup keamanan di VPC bersama dihapus atau koneksi peering VPC dihapus, aturan grup keamanan ditandai sebagai basi. Anda dapat menghapus aturan grup keamanan kedaluwarsa seperti yang Anda lakukan terhadap aturan grup keamanan lainnya.

Grup keamanan default untuk Anda VPCs

Default Anda VPCs dan apa pun VPCs yang Anda buat datang dengan grup keamanan default. Nama grup keamanan default adalah "default".

Kami menyarankan Anda membuat grup keamanan untuk sumber daya atau grup sumber daya tertentu, bukan 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 EC2 instance, kami mengaitkan instance tersebut 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.

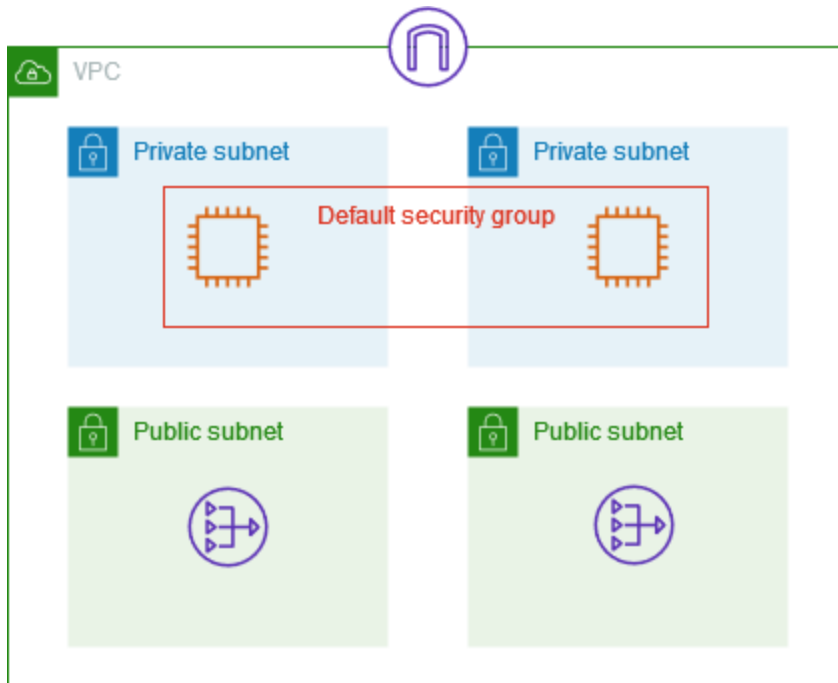
Sumber	Protokol	Rentang Port	Deskripsi
<i>sg-1234567890abcdef0</i>	Semua	Semua	Mengizinkan lalu lintas jalur masuk dari semua sumber daya yang ditetapkan untuk grup keamanan ini. Sumbernya adalah ID dari grup keamanan ini.

Tabel berikut menjelaskan aturan keluar default untuk grup keamanan default.

Tujuan	Protokol	Rentang Port	Deskripsi
0.0.0.0/0	Semua	Semua	Memungkinkan semua IPv4 lalu lintas keluar.
::/0	Semua	Semua	Memungkinkan semua IPv6 lalu lintas keluar. Aturan ini ditambahkan hanya jika VPC Anda memiliki blok IPv6 CIDR terkait.

Contoh

Diagram berikut menunjukkan VPC dengan grup keamanan default, gateway internet, dan gateway NAT. Keamanan default hanya berisi aturan defaultnya, dan dikaitkan dengan dua EC2 instance yang berjalan di VPC. Dalam skenario ini, setiap instance dapat menerima lalu lintas masuk dari instance lain di 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 Anda membuat grup keamanan dengan aturan yang diperlukan dan mengaitkan grup keamanan baru dengan instans, bukan grup keamanan default.



Buat 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 tempat ia dibuat.

Secara default, grup keamanan baru dimulai dengan hanya 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 nanti. Untuk informasi selengkapnya, lihat [Aturan-aturan grup keamanan](#).

Izin yang diperlukan

Sebelum memulai, 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 VPC Amazon 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 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 yang sudah ada

1. Buka konsol VPC Amazon di. <https://console.aws.amazon.com/vpc/>
2. Pada panel navigasi, pilih Grup keamanan.
3. Pilih grup keamanan.
4. Pilih Tindakan, 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 memulai, pastikan Anda memiliki izin yang diperlukan. Untuk informasi selengkapnya, lihat [Mengelola aturan grup keamanan](#).

Sumber dan tujuan

Anda dapat menentukan berikut ini sebagai sumber untuk aturan masuk atau tujuan untuk aturan keluar.

- Kustom — Blok IPv4 CIDR, dan blok IPv6 CIDR, grup keamanan lain, atau daftar awalan.
- Di mana saja- IPv4 - Blok CIDR 0.0.0.0/0 IPv4 .
- Di mana saja- IPv6 - Blok IPv6 CIDR: :/0.
- IP saya — IPv4 Alamat publik komputer lokal Anda.

Warning

Jika Anda memilih Anywhere- IPv4, Anda mengizinkan lalu lintas dari semua IPv4 alamat.
Jika Anda memilih Anywhere- IPv6, Anda mengizinkan lalu lintas dari semua IPv6 alamat.

Ini adalah praktik terbaik untuk mengotorisasi hanya rentang alamat IP tertentu yang memerlukan akses ke sumber daya Anda.

Untuk mengonfigurasi aturan grup keamanan menggunakan konsol

1. Buka konsol VPC Amazon 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 adalah 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 dikonfigurasi 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 IPv4 CIDR, Anda tidak dapat menentukan blok IPv6 CIDR, daftar awalan, atau grup keamanan.
 - c. Untuk menghapus aturan, pilih tombol Hapus.
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 adalah 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 dikonfigurasi 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 IPv4 CIDR, Anda tidak dapat menentukan blok IPv6 CIDR, daftar awalan, atau grup keamanan.
 - c. Untuk menghapus aturan, pilih tombol Hapus.

6. Pilih Simpan aturan.

Untuk mengonfigurasi aturan grup keamanan menggunakan AWS CLI

- Tambahkan - Gunakan [authorize-security-group-egress](#) perintah [authorize-security-group-ingress](#) dan.
- Hapus — Gunakan [revoke-security-group-egress](#) perintah [revoke-security-group-ingress](#) dan.
- Memodifikasi — Gunakan perintah [modify-security-group-rules](#), [update-security-group-rule-descriptions-ingress](#), dan [-description-egress](#). [update-security-group-rule](#)

Menghapus grup keamanan

Setelah 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 VPC Amazon 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 itu akan dihapus. Untuk mengonfirmasi penghapusan, masukkan Hapus.
5. Pilih Hapus.

Untuk menghapus grup keamanan menggunakan AWS CLI

Gunakan perintah [delete-security-group](#).

Mengaitkan grup keamanan dengan beberapa VPCs

Jika Anda memiliki beban kerja yang berjalan di beberapa VPCs yang berbagi persyaratan keamanan jaringan, Anda dapat menggunakan fitur Asosiasi VPC Grup Keamanan untuk mengaitkan grup keamanan dengan VPCs beberapa di Wilayah yang sama. Ini memungkinkan Anda untuk mengelola dan memelihara grup keamanan di satu tempat untuk beberapa VPCs di akun Anda.

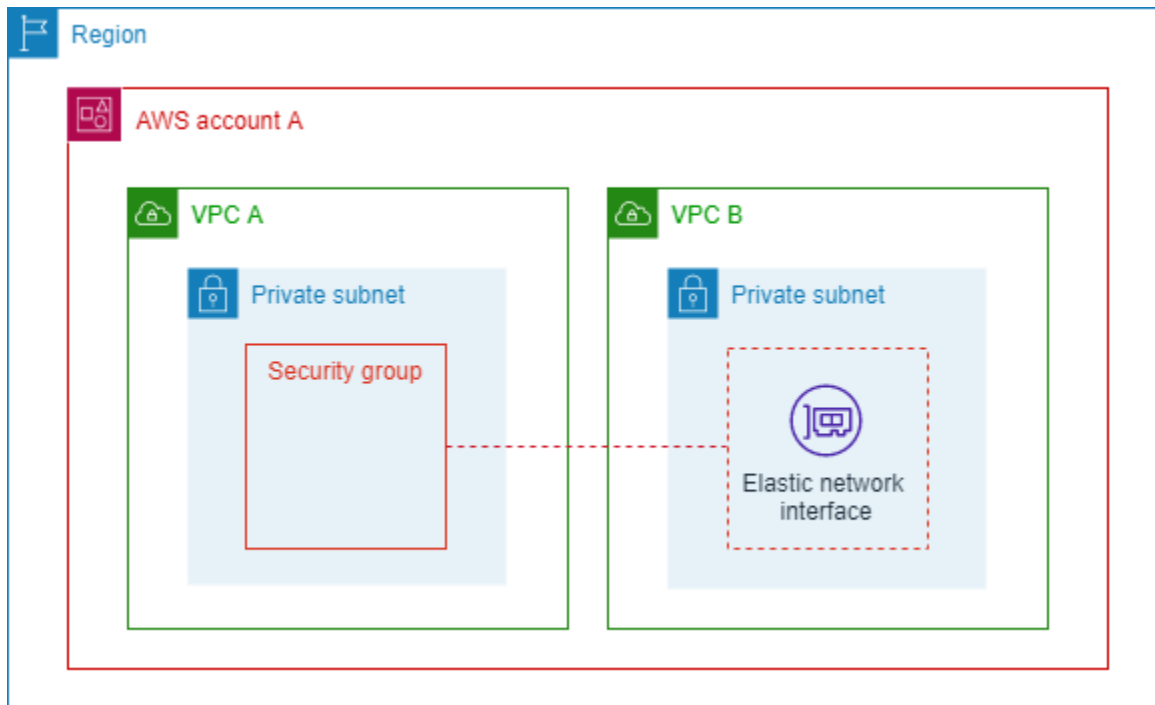


Diagram di atas menunjukkan AWS akun A dengan dua VPCs di dalamnya. Masing-masing VPCs memiliki beban kerja yang berjalan di subnet pribadi. Dalam hal ini, beban kerja di subnet VPC A dan B berbagi persyaratan lalu lintas jaringan yang sama, sehingga Akun A dapat menggunakan fitur asosiasi VPC Grup Keamanan untuk mengaitkan grup keamanan di VPC A dengan VPC B. Setiap pembaruan yang dilakukan ke 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 dan pemilik VPC dapat melihat asosiasi VPC grup keamanan.

Layanan yang mendukung fitur ini

- Amazon API Gateway (APIs hanya REST)
- AWS Auto Scaling
- AWS CloudFormation
- Amazon EC2
- Amazon EFS
- Amazon EKS
- Amazon FSx
- AWS PrivateLink
- Amazon Route 53
- Penyeimbang Beban Elastis
 - Penyeimbang Beban Aplikasi
 - Penyeimbang Beban Jaringan

Kaitkan grup keamanan dengan VPC lain

Bagian ini menjelaskan cara menggunakan AWS Management Console dan AWS CLI untuk mengaitkan grup keamanan dengan VPCs.

AWS Management Console

Untuk mengaitkan grup keamanan dengan VPC lain

1. Buka konsol VPC Amazon 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 diasosiasikan dengan grup keamanan.
7. Pilih Kaitkan VPC.

Command line

Untuk mengaitkan grup keamanan dengan VPC lain

1. Buat asosiasi VPC dengan [associate-security-group-vpc](#)
2. Periksa status asosiasi VPC dengan [describe-security-group-vpc-asosiasi](#) dan tunggu statusnya. `associated`

VPC sekarang dikaitkan dengan grup keamanan.

Setelah Anda mengaitkan 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](#).

Putuskan grup keamanan dari VPC lain

Bagian ini menjelaskan cara menggunakan AWS Management Console dan AWS CLI untuk memisahkan grup keamanan dari VPCs. Anda mungkin ingin melakukan ini jika tujuan Anda adalah menghapus grup keamanan. Grup keamanan tidak dapat dihapus jika mereka terkait. Anda hanya dapat memisahkan grup keamanan jika tidak ada antarmuka jaringan di VPC terkait menggunakan grup keamanan tersebut.

AWS Management Console

Untuk memisahkan grup keamanan dari VPC

1. Buka konsol VPC Amazon 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 Putuskan VPC.
6. Di bawah ID VPC, pilih VPC untuk dipisahkan dari grup keamanan.
7. Pilih Putuskan VPC.
8. Lihat Status pemisahan di tab asosiasi VPC dan tunggu statusnya. `disassociated`

Command line

Untuk memisahkan grup keamanan dari VPC

1. Putuskan asosiasi VPC dengan. [disassociate-security-group-vpc](#)
2. Periksa status pemisahan VPC dengan [describe-security-group-vpc-asosiasi](#) dan tunggu statusnya. `disassociated`

VPC sekarang dipisahkan dengan kelompok keamanan.

Bagikan grup keamanan dengan AWS Organizations

Fitur Grup Keamanan Bersama memungkinkan Anda berbagi grup keamanan dengan akun AWS Organizations lain dalam AWS Wilayah 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 pengelolaan grup keamanan di seluruh akun di Organizations AWS Anda:

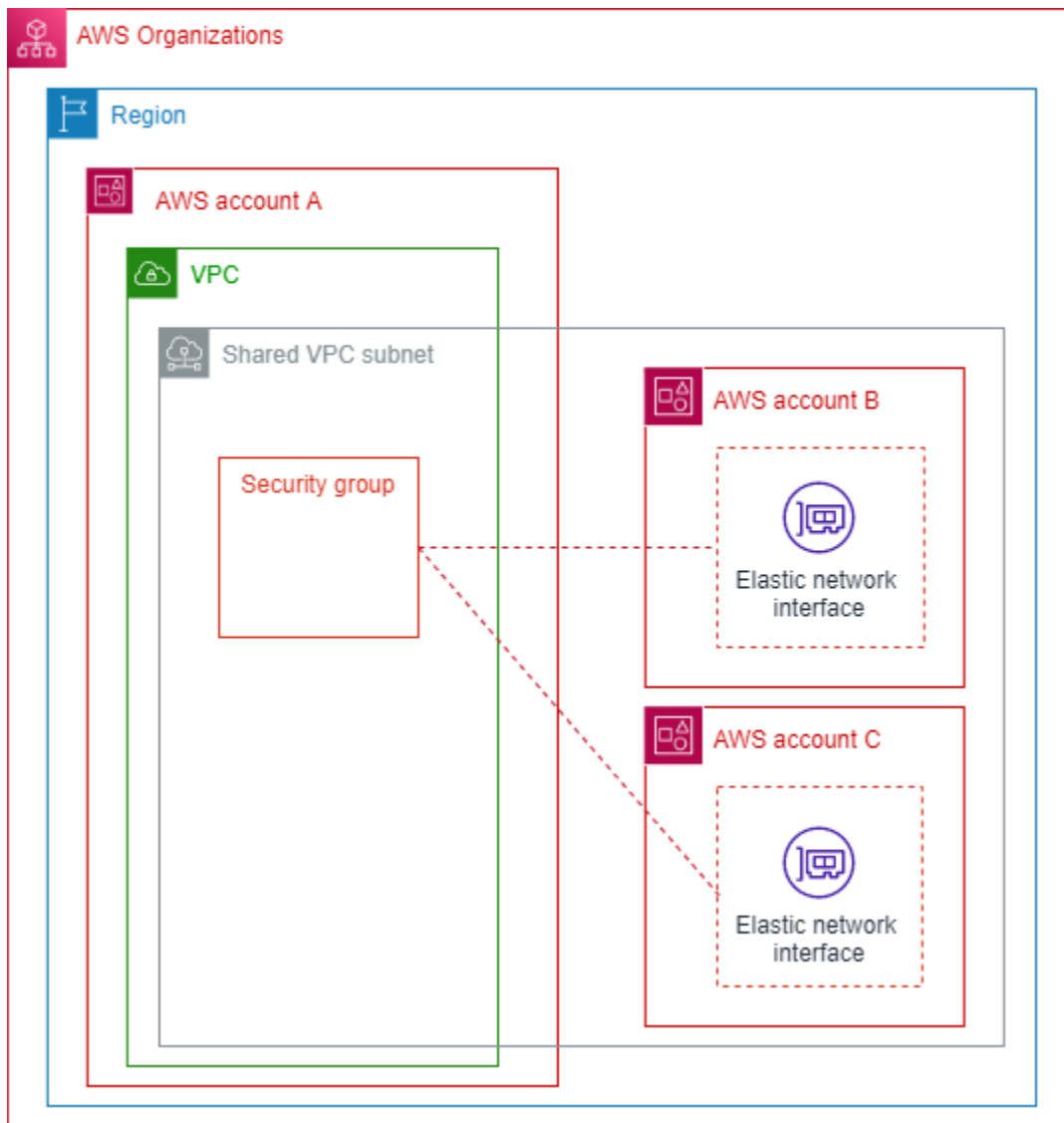


Diagram ini menunjukkan tiga akun yang merupakan bagian dari Organisasi yang sama. Akun A berbagi subnet VPC dengan Akun B dan C. Akun A berbagi grup keamanan dengan Akun B dan C menggunakan fitur Grup Keamanan Bersama. Akun B dan C kemudian menggunakan grup keamanan itu ketika mereka meluncurkan instance di subnet bersama. Ini memungkinkan Akun A untuk mengelola grup keamanan; pembaruan apa pun pada grup keamanan berlaku untuk sumber daya yang telah dijalankan Akun B dan C di subnet VPC bersama.

Persyaratan fitur Grup Keamanan Bersama

- Fitur ini hanya tersedia untuk akun di Organization in AWS Organizations yang sama. [Berbagi sumber daya](#) harus diaktifkan di AWS Organizations.
- 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 ada di VPC default.
- Akun peserta dapat membuat grup keamanan di VPC bersama tetapi mereka tidak dapat berbagi grup keamanan tersebut.
- Satu set izin minimum diperlukan untuk kepala sekolah IAM untuk berbagi grup keamanan dengan. AWS RAM Gunakan kebijakan IAM yang `AWSResourceAccessManagerFullAccess` dikelola `AmazonEC2FullAccess` dan 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 tindakan diperlukan. Ini adalah tindakan IAM khusus izin. Jika prinsipal IAM tidak memiliki izin ini diberikan, kesalahan akan terjadi ketika mencoba untuk 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
- Penyeimbang Beban Elastis
 - 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), minimum kuota 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 milik mereka, 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 mengasosiasikan hingga 4 grup. Dalam hal ini, kuota untuk ENI tersebut 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

Bagikan grup keamanan

Bagian ini menjelaskan cara menggunakan AWS Management Console dan berbagi grup keamanan dengan akun lain di Organisasi Anda. AWS CLI

AWS Management Console

Untuk berbagi grup keamanan

1. Buka konsol VPC Amazon 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 pembagian 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 oleh prinsipal untuk dilakukan dan pilih Berikutnya.
12. Di bawah Prinsipal - opsional, pilih Izinkan berbagi hanya dalam organisasi Anda.
13. Di bawah Prinsipal, pilih salah satu jenis utama berikut dan masukkan nomor yang sesuai:
 - AWS akun: Nomor akun di Organisasi Anda.
 - Organisasi: AWS Organizations ID.
 - 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 pembagian sumber daya ini.
 - Pengguna IAM: ARN dari pengguna IAM. Akun yang membuat pengguna harus menjadi anggota Organisasi yang sama dengan akun yang membuat pembagian sumber daya ini.
 - Prinsipal layanan: Anda tidak dapat berbagi grup keamanan dengan kepala layanan.
14. Pilih Tambahkan.
15. Pilih Berikutnya.
16. Pilih Buat berbagi sumber daya.
17. Di bawah Sumber daya bersama, tunggu untuk melihat StatusAssociated. Jika ada kegagalan asosiasi kelompok keamanan, itu mungkin karena salah satu batasan yang tercantum di atas. Lihat detail grup keamanan dan tab Berbagi di 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. AWS RAM Sumber daya Anda harus terlihat di sana. Jika tidak, pembuatan pembagian sumber daya mungkin gagal dan Anda mungkin perlu membuatnya kembali.

