aws

Panduan Pengguna

Amazon Virtual Private Cloud

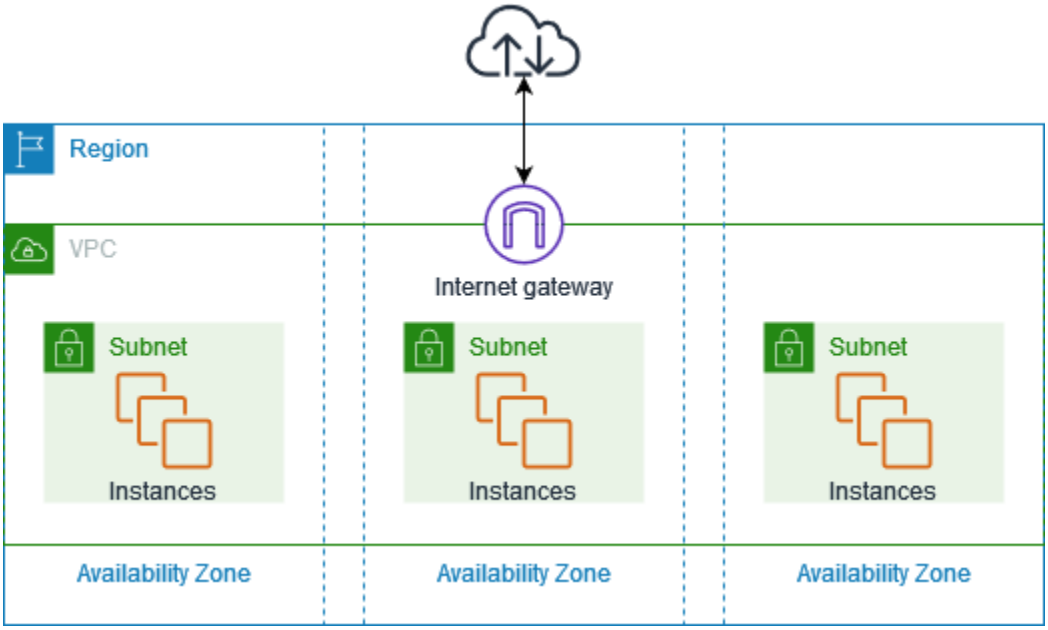
Amazon Virtual Private Cloud: Panduan Pengguna

Table of Contents

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, instans EC2 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 VPC dan subnet Anda. Anda juga dapat membawa alamat IPv4 publik dan alamat IPv6 GUA ke dan mengalokasikannya ke sumber daya di VPC Anda, seperti instans EC2, gateway NAT, AWS 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 dalam dua VPC.

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 VPC, koneksi VPN, dan AWS Direct Connect koneksi Anda.

Log Alur VPC

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

Koneksi VPN

Hubungkan VPC Anda 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 VPC default Anda dikonfigurasi sedemikian rupa sehingga Anda dapat segera mulai meluncurkan dan menghubungkan ke instans EC2. Untuk informasi selengkapnya, lihat Memulai .

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

Bekerja dengan Amazon VPC

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

- AWS Management Console — Menyediakan antarmuka web yang dapat Anda gunakan untuk mengakses VPC Anda.
- 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 SDK — Menyediakan API khusus bahasa dan menangani banyak detail koneksi, seperti menghitung tanda tangan, menangani percobaan ulang permintaan, dan penanganan kesalahan. Untuk informasi selengkapnya, lihat AWS SDK.
- 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 API Amazon EC2.

Harga untuk Amazon VPC

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

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

Harga untuk alamat IPv4 publik

Alamat IPv4 publik adalah alamat IPv4 yang dapat dirutekan dari internet. Alamat IPv4 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 alamat IPv4 publik tanpa biaya. Jika Anda tidak menggunakan Tingkat AWS Gratis, alamat IPv4 Publik dikenakan biaya. Untuk informasi harga tertentu, lihat tab Alamat IPv4 Publik di Harga Amazon VPC.

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

Alamat IPv4 publik memiliki jenis berikut:

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

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

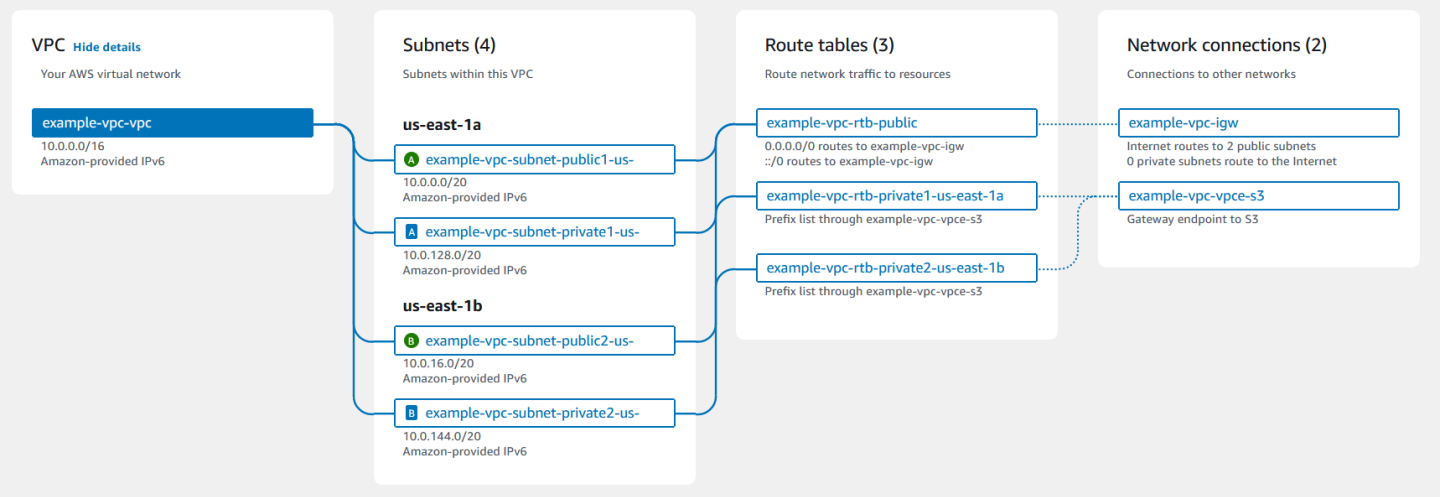
- Amazon AppStream 2.0
- AWS Client VPN
- AWS Database Migration Service
- Amazon EC2
- Amazon Elastic Container Service
- Amazon EKS
- Amazon EMR

- Amazon GameLift
- 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 IPv6 CIDR yang disediakan Amazon, 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

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

- AWS jaringan global pribadi

VPC dan subnet

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

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

Pelajari selengkapnya

- Penentuan alamat IP
- Virtual private cloud
- Subnet

VPC default dan nondefault

Jika akun Anda dibuat setelah 4 Desember 2013, 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 di VPC Anda Oleh karena itu, instans EC2 yang diluncurkan di subnet default secara otomatis memiliki akses ke internet. Jika Anda memiliki VPC default di Wilayah dan Anda tidak menentukan subnet saat meluncurkan instans EC2 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 “VPC default”
- the section called “Buat VPC”

Tabel rute

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

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

Pelajari selengkapnya

- Konfigurasikan tabel rute

Mengakses internet

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

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

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

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

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

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

Pelajari selengkapnya

- Connect ke internet menggunakan gateway internet
- Aktifkan lalu lintas IPv6 keluar menggunakan gateway internet khusus egres
- 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 koneksi AWS Site-to-Site VPN IPsec, menjadikan AWS Cloud sebagai perpanjangan dari pusat data Anda.

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

Pelajari selengkapnya

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

Connect VPC dan jaringan

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

Anda juga dapat membuat transit gateway dan menggunakannya untuk menghubungkan VPC dan jaringan on-premise Anda. Gateway transit bertindak sebagai router virtual Regional untuk lalu lintas yang mengalir di antara lampirannya, yang dapat mencakup VPC, koneksi VPN, 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 (ISP) serta tulang punggung jaringan global privat, yang memberikan peningkatan performa jaringan untuk lalu lintas lintas Wilayah yang dikirim oleh pelanggan.

Pertimbangan berikut berlaku:

- Lalu lintas yang berada di Availability Zone, atau antara Availability Zone di semua Wilayah, rute melalui jaringan global AWS pribadi.
- Lalu lintas yang berada di antara Wilayah selalu rute melalui jaringan global AWS pribadi, kecuali untuk Wilayah China.

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%.

Memulai dengan Amazon VPC

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

Tugas

- Mendaftar untuk Akun AWS
- Memverifikasi izin
- Tentukan rentang alamat IP Anda
- Pilih 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/signup.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. 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 mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan mengunjungi https://aws.amazon.com/ 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 VPC dan subnet, Anda dapat memilih rentang alamat IP mereka. Saat Anda menyebarkan sumber daya di subnet, seperti instans EC2, 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 VPC Akun AWS dan VPC Anda. Pastikan bahwa rentang alamat IP untuk VPC Anda tidak tumpang tindih dengan rentang alamat IP untuk jaringan Anda sendiri. Jika Anda memerlukan konektivitas antara beberapa VPC, Anda harus memastikan bahwa mereka tidak memiliki alamat IP yang tumpang tindih.

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

Pilih 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. Sebagai contoh:

- 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 VPC dan subnet yang Anda butuhkan, blok CIDR apa yang akan ditetapkan ke VPC dan subnet Anda, 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.

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

Lingkungan pengembangan atau pengujian

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

Pengalamatan IP untuk VPC dan subnet Anda

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

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

- Alamat IPv4 individu adalah 32 bit, dengan 4 kelompok hingga 3 digit desimal. Misalnya, 10.0.1.0.
- Blok IPv4 CIDR memiliki empat kelompok hingga tiga digit desimal, 0-255, dipisahkan oleh titik, diikuti oleh garis miring dan angka dari 0 hingga 32. Misalnya, 10.0.0.0/16.
- Alamat IPv6 individu adalah 128 bit, dengan 8 kelompok 4 digit heksadesimal. Misalnya, 2001:0 db 8:85 a 3:0000:0000:8 a2e: 0370:7334.
- Blok CIDR IPv6 memiliki empat kelompok hingga empat digit heksadesimal, dipisahkan oleh titik dua, diikuti oleh titik dua, diikuti oleh garis miring dan angka dari 1 hingga 128. Misalnya, 2001:db 8:1234:1 a00: :/56.

Untuk informasi lebih lanjut, lihat Apa itu CIDR?

Daftar Isi

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 dan IPv6) dan konfigurasi khusus IPv6, lihat. Layanan yang mendukung IPv6

Karakteristik	IPv4	IPv6
Ukuran VPC	Hingga 5 CIDR dari /16 hingga /28. Kuota ini dapat disesuaikan.	Hingga 5 CIDR 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 mengalokasikan blok CIDR dari Amazon VPC IP Address Manager (IPAM). Untuk informasi lebih lanjut, lihat Apa itu IPAM? di Panduan Pengguna Amazon VPC IPAM.	Anda dapat membawa blok IPv6 CIDR Anda sendiri untuk VPC AWS Anda, memilih blok CIDR IPv6 yang disediakan Amazon, atau Anda dapat mengalokasikan blok CIDR dari Amazon VPC IP Address Manager (IPAM). Untuk informasi lebih lanjut, lihat Apa itu IPAM? di Panduan Pengguna Amazon VPC IPAM.
Akses internet	Membutuhkan gateway internet.	Membutuhkan gateway internet. Mendukung komunikasi outbound-only menggunakan gateway internet khusus egres.
Alamat IP elastis	Didukung. Memberikan instance EC2 alamat IPv4 publik statis permanen.	Tidak didukung. EIP menjaga alamat IPv4 publik dari sebuah instans statis saat instance restart. Alamat IPv6 bersifat statis secara default.
Gateway NAT	Didukung. Contoh dalam subnet pribadi dapat terhubung ke internet menggunakan gateway NAT publik	Didukung. Anda dapat menggunakan gateway NAT dengan NAT64 untuk mengaktifkan instance di subnet

Karakteristik	IPv4	IPv6
	atau ke sumber daya di VPC lain menggunakan gateway NAT pribadi.	khusus IPv6 untuk berkomunikasi dengan sumber daya khusus IPv4 dalam VPC, antara VPC, di jaringan lokal Anda, 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.

Alamat IPv4 privat

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

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

Kami merujuk ke alamat IP privat sebagai alamat IP yang berada dalam rentang CIDR IPv4 VPC. Sebagian besar rentang alamat IP VPC jatuh dalam rentang alamat IP privat (yang tidak dapat dirutekan secara publik) yang ditentukan di RFC 1918; namun, Anda dapat menggunakan blok CIDR publik untuk VPC Anda. Terlepas dari rentang alamat IP VPC Anda, kami tidak mendukung akses langsung ke internet dari blok CIDR VPC Anda, termasuk blok CIDR yang dapat dirutekan secara

publik. Anda harus mengatur akses internet melalui gateway; misalnya, gateway internet, gateway pribadi virtual, AWS Site-to-Site VPN koneksi, atau AWS Direct Connect.

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

Alamat IPv4 publik

Semua subnet memiliki atribut yang menentukan apakah antarmuka jaringan yang dibuat di subnet secara otomatis menerima alamat IPv4 publik (juga disebut sebagai alamat IP publik dalam topik ini). Oleh karena itu, ketika Anda meluncurkan sebuah instans ke subnet yang mengaktifkan atribut seperti ini, alamat IP publik ditetapkan ke antarmuka jaringan primer (eth0) yang dibuat untuk instans tersebut. Alamat IP publik dipetakan ke alamat IP privat primer melalui terjemahan alamat jaringan (NAT).

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

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

- Memodifikasi atribut pengalamatan IP publik dari subnet Anda. Untuk informasi selengkapnya, lihat Memodifikasi atribut pengalamatan IPv4 publik untuk 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 Pengguna Amazon EC2.

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

Jika Anda memerlukan alamat IP publik yang persisten yang dialokasikan ke akun Anda dan yang dapat ditetapkan ke dan dilepaskan dari instans sesuai kebutuhan, gunakan alamat IP Elastis. Untuk informasi selengkapnya, lihat 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.

Alamat IPv6

Atau, Anda dapat mengaitkan blok CIDR IPv6 dengan VPC Anda, dan mengaitkan blok CIDR IPv6 dengan subnet Anda. Untuk informasi selengkapnya, lihat topik berikut.

- Tambahkan blok CIDR IPv6 ke VPC Anda
- Tambahkan blok CIDR IPv6 ke subnet Anda

Alamat IPv6 bersifat unik secara global dan dapat dikonfigurasi agar tetap privat atau dapat dijangkau melalui Internet. Instans Anda menerima alamat IPv6 jika blok CIDR IPv6 dikaitkan dengan VPC dan subnet Anda, dan jika salah satu dari pernyataan berikut adalah benar:

- Subnet Anda dikonfigurasi untuk secara otomatis menetapkan alamat IPv6 ke sebuah instans selama peluncuran. Untuk informasi selengkapnya, lihat Memodifikasi atribut pengalamatan IPv6 untuk subnet Anda.
- Anda menetapkan alamat IPv6 ke instans Anda selama peluncuran.
- Anda menetapkan alamat IPv6 ke antarmuka jaringan primer instans Anda setelah peluncuran.
- Anda menetapkan alamat IPv6 ke antarmuka jaringan di subnet yang sama, dan menyertakan antarmuka jaringan ke instans Anda setelah peluncuran.

Saat instans Anda menerima alamat IPv6 selama peluncuran, alamat tersebut dikaitkan dengan antarmuka jaringan primer (eth0) dari instans. Anda dapat mengelola alamat IPv6 untuk antarmuka jaringan primer instans Anda (eth0) dengan cara berikut:

- Tetapkan dan batalkan penetapan alamat IPv6 dari antarmuka jaringan. Jumlah alamat IPv6 yang dapat Anda tetapkan ke antarmuka jaringan dan jumlah antarmuka jaringan yang dapat Anda

sertakan ke sebuah instans bervariasi tergantung tipe instans. Untuk informasi selengkapnya, lihat alamat IP per antarmuka jaringan per jenis instans di Panduan Pengguna Amazon EC2.

- Aktifkan alamat IPv6 primer. Alamat IPv6 primer memungkinkan Anda untuk menghindari mengganggu lalu lintas ke instans atau ENI. Untuk informasi selengkapnya, lihat Membuat antarmuka jaringan dan Mengelola alamat IP di Panduan Pengguna Amazon EC2.

Alamat IPv6 tetap ada saat Anda menghentikan dan memulai, atau menghibernasikan dan memulai instans Anda, dan akan dilepas saat Anda menghentikan instans. Anda tidak dapat menetapkan ulang alamat IPv6 saat ditetapkan ke antarmuka jaringan lain—Anda harus membatalkan penetapannya terlebih dahulu.

Anda dapat mengontrol apakah instans dapat dicapai melalui alamat IPv6 mereka dengan mengontrol perutean untuk subnet Anda, atau dengan menggunakan grup keamanan dan aturan ACL jaringan. Untuk informasi selengkapnya, lihat Privasi lalu lintas antar jaringan di Amazon VPC.

Untuk informasi selengkapnya tentang rentang alamat IPv6 yang disimpan, lihat Daftar Alamat Tujuan Khusus IANA IPv6 dan RFC4291.

Gunakan Alamat IP Anda sendiri

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

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

Gunakan Manajer Alamat IP 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 CIDR alamat IP ke VPC 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 CIDR IPv4 terkait. Anda dapat secara opsional mengaitkan blok IPv4 CIDR tambahan dan satu atau lebih blok CIDR IPv6. Untuk informasi selengkapnya, lihat Pengalamatan IP untuk VPC dan subnet Anda.

Daftar Isi

Blok CIDR IPv4 VPC

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

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

Rentang RFC 1918	Contoh Blok CIDR
10.0.0.0 - 10.255.255.255 (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. Untuk menghindari konflik di masa depan, jangan gunakan rentang ini saat membuat VPC Anda. Misalnya,

layanan seperti AWS Cloud9 atau Amazon SageMaker dapat mengalami konflik alamat IP jika rentang alamat `172.17.0.0/16` IP sudah digunakan di mana saja di jaringan Anda. Untuk informasi selengkapnya, lihat Tidak dapat terhubung ke lingkungan EC2 karena alamat IP VPC digunakan oleh Docker di Panduan Pengguna.AWS Cloud9

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

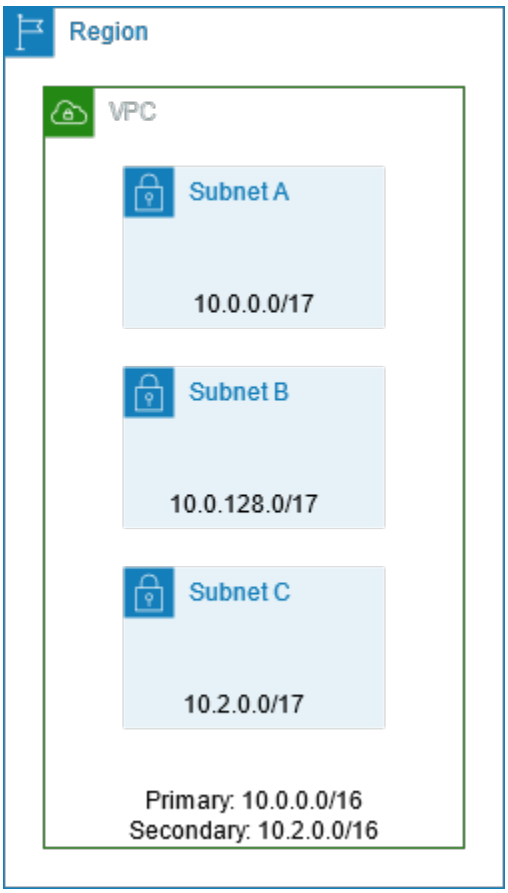
Saat Anda membuat VPC untuk digunakan dengan AWS layanan, periksa dokumentasi layanan untuk memverifikasi apakah ada persyaratan khusus untuk konfigurasinya.

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

Dalam contoh berikut, VPC memiliki blok CIDR primer dan sekunder. Blok CIDR untuk Subnet A dan Subnet B berasal dari blok 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 pembatasan pada rentang alamat IPv4 yang dapat Anda gunakan. Untuk informasi selengkapnya, lihat Pembatasan pengaitan blok CIDR IPv4.
- Anda tidak dapat menambah atau mengurangi ukuran blok CIDR yang ada.

- Anda memiliki kuota pada jumlah blok CIDR yang dapat Anda kaitkan dengan VPC dan pada jumlah rute yang dapat Anda tambahkan ke tabel rute. Anda tidak dapat mengaitkan blok CIDR jika hal ini membuat Anda melebihi kuota Anda. Untuk informasi selengkapnya, lihat Kuota Amazon VPC.
- Blok CIDR tidak boleh sama besar atau lebih besar dari kisaran CIDR tujuan di sebuah rute di salah satu tabel rute VPC. Sebagai contoh, dalam sebuah VPC dimana blok CIDR utama adalah `10.2.0.0/16`, Anda memiliki rute yang ada dalam tabel rute dengan tujuan `10.0.0.0/24` ke virtual private gateway. Anda ingin mengaitkan blok CIDR sekunder di rentang `10.0.0.0/16`. Karena rute yang ada, Anda tidak dapat mengaitkan blok CIDR `10.0.0.0/24` atau yang lebih besar. Namun, Anda dapat mengaitkan blok CIDR sekunder `10.0.0.0/25` atau yang lebih kecil.
- Aturan berikut berlaku saat Anda menambahkan blok CIDR IPv4 ke VPC yang merupakan bagian dari koneksi peering VPC:
  - Jika koneksi peering VPC `active`, Anda dapat menambahkan blok CIDR ke VPC asalkan blok-blok tersebut tidak tumpang tindih dengan blok CIDR dari VPC rekan.
  - Jika koneksi peering VPC adalah `pending-acceptance`, pemilik peminta VPC tidak dapat menambahkan blok CIDR ke VPC, terlepas apakah blok tumpang tindih dengan blok CIDR dari VPC penerima. Baik pemilik VPC penerima harus menerima koneksi peering, atau pemilik VPC peminta harus menghapus permintaan koneksi peering VPC, menambahkan blok CIDR, dan kemudian meminta koneksi peering VPC.
  - Jika koneksi peering VPC adalah `pending-acceptance`, pemilik VPC penerimsa dapat menambahkan blok CIDR ke VPC. Jika blok CIDR sekunder tumpang tindih dengan blok CIDR dari VPC peminta, permintaan koneksi peering VPC mengintip menjadi gagal dan tidak dapat diterima.
- Jika Anda menggunakan AWS Direct Connect untuk terhubung ke beberapa VPC melalui gateway Direct Connect, VPC yang terkait dengan gateway Direct Connect tidak boleh memiliki blok CIDR yang tumpang tindih. Jika Anda menambahkan blok CIDR ke VPC yang dikaitkan dengan gateway Direct Connect, pastikan bahwa blok CIDR yang baru tidak tumpang tindih dengan blok CIDR yang sudah ada dari VPC manapun yang dikaitkan lainnya. Untuk informasi selengkapnya, lihat Gateway Direct Connect di Panduan Pengguna 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 VPC Anda, pilih kotak centang untuk VPC Anda, dan pilih tab CIDR. Untuk melihat CIDR utama menggunakan AWS CLI, gunakan perintah deskripsi-vpcs sebagai berikut. CIDR utama dikembalikan di tingkat atas`CidrBlock element`.

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

Berikut ini adalah output contoh.

```
10.0.0.0/16
```

Pembatasan pengaitan blok CIDR IPv4

Tabel berikut memberikan 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 netmask /16 dan /28 netmask dari rentang 100.64.0.0/10.
169.254.0.0/16	Blok CIDR dari blok “tautan lokal” dicadangkan seperti yang dijelaska	

Rentang alamat IP	Asosiasi terbatas	Asosiasi yang diizinkan
	n dalam RFC 5735 dan tidak dapat ditetapkan ke VPC.	
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 netmask /16 dan /28 netmask dari rentang 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 netmask /16 dan /28 netmask dari rentang 100.64.0.0/10.

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

Blok CIDR IPv6 VPC

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

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

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

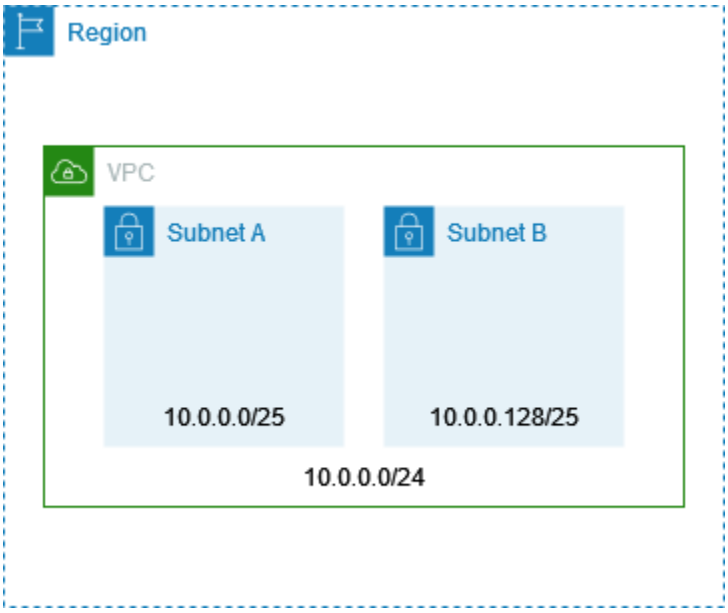
Anda dapat memisahkan blok IPv6 CIDR dari VPC. Setelah Anda memutus pengaitan blok CIDR IPv6 dari sebuah VPC, Anda tidak dapat mengharapkan untuk menerima CIDR yang sama jika Anda mengaitkan blok CIDR IPv6 dengan VPC Anda lagi nanti.

Blok 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 men-support 256 alamat IP. Anda dapat memecahkan blok CIDR ini menjadi dua subnet, masing-masing mendukung 128 alamat IP. Satu subnet menggunakan blok CIDR `10.0.0.0/25` (untuk alamat `10.0.0.0` - `10.0.0.127`) dan yang lain menggunakan blok CIDR `10.0.0.128/25` (untuk alamat `10.0.0.128` - `10.0.0.255`).



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

Ukuran subnet untuk IPv4

Ukuran blok IPv4 CIDR yang diizinkan untuk subnet adalah antara netmask dan netmask. `/28` `/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 instans EC2. Sebagai contoh, dalam sebuah subnet dengan blok CIDR `10.0.0.0/24`, lima alamat IP berikut dicadangkan:

- 10.0.0.0: Alamat jaringan.
- 10.0.0.1: Dicadangkan oleh AWS untuk router VPC.

- 10.0.0.2: Dicadangkan oleh. AWS Alamat IP server DNS adalah basis rentang jaringan VPC plus dua. Untuk VPC dengan beberapa blok CIDR, alamat IP server DNS terletak di CIDR utama. Kami juga mencadangkan basis setiap rentang subnet ditambah dua untuk semua blok CIDR di VPC. Untuk informasi selengkapnya, lihat Server Amazon DNS.
- 10.0.0.3: Dicadangkan 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 alamat IPv4 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 CIDR IPv6 dengan VPC Anda, Anda dapat mengaitkan blok CIDR IPv6 dengan subnet yang ada di VPC Anda, atau saat Anda membuat subnet baru. Kemungkinan panjang netmask IPv6 adalah antara `/44` dan `/64` secara bertahap. `/4`

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

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

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

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

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

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

Grup CIDR memblokir menggunakan daftar awalan terkelola

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

Ada dua tipe daftar prefiks:

- 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

- Bekerja dengan daftar prefiks bersama
- Sebutkan daftar prefiks di sumber daya AWS Anda

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 prefiks mendukung satu jenis pengalamatan IP saja (IPv4 atau IPv6). Anda tidak dapat menggabungkan blok CIDR IPv4 dan IPv6 dalam satu daftar prefiks.
- Daftar prefiks hanya berlaku untuk Wilayah tempat Anda membuatnya.
- Ketika Anda membuat daftar prefiks, Anda harus menentukan jumlah maksimum entri yang dapat didukung oleh daftar prefiks tersebut.
- Ketika Anda menyebutkan daftar prefiks di suatu sumber daya, jumlah maksimum entri untuk daftar prefiks tersebut dihitung berdasarkan kuota untuk jumlah entri untuk sumber daya tersebut. Sebagai contoh, jika Anda membuat daftar prefiks dengan maksimum 20 entri dan Anda sebutkan daftar prefiks tersebut dalam aturan grup keamanan, ini dianggap sebagai 20 aturan grup keamanan.
- Ketika Anda menyebutkan daftar prefiks dalam tabel rute, maka aturan rute prioritas akan berlaku. Untuk informasi selengkapnya, lihat Prioritas rute dan daftar awalan.
- Anda dapat memodifikasi 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 China).

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 Amazon VPC dan sumber daya dan kunci syarat yang dapat Anda gunakan di kebijakan IAM, lihat Tindakan, Sumber Daya, dan Kunci Syarat untuk Amazon EC2 di Panduan Pengguna IAM.

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

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

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

Bekerja dengan daftar prefiks yang dikelola konsumen

Anda dapat membuat dan mengelola daftar awalan yang dikelola pelanggan. Anda dapat melihat AWS daftar awalan -managed.

Tugas

- Membuat daftar prefiks
- Lihat daftar prefiks
- Melihat entri untuk daftar prefiks
- Melihat asosiasi (referensi) untuk daftar prefiks Anda
- Memodifikasi daftar awalan
- Ubah ukuran daftar awalan
- Memulihkan versi sebelumnya dari daftar prefiks
- Menghapus daftar prefiks

Membuat daftar prefiks

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

Batasan

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

Untuk membuat daftar prefiks menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Daftar Prefiks yang Dikelola.
3. Pilih Buat daftar prefiks.
4. Untuk Nama daftar prefiks, masukkan nama untuk daftar prefiks.
5. Untuk Entri maksimum, masukkan jumlah maksimum entri untuk daftar prefiks.
6. Untuk Keluarga alamat, pilih apakah daftar prefiks mendukung entri IPv4 atau IPv6.

7. Untuk Entri daftar prefiks, pilih Tambahkan entri baru, dan masukkan blok CIDR dan deskripsi untuk entri tersebut. Ulangi langkah ini untuk setiap entri.
8. (Opsional) Untuk Tag, tambahkan tag ke daftar prefiks untuk membantu Anda untuk mengidentifikasinya nanti.
9. Pilih Buat daftar prefiks.

Untuk membuat daftar awalan menggunakan AWS CLI

Gunakan perintah create-managed-prefix-list.

Lihat daftar prefiks

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

Untuk melihat daftar prefiks menggunakan konsol

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

Untuk melihat entri untuk daftar awalan menggunakan AWS CLI

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

Melihat asosiasi (referensi) untuk daftar prefiks Anda

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

Batasan

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

Untuk melihat asosiasi daftar prefiks menggunakan konsol ini

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

Untuk melihat asosiasi daftar awalan menggunakan AWS CLI

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

Memodifikasi daftar awalan

Anda dapat mengubah nama daftar prefiks Anda, dan Anda dapat menambahkan atau menghapus entri. Untuk mengubah jumlah maksimum entri, lihatUbah 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 Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Daftar Prefiks yang Dikelola.
3. Pilih kotak centang untuk daftar awalan, dan pilih Tindakan, Ubah daftar awalan.
4. Untuk Nama daftar prefiks, masukkan nama baru untuk daftar prefiks.
5. 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 Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Daftar Prefiks yang Dikelola.
3. Pilih kotak centang untuk daftar awalan, dan pilih Tindakan, Ubah ukuran daftar awalan.
4. Untuk entri maks baru, masukkan nilai.
5. Pilih Ubah Ukuran.

Untuk mengubah ukuran daftar awalan menggunakan AWS CLI

Gunakan perintah modify-managed-prefix-list.

Memulihkan versi sebelumnya dari daftar prefiks

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

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

Untuk memulihkan versi sebelumnya dari daftar prefiks menggunakan konsol ini

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

Untuk menghapus daftar awalan menggunakan AWS CLI

Gunakan perintah delete-managed-prefix-list.

Bekerja dengan daftar awalan AWS-managed

AWS Daftar awalan terkelola adalah kumpulan rentang alamat IP untuk AWS layanan.

Daftar Isi

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 Sebutkan daftar prefiks di sumber daya AWS Anda.

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.

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. *wilayah* .dynamodb	1
AWS Ground Station	com.amazonaws.global.groundstation	5
Rute Amazon 53	com.amazonaws. *wilayah* .ipv6.route53-healthchecks	25
	com.amazonaws. *wilayah* .route53-healthchecks	25
Amazon S3	com.amazonaws.*wilayah*.s3	1
Amazon S3 Express Satu Zona	com.amazonaws. *wilayah* .s3express	6
Kisi VPC Amazon	com.amazonaws. *wilayah* .vpc-kisi	10
	com.amazonaws. *wilayah* .ipv6.vpc-kisi	10

Untuk melihat daftar awalan AWS-managed menggunakan konsol

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

Untuk melihat 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
```

Bekerja dengan daftar prefiks bersama

Dengan AWS Resource Access Manager (AWS RAM), pemilik daftar awalan 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 di sumber daya mereka. AWS

Untuk informasi selengkapnya AWS RAM, lihat Panduan AWS RAM Pengguna.

Daftar Isi

Prasyarat untuk membagikan daftar prefiks

- 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 .

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.

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

Mengidentifikasi daftar prefiks bersama

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

Untuk mengidentifikasi daftar prefiks bersama menggunakan konsol Amazon VPC

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

Untuk mengidentifikasi daftar awalan bersama menggunakan AWS CLI

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

Mengidentifikasi referensi ke daftar prefiks bersama

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

Untuk mengidentifikasi referensi ke daftar prefiks bersama menggunakan konsol Amazon VPC

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

Untuk mengidentifikasi referensi ke daftar awalan bersama menggunakan AWS CLI

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

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.

Izin daftar prefiks bersama

Izin untuk pemilik

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

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

Izin untuk konsumen

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

Tagihan dan pengukuran

Tidak ada biaya tambahan untuk membagikan daftar prefiks.

Kuota untuk AWS RAM

Untuk informasi selengkapnya, lihat Kuota layanan.

Sebutkan daftar prefiks di sumber daya AWS Anda

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.

Untuk menyebutkan daftar prefiks dalam aturan grup keamanan menggunakan konsol ini

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di 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 ke dalam) atau Tujuan (aturan keluar), pilih ID dari daftar prefiks.
6. Pilih Simpan aturan.

Untuk mereferensikan daftar awalan dalam aturan grup keamanan menggunakan AWS CLI

Gunakan authorize-security-group-ingressdan authorize-security-group-egressperintah. Untuk parameter `--ip-permissions`, tentukan ID dari daftar prefiks menggunakan `PrefixListIds`.

Tabel rute subnet

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

Untuk menyebutkan daftar prefiks dalam tabel rute menggunakan konsol ini

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

Untuk mereferensikan daftar awalan dalam tabel rute menggunakan AWS CLI

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

Tabel rute transit gateway

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

AWS Network Firewall kelompok aturan

Grup AWS Network Firewall aturan adalah seperangkat kriteria yang dapat digunakan kembali untuk memeriksa dan menangani lalu lintas jaringan. Jika Anda membuat grup aturan 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 CIDR yang sering

Anda gunakan dalam daftar awalan dan mereferensikan daftar ini sebagai target rute di tabel rute gateway lokal Anda. Untuk informasi selengkapnya, lihat 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 AWS layanan.

> **Note**
>
> - Hanya beberapa rentang alamat IP AWS layanan yang diterbitkan di ip-ranges.json; kami mempublikasikan rentang alamat IP untuk layanan yang biasanya ingin dilakukan oleh pelanggan untuk melakukan pemfilteran jalan keluar.
> - Layanan dapat menggunakan rentang alamat IP untuk berkomunikasi dengan layanan atau layanan lain dapat menggunakan rentang IP untuk berkomunikasi dengan jaringan pelanggan.

Untuk melihat rentang saat ini, unduh file `.json`. Untuk mempertahankan riwayat, simpan versi file `.json` secara berurutan di sistem Anda. 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.

Rentang alamat IP yang Anda bawa AWS membawa alamat IP Anda sendiri (BYOIP) tidak termasuk dalam file. `.json`

Atau, 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

- Memfilter file JSON
- Menerapkan kontrol jalan keluar
- AWS Pemberitahuan rentang alamat IP
- Catatan rilis
- Pelajari selengkapnya

Unduh

Unduh 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.

Sintaks

Sintaks `ip-ranges.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.

Jenis: String

Contoh: `"syncToken": "1416435608"`

createDate

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

Jenis: String

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

prefiks

Prefiks IP untuk rentang alamat IPv4.

Jenis: Array

ipv6_prefixes

Prefiks IP untuk rentang alamat IPv6.

Jenis: Array

ip_prefix

Rentang alamat IPv4 publik, dalam notasi CIDR. Perhatikan bahwa AWS mungkin mengiklankan awalan dalam rentang yang lebih spesifik. Misalnya, 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.

Jenis: String

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

ipv6_prefix

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

Jenis: 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.

Jenis: 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.

Jenis: String

Nilai yang valid: `af-south-1` `ap-east-1` `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` | `ca-central-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` | `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).

Jenis: String

Nilai yang valid: `AMAZON` `AMAZON_APPFLOW` | `AMAZON_CONNECT` | `API_GATEWAY` | `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 layanan dan `S3` kode layanan. `EC2` 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.

Memfilter file JSON

Anda dapat mengunduh alat baris perintah untuk membantu Anda memfilter informasi sesuai dengan apa yang Anda cari.

Windows

AWS Tools for Windows PowerShell menyertakan cmdlet, `Get-AWSPublicIpAddressRange`, untuk mengurai file JSON. Contoh berikut menunjukkan penggunaannya. Untuk informasi selengkapnya, lihat Menanyakan Rentang Alamat IP Publik untuk AWS dan Dapatkan-AWSPublicIpAddressRange.

Example 1. Dapatkan tanggal pembuatan

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

Wednesday, August 22, 2018 9:22:35 PM
```

Example 2. Dapatkan informasi untuk Wilayah tertentu

```
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
...
```

Example 3. Dapatkan semua alamat IP

```
PS C:\> (Get-AWSPublicIpAddressRange).IpPrefix
23.20.0.0/14
27.0.0.0/22
43.250.192.0/24
...
2406:da00:ff00::/64
2600:1fff:6000::/40
2a01:578:3::/64
2600:9000::/28
```

Example 4. Dapatkan semua alamat IPv4

```
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
...
```

Example 5. Dapatkan semua alamat IPv6

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

IpPrefix
--------
```

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

Example 6. Dapatkan semua alamat IP untuk layanan tertentu

```
PS C:\> Get-AWSPublicIpAddressRange -ServiceKey CODEBUILD | select IpPrefix

IpPrefix
--------
52.47.73.72/29
13.55.255.216/29
52.15.247.208/29
...
```

Linux

Contoh perintah berikut menggunakan alat jq untuk mengurai salinan lokal file JSON.

Example 1. Dapatkan tanggal pembuatan

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

"2016-02-18-17-22-15"
```

Example 2. Dapatkan informasi untuk Wilayah tertentu

```
$ 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"
},
...
```

Example 3. Dapatkan semua alamat IPv4

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

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

Example 4. Dapatkan semua alamat IPv6

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

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

Example 5. Dapatkan semua alamat IPv4 untuk layanan tertentu

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

52.47.73.72/29
13.55.255.216/29
52.15.247.208/29
...
```

Example 6. Dapatkan semua alamat IPv4 untuk layanan tertentu di Wilayah tertentu

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

34.228.4.208/28
```

Example 7. Dapatkan informasi untuk grup perbatasan jaringan tertentu

```
$ jq -r '.prefixes[] | select(.region=="us-west-2") |
 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
...
```

Menerapkan 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 di atas EC2 dan menggunakan ruang alamat IP EC2. Jika Anda memblokir lalu lintas ke ruang alamat IP EC2, Anda memblokir lalu lintas ke layanan non-EC2 ini juga.

AWS Pemberitahuan rentang alamat IP

Setiap kali ada perubahan pada rentang alamat AWS IP, kami mengirim pemberitahuan ke pelanggan `AmazonIpSpaceChanged` topik. Muatan 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`.

Jika Anda ingin diberi tahu setiap kali ada perubahan pada rentang alamat AWS IP, Anda dapat berlangganan sebagai berikut untuk menerima pemberitahuan menggunakan Amazon SNS.

Untuk berlangganan pemberitahuan rentang alamat AWS IP

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home.
2. Di bilah navigasi, ubah Wilayah menjadi AS Timur (Virginia Utara), jika perlu. Anda harus memilih Wilayah ini karena notifikasi SNS tempat Anda berlangganan dibuat di Wilayah ini.
3. Di panel navigasi, pilih Langganan.
4. Pilih Buat langganan.
5. Di kotak dialog Create subscription (Buat langganan), lakukan hal berikut:
   a. Untuk Topic ARN (ARN Topik), salin Amazon Resource Name (ARN) berikut:

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

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

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

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

Untuk berhenti berlangganan dari AWS pemberitahuan rentang alamat IP

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

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

Catatan rilis

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

Deskripsi	Tanggal rilis
Menambahkan kode layanan `IVS_REALTIME` .	Juni 11, 2024
Menambahkan kode layanan `MEDIA_PACKAGE_V2` .	9 Mei 2023
Menambahkan kode layanan `CLOUDFRONT_ORIGIN_FACING` .	Oktober 12, 2021
Menambahkan kode layanan `ROUTE53_RESOLVER` .	24 Juni 2021
Menambahkan kode layanan `EBS`.	12 Mei 2021

Deskripsi	Tanggal rilis
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 `WORKSPACES_GATEWAYS` .	30 Maret 2020
Menambahkan kode layanan `ROUTE53_HEALTHCHECK_PUBLISHING` .	30 Januari 2020
Menambahkan kode layanan `API_GATEWAY` .	26 September 2019
Menambahkan kode layanan `EC2_INSTANCE_CONNECT` .	26 Juni 2019
Menambahkan kode layanan `DYNAMODB`.	25 April 2019
Menambahkan kode layanan `GLOBALACCELERATOR` .	20 Desember 2018
Menambahkan kode layanan `AMAZON_CONNECT` .	20 Juni 2018
Menambahkan kode layanan `CLOUD9`.	20 Juni 2018
Menambahkan kode layanan `CODEBUILD` .	19 April 2018
Menambahkan kode layanan `S3`.	28 Februari 2017

Deskripsi	Tanggal rilis
Menambahkan dukungan untuk rentang alamat IPv6.	22 Agustus 2016
Rilis awal	19 November 2014

Pelajari selengkapnya

- `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`— Alamat IPV4 Publik
- `EC2_INSTANCE_CONNECT`— Prasyarat Connect Instans EC2
- `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 PCoIP

Tambahkan dukungan IPv6 ke VPC Anda

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

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

Pertimbangan

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

Proses

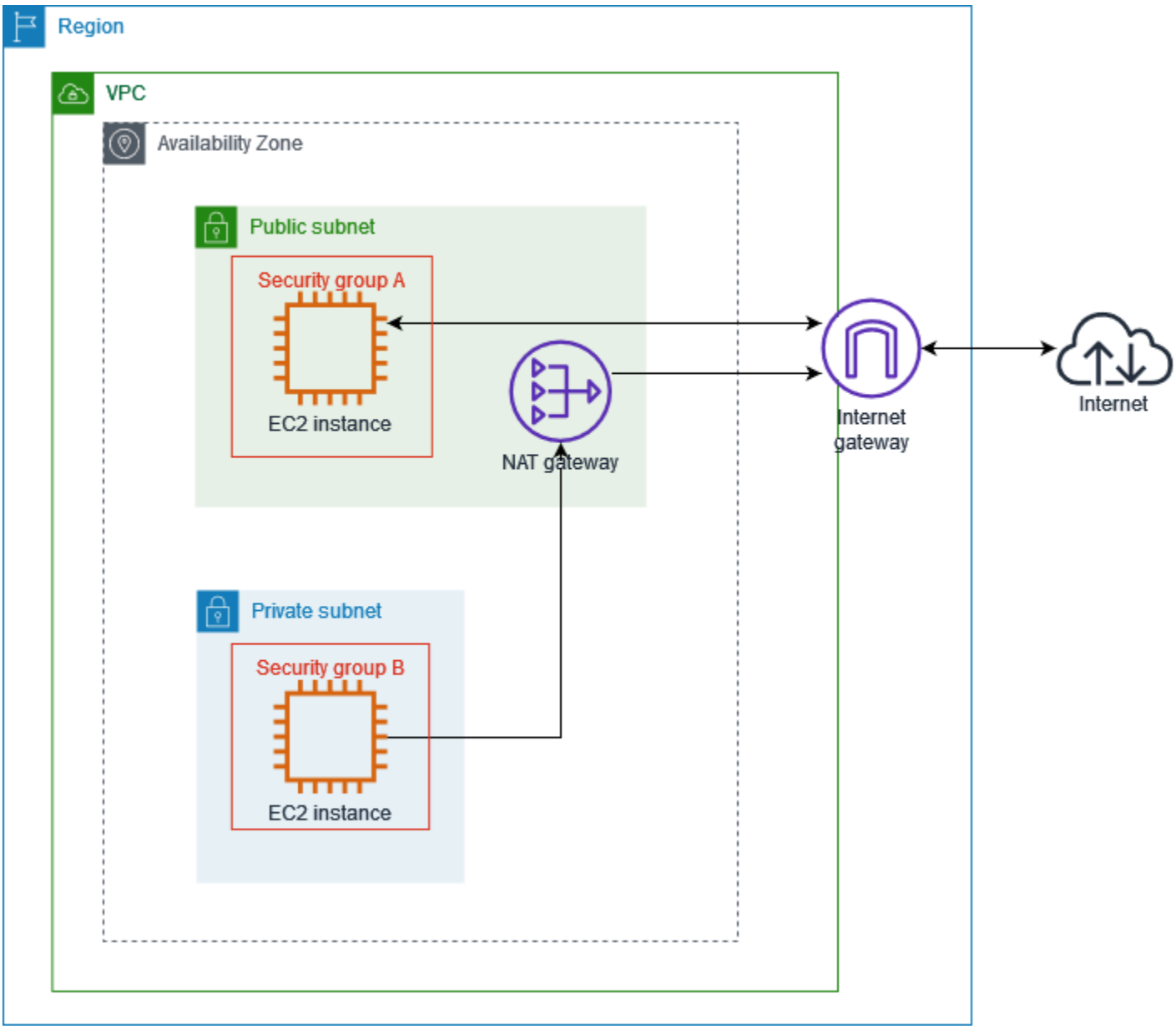
Tabel berikut memberikan ikhtisar proses untuk mengaktifkan IPv6 untuk VPC Anda.