Command line

Untuk berbagi grup keamanan

1. Anda harus terlebih dahulu membuat pembagian 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 [get-resource-share-associations](#).

Kelompok keamanan sekarang dibagikan. Anda dapat memilih grup keamanan saat [meluncurkan EC2 instance](#) di subnet bersama dalam VPC yang sama.

Berhenti berbagi grup keamanan

Bagian ini menjelaskan cara menggunakan AWS Management Console dan AWS CLI menghentikan berbagi grup keamanan dengan akun lain di Organisasi Anda.

AWS Management Console

Untuk berhenti berbagi grup keamanan

1. Buka konsol VPC Amazon 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 Berhenti berbagi.
6. Pilih Ya, berhenti berbagi.

Command line

Untuk berhenti berbagi grup keamanan

Hapus berbagi sumber daya dengan [delete-resource-share](#).

Kelompok keamanan tidak lagi dibagikan. Setelah pemilik berhenti berbagi grup keamanan, aturan berikut berlaku:

- Peserta yang ada Elastic Network Interfaces (ENIs) terus mendapatkan pembaruan aturan grup keamanan apa pun yang dibuat untuk grup keamanan yang tidak dibagikan. Tidak berbagi hanya mencegah peserta membuat asosiasi baru dengan grup yang tidak dibagikan.

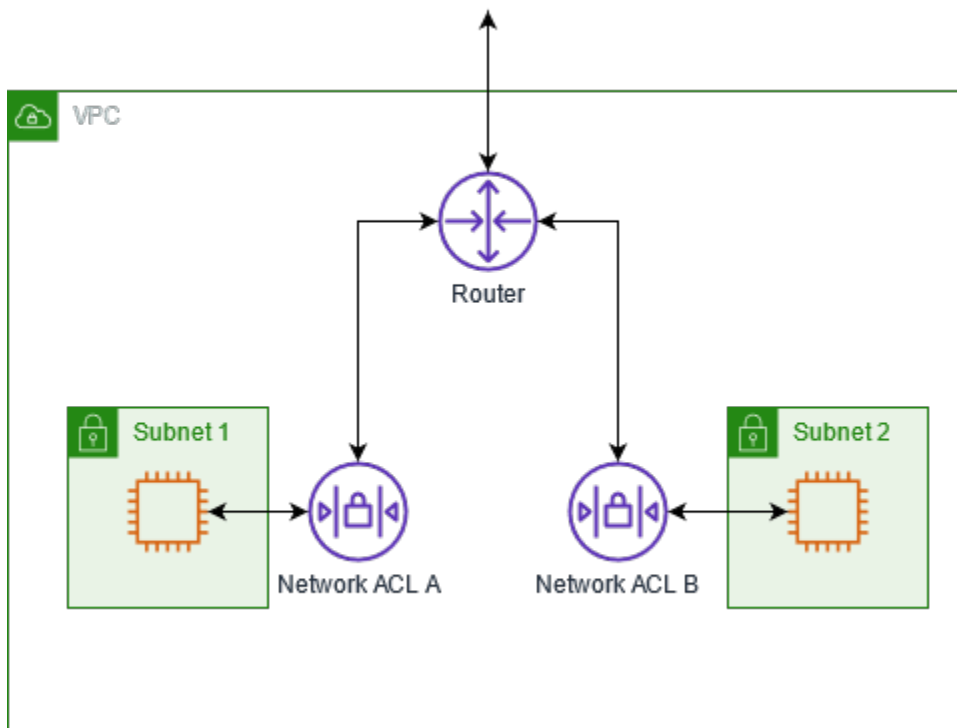
- Peserta tidak dapat lagi mengaitkan grup keamanan yang tidak dibagikan dengan yang ENIs mereka miliki.
- Peserta dapat mendeskripsikan dan menghapus ENIs yang masih terkait dengan grup keamanan yang tidak dibagikan.
- Jika peserta masih ENIs terkait dengan grup keamanan yang tidak dibagikan, pemilik tidak dapat menghapus grup keamanan yang tidak dibagikan. Pemilik hanya dapat menghapus grup keamanan setelah peserta memisahkan (menghapus) grup keamanan dari semua grup keamanan mereka ENIs.
- Peserta tidak dapat meluncurkan EC2 instans 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 untuk grup keamanan Anda untuk menambahkan lapisan keamanan tambahan ke VPC Anda.

Tidak ada biaya tambahan untuk menggunakan jaringan ACLs.

Diagram berikut menunjukkan VPC dengan dua subnet. Setiap subnet memiliki jaringan ACL. 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 yang ditujukan untuk subnet 1 yang diizinkan masuk ke subnet 1, dan lalu lintas mana yang ditujukan untuk lokasi di luar subnet 1 diizinkan untuk 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 jaringan ACLs, lihat [Bandingkan grup keamanan dan jaringan ACLs](#).

Daftar Isi

- [Dasar-dasar ACL jaringan](#)
- [Aturan ACL Jaringan](#)
- [ACL jaringan default untuk VPC](#)
- [Jaringan khusus ACLs untuk VPC Anda](#)
- [Jalur MTU Penemuan dan jaringan ACLs](#)
- [Membuat ACL jaringan untuk VPC anda](#)
- [Kelola asosiasi ACL jaringan untuk VPC Anda](#)
- [Hapus 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 jaringan ACLs 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 [kuota \(atau batasan\) 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 memasukkan aturan baru nanti, jika diperlukan.
- Kami mengevaluasi aturan ACL jaringan ketika lalu lintas masuk dan meninggalkan subnet, bukan karena dirutekan dalam subnet.
- NACLs tanpa kewarganegaraan, 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. Kelompok 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 suatu EC2 instans, respons secara otomatis diizinkan terlepas dari aturan grup keamanan keluar.

Batasan

- Ada kuota (juga dikenal sebagai batas) untuk jaringan ACLs. Untuk informasi selengkapnya, lihat [Jaringan ACLs](#).

- Jaringan tidak ACLs dapat memblokir permintaan DNS ke atau dari Resolver Route 53 (juga dikenal sebagai alamat IP VPC+2 atau DNS). AmazonProvided Untuk memfilter permintaan DNS melalui Resolver Route 53, Anda dapat mengaktifkan [Route 53 Resolver](#) DNS Firewall.
- Jaringan tidak ACLs dapat memblokir lalu lintas ke Layanan Metadata Instans (IMDS). Untuk mengelola akses ke IMDS, lihat [Mengonfigurasi opsi metadata instans](#) di Panduan Pengguna Amazon EC2 .
- Jaringan ACLs tidak memfilter lalu lintas yang ditujukan ke dan dari yang berikut ini:
 - Layanan Nama Domain Amazon (DNS)
 - Protokol Konfigurasi Host Dinamis (DHCP)
 - EC2 Metadata contoh Amazon
 - Titik akhir metadata tugas Amazon ECS
 - Aktivasi lisensi untuk instance Windows
 - Layanan Amazon Time Sync
 - Alamat IP cadangan yang digunakan oleh router VPC default

Aturan ACL Jaringan

Anda dapat menambah atau menghapus aturan dari ACL jaringan default, atau membuat jaringan tambahan ACLs 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).

- Izinkan/Tolak. Apakah mengizinkan atau menolak lalu lintas yang ditentukan.

Misalnya aturan, lihat [the section called “Contoh: Kontrol akses ke instans dalam subnet”](#).

Pertimbangan

- Ada kuota (juga dikenal sebagai batas) untuk jumlah aturan per jaringan ACLs. 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 Amazon EC2 API, rentang CIDR secara otomatis dimodifikasi 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 penolakan dalam situasi di mana Anda harus membuka berbagai port, tetapi ada port tertentu dalam kisaran yang ingin Anda tolak. Pastikan untuk memberikan aturan penolakan angka yang lebih rendah daripada aturan yang memungkinkan jangkauan lalu lintas pelabuhan yang lebih luas.
- Jika Anda menambahkan dan menghapus aturan dari ACL jaringan secara bersamaan, berhati-hatilah. Jika Anda menghapus aturan masuk atau keluar dan kemudian menambahkan lebih banyak entri baru daripada yang diizinkan (lihat [Kuota Amazon VPC](#), entri yang dipilih untuk dihapus akan dihapus dan entri baru tidak ditambahkan. 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 jaringan ACL juga mencakup aturan di mana nomor aturan adalah tanda bintang (*). Aturan-aturan ini memastikan bahwa jika sebuah 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 masuk default untuk ACL jaringan default. Aturan untuk IPv6 ditambahkan hanya jika Anda membuat VPC dengan blok CIDR terkait atau mengaitkan blok IPv6 IPv6 CIDR dengan VPC. Namun, jika Anda telah mengubah aturan masuk ACL jaringan default, kami tidak menambahkan aturan yang mengizinkan semua IPv6 lalu lintas masuk saat Anda mengaitkan IPv6 blok dengan VPC.

Aturan #	Jenis	Protokol	Rentang port	Sumber	Izinkan/Tolak
100	Semua IPv4 lalu lintas	Semua	Semua	0.0.0.0/0	IZINKAN
101	Semua IPv6 lalu lintas	Semua	Semua	::/0	IZINKAN
*	Semua Lalu lintas	Semua	Semua	0.0.0.0/0	MENOLAK
*	Semua IPv6 lalu lintas	Semua	Semua	::/0	TOLAK

Aturan keluar default

Tabel berikut menunjukkan aturan outbound default untuk ACL jaringan default. Aturan untuk IPv6 ditambahkan hanya jika Anda membuat VPC dengan blok CIDR terkait atau mengaitkan blok IPv6 IPv6 CIDR dengan VPC. Namun, jika Anda telah memodifikasi aturan keluar dari ACL jaringan default, kami tidak menambahkan aturan yang memungkinkan semua IPv6 lalu lintas keluar saat Anda mengaitkan IPv6 blok dengan VPC.

Aturan #	Jenis	Protokol	Rentang Port	Tujuan	Izinkan/Tolak
100	Semua Lalu lintas	Semua	Semua	0.0.0.0/0	IZINKAN
101	Semua IPv6 lalu lintas	Semua	Semua	::/0	IZINKAN
*	Semua Lalu lintas	Semua	Semua	0.0.0.0/0	MENOLAK

Aturan #	Jenis	Protokol	Rentang Port	Tujuan	Izinkan/Tolak
*	Semua IPv6 lalu lintas	Semua	Semua	::/0	TOLAK

Jaringan khusus ACLs 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 masuk default dan aturan keluar default yang nomor aturannya adalah tanda bintang (*). Aturan ini memastikan bahwa jika paket tidak cocok dengan aturan lainnya, 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. IPv4 Lalu IPv6 lintas dievaluasi secara terpisah. Oleh karena itu, tidak ada aturan untuk IPv4 lalu lintas yang berlaku untuk IPv6 lalu lintas. Anda dapat menambahkan IPv6 aturan di sebelah IPv4 aturan yang sesuai, atau menambahkan IPv6 aturan setelah IPv4 aturan terakhir.

Ketika sebuah paket datang ke subnet, kami mengevaluasinya terhadap aturan inbound ACL jaringan yang terkait dengan subnet, dimulai dengan aturan bernomor terendah. Misalnya, ada IPv4 lalu lintas 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 ditakdirkan untuk port 139 (NetBIOS), itu tidak akan cocok dengan salah satu aturan bernomor, sehingga aturan* untuk IPv4 lalu lintas pada akhirnya menyangkal paket tersebut.

Aturan #	Jenis	Protokol	Rentang port	Sumber	Izinkan/Tolak	Komentar
100	HTTP	TCP	80	0.0.0.0/0	IZINKAN	Mengizinkan lalu lintas HTTP masuk dari IPv4 alamat apa pun.
105	HTTP	TCP	80	::/0	IZINKAN	Mengizinkan lalu lintas HTTP masuk dari IPv6 alamat apa pun.
110	HTTPS	TCP	443	0.0.0.0/0	IZINKAN	Mengizinkan lalu lintas HTTPS masuk dari IPv4 alamat apa pun.
115	HTTPS	TCP	443	::/0	IZINKAN	Mengizinkan lalu lintas HTTPS masuk dari IPv6 alamat apa pun.
120	SSH	TCP	22	192.0.2.0/24	IZINKAN	Memungkinkan lalu lintas SSH masuk dari jangkauan IPv4 alamat publik jaringan rumah Anda (melalui gateway internet).
140	TCP Kustom	TCP	32768-65535	0.0.0.0/0	IZINKAN	Memungkinkan IPv4 lalu lintas pengembalian masuk dari internet (untuk permintaan yang berasal dari subnet).

Aturan #	Jenis	Protokol	Rentang port	Sumber	Izinkan/Tolak	Komentar
145	TCP Kustom	TCP	32768-65535	::/0	IZINKAN	Memungkinkan IPv6 lalu lintas pengembalian masuk dari internet (untuk permintaan yang berasal dari subnet).
*	Semua Lalu lintas	Semua	Semua	0.0.0.0/0	MENOLAK	Menyangkal semua IPv4 lalu lintas masuk yang belum ditangani oleh aturan sebelumnya (tidak dapat dimodifikasi).
*	Semua Lalu lintas	Semua	Semua	::/0	TOLAK	Menyangkal semua IPv6 lalu lintas masuk 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. IPv4 Lalu IPv6 lintas dievaluasi secara terpisah. Oleh karena itu, tidak ada aturan untuk IPv4 lalu lintas yang berlaku untuk IPv6 lalu lintas. Anda dapat menambahkan IPv6 aturan di sebelah IPv4 aturan yang sesuai, atau menambahkan IPv6 aturan setelah IPv4 aturan terakhir.

Aturan #	Jenis	Protokol	Rentang Port	Tujuan	Izinkan/Tolak	Komentar
100	HTTP	TCP	80	0.0.0.0/0	IZINKAN	Memungkinkan lalu lintas IPv4 HTTP

Aturan #	Jenis	Protokol	Rentang Port	Tujuan	Izinkan/Tolak	Komentar
						keluar dari subnet ke internet.
105	HTTP	TCP	80	::/0	IZINKAN	Memungkinkan lalu lintas IPv6 HTTP keluar dari subnet ke internet.
110	HTTPS	TCP	443	0.0.0.0/0	IZINKAN	Memungkinkan lalu lintas IPv4 HTTPS keluar dari subnet ke internet.
115	HTTPS	TCP	443	::/0	IZINKAN	Memungkinkan lalu lintas IPv6 HTTPS keluar dari subnet ke internet.
120	TCP Kustom	TCP	1024-65535	192.0.2.0/24	IZINKAN	Memungkinkan respons keluar untuk lalu lintas SSH dari jaringan rumah Anda.
140	TCP Kustom	TCP	32768-65535	0.0.0.0/0	IZINKAN	Memungkinkan IPv4 tanggapan keluar ke klien di internet (misalnya, melayani halaman web).
145	TCP Kustom	TCP	32768-65535	::/0	IZINKAN	Memungkinkan IPv6 tanggapan keluar ke klien di internet (misalnya, melayani halaman web).

Aturan #	Jenis	Protokol	Rentang Port	Tujuan	Izinkan/Tolak	Komentar
*	Semua Lalu lintas	Semua	Semua	0.0.0.0/0	MENOLAK	Menyangkal semua IPv4 lalu lintas keluar yang belum ditangani oleh aturan sebelumnya.
*	Semua Lalu lintas	Semua	Semua	::/0	TOLAK	Menyangkal semua IPv6 lalu lintas 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 jaringan Anda ACLs tergantung pada jenis klien yang Anda gunakan atau dengan mana Anda berkomunikasi.

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 instance.

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.

Jaringan khusus ACLs dan AWS layanan lainnya

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, lihat berikut ini:

- [Jaringan ACLs untuk Application Load Balancer Anda](#)
- [Jaringan ACLs untuk Network Load Balancer Anda](#)
- [Jaringan ACLs untuk Classic Load Balancer Anda](#)

Memecahkan masalah jangkauan

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 hop-by-hop menghasilkan rincian 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 konfigurasi.

Untuk informasi selengkapnya, lihat Panduan [Reachability Analyzer](#).

Jalur MTU Penemuan dan jaringan ACLs

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.

Sebab IPv4, ketika host mengirim paket yang lebih besar dari MTU host penerima atau yang lebih besar dari MTU perangkat di sepanjang jalur, host penerima atau perangkat menjatuhkan paket, dan 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 mentransmisikannya kembali.

IPv6 Protokol tidak mendukung fragmentasi dalam jaringan. Jika suatu host mengirimkan paket yang lebih besar daripada MTU host penerima atau yang lebih besar daripada MTU perangkat di sepanjang jalur, host atau perangkat penerima menjatuhkan paket, lalu 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 mentransmisikannya 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 EC2 instans Anda](#) di Panduan EC2 Pengguna Amazon.

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: Kaitkan subnet dengan ACL jaringan](#)
- [\(Opsional\) Kelola jaringan ACLs menggunakan Firewall Manager](#)

Langkah 1: Buat ACL jaringan

Anda dapat membuat ACL jaringan kustom untuk VPC Anda. Aturan awal untuk jaringan khusus ACL 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 VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Jaringan ACLs.
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 Tambahkan tag lalu masukkan kunci tag dan nilai tag.
7. Pilih Buat ACL jaringan.

Untuk membuat jaringan ACL 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 Amazon EC2 API 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 VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Jaringan ACLs.
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 Kustom untuk jenis 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 Kustom untuk jenis 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-EC2NetworkAcEntry](#) (AWS Tools for Windows PowerShell)

Untuk mengganti aturan dalam jaringan ACL menggunakan baris perintah

- [replace-network-acl-entry](#) (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: Kaitkan 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 VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Jaringan ACLs, lalu 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) Kelola jaringan ACLs menggunakan Firewall Manager

AWS Firewall Manager menyederhanakan administrasi ACL jaringan dan tugas pemeliharaan 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 Manajer Firewall, menggunakan satu akun administrator, Anda dapat mengonfigurasi, memantau, dan mengelola kumpulan aturan minimum yang ingin Anda tetapkan di jaringan ACLs yang Anda gunakan di seluruh organisasi. Anda menentukan akun dan subnet di organisasi Anda yang berada dalam cakupan kebijakan Firewall Manager. Firewall

Manager melaporkan status kepatuhan jaringan ACLs untuk subnet dalam lingkup, dan Anda dapat mengonfigurasi Firewall Manager untuk mengotomatiskan remediasi jaringan yang tidak sesuai. ACLs

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 terkait 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](#)
- [Ubah subnet yang terkait dengan ACL jaringan](#)
- [Ubah ACL jaringan yang terkait dengan subnet](#)

Jelaskan asosiasi ACL jaringan Anda

Anda dapat menggambarkan jaringan ACL yang terkait dengan subnet dan Anda juga dapat menjelaskan subnet mana yang terkait dengan jaringan ACL.

Untuk menggambarkan ACL jaringan yang terkait dengan subnet menggunakan konsol

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Pengguna.
3. Pilih subnet.
4. Pilih tab Network ACL.

Untuk menggambarkan ACL jaringan yang terkait dengan subnet menggunakan AWS CLI

Gunakan [describe-network-acls](#) perintah berikut untuk daftar 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 menggambarkan subnet yang terkait dengan jaringan ACL menggunakan konsol

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Jaringan ACLs.
3. Pilih ACL jaringan.
4. Pilih tab Asosiasi Subnet.

Untuk menggambarkan subnet yang terkait dengan jaringan ACL menggunakan AWS CLI

Gunakan [describe-network-acls](#) perintah berikut untuk daftar subnet yang terkait dengan ACL jaringan yang ditentukan.

```
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"  
]
```

Ubah subnet yang terkait dengan ACL jaringan

Anda dapat melepaskan ACL jaringan dari subnet. Setelah Anda memisahkan subnet dari ACL jaringan kustom, kami secara otomatis mengaitkannya dengan ACL jaringan default untuk VPC. Perubahan berlaku setelah periode waktu yang singkat.

Untuk mengubah subnet yang terkait dengan jaringan ACL

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Jaringan ACLs.
3. Pilih ACL jaringan.
4. Pilih Tindakan, Edit asosiasi subnet.
5. Hapus subnet dari subnet yang dipilih.
6. Pilih Simpan perubahan.

Ubah ACL jaringan yang terkait dengan subnet

Anda dapat mengubah ACL jaringan yang terkait dengan suatu subnet. Misalnya, ketika Anda membuat subnet, 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 beberapa 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 VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Pengguna.
3. Pilih subnet.
4. Pilih Tindakan, Edit asosiasi ACL jaringan.
5. Untuk ID ACL Jaringan, pilih ACL jaringan yang akan dikaitkan 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)

Hapus ACL jaringan untuk VPC Anda

Setelah 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 VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Jaringan ACLs. Kolom Terkait dengan menunjukkan jumlah subnet yang terkait dengan setiap jaringan ACL. Kolom ini - jika tidak ada subnet terkait.
3. Pilih ACL jaringan.
4. Pilih Tindakan, Edit asosiasi subnet.
5. Hapus asosiasi subnet.
6. Pilih Simpan perubahan.

Untuk menggambarkan jaringan Anda ACLs, 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 VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Jaringan ACLs.

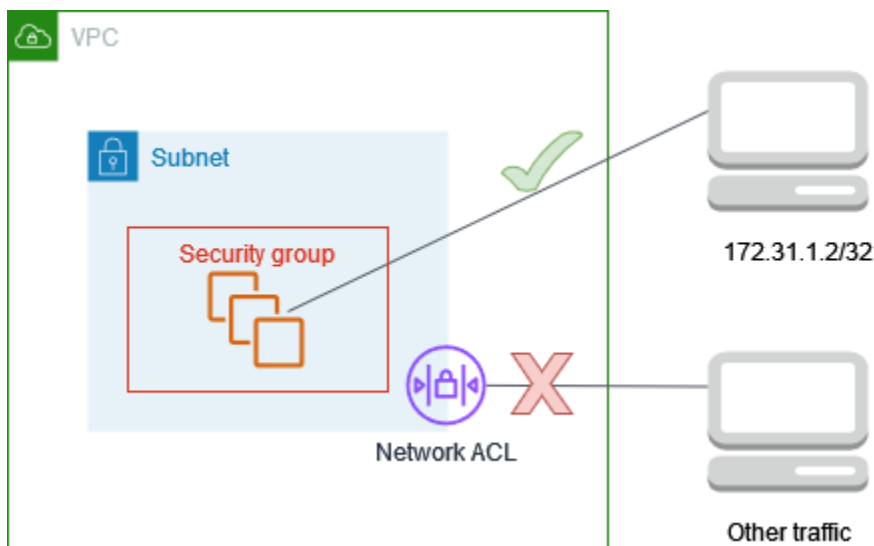
3. Pilih ACL jaringan.
4. Pilih Tindakan, Hapus jaringan ACLs.
5. Saat diminta konfirmasi, masukkan **delete**, lalu pilih Hapus.

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, contoh di subnet dapat berkomunikasi satu sama lain, dan dapat diakses dari komputer jarak jauh tepercaya untuk melakukan tugas-tugas administratif. Komputer jarak jauh mungkin 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 instance Anda sambil mengandalkan ACL jaringan sebagai lapisan pertahanan cadangan. Misalnya, jika Anda secara tidak sengaja memperbarui grup keamanan untuk memungkinkan akses SSH masuk dari mana saja, tetapi ACL jaringan hanya mengizinkan akses dari rentang alamat IP komputer jarak jauh, maka jaringan ACL 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 #	Jenis	Protokol	Rentang port	Sumber	Izinkan/Tolak	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	MENOLAK	Tolak semua lalu lintas masuk lainnya.

Berikut ini adalah contoh aturan outbound untuk ACL jaringan yang terkait dengan subnet. Jaringan ACLs tidak memiliki kewarganegaraan. Oleh karena itu, Anda harus menyertakan aturan yang memungkinkan tanggapan terhadap lalu lintas masuk.

Aturan #	Jenis	Protokol	Rentang Port	Tujuan	Izinkan/Tolak	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	TOLAK	Menolak semua lalu lintas

Aturan #	Jenis	Protokol	Rentang Port	Tujuan	Izinkan/Tolak	Komentar
						keluar lainnya.

Aturan-aturan grup keamanan

Berikut ini adalah contoh aturan masuk untuk grup keamanan yang terkait dengan instans. Aturan ini berlaku untuk semua instance yang terkait dengan grup keamanan. Seorang pengguna dengan kunci pribadi untuk key pair 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	<i>sg-1234567890abcde f0</i>	Izinkan komunikasi antara instans yang terkait dengan grup keamanan ini.
SSH	TCP	22	<i>172.31.1.2/32</i>	Izinkan akses SSH masuk dari komputer jarak jauh.

Berikut ini adalah contoh aturan outbound bound 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	<i>sg-1234567890abcde f0</i>	Izinkan komunikasi antara instans

Jenis protokol	Protokol	Rentang Port	Tujuan	Komentar
				yang terkait dengan grup keamanan ini.

Perbedaan antara jaringan ACLs dan kelompok keamanan

Tabel berikut merangkum perbedaan dasar antara jaringan ACLs dan kelompok keamanan.

Karakteristik	ACL jaringan	Grup keamanan
Tingkat operasi	Tingkat subnet	Tingkat instans
Cakupan	Berlaku untuk semua instance di subnet terkait	Berlaku untuk semua instance yang terkait dengan grup keamanan
Jenis aturan	Izinkan dan tolak aturan	Izinkan aturan saja
Evaluasi aturan	Mengevaluasi aturan dalam urutan menaik sampai kecocokan untuk lalu lintas ditemukan	Mengevaluasi semua aturan sebelum memutuskan apakah akan mengizinkan lalu lintas
Kembalikan 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 Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone 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. Availability

Zone ini terhubung melalui 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 Availability Zone dalam suatu 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 yang sangat penting dan memungkinkan organisasi untuk membangun solusi cloud-native yang tangguh.

Selain itu, skala dan jangkauan global AWS infrastruktur memberdayakan pelanggan untuk menyebarkan 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 disyaratkan oleh kebutuhan regulasi dan bisnis spesifik mereka.

Dengan memanfaatkan infrastruktur AWS global, organisasi dapat merancang lingkungan cloud mereka agar sangat tersedia, toleran terhadap kesalahan, dan skalabel, dengan fleksibilitas untuk beradaptasi dengan perubahan persyaratan dan kebutuhan bisnis yang berkembang. Fondasi yang kuat ini adalah enabler kunci untuk keberhasilan implementasi aplikasi dan layanan berbasis cloud modern.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat [Infrastruktur AWS Global](#).

Anda dapat mengonfigurasi VPCs untuk memenuhi persyaratan ketahanan untuk beban kerja Anda. Untuk informasi selengkapnya, lihat berikut ini:

- [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)

Validasi kepatuhan untuk Amazon Virtual Private Cloud

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat [Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS](#) dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat [Program AWS Kepatuhan Program AWS](#).

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. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- [Kepatuhan dan Tata Kelola Keamanan](#) – Panduan implementasi solusi ini membahas pertimbangan arsitektur serta memberikan langkah-langkah untuk menerapkan fitur keamanan dan kepatuhan.
- [Referensi Layanan yang Memenuhi Syarat HIPAA](#) — Daftar layanan yang memenuhi syarat HIPAA. Tidak semua memenuhi Layanan AWS syarat HIPAA.
- [AWS Sumber Daya AWS](#) — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- [AWS Panduan Kepatuhan Pelanggan](#) - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- [Mengevaluasi Sumber Daya dengan Aturan](#) dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- [AWS Security Hub](#)— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat [Referensi kontrol Security Hub](#).
- [Amazon GuardDuty](#) — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan,

seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.

- [AWS Audit Manager](#)Ini Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Memblokir akses publik ke VPCs dan subnet

VPC Block Public Access (BPA) adalah fitur keamanan terpusat yang memungkinkan Anda untuk secara otoritatif mencegah akses internet publik ke sumber daya VPC di seluruh AWS akun, memastikan kepatuhan terhadap persyaratan keamanan sambil memberikan fleksibilitas untuk pengecualian dan kemampuan audit tertentu.

Fitur VPC BPA memiliki mode berikut:

- Dua arah: Semua lalu lintas ke dan dari gateway internet dan gateway internet khusus pintu masuk di Wilayah ini (kecuali untuk dikecualikan dan subnet) diblokir. VPCs
- Ingress-only: Semua lalu lintas internet ke VPCs dalam Wilayah ini (kecuali untuk VPCs atau subnet yang dikecualikan) diblokir. Hanya lalu lintas ke dan dari gateway NAT dan gateway internet khusus egress yang diizinkan karena gateway ini hanya memungkinkan koneksi keluar 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 mengecualikannya dari mode VPC BPA akun dan akan memungkinkan akses dua arah atau egress-only.

Pengecualian dapat memiliki salah satu dari mode berikut:

- Dua arah: Semua lalu lintas internet ke dan dari yang dikecualikan VPCs dan subnet diperbolehkan.
- Egress-only: Lalu lintas internet keluar dari yang dikecualikan VPCs dan subnet diizinkan. Lalu lintas internet masuk ke yang dikecualikan VPCs dan subnet diblokir. Ini hanya berlaku ketika VPC BPA disetel 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 dan dukungan layanan](#)
- [Batasan VPC BPA](#)
- [Kontrol akses ke VPC BPA dengan kebijakan IAM](#)
- [Aktifkan mode dua arah VPC BPA untuk akun Anda](#)
- [Ubah mode BPA VPC menjadi hanya masuk](#)
- [Membuat dan menghapus pengecualian](#)
- [Aktifkan BPA VPC di tingkat Organisasi](#)

Ketersediaan wilayah

VPC BPA tersedia di semua [AWS Wilayah komersial termasuk dan Wilayah](#) GovCloud Tiongkok.

Dalam panduan ini, Anda juga akan menemukan informasi tentang penggunaan 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 Batasan dalam Panduan dan Pertimbangan Penganalisis Akses Jaringan dalam Panduan Reachability Analyzer.](#)

AWS dampak dan dukungan layanan

Sumber daya dan layanan berikut mendukung VPC BPA dan lalu lintas ke layanan dan sumber daya ini dipengaruhi oleh VPC BPA:

- Internet gateway: Semua lalu lintas masuk dan keluar diblokir.
- Gateway internet khusus Egress: Semua lalu lintas keluar diblokir. Gateway internet khusus Egress tidak mengizinkan lalu lintas masuk.

- Gateway Load Balancer (GWLB): Semua lalu lintas masuk dan keluar diblokir meskipun subnet yang berisi titik akhir GWLB dikecualikan.
- Gateway NAT: Semua lalu lintas masuk dan keluar diblokir. Gateway NAT membutuhkan gateway internet untuk konektivitas internet.
- Network Load Balancer yang menghadap ke Internet: Semua lalu lintas masuk dan keluar diblokir. Network Load Balancer yang menghadap ke internet memerlukan gateway internet untuk konektivitas internet.
- Application Load Balancer yang menghadap ke Internet: Semua lalu lintas masuk dan keluar diblokir. Application Load Balancer yang menghadap ke Internet memerlukan gateway internet untuk konektivitas internet.
- Amazon CloudFront VPC Origins: Semua lalu lintas masuk dan keluar diblokir.
- AWS Direct Connect: Semua lalu lintas masuk dan keluar yang menggunakan antarmuka virtual publik (IPv6 alamat unicast publik IPv4 atau global) diblokir. Lalu lintas ini menggunakan gateway internet (atau egress-only internet-gateway) untuk konektivitas.
- AWS Akselerator Global: Lalu lintas masuk ke VPCs diblokir, terlepas dari apakah target tersebut dapat diakses dari internet atau tidak.
- AWS Network Firewall: Semua lalu lintas masuk dan keluar diblokir bahkan jika 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 dipengaruhi oleh VPC BPA:

- 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 EC2 instance di subnet, saat menggunakan VPC BPA, subnet tersebut harus menjadi pengecualian agar lalu lintas mengalir masuk dan keluar darinya. Subnet lain yang mengirimkan lalu lintas ke subnet alat dan bukan ke gateway internet tidak perlu ditambahkan sebagai pengecualian.
- Lalu lintas yang dikirim secara pribadi dari sumber daya di VPC Anda ke layanan lain yang berjalan di VPC Anda, seperti EC2 DNS Resolver atau Amazon OpenSearch Service, diizinkan bahkan ketika VPC BPA dihidupkan karena tidak melewati gateway internet di VPC Anda. Ada kemungkinan bahwa layanan ini dapat mengajukan 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.

Batasan VPC BPA

Mode khusus masuk VPC BPA tidak didukung di Local Zones (LZs) di mana gateway NAT dan gateway internet khusus pintu masuk tidak diizinkan.

Kontrol akses ke VPC BPA dengan kebijakan IAM

Untuk contoh kebijakan IAM yang allow/deny mengakses fitur BPA VPC, lihat. [Memblokir akses publik ke VPCs 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 jalan keluar di Wilayah ini (kecuali untuk dikecualikan dan subnet). VPCs Untuk informasi selengkapnya tentang pengecualian, lihat [Membuat dan menghapus pengecualian](#).

Important

Kami sangat menyarankan agar Anda meninjau secara menyeluruh beban kerja yang memerlukan akses Internet sebelum mengaktifkan VPC BPA di akun produksi Anda.

 Note

- Untuk mengaktifkan VPC BPA pada VPCs dan subnet di akun Anda, Anda harus memiliki dan subnet. VPCs
- 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.

AWS Management Console

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi kiri, pilih Pengaturan.
3. Pilih Edit pengaturan akses publik.
4. Pilih Aktifkan blokir akses publik dan dua arah, lalu pilih Simpan perubahan.
5. Tunggu Status berubah menjadi On. Mungkin perlu beberapa menit agar pengaturan VPC BPA berlaku dan statusnya diperbarui.

Mode dua arah VPC BPA sekarang aktif.

AWS CLI

1. Aktifkan 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 statusnya diperbarui.

2. Lihat status VPC BPA:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

Ubah mode BPA VPC menjadi hanya masuk

Mode hanya masuk VPC BPA memblokir semua lalu lintas internet ke VPCs dalam Wilayah ini (kecuali untuk VPCs atau subnet yang dikecualikan). Hanya lalu lintas ke dan dari gateway NAT dan

gateway internet khusus egress yang diizinkan karena gateway ini hanya memungkinkan koneksi keluar dibuat.

AWS Management Console

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi kiri, pilih Pengaturan.
3. Pilih Edit pengaturan akses publik.
4. Ubah arah ke Ingress-only.
5. Simpan perubahan dan tunggu statusnya diperbarui. Mungkin perlu beberapa menit agar pengaturan VPC BPA berlaku dan statusnya 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 statusnya 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 mengecualikannya dari mode BPA VPC akun dan akan memungkinkan akses dua arah atau egress-only. Anda dapat membuat pengecualian BPA VPC untuk VPCs dan subnet bahkan ketika VPC BPA tidak diaktifkan pada akun untuk memastikan bahwa tidak ada gangguan lalu lintas ke pengecualian ketika VPC BPA dihidupkan. 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](#)

AWS Management Console

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi kiri, pilih Pengaturan.
3. Di tab Blokir akses publik, di bawah Pengecualian, lakukan salah satu hal berikut:
 - Untuk menghapus pengecualian, pilih pengecualian dan kemudian pilih Tindakan > Hapus 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 yang dikecualikan VPCs dan subnet.
 - Egress-only: Memungkinkan lalu lintas internet keluar dari yang dikecualikan dan subnet. VPCs Memblokir lalu lintas internet masuk ke yang dikecualikan VPCs dan subnet. Pengaturan ini berlaku ketika VPC BPA diatur 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 perubahannya.

Pengecualian telah dibuat.

AWS CLI

1. Ubah arah izin pengecualian:

```
aws ec2 --region us-east-2 create-vpc-block-public-access-exclusion --subnet-id subnet-id --internet-gateway-exclusion-mode allow-bidirectional
```

2. Diperlukan 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 BPA VPC di tingkat Organisasi

Jika Anda menggunakan AWS Organizations untuk mengelola akun di organisasi, Anda dapat menggunakan [kebijakan deklaratif AWS Organizations untuk menerapkan](#) BPA VPC pada akun di organisasi. Untuk informasi selengkapnya tentang kebijakan deklaratif VPC BPA, lihat Kebijakan deklaratif yang [didukung di Panduan Pengguna Organizations](#).AWS

Note

- Anda dapat menggunakan kebijakan deklaratif VPC BPA untuk mengonfigurasi jika 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 Blokir pengaturan akses publik, Anda akan melihat Dikelola oleh Kebijakan Deklaratif dan Anda tidak akan dapat mengubah pengaturan 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 dengan Network Access Analyzer](#)
- [Pantau dampak VPC BPA dengan log aliran](#)
- [Lacak penghapusan pengecualian dengan CloudTrail](#)
- [Verifikasi konektivitas diblokir dengan Reachability Analyzer](#)

Menilai 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 sebelum Anda mengaktifkan VPC BPA dan memblokir

akses. Gunakan analisis ini untuk memahami dampak 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 dampak potensial VPC BPA pada lalu lintas keluar gateway internet khusus egres. IPv6
- Anda dikenakan biaya untuk analisis yang Anda lakukan dengan Network Access Analyzer. Untuk informasi selengkapnya, lihat [Harga](#) di Network Access Analyzer Panduan.
- Untuk informasi tentang ketersediaan regional Network Access Analyzer, lihat [Batasan](#) dalam Panduan Penganalisis Akses Jaringan.