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

Langkah	Catatan
Langkah 4: Tetapkan alamat IPv6 ke instans Anda	Anda menetapkan alamat IPv6 ke instans Anda dari rentang alamat IPv6 subnet Anda.

Contoh: Aktifkan IPv6 di VPC dengan subnet publik dan privat

Dalam contoh ini, VPC Anda memiliki subnet publik dan privat. Anda memiliki instans basis data di subnet privat Anda yang memiliki komunikasi keluar dengan internet melalui gateway NAT di VPC Anda. Anda memiliki server web yang menghadap publik di subnet publik Anda yang memiliki akses internet melalui gateway internet. Diagram berikut merupakan arsitektur VPC Anda.



Grup keamanan untuk server web Anda (misalnya dengan ID grup keamanan`sg-11aa22bb11aa22bb1`) memiliki aturan masuk berikut:

Jenis	Protokol	Jangkauan pelabuhan	Sumber	Komentar
Semua Lalu lintas	Semua	Semua	sg-33cc44 dd33cc44dd3	Memungkinkan akses masuk untuk semua lalu lintas dari

Jenis	Protokol	Jangkauan pelabuhan	Sumber	Komentar
				instans yang terkait dengan sg-33cc44 dd33cc44dd3 (instans basis data).
HTTP	TCP	80	0.0.0.0/0	Memungkinkan lalu lintas masuk dari internet melalui HTTP.
HTTPS	TCP	443	0.0.0.0/0	Memungkinkan lalu lintas masuk dari internet melalui HTTPS.
SSH	TCP	22	203.0.113 .123/32	Memungkin kan akses SSH masuk dari komputer lokal Anda; misalnya, ketika Anda perlu untuk terhubung ke instans Anda untuk melakukan tugas-tugas administrasi.

Grup keamanan untuk instance database Anda (misalnya dengan ID grup keamanan`sg-33cc44dd33cc44dd3`) memiliki aturan masuk berikut:

Jenis	Protokol	Jangkauan pelabuhan	Sumber	Komentar
MySQL	TCP	3306	sg-11aa22 bb11aa22bb1	Memungkinkan akses masuk untuk lalu lintas MySQL dari instans yang terkait dengan sg-11aa22 bb11aa22bb1 (instans server web).

Kedua grup keamanan memiliki aturan keluar default yang mengizinkan semua lalu lintas IPv4 ke luar, dan tidak ada aturan keluar lainnya.

Server web Anda adalah tipe instans `t2.medium`. Server basis data Anda adalah `m3.large`.

Anda ingin VPC dan sumber daya Anda untuk diaktifkan untuk IPv6, dan Anda ingin keduanya beroperasi dalam mode dual-stack; dengan kata lain, Anda ingin menggunakan kedua pengalamatan IPv6 dan IPv4 antara sumber daya di VPC Anda dan sumber daya melalui internet.

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

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

Untuk mengaitkan Blok CIDR IPv6 dengan VPC

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih VPC Anda.
3. Pilih VPC Anda.
4. Pilih Actions, Edit CIDR dan kemudian pilih Add new IPv6 CIDR.
5. Pilih salah satu opsi berikut, lalu pilih Pilih CIDR:

- Blok CIDR IPv6 yang disediakan Amazon - Gunakan blok CIDR IPv6 dari kumpulan alamat IPv6 Amazon. Untuk Grup Perbatasan Jaringan, pilih grup tempat AWS mengiklankan alamat IP.
- Blok IPv6 CIDR yang dialokasikan IPAM — Gunakan blok CIDR IPv6 dari kolam IPAM. Pilih kolam IPAM dan blok IPv6 CIDR.
- IPv6 CIDR yang dimiliki oleh saya - Gunakan blok CIDR IPv6 dari kumpulan alamat IPv6 Anda (BYOIP). Pilih kumpulan alamat IPv6 dan blok IPv6 CIDR.

6. Pilih Tutup.

Untuk mengaitkan Blok CIDR IPv6 dengan subnet

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Pengguna.
3. Pilih subnet.
4. Pilih Actions, Edit IPv6 CIDR 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 Blok CIDR IPv6 VPC.

Langkah 2: Perbarui tabel rute VPC Anda

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

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

Untuk memperbarui tabel rute untuk subnet publik

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

2. Di panel navigasi, pilih Pengguna. Pilih subnet publik. Pada tab tabel 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 Amazon VPC 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 lalu lintas IPv6 keluar menggunakan gateway internet khusus egres.
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.

Untuk informasi selengkapnya, lihat Opsi perutean contoh.

Langkah 3: Perbarui aturan grup keamanan Anda

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

Untuk memperbarui aturan grup keamanan masuk

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

2. Di panel navigasi, pilih Grup keamanan dan pilih grup keamanan server web Anda.
3. Di tab Aturan masuk, pilih Edit aturan masuk.
4. Untuk setiap aturan yang memungkinkan lalu lintas IPv4, pilih Tambahkan aturan dan konfigurasikan aturan untuk mengizinkan lalu lintas IPv6 yang sesuai. Misalnya, untuk menambahkan aturan yang memungkinkan semua lalu lintas HTTP melalui IPv6, pilih HTTP untuk Jenis dan Sumber**::/0**.
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 asal untuk grup keamanan Anda, aturan ini tidak secara otomatis ditambahkan, dan Anda harus menambahkan aturan keluar setara untuk lalu lintas IPv6.

Memperbarui aturan ACL jaringan Anda

Saat Anda mengaitkan blok IPv6 CIDR dengan VPC, kami secara otomatis menambahkan aturan ke ACL jaringan default untuk memungkinkan lalu lintas IPv6. Namun, jika Anda memodifikasi ACL jaringan default atau jika Anda telah membuat ACL jaringan khusus, Anda harus menambahkan aturan secara manual untuk lalu lintas IPv6. Untuk informasi selengkapnya, lihat Bekerja dengan ACL jaringan.

Langkah 4: Tetapkan alamat IPv6 ke instans Anda

Semua tipe instans generasi saat ini yang mendukung IPv6. Jika jenis instans Anda tidak mendukung IPv6, Anda harus mengubah ukuran instance menjadi tipe instans yang didukung sebelum 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 Pengguna Amazon EC2. Jika Anda harus meluncurkan instance dari AMI baru untuk mendukung IPv6, Anda dapat menetapkan alamat IPv6 ke instans Anda selama peluncuran.

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

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

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

AWS Layanan yang mendukung IPv6

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

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

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

Layanan yang mendukung IPv6

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

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Titik akhir publik mendukung IPv6	Titik akhir pribadi mendukung IPv6 1
AWS App Mesh	Ya	Ya	Ya	Tidak
Amazon AppStream 2.0	Ya	Tidak	Tidak	Tidak
Amazon Athena	Ya	Tidak	Ya	Ya
Amazon Aurora	Y	Tidak	Ya	Tidak
AWS Cloud9	Y	Tidak	Ya	
Amazon CloudFront	Y	Tidak	Tidak	

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Titik akhir publik mendukung IPv6	Titik akhir pribadi mendukung IPv6 1
CloudWatch Log Amazon	 Y	 Tidak	 Ya	 Tidak
AWS Cloud Map	 Y	 Ya	 Ya	 Ya
AWS Awan WAN	 Ya	 Tidak	 Ya	 Tidak
Amazon Cognito	 Ya	 Tidak	 Ya	
AWS Database Migration Service	 Y	 Tidak	 Tidak	 Tidak
AWS Direct Connect	 Ya	 Ya	 Tidak	

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Titik akhir publik mendukung IPv6	Titik akhir pribadi mendukung IPv6 1
Amazon EC2	 Y	 Ya	 Y	 Tidak
Amazon ECS	 Y	 Tidak	 Tidak	 Tidak
Amazon EKS	Node: Ya/Pod: Tidak	Pod: Ya/Node: Tidak	 Tidak	 Tidak
Penyeimbang Beban Elastis	Load balancer: Ya Grup target: Tidak	Load balancer: Tidak Ada Grup target: Ya	 Tidak	 Tidak
Amazon ElastiCache	 Y	 Ya	 Tidak	 Tidak
AWS Fargate	 Y	 Tidak	 Tidak	 Tidak

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Titik akhir publik mendukung IPv6	Titik akhir pribadi mendukung IPv6 [1]
AWS Global Accelerator		 Tidak	 Tidak	
AWS Glue	 Tidak	 Tidak	 Tidak	 Ya
AWS IoT	 Ya	 Tidak		 Tidak
AWS Lake Formation	 Tidak	 Tidak	 Tidak	 Ya
AWS Lambda		 Tidak		 Tidak
Amazon Lightsail			 Tidak	

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Titik akhir publik mendukung IPv6	Titik akhir pribadi mendukung IPv6 1
AWS Network Firewall	 Y	 Y	 Tidak	
OpenSearch Layanan Amazon	 Y	 Tidak	 Ya	 Tidak
AWS PrivateLink	 Ya	 Ya	 Ya	
Amazon RDS	 Y	 Tidak	 Ya	 Tidak
Amazon Route 53	 Ya	 Ya	 Tidak	
Amazon S3	 Y	 Tidak	 Y	 Tidak

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Titik akhir publik mendukung IPv6	Titik akhir pribadi mendukung IPv6 1
AWS Secrets Manager	Ya	Tidak	Y	Tidak
AWS Shield	Ya	Ya	Tidak	
AWS Site-to-Site VPN	Y	Tidak	Y	Tidak
AWS Transit Gateway	Ya	Tidak	Ya	Tidak
Amazon VPC	Y	Ya	Y	Tidak
AWS WAF	Y	Ya	Tidak	

Nama layanan	Dukungan tumpukan ganda	IPv6 hanya mendukung	Titik akhir publik mendukung IPv6	Titik akhir pribadi mendukung IPv6 [1]
Amazon WorkSpaces		Y  Tidak	 Tidak	 Tidak

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

Dukungan IPv6 tambahan

Hitung

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

Jaringan dan Pengiriman Konten

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

Keamanan, Identitas, dan Kepatuhan

- AWS Identity and Access Management (IAM) mendukung alamat IPv6 dalam kebijakan IAM.
- Amazon Macie mendukung alamat IPv6 dalam informasi identitas pribadi (PII).

Pengelolaan dan Tata Kelola

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

Pelajari selengkapnya

- IPv6 aktif AWS
- Arsitektur Referensi VPC Amazon Dual Stack dan IPv6 saja (PDF)

Awan pribadi virtual (VPC)

Virtual Private Cloud (VPC) adalah jaringan virtual yang didedikasikan untuk Anda. Akun AWS VPC diisolasi secara logis dari jaringan virtual lain di AWS Cloud. Anda dapat meluncurkan AWS sumber daya, seperti instans Amazon EC2, ke dalam VPC Anda.

Akun Anda berisi VPC default untuk setiap AWS Wilayah. Anda juga dapat membuat VPC tambahan.

Daftar Isi

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

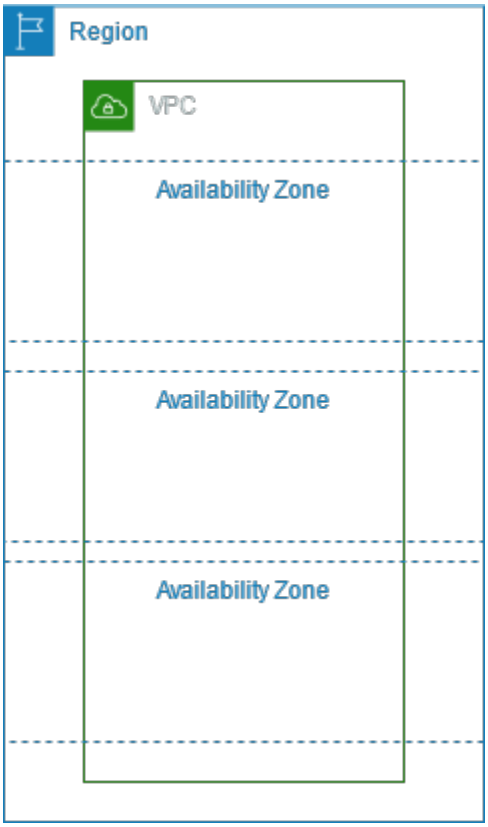
Saat Anda membuat VPC, Anda menentukan alamat IP-nya sebagai berikut:

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

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

Diagram VPC

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



Sumber daya VPC

Setiap VPC secara otomatis dilengkapi dengan sumber daya berikut:

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

Anda dapat membuat sumber daya berikut untuk VPC Anda:

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

VPC default

Saat Anda mulai menggunakan Amazon VPC, Anda memiliki VPC default di masing-masingAWSWilayah. 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 instans Amazon EC2 ke VPC default. Anda juga dapat menggunakan layanan seperti Elastic Load Balancing, Amazon RDS, dan Amazon EMR di VPC default Anda.

VPC default cocok untuk memulai dengan cepat dan untuk meluncurkan 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

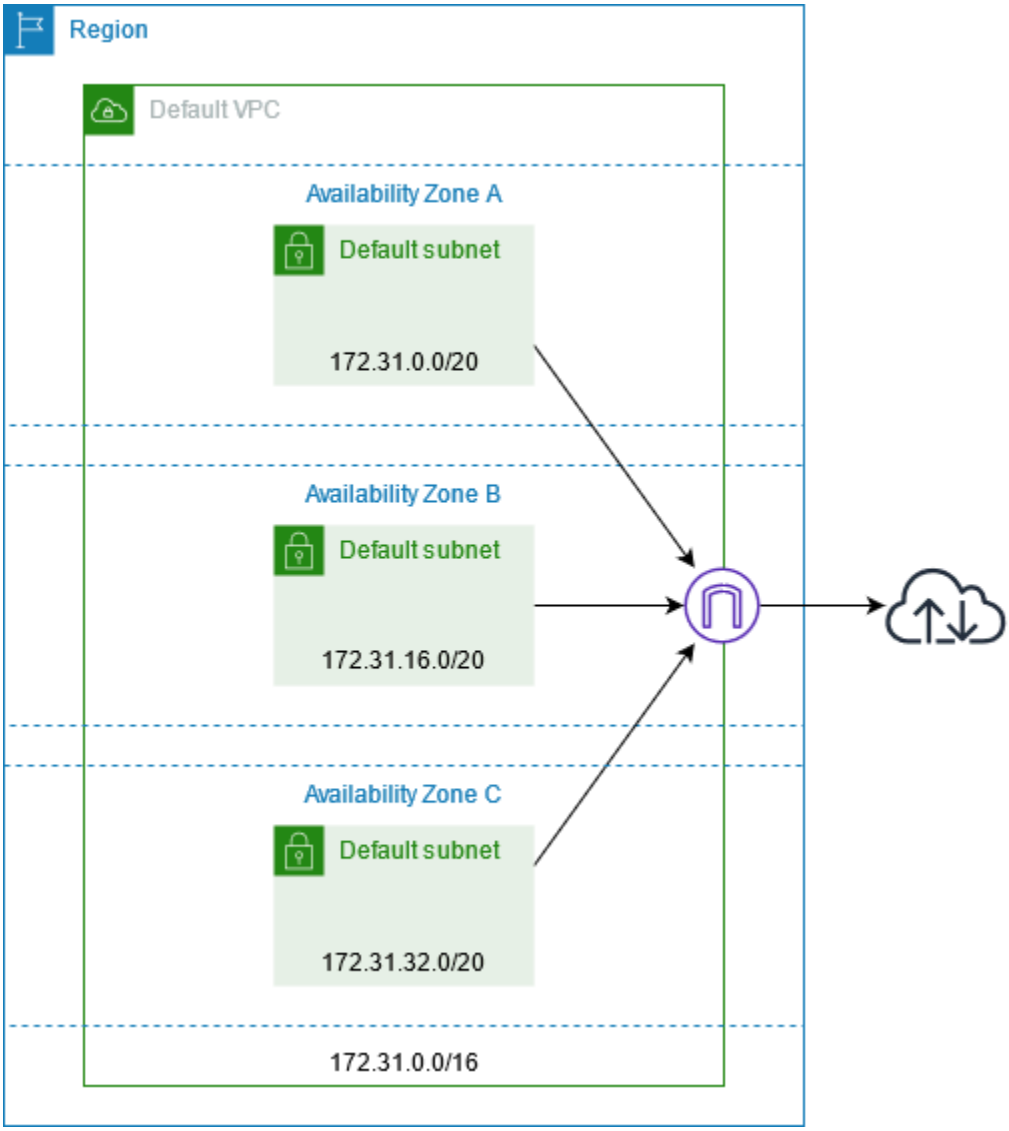
Ketika kita membuat VPC default, kita melakukan hal berikut untuk menyiapkannya untuk Anda:

- Membuat VPC dengan ukuran blok CIDR IPv4 `/16` (`172.31.0.0/16`). Tindakan ini menyediakan 65.536 alamat IPv4 privat.

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

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	*internet_gateway_id*

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

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

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

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

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

Subnet default

Secara default, suatu subnet default adalah subnet publik, karena tabel rute utama mengirimkan lalu lintas subnet yang ditujukan untuk internet ke gateway internet. Anda dapat membuat subnet default ke subnet privat dengan menghapus rute dari tujuan 0.0.0.0/0 ke gateway internet. Namun, jika Anda melakukan ini, tidak ada instans EC2 berjalan di subnet tersebut yang dapat mengakses internet.

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

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

Menampilkan VPC default dan subnet default

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

Untuk melihat VPC dan subnet default Anda menggunakan konsol

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

Untuk mendeskripsikan VPC default Anda menggunakan baris perintah

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

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

Untuk mendeskripsikan subnet default Anda menggunakan baris perintah

- Gunakan describe-subnets (AWS CLI)
- Gunakan Get-EC2Subnet (AWS Tools for Windows PowerShell)

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

Membuat VPC default

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

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

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

Untuk membuat VPC default menggunakan konsol

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

Untuk membuat VPC default menggunakan baris perintah

Anda dapat menggunakancreate-default-vpc AWS CLIperintah. Perintah ini tidak memiliki parameter input.

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

Berikut ini adalah keluaran contoh.

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

Atau, Anda dapat menggunakanBaru-EC2DefaultVpcAlat untuk WindowsPowerShellperintah atauCreateDefaultVpcTindakan API Amazon EC2.

Membuat subnet default

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.

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

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

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

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

Anda tidak dapat membuat subnet default menggunakan AWS Management Console.

Untuk membuat subnet default menggunakan AWS CLI

Gunakancreate-default-subnet AWS CLIperintah dan menentukan Availability Zone di mana untuk membuat subnet.

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

Berikut ini adalah contoh output.

```
{
    "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 Pengguna AWS Command Line Interface.

Atau, Anda dapat menggunakanBaru-EC2DefaultSubnetAlat untuk WindowsPowerShellperintah atauCreateDefaultSubnetTindakan API Amazon EC2.

Menampilkan subnet default dan VPC default

Anda dapat menghapus subnet default atau VPC default sebagaimana Anda menghapus subnet atau VPC lainnya. Namun, jika Anda menghapus subnet default atau VPC default, Anda harus secara eksplisit menentukan subnet di salah satu VPC Anda saat meluncurkan instance. Jika Anda tidak memiliki VPC lain, Anda harus membuat VPC dengan subnet di setidaknya satu 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 Memodifikasi atribut pengalamatan IPv4 publik untuk 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

Untuk informasi tentang melihat atau memodifikasi VPC, lihat. the section called “Mengkonfigurasi VPC Anda”

Opsi konfigurasi VPC

Anda dapat menentukan opsi konfigurasi berikut saat membuat VPC.

Zona Ketersediaan

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

Blok CIDR

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

Opsi DNS

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

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

gateway internet

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 *nama* format - *sumber daya*.

Gateway NAT

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

Tabel rute

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

Subnet

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

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

Untuk informasi selengkapnya, lihat Subnet.

Penghunian

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

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 Amazon VPC 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 alamat IPv4 untuk VPC. VPC harus memiliki rentang alamat IPv4.
6. (Opsional) Untuk mendukung lalu lintas IPv6, pilih blok CIDR IPv6, blok CIDR IPv6 yang disediakan Amazon.
7. Pilih opsi Sewa. Opsi ini menentukan apakah instans EC2 yang Anda luncurkan ke VPC akan berjalan pada perangkat keras yang dibagikan dengan perangkat keras lain Akun AWS atau pada perangkat keras yang didedikasikan untuk penggunaan Anda saja. Jika Anda memilih penyewaan VPC yang `Default` akan menjadi, instans EC2 yang diluncurkan ke VPC ini akan menggunakan atribut penyewaan yang ditentukan saat Anda meluncurkan instance. Untuk informasi selengkapnya, lihat Meluncurkan instance menggunakan parameter yang ditentukan

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. Untuk Jumlah Availability Zones (AZ), sebaiknya Anda menyediakan subnet di setidaknya dua Availability Zone untuk lingkungan produksi. Untuk memilih AZ untuk subnet Anda, perluas Kustomisasi AZ. 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 AZ 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.
11. (Opsional) Jika sumber daya dalam 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 VPC Gateway di Panduan.AWS PrivateLink
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 Amazon VPC 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 alamat IPv4 untuk VPC Anda.
   - Pilih blok IPv4 CIDR yang dialokasikan IPAM, pilih kumpulan alamat IPv4 Amazon VPC IP Address Manager (IPAM) dan netmask. 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 alamat IPv6 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 IPv6 CIDR dari kolam IPAM. 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 kumpulan IPv6 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 alamat IPv6 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 netmask IPv6 adalah antara /44 dan /60 dengan kelipatan /4.

- Pilih blok IPv6 CIDR yang disediakan Amazon untuk meminta blok IPv6 CIDR dari kumpulan alamat IPv6 Amazon. 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 Panduan Pengguna Amazon EC2. 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 alamat IPv6 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 netmask IPv6 adalah antara /44 dan /60 dengan kelipatan /4.

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

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

Penandaan

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

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

Untuk membuat VPC plus sumber daya VPC dengan menggunakan AWS CLI

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

   ```
   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 CIDR IPv6 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
     ```

   - Subnet khusus IPv6 - Jika Anda membuat VPC tumpukan ganda, Anda dapat menggunakan `--ipv6-native` opsi untuk membuat subnet khusus IPv6, 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 perintah create-internet-gateway 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 attach-internet-gateway berikut. 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 perintah create-route-table 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 lalu lintas IPv4 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 perintah associate-route-table berikut. Gunakan ID tabel rute untuk subnet publik dan ID subnet publik.

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

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

   a. Buat gateway internet khusus egress dengan menggunakan perintah create-egress-only-internet-gateway berikut. 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 perintah create-route-table 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 lalu lintas IPv6 ke gateway internet khusus egres dengan menggunakan perintah create-route berikut. Gunakan ID tabel rute yang dikembalikan pada langkah sebelumnya.