AWS Management Console

1. Buka konsol AWS Network Insights di <https://console.aws.amazon.com/networkinsights/>.
2. Pilih Network Access Analyzer.
3. Pilih Buat Lingkup Akses Jaringan.
4. Pilih Menilai dampak VPC Blokir Akses Publik dan pilih Berikutnya.
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 subnet VPCs dan atau yang muncul dalam temuan ini dikonfigurasi sebagai pengecualian VPC BPA, lalu lintas ke subnet tersebut dan subnet akan dibatasi. VPCs
11. Analisis setiap temuan untuk memahami dampak VPC BPA pada sumber daya di Anda. VPCs

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 ruang 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 akun Anda. VPCs Hasilnya diatur sebagai “temuan”. FindingId:” AnalysisFinding -1” menunjukkan bahwa ini adalah temuan pertama dalam analisis. Perhatikan bahwa ada beberapa temuan dan masing-masing menunjukkan arus lalu lintas yang akan terpengaruh dengan menyalakan 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 sebuah instance (“ SequenceNumber “: 4).

4. Analisis temuan untuk memahami dampak VPC BPA pada sumber daya di Anda. VPCs

Analisis dampak selesai.

Pantau dampak VPC BPA dengan log aliran

VPC Flow Logs adalah fitur yang memungkinkan Anda menangkap informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan Elastis 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 di [Bekerja dengan log alur](#)

Saat Anda membuat log alur, pastikan Anda menggunakan format kustom yang menyertakan bidang `reject-reason`.

Saat Anda melihat log aliran, jika lalu lintas ke ENI ditolak karena VPC BPA, Anda akan melihat `reject-reason` entri BPA log aliran.

Selain [batasan](#) standar untuk log aliran VPC, perhatikan batasan berikut khusus untuk VPC BPA:

- [Log aliran untuk VPC BPA tidak termasuk catatan yang dilewati](#).
- Log aliran untuk VPC BPA tidak termasuk [bytes](#) bahkan jika Anda menyertakan `bytes` bidang dalam log aliran Anda.

Lacak penghapusan pengecualian dengan CloudTrail

Bagian ini menjelaskan bagaimana Anda dapat menggunakan AWS CloudTrail untuk memantau dan melacak penghapusan pengecualian VPC BPA.

AWS Management Console

Anda dapat melihat pengecualian yang dihapus dalam riwayat CloudTrail Acara dengan mencari Jenis sumber daya > `AWS::EC2::VPCLockPublicAccessExclusion` di AWS CloudTrail konsol di <https://console.aws.amazon.com/cloudtrailv2/>.

AWS CLI

Anda dapat menggunakan `lookup-events` perintah untuk melihat peristiwa yang terkait dengan penghapusan pengecualian:

```
aws cloudtrail lookup-events --lookup-attributes
AttributeKey=ResourceType,AttributeValue=AWS::EC2::VPCLockPublicAccessExclusion
```

Verifikasi konektivitas diblokir dengan Reachability Analyzer

[VPC Reachability Analyzer](#) dapat digunakan untuk mengevaluasi apakah jalur jaringan tertentu dapat dicapai mengingat konfigurasi jaringan Anda, termasuk pengaturan VPC BPA.

Untuk informasi tentang ketersediaan regional Reachability Analyzer, lihat [Pertimbangan](#) dalam Panduan Reachability Analyzer.

AWS Management Console

1. Buka konsol AWS Network Insights di <https://console.aws.amazon.com/networkinsights/home#ReachabilityAnalyzer>.
2. Klik Buat dan analisis jalur.
3. Untuk Jenis Sumber, pilih Internet Gateways dan pilih gateway internet yang ingin Anda blokir lalu lintas dari dropdown Sumber.
4. Untuk Jenis Tujuan, pilih Instans dan pilih instance yang ingin Anda blokir lalu lintas dari dropdown Tujuan.
5. Klik Buat dan analisis jalur.
6. Tunggu analisis selesai. Ini bisa memakan waktu beberapa menit.
7. Setelah selesai, Anda akan melihat bahwa Status Reachability Tidak dapat dijangkau dan detail Path menunjukkan bahwa VPC_BLOCK_PUBLIC_ACCESS_ENABLED adalah penyebab masalah jangkauan ini.

AWS CLI

1. Buat jalur jaringan menggunakan ID Internet Gateway yang ingin Anda blokir lalu lintas (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 bahwa VPC_BLOCK_PUBLIC_ACCESS_ENABLED 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-langkahnya secara berurutan.

Important

Jangan melalui contoh ini di akun produksi. Kami sangat menyarankan agar Anda meninjau secara menyeluruh beban kerja yang memerlukan akses Internet sebelum mengaktifkan VPC BPA di akun produksi Anda.

Note

Untuk sepenuhnya memahami fitur VPC BPA, Anda memerlukan sumber daya tertentu di akun Anda. Di bagian ini, kami menyediakan AWS CloudFormation templat yang dapat Anda gunakan untuk menyediakan sumber daya yang Anda butuhkan untuk sepenuhnya memahami cara kerja fitur ini. Ada biaya yang terkait dengan sumber daya yang Anda berikan 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 selesai dengan contoh ini.

Daftar Isi

- [Menyebarkan CloudFormation template \(opsional\)](#)
- [Lihat dampak VPC BPA dengan Network Access Analyzer](#)
- [Skenario 1 - Connect ke instance tanpa VPC BPA diaktifkan](#)
- [Skenario 2 - Nyalakan 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 - Memodifikasi mode VPC BPA](#)
- [Pembersihan](#)

Menyebarkan CloudFormation template (opsional)

Untuk mendemonstrasikan cara kerja fitur ini, Anda memerlukan VPC, subnet, instance, dan sumber daya lainnya. Untuk membuatnya lebih mudah untuk menyelesaikan demonstrasi ini, kami telah menyediakan AWS 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 hanya 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 IPv4 alamat publik. Untuk menghindari kelebihan biaya, pastikan Anda menyelesaikan langkah-langkah Pembersihan untuk menghapus semua sumber daya yang dibuat untuk tujuan contoh ini.
- CloudFormation Template ini menciptakan 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:

- Gateway internet khusus egress
- gateway internet
- Gateway NAT
- Dua subnet publik
- Satu subnet pribadi
- Dua EC2 contoh dengan alamat publik dan pribadi IPv4
- Satu EC2 contoh dengan IPv6 alamat dan IPv4 alamat pribadi
- Satu EC2 contoh dengan IPv4 alamat pribadi saja
- Grup keamanan dengan lalu lintas masuk SSH dan ICMP diizinkan dan SEMUA lalu lintas keluar diizinkan
- Log aliran VPC
- Titik akhir One EC2 Instance 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 Amazon 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**VPCBPAPFlowLogRole:**

```
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
```

VPCBPAPFlowLogPolicy:

```
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
```

AWS Management Console

1. Buka AWS CloudFormation konsol di <https://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 bagi Anda untuk pembuatan log alur dan izin untuk Amazon 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 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 mengaktifkan VPC BPA di akun Anda dan memblokir lalu lintas.

Untuk informasi tentang ketersediaan regional Network Access Analyzer, lihat [Batasan](#) dalam Panduan Penganalisis Akses Jaringan.

AWS Management Console

1. Buka konsol AWS Network Insights di <https://console.aws.amazon.com/networkinsights/>.
2. Pilih Network Access Analyzer.
3. Pilih Buat Lingkup Akses Jaringan.
4. Pilih Menilai dampak VPC Blokir Akses Publik dan pilih Berikutnya.
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 subnet VPCs dan atau yang muncul dalam temuan ini dikonfigurasi sebagai pengecualian VPC BPA, lalu lintas ke subnet tersebut dan subnet akan dibatasi. VPCs
11. Analisis setiap temuan untuk memahami dampak VPC BPA pada sumber daya di Anda. VPCs

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 ruang 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-035d235a762eed04",
        "Arn": "arn:aws:ec2:us-east-2:470889052923:subnet/subnet-035d235a762eed04",
        "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":
"eyJ0ZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxfgQ=="
}

```

Hasilnya menunjukkan lalu lintas ke dan dari gateway internet di semua akun Anda. VPCs Hasilnya diatur sebagai “temuan”. FindingId: " AnalysisFinding -1" menunjukkan bahwa ini adalah temuan pertama dalam analisis. Perhatikan bahwa ada beberapa temuan dan masing-masing menunjukkan arus lalu lintas yang akan terpengaruh dengan menyalakan 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 sebuah instance (" SequenceNumber ": 4).

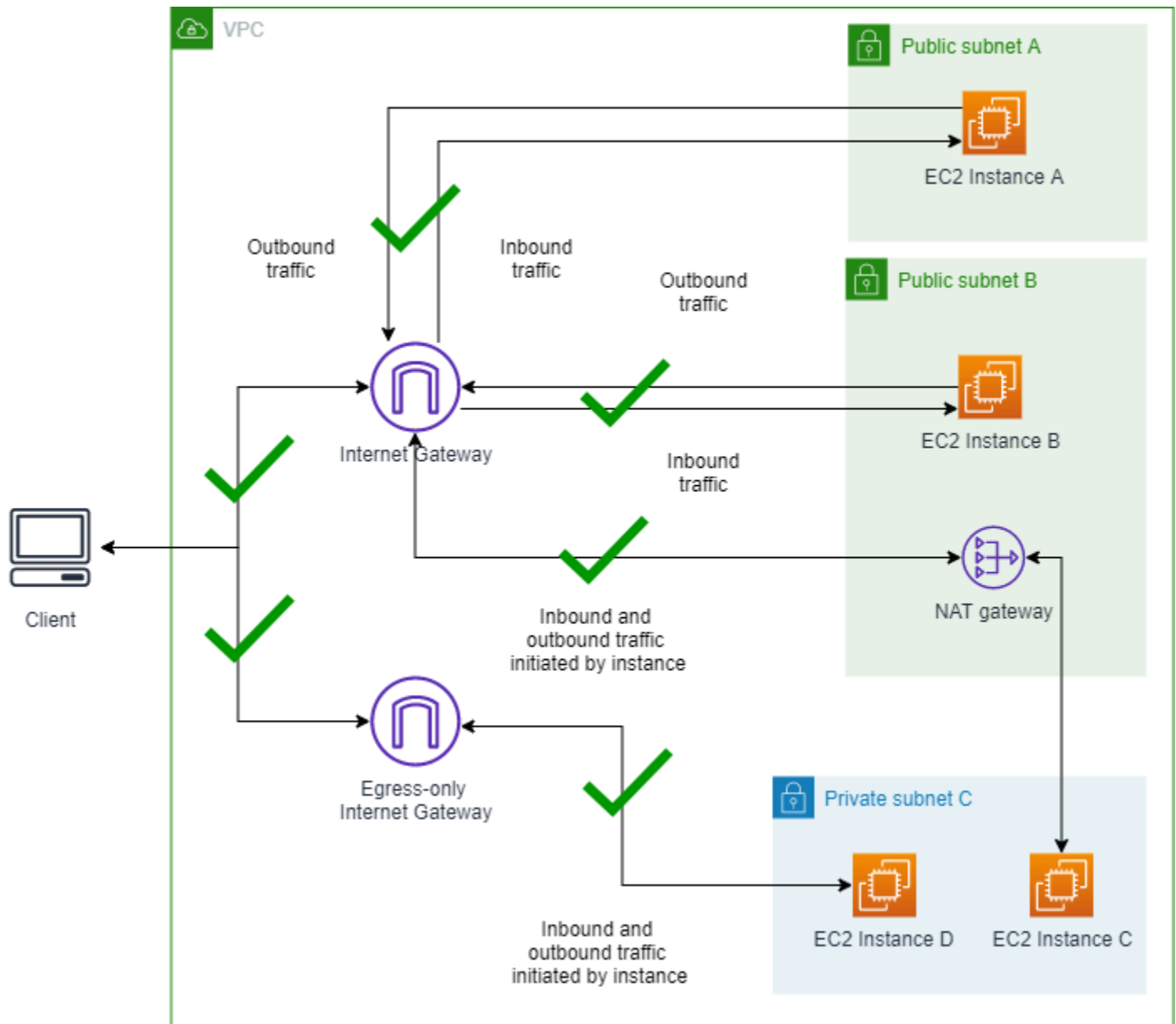
4. Analisis temuan untuk memahami dampak VPC BPA pada sumber daya di Anda. VPCs

Analisis dampak selesai.

Skenario 1 - Connect ke instance tanpa VPC BPA diaktifkan

Pada bagian ini, EC2 contoh di subnet publik A dan B dapat dijangkau dari internet melalui Internet Gateway, yang memungkinkan lalu lintas masuk dan keluar. Contoh C dan D di subnet pribadi dapat memulai lalu lintas keluar melalui NAT Gateway atau Egress-Only Internet Gateway, tetapi tidak dapat dijangkau secara langsung dari internet. Pengaturan ini menyediakan akses internet ke beberapa sumber daya sambil melindungi yang lain. Tujuan dari pengaturan ini adalah untuk menetapkan garis dasar dan memastikan bahwa, sebelum Anda mengaktifkan VPC BPA, semua instance dapat dicapai, Anda akan terhubung ke semua instance dan melakukan ping ke alamat IP publik.

Diagram VPC tanpa VPC BPA dihidupkan:



1.1 Connect ke instance

Lengkapi bagian ini untuk terhubung ke instans Anda dengan VPC BPA dimatikan untuk memastikan Anda dapat terhubung tanpa masalah. Semua instance yang dibuat dengan CloudFormation untuk contoh ini memiliki nama seperti, "VPC BPA Instance A".

AWS Management Console

1. Buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Buka detail Instance A.

3. Connect ke instance A menggunakan opsi EC2 Instance Connect > Connect menggunakan EC2 Instance Connect Endpoint.
4. Pilih Hubungkan. Setelah Anda berhasil terhubung ke instans, ping www.amazon.com untuk memverifikasi Anda dapat mengirim permintaan keluar ke internet.
5. Gunakan metode yang sama yang Anda gunakan untuk terhubung ke instance A untuk terhubung ke instance B, C, dan D. Dari setiap instance, ping www.amazon.com untuk memverifikasi Anda dapat mengirim permintaan keluar ke internet.

AWS CLI

1. Ping Instance A menggunakan IPv4 alamat 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 IPv4 alamat 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 IPv4 alamat 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 IPv4 alamat 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. Connect to Instance C. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian ping 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. Connect to Instance D. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian ping 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:

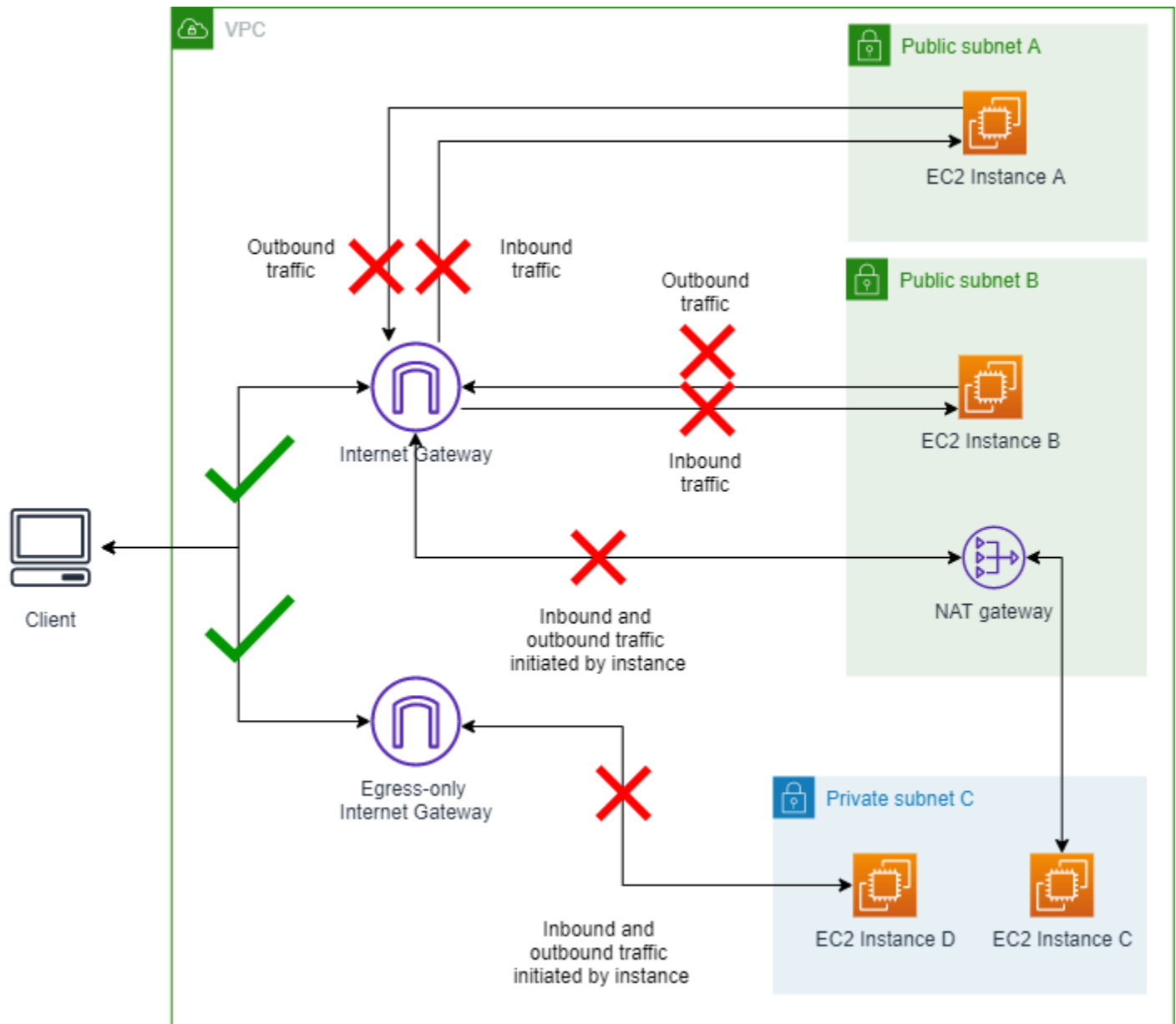
```
The authenticity of host '10.0.3.59' can't be established.
ECDSA key fingerprint is SHA256:c4naBCqbC61/cExDyccEproNU+1HHSpMSzl2J6c0tIZA8g.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.3.59' (ECDSA) to the list of known hosts.
A newer release 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 - Nyalakan 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 diaktifkan:



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 jalan keluar di Wilayah ini (kecuali untuk dikecualikan dan subnet). VPCs

AWS Management Console

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi kiri, pilih Pengaturan.
3. Pilih Edit pengaturan akses publik.