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

   d. Kaitkan tabel rute dengan subnet pribadi dengan menggunakan perintah associate-route-table 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 create-nat-gateway berikut. 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 perintah create-route-table 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 lalu lintas IPv4 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 perintah associate-route-table 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
```

Mengkonfigurasi VPC Anda

Gunakan prosedur berikut untuk melihat dan mengkonfigurasi virtual private cloud (VPC) Anda.

Tugas

- Lihat detail tentang VPC Anda
- Visualisasikan sumber daya di VPC Anda
- Tambahkan blok CIDR IPv4 ke VPC Anda
- Tambahkan blok CIDR IPv6 ke VPC Anda

- Hapus blok CIDR IPv4 dari VPC Anda
- Hapus blok CIDR IPv6 dari VPC Anda

Untuk informasi tentang membuat atau menghapus VPC, the section called “Buat VPC” lihat atau. the section called “Hapus VPC Anda”

Lihat detail tentang VPC Anda

Gunakan langkah-langkah berikut untuk melihat detail tentang VPC Anda.

Untuk melihat detail VPC menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih VPC.
3. Pilih VPC, lalu pilih Lihat Detail untuk melihat detail konfigurasi VPC Anda.

Untuk mendeskripsikan VPC menggunakan AWS CLI

Gunakan perintah deskripsi-vpcs.

Untuk melihat semua VPC Anda di semua Wilayah

Buka konsol Amazon EC2 Global View di https://console.aws.amazon.com/ec2globalview/home. Untuk informasi selengkapnya, lihat Daftar dan filter sumber daya menggunakan Tampilan Global Amazon EC2 di Panduan Pengguna Amazon EC2.

Visualisasikan sumber daya di VPC Anda

Gunakan langkah-langkah berikut untuk melihat representasi visual 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 Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih VPC.
3. Pilih VPC.
4. Pilih tab Peta sumber daya untuk menampilkan visualisasi sumber daya.
5. Pilih Tampilkan detail untuk melihat detail selain ID sumber daya 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 blok CIDR IPv4 ke VPC Anda

VPC Anda dapat memiliki hingga lima blok CIDR IPv4 secara default, tetapi batas ini dapat disesuaikan. Untuk informasi selengkapnya, lihat Kuota Amazon VPC. Untuk informasi tentang pembatasan blok IPv4 CIDR untuk VPC, lihat. Blok VPC CIDR

Untuk menambahkan blok IPv4 CIDR ke VPC menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih VPC Anda.
3. Pilih VPC, lalu pilih Tindakan, Edit CIDR.
4. Pilih Tambahkan IPv4 CIDR baru.
5. Untuk blok IPv4 CIDR, lakukan salah satu hal berikut:
   - Pilih input manual IPv4 CIDR dan masukkan blok CIDR IPv4.
   - Pilih IPv4 CIDR yang dialokasikan IPAM dan pilih CIDR dari kolam IPv4 IPAM.
6. Pilih Simpan dan kemudian pilih Tutup.
7. Setelah Anda menambahkan blok IPv4 CIDR ke VPC Anda, Anda dapat membuat subnet yang menggunakan blok CIDR baru. Untuk informasi selengkapnya, lihat Membuat subnet.

Untuk mengaitkan blok IPv4 CIDR dengan VPC menggunakan AWS CLI

Gunakan perintah associate-vpc-cidr-block.

Tambahkan blok CIDR IPv6 ke VPC Anda

VPC Anda dapat memiliki hingga lima blok CIDR IPv6 secara default, tetapi batas ini dapat disesuaikan. Untuk informasi selengkapnya, lihat Kuota Amazon VPC. Untuk informasi tentang pembatasan blok IPv6 CIDR untuk VPC, lihat. Blok VPC CIDR

Untuk menambahkan blok IPv6 CIDR ke VPC menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih VPC Anda.
3. Pilih VPC, lalu pilih Tindakan, Edit CIDR.
4. Pilih Tambahkan IPv6 CIDR baru.
5. 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 IPv6 CIDR dari kolam IPAM. 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 kumpulan IPv6 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 alamat IPv6 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 netmask IPv6 adalah antara /44 dan /60 dengan kelipatan /4.

- Pilih blok IPv6 CIDR yang disediakan Amazon untuk meminta blok IPv6 CIDR dari kumpulan alamat IPv6 Amazon. 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 Amazon EC2 di Panduan Pengguna Amazon EC2. 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 alamat IPv6 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 netmask IPv6 adalah antara /44 dan /60 dengan kelipatan /4.

6. Pilih Pilih CIDR dan kemudian pilih Tutup.
7. Setelah Anda menambahkan blok IPv6 CIDR ke VPC Anda, Anda dapat membuat subnet yang menggunakan blok CIDR baru. Untuk informasi selengkapnya, lihat Membuat subnet.

Untuk mengaitkan blok IPv6 CIDR dengan VPC menggunakan AWS CLI

Gunakan perintah associate-vpc-cidr-block.

Hapus blok CIDR IPv4 dari VPC Anda

Jika VPC Anda memiliki lebih dari satu blok CIDR IPv4 yang terkait dengannya, Anda dapat menghapus blok CIDR IPv4 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.

Untuk menghapus blok CIDR dari VPC menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih VPC Anda.
3. Pilih VPC, dan pilih Tindakan, Sunting CIDR.
4. Di bawah VPC IPv4 CIDR, hapus CIDR dengan memilih Hapus.
5. Pilih Tutup.

Untuk memisahkan blok CIDR IPv4 dari VPC menggunakan AWS CLI

Gunakan perintah disassociate-vpc-cidr-block.

Hapus blok CIDR IPv6 dari VPC Anda

Jika Anda tidak lagi menginginkan dukungan IPv6 di VPC Anda, tetapi Anda ingin terus menggunakan VPC Anda untuk membuat dan berkomunikasi dengan sumber daya IPv4, Anda dapat menghapus blok IPv6 CIDR.

Untuk menghapus blok IPv6 CIDR, Anda harus terlebih dahulu membatalkan penetapan alamat IPv6 yang ditetapkan ke instans apa pun di subnet Anda.

Menghapus blok CIDR IPv6 tidak secara otomatis menghapus aturan grup keamanan, aturan ACL jaringan, atau rute tabel rute yang telah Anda konfigurasi untuk jaringan IPv6. Anda harus secara manual mengubah atau menghapus aturan-aturan atau rute-rute ini.

Untuk menghapus blok IPv6 CIDR dari VPC menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih VPC Anda.
3. Pilih VPC Anda, pilih Tindakan, Sunting CIDR.
4. Di bawah IPv6 CIDR, hapus blok CIDR IPv6 dengan memilih Hapus.
5. Pilih Tutup.

Untuk memisahkan blok CIDR IPv6 dari VPC menggunakan AWS CLI

Gunakan perintah disassociate-vpc-cidr-block.

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?

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 instans EC2 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 DHCP Amazon IPv6, perhatikan hal berikut:

- Instans EC2 dalam subnet dual-stack hanya dapat mengambil alamat IPv6 dari server IPv6 DHCP. Itu tidak dapat mengambil konfigurasi jaringan tambahan dari server IPv6 DHCP, seperti nama server DNS atau nama domain.
- Instans EC2 dalam subnet khusus IPv6 dapat mengambil alamat IPv6 dari server IPv6 DHCP dan dapat mengambil informasi konfigurasi jaringan tambahan, seperti nama server DNS dan nama domain.
- Untuk instance EC2 dalam subnet khusus IPv6, IPv4 DHCP Server akan mengembalikan 169.254.169.253 sebagai server nama jika “DNS” secara eksplisit disebutkan dalam set opsi DHCP. AmazonProvided Jika “AmazonProvidedDNS” hilang dari set opsi, IPv4 DHCP Server tidak akan mengembalikan alamat apakah server nama IPv4 lainnya disebutkan dalam set opsi atau tidak.

Server Amazon DHCP juga dapat menyediakan seluruh awalan IPv4 atau IPv6 ke antarmuka jaringan di VPC Anda menggunakan delegasi awalan (lihat Menetapkan awalan ke antarmuka

jaringan Amazon EC2 di Panduan Pengguna Amazon EC2). Delegasi awalan IPv4 tidak disediakan dalam tanggapan DHCP. Awalan IPv4 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, seperti instans EC2, 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 instans EC2 dibangun pada Sistem Nitro, AWS akan dikonfigurasi `169.254.169.253` sebagai server nama domain default.
- Untuk instans EC2 yang dibangun di Xen, tidak ada server nama domain yang akan dikonfigurasi dan, karena instance di VPC tidak memiliki akses ke server DNS, mereka tidak akan dapat mengakses internet.

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

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

Daftar Isi

Set opsi DHCP default

Set opsi DHCP default berisi pengaturan berikut:

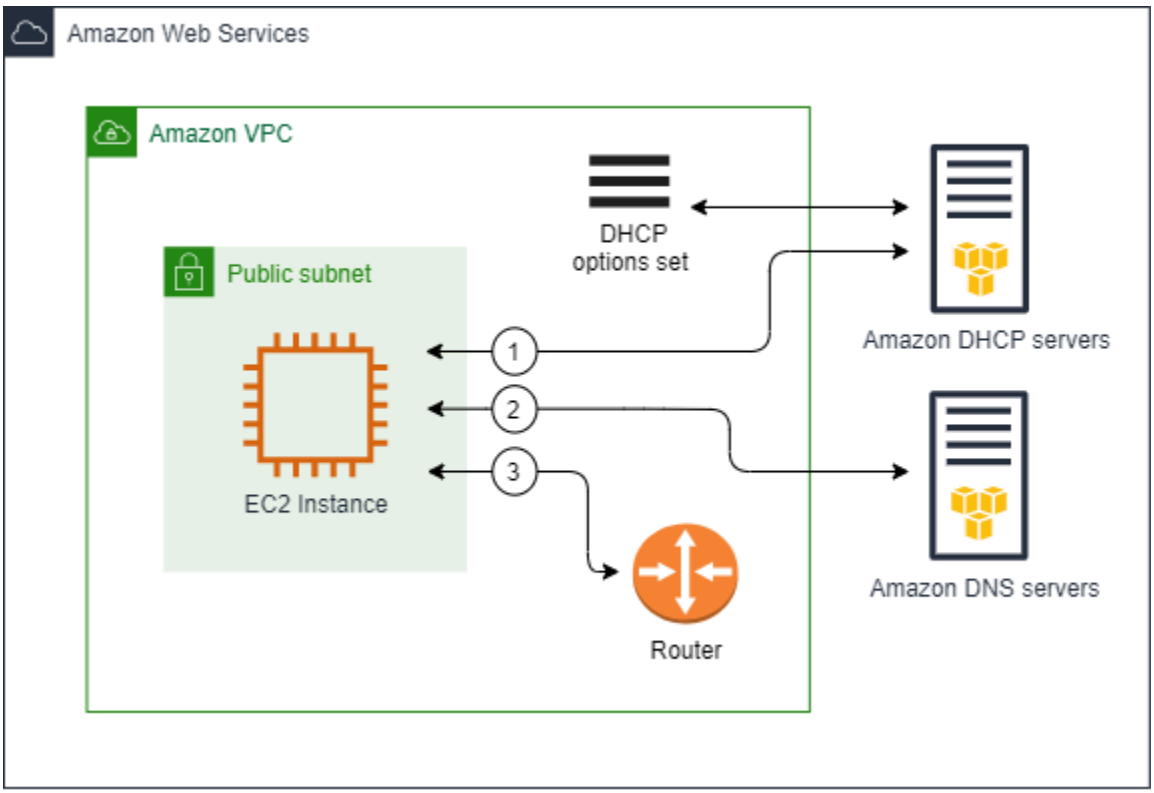
- Server nama domain: Server DNS yang digunakan antarmuka jaringan Anda untuk resolusi nama domain. Untuk set opsi DHCP default, ini selalu`AmazonProvidedDNS`. Untuk informasi selengkapnya, lihat Server Amazon DNS.

- Nama domain: Nama domain yang harus digunakan klien saat menyelesaikan nama host menggunakan Domain Name System (DNS). Untuk informasi selengkapnya tentang nama domain yang digunakan untuk instans EC2, lihat nama host instans Amazon EC2.
- IPv6 Preferred Lease Time: Seberapa sering instance yang berjalan dengan IPv6 yang ditetapkan padanya melewati perpanjangan sewa DHCPv6. 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 instans EC2:

- Server NTP: Secara default, instans EC2 menggunakan Layanan Sinkronisasi Waktu Amazon untuk mengambil waktu.
- Server nama NetBIOS: Untuk instance EC2 yang menjalankan 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: Untuk instance EC2 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 dan pengaturan jaringan tambahan.



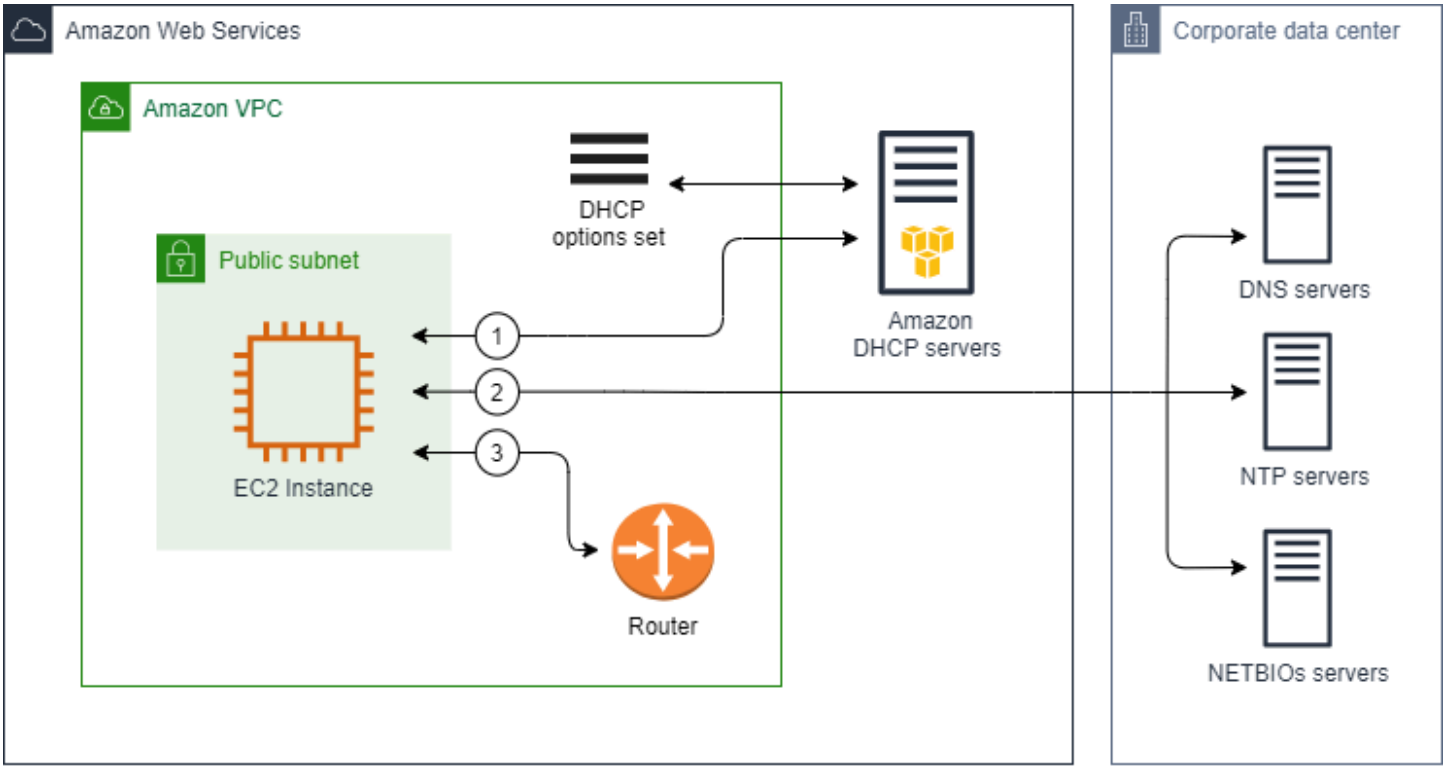
Set opsi DHCP kustom

Anda dapat membuat opsi DHCP khusus yang diatur 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 instance EC2 yang menjalankan 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: Untuk instance EC2 yang menjalankan Windows, metode yang digunakan instance untuk menyelesaikan nama NetBIOS ke alamat IP.
- IPv6 Preferred Lease Time (opsional): Nilai (dalam detik, menit, jam, atau tahun) untuk seberapa sering instance yang berjalan dengan IPv6 yang ditetapkan padanya melewati perpanjangan sewa DHCPv6. Nilai yang dapat diterima adalah antara 140 dan 4294967295 detik (sekitar 138

tahun). Jika tidak ada nilai yang dimasukkan, waktu sewa default adalah 140 detik. Jika Anda menggunakan pengalamatan jangka panjang untuk instans EC2, Anda dapat meningkatkan waktu sewa dan menghindari permintaan perpanjangan sewa yang sering. Perpanjangan sewa biasanya terjadi ketika setengah dari waktu sewa telah berlalu.

Saat Anda menggunakan 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, lihatthe section called “Konsep set opsi DHCP”.

Tugas

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

Lihat set opsi DHCP Anda

Anda dapat melihat set opsi DHCP Anda sebagai berikut. Untuk set opsi DHCP default, satu-satunya pengaturan dengan nilai adalah nama Domain dan server nama Domain.

Untuk melihat set opsi DHCP Anda menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih set opsi DHCP.
3. Pilih ID opsi DHCP yang disetel untuk membuka halaman detailnya.

Untuk melihat set opsi DHCP Anda menggunakan baris perintah

Untuk informasi selengkapnya tentang antarmuka baris perintah ini, lihat Bekerja dengan Amazon VPC.

- describe-dhcp-options (AWS CLI)
- Get-EC2DhcpOption (AWS Tools for Windows PowerShell)

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 Amazon VPC 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.

     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 domain IPv4 (atau hingga tiga server nama domain IPv4 dan**`AmazonProvidedDNS`**) dan empat server nama domain IPv6 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 alamat IPv4 dan empat alamat IPv6).

  Server NTP menyediakan waktu untuk jaringan Anda. Anda dapat menentukan Layanan Sinkronisasi Waktu Amazon di alamat IPv4 `169.254.169.123` atau alamat IPv6. `fd00:ec2::123` Instans berkomunikasi dengan Layanan Sinkronisasi Waktu Amazon secara default. Perhatikan bahwa alamat IPv6 hanya dapat diakses pada instans EC2 yang dibangun di 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 Pengguna Amazon EC2.
- Server nama NetBIOS (opsional): Masukkan alamat IP hingga empat server nama NetBIOS.

  Untuk instans EC2 yang menjalankan OS 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 (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 simpul ini, lihat bagian 8.7 RFC 2132 dan bagian 10 dari RFC1001.

  Untuk instans EC2 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 Preferred Lease Time (opsional): Nilai (dalam detik, menit, jam, atau tahun) untuk seberapa sering instance yang berjalan dengan IPv6 yang ditetapkan padanya melewati perpanjangan sewa DHCPv6. 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 instans EC2, Anda dapat meningkatkan waktu sewa dan menghindari permintaan perpanjangan sewa yang sering. Perpanjangan sewa biasanya terjadi ketika setengah dari waktu sewa telah berlalu.

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

Untuk informasi selengkapnya tentang antarmuka baris perintah ini, lihat Bekerja dengan Amazon VPC.

- 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 VPC. Anda hanya dapat mengaitkan satu set opsi DHCP dengan VPC sekaligus. Jika Anda tidak mengaitkan opsi DHCP yang disetel dengan VPC, ini menonaktifkan resolusi nama domain di VPC.

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

Untuk mengubah set opsi DHCP yang terkait dengan VPC menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih VPC Anda.
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

Untuk informasi selengkapnya tentang antarmuka baris perintah ini, lihat Bekerja dengan Amazon VPC.

- 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 Amazon VPC 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

Untuk informasi selengkapnya tentang antarmuka baris perintah ini, lihat Bekerja dengan Amazon VPC.

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

Atribut DNS untuk VPC Anda

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

yang terdiri dari nama host dan nama domain. Server DNS mengubah nama host DNS menjadi alamat IP yang sesuai.

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

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

Daftar Isi

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 CIDR IPV4 pribadi utama yang disediakan untuk VPC Anda ditambah dua. Misalnya, jika Anda memiliki VPC dengan IPv4 CIDR `10.0.0.0/16` dan IPv6 CIDR, Anda `fd00:ec2::253` dapat mencapai Route 53 Resolver di (IPv4), (IPv6), atau `169.254.169.253` (IPv4). `fd00:ec2::253` `10.0.0.2` Sumber daya dalam VPC menggunakan alamat lokal tautan untuk kueri DNS. Kueri ini diangkut ke Route 53 Resolver secara pribadi dan tidak terlihat di jaringan. Dalam subnet khusus IPv6, alamat link-lokal IPv4 (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 alamat IPv4 publik dan atribut DNS VPC diaktifkan.

Format nama host DNS pribadi tergantung pada bagaimana Anda mengonfigurasi instans EC2 saat Anda meluncurkannya. Untuk informasi selengkapnya tentang jenis nama host DNS pribadi, lihat penamaan instans EC2.

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

Aturan dan pertimbangan

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

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

Nama host DNS

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

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

Nama DNS IP pribadi (hanya IPv4)

Anda dapat menggunakan nama host Private IP DNS (hanya IPv4) untuk komunikasi antar instance di VPC yang sama. Anda dapat menyelesaikan nama host Private IP DNS (hanya IPv4) dari

instance lain di VPC lain selama instance berada di AWS Wilayah yang sama dan nama host dari instance lainnya berada dalam rentang ruang alamat pribadi yang ditentukan oleh RFC 1918:,, dan. `10.0.0.0 - 10.255.255.255 (10/8 prefix)` `172.16.0.0 - 172.31.255.255 (172.16/12 prefix)` `192.168.0.0 - 192.168.255.255 (192.168/16 prefix)`

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 IPv6 saja. Untuk informasi selengkapnya tentang RBN, lihat jenis nama host instans EC2.

DNS IPv4 Publik

Nama host DNS IPv4 publik (eksternal) mengambil formulir `ec2-`*`public-ipv4-address`*`.compute-1.amazonaws.com` untuk `us-east-1` Wilayah, dan `ec2-`*`public-ipv4-address`*`.`*`region`*`.compute.amazonaws.com` untuk Wilayah lainnya. Server DNS Amazon mengubah nama host DNS publik menjadi alamat IPv4 publik pada instans di luar jaringan instans, dan di alamat IPv4 pribadi instans dari dalam jaringan instans. Untuk informasi selengkapnya, lihat Alamat IPv4 publik dan nama host DNS eksternal di Panduan Pengguna Amazon EC2.

Atribut DNS di 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 alamat IPv4 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 menerima nama host DNS publik jika mereka memiliki alamat IPv4 publik atau alamat IP Elastis.

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

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

Atribut	Deskripsi
`enableDnsSupport`	Menentukan apakah VPC mendukung resolusi DNS melalui server DNS yang disediakan Amazon. Jika atribut ini`true`, kueri ke server DNS yang disediakan Amazon berhasil. Untuk informasi selengkapnya, lihat Server Amazon DNS. Default untuk atribut ini adalah`true`. Perhatikan 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 k`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 kustom yang ditentukan di zona yang dihosting 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 alamat IPv4 pribadi untuk semua ruang alamat, termasuk di mana rentang alamat IPv4 VPC Anda berada di luar rentang alamat IPv4 pribadi yang ditentukan oleh RFC 1918. Namun, jika Anda membuat VPC Anda sebelum Oktober 2016, Amazon Route 53 Resolver tidak akan mengubah nama host DNS pribadi jika kisaran alamat IPv4 VPC Anda jatuh di luar kisaran ini. Untuk mengaktifkan support untuk ini, hubungi AWS Support.

- Jika Anda menggunakan peering VPC, Anda harus mengaktifkan kedua atribut untuk kedua VPC, dan Anda harus mengaktifkan resolusi DNS untuk koneksi peering. Untuk informasi selengkapnya, lihat Mengaktifkan resolusi DNS untuk koneksi peering VPC.

Kuota DNS

Setiap instans EC2 dapat mengirim 1024 paket per detik per antarmuka jaringan ke Route 53 Resolver (khususnya alamat.2, seperti 10.0.0.2 dan 169.254.169.253). Kuota ini tidak dapat dinaikkan jumlahnya. Jumlah kueri DNS per detik yang didukung oleh Route 53 Resolver bervariasi 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 instans, lihat Mengambil metadata instans di Panduan Pengguna Amazon EC2.

Lihat nama host DNS untuk instans EC2 Anda

Anda dapat melihat nama host DNS untuk sebuah instans yang berjalan atau antarmuka jaringan menggunakan konsol Amazon EC2 atau baris perintah.

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

Instans

Untuk melihat nama host DNS untuk sebuah instans menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Instans.
3. Pilih Instans Anda dari daftar.

4. Di panel rincian, DNS Publik (IPv4) dan DNS Pribadi menampilkan nama host DNS, jika ada.

Untuk melihat nama host DNS untuk sebuah instans menggunakan baris perintah

Anda dapat menggunakan salah satu dari perintah-perintah berikut ini. Untuk informasi selengkapnya tentang antarmuka baris perintah ini, lihat Bekerja dengan Amazon VPC.

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

Antarmuka jaringan

Untuk melihat nama host DNS pribadi untuk antarmuka jaringan menggunakan konsol

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

Untuk melihat nama host DNS untuk antarmuka jaringan menggunakan baris perintah

Anda dapat menggunakan salah satu perintah berikut ini. Untuk informasi selengkapnya tentang antarmuka baris perintah ini, lihat Bekerja dengan Amazon VPC.

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

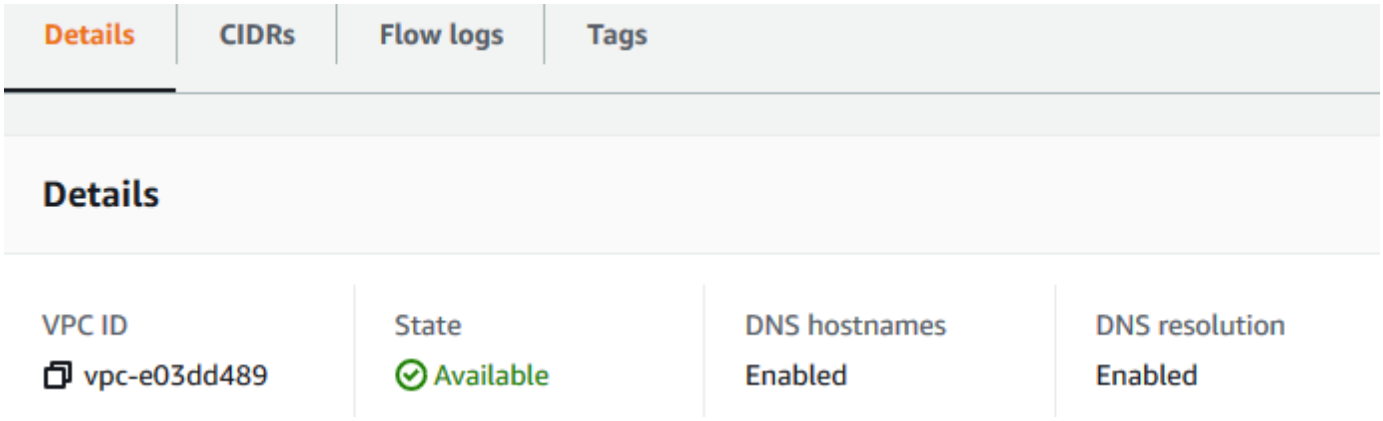
Melihat dan memperbarui atribut DNS untuk VPC Anda

Anda dapat melihat dan memperbarui atribut support DNS untuk VPC Anda menggunakan konsol Amazon VPC.

Untuk menjelaskan dan memperbarui support DNS untuk VPC menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih VPC Anda.

3. Pilih kotak centang untuk VPC.
4. Tinjau informasi dalam Detail. Dalam contoh ini, nama host DNS dan resolusi DNS diaktifkan.



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

Anda dapat menggunakan salah satu perintah berikut ini. Untuk informasi selengkapnya tentang antarmuka baris perintah ini, lihat Bekerja dengan Amazon VPC.

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

Untuk memperbarui support DNS untuk VPC menggunakan baris perintah

Anda dapat menggunakan salah satu dari perintah-perintah berikut. Untuk informasi selengkapnya tentang antarmuka baris perintah ini, lihat Bekerja dengan Amazon VPC.

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

Zona host pribadi

Untuk mengakses sumber daya di VPC Anda menggunakan nama domain DNS kustom, seperti`example.com`, alih-alih menggunakan alamat IPv4 pribadi atau nama host DNS pribadi yang AWS disediakan, Anda dapat membuat zona host pribadi di Route 53. Zona host pribadi adalah wadah yang menyimpan informasi tentang bagaimana Anda ingin mengarahkan lalu lintas

untuk domain dan subdomainnya dalam satu atau lebih VPC tanpa mengekspos sumber daya Anda ke internet. Anda kemudian dapat membuat kumpulan catatan sumber daya Route 53, yang menentukan bagaimana Route 53 menanggapi kueri untuk domain dan subdomain Anda. Misalnya, jika Anda ingin browser meminta example.com diarahkan ke server web di VPC Anda, Anda akan membuat catatan A di zona host pribadi Anda dan menentukan alamat IP atas server web tersebut. Untuk informasi selengkapnya tentang membuat sebuah zona yang di-hosting privat, lihat Bekerja dengan Zona yang di-hosting privat di Panduan Developer Amazon Route 53.

Untuk mengakses sumber daya menggunakan nama domain DNS kustom, Anda harus terhubung ke sebuah instans dalam VPC Anda. Dari instans Anda, Anda dapat menguji bahwa sumber daya Anda di zona host pribadi Anda dapat diakses dari nama DNS kustom dengan menggunakan perintah `ping`; sebagai contoh, `ping mywebserver.example.com`. (Anda harus memastikan bahwa aturan grup keamanan instans Anda mengizinkan lalu lintas inbound ICMP untuk perintah `ping` untuk bekerja.)

Zona yang dihosting pribadi tidak mendukung hubungan transitif di luar VPC; misalnya, Anda tidak dapat mengakses sumber daya 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 ke`true`.

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 VPC peered nya. Jika VPC diintip dengan VPC lain di Wilayah yang sama, gabungan VPC dapat memiliki hingga 128.000 unit NAU secara default. Anda dapat meminta kenaikan kuota hingga 512.000. VPC 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 VPC.
- 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 VPC Anda.

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

Sumber Daya	Unit NAU
Setiap IPv4 pribadi atau publik dan setiap alamat IPv6 ditetapkan ke antarmuka jaringan untuk instans EC2 di VPC	1
Antarmuka jaringan tambahan yang dilampirkan ke instans 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

Sumber Daya	Unit NAU
Lampiran gerbang transit	6
Fungsi Lambda	6
Gateway NAT	6
Target pemasangan EFS	6

Contoh NAU

Contoh berikut menunjukkan cara menghitung NAU.

Contoh 1 - Dua VPC terhubung menggunakan VPC peering

VPC peered 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 alamat IPv4 dan alamat IPv6) dalam satu subnet dan 5.000 instance (masing-masing dengan alamat IPv4 dan alamat IPv6) 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 alamat IPv4 dan alamat IPv6) dalam satu subnet dan 5.000 instance (masing-masing dengan alamat IPv4 dan alamat IPv6) di subnet lain - 20.000 unit
  - 100 fungsi Lambda - 600 unit NAU
- Jumlah total pengintipan NAU: 42.400 unit
- Kuota NAU peering default: 128.000 unit

Contoh 2 - Dua VPC terhubung menggunakan gateway transit

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

- VPC 1

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

Berbagi VPC memungkinkan beberapa orang Akun AWS untuk membuat sumber daya aplikasinya, seperti instans Amazon EC2, database Amazon Relational Database Service (RDS), cluster AWS Lambda Amazon Redshift, dan fungsi, ke dalam cloud pribadi virtual (VPC) bersama yang dikelola secara terpusat. Dalam model ini, akun yang memiliki VPC (pemilik) berbagi satu atau lebih subnet dengan akun lain (peserta) 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 VPC Anda untuk memanfaatkan perutean implisit dalam VPC untuk aplikasi yang memerlukan tingkat interkonektivitas yang tinggi dan berada dalam batas kepercayaan yang sama. Hal ini mengurangi jumlah VPC yang Anda buat dan kelola, saat menggunakan akun terpisah untuk penagihan dan kontrol akses. Anda dapat menyederhanakan topologi jaringan dengan menghubungkan VPC Amazon bersama menggunakan fitur konektivitas, AWS PrivateLink seperti gateway transit, dan pengintipan VPC. Untuk informasi selengkapnya tentang manfaat pembagian VPC, lihat Pembagian VPC: Pendekatan baru untuk pengelolaan banyak akun dan VPC.

Daftar Isi

- Membatalkan pembagian subnet bersama
- Mengidentifikasi pemilik subnet bersama
- Kelola sumber daya VPC
- Tanggung jawab dan izin untuk pemilik dan peserta
- AWS sumber daya dan subnet VPC bersama
- Kuota berbagi VPC
- Contoh berbagi subnet publik dan subnet pribadi

Prasyarat VPC 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.

Membagikan subnet

Anda dapat berbagi subnet non-default dengan akun lain dalam organisasi Anda sebagai berikut.

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

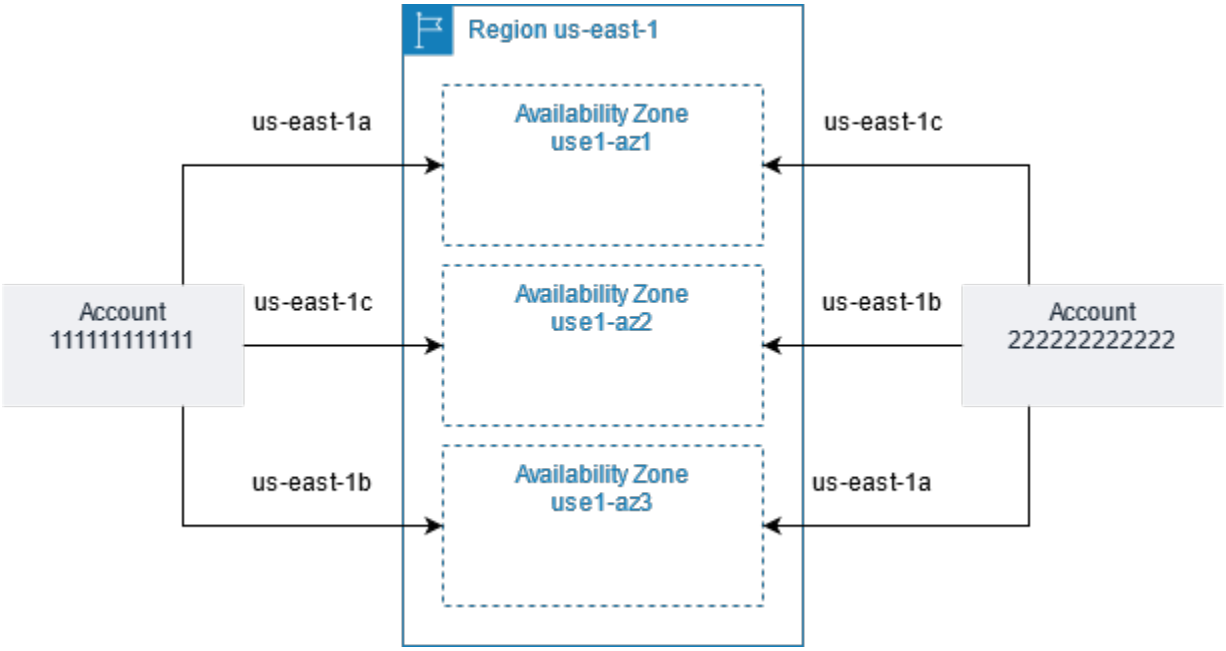
Gunakan create-resource-sharedan associate-resource-shareperintah.

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 pengenal unik dan konsisten untuk Availability Zone. Misalnya, `use1-az1` adalah ID AZ untuk salah satu Availability Zone di `us-east-1` Region. Gunakan ID AZ untuk menentukan lokasi sumber daya dalam satu akun relatif terhadap akun lain. Anda dapat melihat ID AZ untuk setiap subnet di konsol 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 alur kerja otomatis/terkelola (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 pembagian 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.

Kelola sumber daya VPC

Pemilik dan peserta bertanggung jawab atas sumber daya VPC yang mereka miliki.

Sumber daya pemilik

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

Sumber daya peserta

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 Pembagian VPC.

Penagihan dan pengukuran untuk pemilik dan peserta

- Dalam VPC bersama, setiap peserta membayar sumber daya aplikasi mereka termasuk instans Amazon EC2, database Layanan 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, alamat IPv4 publik yang digunakan dalam VPC bersama ditagih ke pemilik VPC. Untuk informasi selengkapnya tentang harga alamat IPv4 publik, lihat tab Alamat IPv4 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

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

Log alur

- Peserta tidak dapat membuat, menghapus, atau mendeskripsikan log alur di subnet VPC bersama yang tidak mereka miliki.
- Peserta dapat membuat, menghapus, dan mendeskripsikan flow log di subnet VPC bersama yang mereka miliki.
- Pemilik VPC tidak dapat mendeskripsikan 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 NACL di subnet VPC bersama. Peserta dapat mendeskripsikan NACL yang dibuat oleh pemilik VPC di subnet VPC bersama.

Antarmuka jaringan

- Peserta dapat membuat antarmuka jaringan di subnet VPC bersama. Peserta tidak dapat bekerja dengan antarmuka jaringan yang dibuat oleh pemilik VPC di subnet VPC bersama dengan cara lain, seperti melampirkan, melepaskan, atau memodifikasi antarmuka jaringan. Peserta dapat memodifikasi atau menghapus antarmuka jaringan dalam VPC bersama yang mereka buat. Misalnya, peserta dapat mengaitkan atau memisahkan alamat IP dengan antarmuka jaringan yang mereka buat.
- Pemilik VPC dapat mendeskripsikan 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 mendeskripsikan 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 tidak dapat bekerja dengan grup keamanan yang dibuat oleh pemilik VPC dengan cara apa pun.
- 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 instans menggunakan grup keamanan yang dimiliki oleh pemilik VPC atau peserta lain. Peserta tidak dapat meluncurkan instance menggunakan grup keamanan default untuk VPC karena milik pemilik.
- Pemilik VPC dapat mendeskripsikan 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.

VPC

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

AWS sumber daya dan subnet VPC bersama

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

- Amazon Aurora
- AWS CodeBuild
- AWS Database Migration Service
- Amazon EC2
- Layanan Amazon Elastic Kubernetes
- Penyeimbang Beban Elastis
  - Penyeimbang Beban Aplikasi
  - Penyeimbang Beban Gateway
  - Penyeimbang Beban Jaringan
- Amazon EMR
- AWS Glue
- AWS Lambda
- AWS Network Manager
  - AWS Awan WAN
  - Penganalisis Akses Jaringan
  - Reachability Analyzer

- 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.

Kuota berbagi VPC

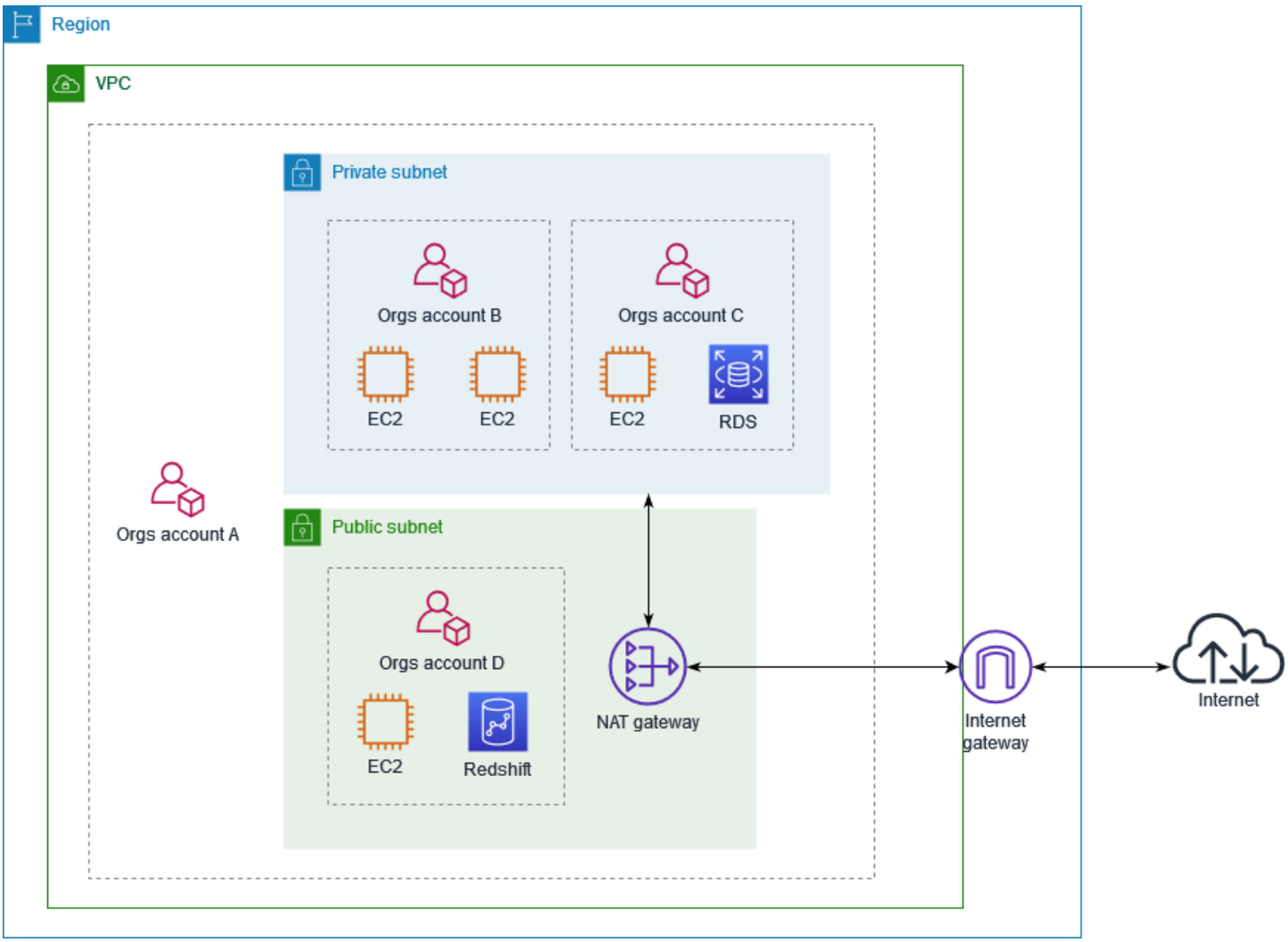
Ada kuota yang terkait dengan berbagi VPC. Untuk informasi selengkapnya, lihat Pembagian VPC.

Contoh berbagi subnet publik dan subnet pribadi

Pertimbangkan skenario ini di mana Anda ingin akun (Akun A) mengelola infrastruktur, termasuk VPC, subnet, tabel rute, gateway, dan rentang CIDR, dan akun anggota lainnya untuk menggunakan subnet untuk aplikasi mereka. Akun D memiliki aplikasi yang perlu terhubung ke internet. Akun B dan Akun C memiliki aplikasi yang tidak perlu terhubung ke internet.

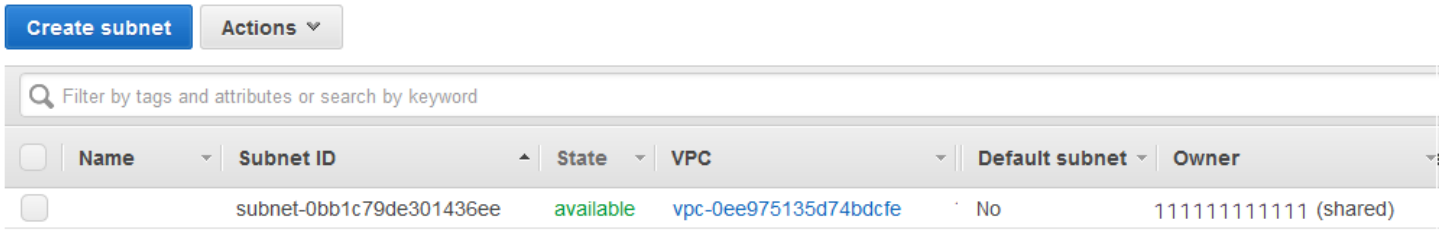
Akun A digunakan AWS Resource Access Manager untuk membuat Pembagian Sumber Daya untuk subnet, dan berbagi subnet publik dengan Akun D dan subnet pribadi dengan Akun B dan Akun C. Akun B, Akun C, dan Akun D dapat membuat sumber daya di subnet. Setiap akun hanya dapat melihat dan membuat sumber daya di subnet yang dibagikan dengannya. Setiap akun dapat mengontrol sumber daya yang mereka buat di subnet ini (misalnya, instans EC2 dan grup keamanan).

Tidak ada konfigurasi tambahan yang diperlukan untuk subnet bersama, sehingga tabel rutenya sama dengan tabel rute yang digunakan oleh subnet yang tidak dibagikan.



Akun A (111111111111) berbagi subnet publik dengan Akun D (44444444444444). Akun D melihat subnet berikut, dan kolom Pemilik menyediakan dua indikator yang dibagikan ke subnet tersebut.

- ID akun pemilik adalah Akun A (11111111111111), bukan Akun D (444444444444).
- Kata "dibagikan" muncul di samping ID akun pemilik.



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 menghadirkan layanan, infrastruktur, dan model operasi AWS asli ke hampir semua pusat data, ruang kolokasi, atau fasilitas on-premise virtual.
- Wavelength Zones memungkinkan pengembang membangun aplikasi yang menghadirkan latensi sangat rendah ke perangkat 5G dan pengguna akhir. Wavelength men-deploy layanan komputasi dan penyimpanan AWS standar ke edge jaringan 5G operator telekomunikasi.

AWSberoperasi 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.

Untuk membantu Anda menentukan deployment mana yang terbaik untuk Anda, lihat FAQ AWS Wavelength.

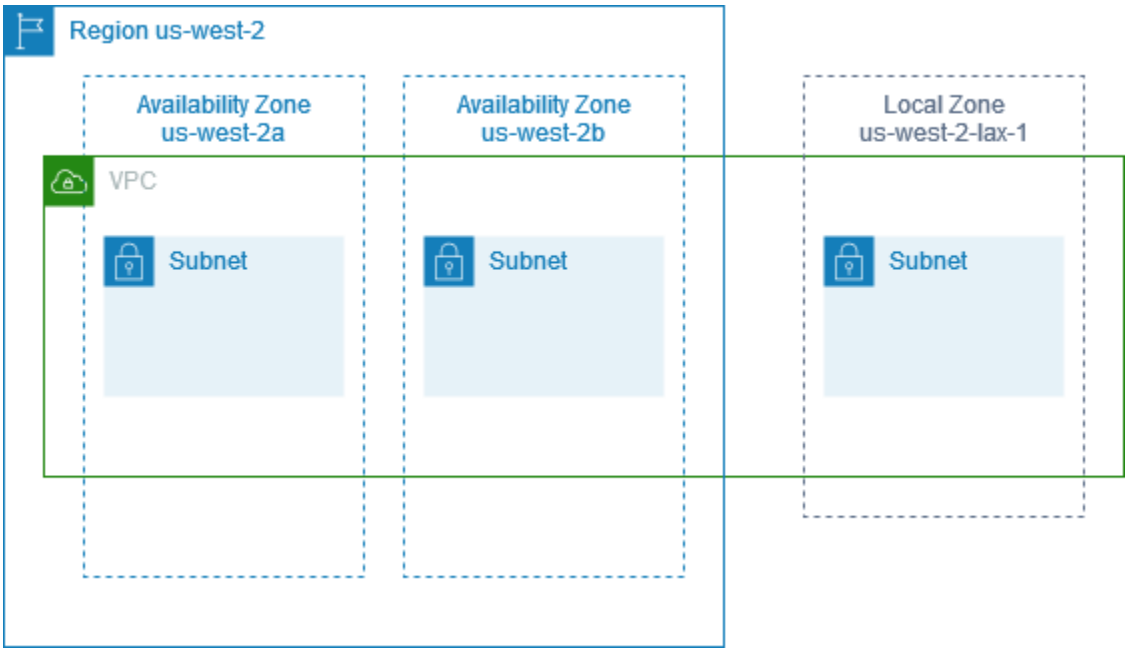
Subnet di AWS Local Zones

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

Untuk menggunakan Zona Lokal, Anda menggunakan proses berikut:

- Ikut serta ke Zona Lokal.
- Membuat 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 sebagaimana subnet Availability Zone, termasuk tabel rute, grup keamanan, dan ACL jaringan.
- Lalu lintas internet keluar meninggalkan suatu Zona Lokal dari Zona Lokal tersebut.
- Anda harus menyediakan alamat IP publik untuk digunakan di Zona Lokal. Bila Anda mengalokasikan alamat, Anda dapat menyebutkan lokasi yang darinya alamat IP diiklankan. Kami menyebut ini sebagai grup perbatasan jaringan, dan Anda dapat mengatur parameter ini untuk membatasi alamat ke lokasi ini. Setelah Anda menyediakan alamat IP, Anda tidak dapat memindahkannya dari Zona Lokal ke Wilayah induk atau sebaliknya (misalnya, dari `us-west-2-lax-1a` ke `us-west-2`).

- Jika Local Zone mendukung IPv6, Anda dapat meminta alamat IP yang disediakan IPv6 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 AWSLocal 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 lokasi AWS Direct Connect di Wilayah. Pusat data on-premise memiliki koneksi AWS Direct Connect ke lokasi AWS Direct Connect.

> **Note**
>
> Lalu lintas di AS 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 rincian subnet di Amazon Virtual Private Cloud Console, atau menggunakan describe-subnets.

  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 rekomendasikan agar Anda menggunakan lokasi Direct Connect yang paling dekat dengan Zona Lokal tempat Anda akan memperluas subnet Anda.

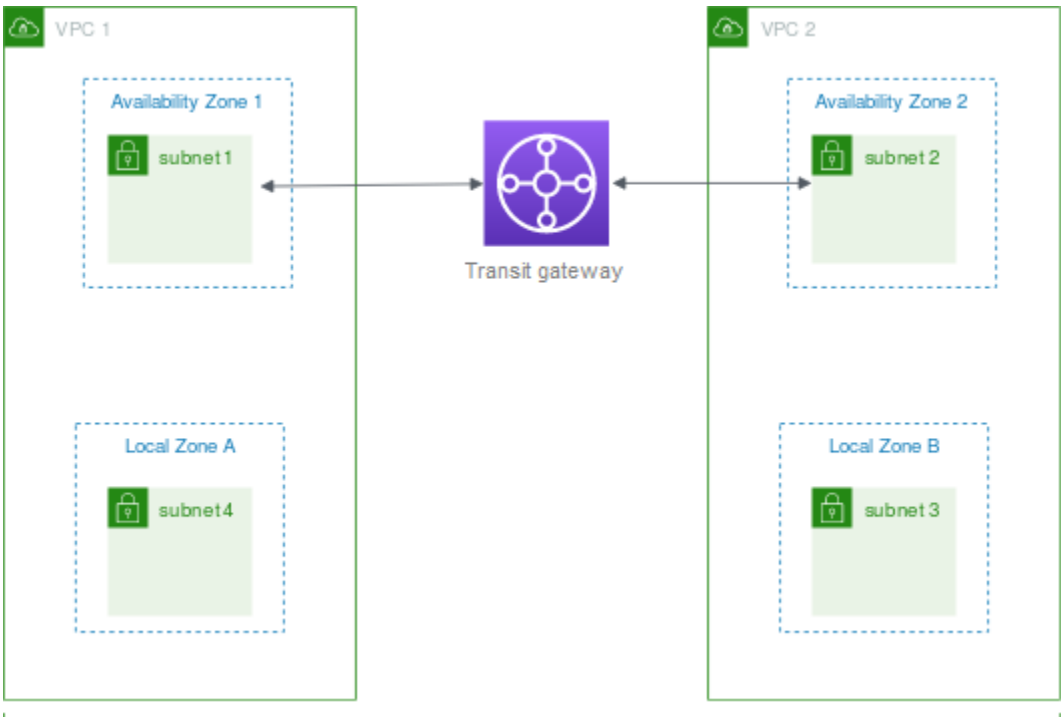
  Untuk informasi tentang memerintahkan koneksi, lihat Koneksi silang dalam Panduan Pengguna AWS Direct Connect.
- Sebuah gateway Direct Connect. Untuk informasi tentang cara membuat gateway Direct Connect, lihat Membuat gateway Direct Connect di Panduan Pengguna AWS Direct Connect.
- Pengaitan virtual 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 privat pada koneksi dari lokasi AWS Direct Connect ke pusat data on-premise. 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 Amazon VPC Transit Gateways.
- Lampiran gateway transit untuk setiap VPC menggunakan Availability Zone induk. Untuk informasi selengkapnya, lihat Membuat lampiran gateway transit ke VPC di Amazon VPC Transit Gateways.
- 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 VPC 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
VPC 1 CIDR	*lokal*
VPC 2 CIDR	*vpc1- attachment-network-interface-id*

Berikut ini adalah contoh tabel rute untuk VPC 2.

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

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

CIDR	Lampiran	Jenis rute
VPC 1 CIDR	*Lampiran untuk VPC 1*	diperbanyak
VPC 2 CIDR	*Lampiran untuk VPC 2*	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 seperti instans AWS Amazon EC2 untuk menjalankan aplikasi yang memerlukan latensi ultra-rendah dan terhubung ke Wilayah. Layanan AWS

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

Aturan berikut berlaku untuk Wavelength Zones:

- Sebuah VPC meluas ke Zona Wavelength ketika Anda membuat subnet di VPC dan mengaitkannya dengan Zona Wavelength.
- Secara default, setiap subnet yang Anda buat di VPC yang mencakup Zona Wavelength mewarisi tabel rute VPC utama, termasuk rute lokal.
- Ketika Anda meluncurkan instans EC2 di subnet di Zona Wavelength, Anda menetapkan alamat IP operator untuk itu. Carrier operator menggunakan alamat untuk lalu lintas dari antarmuka ke internet, atau perangkat seluler. Gateway operator menggunakan NAT untuk menerjemahkan alamat, dan kemudian mengirimkan lalu lintas ke tujuan. Lalu lintas dari rute jaringan operator telekomunikasi melalui gateway operator.
- Anda dapat mengatur target tabel rute VPC, atau subnet tabel rute di Zona Wavelength untuk gateway operator, yang memungkinkan lalu lintas masuk dari jaringan operator di lokasi tertentu, dan lalu lintas keluar ke jaringan operator dan internet. Untuk informasi lebih lanjut tentang pilihan perutean di Zona Wavelength, lihat Perutean di Panduan Developer AWS Wavelength.
- Subnet di Wavelength Zones memiliki komponen jaringan yang sama dengan subnet di Availability Zones, termasuk alamat IPv4, set opsi DHCP, dan ACL jaringan.

- Anda tidak dapat membuat lampiran gateway transit ke subnet di 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

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

Rute lalu lintas Zona Wavelength ke Zona Wavelength Zona 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:

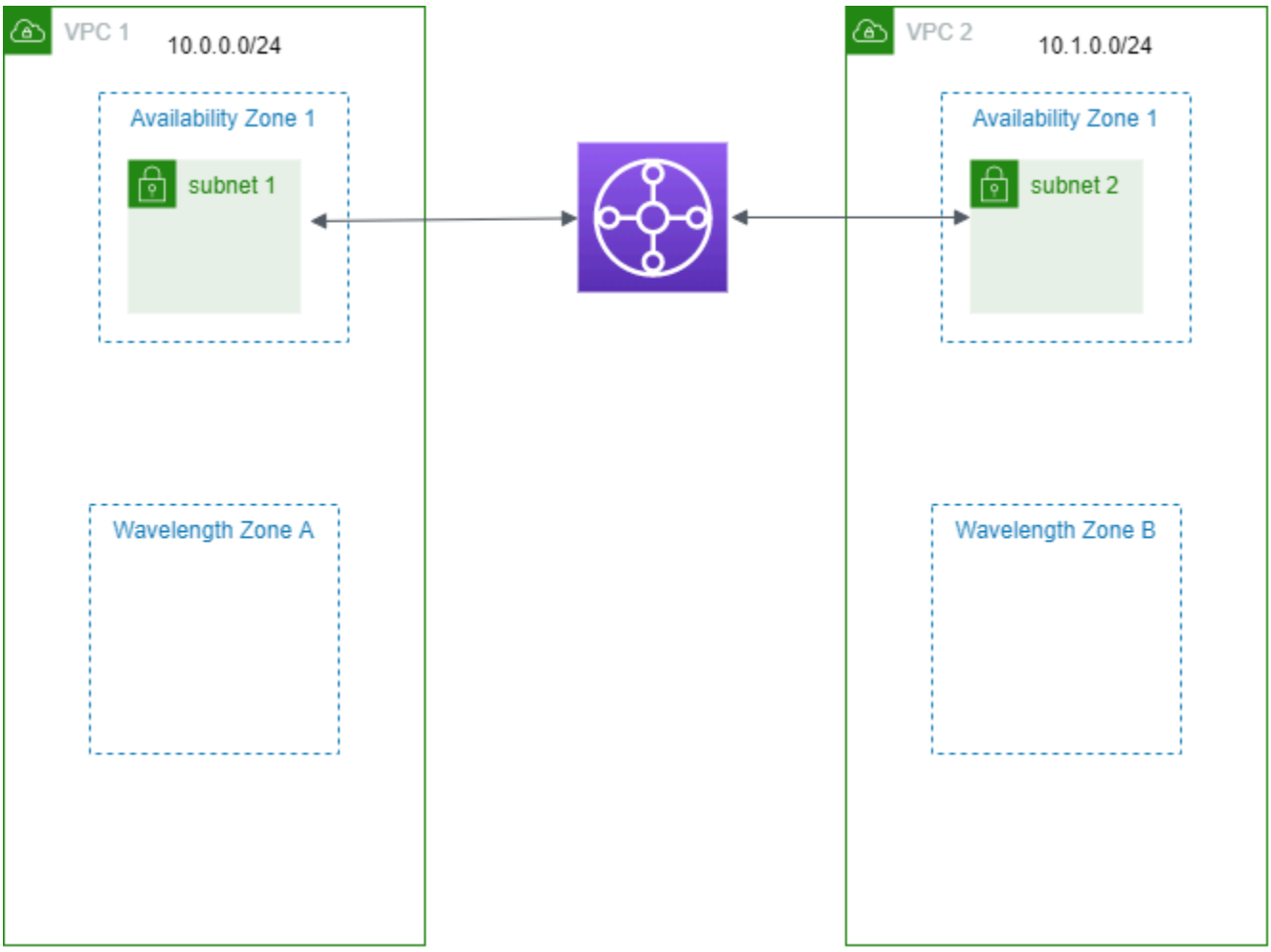
- Untuk setiap Zona Wavelength, subnet di Availability Zone yang merupakan Availability Zone induk untuk Zona Wavelength. Misalnya, Anda membuat subnet 1 dan subnet 2. Untuk informasi tentang membuat subnet, lihat the section called “Membuat subnet”. Gunakan describe-availability-zonesuntuk menemukan zona induk.
- Transit gateway. Transit gateway menghubungkan VPC. Untuk informasi selengkapnya tentang membuat transit gateway, lihat Membuat transit gateway di Panduan Amazon VPC Transit Gateways.
- Untuk setiap VPC, lampiran VPC ke gateway transit di 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-22222222222222222

Misalnya, tabel rute untuk VPC 2 memiliki entri berikut:

Tujuan	Target
10.0.0.0/24	tgw-22222222222222222



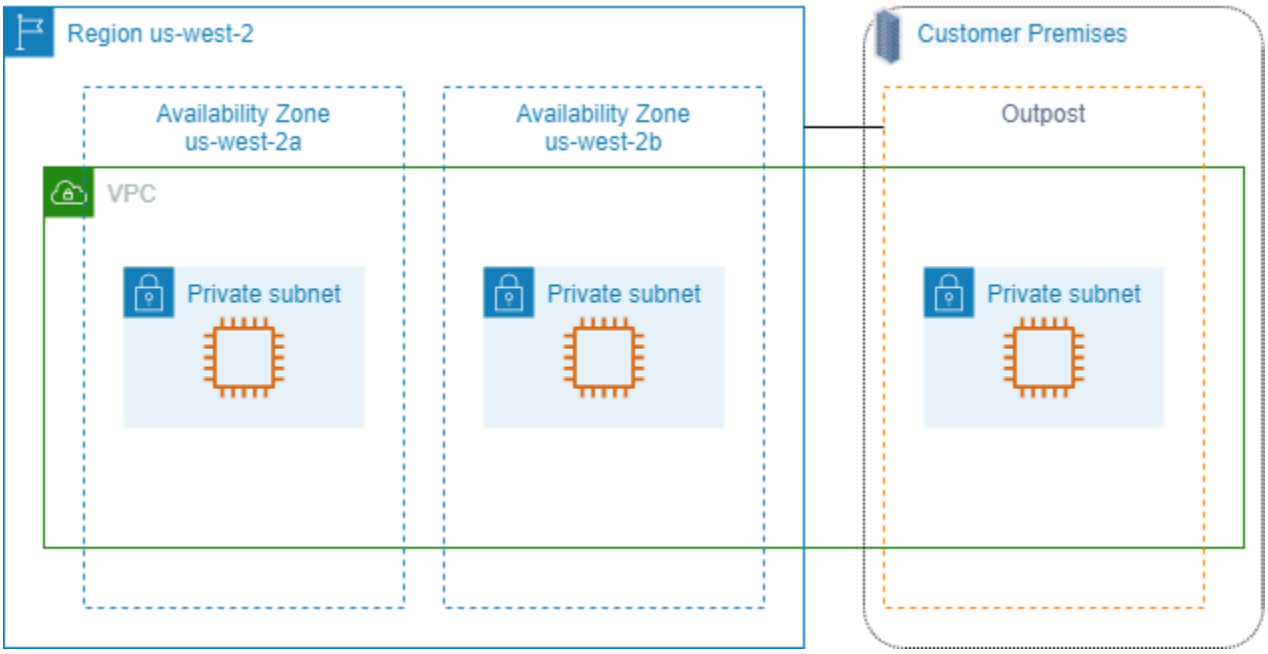
Subnet di AWS Outposts

AWS Outposts menawarkan infrastruktur hardware, layanan, API dan alat AWS yang sama untuk membuat dan menjalankan aplikasi Anda di lokasi dan di cloud. AWS Outposts ideal untuk beban kerja yang memerlukan akses latensi rendah ke aplikasi atau sistem on-premise, dan untuk beban kerja yang perlu menyimpan dan memproses data secara lokal. Untuk informasi selengkapnya 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 instans EC2 dan menghapus penyeimbang beban, gateway NAT, lampiran VPC gateway transit, dan titik akhir VPC antarmuka.

Daftar Isi

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
- ACL jaringan
- Tabel rute
- Grup keamanan
- Subnet

Untuk menghapus VPC Anda menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Akhiri semua instans di VPC. Untuk informasi selengkapnya, lihat Menghentikan Instans Anda di Panduan Pengguna Amazon EC2.
3. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
4. Di panel navigasi, pilih VPC Anda.
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 VPN Site-to-Site, Anda dapat memilih opsi untuk menghapusnya. Jika Anda berencana untuk menggunakan gateway pelanggan dengan VPC lain, kami sarankan agar Anda tetap mempertahankan koneksi Site-to-Site VPN dan gateway-nya. Jika tidak, Anda harus mengonfigurasi perangkat gateway pelanggan Anda lagi setelah Anda membuat koneksi Site-to-Site VPN yang 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, ACL 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 perintah delete-security-group.

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

2. Hapus setiap ACL jaringan dengan menggunakan perintah delete-network-acl.

```
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 perintah delete-route-table.

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

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

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

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

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

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

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

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

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

Subnet untuk VPC Anda

Sebuah subnet adalah rentang alamat IP di VPC Anda. Anda dapat membuat AWS sumber daya, seperti instans EC2, di subnet tertentu.

Daftar Isi

Dasar-dasar subnet

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

Saat Anda membuat subnet, Anda menentukan alamat IP-nya, tergantung pada konfigurasi VPC:

- Hanya IPv4 - Subnet memiliki blok CIDR IPv4 tetapi tidak memiliki blok CIDR IPv6. Sumber daya dalam subnet khusus IPv4 harus berkomunikasi melalui IPv4.

- Dual stack — Subnet memiliki blok IPv4 CIDR dan blok IPv6 CIDR. VPC harus memiliki blok IPv4 CIDR dan blok IPv6 CIDR. Sumber daya dalam subnet dual-stack dapat berkomunikasi melalui IPv4 dan IPv6.
- Hanya IPv6 - Subnet memiliki blok CIDR IPv6 tetapi tidak memiliki blok CIDR IPv4. VPC harus memiliki blok CIDR IPv6. Sumber daya dalam subnet khusus IPv6 harus berkomunikasi melalui IPv6.

> **Note**
>
> Sumber daya dalam subnet khusus IPv6 diberikan alamat link-lokal IPv4 dari blok CIDR. `169.254.0.0/16` Alamat ini digunakan untuk berkomunikasi dengan layanan VPC seperti Instance Metadata Service (IMDS).

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

Jenis subnet

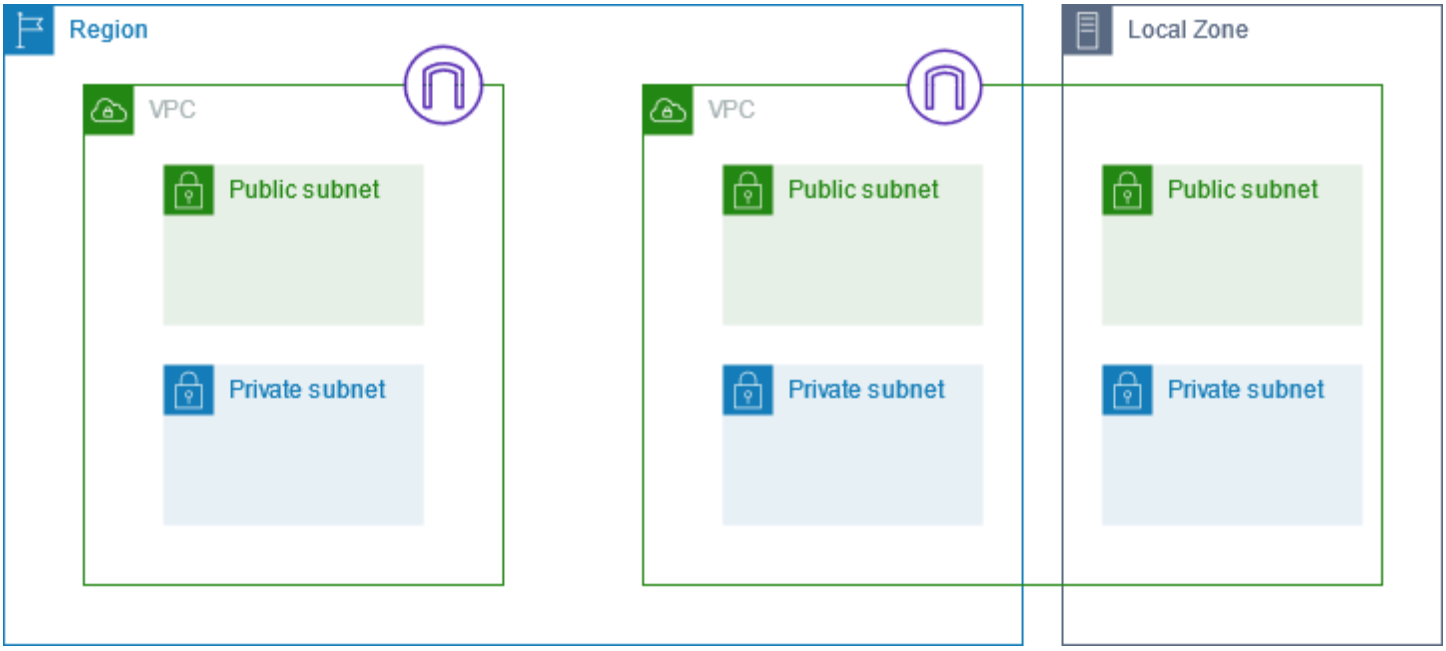
Jenis subnet ditentukan oleh bagaimana Anda mengkonfigurasi routing untuk subnet Anda. Sebagai contoh:

- Subnet publik — Subnet memiliki rute langsung ke gateway internet. Sumber daya dalam subnet publik dapat mengakses internet publik.
- Subnet pribadi — Subnet tidak memiliki rute langsung ke gateway internet. Sumber daya dalam subnet pribadi memerlukan perangkat NAT untuk mengakses internet publik.
- Subnet khusus VPN — Subnet memiliki rute ke koneksi VPN Site-to-Site 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.

Diagram subnet

Diagram berikut menunjukkan dua VPC di Wilayah. Setiap VPC memiliki subnet publik dan pribadi dan gateway internet. Anda dapat menambahkan subnet secara opsional di Zona Lokal, seperti yang ditunjukkan pada diagram. Local Zone adalah penyebaran AWS infrastruktur yang menempatkan

komputasi, penyimpanan, dan layanan database lebih dekat ke pengguna akhir Anda. Saat Anda menggunakan Zona Lokal, pengguna akhir dapat menjalankan aplikasi yang memerlukan latensi milidetik satu digit. Untuk informasi selengkapnya, lihat Zona Lokal AWS.



Perutean subnet

Setiap subnet harus dikaitkan dengan sebuah tabel rute, yang menentukan rute yang diizinkan untuk lalu lintas outbound meninggalkan subnet. Setiap subnet yang Anda buat secara otomatis dikaitkan dengan tabel rute utama untuk VPC. Anda dapat mengubah pengaitan, dan Anda dapat mengubah isi dari tabel rute utama. Untuk informasi selengkapnya, lihat Konfigurasikan tabel rute.

Pengaturan subnet

Semua subnet memiliki atribut yang dapat dimodifikasi yang menentukan apakah antarmuka jaringan yang dibuat di subnet tersebut ditetapkan sebagai alamat IPv4 publik dan, jika berlaku, alamat IPv6. Ini termasuk antarmuka jaringan primer (eth0) yang dibuat untuk sebuah instans saat Anda meluncurkan sebuah instans 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 alamat IPv4 atau IPv6 publik untuk antarmuka jaringan baru di subnet ini.

- Pengaturan Nama Berbasis Sumber Daya (RBN): Memungkinkan Anda menentukan jenis nama host untuk instans EC2 di subnet ini dan mengonfigurasi bagaimana kueri catatan DNS A dan AAAA ditangani. Untuk informasi selengkapnya, lihat jenis nama host instans Amazon EC2 di Panduan Pengguna Amazon EC2.

Keamanan subnet

Untuk melindungi AWS sumber daya Anda, kami sarankan Anda menggunakan subnet pribadi. Gunakan host bastion atau perangkat NAT untuk menyediakan akses internet ke sumber daya, seperti instans EC2, di subnet pribadi.

AWS menyediakan fitur yang dapat Anda gunakan untuk meningkatkan keamanan sumber daya di VPC Anda. Grup keamanan memungkinkan lalu lintas masuk dan keluar untuk sumber daya terkait, seperti instans EC2. ACL jaringan memungkinkan atau menolak lalu lintas masuk dan keluar di tingkat subnet. Dalam kebanyakan kasus, kelompok keamanan dapat memenuhi kebutuhan Anda. Namun, Anda dapat menggunakan ACL jaringan jika Anda menginginkan lapisan keamanan tambahan. Untuk informasi selengkapnya, lihat the section called “Membandingkan grup keamanan dan ACL jaringan”.

Berdasarkan desain, setiap subnet harus dikaitkan dengan ACL jaringan. Setiap subnet yang Anda buat secara otomatis dikaitkan dengan ACL jaringan default untuk VPC. ACL jaringan default memungkinkan semua lalu lintas masuk dan keluar. Anda dapat memperbarui ACL jaringan default, atau membuat ACL jaringan khusus dan mengaitkannya dengan subnet Anda. Untuk informasi selengkapnya, lihat Kontrol lalu lintas ke subnet menggunakan ACL 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. Untuk informasi selengkapnya, lihat 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 CIDR IPv4 untuk subnet dari rentang VPC Anda. Anda dapat secara opsional menentukan blok IPv6 CIDR untuk subnet jika ada blok CIDR IPv6 yang terkait dengan VPC. Untuk informasi selengkapnya, lihat Pengalamatan IP untuk VPC dan subnet Anda.
- Jika Anda membuat subnet khusus IPv6, perhatikan hal berikut. Instans EC2 yang diluncurkan di subnet khusus IPv6 menerima alamat IPv6, tetapi tidak alamat IPv4. Setiap instans yang Anda luncurkan ke subnet khusus IPv6 harus berupa instans yang dibangun di Nitro System.
- Untuk membuat subnet di Zona Lokal atau Zona Wavelength, Anda harus mengaktifkan Zona. Untuk informasi selengkapnya, lihat Wilayah dan Zona di Panduan Pengguna Amazon EC2.

Untuk menambahkan subnet ke VPC Anda

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Pengguna.
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 IPv4 CIDR. 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 CIDR IPv6 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 CIDR VPC IPv6.
10. Untuk blok CIDR subnet IPv6, 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 netmask IPv6 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:

- Konfigurasikan perutean. Anda kemudian dapat membuat tabel rute khusus dan rute yang mengirim lalu lintas ke gateway yang terkait dengan VPC, seperti gateway internet. Untuk informasi selengkapnya, lihat Konfigurasikan tabel rute.
- Ubah alamat IP subnet. Untuk informasi selengkapnya, lihat the section called “Konfigurasikan subnet Anda”.
- Memodifikasi perilaku pengalamatan IP. Anda dapat menentukan apakah instance yang diluncurkan di subnet menerima alamat IPv4 publik, alamat IPv6, atau keduanya. Untuk informasi selengkapnya, lihat Pengaturan subnet.
- Ubah pengaturan nama berbasis sumber daya (RBN). Untuk informasi selengkapnya, lihat jenis nama host instans Amazon EC2.
- Membuat atau memodifikasi ACL jaringan Anda. Untuk informasi selengkapnya, lihat Kontrol lalu lintas ke subnet menggunakan ACL jaringan.
- Berbagi subnet dengan akun lain. Untuk informasi selengkapnya, lihat ???.

Konfigurasikan subnet Anda

Gunakan prosedur berikut untuk mengonfigurasi subnet untuk virtual private cloud (VPC) Anda.

Tugas

Lihat subnet Anda

Gunakan bagian langkah-langkah berikut untuk melihat detail tentang subnet Anda.

Untuk melihat rincian subnet menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Pengguna.
3. Pilih kotak centang untuk subnet atau pilih subnet ID untuk membuka halaman detail.

Untuk mendeskripsikan subnet menggunakan AWS CLI

Gunakan perintah deskripsi-subnet.

Untuk melihat subnet Anda di semua Wilayah

Buka konsol Amazon EC2 Global View di https://console.aws.amazon.com/ec2globalview/home. Untuk informasi selengkapnya, lihat Daftar dan filter sumber daya menggunakan Tampilan Global Amazon EC2 di Panduan Pengguna Amazon EC2.

Tambahkan blok CIDR IPv6 ke subnet Anda

Anda dapat mengaitkan blok CIDR IPv6 dengan subnet yang sudah ada di VPC Anda. Subnet tidak boleh memiliki blok CIDR IPv6 yang sudah ada yang dikaitkan dengannya.

Untuk menambahkan blok CIDR IPv6 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 Actions, Edit IPv6 CIDR.

4. Pilih Tambahkan CIDR IPv6.
5. Pilih blok CIDR VPC, 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 netmask IPv6 adalah antara /44 dan /64 dengan kelipatan /4.
6. Pilih Simpan.

Untuk mengaitkan blok IPv6 CIDR dengan subnet menggunakan AWS CLI

Gunakan perintah associate-subnet-cidr-block.

Hapus blok CIDR IPv6 dari subnet Anda

Jika Anda tidak lagi menginginkan dukungan IPv6 di subnet Anda, tetapi Anda ingin terus menggunakan subnet Anda untuk membuat dan berkomunikasi dengan sumber daya IPv4, Anda dapat menghapus blok IPv6 CIDR.

Sebelum Anda dapat menghapus blok IPv6 CIDR, Anda harus terlebih dahulu membatalkan penetapan alamat IPv6 yang ditetapkan ke instans apa pun di subnet Anda.

Untuk menghapus blok IPv6 CIDR dari subnet

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Pengguna.
3. Pilih subnet dan pilih Actions, Edit IPv6 CIDR.
4. Temukan blok IPv6 CIDR dan pilih Hapus.
5. Pilih Simpan.

Untuk memisahkan blok CIDR IPv6 dari subnet menggunakan AWS CLI

Gunakan perintah disassociate-subnet-cidr-block.

Memodifikasi atribut pengalamatan IPv4 publik untuk subnet Anda

Secara default, subnet non-default mengatur atribut pengalamatan IPv4 publik ini ke `false`, dan subnet default mengatur atribut ini ke `true`. Pengecualian adalah subnet nondefault yang dibuat oleh

wizard instans peluncuran Amazon EC2 - wizard tersebut menetapkan atribut ke `true`. Anda dapat mengubah atribut ini menggunakan konsol Amazon VPC.

Untuk mengubah perilaku pengalamatan IPv4 publik subnet Anda

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 pengaturan subnet.
4. Kotak centang Aktifkan penetapan alamat IPv4 publik otomatis, jika dipilih, permintaan alamat IPv4 publik untuk semua instans diluncurkan ke 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.

Memodifikasi atribut pengalamatan IPv6 untuk subnet Anda

Secara default, semua subnet memiliki atribut pengalamatan IPv6 diatur ke `false`. Anda dapat mengubah atribut ini menggunakan konsol Amazon VPC. Jika Anda mengaktifkan atribut pengalamatan IPv6 untuk subnet Anda, antarmuka jaringan yang dibuat di subnet menerima alamat IPv6 dari rentang subnet. Instans yang diluncurkan ke subnet menerima alamat IPv6 pada antarmuka jaringan primer.

Subnet Anda harus memiliki blok CIDR IPv6 terkait.

> **Note**
>
> Jika Anda mengaktifkan fitur pengalamatan IPv6 untuk subnet Anda, antarmuka jaringan Anda atau instans hanya menerima alamat IPv6 jika dibuat menggunakan API Amazon EC2 versi `2016-11-15` atau yang lebih baru. Konsol Amazon EC2 menggunakan API versi terbaru.

Untuk mengubah perilaku pengalamatan IPv6 subnet Anda

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 pengaturan subnet.
4. Kotak centang Aktifkan penetapan alamat IPv6 otomatis, jika dipilih, meminta alamat IPv6 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 alamat IPv4 atau IPv6 yang Anda sisihkan sehingga tidak AWS dapat menetapkannya ke antarmuka jaringan Anda. Ini memungkinkan Anda untuk memesan blok IPv4 atau 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 — AWS menetapkan alamat dari rentang alamat IP yang dicadangkan ke antarmuka jaringan. Untuk informasi selengkapnya, lihat Menetapkan awalan ke antarmuka jaringan Amazon EC2 di Panduan Pengguna Amazon EC2.
- Eksplisit - Anda secara manual menetapkan alamat IP ke 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

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 Amazon VPC 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-05eef9fb78EXAMPLE
```

Menghapus reservasi CIDR subnet

Anda dapat menggunakan create-subnet-cidr-reservation untuk menghapus reservasi CIDR subnet.

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

Konfigurasikan tabel rute

Tabel rute berisi seperangkat aturan, yang disebut rute, yang menentukan ke mana lalu lintas jaringan dari subnet atau gateway Anda diarahkan.

Daftar Isi

- Opsi perutean contoh
- Cara menggunakan tabel rute
- Wisaya perutean Middlebox

Konsep tabel rute

Berikut ini adalah konsep utama 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.
- 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.
- Rute lokal—Rute default untuk komunikasi dalam VPC.
- 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 VPN Site-to-Site di Panduan Pengguna VPN Site-to-Site.
- 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.

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

Setiap rute dalam sebuah tabel rute menentukan tujuan dan target. Misalnya, untuk mengaktifkan subnet Anda mengakses internet melalui gateway internet, tambahkan rute berikut ke tabel rute subnet Anda. Tujuan untuk rute tersebut adalah `0.0.0.0/0`, yang mewakili semua alamat IPv4. Targetnya adalah gateway internet yang melekat pada VPC Anda.

Tujuan	Target
0.0.0.0/0	*igw-id*

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

Jika Anda sering mereferensikan kumpulan blok CIDR yang sama di seluruh AWS sumber daya Anda, Anda dapat membuat daftar awalan yang dikelola pelanggan untuk 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 CIDR IPv4, tabel rute Anda akan berisikan rute lokal untuk setiap blok CIDR IPv4. Jika Anda telah mengaitkan sebuah blok CIDR IPv6 dengan VPC Anda, tabel rute Anda berisikan rute lokal untuk blok CIDR IPv6. Anda dapat mengganti atau mengembalikan target setiap rute lokal sesuai kebutuhan.

Aturan dan pertimbangan

- Anda dapat menambahkan rute ke tabel rute Anda yang lebih spesifik daripada rute lokal. Tujuan harus cocok dengan seluruh blok IPv4 atau IPv6 CIDR subnet di VPC Anda. Target harus berupa gateway NAT, antarmuka jaringan, atau titik akhir Gateway Load Balancer.
- Jika tabel rute Anda memiliki beberapa rute, kami menggunakan rute paling spesifik yang bersesuaian dengan lalu lintas (prefiks terpanjang yang sesuai) untuk menentukan cara merutekan lalu lintas.
- Anda tidak dapat menambahkan rute ke alamat IPv4 yang sama persis atau subset dari rentang berikut: 169.254.168.0/22. Rentang ini berada dalam ruang alamat link-lokal dan dicadangkan untuk digunakan oleh AWS layanan. Misalnya, Amazon EC2 menggunakan alamat dalam rentang ini untuk layanan yang hanya dapat diakses dari instans EC2, seperti 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 alamat IPv6 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 instans EC2, 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 IPv4 CIDR dan blok IPv6 CIDR. Lalu lintas IPv4 dan IPv6 diperlakukan secara terpisah, seperti yang ditunjukkan pada tabel rute berikut.

Tujuan	Target
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Local
172.31.0.0/16	pcx-11223344556677889
0.0.0.0/0	igw-12345678901234567
::/0	eigw-aabbccddee1122334

- Lalu lintas IPv4 yang akan diarahkan dalam VPC (10.0.0.0/16) dicakup oleh rute. Local
- Lalu lintas IPv6 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 lalu lintas IPv4 (0.0.0.0/0) mengirimkan lalu lintas ke gateway internet. Oleh karena itu, semua lalu lintas IPv4, kecuali untuk lalu lintas di dalam VPC dan ke koneksi peering, diarahkan ke gateway internet.
- Rute untuk semua lalu lintas IPv6 (:: /0) mengirimkan lalu lintas ke gateway internet khusus egres. Oleh karena itu, semua lalu lintas IPv6, kecuali untuk lalu lintas di dalam VPC, diarahkan 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.

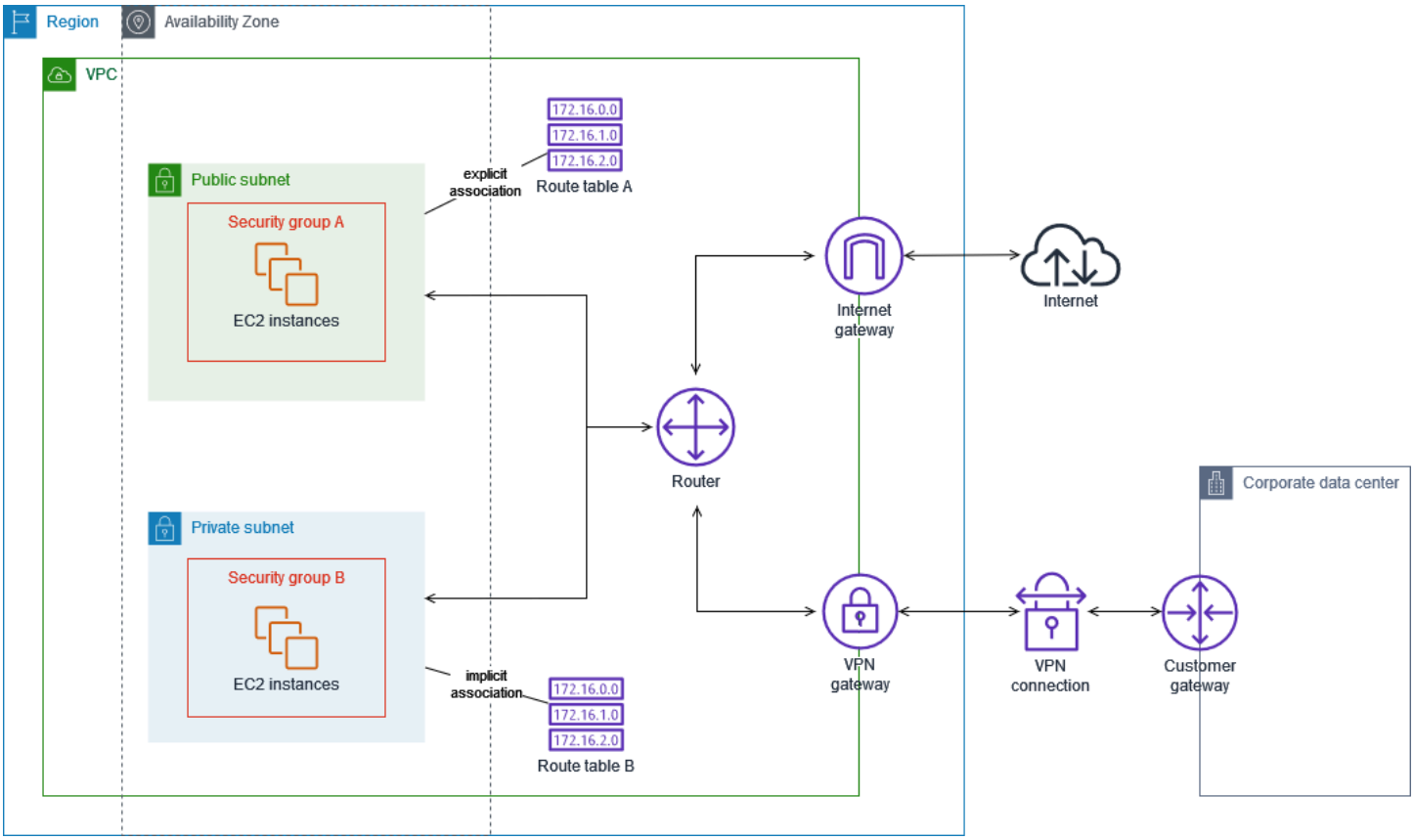
Pengaitan tabel rute subnet

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 subnet dan atau gateway mana yang secara eksplisit terkait.

Subnet yang ada di VPC yang dikaitkan dengan Outposts dapat memiliki target tambahan jenis gateway lokal. Ini adalah satu-satunya perbedaan perutean dari subnet non-Outposts.

Contoh 1: pengaitan subnet implisit dan eksplisit

Diagram berikut menunjukkan 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
VPC CIDR	Lokal:
0.0.0.0/0	*igw-id*

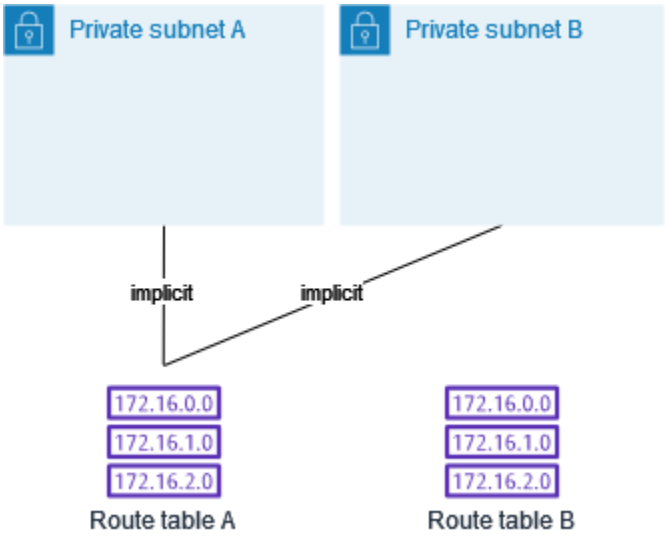
Tabel rute B adalah tabel rute utama. Ini secara implisit terkait dengan subnet pribadi. Ini memiliki rute yang mengirimkan semua lalu lintas ke gateway pribadi virtual, tetapi tidak ada rute ke gateway internet, yang membuat subnet menjadi subnet khusus VPN. Jika Anda membuat subnet lain di VPC ini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

Tujuan	Target
VPC CIDR	Lokal:
0.0.0.0/0	*vgw-id*

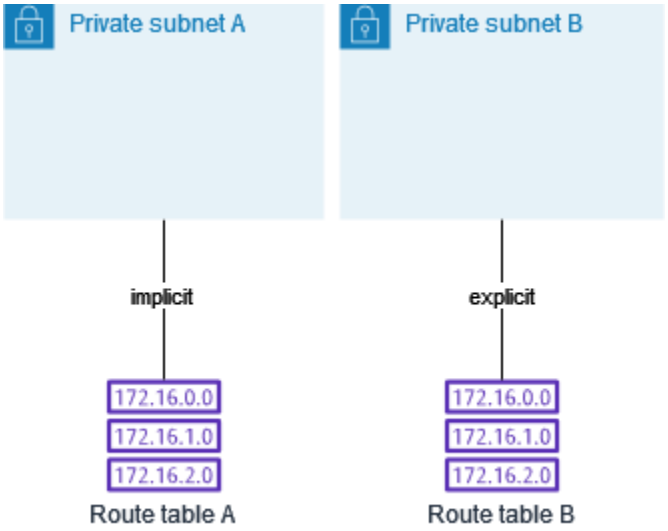
Contoh 2: Mengganti tabel rute utama

Anda mungkin ingin membuat perubahan ke tabel rute utama. Untuk menghindari gangguan pada lalu lintas Anda, sebaiknya Anda terlebih dahulu menguji perubahan rute menggunakan tabel rute kustom. Setelah Anda puas dengan pengujian tersebut, Anda dapat mengganti tabel rute utama dengan tabel kustom yang baru.

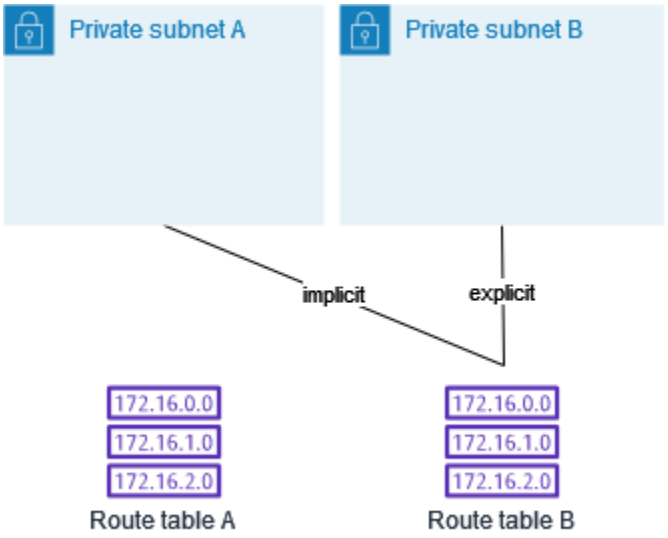
Diagram berikut menunjukkan dua subnet dan dua tabel rute. Subnet A secara implisit dikaitkan dengan tabel rute A, tabel rute utama. Subnet B secara implisit dikaitkan dengan tabel rute A. Tabel rute B, tabel rute khusus, tidak terkait dengan subnet mana pun.



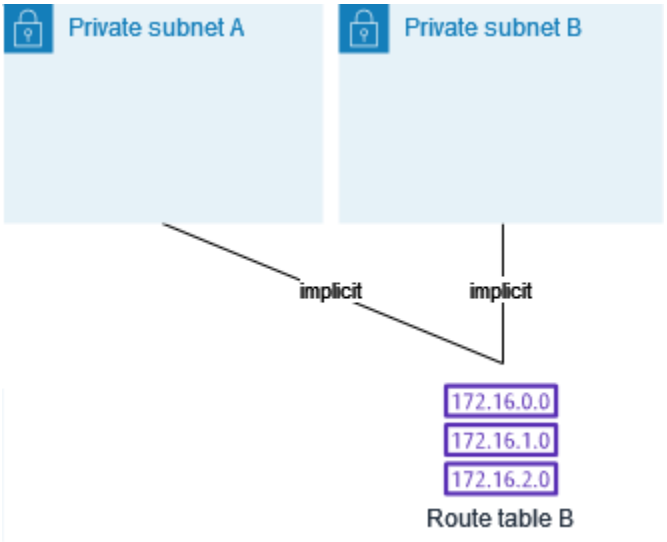
Untuk mengganti tabel rute utama, mulailah dengan membuat asosiasi eksplisit antara subnet B dan tabel rute B. Tabel rute uji B.



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 mencegat lalu lintas yang memasuki VPC Anda melalui gateway internet dengan mengarahkan lalu lintas ke perangkat middlebox (seperti perangkat keamanan) di VPC Anda.

Daftar Isi

Rute tabel rute gateway

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 blok CIDR IPv4 atau IPv6 dari VPC Anda. Dalam kasus ini, Anda ganti target rute lokal default.
- Seluruh blok CIDR IPv4 atau IPv6 dari subnet di VPC Anda. Ini adalah rute yang lebih spesifik dari rute lokal default.

Jika Anda mengubah target rute lokal dalam sebuah tabel rute gerbang ke antarmuka jaringan di VPC Anda, Anda nanti dapat mengembalikannya ke target `local` default. Untuk informasi selengkapnya, lihat Mengganti atau memulihkan target untuk rute lokal.

Contoh

Dalam tabel rute gateway berikut, lalu lintas yang ditujukan untuk subnet dengan blok CIDR `172.31.0.0/20` diarahkan ke antarmuka jaringan tertentu. Lalu lintas yang ditujukan untuk semua subnet lain di VPC menggunakan rute lokal.

Tujuan	Target
172.31.0.0/16	Lokal
172.31.0.0/20	*eni-id*

Contoh

Dalam tabel rute gateway berikut, target untuk rute lokal diganti dengan ID antarmuka jaringan. Lalu lintas yang ditujukan untuk semua subnet di dalam VPC diarahkan menuju antarmuka jaringan.

Tujuan	Target
172.31.0.0/16	*eni-id*

Aturan dan pertimbangan

Anda tidak dapat mengaitkan sebuah tabel rute dengan gateway jika salah satu dari berikut ini berlaku:

- Tabel rute berisikan rute-rute yang ada dengan target selain dari antarmuka jaringan, titik akhir Penyeimbang Beban Gateway, atau rute lokal default.
- Tabel rute berisikan rute yang ada untuk blok CIDR di luar kisaran di VPC Anda.
- Rute propagasi diaktifkan untuk tabel rute.

Sebagai tambahan, aturan dan pertimbangan berikut berlaku:

- Anda tidak dapat menambahkan rute ke setiap blok CIDR di luar kisaran di VPC Anda, termasuk kisaran yang lebih besar dari masing-masing blok CIDR VPC.
- Anda hanya dapat menentukan `local`, titik akhir Penyeimbang Beban Gateway, atau antarmuka jaringan sebagai target. Anda tidak dapat menentukan jenis target lainnya, termasuk alamat IP host individu. Untuk informasi selengkapnya, lihat the section called “Opsi perutean contoh”.
- Anda tidak dapat menentukan daftar prefiks sebagai tujuan.
- Anda tidak dapat menggunakan tabel rute gateway untuk mengendalikan atau mencegat lalu lintas di luar VPC Anda, misalnya, lalu lintas melalui Transit Gateway yang terlampir. Anda dapat mencegat lalu lintas yang memasuki VPC Anda dan mengarahkannya kembali ke target lain di VPC yang sama.
- Untuk memastikan lalu lintas mencapai perangkat middlebox Anda, antarmuka jaringan target harus dilampirkan ke instans yang sedang berjalan. Untuk lalu lintas yang mengalir melalui gateway internet, antarmuka jaringan target juga harus memiliki alamat IP publik.
- Saat mengkonfigurasi perangkat middlebox Anda, perhatikan Pertimbangan perangkat.
- Ketika Anda mengarahkan lalu lintas melalui perangkat middlebox, lalu lintas yang kembali dari subnet tujuan harus diarahkan melalui perangkat yang sama. Perutean asimetris tidak di-support.
- Aturan tabel rute berlaku untuk semua lalu lintas yang meninggalkan subnet. Lalu lintas yang meninggalkan subnet didefinisikan sebagai lalu lintas yang ditujukan ke alamat MAC router gateway subnet 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.

Prioritas rute

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 Isi

Pertandingan awalan terpanjang

Rute ke alamat IPv4 dan IPv6 atau blok CIDR tidak saling ketergantungan satu sama lain. Kami menggunakan rute yang paling spesifik yang sesuai baik lalu lintas IPv4 atau lalu lintas IPv6 untuk menentukan bagaimana mengarahkan lalu lintas.

Contoh tabel rute subnet berikut memiliki rute untuk lalu lintas internet IPv4 (`0.0.0.0/0`) yang menunjuk ke gateway internet, dan rute untuk lalu lintas `172.31.0.0/16` IPv4 yang menunjuk ke koneksi peering (). `pcx-11223344556677889` Setiap lalu lintas dari subnet yang ditujukan untuk kisaran alamat IP `172.31.0.0/16` menggunakan koneksi peering, karena rute ini lebih spesifik daripada rute untuk gateway internet. Setiap lalu lintas yang ditujukan untuk target di dalam VPC (`10.0.0.0/16`) tercakup oleh rute `local`, dan oleh karenanya lalu lintas diarahkan di dalam VPC. Semua lalu lintas lainnya dari subnet menggunakan gateway internet.

Tujuan	Target
10.0.0.0/16	lokal
172.31.0.0/16	pcx-11223344556677889
0.0.0.0/0	igw-12345678901234567

Prioritas rute dan rute yang disebarkan

Jika Anda telah melampirkan sebuah virtual private gateway 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 disebarkan di tabel rute Anda.

Jika tujuan rute propagasi tumpang tindih dengan rute statis, rute statis akan diprioritaskan.

Jika tujuan rute propagasi identik dengan tujuan rute statis, rute statis akan diprioritaskan jika targetnya adalah salah satu dari yang berikut:

- 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 disebarkan 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 dan daftar awalan

Jika tabel rute Anda mereferensikan daftar prefiks, aturan berikut berlaku:

- Jika tabel rute Anda berisi rute statis dengan blok CIDR tujuan yang tumpang tindih dengan rute statis dengan daftar awalan, rute statis dengan blok CIDR akan diprioritaskan.
- Jika tabel rute 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 disebarkan, rute statis, atau rute yang mereferensikan daftar awalan.
- Jika tabel rute Anda mereferensikan beberapa daftar prefiks yang memiliki blok-blok CIDR yang tumpang tindih ke target-target yang berbeda, kami secara acak memilih rute mana yang menjadi prioritas. Setelah itu, rute yang sama selalu menjadi prioritas.

Kuota tabel rute

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.

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 rute tabel rute yang hilang atau salah konfigurasi.

Untuk informasi selengkapnya, lihat Panduan Reachability Analyzer.

Opsi perutean contoh

Topik berikut menjelaskan perutean untuk gateway atau koneksi tertentu di VPC Anda.

Daftar Isi

- Perutean ke koneksi peering VPC
- Perutean ke VPC endpoint gateway
- Perutean ke gateway internet egress-only
- Perutean untuk Transit Gateway
- Perutean untuk perangkat middlebox
- Perutean menggunakan daftar prefiks
- Perutean ke titik akhir Penyeimbang Beban Gateway

Perutean ke gateway internet

Anda dapat membuat sebuah subnet menjadi subnet publik dengan menambahkan sebuah rute di tabel rute subnet Anda ke gateway internet. Untuk melakukannya, buat dan lampirkan gateway internet untuk VPC Anda, dan kemudian tambahkan rute dengan tujuan `0.0.0.0/0` untuk lalu lintas IPv4 atau lalu lintas IPv6 `::/0`, dan target ID gateway internet (`igw-xxxxxxxxxxxxxxxxx`).

Tujuan	Target
0.0.0.0/0	*igw-id*
::/0	*igw-id*

Untuk informasi selengkapnya, lihat Connect ke internet menggunakan gateway internet.

Perutean ke perangkat NAT

Untuk mengaktifkan instans di subnet pribadi agar terhubung ke internet, Anda dapat membuat gateway NAT atau meluncurkan instans NAT di subnet publik. Kemudian tambahkan rute untuk tabel rute subnet pribadi yang mengarahkan lalu lintas internet IPv4 (`0.0.0.0/0`) ke perangkat NAT.

Tujuan	Target
0.0.0.0/0	*nat-gateway-id*

Anda juga dapat membuat rute yang lebih spesifik ke target lain untuk menghindari biaya pemrosesan data yang tidak perlu untuk menggunakan gateway NAT, atau untuk mengarahkan

lalu lintas tertentu secara pribadi. Dalam contoh berikut, lalu lintas Amazon S3 (pl-xxxxxxxx, daftar awalan yang berisi rentang alamat IP untuk Amazon S3 di Wilayah tertentu) 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	*nat-gateway-id*
pl-*xxxxxxxx*	*vpce-id*
10.25.0.0/16	*pcx-id*

Untuk informasi selengkapnya, lihat Perangkat NAT.

Perutean ke virtual private gateway

Anda dapat menggunakan AWS Site-to-Site VPN koneksi untuk mengaktifkan instance di VPC Anda untuk berkomunikasi dengan jaringan Anda sendiri. Untuk melakukannya, buat dan lampirkan virtual private gateway ke VPC Anda. Kemudian tambahkan rute di tabel rute subnet Anda dengan tujuan jaringan Anda dan target virtual private gateway (`vgw-xxxxxxxxxxxxxxxxx`).

Tujuan	Target
10.0.0.0/16	*vgw-id*

Anda kemudian dapat membuat dan mengonfigurasi koneksi Site-to-Site VPN. 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 di virtual private gateway tidak men-support lalu lintas IPv6. Namun, kami men-support lalu lintas IPv6 diarahkan melalui virtual private gateway ke koneksi AWS Direct Connect . Untuk informasi selengkapnya, 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

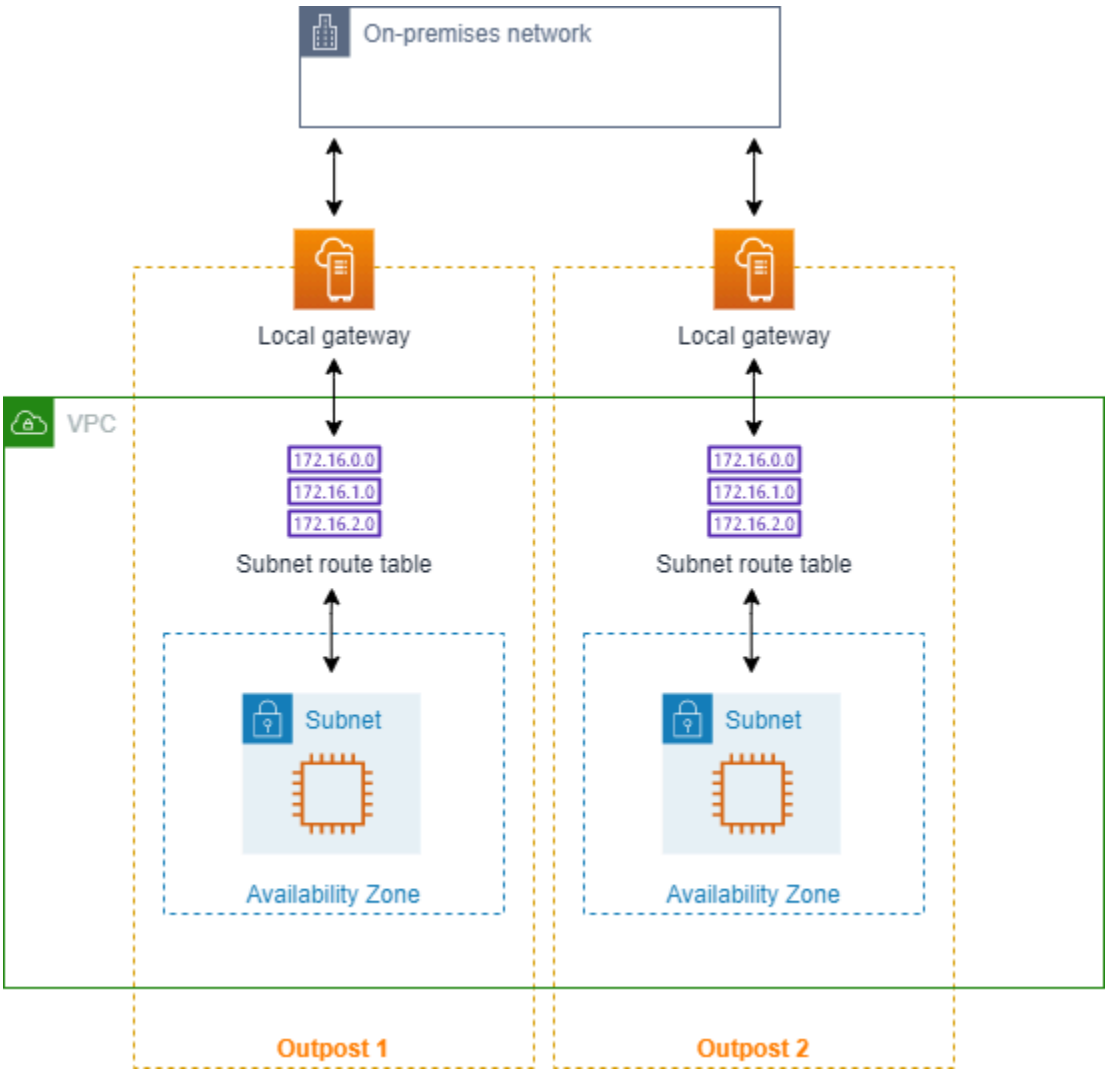
Subnet yang ada di VPC yang terkait dengan AWS Outposts dapat memiliki jenis target tambahan dari gateway lokal. Pertimbangkan kasus di mana Anda ingin memiliki lalu lintas rute gateway lokal dengan alamat tujuan 192.168.10.0/24 ke jaringan pelanggan. Untuk melakukannya, tambahkan rute berikut dengan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

Tujuan	Target
192.168.10.0/24	*lgw-id*

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 ditambatkan ke AZ yang berbeda.



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 blok IPv4 subnet di VPC Anda yang ada di Outpost lain. Ulangi konfigurasi ini untuk semua subnet Outpost yang perlu berkomunikasi.

Important

- Untuk menggunakan fitur ini, Anda harus menggunakan routing VPC langsung. Anda tidak dapat menggunakan alamat IP milik pelanggan Anda sendiri.
- Jaringan 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 ID grup keamanan.
- 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	*lgw-1-id*

Entri untuk tabel rute subnet Outpost 2 adalah sebagai berikut:

Tujuan	Target
10.0.0.0/16	Lokal
10.0.1.0/24	*lgw-2-id*

Perutean ke koneksi peering VPC

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

Untuk mengaktifkan perutean lalu lintas antar VPC dalam koneksi peering VPC, Anda harus menambahkan rute ke satu atau lebih tabel rute subnet yang mengarah ke koneksi peering VPC. Ini

memungkinkan Anda mengakses semua atau sebagian blok CIDR dari VPC yang lain dalam koneksi peering. Demikian pula, pemilik VPC yang lain harus menambahkan rute ke tabel rute subnet mereka untuk mengarahkan lalu lintas kembali ke VPC Anda.

Misalnya, Anda memiliki koneksi peering VPC (`pcx-11223344556677889`) di antara dua VPC, dengan informasi berikut:

- VPC A: Blok CIDR adalah 10.0.0.0/16
- VPC B: Blok CIDR adalah 172.31.0.0/16

Untuk mengaktifkan lalu lintas antar VPC dan mengizinkan akses ke seluruh blok CIDR IPv4 dari VPC manapun, tabel rute VPC A dikonfigurasi sebagai berikut.

Tujuan	Target
10.0.0.0/16	Lokal
172.31.0.0/16	pcx-11223344556677889

Tabel rute VPC B dikonfigurasi sebagai berikut.

Tujuan	Target
172.31.0.0/16	Lokal
10.0.0.0/16	pcx-11223344556677889

Koneksi peering VPC Anda juga dapat men-support komunikasi IPv6 antar instans di VPC, jika VPC dan instans diaktifkan untuk komunikasi IPv6. Untuk mengaktifkan perutean lalu lintas IPv6 antar VPC, Anda harus menambahkan rute ke tabel rute Anda yang mengarah ke koneksi peering VPC untuk mengakses semua atau sebagian blok CIDR IPv6 dari VPC rekan.

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

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

Untuk mengaktifkan komunikasi IPv6 melalui koneksi peering VPC, tambahkan rute berikut ke tabel rute subnet untuk VPC A.

Tujuan	Target
10.0.0.0/16	Lokal
172.31.0.0/16	pcx-11223344556677889
2001:db8:5678:2b00::/56	pcx-11223344556677889

Tambahkan rute berikut ke tabel rute untuk VPC B.

Tujuan	Target
172.31.0.0/16	Lokal
10.0.0.0/16	pcx-11223344556677889
2001:db8:1234:1a00::/56	pcx-11223344556677889

Untuk informasi selengkapnya tentang koneksi peering VPC, lihat Panduan Peering Amazon VPC.

Perutean ke VPC endpoint gateway

Titik akhir VPC gateway memungkinkan Anda membuat koneksi pribadi antara VPC Anda dan layanan lain. AWS Ketika Anda membuat titik akhir gateway, Anda menentukan tabel rute subnet di VPC Anda yang digunakan oleh titik akhir gateway. Sebuah rute secara otomatis ditambahkan ke masing-masing tabel rute dengan tujuan yang menentukan ID layanan daftar prefiks (`pl-xxxxxxxx`), dan target dengan ID titik akhir (`vpce-xxxxxxxxxxxxxxxxx`). Anda tidak dapat secara eksplisit menghapus atau memodifikasi rute titik akhir, tetapi Anda dapat mengubah tabel rute yang digunakan oleh titik akhir.

Untuk informasi lebih lanjut tentang perutean untuk titik akhir, dan implikasi untuk rute ke layanan AWS , lihat Perutean untuk titik akhir gateway.

Perutean ke gateway internet egress-only

Anda dapat membuat gateway internet egress-only untuk VPC Anda untuk mengaktifkan instans di subnet pribadi untuk mulai berkomunikasi outbound ke internet, tetapi mencegah internet untuk terhubung dengan instans. Gateway internet egress-only digunakan untuk lalu lintas IPv6 saja. Untuk mengonfigurasi perutean untuk gateway internet egress-only, tambahkan sebuah rute dalam tabel rute subnet pribadi yang mengarahkan lalu lintas internet IPv6 (`::/0`) ke gateway internet egress-only.

Tujuan	Target
::/0	*eigw-id*

Untuk informasi selengkapnya, lihat Aktifkan lalu lintas IPv6 keluar menggunakan gateway internet khusus egres.

Perutean untuk Transit Gateway

Ketika Anda melampirkan sebuah VPC ke Transit Gateway, Anda perlu menambahkan rute ke tabel rute subnet Anda agar lalu lintas dapat terarahkan melalui Transit Gateway.

Pertimbangkan skenario berikut di mana Anda memiliki tiga VPC yang dipasangkan ke Transit Gateway. Dalam skenario ini, semua lampiran dikaitkan dengan tabel rute transit gateway dan mempropagasi tabel rute transit gateway. Oleh karena itu, semua lampiran dapat mengarahkan paket satu sama lain, dengan Transit Gateway yang berfungsi sebagai pusat IP 3 lapis sederhana.

Misalnya, Anda memiliki dua VPC, dengan informasi berikut:

- VPC A: 10.1.0.0/16, ID lampiran tgw-attach-11111111111111111
- VPC B: 10.2.0.0/16, ID lampiran tgw-attach-22222222222222222

Untuk mengaktifkan lalu lintas antar VPC dan mengizinkan akses ke Transit Gateway, tabel rute VPC A dikonfigurasi sebagai berikut.

Tujuan	Target
10.1.0.0/16	Lokal

Tujuan	Target
10.0.0.0/8	*tgw-id*

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

Tujuan	Target
10.1.0.0/16	tgw-attach-11111111111111111
10.2.0.0/16	tgw-attach-22222222222222222

Untuk informasi selengkapnya tabel rute Transit Gateway, lihat Perutean di Transit Gateway Amazon VPC.

Perutean untuk perangkat middlebox

Anda dapat menambahkan peralatan middlebox ke jalur 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. Perangkat ini digunakan sebagai instans Amazon EC2 di subnet di VPC Anda, dan diwakili oleh antarmuka jaringan elastis (antarmuka jaringan) di subnet Anda.

Jika Anda mengaktifkan propagasi rute untuk tabel rute subnet tujuan, perhatikan prioritas rute. Kami memprioritaskan rute yang paling spesifik, dan jika rute cocok, kami memprioritaskan rute statis atas rute yang disebarkan. Tinjau rute Anda untuk memastikan bahwa lalu lintas dirutekan dengan benar dan tidak ada konsekuensi yang tidak diinginkan jika Anda mengaktifkan atau menonaktifkan propagasi rute (misalnya, propagasi rute diperlukan untuk 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 perutean middlebox, lihat. Skenario Middlebox

Daftar Isi

Pertimbangan perangkat

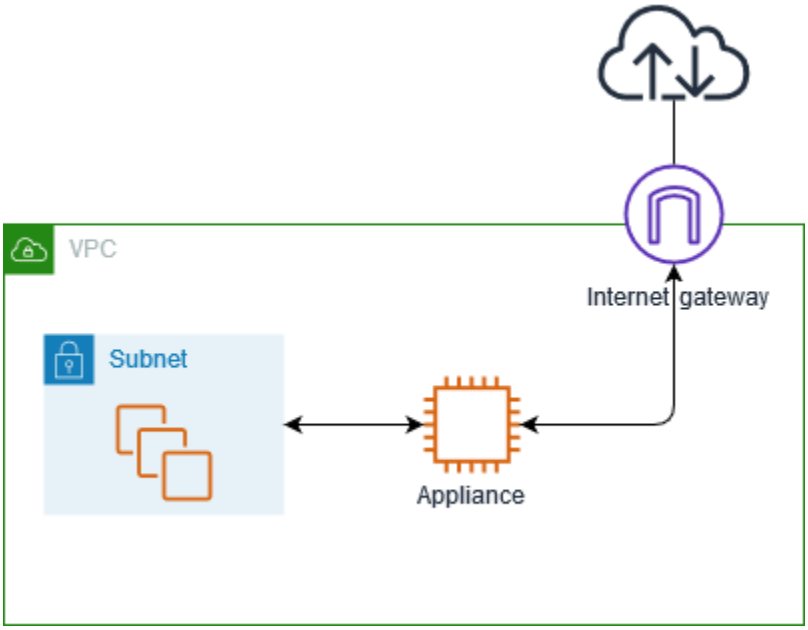
Anda dapat memilih perangkat pihak ketiga dari AWS Marketplace, atau Anda dapat mengonfigurasi perangkat Anda sendiri. Saat Anda membuat atau mengonfigurasi sebuah perangkat, perhatikan hal berikut:

- Perangkat harus dikonfigurasi di subnet terpisah ke lalu lintas sumber atau tujuan.
- Anda harus menonaktifkan pemeriksaan sumber/tujuan pada perangkat. Untuk informasi selengkapnya, lihat Mengubah Pemeriksaan Sumber atau Tujuan di Panduan Pengguna Amazon EC2.
- Anda tidak dapat mengarahkan lalu lintas antar host di subnet yang sama melalui sebuah perangkat.
- Alat tidak harus melakukan penerjemahan alamat jaringan (NAT).
- Anda dapat menambahkan rute ke tabel rute 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 sesuai dengan seluruh blok IPv4 atau IPv6 CIDR dari subnet di VPC Anda.

- Untuk mencegat lalu lintas IPv6, pastikan VPC, subnet, dan alat Anda mendukung IPv6. Gateway privat virtual tidak men-support lalu lintas 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 lalu lintas IPv4 yang ditujukan untuk subnet ke antarmuka jaringan untuk alat. Rute ini lebih spesifik daripada rute lokal.

Tujuan	Target
VPC CIDR	Lokal:
Subnet CIDR	*ID antarmuka jaringan alat*

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
VPC CIDR	*ID antarmuka jaringan alat*

Untuk mengarahkan lalu lintas dari subnet Anda ke perangkat di subnet lain, tambahkan rute ke tabel rute subnet Anda yang mengarahkan lalu lintas ke antarmuka jaringan perangkat. Tujuan seharusnya tidak lebih spesifik dibandingkan tujuan untuk rute lokal. Misalnya, untuk lalu lintas yang ditujukan untuk internet, tentukan `0.0.0.0/0` (semua alamat IPv4) untuk tujuan tersebut.

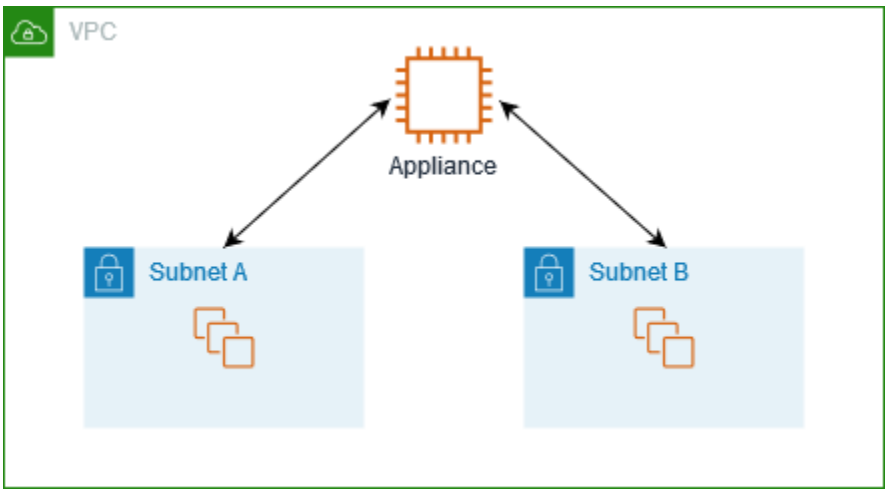
Tujuan	Target
VPC CIDR	Lokal:
0.0.0.0/0	*ID antarmuka jaringan alat*

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
VPC CIDR	Lokal:
0.0.0.0/0	*igw-id*

Merutekan lalu lintas antar-subnet ke alat

Anda dapat merutekan lalu lintas yang ditujukan untuk subnet tertentu ke antarmuka jaringan alat. Dalam contoh berikut, VPC berisi dua subnet dan alat. Lalu lintas 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
VPC CIDR	Lokal:
Subnet B CIDR	*ID antarmuka jaringan alat*

Berikut ini adalah contoh tabel rute untuk subnet B. Entri pertama memungkinkan instance di VPC untuk berkomunikasi satu sama lain. Entri kedua merutekan semua lalu lintas dari subnet B ke subnet A ke antarmuka jaringan alat.

Tujuan	Target
VPC CIDR	Lokal:
Subnet Untuk CIDR	*ID antarmuka jaringan alat*

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
VPC CIDR	*ID antarmuka jaringan alat*

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. VPC harus dapat berkomunikasi dengan dua lampiran VPC tertentu yang memiliki blok CIDR berikut:

- 10.0.0.0/16
- 10.2.0.0/16

Anda buat daftar prefiks dengan kedua entri. Dalam tabel rute subnet Anda, Anda membuat rute dan menentukan daftar prefiks sebagai tujuan, dan Transit Gateway sebagai target.

Tujuan	Target
172.31.0.0/16	Lokal
pl-123abc123abc123ab	*tgw-id*

Jumlah entri maksimal untuk daftar prefiks sama dengan jumlah entri dalam tabel rute.

Perutean ke titik akhir Penyeimbang Beban Gateway

Sebuah Penyeimbang Beban Gateway memungkinkan Anda untuk mendistribusikan lalu lintas ke sebuah armada perangkat virtual, seperti firewall. Anda dapat mengonfigurasi penyeimbang beban sebagai layanan dengan membuat konfigurasi layanan VPC endpoint. Anda kemudian membuat Titik akhir Penyeimbang Beban Gateway di VPC Anda untuk meng-connect VPC Anda 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	*vpc-titik akhir id*

Untuk informasi selengkapnya, lihat Gateway Load Balancers.

Cara menggunakan tabel rute

Bagian ini menjelaskan cara bekerja dengan tabel rute.

Daftar Isi

- Ubah tabel rute untuk subnet
- Memutus pengaitan subnet dari tabel rute
- Ganti tabel rute utama
- Kaitkan gateway dengan tabel rute
- Putuskan pengaitan gateway dari tabel rute
- Mengganti atau memulihkan target untuk rute lokal
- Hapus tabel rute

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

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 rutenya. Untuk menentukan apakah asosiasi ke tabel rute utama, dan jika asosiasi itu eksplisit, lihatTentukan subnet dan atau gateway mana yang secara eksplisit terkait.

Tentukan subnet dan atau gateway mana yang secara eksplisit terkait

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 menggambarkan satu atau lebih tabel rute dan melihat kemana pengaitannya dengan menggunakan baris perintah

- describe-route-tables (AWS CLI)
- Get-EC2RouteTable (AWS Tools for Windows PowerShell)

Membuat tabel rute kustom

Anda dapat membuat tabel rute kustom untuk VPC Anda menggunakan konsol Amazon VPC.

Untuk membuat tabel rute kustom 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 kustom menggunakan baris perintah

- create-route-table (AWS CLI)
- New-EC2RouteTable (AWS Tools for Windows PowerShell)

Tambahkan dan hapus rute dari tabel rute

Anda dapat menambahkan, menghapus, dan memodifikasi rute dalam tabel rute Anda. Anda hanya dapat memodifikasi rute yang telah Anda tambahkan.

Untuk informasi selengkapnya tentang bekerja dengan rute statis untuk koneksi Site-to-Site VPN, lihat Menyunting Rute Statis untuk Koneksi Site-to-Site VPN di Panduan Pengguna AWS Site-to-Site VPN .

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 blok CIDR tujuan, alamat IP tunggal, atau ID dari daftar prefiks.
5. Untuk mengubah rute, untuk Tujuan, ganti blok CIDR tujuan atau alamat IP tunggal. Untuk Target, pilih target.
6. Untuk menghapus rute, pilih Hapus.
7. Pilih Simpan perubahan.

Untuk memperbarui rute untuk tabel rute menggunakan baris perintah

- create-route (AWS CLI)
- replace-route (AWS CLI)
- delete-route (AWS CLI)
- New-EC2Route (AWS Tools for Windows PowerShell)
- Set-EC2Route (AWS Tools for Windows PowerShell)
- Remove-EC2Route (AWS Tools for Windows PowerShell)

> **Note**
>
> 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`.

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 VPN Site-to-Site di Panduan Pengguna VPN Site-to-Site.

Untuk mengaktifkan 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 Aktifkan kotak centang di samping virtual private gateway, dan kemudian pilih Simpan.

Untuk mengaktifkan propagasi rute menggunakan baris perintah

- enable-vgw-route-propagation (AWS CLI)
- Enable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

Untuk 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. Kosongkan kotak centang Aktifkan di sebelah gateway pribadi virtual, lalu pilih Simpan.

Untuk menonaktifkan propagasi rute menggunakan baris perintah

- disable-vgw-route-propagation (AWS CLI)
- Disable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

Kaitkan subnet dengan tabel rute

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.

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 subnet dengan tabel rute menggunakan baris perintah

- associate-route-table (AWS CLI)
- Register-EC2RouteTable (AWS Tools for Windows PowerShell)

Ubah tabel rute untuk subnet

Anda dapat mengubah pengaitan tabel rute untuk subnet.

Ketika Anda mengubah tabel rute, koneksi yang ada di subnet ditiadakan kecuali tabel rute yang baru berisikan rute untuk lalu lintas yang sama dengan target yang sama.

Untuk mengubah pengaitan tabel rute subnet menggunakan konsol tersebut

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

2. Di panel navigasi, pilih Subnet, lalu pilih subnet.
3. Dari tab Tabel rute, pilih Edit asosiasi tabel rute.
4. Untuk ID tabel Route, pilih tabel rute baru.
5. Pilih Simpan.

Untuk mengubah tabel rute yang dikaitkan dengan subnet menggunakan baris perintah

- replace-route-table-association (AWS CLI)
- Set-EC2RouteTableAssociation (AWS Tools for Windows PowerShell)

Memutus pengaitan subnet dari tabel rute

Anda dapat memutus pengaitan subnet dari tabel rute. Sebelum Anda mengaitkan subnet dengan tabel rute lain, subnet secara implisit terkait dengan tabel rute utama.

Untuk memutus pengaitan subnet dari tabel rute 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. Dari tab Asosiasi subnet, pilih Edit asosiasi subnet.
4. Kosongkan kotak centang untuk subnet.
5. Pilih Simpan pengaitan.

Untuk memutuskan pengaitan subnet dari tabel rute menggunakan baris perintah

- disassociate-route-table (AWS CLI)
- Unregister-EC2RouteTable (AWS Tools for Windows PowerShell)

Ganti tabel rute utama

Anda dapat mengubah tabel rute mana yang menjadi tabel rute utama di VPC Anda.

Untuk mengganti tabel rute utama menggunakan konsol

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

2. Di panel navigasi, pilih Tabel rute, lalu pilih tabel rute utama yang baru.
3. Pilih Tindakan, Atur tabel rute utama.
4. Saat diminta konfirmasi, masukkan**`set`**, lalu pilih OK.

Untuk mengganti tabel rute utama menggunakan baris perintah

- replace-route-table-association (AWS CLI)
- Set-EC2RouteTableAssociation (AWS Tools for Windows PowerShell)

Prosedur berikut ini menjelaskan cara menghapus pengaitan eksplisit antara subnet dan tabel rute utama. Hasilnya adalah pengaitan implisit antara subnet dan tabel rute utama. Proses ini sama dengan memutus pengaitan subnet apapun dari setiap tabel rute.

Untuk menghapus pengaitan eksplisit dengan tabel rute utama

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Tabel rute, lalu pilih tabel rute.
3. Dari tab Asosiasi subnet, pilih Edit asosiasi subnet.
4. Kosongkan kotak centang untuk subnet.
5. Pilih Simpan pengaitan.

Kaitkan gateway dengan tabel rute

Anda dapat mengaitkan gateway internet atau virtual private gateway dengan tabel rute. Untuk informasi selengkapnya, lihat Tabel rute gateway.

Untuk mengaitkan gateway dengan tabel rute 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. Dari tab Asosiasi tepi, pilih Edit asosiasi tepi.
4. Pilih kotak centang untuk gateway.
5. Pilih Simpan perubahan.

Untuk mengaitkan gateway dengan tabel rute menggunakan AWS CLI

Gunakan perintah associate-route-table. Contoh berikut mengaitkan gateway internet `igw-11aa22bb33cc44dd1` dengan tabel rute `rtb-01234567890123456`.