4. Pilih Aktifkan blokir akses publik dan dua arah, lalu pilih Simpan perubahan.
5. Tunggu Status berubah menjadi On. Mungkin perlu beberapa menit agar pengaturan VPC BPA berlaku dan statusnya 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 statusnya diperbarui.

2. Lihat status VPC BPA:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

2.2 Connect ke instance

Lengkapi bagian ini untuk terhubung ke instans Anda.

AWS Management Console

1. Ping IPv4 alamat publik Instance A dan Instance B seperti yang Anda lakukan di Skenario 1. Perhatikan bahwa lalu lintas diblokir.
2. Connect ke instance 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 terhubung ke instance A untuk terhubung ke instance B, C, dan D, uji permintaan keluar ke internet. Perhatikan bahwa semua lalu lintas keluar diblokir.

AWS CLI

1. Ping Instance A menggunakan IPv4 alamat 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 IPv4 alamat 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+7eTyWl0B/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 IPv4 alamat 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.

- Gunakan IPv4 alamat 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 SHA256:0IjXKKyVLDthcCfI0IPIJMUiItA0LYKRNLTGYURnFXo.
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.

- Connect to Instance C. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian ping 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. Connect to Instance D. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian ping 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 mengingat konfigurasi jaringan Anda, termasuk pengaturan VPC BPA. Dalam contoh ini Anda akan menganalisis jalur jaringan yang sama yang telah dicoba sebelumnya untuk mengonfirmasi bahwa VPC BPA adalah alasan mengapa konektivitas gagal.

AWS Management Console

1. Buka konsol Network Insights di <https://console.aws.amazon.com/networkinsights/home#ReachabilityAnalyzer>.
2. Klik Buat dan analisis jalur.
3. Untuk Jenis Sumber, pilih Internet Gateways dan pilih gateway internet yang diberi tag VPC BPA Internet Gateway dari dropdown Sumber.
4. Untuk Jenis Tujuan, pilih Instans dan pilih instance yang ditandai dengan VPC BPA Instance A dari dropdown Destination.
5. Klik Buat dan analisis jalur.
6. Tunggu analisis selesai. Ini bisa memakan waktu beberapa menit.
7. Setelah selesai, Anda akan melihat bahwa Status Reachability tidak dapat dijangkau dan detail Path menunjukkan bahwa itulah VPC_BLOCK_PUBLIC_ACCESS_ENABLED penyebabnya.

AWS CLI

1. Buat jalur jaringan menggunakan ID gateway internet yang diberi tag VPC BPA Internet Gateway dan ID instance yang ditandai 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
```

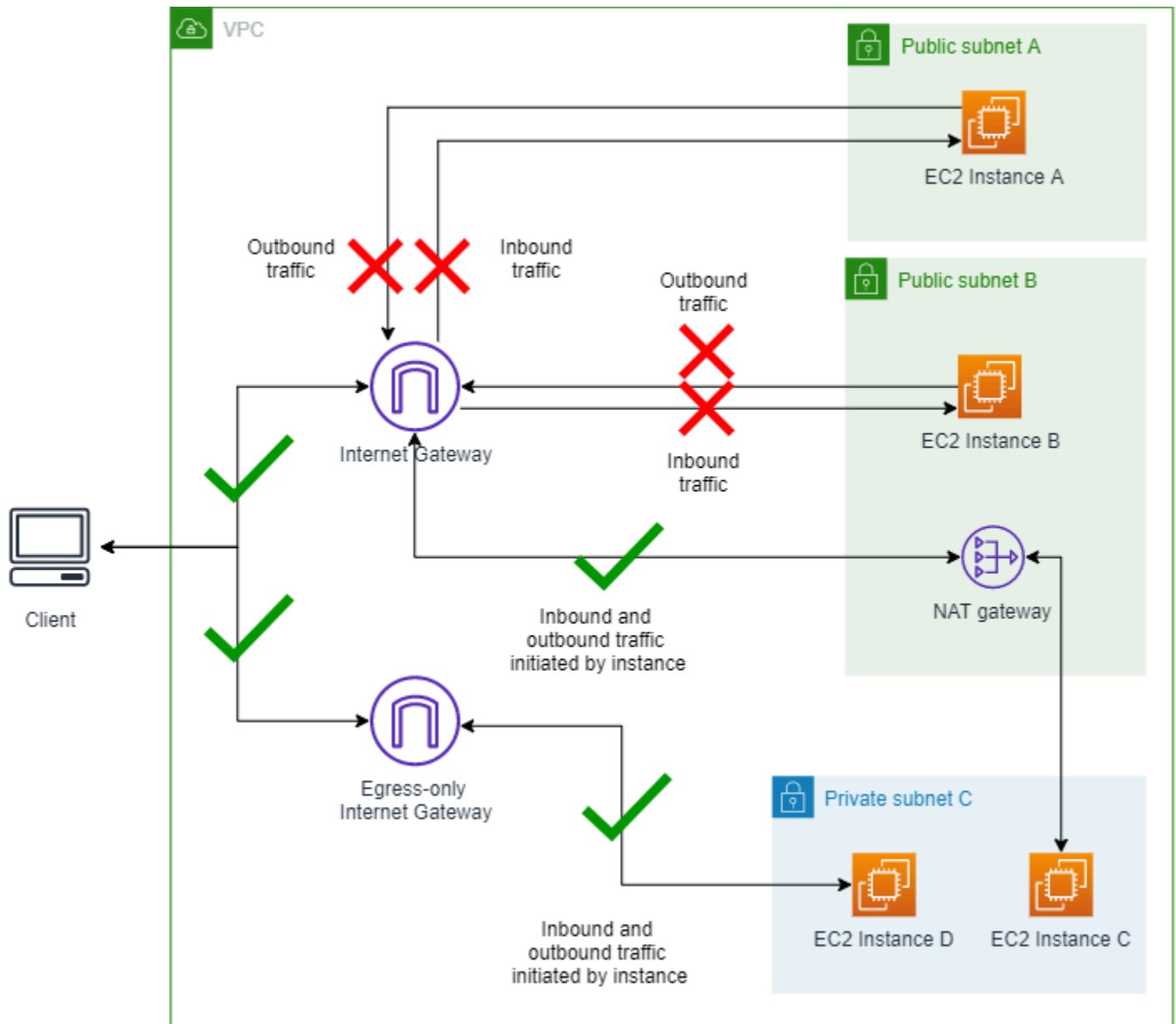
4. Verifikasi bahwa VPC_BLOCK_PUBLIC_ACCESS_ENABLED itu ExplanationCode karena kurangnya jangkauan.

Perhatikan bahwa Anda juga bisa [Pantau dampak VPC BPA 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 egres. EC2 Contoh A dan B di subnet publik tidak dapat dijangkau dari internet karena BPA memblokir lalu lintas masuk melalui Internet Gateway. Contoh C dan D di subnet pribadi akan tetap dapat memulai lalu lintas keluar melalui gateway NAT dan Egress-Only Internet Gateway, dan karena itu masih dapat menjangkau internet.

Diagram mode VPC BPA Ingress-only dihidupkan:



3.1 Ubah mode ke ingress-only

Lengkapi bagian ini untuk mengubah mode.

AWS Management Console

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi kiri, pilih Pengaturan.
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 statusnya diperbarui. Mungkin perlu beberapa menit agar pengaturan VPC BPA berlaku dan statusnya 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 statusnya diperbarui.

2. Lihat status VPC BPA:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

3.2 Connect ke instance

Lengkapi bagian ini untuk terhubung ke instance.

AWS Management Console

1. Ping IPv4 alamat publik Instance A dan Instance B seperti yang Anda lakukan di Skenario 1. Perhatikan bahwa lalu lintas diblokir.
2. Connect ke Instance A dan B menggunakan EC2 instance connect seperti yang Anda lakukan di Skenario 1 dan ping www.amazon.com dari mereka. Perhatikan bahwa Anda tidak dapat melakukan ping ke situs publik di internet dari Instance A atau B dan lalu lintas diblokir.
3. Connect ke Instance C dan D menggunakan EC2 instance connect seperti yang Anda lakukan di Skenario 1 dan ping www.amazon.com dari mereka. 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 IPv4 alamat 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.

- Gunakan IPv4 alamat 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+7eTyWl0B/Ke04IM+hadjs0LJeRTWBk.
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.

- Ping Instance B menggunakan IPv4 alamat 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.

- Gunakan IPv4 alamat 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 SHA256:0IjXKKyVlDthcCfI0IPIJMUiItA0LYKRNlGTYURnFXo.
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.

- Connect to Instance C. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian ping 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. Connect to Instance D. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian ping 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/'

```

```
      _/ _/
    _/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
```

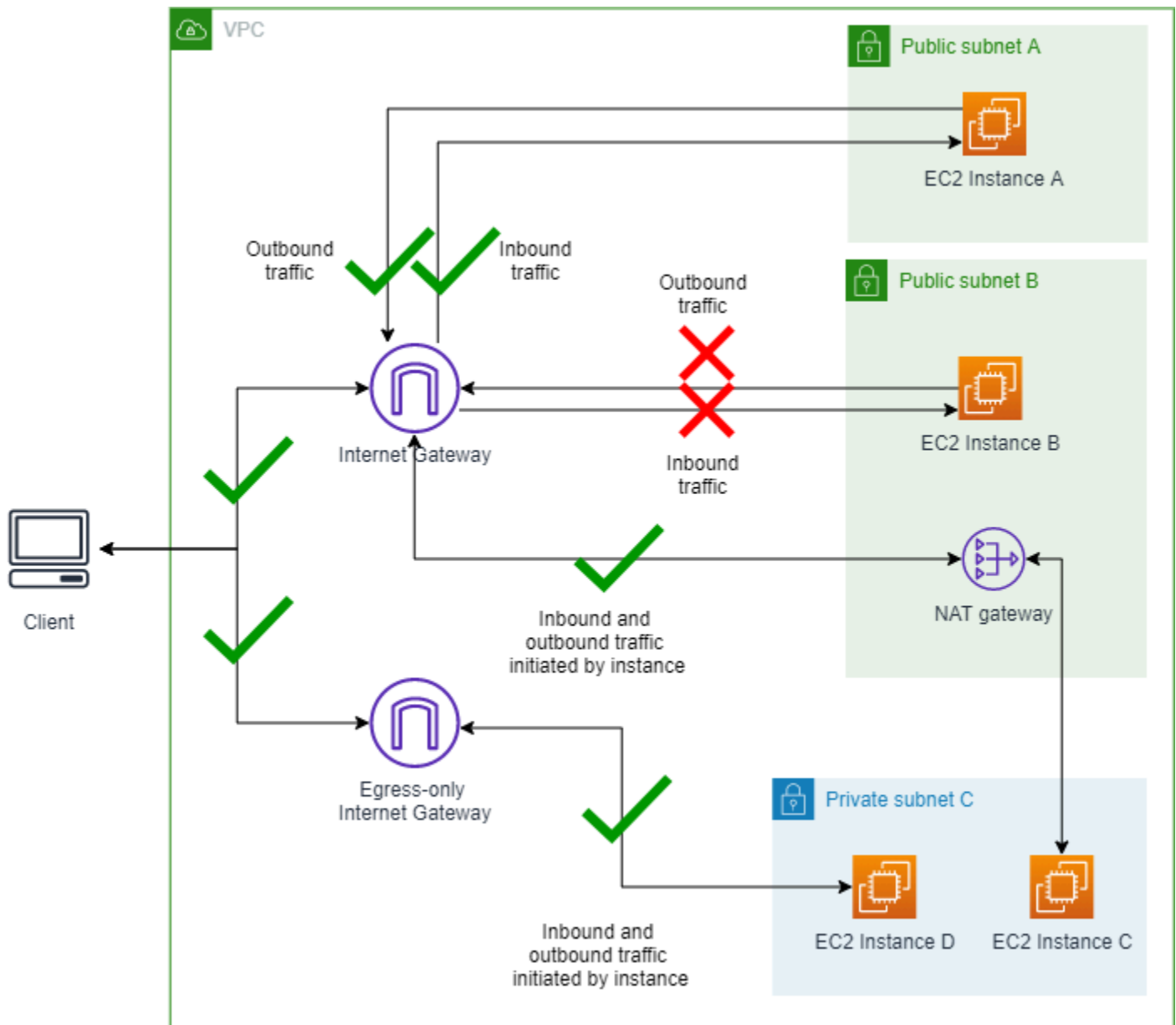
Perhatikan bahwa ping berhasil dan lalu lintas tidak diblokir.

Skenario 4 - Buat pengecualian

Di bagian ini, Anda akan membuat pengecualian. VPC BPA kemudian hanya akan memblokir lalu lintas pada subnet tanpa pengecualian. Pengecualian VPC BPA adalah mode yang dapat diterapkan ke satu VPC atau subnet yang mengecualikannya dari mode BPA VPC akun dan akan memungkinkan akses dua arah atau egress-only. Anda dapat membuat pengecualian BPA VPC untuk VPCs dan subnet bahkan ketika VPC BPA tidak diaktifkan pada akun untuk memastikan bahwa tidak ada gangguan lalu lintas ke pengecualian ketika VPC BPA dihidupkan.

Dalam contoh ini, kita akan membuat pengecualian untuk Subnet A untuk menunjukkan bagaimana lalu lintas ke pengecualian dipengaruhi oleh VPC BPA.

Diagram mode VPC BPA Ingress-only diaktifkan dan Subnet Pengecualian dengan mode Dua Arah diaktifkan:



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 mengecualikannya dari mode BPA VPC akun dan akan memungkinkan akses dua arah atau egress-only. Anda dapat membuat pengecualian BPA VPC untuk VPCs dan subnet bahkan ketika VPC BPA tidak diaktifkan pada akun untuk memastikan bahwa tidak ada gangguan lalu lintas ke pengecualian ketika VPC BPA dihidupkan.

AWS Management Console

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>

2. Di panel navigasi kiri, pilih Pengaturan.
3. Di tab Blokir akses publik, di bawah Pengecualian, pilih Buat pengecualian.
4. Pilih VPC BPA Public Subnet A, pastikan bahwa allow direction Dua Arah dipilih, dan pilih Buat pengecualian.
5. Tunggu status Pengecualian berubah menjadi Aktif. Anda mungkin perlu menyegarkan tabel pengecualian untuk melihat perubahannya.

Pengecualian telah dibuat.

AWS CLI

1. Ubah arah izin pengecualian:

```
aws ec2 --region us-east-2 create-vpc-block-public-access-exclusion --subnet-id subnet-id --internet-gateway-exclusion-mode allow-bidirectional
```

2. Diperlukan 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 Connect ke instance

Lengkapi bagian ini untuk terhubung ke instance.

AWS Management Console

1. Ping IPv4 alamat publik Instance A. Perhatikan bahwa lalu lintas diperbolehkan.
2. Ping IPv4 alamat publik Instance B. Perhatikan bahwa lalu lintas diblokir.
3. Connect to Instance A menggunakan EC2 instance connect 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. Connect ke Instance B menggunakan EC2 instance connect 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. Connect ke Instance C dan D menggunakan EC2 instance connect seperti yang Anda lakukan di Skenario 1 dan ping www.amazon.com dari mereka. 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 IPv4 alamat 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 IPv4 alamat 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 IPv4 alamat 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 IPv4 alamat 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. Connect to Instance C. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian ping 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. Connect to Instance D. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian ping 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.akamaitechnologies.com
(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 tersebut dapat dijangkau sekarang setelah pengecualian telah dibuat untuk Public Subnet A.

Untuk informasi tentang ketersediaan regional Reachability Analyzer, lihat [Pertimbangan](#) dalam Panduan Reachability Analyzer.

AWS Management Console

1. Dari Jalur Jaringan yang Anda buat sebelumnya di konsol Network Insights, klik Re-run analysis.
2. Tunggu analisis selesai. Mungkin perlu beberapa menit.
3. Konfirmasikan bahwa jalurnya sekarang Dapat Dijangkau.

AWS CLI

1. Menggunakan ID jalur jaringan yang dibuat sebelumnya, mulai 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.

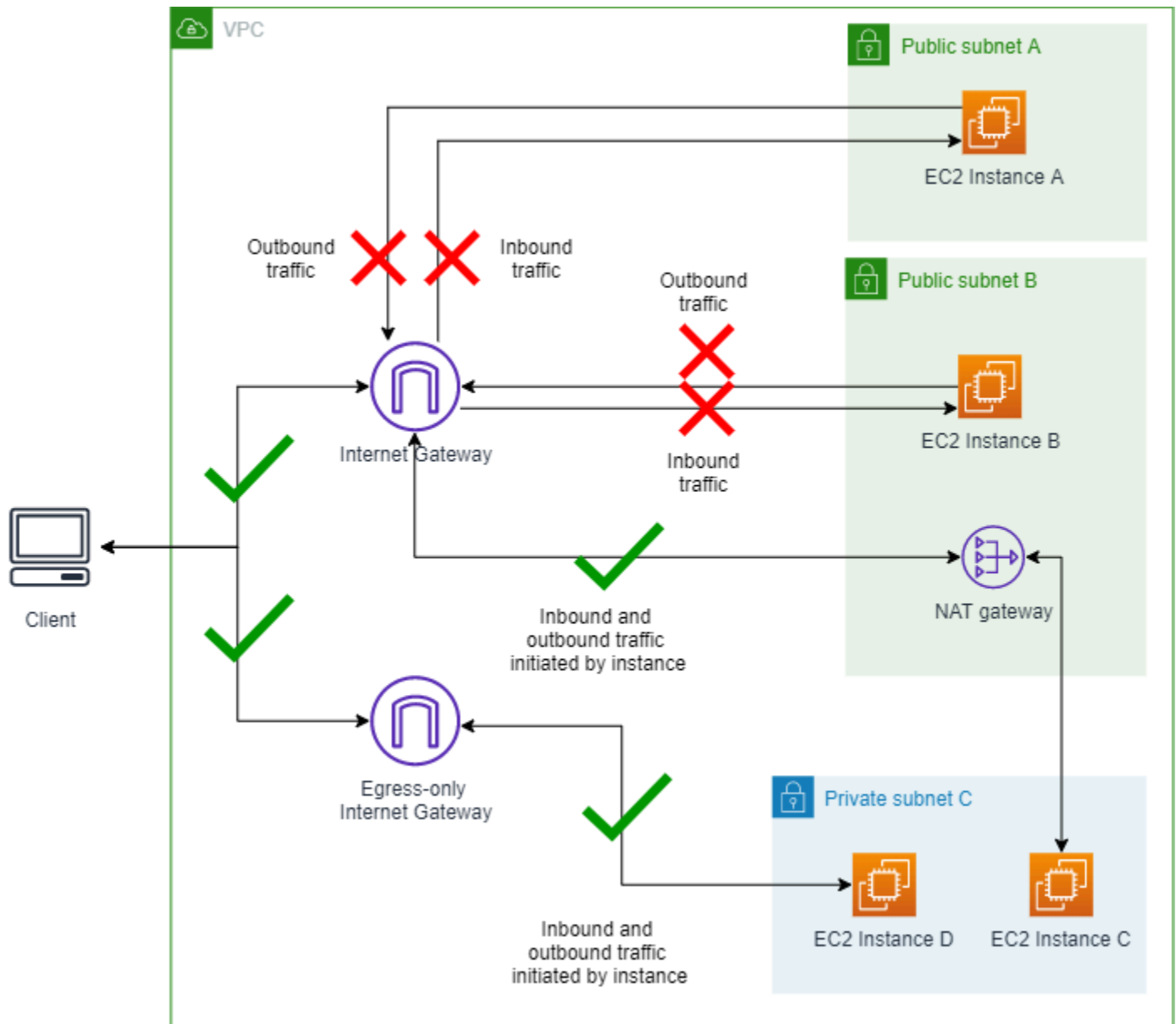
Skenario 5 - Ubah mode pengecualian

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, pengecualian khusus Egress di Subnet A tidak mengizinkan lalu lintas keluar, yang berlawanan dengan intuisi karena Anda mengharapkannya mengizinkan lalu lintas keluar. Namun, karena BPA tingkat akun hanya masuk, pengecualian khusus Egress 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 mengganti VPC BPA ke mode Bidirectional.