```
aws ec2 associate-route-table --route-table-id rtb-01234567890123456 --gateway-id
 igw-11aa22bb33cc44dd1
```

Putuskan pengaitan gateway dari tabel rute

Anda dapat memutus pengaitan gateway internet atau virtual private gateway dari tabel rute.

Untuk mengaitkan gateway dengan tabel rute 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. Dari tab Asosiasi tepi, pilih Edit asosiasi tepi.
4. Kosongkan kotak centang untuk gateway.
5. Pilih Simpan perubahan.

Untuk memutus pengaitan gateway dari tabel rute menggunakan baris perintah

- disassociate-route-table (AWS CLI)
- Unregister-EC2RouteTable (AWS Tools for Windows PowerShell)

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 memperbarui rute lokal menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Tabel rute, lalu pilih tabel rute.
3. Dari tab Rute, pilih Edit rute.
4. Untuk rute lokal, hapus Target dan kemudian pilih target baru.
5. Pilih Simpan perubahan.

Untuk memulihkan target untuk rute lokal menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Tabel rute, lalu pilih tabel rute.
3. Pilih Tindakan, Sunting rute.
4. Untuk rute, hapus Target, lalu pilih lokal.
5. Pilih Simpan perubahan.

Untuk mengganti target untuk rute lokal menggunakan AWS CLI

Gunakan perintah replace-route. Contoh berikut menggantikan target rute lokal dengan `eni-11223344556677889`.

```
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 memulihkan target lokal untuk tabel rute `rtb-01234567890123456`.

```
aws ec2 replace-route --route-table-id rtb-01234567890123456 --destination-cidr-block
 10.0.0.0/16 --local-target
```

Hapus tabel rute

Anda dapat menghapus tabel rute hanya jika tidak ada subnet yang dikaitkan dengannya. Anda tidak dapat menghapus tabel rute utama.

Untuk menghapus tabel rute 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. Pilih Tindakan, Hapus tabel rute.
4. Saat diminta konfirmasi, masukkan**`delete`**, lalu pilih Hapus.

Untuk menghapus tabel rute menggunakan baris perintah

- delete-route-table (AWS CLI)

- Remove-EC2RouteTable (AWS Tools for Windows PowerShell)

Wisaya perutean Middlebox

Jika Anda ingin mengonfigurasi kontrol butir halus atas jalur perutean lalu lintas yang memasuki atau meninggalkan VPC Anda, misalnya, dengan mengarahkan lalu lintas ke alat keamanan, Anda dapat menggunakan wizard perutean middlebox di konsol VPC. Wizard routing middlebox membantu Anda dengan secara otomatis membuat tabel rute dan rute yang diperlukan (hop) untuk mengarahkan lalu lintas sesuai kebutuhan.

Wizard routing middlebox dapat membantu Anda mengonfigurasi perutean untuk skenario berikut:

- Merutekan lalu lintas ke perangkat middlebox, misalnya, instans Amazon EC2 yang dikonfigurasi sebagai alat keamanan.
- Merutekan lalu lintas ke Load Balancer Gateway. Untuk informasi selengkapnya, lihat Panduan Pengguna untuk Penyeimbang Beban Gateway.

Untuk informasi selengkapnya, lihat the section called “Skenario Middlebox”.

Daftar Isi

Prasyarat wizard perutean Middlebox

Ulasanthe section called “Pertimbangan wizard perutean Middlebox”. Kemudian, pastikan bahwa Anda memiliki informasi berikut sebelum Anda menggunakan middlebox routing wizard.

- VPC.
- Sumber daya tempat lalu lintas berasal dari atau memasuki VPC, misalnya, gateway internet, gateway pribadi virtual, atau antarmuka jaringan.
- Antarmuka jaringan middlebox atau titik akhir Gateway Load Balancer.
- Subnet tujuan untuk lalu lintas.

Kelola rute middlebox

Wizard routing middlebox tersedia di file. Amazon Virtual Private Cloud Console

Daftar Isi

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. Pada panel navigasi, pilih VPC Anda.
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 Tujuan IPv4 CIDR, 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 Selanjutnya.
9. Pada halaman Tinjau dan buat, verifikasi rute, lalu pilih Buat rute.

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. Pada panel navigasi, pilih VPC Anda.
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 Selanjutnya.

8. Pada halaman Tinjau dan perbarui, daftar tabel rute dan rutenya yang akan dibuat oleh wizard perutean middlebox ditampilkan. Verifikasi rute, lalu di kotak dialog konfirmasi, pilih Perbarui rute.

Melihat tabel rute wizard routing middlebox

Untuk melihat tabel rute wizard routing middlebox

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih VPC Anda.
3. Pilih VPC Anda, lalu pilih Tindakan, Kelola rute middlebox.
4. Di bawah tabel rute Middlebox, angka tersebut menunjukkan berapa banyak rute yang dibuat oleh wizard routing middlebox. Pilih nomor untuk melihat rute.

Kami menampilkan rute wizard routing middlebox pada halaman tabel rute terpisah.

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. Untuk informasi selengkapnya, lihat the section called “Melihat 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. Untuk informasi selengkapnya, lihat the section called “Hapus tabel rute”.

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 Pengguna Amazon EC2.
- Tabel rute dan rute yang dibuat oleh wizard routing middlebox dihitung terhadap kuota Anda. Untuk informasi selengkapnya, lihat the section called “Tabel rute”.
- Jika Anda menghapus sumber daya, misalnya antarmuka jaringan, asosiasi tabel rute dengan sumber daya akan dihapus. Jika sumber daya adalah target, tujuan rute diatur ke lubang hitam. Tabel rute tidak dihapus.
- Subnet middlebox dan subnet tujuan harus dikaitkan dengan tabel rute non-default.

> **Note**
>
> Sebaiknya gunakan wizard perutean middlebox untuk memodifikasi atau menghapus tabel rute apa pun yang Anda buat menggunakan wizard perutean middlebox.

Skenario Middlebox

Contoh berikut menjelaskan skenario untuk wizard middlebox routing.

Daftar Isi

Periksa lalu lintas yang ditakdirkan untuk subnet

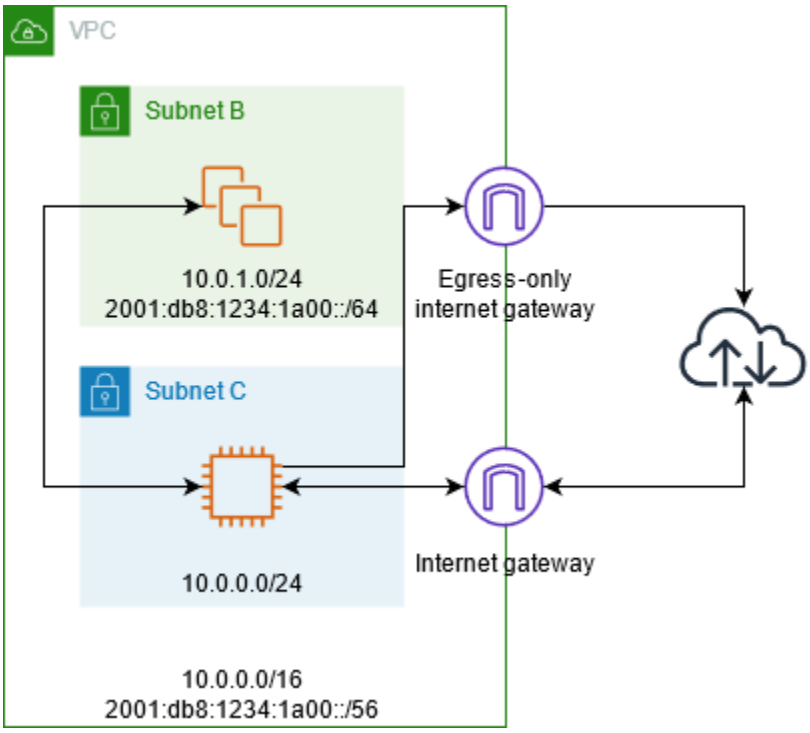
Pertimbangkan skenario di mana Anda memiliki lalu lintas yang masuk ke VPC melalui gateway internet dan Anda ingin memeriksa semua lalu lintas yang ditujukan untuk subnet, katakanlah subnet B, menggunakan alat firewall yang diinstal pada instans EC2. Alat firewall harus diinstal dan dikonfigurasi pada instans EC2 di subnet terpisah dari subnet B di VPC Anda, katakanlah subnet C. Anda kemudian dapat menggunakan wizard perutean middlebox untuk mengkonfigurasi rute untuk lalu lintas antara subnet B dan gateway internet.

Wizard perutean kotak tengah, secara otomatis melakukan operasi berikut:

- Menciptakan tabel rute berikut:
  - Tabel rute untuk gateway internet
  - Tabel rute untuk subnet tujuan tujuan untuk tujuan tujuan tujuan
  - Tabel rute untuk subnet Middlebox
- Menambahkan rute yang diperlukan ke tabel rute baru seperti yang dijelaskan di bagian berikut.
- Disassociates tabel rute saat ini terkait dengan gateway internet, subnet B, dan subnet C.
- Asosiasi rute tabel A dengan gateway internet (Sumber di middlebox routing wizard), rute tabel C dengan subnet C (Middlebox di middlebox routing wizard), dan rute tabel B dengan subnet B (Tujuan di middlebox routing wizard).
- Membuat tag yang menunjukkan itu dibuat oleh wizard perutean middlebox, dan tag yang menunjukkan tanggal pembuatan.

Wisaya perutean middlebox tidak memodifikasi tabel rute yang ada. Ini menciptakan tabel rute baru, dan kemudian mengaitkannya dengan gateway dan sumber daya subnet Anda. Jika sumber daya Anda sudah secara eksplisit terkait dengan tabel rute yang ada, tabel rute yang ada terlebih dahulu dipisahkan, dan kemudian tabel rute baru dikaitkan dengan sumber daya Anda. Tabel rute Anda yang ada tidak dihapus.

Jika Anda tidak menggunakan wizard perutean middlebox, Anda harus mengkonfigurasi secara manual, dan kemudian menetapkan tabel rute ke subnet dan gateway internet.



Tabel rute gateway Internet

Tambahkan rute berikut ke tabel rute untuk gateway internet.

Tujuan	Target	Tujuan
10.0.0.0/16	Lokal:	Rute lokal untuk IPv4
10.0.1.0/24	*alat-eni*	Rute lalu lintas IPv4 yang ditujukan untuk subnet B ke middlebox
2004:1 a00: /56	Lokal:	rute lokal untuk IPv6
2004:1 a00:1234:1 a00: :/64	*alat-eni*	Rute lalu lintas IPv6 yang ditujukan untuk subnet B ke middlebox

Ada hubungan tepi antara gateway internet dan VPC.

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

- Kuncinya adalah “Asal” dan nilainya adalah “wizard Middlebox”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-02-18T 22:25:49 .137Z”)

Tabel rute subnet tujuan tujuan

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

Tujuan	Target	Tujuan
10.0.0.0/16	Lokal:	Rute lokal untuk IPv4
0.0.0.0/0	*alat-eni*	Rute lalu lintas IPv4 yang ditujukan untuk internet ke middlebox
2004:1 a00: /56	Lokal:	rute lokal untuk IPv6
::/0	*alat-eni*	Rute lalu lintas IPv6 yang ditujukan untuk internet ke middlebox

Ada asosiasi subnet dengan subnet middlebox.

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

- Kuncinya adalah “Asal” dan nilainya adalah “wizard Middlebox”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-02-18T 22:25:49 .137Z”)

Tabel rute subnet Middlebox

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

Tujuan	Target	Tujuan
10.0.0.0/16	Lokal:	Rute lokal untuk IPv4
0.0.0.0/0	*igw-id*	Rute lalu lintas IPv4 ke gateway internet
2004:1 a00: /56	Lokal:	rute lokal untuk IPv6
::/0	*eigw-id*	Perutean lalu lintas IPv6 ke gateway internet khusus keluar

Ada asosiasi subnet dengan subnet tujuan.

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

- Kuncinya adalah “Asal” dan nilainya adalah “wizard Middlebox”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-02-18T 22:25:49 .137Z”)

Memeriksa lalu lintas menggunakan peralatan di VPC keamanan

Pertimbangkan skenario di mana Anda perlu memeriksa lalu lintas memasuki VPC dari gateway internet dan ditakdirkan untuk subnet menggunakan armada peralatan keamanan yang dikonfigurasi di belakang Gateway Load Balancer. Pemilik layanan VPC konsumen menciptakan titik akhir Load Balancer Gateway di sebuah subnet di VPC mereka (diwakili oleh antarmuka jaringan titik akhir). Semua lalu lintas yang masuk ke VPC melalui gateway internet pertama-tama diarahkan ke titik akhir

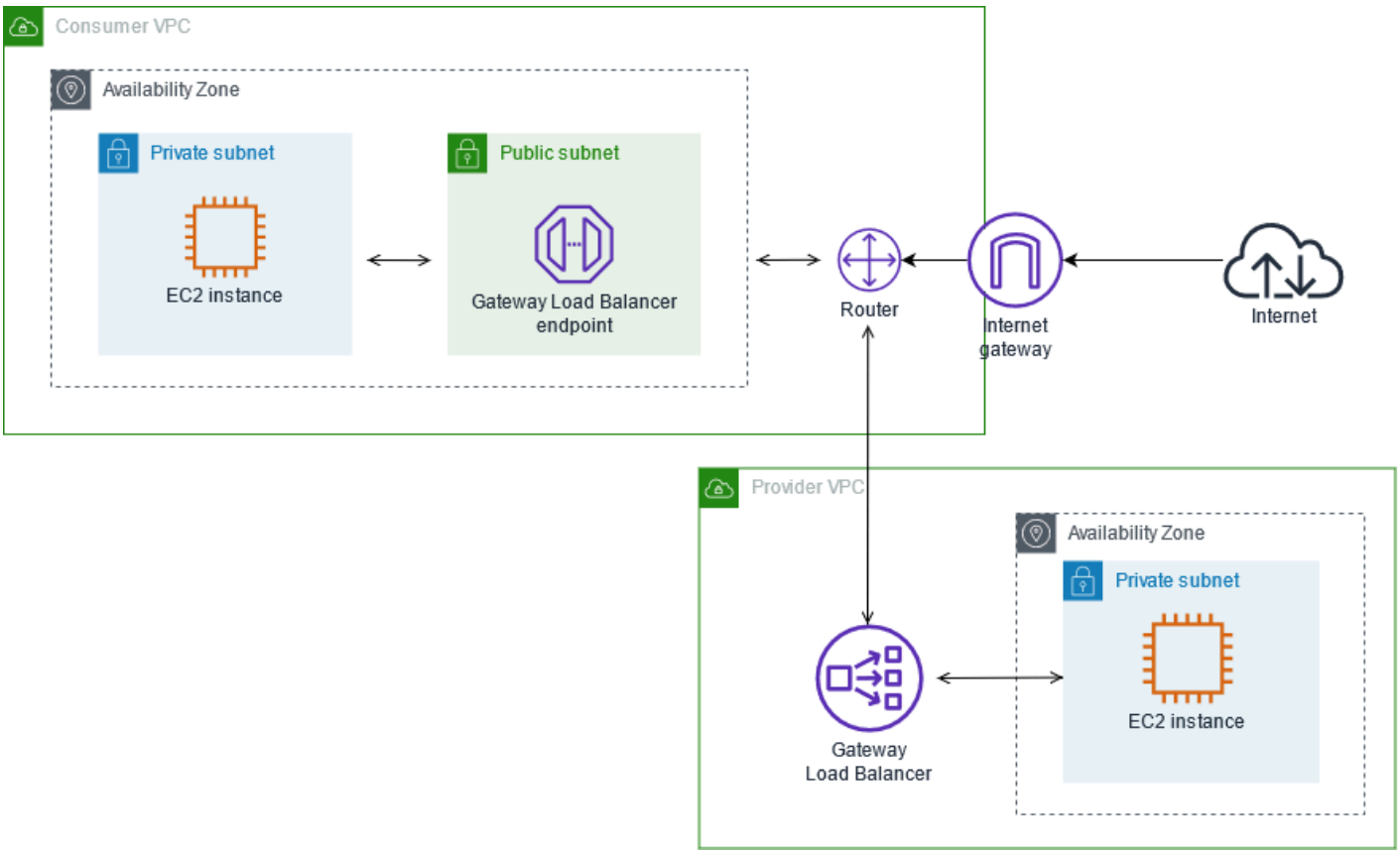
Load Balancer Gateway untuk pemeriksaan sebelum diarahkan ke titik akhir Penyeimbang Beban Gateway untuk pemeriksaan sebelum diarahkan ke titik akhir Penyeimbang Beban Gateway untuk pemeriksaan sebelum diarahkan ke titik akhir Penyeimbang Beban Gateway untuk pemeriksaan sebelum diarahkan ke titik akhir Penye Sama halnya, semua lalu lintas yang meninggalkan subnet aplikasi pertama-tama diarahkan ke titik akhir Load Balancer Gateway untuk pemeriksaan sebelum diarahkan ke titik akhir Penyeimbang Beban Gateway untuk pemeriksaan sebelum diarahkan ke titik akhir Penyeimbang Beban Gateway untuk pemeriksaan sebelum diarahkan ke titik akhir Penyeimbang Beban Gateway

Wizard perutean kotak tengah, secara otomatis melakukan operasi berikut:

- Menciptakan tabel rute.
- Menambahkan rute yang diperlukan ke tabel rute baru.
- Disassociates tabel rute saat ini terkait dengan subnet.
- Mengaitkan tabel rute yang dibuat oleh wizard perutean middlebox dengan subnet.
- Membuat tag yang menunjukkan itu dibuat oleh wizard perutean middlebox, dan tag yang menunjukkan tanggal pembuatan.

Wisaya perutean middlebox tidak memodifikasi tabel rute yang ada. Ini menciptakan tabel rute baru, dan kemudian mengaitkannya dengan gateway dan sumber daya subnet Anda. Jika sumber daya Anda sudah secara eksplisit terkait dengan tabel rute yang ada, tabel rute yang ada terlebih dahulu dipisahkan, dan kemudian tabel rute baru dikaitkan dengan sumber daya Anda. Tabel rute Anda yang ada tidak dihapus.

Jika Anda tidak menggunakan wizard perutean middlebox, Anda harus mengkonfigurasi secara manual, dan kemudian menetapkan tabel rute ke subnet dan gateway internet.



Tabel rute gateway Internet

Tabel rute untuk gateway internet memiliki rute berikut.

Tujuan	Target	Tujuan
Konsumen VPC CIDR	Lokal:	Rute lokal
Aplikasi subnet CIDR	*endpoint-id*	Lalu lintas rute untuk subnet aplikasi ke titik akhir Load Balancer Gateway.

Ada asosiasi tepi dengan gateway.

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

- Kuncinya adalah “Asal” dan nilainya adalah “wizard Middlebox”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-02-18T 22:25:49 .137Z”)

Tabel rute subnet aplikasi

Tabel rute untuk subnet aplikasi memiliki rute berikut.

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

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

- Kuncinya adalah “Asal” dan nilainya adalah “wizard Middlebox”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-02-18T 22:25:49 .137Z”)

Tabel rute penyeimbang rute subnet penyedia rute penyedia

Tabel rute untuk subnet penyedia memiliki rute berikut.

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

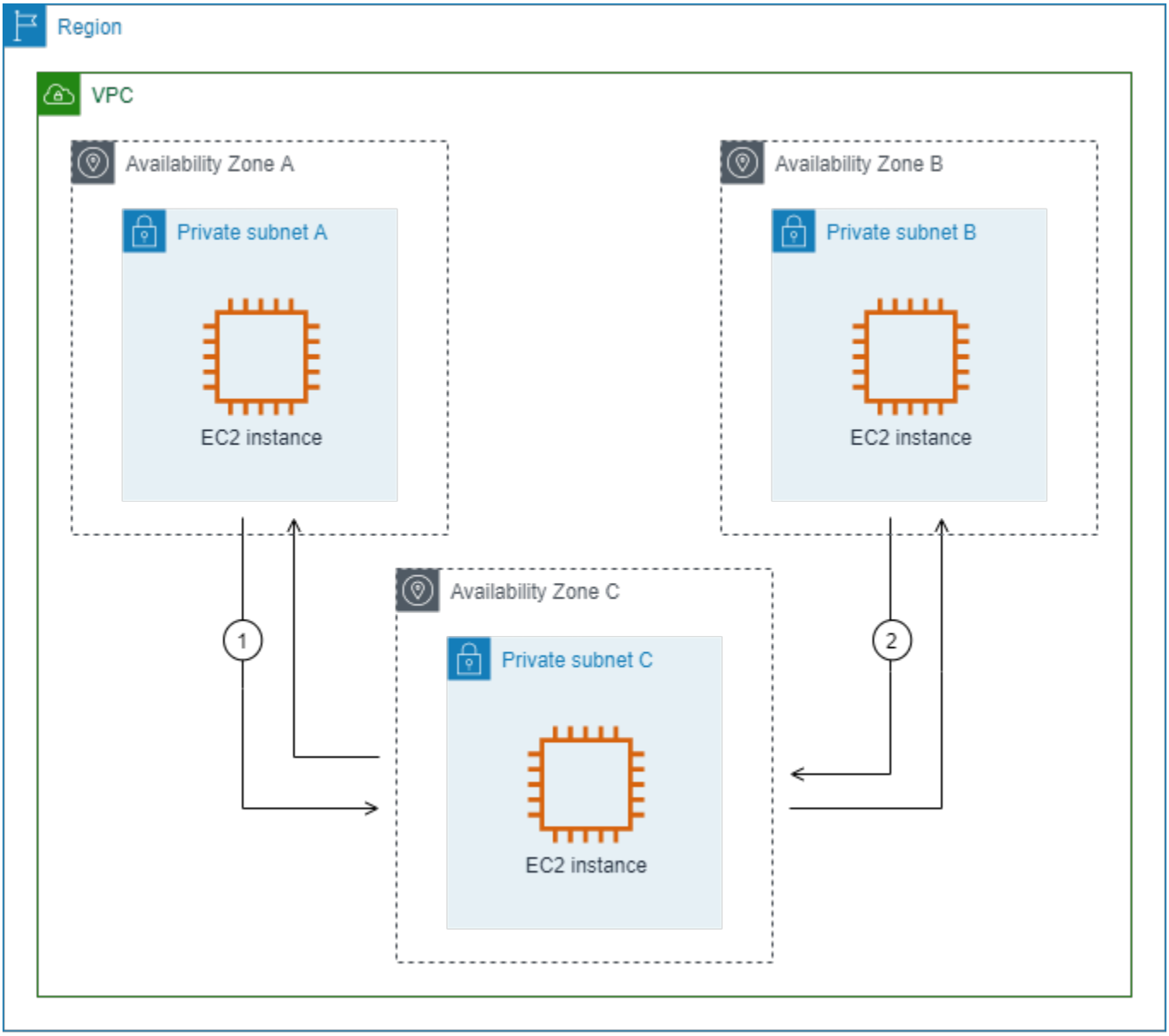
Saat Anda menggunakan wizard perutean middlebox, ia mengaitkan tag berikut dengan tabel rute:

- Kuncinya adalah “Asal” dan nilainya adalah “wizard Middlebox”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-02-18T 22:25:49 .137Z”)

Memeriksa lalu lintas antar subnet

Pertimbangkan skenario di mana Anda memiliki beberapa subnet di VPC dan Anda ingin memeriksa lalu lintas di antara mereka menggunakan alat firewall. Konfigurasikan dan instal alat firewall pada instans EC2 di subnet terpisah di VPC Anda.

Diagram berikut menunjukkan alat firewall diinstal pada contoh EC2 di subnet C. alat memeriksa semua lalu lintas yang bergerak dari subnet A ke subnet B (lihat 1) dan dari subnet B ke subnet A (lihat 2).



Anda menggunakan tabel rute utama untuk VPC dan subnet middlebox. Subnet A dan B masing-masing memiliki tabel rute khusus.

Wizard perutean kotak tengah, secara otomatis melakukan operasi berikut:

- Menciptakan tabel rute.
- Menambahkan rute yang diperlukan ke tabel rute baru.
- Disassociates tabel rute saat ini terkait dengan subnet.
- Mengaitkan tabel rute yang dibuat oleh wizard perutean middlebox dengan subnet.
- Membuat tag yang menunjukkan itu dibuat oleh wizard perutean middlebox, dan tag yang menunjukkan tanggal pembuatan.

Wisaya perutean middlebox tidak memodifikasi tabel rute yang ada. Ini menciptakan tabel rute baru, dan kemudian mengaitkannya dengan gateway dan sumber daya subnet Anda. Jika sumber daya Anda sudah secara eksplisit terkait dengan tabel rute yang ada, tabel rute yang ada terlebih dahulu dipisahkan, dan kemudian tabel rute baru dikaitkan dengan sumber daya Anda. Tabel rute Anda yang ada tidak dihapus.

Jika Anda tidak menggunakan wizard perutean middlebox, Anda harus mengkonfigurasi secara manual, dan kemudian menetapkan tabel rute ke subnet dan gateway internet.

Tabel rute kustom untuk subnet A

Tabel rute untuk subnet A memiliki rute berikut.

Tujuan	Target	Tujuan
VPC	Lokal:	Rute lokal
Subnet B CIDR	*alat-eni*	Lalu lintas rute yang ditujukan untuk subnet B ke middlebox

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

- Kuncinya adalah “Asal” dan nilainya adalah “wizard Middlebox”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-02-18T 22:25:49 .137Z”)

Tabel rute kustom untuk subnet B

Tabel rute untuk subnet B memiliki rute berikut.

Tujuan	Target	Tujuan
VPC	Lokal:	Rute lokal
Subnet Sebuah CIDR	*alat-eni*	Lalu lintas rute ditakdirkan untuk subnet A ke middlebox

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

- Kuncinya adalah “Asal” dan nilainya adalah “wizard Middlebox”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-02-18T 22:25:49 .137Z”)

Tabel rute utama

Pengaitan tabel rute utama. Tabel rute utama memiliki rute berikut.

Tujuan	Target	Tujuan
VPC	Lokal:	Rute lokal

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

- Kuncinya adalah “Asal” dan nilainya adalah “wizard Middlebox”
- Kuncinya adalah “date_created” dan nilainya adalah waktu pembuatan (misalnya, “2021-02-18T 22:25:49 .137Z”)

Hapus subnet

Jika Anda tidak lagi memerlukan subnet, Anda dapat menghapusnya. Anda tidak dapat menghapus subnet jika berisi antarmuka jaringan apa pun. Misalnya, Anda harus menghentikan instans di subnet sebelum Anda dapat menghapusnya.

Untuk menghapus subnet menggunakan konsol

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Mengakhiri semua instans di subnet. Untuk informasi selengkapnya, lihat Menghentikan instans Anda di Panduan Pengguna Amazon EC2.
3. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
4. Di panel navigasi, pilih Subnet.
5. Pilih subnet dan pilih Tindakan, Hapus subnet.
6. Ketika diminta konfirmasi, ketik**`delete`** lalu pilih Hapus.

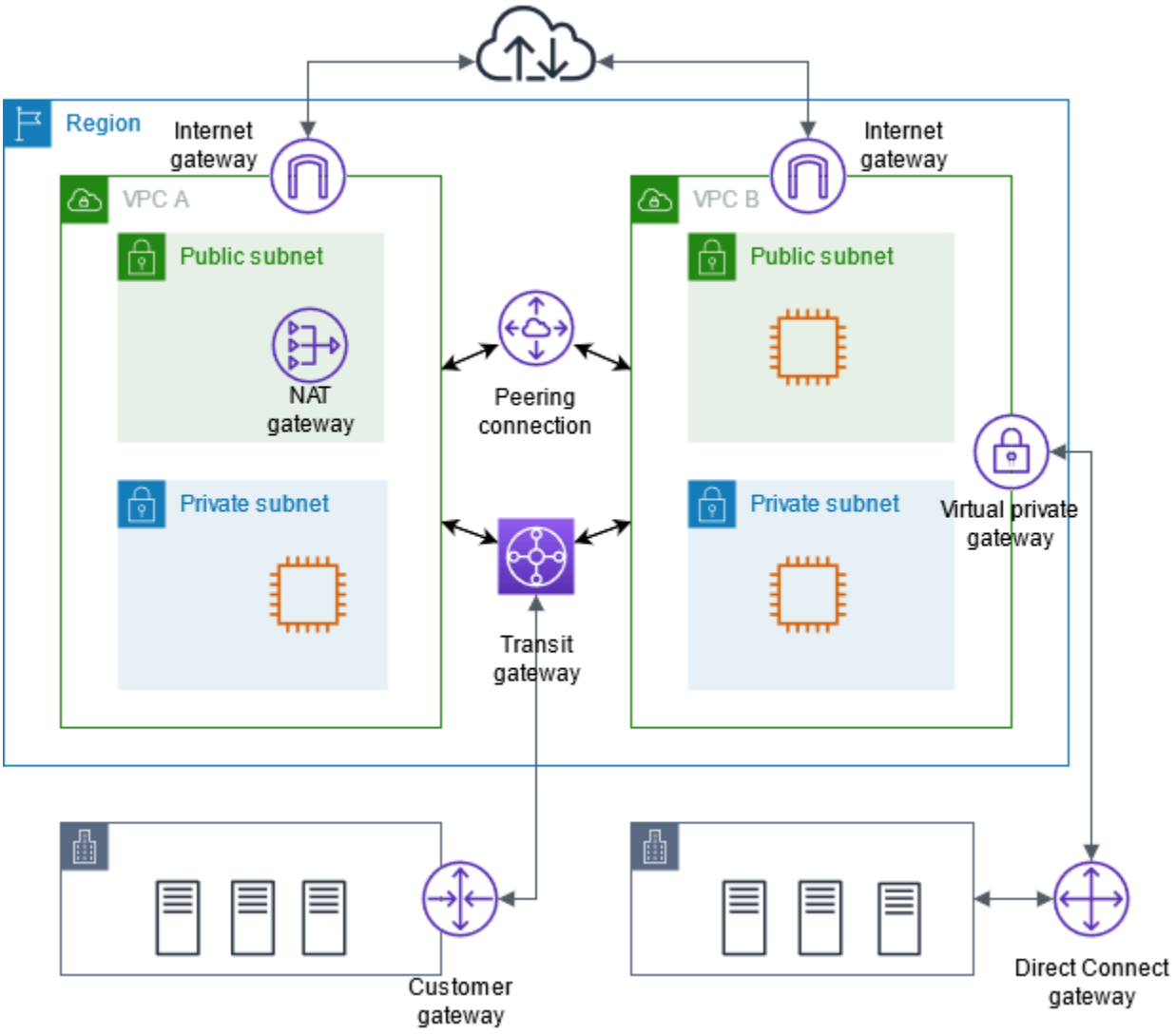
Untuk menghapus subnet menggunakanAWS CLI

Gunakan perintah delete-subnet.

Hubungkan VPC Anda ke jaringan lain

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

Diagram berikut menunjukkan beberapa opsi konektivitas ini. VPC A terhubung ke internet melalui gateway internet. Instans EC2 di subnet pribadi VPC A dapat terhubung ke internet menggunakan gateway NAT di subnet publik VPC A. VPC B terhubung ke internet melalui gateway internet. Instans EC2 di subnet publik VPC B dapat terhubung ke internet menggunakan gateway internet. VPC A dan VPC B terhubung satu sama lain melalui koneksi peering VPC dan gateway transit. Gateway transit memiliki lampiran VPN ke pusat data. VPC B memiliki AWS Direct Connect koneksi ke pusat data.



Untuk informasi selengkapnya, lihat Opsi Konektivitas Amazon Virtual Private Cloud.

Daftar Isi

Connect ke internet menggunakan gateway internet

Gateway internet diskalakan secara horizontal, berlebihan, dan merupakan komponen VPC yang sangat tersedia yang mengizinkan komunikasi antara VPC Anda dan internet. Ini mendukung lalu lintas IPv4 dan IPv6. Gateway internet tidak menimbulkan risiko ketersediaan atau kendala bandwidth pada lalu lintas jaringan Anda.

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

Gateway internet menyediakan target dalam tabel rute VPC Anda untuk lalu lintas yang dapat dirutekan internet. Untuk komunikasi menggunakan IPv4, gateway internet juga melakukan terjemahan alamat jaringan (NAT). Untuk komunikasi menggunakan IPv6, NAT tidak diperlukan karena alamat IPv6 bersifat publik. Untuk informasi selengkapnya, lihat Alamat IP dan NAT.

Konfigurasi untuk akses internet

Untuk mengaktifkan instans Anda menerima atau mengirim lalu lintas dari internet, lakukan hal berikut:

- Buat gateway internet dan lampirkan ke VPC Anda.
- Tambahkan rute ke tabel rute untuk subnet yang mengarahkan lalu lintas internet ke gateway internet.

- Pastikan bahwa instance di subnet Anda memiliki alamat IPv4 publik atau alamat IPv6. Untuk informasi selengkapnya, lihat Pengalamatan IP instans di Panduan Pengguna Amazon EC2.
- Pastikan grup keamanan dan daftar kontrol akses jaringan memungkinkan lalu lintas internet yang diinginkan mengalir ke dan dari instans Anda.

Untuk menyediakan instans Anda dengan akses internet tanpa menetapkannya alamat IP publik, gunakan perangkat NAT sebagai gantinya. Perangkat NAT mengaktifkan instans di subnet pribadi untuk terhubung ke internet, tetapi mencegah host di internet menginisiasi koneksi ke instans. Untuk informasi selengkapnya, lihat Perangkat NAT.

Subnet publik dan pribadi

Jika subnet dikaitkan dengan tabel rute yang memiliki rute ke gateway internet, hal ini dikenal sebagai subnet publik. Jika subnet dikaitkan dengan tabel rute yang tidak memiliki rute ke gateway internet, itu dikenal sebagai subnet pribadi.

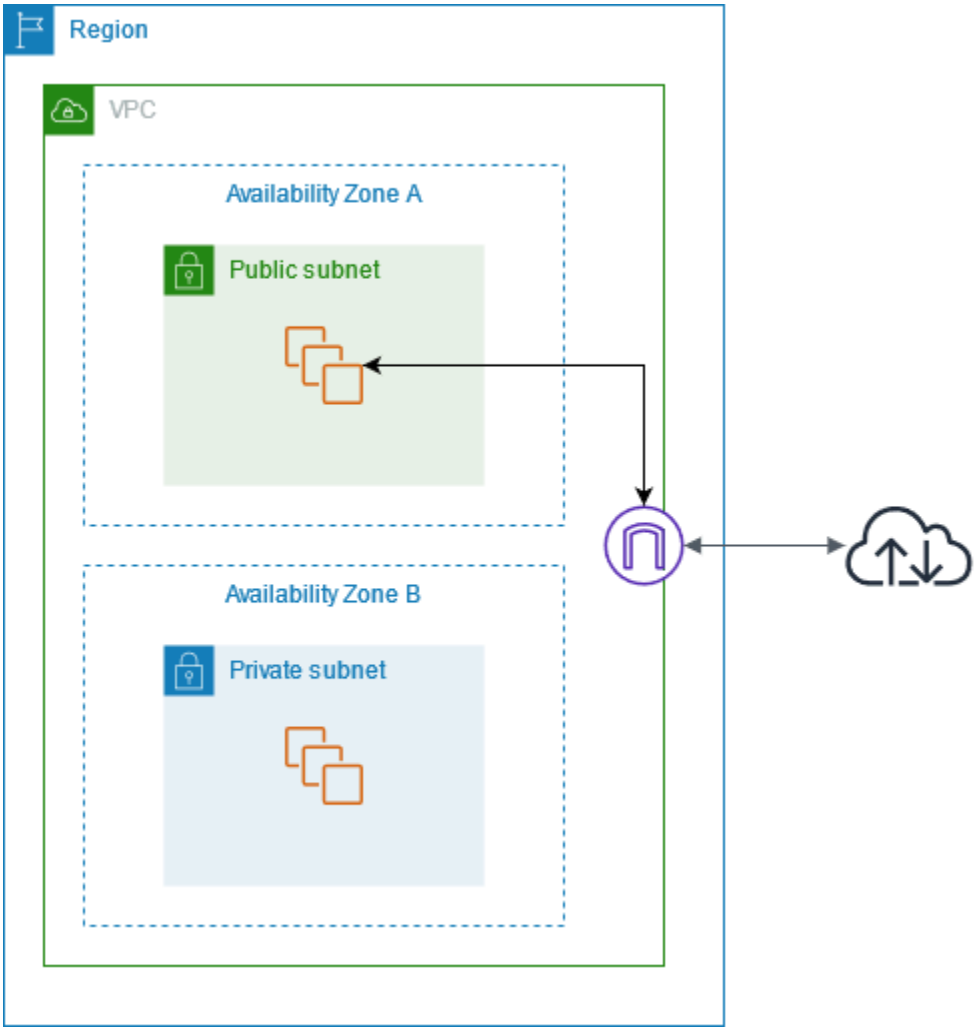
Di tabel rute subnet publik Anda, Anda dapat menentukan rute untuk gateway internet ke semua tujuan yang tidak secara eksplisit dikenal oleh tabel rute (`0.0.0.0/0` untuk IPv4 atau `::/0` untuk IPv6). Atau, Anda dapat menjangkau rute ke rentang alamat IP yang lebih sempit; misalnya, alamat IPv4 publik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

Alamat IP dan NAT

Untuk mengaktifkan komunikasi melalui internet untuk IPv4, instans Anda harus memiliki alamat IPv4 publik. Anda dapat mengonfigurasi VPC Anda untuk secara otomatis menetapkan alamat IPv4 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 alamat IPv4 publik atau alamat IP Elastis dari instans Anda yang memiliki alamat tujuannya ditranslasikan ke dalam instans alamat IPv4 pribadi sebelum lalu lintas dikirim ke VPC.

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

Dalam diagram berikut, subnet di Availability Zone A adalah subnet publik. Tabel rute untuk subnet ini memiliki rute yang mengirimkan semua lalu lintas IPv4 yang terikat internet 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, contoh di subnet pribadi tidak dapat berkomunikasi dengan internet bahkan jika mereka memiliki alamat IP publik.



Akses Internet untuk VPC default dan nondefault

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

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

Untuk informasi selengkapnya tentang VPC default, lihat VPC default. Untuk informasi selengkapnya tentang membuat VPC, lihat. Buat VPC

Bekerja dengan gateway internet

Berikut ini menjelaskan cara mendukung akses internet dari subnet di VPC Anda menggunakan gateway internet. Untuk menghapus akses internet, Anda dapat melepaskan gateway internet dari VPC Anda dan kemudian menghapusnya.

Tugas

- Membuat gateway internet baru
- Pasangkan gateway internet ke VPC
- Lepaskan gateway internet dari VPC
- Menghapus gateway internet

Membuat gateway internet baru

Gunakan prosedur berikut untuk membuat gateway internet.

Untuk membuat gateway internet

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.

Pasangkan gateway internet ke VPC

Untuk menggunakan gateway internet, Anda harus melampirkannya ke VPC.

Untuk melampirkan gateway internet ke VPC

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, Lampirkan ke VPC.
5. Pilih VPC yang tersedia.
6. Pilih Lampirkan gateway internet.

Lepaskan gateway internet dari VPC

Jika Anda tidak lagi memerlukan akses internet untuk instance yang Anda luncurkan ke VPC, Anda dapat melepaskan gateway internet dari 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

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, Lepaskan dari VPC.
5. Saat diminta konfirmasi, pilih Lepaskan gateway internet.

Menghapus gateway internet

Jika Anda tidak lagi memerlukan gateway internet, Anda dapat menghapusnya. Anda tidak dapat menghapus gateway internet jika masih terpasang ke VPC.

Untuk menghapus gateway internet

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.

gambaran umum API dan perintah

Anda dapat melakukan tugas yang dideskripsikan di halaman ini menggunakan baris perintah atau API. Untuk informasi selengkapnya tentang antarmuka baris perintah dan daftar tindakan API yang tersedia, lihat Bekerja dengan Amazon VPC.

Membuat gateway internet

- create-internet-gateway (AWS CLI)
- New-EC2InternetGateway (AWS Tools for Windows PowerShell)

Pasangkan gateway internet ke VPC

- attach-internet-gateway (AWS CLI)
- Add-EC2InternetGateway (AWS Tools for Windows PowerShell)

Deskripsikan gateway internet

- describe-internet-gateways (AWS CLI)
- Get-EC2InternetGateway (AWS Tools for Windows PowerShell)

Lepaskan gateway internet dari VPC

- detach-internet-gateway (AWS CLI)
- Dismount-EC2InternetGateway (AWS Tools for Windows PowerShell)

Menghapus gateway internet

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

Harga

Tidak ada biaya untuk gateway internet, tetapi ada biaya transfer data untuk instans EC2 yang menggunakan gateway internet. Untuk informasi selengkapnya, lihat Harga Sesuai Permintaan Amazon EC2.

Aktifkan lalu lintas IPv6 keluar menggunakan gateway internet khusus egres

Sebuah gateway internet egress-only adalah komponen VPC yang terskala secara horizontal, redundan, dan sangat tersedia yang memungkinkan komunikasi outbound melalui IPv6 pada instans di VPC Anda ke internet, dan mencegah internet memulai koneksi IPv6 dengan instans Anda.

> **Note**
>
> Gateway internet egress-only adalah untuk digunakan bersama lalu lintas IPv6 saja. Untuk mengaktifkan komunikasi internet outbound-only melalui IPv4, gunakan gateway NAT sebagai gantinya. Untuk informasi selengkapnya, lihat Gateway NAT.

Daftar Isi

Dasar-dasar gateway internet egress-only

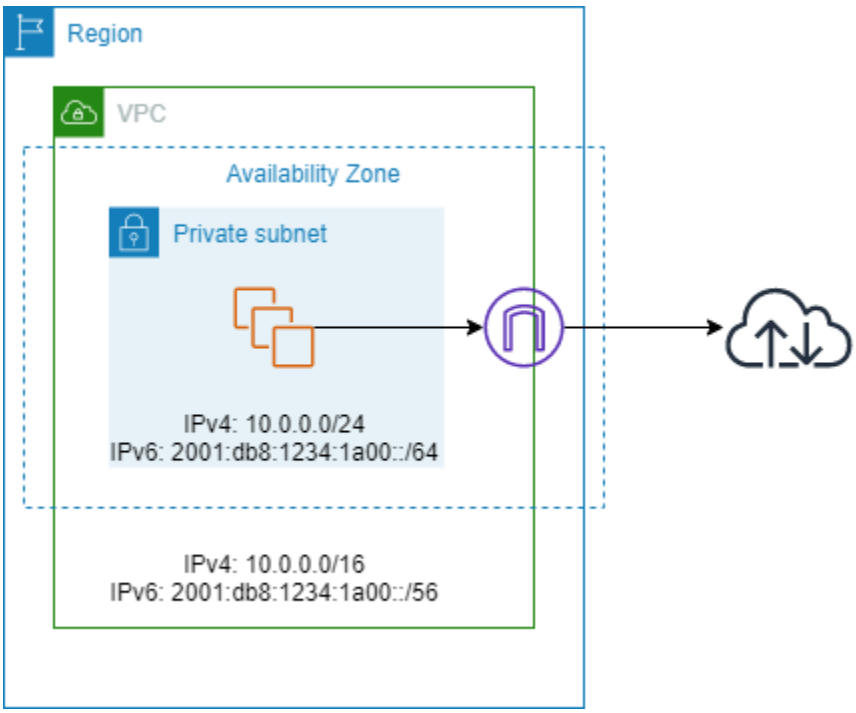
Alamat IPv6 bersifat unik secara global, dan oleh karenanya bersifat publik secara default. Jika Anda ingin instans Anda dapat mengakses internet, tetapi Anda ingin mencegah sumber daya di internet memulai komunikasi dengan instans Anda, Anda dapat menggunakan gateway internet yang egres-only. Untuk melakukannya, buat gateway internet egress-only di VPC Anda, dan kemudian tambahkan rute ke tabel rute Anda yang mengarah ke semua lalu lintas IPv6 (`::/0`) atau kisaran alamat IPv6 tertentu ke gateway internet egress-only. Lalu lintas IPv6 di subnet yang terkait dengan tabel rute diarahkan ke gateway internet egress-only.

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

Gateway internet egress-only memiliki karakteristik sebagai berikut:

- Anda tidak dapat mengaitkan grup keamanan dengan gateway internet egress-only. Anda dapat menggunakan grup keamanan untuk instans Anda di subnet pribadi untuk mengontrol lalu lintas ke dan dari instans-instans tersebut.
- Anda dapat menggunakan ACL jaringan untuk mengontrol lalu lintas ke dan dari subnet yang mana gateway internet egress-only mengarahkan lalu lintas.

Dalam diagram berikut, VPC memiliki blok IPv4 dan IPv6 CIDR, dan subnet kedua blok IPv4 dan IPv6 CIDR. VPC memiliki gateway internet khusus egress-only.



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

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

Bekerja dengan gateway internet egress-only

Tugas-tugas berikut menjelaskan cara membuat gateway internet egress-only (outbound) untuk subnet pribadi Anda, dan mengkonfigurasi perutean untuk subnet.

Tugas

- Buat gateway internet egress-only
- Lihat gateway internet egress-only Anda
- Membuat tabel rute kustom
- Hapus gateway internet egress-only

Buat gateway internet egress-only

Anda dapat membuat gateway internet egress-only untuk VPC Anda menggunakan konsol Amazon VPC.

Untuk membuat gateway internet egress-only

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Gateway Internet Egress Only.
3. Pilih Buat Gateway Internet Egress Only.
4. (Opsional) Tambahkan atau hapus tag.

   [Menambahkan tanda] Pilih Tambahkan tanda baru dan lakukan hal berikut:

   - Untuk Kunci, masukkan nama kunci.
   - Untuk Nilai, masukkan nilai kunci.

   [Hapus tag] Pilih Hapus di sebelah kanan Kunci dan Nilai tag.
5. Pilih VPC tempat untuk membuat gateway internet egress-only.
6. Pilih Buat.

Lihat gateway internet egress-only Anda

Anda dapat melihat informasi tentang gateway internet egress-only Anda di konsol Amazon VPC.

Untuk melihat informasi tentang gateway internet egress-only

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Gateway Internet Egress Only.
3. Pilih gateway internet egress-only untuk melihat informasinya di panel detail.

Membuat tabel rute kustom

Untuk mengirimkan lalu lintas yang ditujukan di luar VPC untuk gateway internet egress-only, Anda harus membuat tabel rute kustom, menambahkan rute yang mengirimkan lalu lintas ke gateway, dan kemudian mengaitkannya dengan subnet Anda.

Untuk membuat tabel rute kustom dan menambahkan rute ke gateway internet egress-only

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Tabel Rute, Buat tabel.
3. Di kotak dialog Buat tabel rute, secara opsional namai tabel rute Anda, kemudian pilih VPC Anda dan pilih Buat tabel rute.
4. Pilih tabel rute kustom yang baru saja Anda buat. Panel rincian menampilkan tab untuk bekerja dengan rute, asosiasi, dan propagasi rute.
5. Pada tab Rute, pilih Edit rute, tentukan `::/0` di kotak Tujuan, pilih ID gateway internet egress-only di daftar Target, dan kemudian pilih Simpan perubahan.
6. Pada tab Keterkaitan subnet, pilih Sunting keterkaitan subnet, lalu pilih kotak centang untuk subnet. Pilih Simpan.

Atau, Anda dapat menambahkan rute ke tabel rute yang ada yang terkait dengan subnet Anda. Pilih tabel rute yang ada, dan ikuti langkah 5 dan 6 di atas untuk menambahkan rute untuk gateway internet egress-only.

Untuk informasi selengkapnya tentang tabel rute, lihat Konfigurasikan tabel rute.

Hapus gateway internet egress-only

Jika Anda tidak lagi memerlukan gateway internet egress-only, Anda dapat menghapusnya. Setiap rute dalam tabel rute yang mengarah ke gateway internet egress-only yang terhapus tetap berstatus `blackhole` hingga Anda menghapus atau memperbarui rute secara manual.

Untuk menghapus gateway internet egress-only

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih gateway Internet Egress Only, dan pilih gateway internet egress-only.
3. Pilih Hapus.
4. Pilih Hapus Gateway Internet Egress-Only di kotak dialog konfirmasi.

Gambaran umum API dan CLI

Anda dapat melakukan tugas yang dijelaskan di halaman ini menggunakan baris perintah atau API. Untuk informasi selengkapnya tentang antarmuka baris perintah dan daftar tindakan API yang tersedia, lihat Bekerja dengan Amazon VPC.

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)

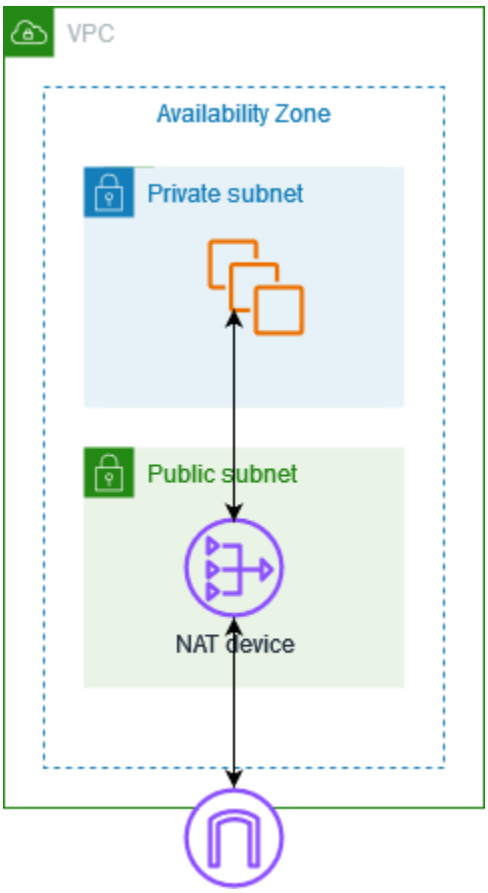
Harga

Tidak ada biaya untuk gateway internet khusus egres, tetapi ada biaya transfer data untuk instans EC2 yang menggunakan gateway internet. Untuk informasi selengkapnya, lihat Harga Sesuai Permintaan Amazon EC2.

Connect ke internet atau jaringan lain menggunakan perangkat NAT

Anda dapat menggunakan perangkat NAT untuk memungkinkan sumber daya di subnet pribadi terhubung ke internet, VPC lain, atau jaringan lokal. Instans ini dapat berkomunikasi dengan layanan di luar VPC, tetapi tidak dapat menerima permintaan koneksi yang tidak diminta.

Misalnya, diagram berikut menunjukkan perangkat NAT di subnet publik yang memungkinkan instans EC2 di subnet pribadi untuk terhubung ke internet melalui gateway internet. Perangkat NAT menggantikan alamat IPv4 sumber instans dengan alamat perangkat NAT. Saat mengirim lalu lintas respons ke instans, perangkat NAT menerjemahkan alamat kembali ke alamat IPv4 sumber asal.



Important

- Kami menggunakan istilah NAT dalam dokumentasi ini untuk mengikuti praktek IT umum, meskipun peran sebenarnya dari perangkat NAT adalah terjemahan alamat dan terjemahan alamat port (PAT).
- Anda dapat menggunakan perangkat NAT terkelola yang ditawarkan oleh AWS, yang disebut gateway NAT, atau Anda dapat membuat perangkat NAT Anda sendiri pada instans EC2, yang disebut 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.

Daftar Isi

Gateway NAT

Gateway NAT adalah layanan Network Address Translation (NAT). Anda dapat menggunakan gateway NAT sehingga instans di subnet privat dapat terhubung ke layanan di luar VPC Anda tetapi layanan eksternal tidak dapat memulai koneksi dengan instans-instans tersebut.

Ketika Anda membuat gateway NAT, Anda menentukan salah satu dari jenis konektivitas berikut:

- Publik — (Default) Instans dalam subnet privat dapat terhubung ke internet melalui gateway NAT publik, tetapi 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 VPC lain atau jaringan on-premise Anda. Dalam hal ini, Anda merutekan lalu lintas dari gateway NAT melalui transit gateway atau virtual private gateway.
- Privat — Instans dalam subnet privat dapat terhubung ke VPC lain atau jaringan on-premise Anda melalui gateway NAT privat. 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 privat. 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 pribadi dan publik memetakan alamat IPv4 pribadi sumber dari instance ke alamat IPv4 pribadi dari gateway NAT, tetapi dalam kasus gateway NAT publik, gateway internet kemudian memetakan alamat IPv4 pribadi dari Gateway NAT publik ke alamat IP Elastis yang terkait dengan NAT Gateway. 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

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 kecuali Anda menggunakan gateway internet. Gateway NAT publik hanya akan menggunakan EIP sebagai alamat IP sumber ketika digunakan bersama dengan gateway internet.

Daftar Isi

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 konfigurasikan 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 lalu lintas IPv4 atau IPv6. Untuk lalu lintas IPv6, gateway NAT melakukan NAT64. Dengan menggunakan ini bersama dengan DNS64 (tersedia di resolver Route 53), beban kerja IPv6 Anda di subnet di Amazon VPC dapat berkomunikasi dengan sumber daya IPv4. Layanan IPv4 ini 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 alamat IPv4 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 alamat IPv4 ke Gateway NAT Anda (1 alamat IPv4 utama dan 7 alamat IPv4 sekunder). 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 alamat IPv4 pribadi untuk ditetapkan ke gateway NAT atau menetapkannya secara otomatis dari rentang alamat IPv4 subnet. Alamat IPv4 pribadi yang ditetapkan tetap ada hingga Anda menghapus gateway NAT pribadi. Anda tidak dapat melepaskan alamat IPv4 pribadi dan Anda tidak dapat melampirkan alamat IPv4 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 ke subnet menggunakan ACL jaringan.
- Gateway NAT menerima antarmuka jaringan. Anda dapat memilih alamat IPv4 pribadi untuk ditetapkan ke antarmuka atau secara otomatis ditetapkan dari rentang alamat IPv4 subnet. Anda dapat melihat antarmuka jaringan untuk gateway NAT menggunakan konsol Amazon EC2. 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 melalui NAT Gateway ketika lalu lintas tiba melalui koneksi hybrid (Site to Site VPN atau Direct Connect) melalui Virtual Private Gateway. Anda dapat merutekan lalu lintas melalui NAT Gateway ketika lalu lintas tiba melalui koneksi hybrid (Site to Site VPN atau Direct Connect) melalui gateway transit.
- Gateway NAT mendukung lalu lintas dengan unit transmisi maksimum (MTU) 8500, tetapi penting untuk dicatat hal berikut:

- Untuk mencegah potensi kehilangan paket saat berkomunikasi dengan sumber daya melalui internet menggunakan gateway NAT publik, pengaturan MTU untuk instans EC2 Anda tidak boleh melebihi 1500 byte. Untuk informasi selengkapnya tentang memeriksa dan menyetel MTU pada instans, lihat Memeriksa dan mengatur MTU pada instans Linux Anda di Panduan Pengguna Amazon EC2.
- Gateway NAT mendukung Path MTU Discovery (PMTUD) melalui paket ICMPv4 FRAG_NEEDED dan paket ICMPv6 Packet Too Big (PTB).
- Gateway NAT memberlakukan penjepitan Ukuran Segmen Maksimum (MSS) untuk semua paket. Untuk informasi lebih lanjut, lihat RFC879.

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.

Bekerja dengan gateway NAT

Anda dapat menggunakan konsol Amazon VPC untuk membuat dan mengelola gateway NAT Anda.

Tugas

- Buat gateway NAT
- Edit asosiasi alamat IP sekunder
- Menandai gateway NAT
- Menghapus gateway NAT

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 EIP yang dialokasikan ke akun Anda. Untuk informasi lebih lanjut tentang kuota EIP dan cara menyesuaikannya, lihat. Alamat IP elastis

- Anda dapat menetapkan hingga 8 alamat IPv4 pribadi ke Gateway NAT pribadi Anda. Batas ini tidak dapat disesuaikan.
- Anda dibatasi untuk mengaitkan 2 alamat IP 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, lihatGateway 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 EIP, lihatAlokasikan sebuah alamat IP Elastis.

2. (Opsional) Pilih Pengaturan tambahan dan, di bawah Alamat IP pribadi - opsional, masukkan alamat IPv4 pribadi untuk gateway NAT. Jika Anda tidak memasukkan alamat, secara otomatis AWS akan menetapkan alamat IPv4 pribadi ke gateway NAT Anda secara acak dari subnet tempat gateway NAT Anda berada.
3. Lewati ke langkah 11.

8. Jika Anda memilih Private, untuk Pengaturan tambahan, metode penetapan alamat IPv4 pribadi, pilih salah satu dari berikut ini:

   - Tetapkan otomatis: AWS memilih alamat IPv4 pribadi utama untuk gateway NAT. Untuk Jumlah alamat IPv4 pribadi yang ditetapkan secara otomatis, Anda dapat secara opsional menentukan jumlah alamat IPv4 pribadi sekunder untuk gateway NAT. AWS memilih alamat IP ini secara acak dari subnet untuk gateway NAT Anda.
   - Kustom: Untuk alamat IPv4 pribadi Primer, pilih alamat IPv4 pribadi utama untuk gateway NAT. Untuk alamat IPv4 pribadi sekunder, Anda dapat secara opsional menentukan hingga 7 alamat IPv4 pribadi sekunder untuk gateway NAT.

9. Jika Anda memilih Kustom di Langkah 8, lewati langkah ini. Jika Anda memilih Tetapkan otomatis, di bawah Jumlah alamat IP pribadi yang ditetapkan secara otomatis, pilih jumlah alamat IPv4 sekunder yang ingin Anda AWS tetapkan ke gateway NAT pribadi ini. Anda dapat memilih hingga 7 alamat IPv4.

   > **Note**
   >
   > Alamat IPv4 sekunder bersifat opsional dan harus ditetapkan atau dialokasikan ketika beban kerja Anda yang menggunakan Gateway NAT melebihi 55.000 koneksi bersamaan ke satu tujuan (IP tujuan, port tujuan, dan protokol yang sama). Alamat IPv4 sekunder meningkatkan jumlah port yang tersedia, dan oleh karena itu mereka meningkatkan batas jumlah koneksi bersamaan yang dapat dibuat oleh beban kerja Anda menggunakan Gateway NAT.

10. Jika Anda memilih Tetapkan otomatis di Langkah 9, lewati langkah ini. Jika Anda memilih Custom, lakukan hal berikut:

    1. Di bawah alamat IPv4 pribadi utama, masukkan alamat IPv4 pribadi.
    2. Di bawah alamat IPv4 pribadi sekunder, masukkan hingga 7 alamat IPv4 pribadi sekunder.

11. (Opsional) Untuk menambahkan tag ke gateway NAT, pilih Tambahkan tag baru dan masukkan nama kunci dan nilai. Anda dapat menambahkan hingga 50 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 alamat IPv4 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 alamat IPv4 ke Gateway NAT Anda (1 alamat IPv4 utama dan 7 alamat IPv4 sekunder). 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 ErrorPortAlokasi dan PacketsDropHitungan CloudWatch metrik gateway NAT untuk menentukan apakah gateway NAT Anda menghasilkan kesalahan alokasi port atau menjatuhkan paket. Untuk mengatasi masalah ini, tambahkan alamat IPv4 sekunder ke gateway NAT Anda.

Pertimbangan

- Anda dapat menambahkan alamat IPv4 pribadi sekunder saat Anda 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 alamat IPv4 yang terkait dengannya (1 alamat IPv4 primer dan 7 alamat IPv4 sekunder). Anda dapat menetapkan hingga 8 alamat IPv4 pribadi ke Gateway NAT pribadi Anda. Anda dibatasi untuk mengaitkan 2 alamat IP 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 alamat IPv4 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 alamat IPv4 sekundernya ingin Anda edit.
4. Pilih Tindakan, lalu pilih Edit asosiasi alamat IP sekunder.
5. Jika Anda mengedit asosiasi alamat IPv4 sekunder dari gateway NAT pribadi, di bawah Tindakan, pilih Tetapkan alamat IPv4 baru atau Batalkan penetapan alamat IPv4 yang ada. Jika Anda mengedit asosiasi alamat IPv4 sekunder dari gateway NAT publik, di bawah Tindakan, pilih Kaitkan alamat IPv4 baru atau Putuskan alamat IPv4 yang ada.
6. Lakukan salah satu hal berikut ini:

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

- Jika Anda memilih untuk membatalkan penetapan atau memisahkan alamat IPv4 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 pengurasan 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 sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

Tag alokasi biaya didukung untuk gateway NAT. Oleh karena itu, Anda juga dapat menggunakan tag untuk mengatur AWS tagihan Anda dan mencerminkan struktur biaya Anda sendiri. Untuk informasi selengkapnya, lihat Menggunakan tanda alokasi biaya dalam Panduan Pengguna AWS Billing . Untuk informasi selengkapnya tentang menyiapkan laporan alokasi biaya dengan tag, lihat Laporan alokasi biaya bulanan di Tentang Penagihan AWS Akun.

Untuk menandai gateway NAT

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih 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 Melepas alamat IP Elastis.

Gambaran umum API dan CLI

Anda dapat melakukan tugas yang dijelaskan di halaman ini menggunakan baris perintah atau API. Untuk informasi selengkapnya tentang antarmuka baris perintah dan daftar operasi API yang tersedia, lihat Bekerja dengan Amazon VPC.

Tetapkan alamat IPv4 pribadi ke gateway NAT pribadi

- tugas-pribadi-nat-gateway-address ()AWS CLI
- Register-EC2PrivateNatGatewayAddress (AWS Tools for Windows PowerShell)
- AssignPrivateNatGatewayAlamat (API Kueri Amazon EC2)

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

- asosiasi-nat-gateway-address ()AWS CLI
- Register-EC2NatGatewayAddress (AWS Tools for Windows PowerShell)
- AssociateNatGatewayAddress (Amazon EC2 Query API)

Buat gateway NAT

- create-nat-gateway (AWS CLI)
- New-EC2NatGateway (AWS Tools for Windows PowerShell)
- CreateNatGerbang (API Kueri Amazon EC2)

Menghapus gateway NAT

- delete-nat-gateway (AWS CLI)
- Remove-EC2NatGateway (AWS Tools for Windows PowerShell)
- DeleteNatGerbang (API Kueri Amazon EC2)

Menjelaskan gateway NAT

- menjelaskan-nat-gateway (AWS CLI)
- Get-EC2NatGateway (AWS Tools for Windows PowerShell)
- DescribeNatGateway (API Kueri Amazon EC2)

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

- disassociate-nat-gateway-address ()AWS CLI
- Unregister-EC2NatGatewayAddress (AWS Tools for Windows PowerShell)
- DisassociateNatGatewayAddress (Amazon EC2 Query API)

Menandai gateway NAT

- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)
- CreateTags (Amazon EC2 Query API)

Batalkan penetapan alamat IPv4 sekunder dari gateway NAT pribadi

- unassign-private-nat-gateway-address ()AWS CLI
- Unregister-EC2PrivateNatGatewayAddress (AWS Tools for Windows PowerShell)

- UnassignPrivateNatGatewayAlamat (API Kueri Amazon EC2)

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

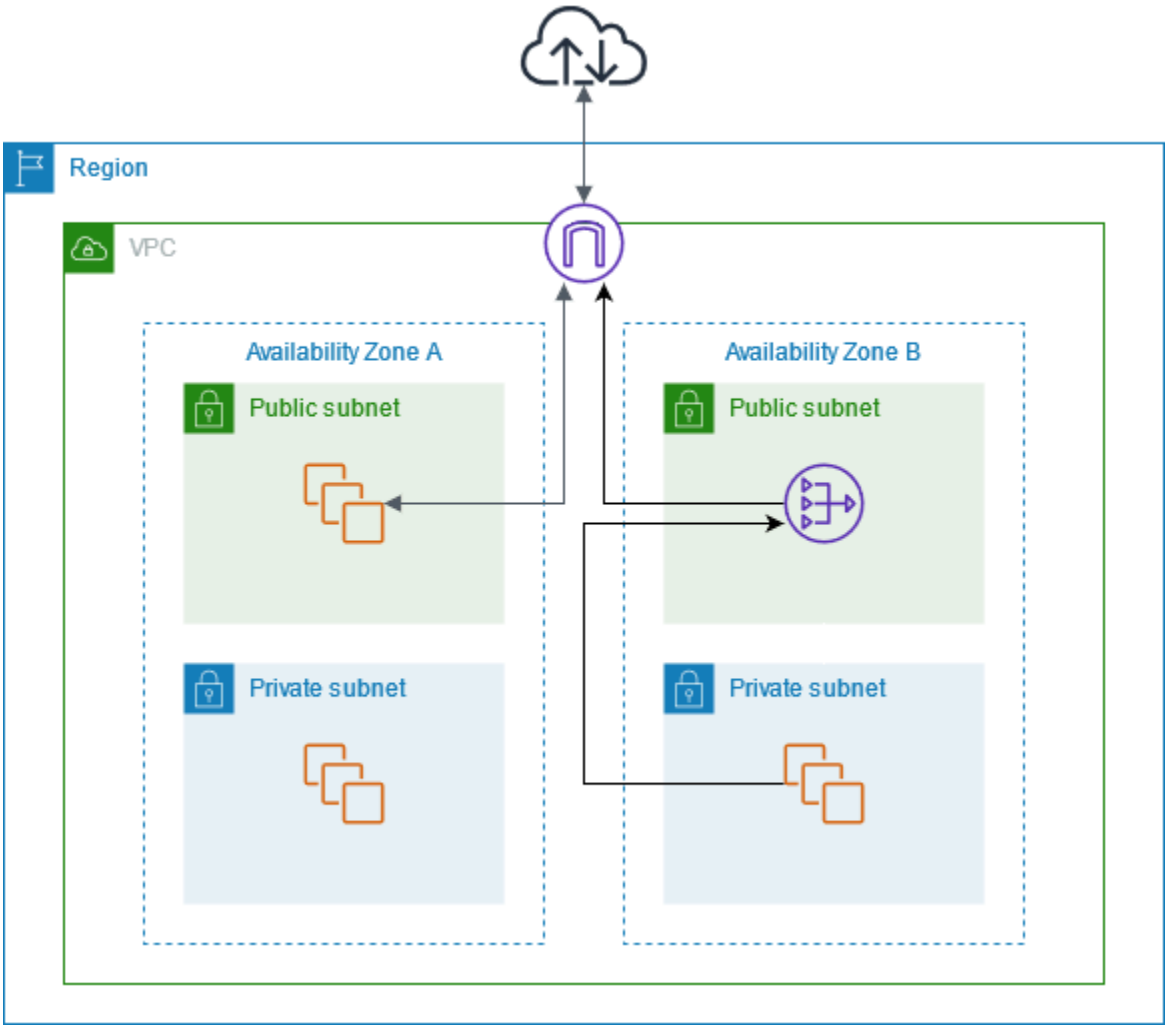
Mengakses internet dari subnet privat

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

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 alamat IPv4 pribadi sumber dari instance ke alamat IPv4 pribadi dari gateway NAT pribadi, tetapi dalam kasus gateway NAT publik, gateway internet kemudian memetakan alamat IPv4 pribadi dari Gateway NAT publik ke alamat IP Elastis yang terkait dengan NAT Gateway. Saat mengirim lalu lintas respons ke instance, apakah itu gateway NAT publik atau pribadi, gateway NAT menerjemahkan alamat kembali ke alamat IP sumber asli.



Perhatikan bahwa jika instance di subnet pribadi di Availability Zone A juga perlu menjangkau internet, Anda dapat membuat rute dari subnet ini ke gateway NAT di Availability Zone B. Atau, Anda dapat meningkatkan ketahanan dengan membuat gateway NAT di setiap Availability Zone yang berisi sumber daya yang memerlukan akses internet. Untuk contoh diagram, lihatthe section called “Server pribadi”.

Perutean

Berikut ini adalah tabel rute yang terkait dengan subnet publik di Availability Zone A. Entri pertama adalah rute lokal; ini memungkinkan 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
VPC CIDR	lokal
0.0.0.0/0	*internet-gateway-id*

Berikut ini adalah tabel rute yang terkait dengan subnet pribadi di Availability Zone A. Entri adalah rute lokal, yang memungkinkan 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
VPC CIDR	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
VPC CIDR	lokal
0.0.0.0/0	*internet-gateway-id*

Berikut ini adalah tabel rute yang terkait dengan subnet pribadi di Availability Zone B. Entri pertama adalah rute lokal; ini memungkinkan instance di subnet untuk berkomunikasi dengan instance lain di VPC menggunakan alamat IP pribadi. Entri kedua mengirimkan semua lalu lintas subnet lainnya ke gateway NAT.

Tujuan	Target
VPC CIDR	lokal
0.0.0.0/0	*nat-gateway-id*

Untuk informasi selengkapnya, lihat the section called “Cara menggunakan tabel rute”.

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 lauch 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 Pengguna Amazon EC2.
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 Menghubungkan ke instans Linux Anda. 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 Mengakhiri instans Anda di Panduan Pengguna Amazon EC2.

Akses jaringan Anda menggunakan alamat IP yang diizinkan

Anda dapat menggunakan gateway NAT pribadi untuk mengaktifkan komunikasi dari VPC Anda ke jaringan lokal menggunakan kumpulan alamat yang diizinkan. Alih-alih menetapkan setiap instans alamat IP terpisah dari rentang alamat IP yang terdaftar 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 diizinkan.

Daftar Isi

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.

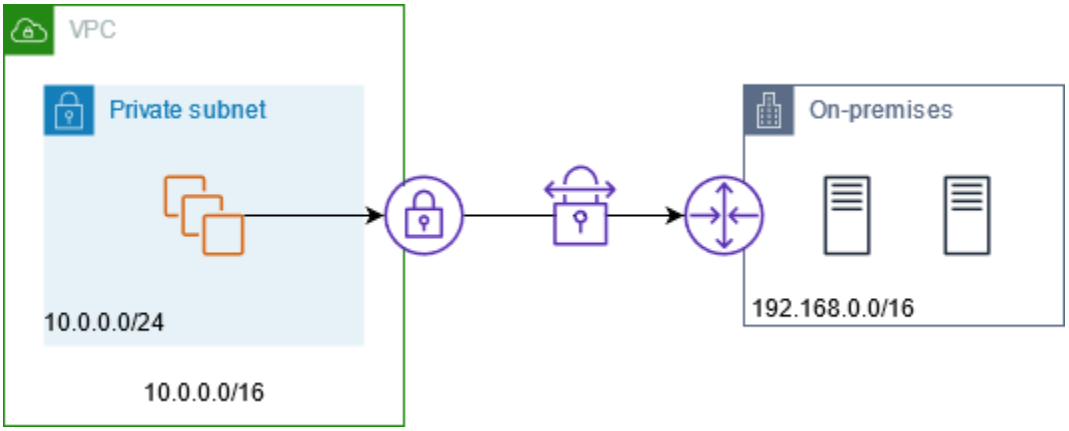
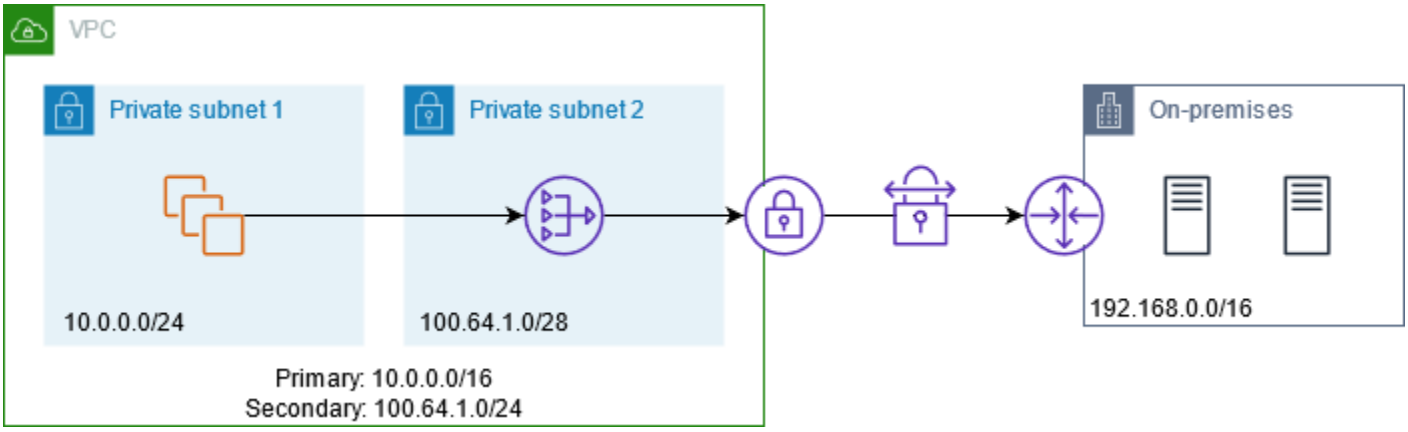


Diagram berikut menunjukkan komponen kunci konfigurasi untuk skenario ini. VPC memiliki rentang alamat IP asli ditambah rentang alamat IP yang diizinkan. VPC memiliki subnet dari rentang alamat IP yang diizinkan dengan gateway NAT pribadi. Lalu lintas dari instans yang ditujukan untuk jaringan lokal 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.

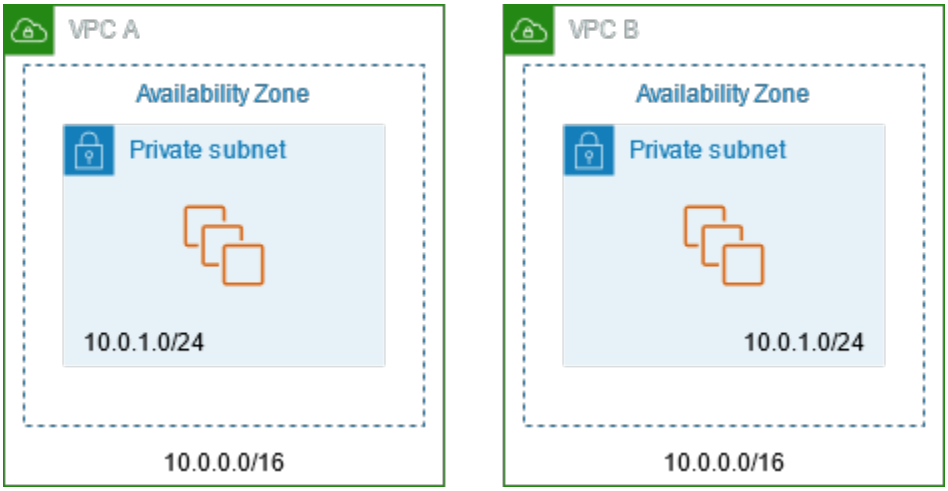
Tujuan	Target
10.0.0.0/16	lokal
100.64.1.0/24	lokal
192.168.0.0/16	*nat-gateway-id*

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

Aktifkan komunikasi antara jaringan yang tumpang tindih

Anda dapat menggunakan gateway NAT pribadi untuk mengaktifkan komunikasi antar jaringan 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.



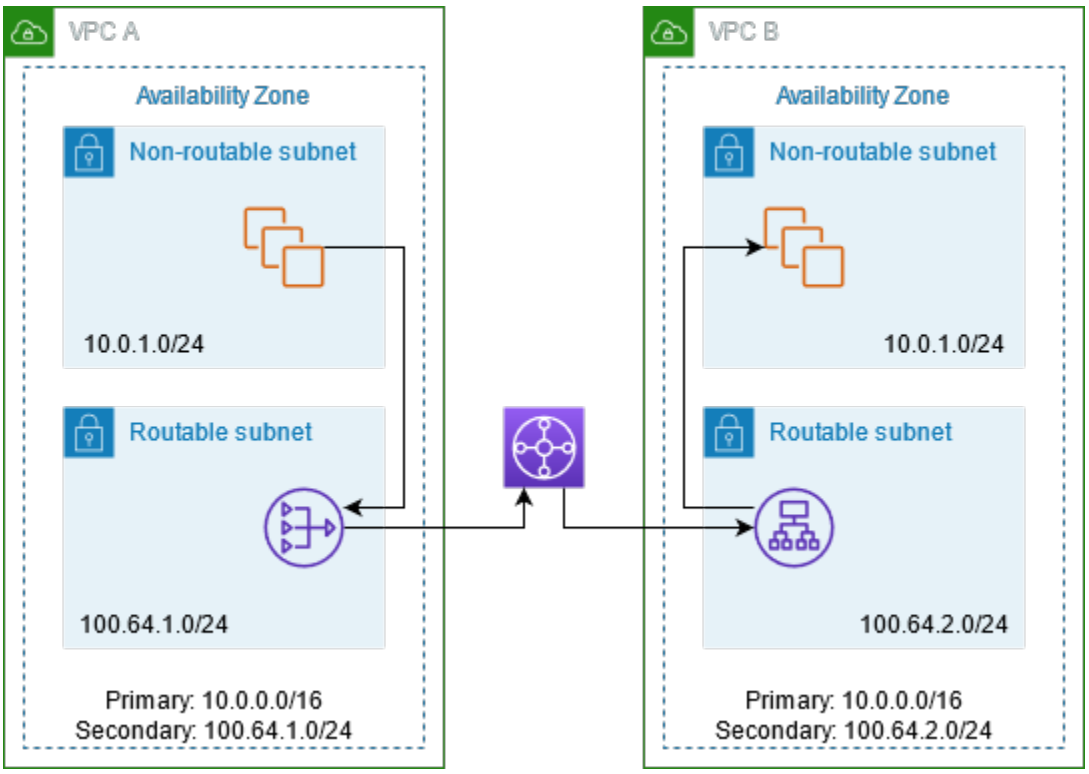
Daftar Isi

Gambaran Umum

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 dapat (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 VPC masing-masing.
- Buat subnet di VPC A dari rentang alamat IP yang dapat dirutekan, dan buat gateway NAT pribadi di subnet baru ini.
- Buat subnet di VPC B dari rentang alamat IP 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 VPC. Pastikan untuk menonaktifkan propagasi rute. Saat Anda melampirkan setiap VPC ke gateway transit, gunakan rentang alamat yang dapat dirutekan dari VPC.
- Perbarui tabel rute subnet 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
10.0.0.0/16	lokal
100.64.1.0/24	lokal
100.64.2.0/24	*nat-gateway-id*

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

Tujuan	Target
10.0.0.0/16	lokal
100.64.1.0/24	lokal
100.64.2.0/24	*transit-gateway-id*

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

Tujuan	Target
10.0.0.0/16	lokal
100.64.2.0/24	lokal

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

Tujuan	Target
10.0.0.0/16	lokal
100.64.2.0/24	lokal

Tujuan	Target
100.64.1.0/24	*transit-gateway-id*

Berikut ini adalah tabel rute transit gateway.