Diagram mode VPC BPA Ingress-only diaktifkan dan Subnet Pengecualian dengan mode egress-only diaktifkan:



5.1 Ubah pengecualian, izinkan arah ke egress-only

Lengkapi bagian ini untuk mengubah arah izin pengecualian.

AWS Management Console

1. Edit pengecualian yang Anda buat di Skenario 4 dan ubah arah allow menjadi Egress-only.
2. Pilih Simpan perubahan.
3. Tunggu status Pengecualian berubah menjadi Aktif. Mungkin perlu beberapa menit agar pengaturan VPC BPA berlaku dan statusnya diperbarui. Anda mungkin perlu menyegarkan tabel pengecualian untuk melihat perubahannya.

AWS CLI

1. Ubah arah izin pengecualian:

```
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 statusnya diperbarui.

2. Diperlukan waktu untuk memperbarui status pengecualian. Untuk melihat status pengecualian:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-exclusion
```

5.2 Connect ke instance

Lengkapi bagian ini untuk terhubung ke instance.

AWS Management Console

1. Ping IPv4 alamat publik Instance A dan B. Perhatikan bahwa lalu lintas diblokir.
2. Connect ke Instance A dan B menggunakan EC2 instance connect 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. Connect ke Instance C dan D menggunakan EC2 instance connect seperti yang Anda lakukan di Skenario 1 dan ping www.amazon.com dari mereka. 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 IPv4 alamat 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.

- Gunakan IPv4 alamat 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.

- Ping Instance B menggunakan IPv4 alamat 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.

- Gunakan IPv4 alamat 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. Connect to Instance C. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian ping 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. Connect to Instance D. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian ping 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
```

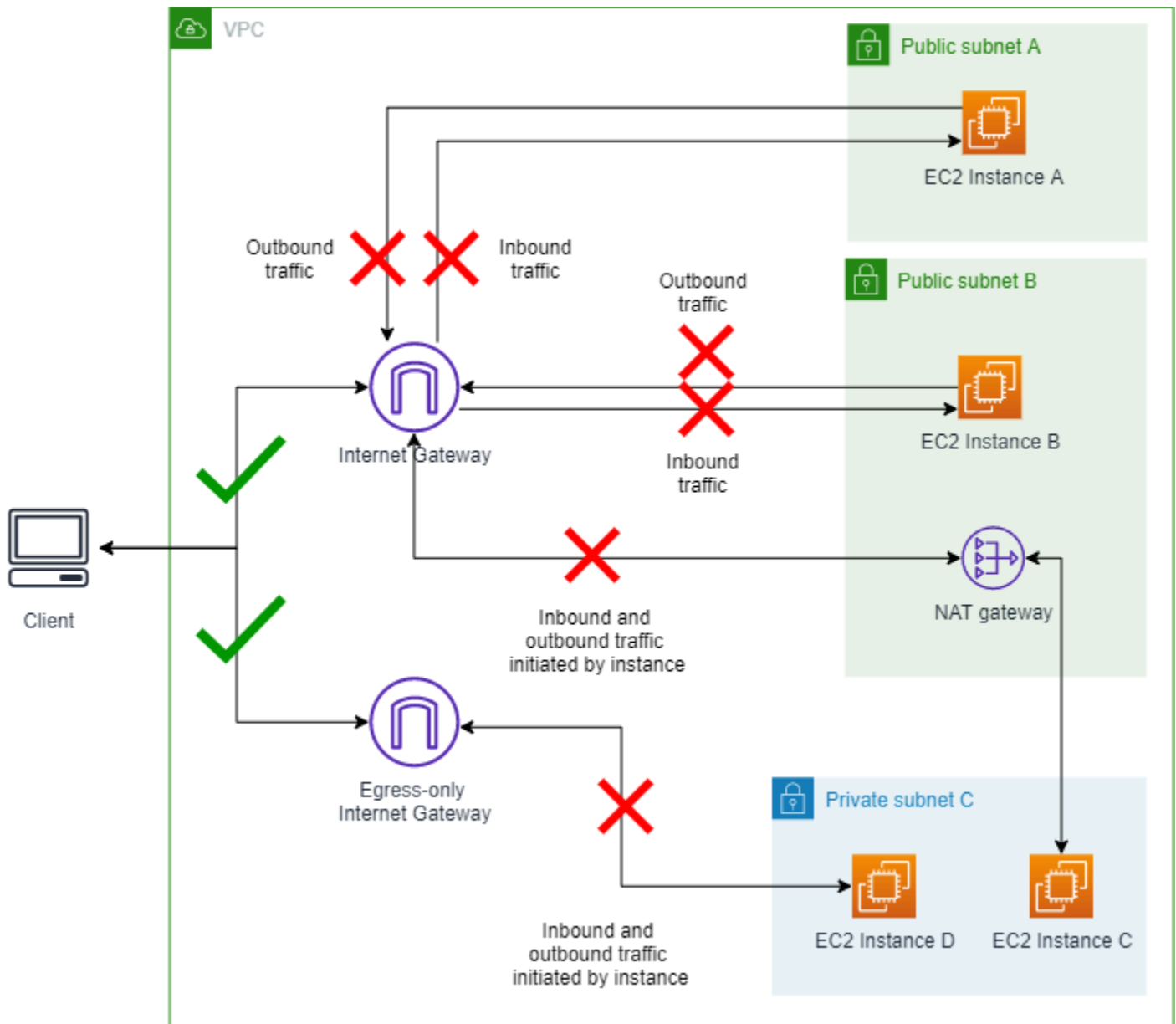
Perhatikan bahwa ping berhasil dan lalu lintas tidak diblokir.

Skenario 6 - Memodifikasi 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 diaktifkan dalam mode dua arah memblokir semua

lalu lintas seperti di Skenario 1. Kecuali pengecualian memiliki akses ke gateway NAT atau gateway internet khusus egres, lalu lintas diblokir.

Diagram mode dua arah VPC BPA dihidupkan dan Subnet Pengecualian dengan mode egress-only diaktifkan:



6.1 Ubah VPC BPA ke mode dua arah

Lengkapi bagian ini untuk mengubah mode VPC BPA.

AWS Management Console

1. Buka konsol VPC Amazon di. <https://console.aws.amazon.com/vpc/>

2. Di panel navigasi kiri, pilih Pengaturan.
3. Pilih Edit pengaturan akses publik.
4. Ubah arah blok menjadi Bidirectional lalu pilih Simpan perubahan.
5. Tunggu Status berubah menjadi On. Mungkin perlu beberapa menit agar pengaturan VPC BPA berlaku dan statusnya 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 statusnya diperbarui.

2. Lihat status VPC BPA:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

6.2 Connect ke instance

Lengkapi bagian ini untuk terhubung ke instance.

AWS Management Console

1. Ping IPv4 alamat publik Instance A dan B. Perhatikan bahwa lalu lintas diblokir.
2. Connect ke Instance A dan B menggunakan EC2 instance connect 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. Connect ke Instance C dan D menggunakan EC2 instance connect seperti yang Anda lakukan di Skenario 1 dan ping www.amazon.com dari mereka. 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 IPv4 alamat 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.

- Gunakan IPv4 alamat 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.

- Ping Instance A menggunakan IPv4 alamat 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.

- Gunakan IPv4 alamat 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.

- Connect to Instance C. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian ping 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. Connect to Instance D. Karena tidak ada alamat IP publik untuk melakukan ping, gunakan EC2 Instance Connect untuk menghubungkan dan kemudian ping 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 CloudFormation sumber daya

Lengkapi bagian ini untuk menghapus sumber daya yang Anda buat dengan AWS CloudFormation templat.

AWS Management Console

1. Buka AWS CloudFormation konsol di <https://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 CloudFormation tumpukan. 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 dengan AWS CloudTrail

Lengkapi bagian ini untuk melacak penghapusan pengecualian dengan. AWS CloudTrail CloudTrail entri muncul saat Anda menghapus pengecualian.

AWS Management Console

Anda dapat melihat pengecualian yang dihapus dalam riwayat CloudTrail Acara dengan mencari Jenis sumber daya > AWS::EC2:: VPCBlock PublicAccessExclusion di AWS CloudTrail konsol di <https://console.aws.amazon.com/cloudtrailv2/>.

AWS CLI

Anda dapat menggunakan perintah `lookup-events` untuk melihat peristiwa yang terkait dengan penghapusan pengecualian:

```
aws cloudtrail lookup-events --lookup-attributes
AttributeKey=ResourceType,AttributeValue=AWS::EC2::VPCBlockPublicAccessExclusion
```

Contoh lanjutan selesai.

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 tidak memadai untuk lingkungan Anda, perlakukan itu sebagai pertimbangan yang bermanfaat, bukan sebagai resep.

- Saat Anda menambahkan subnet ke VPC untuk meng-host aplikasi Anda, buat subnet di beberapa Availability Zone. Availability Zone adalah satu atau lebih pusat data diskrit dengan daya redundan, jaringan, dan konektivitas di suatu Wilayah. AWS Menggunakan beberapa Availability Zone membuat aplikasi produksi Anda sangat tersedia, toleran terhadap kesalahan, dan skalabel.
- Gunakan grup keamanan untuk mengontrol lalu lintas ke EC2 instance di subnet Anda. Untuk informasi selengkapnya, lihat [Grup keamanan](#).
- Gunakan jaringan ACLs 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, pengguna, dan peran AWS Identity and Access Management (IAM). Untuk informasi selengkapnya, lihat [Identity and access management untuk Amazon VPC](#).
- Gunakan VPC Flow Logs untuk memantau lalu lintas IP yang menuju dan dari antarmuka VPC, subnet, atau jaringan. Untuk informasi selengkapnya, lihat [Log Alur VPC](#).

- Gunakan Network Access Analyzer untuk mengidentifikasi akses jaringan yang tidak diinginkan ke sumber daya di kami. VPCs Untuk informasi selengkapnya, lihat [Panduan Penganalisis Akses Jaringan](#).
- Gunakan AWS Network Firewall untuk memantau dan melindungi VPC Anda dengan memfilter lalu lintas masuk dan keluar. Untuk informasi lebih lanjut, lihat [AWS Network Firewall Panduan](#).
- Gunakan Amazon GuardDuty untuk mendeteksi potensi ancaman terhadap akun, container, beban kerja, dan data di AWS lingkungan Anda. Deteksi ancaman mendasar mencakup pemantauan log aliran VPC yang terkait dengan instans Amazon EC2 Anda. Untuk informasi selengkapnya, lihat [Log Aliran VPC](#) di GuardDuty Panduan Pengguna Amazon.

[Untuk jawaban atas pertanyaan umum terkait keamanan VPC, lihat Keamanan dan Pemfilteran di Amazon VPC. FAQs](#)

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 memanfaatkan integrasi antara VPC dan AWS layanan lainnya 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 dalam AWS jaringan dan menghindari paparan ke internet publik. Hal ini sangat berguna untuk menjaga batas-batas keamanan yang ketat dan persyaratan kepatuhan.

Untuk lebih memperkuat keamanan VPC Anda, Anda dapat menggunakannya. AWS Network Firewall Layanan firewall terkelola ini memungkinkan Anda untuk menentukan dan menegakkan kebijakan keamanan tingkat jaringan, memfilter lalu lintas utara-selatan dan timur-barat dalam VPC Anda. Dengan memasang Network Firewall dengan VPC Anda, Anda dapat meningkatkan strategi pertahanan Anda 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 tambahan penegakan keamanan dan kepatuhan.

Jika Anda mengalami masalah jangkauan antara sumber daya dalam VPC atau terhubung ke VPC, Anda dapat memanfaatkan 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 jangkauan menggunakan Reachability Analyzer](#)

Hubungkan VPC Anda ke layanan menggunakan AWS PrivateLink

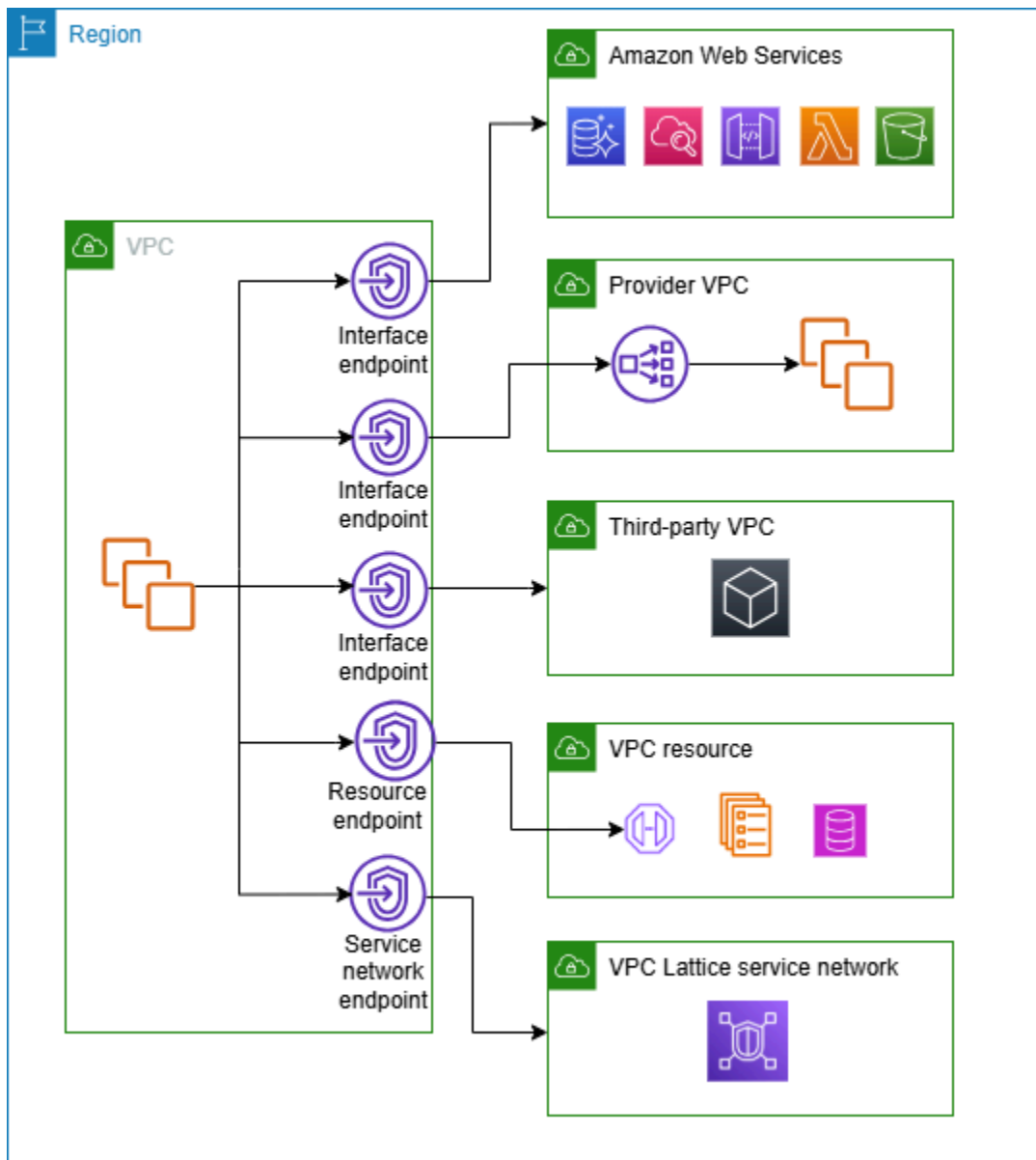
AWS PrivateLink membangun konektivitas pribadi antara virtual private cloud (VPC) dan Layanan AWS didukung, layanan yang dihosting oleh layanan Akun AWS lain yang AWS Marketplace didukung, dan sumber daya yang didukung. Anda tidak perlu menggunakan gateway internet, perangkat NAT, AWS Direct Connect koneksi, atau AWS Site-to-Site VPN koneksi untuk berkomunikasi dengan layanan atau sumber daya.

Untuk menggunakannya AWS PrivateLink, buat titik akhir VPC di subnet apa pun yang Anda perlukan untuk mengakses layanan atau sumber daya. Ini menciptakan antarmuka jaringan elastis dalam subnet tertentu yang berfungsi sebagai titik masuk untuk lalu lintas yang ditujukan ke layanan atau sumber daya.

Anda juga dapat membuat layanan endpoint 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 pelanggan lain. AWS Ini memberdayakan bisnis untuk memonetisasi kemampuan internal mereka, mendorong ekosistem kolaboratif, dan mempertahankan kendali atas bagaimana layanan mereka diakses dan dikonsumsi.

Salah satu manfaat utama penggunaan AWS PrivateLink adalah kemampuan untuk membangun konektivitas pribadi yang aman tanpa memerlukan 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 dalam jaringan. AWS

Diagram berikut menunjukkan kasus penggunaan umum untuk AWS PrivateLink. VPC memiliki beberapa EC2 instance 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.



Untuk informasi selengkapnya, lihat [AWS PrivateLink](#).

Filter lalu lintas jaringan menggunakan AWS Network Firewall

Anda dapat memfilter lalu lintas jaringan di perimeter VPC Anda menggunakan AWS Network Firewall. AWS 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 perlindungan untuk firewall. Rincian perilaku didefinisikan dalam grup aturan yang Anda tambahkan ke kebijakan Anda, dan di beberapa pengaturan 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 Manager](#) di 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 mengizinkan, 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 Manager](#) di AWS WAF AWS Firewall Manager, dan Panduan AWS Shield Advanced Pengembang.

Memecahkan masalah jangkauan 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 hop-by-hop menghasilkan rincian 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:

- Instans
- Gateway internet
- Antarmuka jaringan
- Transit gateway
- Lampiran gateway transit
- Layanan VPC endpoint
- Titik akhir VPC
- Koneksi peering VPC
- Gateway VPN

Untuk informasi selengkapnya, lihat Panduan [Reachability Analyzer](#).

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 resilien 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)
- [Ops Konektivitas Amazon Virtual Private Cloud](#) (AWS Whitepaper)

Contoh: VPC untuk lingkungan pengujian

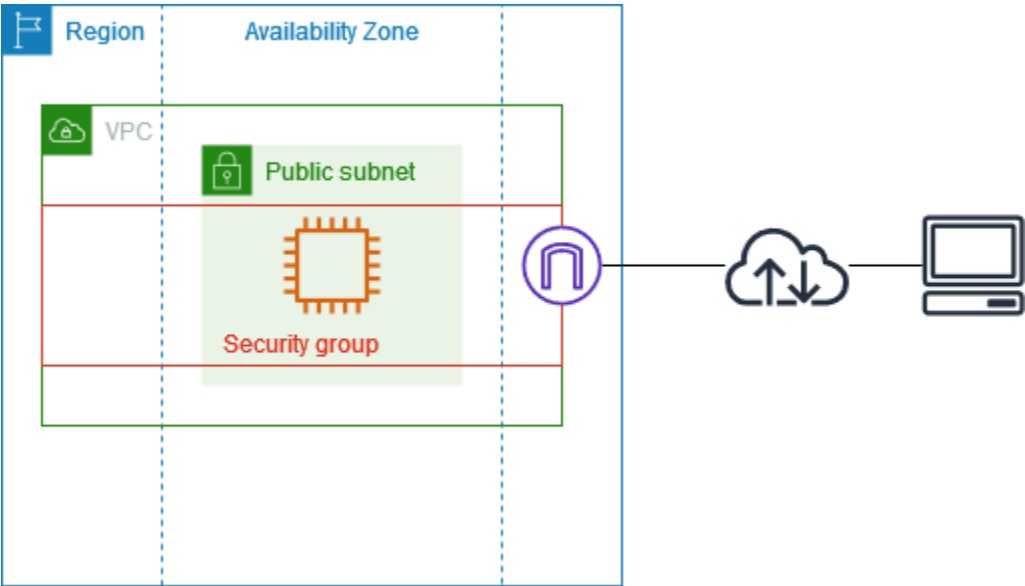
Contoh ini menunjukkan cara membuat VPC yang dapat Anda gunakan sebagai lingkungan pengembangan atau pengujian. Karena VPC ini tidak dimaksudkan untuk digunakan dalam produksi, Anda tidak perlu menyebarkan server Anda di beberapa Availability Zone. Untuk menjaga biaya dan kompleksitas tetap rendah, Anda dapat menerapkan server Anda dalam satu Availability Zone.

Daftar Isi

- [Gambaran Umum](#)
- [1. Buat VPC](#)
- [2. Men-deploy aplikasi Anda](#)
- [3. Uji konfigurasi Anda](#)
- [4. Bersihkan](#)

Gambaran Umum

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 EC2 contoh 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

Tujuan	Target
<i>10.0.0.0/16</i>	lokal
<i>2001:db8:1234:1a00::/56</i>	lokal
0.0.0.0/0	<i>igw-id</i>
::/0	<i>igw-id</i>

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
<i>Public IPv4 address range of your network</i>	TCP	22	(Opsional) Memungkinkan akses SSH masuk dari alamat IPv4 IP di jaringan Anda
<i>IPv6 address range of your network</i>	TCP	22	(Opsional) Memungkinkan akses SSH masuk dari alamat IPv6 IP di jaringan Anda
<i>Public IPv4 address range of your network</i>	TCP	3389	(Opsional) Memungkinkan akses RDP masuk dari alamat IPv4 IP di jaringan Anda
<i>IPv6 address range of your network</i>	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. Konfigurasi 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. Konfigurasi 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 CIDR subnet”](#).
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 menyebarkan EC2 instance. Sebagai contoh:

- [Wisaya instans EC2 peluncuran Amazon](#)

- [EC2 Auto Scaling Amazon](#)
- [AWS CloudFormation](#)
- [Amazon Elastic Container Service \(Amazon ECS\)](#)

Setelah menerapkan EC2 instance, 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 EC2 Pengguna Amazon. 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 EC2 instans 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. Untuk informasi selengkapnya, lihat [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.

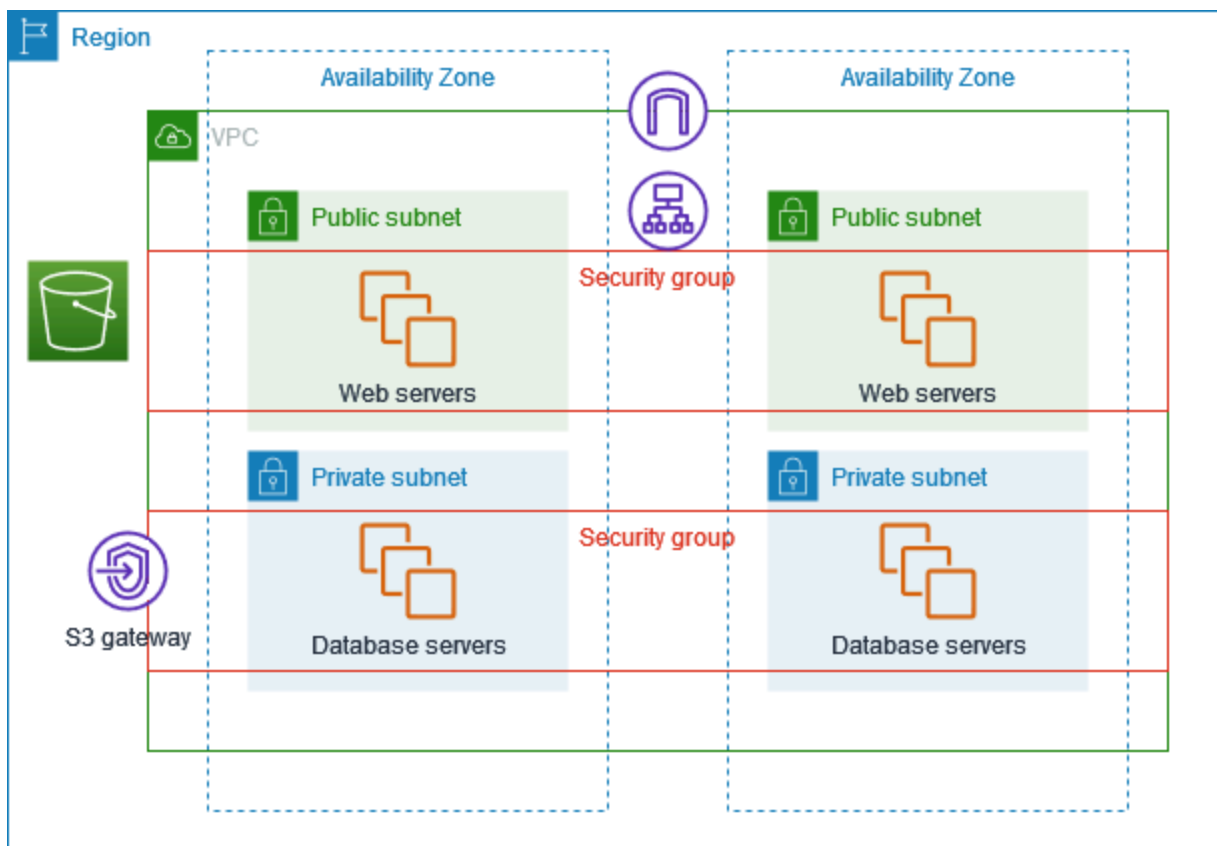
Daftar Isi

- [Gambaran Umum](#)
- [1. Buat VPC](#)
- [2. Men-deploy aplikasi Anda](#)
- [3. Uji konfigurasi Anda](#)

- [4. Bersihkan](#)

Gambaran Umum

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
<i>10.0.0.0/16</i>	lokal
<i>2001:db8:1234:1a00::/56</i>	lokal
0.0.0.0/0	<i>igw-id</i>
::/0	<i>igw-id</i>

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
<i>10.0.0.0/16</i>	lokal
<i>2001:db8:1234:1a00::/56</i>	lokal
<i>s3-prefix-list-id</i>	<i>s3-gateway-id</i>

Keamanan

Untuk konfigurasi contoh ini, Anda membuat grup keamanan untuk penyeimbang beban, grup keamanan untuk server web, dan grup keamanan untuk server database.

Penyeimbang beban

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
<i>ID of the security group for the load balancer</i>	TCP	80	Memungkinkan akses HTTP masuk dari penyeimbang beban
<i>ID of the security group for the load balancer</i>	TCP	443	Memungkinkan akses HTTPS masuk dari penyeimbang beban
<i>Public IPv4 address range of your network</i>	TCP	22	(Opsional) Memungkinkan akses SSH masuk dari alamat IPv4 IP di jaringan Anda
<i>IPv6 address range of your network</i>	TCP	22	(Opsional) Memungkinkan akses SSH masuk dari alamat IPv6 IP di jaringan Anda
<i>Public IPv4 address range of your network</i>	TCP	3389	(Opsional) Memungkinkan akses RDP masuk dari alamat IPv4 IP di jaringan Anda
<i>IPv6 address range of your network</i>	TCP	3389	(Opsional) Memungkinkan akses RDP masuk dari alamat IPv6 IP di jaringan Anda

Tujuan	Protokol	Rentang Port	Deskripsi
<i>ID of the security group for instances running</i>	TCP	1433	Memungkinkan akses Microsoft SQL Server keluar ke server database

Tujuan	Protokol	Rentang Port	Deskripsi
<i>Microsoft SQL Server</i>			
<i>ID of the security group for instances running MySQL</i>	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
<i>ID of the web server security group</i>	TCP	1433	Memungkinkan akses Microsoft SQL Server masuk dari server web
<i>ID of the web server security group</i>	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. Konfigurasi 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 Penyewaan. 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. Konfigurasi 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 CIDR subnet”](#).
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. Sebagai 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. Untuk informasi selengkapnya, lihat [the section called “Hapus VPC Anda”](#).

Contoh: VPC dengan server di subnet pribadi dan NAT

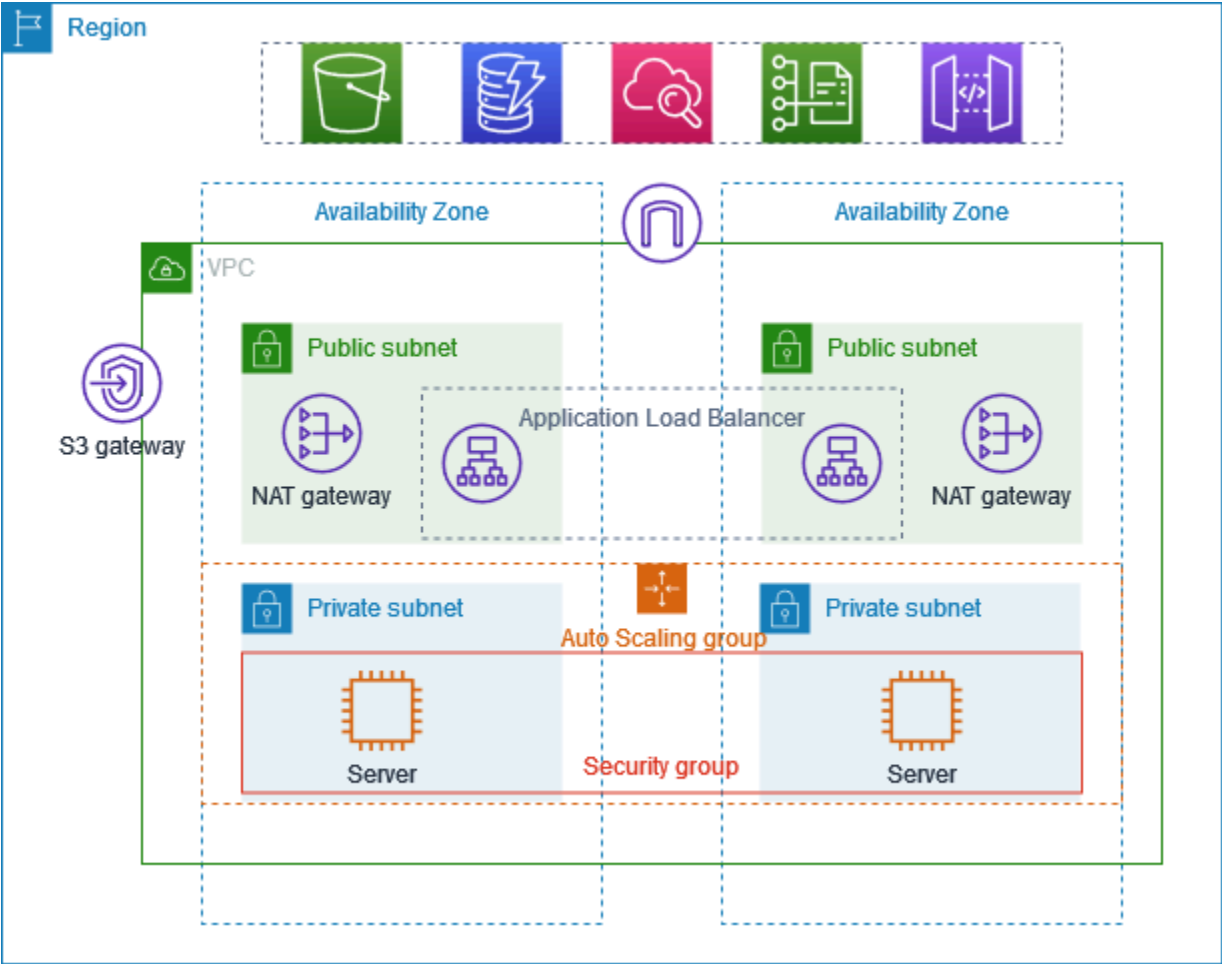
Contoh ini menunjukkan cara membuat VPC yang dapat Anda gunakan untuk server di lingkungan produksi. Untuk meningkatkan ketahanan, Anda menerapkan server di dua Availability Zone, dengan menggunakan grup Auto Scaling dan Application Load Balancer. Untuk keamanan tambahan, Anda menyebarkan server di subnet pribadi. Server menerima permintaan melalui penyeimbang beban. Server dapat terhubung ke internet dengan menggunakan gateway NAT. Untuk meningkatkan ketahanan, Anda menerapkan 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 gambaran umum tentang sumber daya yang termasuk dalam contoh 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.



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. Kami juga membuat tabel rute untuk subnet pribadi dengan rute lokal, dan rute ke gateway NAT , gateway internet khusus egres, dan 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 menyertakan rute. IPv4

Tujuan	Target
10.0.0.0/16	lokal
2001:db8:1234:1a00::/56	lokal

Tujuan	Target
0.0.0.0/0	<i>igw-id</i>
::/0	<i>igw-id</i>

Berikut ini adalah contoh tabel rute untuk salah satu subnet pribadi, dengan rute untuk keduanya IPv4 dan IPv6. Jika Anda membuat subnet IPv4 -only, tabel rute hanya mencakup rute IPv4. Rute terakhir mengirimkan lalu lintas yang ditujukan untuk Amazon S3 ke titik akhir VPC gateway.

Tujuan	Target
<i>10.0.0.0/16</i>	lokal
<i>2001:db8:1234:1a00::/56</i>	lokal
0.0.0.0/0	<i>nat-gateway-id</i>
::/0	<i>eigw-id</i>
<i>s3-prefix-list-id</i>	<i>s3-gateway-id</i>

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. Ini juga harus memungkinkan lalu lintas pemeriksaan kesehatan.

Sumber	Protokol	Rentang Port	Komentar
<i>ID of the load balancer security group</i>	<i>listener protocol</i>	<i>listener port</i>	Mengizinkan lalu lintas masuk dari penyeimbang beban di port pendengar
<i>ID of the load balancer security group</i>	<i>health check protocol</i>	<i>health check port</i>	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 Availability Zones, dan gateway NAT di setiap Availability Zone.

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. Konfigurasi 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 IPv6 alamat, pilih blok CIDR, blok IPv6 CIDR yang disediakan Amazon IPv6 .
5. Konfigurasi subnet
 - a. Untuk Jumlah Availability Zone, pilih 2, sehingga Anda dapat meluncurkan instance di beberapa 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 publik, atau sebagai alternatif Anda dapat memperluas Kustomisasi blok CIDR subnet dan memasukkan blok CIDR. Untuk informasi selengkapnya, lihat [the section called “Blok CIDR subnet”](#).
6. Untuk gateway NAT, pilih 1 per AZ untuk meningkatkan ketahanan.
7. Jika aplikasi Anda berkomunikasi dengan menggunakan IPv6 alamat, 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, instance 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 None, 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 menyebarkan aplikasi Anda dalam produksi.

Anda dapat menggunakan [Amazon EC2 Auto Scaling](#) untuk menyebarkan server di beberapa Availability Zone dan mempertahankan kapasitas server minimum yang diperlukan oleh aplikasi Anda.

Untuk meluncurkan instance dengan menggunakan grup Auto Scaling

1. Buat template peluncuran untuk menentukan informasi konfigurasi yang diperlukan untuk meluncurkan EC2 instans Anda menggunakan Amazon EC2 Auto Scaling. Untuk step-by-step petunjuk arah, lihat [Membuat template peluncuran untuk grup Auto Scaling Anda di Panduan Pengguna Auto EC2 Scaling Amazon](#).
2. Buat grup Auto Scaling, yang merupakan kumpulan EC2 instance dengan ukuran minimum, maksimum, dan yang diinginkan. Untuk step-by-step petunjuk arah, lihat [Membuat grup Auto Scaling menggunakan templat peluncuran di Panduan Pengguna Amazon Auto EC2 Scaling](#).
3. Buat penyeimbang beban, yang mendistribusikan lalu lintas secara merata di seluruh instans di grup Auto Scaling Anda, dan pasang penyeimbang beban ke grup Auto Scaling Anda. Untuk informasi selengkapnya, lihat [Panduan Pengguna Elastic Load Balancing dan Gunakan Elastic Load Balancing di Panduan Pengguna Amazon Auto EC2 Scaling](#).

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 menghapus grup Auto Scaling, menghentikan instance Anda, menghapus gateway NAT, dan menghapus penyeimbang beban. Untuk informasi selengkapnya, lihat [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