CIDR	Lampiran	Jenis rute
100.64.1.0/24	*Lampiran untuk VPC A*	Statis
100.64.2.0/24	*Lampiran untuk VPC B*	Statis

DNS64 dan NAT64

Gateway NAT mendukung terjemahan alamat jaringan dari IPv6 ke IPv4, yang dikenal sebagai NAT64. NAT64 membantu sumber daya IPv6 Anda berkomunikasi dengan AWS sumber daya IPv4 di VPC yang sama atau VPC yang berbeda, di jaringan lokal Anda atau melalui internet. Anda dapat menggunakan NAT64 dengan DNS64 di Amazon Route 53 Resolver atau menggunakan server DNS64 Anda sendiri.

Daftar Isi

Apa itu DNS64?

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

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

Anda dapat mengaktifkan atau menonaktifkan DNS64 pada subnet menggunakan atribut modify-subnet-menggunakan AWS CLI atau dengan konsol VPC dengan memilih subnet dan memilih Actions > Edit pengaturan subnet.

Apa itu NAT64?

NAT64 memungkinkan layanan khusus IPv6 Anda di VPC Amazon untuk berkomunikasi dengan layanan khusus IPv4 dalam VPC yang sama (dalam subnet yang berbeda) atau VPC yang terhubung, 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 dual-stack agar NAT64 berfungsi.

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

- Dari `64:ff9b::/96` awalan, gateway NAT mengakui bahwa tujuan aslinya adalah IPv4 dan menerjemahkan paket IPv6 ke IPv4 dengan mengganti:
  - 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 paket IPv4 yang diterjemahkan ke tujuan melalui gateway internet, gateway pribadi virtual, atau gateway transit dan memulai koneksi.
- Host khusus IPv4 mengirimkan kembali paket respons IPv4. Setelah koneksi dibuat, gateway NAT menerima paket respons IPv4 dari host eksternal.

- Paket IPv4 respon ditujukan untuk gateway NAT, yang menerima paket dan de-NAT mereka dengan mengganti IP (IP tujuan) dengan alamat IPv6 host dan prepending kembali ke alamat IPv4 sumber. `64:ff9b::/96` Paket kemudian mengalir ke host mengikuti rute lokal.

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

Konfigurasikan DNS64 dan NAT64

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

Daftar Isi

Aktifkan komunikasi dengan layanan khusus IPv4 di internet dengan CLI AWS

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

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

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

Perhatikan bahwa menunjuk `::/0` ke gateway internet akan memungkinkan host IPv6 eksternal (di luar VPC) untuk memulai koneksi melalui IPv6.

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-cidr-block
0.0.0.0/0 --nat-gateway-id nat-05dba92075d71c408
```

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-ipv6-cidr-block
64:ff9b::/96 --nat-gateway-id nat-05dba92075d71c408
```

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-ipv6-cidr-block
::/0 --egress-only-internet-gateway-id eigw-c0a643a9
```

2. Aktifkan kemampuan DNS64 di subnet yang berisi beban kerja khusus IPv6.

```
aws ec2 modify-subnet-attribute --subnet-id subnet-1a2b3c4d --enable-dns64
```

Sekarang, sumber daya di subnet pribadi Anda dapat membangun koneksi stateful dengan layanan IPv4 dan IPv6 di internet. Konfigurasikan grup keamanan dan NACL Anda dengan tepat untuk memungkinkan lalu lintas keluar dan masuk ke lalu lintas. `64:ff9b::/96`

Aktifkan komunikasi dengan layanan khusus IPv4 di lingkungan lokal Anda

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 menetapkannya alamat IPv4 yang 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 alamat IPv4 dari resolver lokal.
- Setelah menyiapkan titik akhir keluar Route 53 Resolver, Anda perlu mengaktifkan DNS64 di subnet yang berisi beban kerja khusus IPv6 dan merutekan data apa pun yang ditujukan untuk jaringan lokal Anda melalui gateway NAT.

Cara kerja DNS64 untuk tujuan khusus IPv4 di jaringan lokal:

1. Anda menetapkan alamat IPv4 ke titik akhir keluar Route 53 Resolver di VPC Anda.
2. Kueri DNS dari layanan IPv6 Anda masuk ke Route 53 Resolver melalui IPv6. Route 53 Resolver mencocokkan kueri dengan aturan penerusan dan mendapatkan alamat IPv4 untuk resolver lokal Anda.
3. Route 53 Resolver mengubah paket kueri dari IPv6 menjadi IPv4 dan meneruskannya ke titik akhir keluar. Setiap alamat IP titik akhir mewakili satu ENI yang meneruskan permintaan ke alamat IPv4 lokal dari penyelesai DNS Anda.
4. Penyelesai lokal mengirimkan paket respons melalui IPv4 kembali melalui titik akhir keluar ke Route 53 Resolver.
5. Dengan asumsi kueri dibuat dari subnet berkemampuan DNS64, Route 53 Resolver melakukan dua hal:

    a. Memeriksa isi paket respons. Jika ada alamat IPv6 dalam catatan, itu menyimpan konten apa adanya, tetapi jika hanya berisi catatan IPv4. Ini mensintesis catatan IPv6 juga dengan prepending `64:ff9b::/96` ke alamat IPv4.

    b. Mengepak ulang konten dan mengirimkannya ke layanan di VPC Anda melalui IPv6.

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. Data metrik gateway NAT disediakan pada interval 1 menit, dan statistik dicatat untuk jangka waktu 15 bulan.

Untuk informasi selengkapnya tentang Amazon CloudWatch, lihat Panduan CloudWatch Pengguna Amazon. Untuk informasi selengkapnya tentang harga, lihat CloudWatch Harga Amazon.

Metrik dan dimensi gateway NAT

Metrik berikut tersedia untuk gateway NAT Anda. Kolom deskripsi mencakup deskripsi setiap metrik serta unit dan statistik.

Metrik	Deskripsi
`ActiveConnectionCount`	Jumlah total koneksi TCP aktif bersamaan melalui gateway NAT. Nilai nol menunjukkan bahwa tidak ada koneksi aktif melalui gateway NAT. Unit: Hitungan Statistik: Statistik yang paling berguna adalah`Max`.
`BytesInFromDestination`	Jumlah byte yang diterima oleh gateway NAT dari tujuan. 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: Byte 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: Byte Statistik: Statistik yang paling berguna adalah`Sum`.

Metrik	Deskripsi
`BytesOutToDestination`	Jumlah byte yang dikirim melalui gateway NAT ke tujuan. Nilai yang lebih besar dari nol menunjukkan bahwa ada lalu lintas pergi ke internet dari klien yang berada di belakang gateway NAT. Jika nilai untuk `BytesOutToDestination` kurang dari nilai untuk`BytesInFromSource`, mungkin ada kehilangan data selama pemrosesan gateway NAT. Unit: Bita Statistik: Statistik yang paling berguna adalah`Sum`.
`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: Byte Statistik: Statistik yang paling berguna adalah`Sum`.

Metrik	Deskripsi
`ConnectionAttemptCount`	Jumlah upaya koneksi yang dilakukan melalui gateway NAT. 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`.
`ConnectionEstablishedCount`	Jumlah koneksi yang dibuat melalui gateway NAT. 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
`ErrorPortAllocation`	Berapa kali gateway NAT tidak dapat mengalokasikan port sumber. Nilai yang lebih besar dari nol menunjukkan bahwa terlalu banyak koneksi bersamaan terbuka melalui gateway NAT. Unit: Hitungan Statistik: Statistik yang paling berguna adalah`Sum`.
`IdleTimeoutCount`	Jumlah koneksi yang beralih dari status aktif ke status siaga. Transisi koneksi aktif ke siaga jika itu tidak ditutup dengan baik dan tidak ada aktivitas selama 350 detik terakhir. Nilai yang lebih besar dari nol menunjukkan bahwa ada koneksi yang telah dipindahkan ke status siaga. Jika nilai untuk `IdleTimeoutCount` meningkat, 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: PacketsDropCount/(PacketsInFromSource+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: Hitungan Statistik: Statistik yang paling berguna adalahSum.
PacketsInFromDestination	Jumlah paket yang diterima oleh gateway NAT dari tujuan. Jika nilai untuk PacketsOutToSource kurang dari nilai untukPacketsInFromDestination , mungkin ada kehilangan data selama pemrosesan gateway NAT, atau lalu lintas diblokir secara aktif oleh gateway NAT. Unit: Jumlah Statistik: Statistik yang paling berguna adalahSum.

Metrik	Deskripsi
PacketsInFromSource	Jumlah paket yang diterima oleh gateway NAT dari klien di VPC Anda. Jika nilai untuk PacketsOutToDestination kurang dari nilai untukPacketsInFromSource , mungkin ada kehilangan data selama pemrosesan gateway NAT. Unit: Jumlah Statistik: Statistik yang paling berguna adalahSum.
PacketsOutToDestination	Jumlah paket yang dikirim melalui gateway NAT ke tujuan. Nilai yang lebih besar dari nol menunjukkan bahwa ada lalu lintas pergi ke internet dari klien yang berada di belakang gateway NAT. Jika nilai untuk PacketsOutToDestination kurang dari nilai untukPacketsInFromSource , mungkin ada kehilangan data selama pemrosesan gateway NAT. Unit: Jumlah Statistik: Statistik yang paling berguna adalahSum.

Metrik	Deskripsi
PacketsOutToSource	Jumlah paket yang dikirim melalui gateway NAT untuk klien di VPC Anda. Nilai yang lebih besar dari nol menunjukkan bahwa ada lalu lintas yang datang dari internet ke klien yang berada di belakang gateway NAT. Jika nilai untuk PacketsOutToSource kurang dari nilai untukPacketsInFromDestination , mungkin ada kehilangan data selama pemrosesan gateway NAT, atau lalu lintas diblokir secara aktif oleh gateway NAT. Unit: Jumlah Statistik: Statistik yang paling berguna adalahSum.
PeakBytesPerSecond	Metrik ini melaporkan rata-rata 10 detik byte per detik tertinggi dalam satu menit tertentu. Unit: Hitungan Statistik: Statistik yang paling berguna adalahMaximum.
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: Hitungan Statistik: Statistik yang paling berguna adalahMaximum.

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 metrik NatGateway.
4. Pilih dimensi metrik.

Untuk melihat metrik menggunakan AWS CLI

Pada prompt perintah, gunakan perintah berikut untuk mencantumkan metrik yang tersedia untuk layanan gateway NAT.

```
aws cloudwatch list-metrics --namespace "AWS/NATGateway"
```

Buat CloudWatch alarm untuk memantau gateway NAT

Anda dapat membuat CloudWatch alarm yang mengirimkan pesan Amazon SNS saat alarm berubah status. Alarm mengawasi satu metrik selama suatu periode waktu yang Anda tentukan. Alarm mengirimkan pemberitahuan ke topik Amazon SNS berdasarkan nilai metrik relatif terhadap ambang batas tertentu selama beberapa periode waktu.

Misalnya, Anda dapat membuat alarm yang memantau jumlah lalu lintas yang masuk atau meninggalkan gateway NAT. Alarm berikut memonitor jumlah lalu lintas keluar dari klien di VPC Anda melalui gateway NAT ke internet. Ini mengirimkan pemberitahuan ketika jumlah byte mencapai ambang batas 5.000.000 selama periode 15 menit.

Untuk membuat alarm untuk lalu lintas keluar melalui gateway NAT

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pada panel navigasi, pilih Alarm, Semua alarm.
3. Pilih Buat alarm.
4. Pilih Pilih Metrik.
5. Pilih namespace metrik NatGateway dan kemudian pilih dimensi metrik. Saat Anda masuk ke metrik, pilih kotak centang di sebelah BytesOutToDestinationmetrik untuk gateway NAT, lalu pilih Pilih metrik.
6. Konfigurasikan 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 metrik NatGateway dan kemudian pilih dimensi metrik. Saat Anda masuk ke metrik, pilih kotak centang di sebelah ErrorPortAllocationmetrik untuk gateway NAT, lalu pilih Pilih metrik.
6. Konfigurasikan 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
- Koneksi IPsec 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 IP yang tersedia 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-xxxxxxxx tidak memiliki gateway internet terpasang	Gateway NAT harus dibuat dalam VPC dengan gateway internet.	Buat dan lampirkan gateway internet ke VPC Anda. Untuk informasi selengkapnya, lihat Bekerja dengan gateway internet.
Alamat IP Elastis eipalloc-xxxxxxxx siap diasosiasikan	Alamat IP Elastis yang Anda tentukan sudah dikaitkan dengan sumber daya lain, dan tidak dapat dikaitkan dengan gateway NAT.	Periksa sumber daya mana yang terkait dengan alamat IP Elastis. Pergi ke halaman IP elastis di konsol Amazon VPC, dan tampilkan nilai-nilai yang ditentukan untuk ID instans 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 Bekerja dengan 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 penambahan kuota IP 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 keamanan atau ACL jaringan 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 Amazon VPC, buka halaman gateway NAT dan tampilkan 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 bahwa ACL jaringan yang terkait dengan subnet privat 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.

Koneksi IPsec tidak dapat dibuat

Masalah

Anda tidak dapat membuat koneksi IPsec ke tujuan.

Penyebab

Gateway NAT saat ini tidak support protokol IPsec.

Solusi

Anda dapat menggunakan NAT-Traversal (NAT-T) untuk merangkum lalu lintas IPsec di UDP, yang merupakan protokol yang di-support untuk gateway NAT. Pastikan bahwa Anda menguji konfigurasi NAT-T dan IPsec untuk memverifikasi bahwa lalu lintas IPsec Anda tidak terputus.

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 dari berikut:

- Buat gateway NAT per Availability Zone dan sebarkan klien Anda di seluruh zona tersebut.
- Buat gateway NAT tambahan di subnet publik dan pisahkan klien Anda menjadi beberapa subnet privat, masing-masing dengan rute ke gateway NAT yang berbeda.
- Batasi jumlah koneksi ke tujuan yang dapat dibuat klien Anda.
- Gunakan `IdleTimeoutCount`metrik CloudWatch untuk memantau peningkatan koneksi idle. Tutup koneksi siaga untuk melepaskan kapasitas.
- Buat Gateway NAT dengan beberapa alamat IP atau tambahkan alamat IP sekunder ke Gateway NAT yang ada. Setiap alamat IPv4 baru dapat mendukung hingga 55.000 koneksi bersamaan. Untuk informasi lebih lanjut, lihat Buat gateway NAT atau Edit asosiasi alamat IP sekunder.

Harga

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 lalu lintas IPv4 keluar ke internet, tetapi mereka tidak dapat menerima lalu lintas masuk yang dimulai di internet.

Important

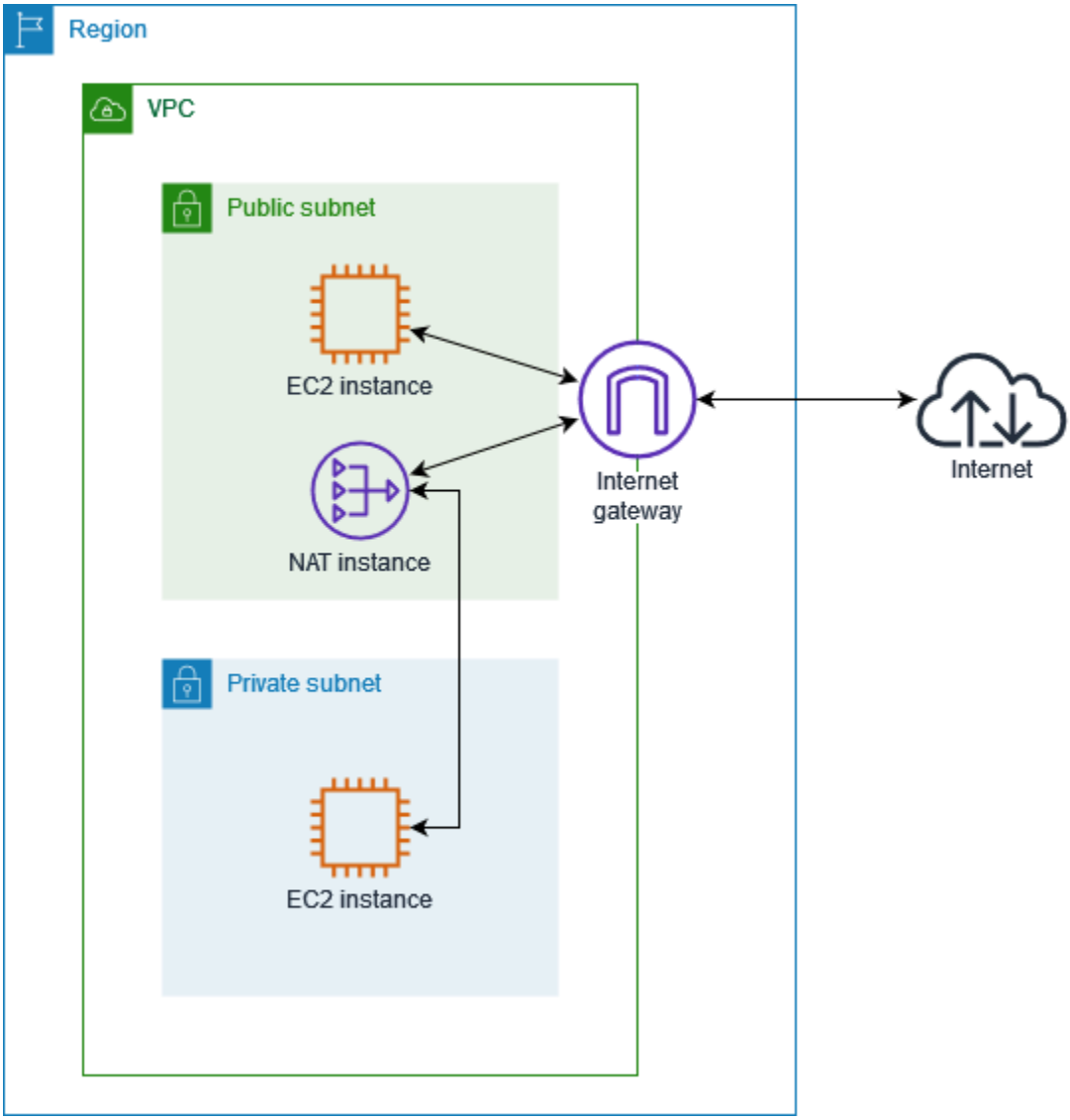
NAT AMI dibangun di atas versi terakhir Amazon Linux AMI, 2018.03, yang mencapai akhir dukungan standar pada 31 Desember 2020 dan akhir dukungan pemeliharaan pada 31 Desember 2023. Untuk informasi selengkapnya, lihat postingan blog berikut: Akhir masa pakai AMI Amazon Linux.
Jika Anda menggunakan NAT 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 “Buat NAT AMI”

Daftar Isi

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 instans 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 layanan Amazon EC2 di. Referensi Umum AWS

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.

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.

Jalur masuk

Sumber	Protokol	Rentang Port	Komentar
CIDR subnet pribadi	TCP	80	Izinkan lalu lintas HTTP masuk dari server di subnet privat
CIDR subnet pribadi	TCP	443	Izinkan lalu lintas HTTPS masuk dari server di subnet privat
Rentang alamat IP publik jaringan Anda	TCP	22	Izinkan akses SSH masuk ke instans NAT dari jaringan Anda (melalui gateway internet)

Jalur keluar

Tujuan	Protokol	Rentang Port	Komentar
0.0.0.0/0	TCP	80	Izinkan akses HTTP keluar ke internet
0.0.0.0/0	TCP	443	Izinkan akses HTTPS keluar ke internet

Untuk membuat grup keamanan

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Grup keamanan.
3. Pilih Buat grup keamanan.
4. Masukkan nama dan deskripsi untuk grup keamanan tersebut.
5. Untuk VPC, pilih ID VPC untuk 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.

Buat NAT AMI

NAT AMI dikonfigurasi untuk menjalankan NAT pada instans EC2. 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 mereka tetap ada bahkan setelah instance reboot.

Untuk membuat NAT AMI untuk Amazon Linux

1. Luncurkan instans EC2 yang menjalankan AL2023 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 atauvim, buat file konfigurasi berikut: `/etc/sysctl.d/custom-ip-forwarding.conf`

   b. Tambahkan baris berikut ke file konfigurasi.

      ```
      net.ipv4.ip_forward=1
      ```

   c. Simpan file konfigurasi dan keluar dari editor teks.

   d. Jalankan perintah berikut untuk menerapkan file konfigurasi.

      ```
      sudo sysctl -p /etc/sysctl.d/custom-ip-forwarding.conf
      ```

4. Jalankan perintah berikut pada instance, dan 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 instans EC2. Untuk informasi selengkapnya, lihat Membuat AMI Linux dari instans di Panduan Pengguna Amazon EC2.

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 konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.

2. Pada dasbor, pilih Luncurkan instans.
3. Untuk Nama, masukkan nama untuk instance NAT Anda.
4. Untuk Gambar Aplikasi dan OS, pilih NAT AMI Anda (pilih Jelajahi AMI lainnya, AMI Saya).
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). Nonaktifkan pemberiksaan sumber/tujuan
10. Perbarui tabel rute untuk mengirim lalu lintas ke instance NAT (lihatPerbarui tabel rute).

Nonaktifkan pemberiksaan sumber/tujuan

Setiap instans EC2 melakukan pemeriksaan sumber/tujuan secara default. Ini berarti bahwa instans harus menjadi sumber atau tujuan dari setiap lalu lintas yang dikirim atau diterima. Namun, instans NAT harus dapat mengirim dan menerima lalu lintas ketika sumber atau tujuan bukan dirinya sendiri. Oleh karena itu, Anda harus menonaktifkan pemeriksaan sumber / tujuan pada instans NAT.

Untuk menonaktifkan pemeriksaan sumber/tujuan

1. Buka konsol Amazon EC2 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.

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 Konfigurasikan tabel rute.

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. Pada panel navigasi, pilih Grup keamanan.
3. Pilih kotak centang untuk grup keamanan yang terkait dengan instans NAT Anda.
4. Pada tab Inbound rules (Aturan ke dalam), pilih Edit inbound rules (Edit aturan ke dalam).
5. Pilih Tambahkan aturan. Pilih Semua ICMP - IPv4 untuk Tipe. Pilih 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 Tipe. 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 konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada dasbor, pilih Luncurkan instans.
3. Pilih subnet pribadi Anda.
4. Jangan menetapkan alamat IP publik 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, konfigurasikan penerusan agen SSH, sehingga Anda dapat menggunakan instance NAT sebagai server bastion.

   Linux and macOS

   ```
   ssh-add key.pem
   ```

   Windows

   Unduh dan instal Pageant, jika belum diinstal.

   Konversi kunci pribadi Anda ke format.ppk 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 Nonaktifkan pemberiksaan sumber/tujuan.
- Verifikasi bahwa Anda mengonfigurasi tabel rute dengan benar. Untuk informasi selengkapnya, lihat 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 Mengakhiri instans Anda di Panduan Pengguna Amazon EC2.

Jika Anda tidak lagi memerlukan instans NAT, Anda dapat menghentikan atau menghentikannya, sehingga Anda tidak lagi ditagih untuk itu. Jika Anda membuat NAT AMI, Anda dapat membuat instance NAT baru kapan pun Anda membutuhkannya.

Bandingkan gateway NAT dan instans NAT

Berikut ini adalah rangkuman tingkat tinggi tentang perbedaan antara gateway NAT dan instans NAT. Kami menyarankan Anda menggunakan gateway NAT karena gateway NAT memberikan tingkat ketersediaan dan bandwidth yang lebih baik dan mudah bagi Anda untuk mengelolanya.

Atribut	Gateway NAT	Instans NAT
Ketersediaan	Hampir selalu tersedia. Gateway NAT di setiap Availability Zone diimplementasikan dengan redundansi. Buat gateway NAT di setiap Availability Zone untuk memastikan arsitektur yang tidak tergantung zona.	Gunakan skrip untuk mengelola failover antara instans.
Bandwidth	Skala hingga 100 Gbps.	Tergantung pada bandwidth dari tipe instans.
Maintenance	Dikelola oleh AWS. Anda tidak perlu melakukan perawatan apa pun.	Dikelola oleh Anda, misalnya, dengan menginstal pembaruan perangkat lunak atau patch sistem operasi pada instans.
Kinerja	Software dioptimalkan untuk menangani lalu lintas NAT.	AMI generik yang dikonfigurasi untuk melakukan NAT.

Atribut	Gateway NAT	Instans 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 dapat mengaitkannya dengan sumber daya di belakang gateway NAT untuk mengontrol lalu lintas masuk dan keluar.	Kaitkan instans NAT Anda dan sumber daya di belakang instans NAT Anda guna mengontrol lalu lintas masuk dan keluar.
ACL jaringan	Anda dapat menggunakan ACL jaringan untuk mengontrol lalu lintas ke dan dari subnet tempat gateway NAT Anda berada.	Menggunakan ACL jaringan untuk mengontrol lalu lintas ke dan dari subnet tempat instans NAT Anda berada.
Log alur	Gunakan log alur untuk menangkap lalu lintas.	Gunakan log alur untuk menangkap lalu lintas.
Penerusan port	Tidak didukung.	Secara manual menyesuaikan konfigurasi untuk mendukung penerusan port.
Server bastion	Tidak didukung.	Gunakan sebagai server bastion.

Atribut	Gateway NAT	Instans NAT
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 sebuah alamat IPv4 yang bersifat publik, statis, didesain untuk komputasi cloud dinamis. Anda dapat mengaitkan alamat IP Elastis dengan instans atau antarmuka jaringan

apa saja di VPC manapun di akun Anda. Dengan alamat IP Elastis, Anda dapat menutupi kegagalan suatu instans dengan meremajakan secara cepat alamat ke instans lain di VPC Anda.

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 Pengguna Amazon EC2.

Aturan-aturan berikut berlaku:

- Sebuah alamat IP Elastis dapat dikaitkan dengan sebuah instans atau antarmuka jaringan.
- Anda dapat memindahkan alamat IP Elastis dari satu instans atau antarmuka jaringan ke instans lainnya.
- Jika Anda mengaitkan sebuah alamat IP Elastis dengan antarmuka jaringan eth0 dari instans Anda, alamat IPv4 publik saat ini (jika ada) akan dilepas ke kumpulan alamat IP publik EC2-VPC. Jika Anda memisahkan alamat IP Elastis, antarmuka jaringan eth0 secara otomatis mendapat alamat IPv4 publik yang 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 di-support.
- Anda dapat memberi tag alamat IP Elastis yang dialokasikan untuk digunakan di VPC, namun, tag alokasi biaya tidak di-support. Jika Anda memulihkan alamat IP Elastis, tag tidak ikut terpulihkan.
- Anda dapat mengakses alamat IP Elastis dari internet ketika grup keamanan dan ACL jaringan mengizinkan lalu lintas dari alamat IP sumber. Lalu lintas balasan dari dalam VPC kembali ke internet akan memerlukan gateway internet. Untuk informasi selengkapnya, lihat Grup keamanan dan ACL jaringan.

- Anda dapat menggunakan salah satu opsi berikut untuk alamat IP Elastis:
  - Biarkan Amazon menyediakan alamat IP Elastis. Saat Anda memilih opsi ini, Anda dapat mengaitkan alamat-alamat IP Elastis dengan grup border jaringan. Ini adalah lokasi tempat kita mengiklankan blok CIDR. Mengatur grup perbatasan jaringan membatasi blok CIDR ke grup ini.
  - Gunakan alamat-alamat IP Anda sendiri. Untuk informasi tentang membawa alamat IP Anda sendiri, lihat Membawa alamat IP Anda sendiri (BYOIP) di Panduan Pengguna Amazon EC2.

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.

Bekerja dengan alamat IP Elastis

Bagian berikut ini menjelaskan bagaimana Anda bekerja dengan alamat IP Elastis.

Tugas

- Alokasikan sebuah alamat IP Elastis
- Kaitkan sebuah alamat IP Elastis
- Lihat alamat IP Elastis Anda
- Tag sebuah alamat IP Elastis
- Pisahkan alamat IP Elastis
- Transfer alamat IP Elastis
- Melepas alamat IP Elastis
- Memulihkan alamat IP Elastis
- gambaran umum API dan perintah

Alokasikan sebuah alamat IP Elastis

Sebelum Anda menggunakan IP Elastic, Anda harus mengalokasikan satu IP Elastis untuk digunakan di VPC Anda.

Untuk mengalokasikan Alamat IP elastis

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih IP Elastis.

3. Pilih Alokasi alamat IP elastis.
4. (Opsional) Ketika Anda mengalokasikan alamat IP elastis (EIP), Anda memilih grup batas jaringan untuk mengalokasikan EIP. Grup perbatasan jaringan adalah kumpulan Availability Zones (AZ), Local Zones, atau Wavelength Zones yang mengiklankan alamat IP publik. AWS Local Zones dan Wavelength Zones mungkin memiliki grup perbatasan jaringan yang berbeda dari AZ di Wilayah untuk memastikan latensi minimum atau jarak fisik antara jaringan dan pelanggan yang mengakses sumber daya AWS di Zona ini.

   > **Important**
   >
   > Anda harus mengalokasikan EIP dalam grup perbatasan jaringan yang sama dengan AWS sumber daya yang akan dikaitkan dengan EIP. EIP dalam satu grup perbatasan jaringan hanya dapat diiklankan di zona dalam grup perbatasan jaringan tersebut dan tidak di zona lain yang diwakili oleh grup perbatasan jaringan lainnya.

   Jika Anda mengaktifkan Local Zones atau Wavelength Zone (untuk informasi selengkapnya, lihat Mengaktifkan Local Zones atau Mengaktifkan Wavelength Zone), Anda dapat memilih grup perbatasan jaringan untuk AZ, Local Zones, atau Wavelength Zone. Pilih grup perbatasan jaringan dengan hati-hati karena EIP dan AWS sumber daya yang terkait dengannya harus berada di grup perbatasan jaringan yang sama. Anda dapat menggunakan konsol EC2 untuk melihat grup perbatasan jaringan tempat Zona Ketersediaan, Local Zones, atau Wavelength Zone berada (lihat Local Zones). Biasanya, semua Zona Ketersediaan di Wilayah milik grup perbatasan jaringan yang sama, sedangkan Local Zones atau Wavelength Zone milik grup perbatasan jaringan mereka sendiri yang terpisah.

   Jika Anda tidak mengaktifkan Local Zones atau Wavelength Zone, saat Anda mengalokasikan EIP, grup perbatasan jaringan yang mewakili semua AZ untuk Wilayah tersebut (seperti `us-west-2`) telah ditentukan sebelumnya untuk Anda dan Anda tidak dapat mengubahnya. Ini berarti bahwa EIP yang Anda alokasikan ke grup perbatasan jaringan ini akan diiklankan di semua AZ di Wilayah tempat Anda berada.
5. Untuk Kumpulan alamat IPv4 publik, pilih salah satu dari berikut ini:

   - Kumpulan alamat IP Amazon—Jika Anda menginginkan sebuah alamat IPv4 dialokasikan dari kumpulan alamat IP Amazon.

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

Kaitkan sebuah alamat IP Elastis

Anda dapat mengaitkan alamat IP Elastis dengan instans atau antarmuka jaringan yang sedang berjalan di VPC Anda.

Setelah Anda mengaitkan alamat IP Elastis dengan instans Anda, instans tersebut menerima nama host DNS publik jika nama host DNS diaktifkan. Untuk informasi selengkapnya, lihat Atribut DNS untuk VPC Anda.

Untuk mengaitkan sebuah alamat IP Elastis dengan sebuah instans atau antarmuka jaringan

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di jendela navigasi, pilih IP Elastis.
3. Pilih alamat IP Elastis yang dialokasikan untuk digunakan dengan VPC (kolom Cakupan memiliki nilai `vpc`), lalu pilih Tindakan, Alamat IP Elastis.
4. Pilih Instans atau Antarmuka jaringan, dan kemudian pilih instans atau ID antarmuka jaringan. Pilih alamat IP pribadi yang untuk dikaitkan dengan alamat IP Elastis. Pilih Kaitkan.

Lihat alamat IP Elastis Anda

Anda dapat melihat alamat IP Elastis yang dialokasikan ke akun Anda.

Untuk melihat alamat IP Elastis Anda

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di jendela navigasi, pilih IP Elastis.
3. Untuk mem-filter daftar yang ditampilkan, mulailah mengetik bagian dari alamat IP elastis atau salah satu dari atributnya di kotak pencarian.

Tag sebuah alamat IP Elastis

Anda dapat menerapkan tag ke alamat IP Elastis Anda untuk membantu Anda mengidentifikasi atau mengkategorikannya sesuai dengan kebutuhan organisasi Anda.

Untuk menandai alamat IP Elastis

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di jendela navigasi, pilih IP Elastic.
3. Pilih alamat IP Elastis dan pilih Tag.
4. Pilih Kelola tag, masukkan kunci tag dan nilai sesuai yang diminta, dan pilih Simpan.

Pisahkan alamat IP Elastis

Untuk mengubah sumber daya yang terkait dengan alamat IP elastis, Anda harus terlebih dahulu memisahkan alamat IP elastis dari sumber daya yang terkait saat ini.

Untuk memisahkan alamat IP Elastis

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di jendela navigasi, pilih IP Elastis.
3. Pilih alamat IP Elastis, dan lalu pilih Tindakan, Pisahkan alamat IP Elastis.
4. Saat diminta, pilih Pisahkan.

Transfer alamat IP Elastis

Bagian ini menjelaskan cara mentransfer alamat IP Elastis dari satu Akun AWS ke yang lain. Mentransfer alamat IP Elastis dapat membantu dalam situasi berikut:

- Restrukturisasi organisasi — Gunakan transfer alamat IP Elastis untuk memindahkan beban kerja dengan cepat dari satu Akun AWS ke yang lain. Anda tidak perlu menunggu alamat IP Elastis baru diizinkan terdaftar di grup keamanan dan NACL Anda.
- Administrasi keamanan terpusat — Gunakan akun AWS keamanan terpusat untuk melacak dan mentransfer alamat IP Elastis yang telah diperiksa untuk kepatuhan keamanan.
- Pemulihan bencana - Gunakan transfer alamat IP Elastis untuk memetakan ulang IP dengan cepat untuk beban kerja internet yang dihadapi publik selama peristiwa darurat.

Tidak ada biaya untuk mentransfer alamat IP Elastis.

Tugas

- Aktifkan transfer alamat IP Elastis
- Nonaktifkan transfer alamat IP Elastis
- Menerima alamat IP Elastis yang ditransfer

Aktifkan transfer alamat IP Elastis

Bagian ini menjelaskan cara menerima alamat IP Elastis yang ditransfer. Perhatikan batasan berikut yang terkait dengan mengaktifkan alamat IP Elastis untuk transfer:

- Anda dapat mentransfer alamat IP 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 perintah AWS CLI deskripsi-alamat-transfer). 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 AWS CLI perintah deskripsi-alamat-transfer) selama tiga 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 alamat IPv4 publik yang Anda bawa ke kolam alamat Bring Your Own IP (BYOIP). Akun AWS
- 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 IP Elastis.
4. Pilih satu atau beberapa alamat IP elastis untuk mengaktifkan transfer dan pilih Tindakan, Aktifkan transfer.
5. Jika Anda mentransfer beberapa alamat IP 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 ID akun AWS yang ingin Anda transfer alamat IP Elastis.

7. Konfirmasikan transfer dengan memasukkan **`enable`** dalam kotak teks.
8. Pilih Kirim.
9. Untuk menerima transfer, lihat Menerima alamat IP Elastis yang ditransfer. Untuk menonaktifkan transfer, lihat Nonaktifkan transfer alamat IP Elastis.

Nonaktifkan transfer alamat IP Elastis

Bagian ini menjelaskan cara menonaktifkan transfer IP Elastis setelah transfer diaktifkan.

Langkah-langkah ini harus diselesaikan oleh akun sumber yang mengaktifkan transfer.

Untuk menonaktifkan transfer alamat IP Elastis

1. Pastikan Anda menggunakan AWS akun sumber.
2. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
3. Di panel navigasi, pilih IP Elastis.
4. Dalam daftar sumber daya IP Elastis, pastikan properti Anda diaktifkan yang menampilkan status Transfer kolom.
5. Pilih satu atau beberapa alamat IP elastis yang memiliki status Transfer Tertunda, dan pilih Tindakan, Nonaktifkan transfer.
6. Konfirmasikan dengan memasukkan **`disable`** di kotak teks.
7. Pilih Kirim.

Menerima alamat IP Elastis yang ditransfer

Bagian ini menjelaskan cara menerima alamat IP Elastis yang ditransfer.

Saat Anda mentransfer alamat IP Elastis, ada jabat tangan dua langkah di antara. Akun AWS Ketika akun sumber memulai transfer, akun transfer memiliki tujuh hari untuk menerima transfer alamat IP Elastis. Selama tujuh hari itu, akun sumber dapat melihat transfer yang tertunda (misalnya di AWS konsol atau dengan menggunakan perintah AWS CLI deskripsi-alamat-transfer). Setelah tujuh hari, transfer berakhir dan kepemilikan alamat IP Elastis kembali ke akun sumber.

Saat menerima transfer, perhatikan pengecualian berikut yang mungkin terjadi dan cara mengatasinya:

- AddressLimitTerlampaui: Jika akun transfer Anda telah melebihi kuota alamat IP Elastis, akun sumber dapat mengaktifkan transfer alamat IP Elastis, tetapi pengecualian ini terjadi ketika akun

transfer mencoba menerima transfer. Secara default, semua AWS akun dibatasi hingga 5 alamat IP Elastis per Wilayah. Lihat Batas alamat IP elastis di Panduan Pengguna Amazon EC2 untuk petunjuk tentang 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 Pengguna Amazon EC2.
- InvalidTransfer. AddressAssociated: Jika alamat IP Elastis dikaitkan dengan instans ENI atau EC2, 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 Pengguna Amazon EC2.

Untuk pengecualian lainnya, hubungi AWS Support.

Langkah-langkah ini harus diselesaikan oleh akun transfer.

Untuk menerima transfer alamat IP Elastis

1. Pastikan Anda menggunakan akun transfer.
2. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
3. Di panel navigasi, pilih IP Elastis.
4. Pilih Tindakan, Terima transfer.
5. Tidak ada tanda yang terkait dengan alamat IP Elastis yang ditransfer dengan alamat IP Elastis saat Anda menerima transfer. Jika Anda ingin menentukan tanda Nama untuk alamat IP Elastis yang Anda terima, pilih Buat tanda dengan kunci 'Nama' dan nilai yang Anda tentukan.
6. Masukkan alamat IP Elastis yang ingin Anda transfer.
7. Jika Anda menerima beberapa alamat IP Elastis yang ditransfer, pilih Tambah alamat untuk memasukkan alamat IP Elastis tambahan.
8. Pilih Kirim.

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 tetapi itu 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 jendela navigasi, pilih IP Elastis.
3. Pilih alamat IP Elastis, lalu pilih Tindakan, Melepas alamat IP Elastis.
4. Saat diminta, pilih Lepas.

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
```

gambaran umum API dan 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

- terima-alamat-transfer ()AWS CLI

- Approve-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Mengalokasikan alamat IP Elastis

- allocate-address (AWS CLI)
- New-EC2Address (AWS Tools for Windows PowerShell)

Kaitkan alamat IP Elastis dengan instans atau antarmuka jaringan

- associate-address (AWS CLI)
- Register-EC2Address (AWS Tools for Windows PowerShell)

Jelaskan transfer alamat IP Elastis

- jelaskan-alamat-transfer ()AWS CLI
- Get-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Nonaktifkan transfer alamat IP Elastis

- menonaktifkan-alamat-transfer ()AWS CLI
- Disable-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Pisahkan alamat IP Elastis

- disassociate-address (AWS CLI)
- Unregister-EC2Address (AWS Tools for Windows PowerShell)

Aktifkan transfer alamat IP Elastis

- aktifkan-alamat-transfer ()AWS CLI
- Enable-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Merilis alamat IP Elastis

- release-address (AWS CLI)

- Remove-EC2Address (AWS Tools for Windows PowerShell)

Menandai alamat IP Elastis

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

Lihat alamat IP Elastis Anda

- describe-addresses (AWS CLI)
- Get-EC2Address (AWS Tools for Windows PowerShell)

Harga

Untuk memastikan penggunaan alamat IP Elastis yang efisien, kami mengenakan biaya per jam yang kecil. Untuk informasi selengkapnya, lihat Alamat IPv4 Publik di Harga Amazon VPC.

Connect VPC Anda ke VPC dan jaringan lain menggunakan gateway transit

Anda dapat menghubungkan virtual private cloud (VPC) dan jaringan on-premise menggunakan transit gateway, yang bertindak sebagai hub pusat, merutekan lalu lintas antara VPC, koneksi VPN, danAWS Direct Connect koneksi. Untuk informasi selengkapnya, lihat AWS Transit Gateway.

Tabel berikut menjelaskan beberapa kasus penggunaan umum untuk gateway transit dan menyediakan tautan ke informasi lebih lanjut di Amazon VPC Transit Gateways.

Contoh	Penggunaan
Router terpusat	Konfigurasikan transit gateway Anda sebagai router terpusat yang menghubungkan semua VPC,,AWS Direct Connect, danAWS Site-to-Site VPN koneksi. Untuk informasi selengkap nya, lihat Contoh: Router terpusat.
VPC Terisolasi	Konfigurasikan transit gateway Anda sebagai beberapa router terisolasi. Hal ini mirip dengan menggunakan beberapa transit

Contoh	Penggunaan
	gateway, tetapi memberikan lebih banyak fleksibilitas dalam kasus di mana rute dan lampiran mungkin berubah. Untuk informasi selengkapnya, lihat Contoh: VPC Terisolasi.
VPC Terisolasi dengan Layanan Bersama	Konfigurasikan transit gateway 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 Contoh: VPC terisolasi dengan layanan bersama.

Connect VPC Anda ke jaringan jarak jauh menggunakanAWS Virtual Private Network

Anda dapat menghubungkan VPC Anda ke jaringan jarak jauh dan pengguna menggunakan opsi koneksi VPN berikut.

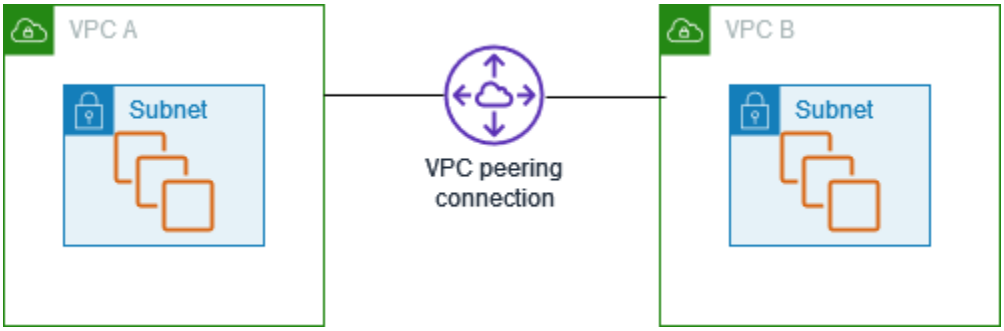
Opsi koneksi VPN	Deskripsi
AWS Site-to-Site VPN	Anda dapat membuat koneksi VPN IPsec antara VPC dan jaringan jarak jauh Anda. Pada sisi koneksi Site-to-Site VPN AWS, virtual private gateway atau transit gateway menyediakan dua titik akhir VPN (terowongan) untuk failover otomatis. Anda mengkonfigurasi perangkat gateway pelanggan di sisi jarak jauh koneksi Site-to-Site VPN. Untuk informasi selengkapnya, lihat Panduan PenggunaAWS Site-to-Site VPN..
AWS Client VPN	AWS Client VPN adalah layanan VPN yang berbasis klien terkelola yang memungkinkan Anda mengakses sumber daya AWS dan sumber daya di jaringan on-premise Anda dengan aman. Dengan AWS Client VPN, Anda mengkonfigurasi titik akhir yang dapat terhubung oleh pengguna Anda untuk membuat sesi TLS VPN yang aman. Hal ini memungkinkan klien untuk mengakses sumber daya di AWS atau on-premise dari lokasi

Opsi koneksi VPN	Deskripsi
	mana pun menggunakan klien VPN berbasis OpenVPN. Untuk informasi selengkapnya, lihat Panduan Administrator AWS Client VPN.
AWSVPN CloudHub	Jika Anda memiliki lebih dari satu jaringan jarak jauh (misalnya, beberapa kantor cabang), Anda dapat membuat beberapa koneksi AWS Site-to-Site VPN melalui virtual private gateway Anda untuk memungkin kan komunikasi antar jaringan ini. Untuk informasi selengkapnya, lihat Menyediakan komunikasi yang aman antar situs menggunakan VPN CloudHub di PanduanAWS Site-to-Site VPN Pengguna.
Peralatan VPN perangkat lunak pihak ke tiga	Anda dapat membuat koneksi VPN ke jaringan jarak jauh Anda dengan menggunakan instans Amazon EC2 di VPC Anda yang menjalankan peralatan perangkat lunak VPN pihak ketiga. AWS tidak menyediakan atau memelihara peralatan VPN perangkat lunak pihak ketiga; namun, Anda dapat memilihnya dari berbagai produk yang disediakan oleh mitra dan komunitas sumber terbuka. Temukan peralatan VPN perangkat lunak pihak ke tiga di AWS Marketplace.

Anda dapat juga menggunakan AWS Direct Connect untuk membuat koneksi privat khusus dari jaringan jarak jauh ke VPC Anda. Anda dapat menggabungkan koneksi ini dengan AWS Site-to-Site VPN untuk membuat sambungan terenkripsi IPsec. Untuk informasi lebih lanjut, lihat Apa AWS Direct Connect? dalam AWS Direct Connect Panduan Pengguna.