- Konfigurasi 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 (CLI). 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. Itu AWS CLI. Jika Anda perlu menginstalnya, ikuti [panduan AWS CLI instalasi](#).
2. Konfigurasi Anda AWS CLI dengan kredensi yang sesuai. Jalankan `aws configure` jika Anda belum menyiapkan kredensial Anda.
3. Pemahaman dasar tentang konsep jaringan.
4. [Identity and access management untuk Amazon VPC](#) untuk 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 selanjutnya. 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.

Konfigurasi koneksi internet

Untuk memungkinkan sumber daya di VPC Anda berkomunikasi dengan internet, Anda perlu membuat dan melampirkan Internet Gateway. Di bagian ini, Anda akan mengatur koneksi 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 konfigurasi tabel rute

Tabel rute berisi aturan (rule) 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.

Konfigurasi pengaturan subnet

Konfigurasi 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

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 melalui 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:

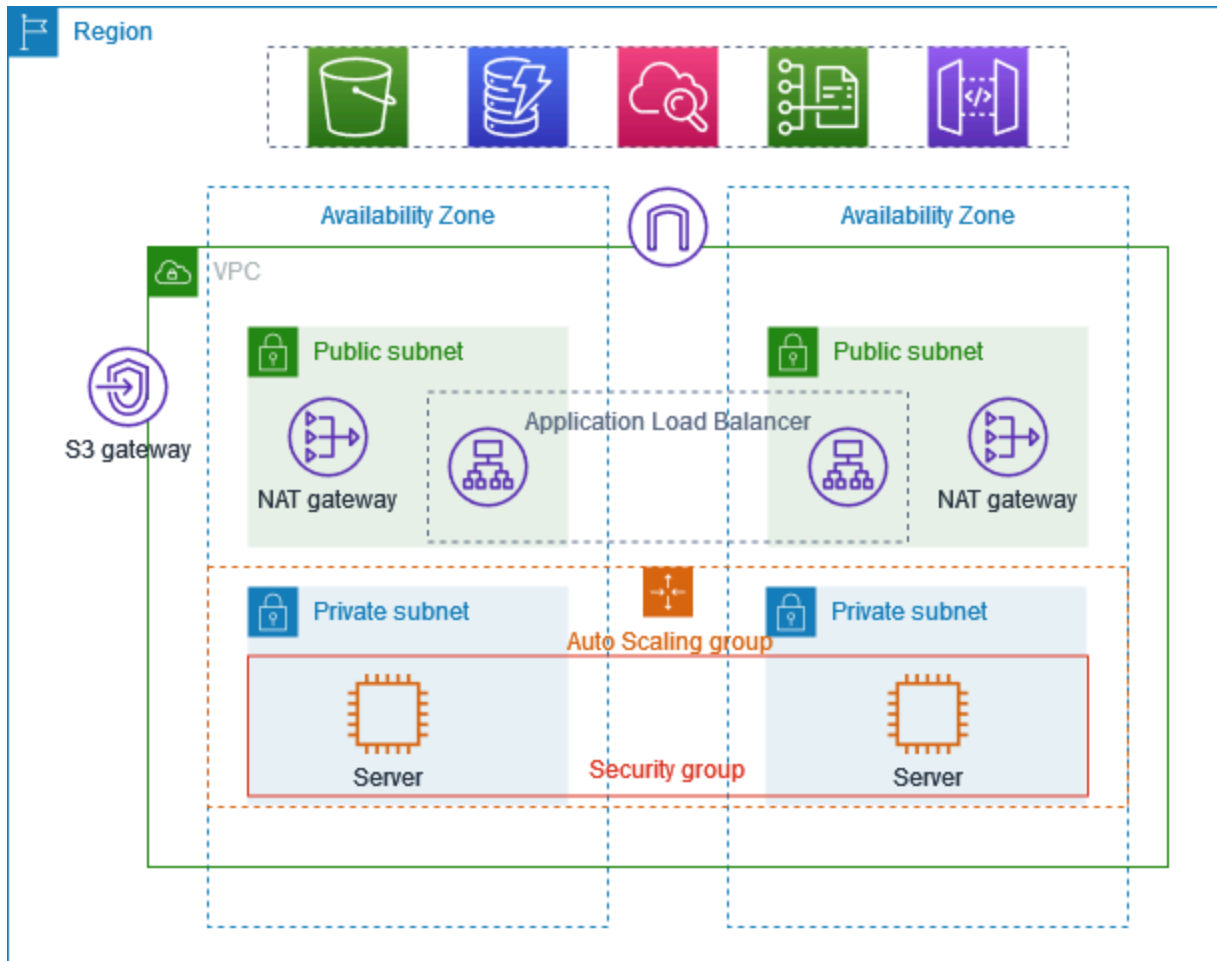
1. [Luncurkan EC2 instance](#) di subnet publik atau pribadi Anda.
2. [Menyebarkan penyeimbang beban](#) untuk mendistribusikan lalu lintas di beberapa instance.
3. [Siapkan grup Auto Scaling](#) untuk ketersediaan dan skalabilitas tinggi.
4. [Konfigurasi database RDS di subnet](#) pribadi Anda.
5. [Menerapkan 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 konfigurasi koneksi 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 \$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":
      "IyEvYmluL2Jhc2gKeXVtIHVwZGF0ZSAteQp5dW0gaW5zdGFsbCAtaSBodHRwZApzeXN0ZW1jdGwgc3RhcnQgaHR0cGQKc
+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 selanjutnya

Sekarang setelah Anda membuat VPC dengan subnet pribadi dan gateway NAT, Anda mungkin ingin menjelajahi topik terkait ini:

- [Praktik terbaik keamanan untuk VPC Anda](#)
- [Mencatat lalu lintas IP menggunakan VPC Flow Logs](#)
- [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 akun Anda. AWS Kecuali dinyatakan lain, kuota ini 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
VPCs 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 VPCs per Wilayah.
Subnet per VPC	200	Ya	
IPv4 Blok CIDR untuk VPC	5	Ya (hingga 50)	Blok CIDR primer ini dan semua blok CIDR sekunder dihitung terhadap kuota ini.
IPv6 Blok CIDR untuk VPC	5	Ya (hingga 50)	Jumlah CIDRs Anda dapat mengalokasikan ke satu VPC.
VPC Blokir Pengecualian Akses Publik per akun per Wilayah	50	Ya. Untuk meminta kenaikan, buka kasus peningkatan batas layanan menggunakan	Jumlah pengecualian VPC BPA yang dapat Anda buat di akun.

Nama	Default	Dapat disesuaikan	Komentar
		AWS Support Center Console.	

DNS

Setiap EC2 instance 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 menurut jenis kueri, ukuran respons, dan protokol yang digunakan. Untuk informasi selengkapnya dan rekomendasi untuk arsitektur DNS yang dapat diskalakan, lihat Panduan Teknis [AWS Hybrid DNS with Active Directory](#).

Alamat IP elastis

Nama	Default	Dapat disesuaikan	Komentar
Alamat IP Elastis per Wilayah	5	Ya	Kuota ini berlaku untuk individu Akun AWS VPCs dan bersama VPCs.
Alamat IP elastis per gateway NAT publik	2	Ya	Anda dapat meminta kenaikan kuota hingga 8.

Gerbang

Nama	Default	Dapat disesuaikan	Komentar
Gateway internet hanya egress per Wilayah	5	Ya	Untuk meningkatkan kuota ini, tingkatkan kuota VPCs 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 meningkatkan kuota ini, tingkatan kuota VPCs per Wilayah. Anda dapat melampirkan hanya satu gateway internet untuk satu VPC pada suatu waktu.
NAT gateway per Availability Zone	5	Ya	Gateway NAT hanya dihitung terhadap kuota Anda depending,, active dan negara bagian. deleting
Kuota alamat IP pribadi per gateway NAT	8	Ya	
Gateway operator per VPC	1	Tidak	

Daftar prefiks yang dikelola konsumen

Meskipun kuota default untuk daftar awalan yang dikelola pelanggan dapat disesuaikan, Anda tidak dapat meminta peningkatan menggunakan konsol Service Quotas. Anda harus [membuka kasus peningkatan batas layanan](#) menggunakan AWS Support Center Console.

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 Ubah 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	5.000	Ya	Kuota ini berlaku per jenis sumber daya yang dapat merujuk ke daftar prefiks. Misalnya, Anda dapat memiliki 5.000 referensi ke daftar prefiks di semua grup keamanan Anda ditambah 5.000 referensi ke daftar prefiks di semua tabel rute subnet Anda. Jika Anda membagikan daftar awalan dengan AWS akun lain, referensi akun lain ke daftar awalan Anda dihitung terhadap kuota ini.

Jaringan ACLs

Nama	Default	Dapat disesuaikan	Komentar
Jaringan untuk ACLs 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 (dengan 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	5.000	Ya	Kuota ini berlaku untuk individu Akun AWS VPCs dan bersama VPCs. Batas ini diberlakukan per Availability Zone (AZ). Jika, misalnya, antarmuka jaringan dalam tiga AZs, setiap AZ akan memiliki

Nama	Default	Dapat disesuaikan	Komentar
			batas 5.000 batas 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 peningkatan kuota untuk tabel rute, Anda mungkin juga ingin meminta peningkatan kuota untuk subnet. Sementara tabel rute dapat dibagi dengan beberapa subnet, subnet hanya dapat dikaitkan dengan tabel rute tunggal.
Rute per tabel rute (rute yang tidak disebar)	500	Ya	Anda dapat menambah kuota ini hingga maksimum 1.000; namun, performa jaringan mungkin terkena dampaknya. Kuota ini diberlakukan secara terpisah untuk IPv4 rute dan IPv6 rute. 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 disebar per tabel rute	100	Tidak	Jika Anda memerlukan prefiks tambahan, iklankan rute default.

Server rute

Nama	Default	Dapat disesuaikan	Komentar
Rute server untuk VPC	5	Ya. Untuk meminta kenaikan, buka kasus peningkatan an batas layanan menggunakan AWS Support Center Console.	
Rute titik akhir server per server rute	10	Ya. Untuk meminta kenaikan, buka kasus peningkatan an batas layanan menggunakan AWS Support Center Console.	

Nama	Default	Dapat disesuaikan	Komentar
Sesi peering per antarmuka jaringan	20	Ya. Untuk meminta kenaikan, buka kasus peningkatan batas layanan menggunakan AWS Support Center Console.	
Rute titik akhir server 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 rute server peer	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	2.500	Ya	Kuota ini berlaku untuk individu Akun AWS VPCs dan bersama VPCs. 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 IPv4 aturan dan IPv6 aturan. Untuk akun dengan kuota default 60 aturan, grup keamanan dapat memiliki 60 aturan masuk untuk IPv4 lalu lintas 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 untuk aturan per grup keamanan tidak boleh melebihi 1.000.

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 subnet dalam VPC dapat dibagikan . 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 CIDRs dalam daftar awalan terkelola. NAU adalah metrik yang diterapkan pada 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 layanan mereka.

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 intra-wilayahnya mengintip . VPCs VPCs yang diintip di berbagai Wilayah tidak berkontribusi pada jumlah ini.

EC2 Pelambatan API Amazon

Untuk informasi tentang EC2 pembatasan Amazon, lihat [Meminta pembatasan 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 AWS Direct Connect](#) dalam Panduan Pengguna AWS Direct Connect
- [Kuota mengintip dalam Panduan](#) Peering VPC Amazon
- [PrivateLink kuota](#) dalam Panduan AWS PrivateLink
- [Site-to-Site Kuota VPN](#) di AWS Site-to-Site VPN Panduan Pengguna
- [Kuota Pencerninan Lalu Lintas di Panduan](#) Pencerninan Lalu Lintas Amazon VPC

- [Kuota gateway transit](#) di Panduan Gerbang Transit VPC Amazon

Riwayat dokumen

Tabel berikut menjelaskan perubahan penting dalam setiap rilis Panduan Pengguna Amazon VPC.

Perubahan	Deskripsi	Tanggal
Perutean dinamis di VPC Anda menggunakan Amazon VPC Route Server	Amazon VPC Route Server menyederhanakan perutean untuk lalu lintas antara beban kerja yang digunakan dalam VPC dan gateway internetnya. Dengan fitur ini, VPC Route Server secara dinamis memperbarui VPC dan tabel rute gateway dengan pilihan IPv4 atau IPv6 rute Anda untuk mencapai toleransi kesalahan perutean untuk beban kerja tersebut. Ini memungkinkan Anda untuk secara otomatis mengalihkan lalu lintas dalam VPC, yang meningkatkan pengelolaan perutean VPC dan interoperabilitas dengan beban kerja pihak ketiga.	Maret 31, 2025
AWS pembaruan kebijakan terkelola	Amazon VPC memperbarui AmazonVPCFullAccess and AmazonVPCReadOnlyAccess kebijakan terkelola.	Desember 9, 2024
Dukungan kebijakan deklaratif untuk VPC BPA	Jika Anda menggunakan AWS Organizations untuk mengelola akun di organisasi, Anda dapat menggunakan kebijakan deklaratif untuk	Desember 1, 2024

menerapkan BPA VPC pada akun di organisasi.

[Akses Publik Blok VPC \(BPA\)](#)

VPC Block Public Access (BPA) memungkinkan Anda memblokir sumber daya VPCs dan subnet yang Anda miliki di suatu Wilayah agar tidak menjangkau atau dijangkau dari internet melalui gateway internet dan gateway internet khusus pintu masuk.

November 19, 2024

[Grup Keamanan Bersama](#)

Fitur ini memungkinkan Anda untuk berbagi grup keamanan dengan akun AWS Organizations lainnya.

Oktober 30, 2024

[Asosiasi VPC Grup Keamanan](#)

Fitur ini memungkinkan Anda untuk mengaitkan grup keamanan dengan beberapa VPCs di Wilayah yang sama.

Oktober 30, 2024

[Dukungan MTU gateway NAT](#)

Gateway NAT mendukung lalu lintas dengan unit transmisi maksimum (MTU) 8500.

September 10, 2024

[IPv6 Pengalamatan pribadi](#)

Informasi tentang IPv6 pengalamatan pribadi telah ditambahkan. IPv6 Alamat pribadi hanya tersedia di Amazon VPC IP Address Manager.

Agustus 8, 2024

IPv6 waktu sewa yang disukai	Anda sekarang dapat memilih seberapa sering instance yang sedang berjalan dengan yang IPv6 ditugaskan kepadanya melalui perpanjangan DHCPv6 sewa.	Februari 20, 2024
Panduan tinjauan struktur dan perbaikan	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 and AmazonVPCReadOnlyAccess kebijakan terkelola.	Februari 8, 2024
AWS pembaruan kebijakan terkelola	Amazon VPC memperbarui AmazonVPCCrossAccountNetworkInterfaceOperations kebijakan terkelola.	25 September 2023
EC2-Classic tidak digunakan lagi	Dengan EC2 -Classic, EC2 instance berjalan dalam satu jaringan datar yang dibagikan dengan pelanggan lain. Amazon VPC menggantikan EC2 -Klasik. Dengan Amazon VPC, instans Anda berjalan di cloud pribadi virtual (VPC) yang secara logis terisolasi untuk Anda. Akun AWS	31 Juli 2023

[Tambahkan IPv4 alamat sekunder ke gateway NAT](#)

Anda dapat menambahkan IPv4 alamat pribadi sekunder ke gateway NAT publik dan pribadi. IPv4 Alamat 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 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

[IPv6 konfigurasi router gateway default](#)

Tiga IPv6 alamat sekarang dicadangkan untuk digunakan oleh router VPC default.

11 November 2022

[Mentransfer alamat IP Elastis](#)

Anda sekarang dapat mentransfer alamat IP Elastis 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 Aliran ke Amazon Data Firehose	Anda dapat menentukan aliran pengiriman Amazon Data Firehose sebagai tujuan untuk data log aliran.	8 September 2022
Bandwidth gateway NAT	Gateway NAT sekarang mendukung bandwidth hingga 100 Gbps (peningkatan dari 45 Gbps) dan dapat memproses hingga sepuluh juta paket per detik (naik dari empat juta paket).	15 Juni 2022
Beberapa IPv6 blok 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 ke IPv6 IPv4	Gateway NAT mendukung terjemahan alamat jaringan dari IPv6 ke IPv4, yang dikenal sebagai. NAT64	24 November 2021
IPv6-hanya subnet di VPCs	Anda dapat membuat subnet IPv6 -only di mana Anda dapat meluncurkan instance IPv6 EC2 -only.	23 November 2021

[Opsi pengiriman VPC Flow
Logs ke Amazon S3](#)

Anda dapat menentukan format file log Apache Parquet, partisi per jam, dan awalan S3 yang kompatibel dengan HIVE.

13 Oktober 2021

[Tampilan EC2 Global Amazon](#)

Amazon EC2 Global View memungkinkan Anda untuk melihat VPCs, subnet, instans, grup keamanan, dan volume di beberapa AWS Wilayah dalam satu konsol.

1 September 2021

[Rute yang lebih spesifik](#)

Anda dapat menambahkan rute ke tabel rute Anda yang lebih spesifik daripada rute lokal. Anda dapat menggunakan rute yang lebih spesifik untuk mengarahkan lalu lintas antar subnet dalam VPC (lalu lintas Timur-Barat) ke alat middlebox. Anda dapat mengatur tujuan rute agar sesuai dengan seluruh IPv4 atau IPv6 CIDR blok subnet di VPC Anda.

Agustus 30, 2021

[Dukungan sumber daya IDs
dan 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

Gateway NAT pribadi	Anda dapat menggunakan gateway NAT pribadi untuk komunikasi pribadi khusus keluar antara atau VPCs antara VPC dan jaringan lokal Anda.	10 Juni 2021
Tag pada 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
Penyempurnaan log aliran	Bidang log aliran baru tersedia, dan Anda dapat menentukan format kustom untuk log aliran yang diterbitkan ke CloudWatch Log.	4 Mei 2020
Menandai dukungan untuk log aliran	Anda dapat menambahkan tag ke log alur Anda.	16 Maret 2020
Tag 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 Anda VPCs dari Amazon Virtual Private Cloud Console.	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
Penyempurnaan 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 AWS sama.	27 November 2018
Buat subnet default	Anda dapat membuat sebuah subnet default di sebuah Availability Zone yang tidak memiliki subnet.	9 November 2017
Menandai dukungan 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 menambahkan deskripsi ke aturan grup keamanan.	31 Agustus 2017

Blok IPv4 CIDR sekunder untuk VPC Anda	Anda dapat menambahkan beberapa blok IPv4 CIDR ke 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
IPv6 dukungan	Anda dapat mengaitkan blok IPv6 CIDR dengan VPC Anda dan IPv6 menetapkan alamat 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
Gateway 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 menggunakan ClassicLink untuk menautkan instans EC2 -Classic Anda ke VPC di akun Anda. Anda dapat mengaitkan grup keamanan VPC dengan instans EC2 -Classic, memungkinkan komunikasi antara instans EC2 -Classic dan instance di VPC Anda menggunakan alamat IP pribadi.	7 Januari 2015
Gunakan zona yang dihosting pribadi	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
Memodifikasi 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 mengaktifkan nama host DNS.	11 Maret 2013

VPC Dimana-mana

Menambahkan dukungan untuk VPC di lima AWS Wilayah, VPCs di beberapa Availability Zone, beberapa VPCs per AWS akun, dan beberapa koneksi VPN per VPC.

3 Agustus 2011

Instans Khusus

Instans Khusus adalah instans Amazon EC2 yang diluncurkan 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.