Connect VPC menggunakan VPC peering

Suatu koneksi peering VPC adalah koneksi jaringan antara dua VPC yang memungkinkan Anda merutekan lalu lintas di antara keduanya secara privat. Sumber daya di VPC yang terpeering dapat berkomunikasi satu sama lain seolah-olah mereka ada di jaringan yang sama. Anda dapat membuat koneksi peering VPC antara VPC Anda sendiri, dengan VPC di lainAkun AWS, atau dengan VPC diAWS Wilayah yang berbeda. Lalu lintas antara VPC yang mengintip tidak pernah melintasi internet publik.



AWSmenggunakan infrastruktur VPC yang ada untuk membuat koneksi peering VPC. koneksi peering VPC bukanlah gateway atauAWS Site-to-Site VPN koneksi, dan itu tidak bergantung pada bagian terpisah dari perangkat keras fisik. Tidak ada satu titik kegagalan untuk komunikasi atau kemacetan bandwidth.

Untuk informasi selengkapnya, lihat Panduan Peering Amazon VPC.

Pemantauan VPC Anda

Anda dapat menggunakan alat berikut untuk memantau lalu lintas atau akses jaringan di virtual private cloud (VPC).

Log Alur VPC

Anda dapat menggunakan Log Aliran VPC untuk menangkap informasi rinci tentang lalu lintas ke dan dari antarmuka jaringan di VPC Anda.

Pengelola Alamat IP Amazon (IPAM)

Anda dapat menggunakan IPAM untuk merencanakan, melacak, dan memantau alamat IP untuk beban kerja Anda. Untuk informasi selengkapnya, lihat Pengelola Alamat IP.

Pencerminan Lalu lintas

Anda dapat menggunakan fitur ini untuk menyalin lalu lintas jaringan dari antarmuka jaringan instans Amazon EC2 dan mengirimkannya ke peralatan out-of-band keamanan dan pemantauan untuk pemeriksaan paket dalam. Anda dapat mendeteksi anomali jaringan dan keamanan, mendapatkan wawasan operasional, menerapkan kontrol kepatuhan dan keamanan, serta memecahkan masalah. Untuk informasi selengkapnya, lihat Mirroring Lalu Lintas.

Analisis Reachability Analyzer

Anda dapat menggunakan alat ini untuk menganalisis dan reachability jaringan debug antara dua sumber daya di VPC Anda. Setelah Anda menentukan sumber daya sumber dan tujuan, Reachability Analyzer menghasilkan hop-by-hop detail jalur virtual di antara keduanya saat dapat dijangkau, dan mengidentifikasi komponen pemblokiran saat tidak dapat dijangkau. Untuk informasi selengkapnya, lihat Reachability Analyzer.

Penganalisis Akses

Anda dapat menggunakan Network Access Analyzer untuk memahami akses jaringan ke sumber daya Anda. Ini membantu Anda mengidentifikasi peningkatan pada postur keamanan jaringan Anda dan menunjukkan bahwa jaringan Anda memenuhi persyaratan kepatuhan tertentu. Untuk informasi selengkapnya, lihat Penganalisis Akses.

CloudTrail log

Anda dapat menggunakanAWS CloudTrail untuk mengambil informasi mendetail tentang panggilan yang dibuat ke API Amazon VPC. Anda dapat menggunakan CloudTrail log yang

dihasilkan untuk menentukan panggilan mana yang dibuat, alamat IP sumber asal panggilan, siapa yang membuat panggilan, kapan panggilan dibuat, dan seterusnya. Untuk informasi selengkapnya, lihat Pencatatan panggilan API Amazon EC2 Amazon EC2, dan panggilan API Amazon VPC menggunakanAWS CloudTrail dalam Referensi API Amazon EC2.

Mencatat lalu lintas IP menggunakan VPC Flow Logs

Log Alur VPC adlaah fitur yang membuat Anda dapat menangkap informasi tentang lalu lintas IP yang pergi ke dan dari antarmuka jaringan. Data log aliran dapat dipublikasikan ke lokasi berikut: Amazon CloudWatch Log, Amazon S3, atau Amazon Data Firehose. Setelah membuat log alur, Anda dapat mengambil dan melihat catatan log alur di grup log, bucket, atau aliran pengiriman yang Anda konfigurasi.

Log alur dapat membantu Anda dengan sejumlah tugas, seperti:

- Mendiagnosis aturan grup keamanan yang terlalu ketat
- Memantau lalu lintas yang mencapai instans Anda
- Menentukan arah lalu lintas ke dan dari antarmuka jaringan

Data log alur dikumpulkan di luar jalur lalu lintas jaringan Anda, dan oleh karena itu tidak mempengaruhi throughput atau latensi jaringan. Anda dapat membuat atau menghapus log alur tanpa risiko dampak terhadap kinerja jaringan.

> **Note**
>
> Bagian ini hanya berbicara tentang flow log untuk VPC. 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

- 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

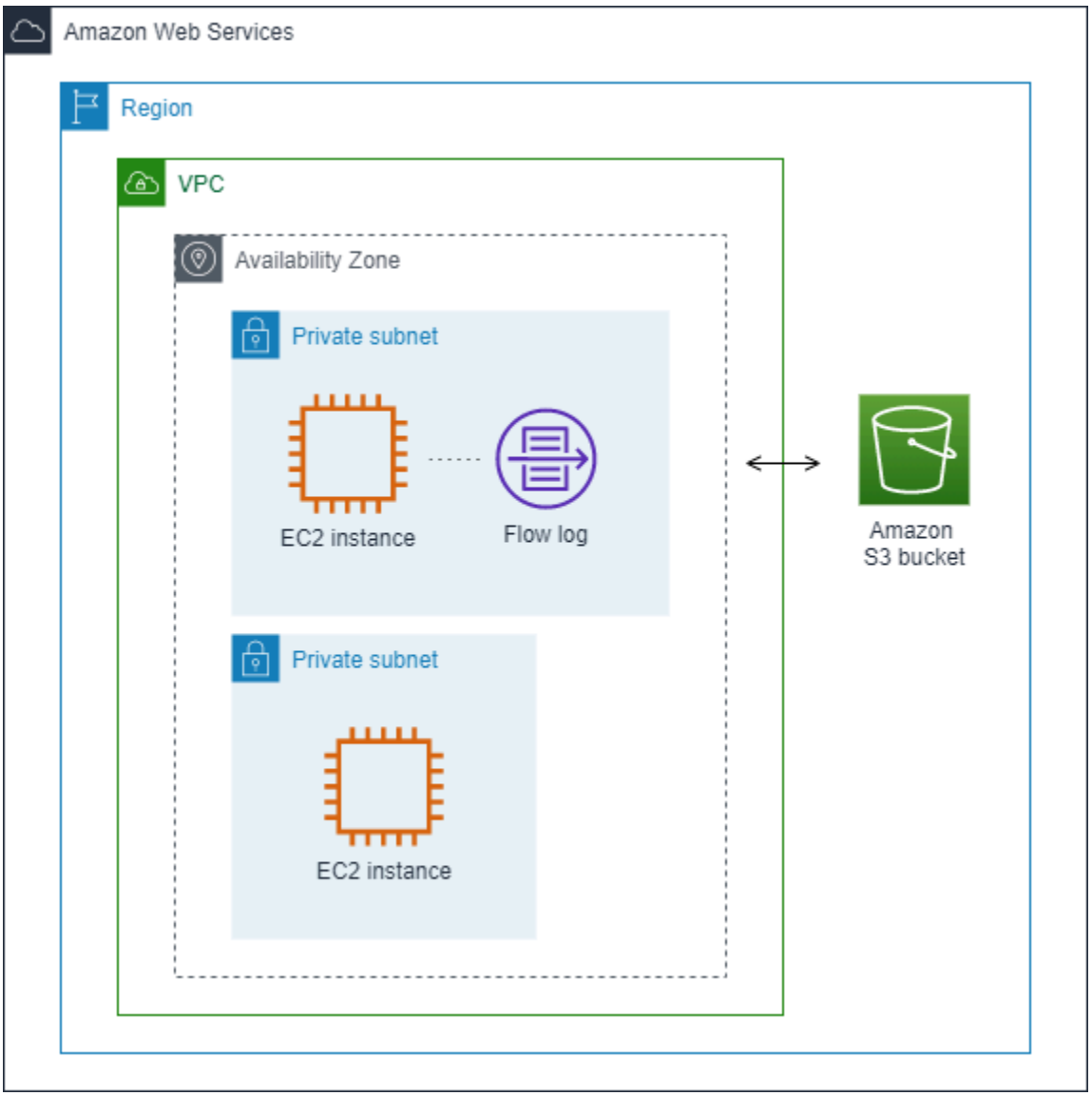
Anda dapat membuat log alur untuk VPC, subnet, atau antarmuka jaringan. Jika Anda membuat log alur untuk subnet atau VPC, setiap antarmuka jaringan di subnet atau VPC dipantau.

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.

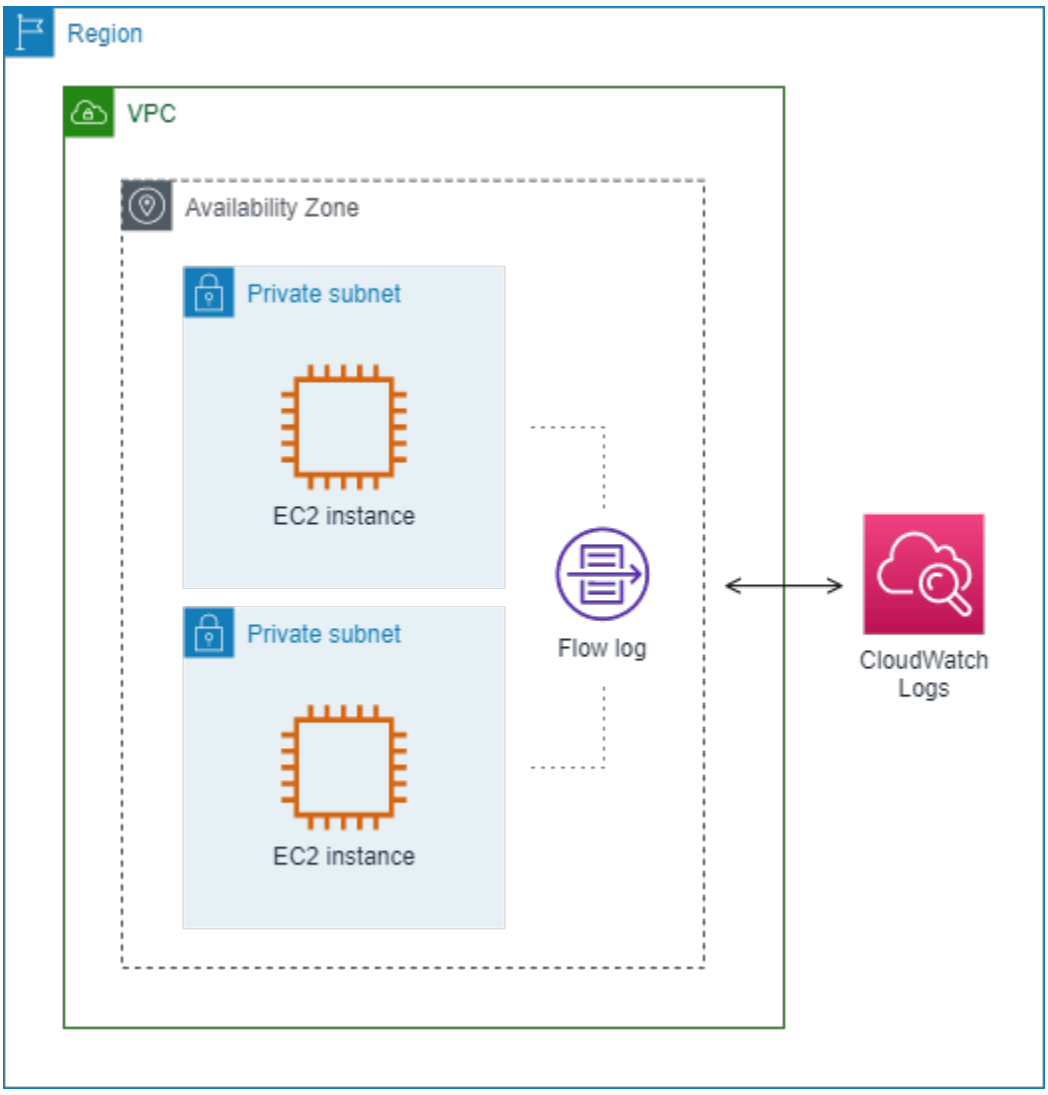
Untuk membuat log alur, Anda menentukan:

- 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 instans EC2 di subnet pribadi dan menerbitkan catatan log aliran 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 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 konsol Amazon EC2 atau Amazon EC2 API untuk membuat log alur untuk antarmuka jaringan.

Anda dapat memberikan tag ke log alur Anda. Setiap tanda terdiri dari sebuah kunci dan sebuah nilai opsional, yang keduanya Anda tentukan. Tag dapat membantu Anda mengatur log alur, misalnya berdasarkan tujuan atau pemilik.

Jika Anda tidak lagi membutuhkan log alur, Anda dapat menghapusnya. Menghapus log 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 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

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 mengizinkan Anda untuk membuat log alur yang kustom untuk kebutuhan Anda dan untuk menghilangkan bidang yang tidak relevan. Menggunakan format kustom dapat mengurangi kebutuhan untuk proses terpisah untuk mengekstrak informasi spesifik dari log alur yang diterbitkan. Anda dapat menentukan berapa pun bidang log alur yang tersedia, tetapi Anda harus menentukan setidaknya satu bidang log alur.

Bidang yang tersedia

Tabel berikut menjelaskan semua bidang yang tersedia untuk catatan log alur. Kolom Versi menunjukkan versi Log Alur VPC di mana bidang diperkenalkan. Format default mencakup 2 bidang semua versi, dalam urutan yang sama sebagaimana yang tercantum di tabel.

Saat 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 Parket, 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 parket: INT_32	2
account-id	ID AWS akun pemilik antarmuka jaringan sumber yang lalu lintas dicatat. 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 parket: STRING	2
interface-id	ID antarmuka jaringan yang lalu lintasnya dicatat. Jenis data parket: STRING	2
srcaddr	Alamat sumber untuk lalu lintas masuk, atau alamat IPv4 atau IPv6 dari antarmuka jaringan untuk lalu lintas keluar pada antarmuka jaringan. Alamat IPv4 antarmuka jaringan selalu merupakan alamat IPv4 privatnya. Lihat juga pkt-srcaddr. Jenis data parket: STRING	2
dstaddr	Alamat tujuan untuk lalu lintas keluar, atau alamat IPv4 atau IPv6 dari antarmuka jaringan untuk lalu lintas masuk pada antarmuka	2

Bidang	Deskripsi	Versi
	jaringan. Alamat IPv4 antarmuka jaringan selalu merupakan alamat IPv4 privatnya. Lihat juga pkt-dstaddr. Jenis data parket: STRING	
srcport	Port sumber lalu lintas. Tipe data parket: INT_32	2
dstport	Port tujuan lalu lintas. Tipe data parket: INT_32	2
protocol	Nomor protokol IANA lalu lintas. Untuk informasi selengkapnya, lihat Nomor Protokol Internet yang Ditugaskan. Tipe data parket: INT_32	2
packets	Jumlah paket yang ditransfer selama aliran. Tipe data parket: INT_64	2
bytes	Jumlah byte yang ditransfer selama aliran. Tipe data parket: INT_64	2
start	Waktu, dalam detik Unix, ketika paket pertama aliran diterima dalam interval agregasi. Ini mungkin sampai 60 detik setelah paket ditransmisikan atau diterima pada antarmuka jaringan. Tipe data parket: 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 parket: 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 grup keamanan atau ACL jaringan, 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. Jenis data parket: STRING	2
vpc-id	ID VPC yang berisi antarmuka jaringan yang lalu lintasnya dicatat. Jenis data parket: STRING	3
subnet-id	ID subnet yang berisi antarmuka jaringan yang lalu lintasnya dicatat. Jenis data parket: STRING	3
instance-id	ID instans yang terkait dengan antarmuka jaringan yang lalu lintasnya dicatat, jika instans dimiliki oleh Anda. Mengembalikan simbol '-' untuk Antarmuka jaringan yang dikelola peminta; sebagai contoh, antaramuka untuk NAT gateway. Jenis data parket: STRING	3

Bidang	Deskripsi	Versi
tcp-flags	Nilai bitmask untuk bendera TCP berikut: • FIN — 1 • SYN — 2 • RST — 4 • SYN-ACK — 18 Jika tidak ada flag yang didukung 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 parket: INT_32	3
type	Jenis lalu lintas. Nilai yang mungkin adalah: IPv4 | IPv6 |EFA. Untuk informasi selengkapnya, lihat Adaptor Elastic Fabric. Jenis data parket: STRING	3

Bidang	Deskripsi	Versi
pkt-srcaddr	Alamat IP sumber tingkat paket (asli) lalu lintas. Gunakan bidang ini dengan bidang srcaddr untuk membedakan antara alamat IP dari lapisan menengah yang dilalui alairan lalu lintas, dan alamat IP sumber asal dari lalu lintas. Misalnya, 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 parket: STRING	3
pkt-dstaddr	Alamat IP tujuan tingkat paket (asli) untuk lalu lintas. Gunakan bidang ini dengan bidang dstaddr untuk membedakan antara alamat IP dari lapisan menengah yang dilalui alairan lalu lintas, dan alamat IP tujuan akhir dari lalu lintas. Misalnya, saat lalu lintas mengalir antaramuka 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 parket: STRING	3
region	Wilayah yang berisi antarmuka jaringan yang lalu lintasnya dicatat. Jenis data parket: STRING	4
az-id	ID dari Availability Zone yang berisi antarmuka jaringan yang lalu lintasnya dicatat. Jika lalu lintas berasal dari sublokasi, catatan akan menampilkan simbol '-' untuk bidang ini. Jenis data parket: STRING	4

Bidang	Deskripsi	Versi
sublocation-type	Jenis sublokasi yang dikembalikan dalam bidang sublocation-id. Nilai yang mungkin adalah: wavelength | outpost | localzone. Jika lalu lintas bukan dari sublokasi, catatan menampilkan simbol '-' untuk bidang ini. Jenis data parket: STRING	4
sublocation-id	ID sublokasi yang berisi antarmuka jaringan yang lalu lintasnya dicatat. Jika lalu lintas bukan dari sublokasi, catatan menampilkan simbol '-' untuk bidang ini. Jenis data parket: STRING	4
pkt-src-aws-service	Nama subset alamat IP berkisar untuk pkt-srcaddr bidang, jika alamat IP sumber adalah untuk AWS layanan. Jika pkt-srcaddr milik rentang tumpang tindih, hanya pkt-src-aws-service akan menampilkan salah satu kode layanan. AWS Nilai yang mungkin adalah: AMAZON AMAZON_APPFLOW | AMAZON_CONNECT | API_GATEWAY | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRONT | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTANCE_CONNECT | GLOBALACCELERATOR KINESIS_VIDEO_STREAMS | ROUTE53 | ROUTE53_HEALTHCHECKS | ROUTE53_HEALTHCHECKS_PUBLISHING | ROUTE53_RESOLVER | S3 | | WORKSPACES_GATEWAYS Jenis data parket: 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 parket: STRING	5

Bidang	Deskripsi	Versi
flow-direction	Arah aliran sehubungan dengan antarmuka di mana lalu lintas ditangkap. Kemungkinan nilai adalah: ingress | egress. Jenis data parket: STRING	5
traffic-path	Jalan yang dilalui lalu lintas egress untuk ke tujuan. Untuk menentukan apakah lalu lintas merupakan lalu lintas keluar, periksa bidang flow-direction. Kemungkinan nilainya adalah sebagai berikut. Jika tidak ada nilai yang berlaku, bidang diatur ke -. • 1 — Melalui sumber daya lain di VPC yang sama, termasuk 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 parket: INT_32	5
ecs-cluster-arn	AWS Nama Sumber Daya (ARN) dari cluster ECS jika lalu lintas berasal dari tugas ECS yang sedang berjalan. Untuk menyertak an bidang ini dalam langganan Anda, Anda memerlukan izin untuk menelepon ecs:ListClusters. Jenis data parket: STRING	7
ecs-cluster-nama	Nama cluster ECS jika lalu lintas berasal dari tugas ECS yang sedang berjalan. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerlukan izin untuk menelepon ecs:ListClusters. Jenis data parket: STRING	7

Bidang	Deskripsi	Versi
ecs-container-instance-arn	ARN dari instance kontainer ECS jika lalu lintas berasal dari tugas ECS yang sedang berjalan pada instance EC2. Jika penyedia kapasitas adalah AWS Fargate, bidang ini akan menjadi '-'. Untuk menyertakan bidang ini dalam langganan Anda, Anda memerluka n izin untuk memanggil ecs: ListClusters dan ecs: ListContainer Instances. Jenis data parket: STRING	7
ecs-container-instance-id	ID instance kontainer ECS jika lalu lintas berasal dari tugas ECS yang sedang berjalan pada instance EC2. Jika penyedia kapasitas adalah AWS Fargate, bidang ini akan menjadi '-'. Untuk menyertak an bidang ini dalam langganan Anda, Anda memerlukan izin untuk memanggil ecs: ListClusters dan ecs: ListContainer Instances. Jenis data parket: 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 parket: 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 parket: STRING	7

Bidang	Deskripsi	Versi
ecs-service-nama-	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 parket: STRING	7
ecs-task-definitio n-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 parket: 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 parket: 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 parket: STRING	7

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

- Tidak ada data dan catatan yang dilewati
- Aturan grup keamanan dan ACL jaringan
- Lalu lintas IPv6
- 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
```

Dalam contoh ini, catatan dilewati selama interval agregasi. VPC Flow Logs melewatkan 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
```

Aturan grup keamanan dan ACL jaringan

Jika Anda menggunakan log alur untuk mendiagnosis aturan grup keamanan yang terlalu ketat atau longgar atau aturan ACL jaringan, perhatikan tingkat stateful sumber daya ini. Grup keamanan bersifat stateful - ini berarti bahwa respon untuk ke lalu lintas yang diizinkan juga diizinkan, bahkan jika aturan dalam grup keamanan Anda tidak mengizinkannya. Sebaliknya, ACL jaringan bersifat stateless, oleh karena itu respon terhadap lalu lintas yang diizinkan tunduk pada aturan ACL jaringan.

Misalnya, Anda menggunakan perintah ping dari komputer rumah Anda (alamat IP adalah 203.0.113.12) ke instans Anda (alamat IP privat antarmuka jaringan adalah 172.31.16.139). Aturan masuk grup keamanan mengizinkan lalu lintas ICMP tetapi aturan keluar tidak mengizinkan lalu lintas ICMP. Karena grup keamanan bersifat stateful, ping respon dari instans Anda diizinkan. ACL jaringan Anda mengizinkan lalu lintas ICMP masuk tetapi tidak mengizinkan lalu lintas ICMP keluar. Karena ACL jaringan bersifat stateless, ping respon dijatuhkan dan tidak mencapai komputer rumah Anda. Dalam log alur default, ini ditampilkan sebagai dua catatan log alur:

- Catatan ACCEPT untuk ping asal yang diizinkan oleh ACL jaringan dan grup keamanan, dan oleh karena itu diizinkan untuk mencapai instans Anda.
- Catatan REJECT untuk ping respon yang ditolak ACL jaringan.

```
2 123456789010 eni-1235b8ca123456789 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027
 1432917142 ACCEPT OK
```

```
2 123456789010 eni-1235b8ca123456789 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094
 1432917142 REJECT OK
```

Jika ACL jaringan Anda mengizinkan lalu lintas ICMP keluar, log alur menampilkan dua catatan ACCEPT (satu untuk ping asal dan satu untuk ping respon). Jika grup keamanan Anda menolak lalu lintas ICMP masuk, log alur menampilkan catatan REJECT, karena lalu lintas tidak diizinkan untuk mencapai instans Anda.

Lalu lintas IPv6

Berikut ini adalah contoh catatan log alur default. Dalam contoh, lalu lintas SSH (port 22) dari alamat IPv6 2001:db8:1234:a100:8d6e:3477:df66:f105 ke antarmuka jaringan eni-1235b8ca123456789 di akun 123456789010 diizinkan.

```
2 123456789010 eni-1235b8ca123456789 2001:db8:1234:a100:8d6e:3477:df66:f105
 2001:db8:1234:a102:3304:8879:34cf:4071 34892 22 6 54 8855 1477913708 1477913820 ACCEPT
 OK
```

Urutan bendera TCP

Bagian ini berisi contoh log 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.

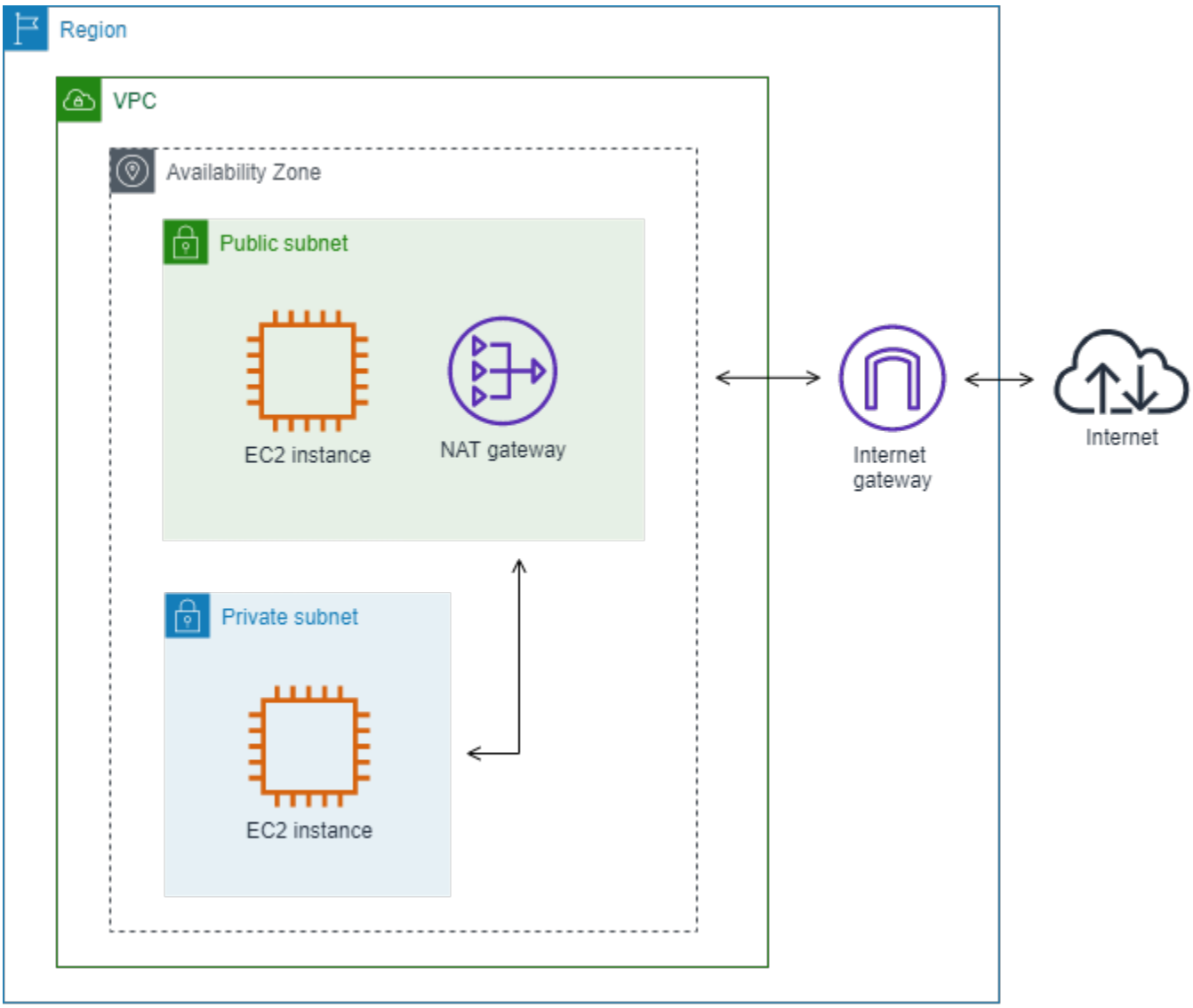
```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43418 10.0.0.62
 52.213.180.42 6 63388 1219 1566848933 1566849113 ACCEPT 1 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 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.

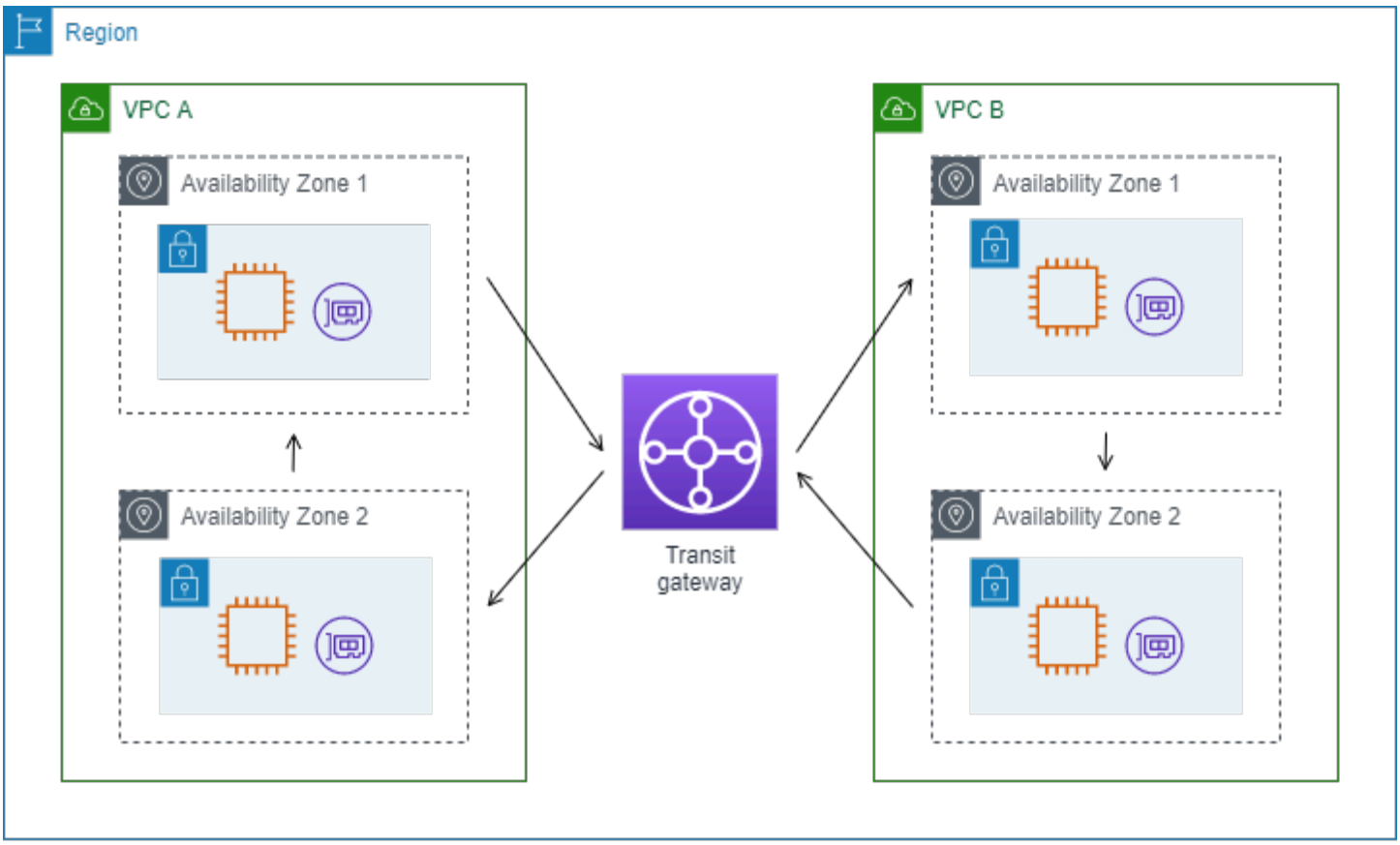
```
- eni-1235b8ca123456789 10.0.0.220 10.0.1.5 203.0.113.5 10.0.1.5
```

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 antaramuka jaringan untuk gateway NAT, antaramuka jaringan ini bukan antaramuka 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-22222222222222222).



Anda membuat log alur kustom untuk VPC B dengan format berikut.

```
version interface-id account-id vpc-id subnet-id instance-id srcaddr dstaddr srcport
 dstport protocol tcp-flags type pkt-srcaddr pkt-dstaddr action log-status
```

Baris berikut dari catatan log alur menunjukkan aliran lalu lintas pada antarmuka jaringan untuk web server. Baris pertama adalah lalu lintas permintaan dari klien, dan baris terakhir adalah lalu lintas respon dari server web.

```
3 eni-33333333333333333 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb
 i-01234567890123456 10.20.33.164 10.40.2.236 39812 80 6 3 IPv4 10.20.33.164
 10.40.2.236 ACCEPT OK
...
3 eni-33333333333333333 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb
 i-01234567890123456 10.40.2.236 10.20.33.164 80 39812 6 19 IPv4 10.40.2.236
 10.20.33.164 ACCEPT OK
```

Baris berikut adalah lalu lintas permintaan di eni-11111111111111111, antarmuka jaringan yang dikelola peminta untuk transit gateway di subnet subnet-11111111aaaaaaaaa. Oleh karena itu

catatan log alur menampilkan simbol '-' untuk bidang instance-id. Bidang srcaddr menampilkan alamat IP privat antarmuka jaringan transit gateway, dan bidang pkt-srcaddr menampilkan alamat IP sumber klien di VPC A.

```
3 eni-11111111111111111 123456789010 vpc-abcdefab012345678 subnet-11111111aaaaaaaaa -
 10.40.1.175 10.40.2.236 39812 80 6 3 IPv4 10.20.33.164 10.40.2.236 ACCEPT OK
```

Baris berikut adalah lalu lintas respon pada eni-22222222222222222, antarmuka jaringan yang dikelola peminta untuk transit gateway di subnet subnet-22222222bbbbbbbbb. Bidang dstaddr menampilkan alamat IP privat antarmuka jaringan transit gateway, dan bidang pkt-dstaddr menampilkan alamat IP klien di VPC A.

```
3 eni-22222222222222222 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb -
 10.40.2.236 10.40.2.31 80 39812 6 19 IPv4 10.40.2.236 10.20.33.164 ACCEPT OK
```

Nama layanan, jalur lalu lintas, dan arah aliran

Berikut ini adalah contoh bidang untuk catatan log alur kustom.

```
version srcaddr dstaddr srcport dstport protocol start end type packets bytes account-
id vpc-id subnet-id instance-id interface-id region az-id sublocation-type sublocation-
id action tcp-flags pkt-srcaddr pkt-dstaddr pkt-src-aws-service pkt-dst-aws-service
 traffic-path flow-direction log-status
```

Dalam contoh berikut, versinya 5 karena catatan meliputi bidang versi 5. Instans EC2 memanggil layanan Amazon S3. Log alur ditangkap pada antarmuka jaringan untuk instans. Catatan pertama memiliki arah aliran ingress dan catatan kedua memiliki arah aliran egress. Untuk catatan egress, traffic-path-nya 8, menunjukkan bahwa lalu lintas melewati gateway internet. Bidang traffic-path tidak didukung untuk lalu lintas ingress. Saat pkt-srcaddr atau pkt-dstaddr adalah alamat IP publik, nama layanan ditampilkan.

```
5 52.95.128.179 10.0.0.71 80 34210 6 1616729292 1616729349 IPv4 14 15044
 123456789012 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-0c50d5961bcb2d47b
 eni-1235b8ca123456789 ap-southeast-2 apse2-az3 - - ACCEPT 19 52.95.128.179 10.0.0.71
 S3 - - ingress OK
5 10.0.0.71 52.95.128.179 34210 80 6 1616729292 1616729349 IPv4 7 471 123456789012 vpc-
abcdefab012345678 subnet-aaaaaaaa012345678 i-0c50d5961bcb2d47b eni-1235b8ca123456789
 ap-southeast-2 apse2-az3 - - ACCEPT 3 10.0.0.71 52.95.128.179 - S3 8 egress OK
```

Batasan log alur

Untuk menggunakan log alur , Anda perlu memahami batasan-batasan berikut:

- Anda tidak dapat mengaktifkan log alur untuk VPC yang di-peering-kan dengan VPC Anda kecuali VPC peer berada di akun Anda.
- Setelah Anda 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 alamat IPv4 dan lalu lintas dikirim ke alamat IPv4 privat sekunder, log alur menampilkan alamat IPv4 privat utama di bidang `dstaddr`. Untuk menangkap alamat IP tujuan asal, buat log alur dengan bidang `pkt-dstaddr`.
- Jika lalu lintas dikirim ke antarmuka jaringan dan tujuan bukan salah satu alamat IP antarmuka jaringan, log alur menampilkan alamat IPv4 privat utama di bidang `dstaddr`. Untuk menangkap alamat IP tujuan asal, buat log alur dengan bidang `pkt-dstaddr`.
- Jika lalu lintas dikirim dari antarmuka jaringan dan sumber bukan salah satu alamat IP antarmuka jaringan, log alur menampilkan alamat IPv4 privat utama di bidang `srcaddr`. Untuk menangkap alamat IP sumber asal, buat log alur dengan bidang `pkt-srcaddr`.
- Jika lalu lintas dikirim ke atau dikirim dari antarmuka jaringan, bidang `srcaddr` dan `dstaddr` di log alur selalu menampilkan alamat IPv4 privat utama, terlepas dari sumber paket atau tujuan. Untuk menangkap sumber paket atau tujuan, buat log alur dengan bidang `pkt-srcaddr` dan `pkt-dstaddr`.
- Saat antarmuka jaringan Anda terpasang ke Instans berbasis Nitro, interval agregasi selalu 1 menit atau kurang, terlepas dari interval agregasi maksimum yang ditentukan.

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 cermin.
- Lalu lintas ke alamat IP yang dipesan untuk router VPC default.
- Lalu lintas antara antarmuka jaringan titik akhir dan antarmuka jaringan Penyeimbang Beban Jaringan.

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 sumber daya VPC/SubNet, lalu lintas apa pun yang dihasilkan untuk antarmuka jaringan non-ECS juga akan dikirimkan untuk langganan Anda. Nilai untuk bidang ECS adalah '-' untuk lalu lintas IP non-ECS. Misalnya, Anda memiliki subnet (`subnet-000000`) dan Anda membuat langganan log aliran untuk subnet ini dengan bidang ECS (). `fl-00000000` Di`subnet-000000`, Anda meluncurkan instans EC2 (`i-0000000`) yang terhubung ke internet dan secara aktif menghasilkan lalu lintas IP. Anda juga meluncurkan tugas ECS (`ECS-Task-1`) yang sedang berjalan di subnet yang sama. Karena `ECS-Task-1` keduanya `i-0000000` dan menghasilkan lalu lintas IP, langganan log aliran Anda `fl-00000000` akan mengirimkan log lalu lintas untuk kedua entitas. Namun, hanya `ECS-Task-1` akan memiliki metadata ECS aktual untuk bidang ECS yang Anda sertakan dalam LogFormat Anda. Untuk lalu lintas `i-0000000` terkait, bidang ini akan memiliki nilai '-'.
- `ecs-container-id`dan `ecs-second-container-id` dipesan saat layanan VPC Flow Logs menerimanya dari aliran 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 STOPTED 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 `awsvpc` 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

- Mengontrol penggunaan log alur
- Membuat log alur
- Melihat log aliran
- Tandai log aliran
- Menghapus log alur

- Gambaran umum API dan CLI

Mengontrol penggunaan log alur

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.

```
{
  "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”.

Membuat log alur

Anda dapat membuat log alur untuk VPC, subnet, atau antarmuka jaringan. 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 dipublikasikan ke Amazon Data Firehose”

Melihat log aliran

Anda dapat melihat informasi tentang log aliran untuk sumber daya, seperti antarmuka jaringan. Informasi yang ditampilkan termasuk ID log alur, konfigurasi log alur, dan informasi tentang status log alur.

Untuk melihat informasi tentang log aliran

1. Lakukan salah satu hal berikut ini:
   - Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/. Di panel navigasi, pilih Antarmuka Jaringan. Pilih kotak centang untuk antarmuka jaringan.
   - Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Pada panel navigasi, pilih VPC Anda. Pilih kotak centang untuk VPC.
   - Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Di panel navigasi, pilih Pengguna. Pilih kotak centang untuk subnet.
2. Pilih Log Aliran.
3. (Opsional) Untuk melihat data log aliran, buka tujuan log.

Tandai log aliran

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

Untuk mengelola tag untuk log alur

1. Lakukan salah satu hal berikut ini:
   - Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/. Di panel navigasi, pilih Antarmuka Jaringan. Pilih kotak centang untuk antarmuka jaringan.
   - Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Pada panel navigasi, pilih VPC Anda. Pilih kotak centang untuk VPC.
   - Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Di panel navigasi, pilih Pengguna. Pilih kotak centang untuk subnet.
2. Pilih Log Aliran.
3. Pilih Tindakan, Kelola tag.
4. Untuk menambahkan tag baru, pilih Tambahkan tag baru dan masukkan kunci dan nilai. Untuk menghapus sebuah tag, pilih Hapus.
5. Setelah selesai menambahkan atau menghapus tag, pilih Simpan.

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 hal berikut ini:
   - Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/. Di panel navigasi, pilih Antarmuka Jaringan. Pilih kotak centang untuk antarmuka jaringan.
   - Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Pada panel navigasi, pilih VPC Anda. Pilih kotak centang untuk VPC.
   - Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Di panel navigasi, pilih Pengguna. Pilih kotak centang untuk subnet.
2. Pilih Log Aliran.
3. Pilih Tindakan, Hapus log aliran.
4. Saat diminta konfirmasi, ketik **`delete`** lalu pilih Hapus.

Gambaran umum API dan CLI

Anda dapat melakukan tugas yang dijelaskan di halaman ini menggunakan baris perintah atau API. Untuk informasi selengkapnya tentang antarmuka baris perintah dan daftar API yang tersedia, lihat Bekerja dengan Amazon VPC.

Membuat log alur

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)
- CreateFlowLog (API Kueri Amazon EC2)

Jelaskan log aliran

- describe-flow-logs (AWS CLI)

- Get-EC2FlowLog (AWS Tools for Windows PowerShell)
- DescribeFlowLog (API Kueri Amazon EC2)

Tandai log aliran

- buat-tag dan hapus-tag ()AWS CLI
- New-EC2Tagdan Remove-EC2TagAWS Tools for Windows PowerShell
- CreateTagsdan DeleteTags(API Kueri Amazon EC2)

Menghapus log alur

- delete-flow-logs (AWS CLI)
- Remove-EC2FlowLog (AWS Tools for Windows PowerShell)
- DeleteFlowLog (API Kueri Amazon EC2)

Publikasikan log aliran ke CloudWatch Log

Log aliran dapat mempublikasikan data log aliran langsung ke Amazon CloudWatch.

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 penjual berlaku saat Anda mempublikasikan 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

Peran IAM yang terkait dengan log alur Anda harus memiliki izin yang cukup untuk mempublikasikan 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.

```
{
  "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.

```
{
  "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 dijelaskan di atas. Atau, Anda dapat menggunakan prosedur berikut untuk membuat peran baru untuk digunakan dengan log aliran. Anda akan menentukan peran ini saat membuat log alur.

Untuk membuat IAM role untuk log alur

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Kebijakan.
3. Pilih Buat kebijakan.

4. Pada halaman Buat kebijakan, lakukan hal berikut:
   a. PilihJSON.
   b. Ganti isi jendela ini dengan kebijakan izin di awal bagian ini.
   c. Pilih Selanjutnya.
   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.

Izin untuk prinsipal IAM yang menerbitkan log aliran ke Log CloudWatch

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

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

Buat log alur yang diterbitkan ke CloudWatch Log

Anda dapat membuat log alur untuk VPC, subnet, atau antarmuka jaringan. Jika Anda melakukan langkah-langkah ini sebagai pengguna menggunakan peran IAM tertentu, pastikan peran tersebut memiliki izin untuk menggunakan tindakan tersebut`iam:PassRole`. Untuk informasi selengkapnya, lihat Izin untuk prinsipal IAM yang menerbitkan log aliran ke Log CloudWatch .

Prasyarat

- Buat peran IAM, seperti yang dijelaskan dalamthe section called “Peran IAM untuk menerbitkan log alur ke CloudWatch Log”.

Untuk membuat log aliran menggunakan konsol

1. Lakukan salah satu hal berikut ini:
   - Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/. Di panel navigasi, pilih Antarmuka Jaringan. Pilih kotak centang untuk antarmuka jaringan.
   - Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Pada panel navigasi, pilih VPC Anda. Pilih kotak centang untuk VPC.
   - Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Di panel navigasi, pilih Pengguna. Pilih kotak centang untuk subnet.
2. Pilih 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 yang akan dibuat saat Anda membuat log alur ini.
7. Untuk peran IAM, tentukan nama peran yang memiliki izin untuk menerbitkan log ke CloudWatch Log.
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-EC2FlowLogs (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
```

Melihat catatan log alur

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)

- LogEventDapatkan-CWL ()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 bekerja dengan 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 Mencari dan Memfilter Data Log di Panduan CloudWatch Pengguna 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. Konfigurasikan alarm sebagai berikut, lalu pilih Next (Selanjutnya):

    - Untuk Statistik pilih Jumlah. Ini memastikan bahwa Anda menangkap jumlah total titik data untuk periode waktu yang ditentukan.
    - Untuk 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 Selanjutnya.
13. Untuk Pemberitahuan, pilih topik SNS yang ada atau pilih Buat topik baru untuk membuat topik baru. Pilih Selanjutnya.
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.

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 Layanan Penyimpanan Sederhana Amazon.

Untuk informasi selengkapnya tentang pencatatan beberapa akun, lihat Pencatatan Pusat dalam Perpustakaan Solusi 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

- 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
- Melihat catatan log alur
- Catatan log alur proses di Amazon S3

Berkas log alur

VPC Flow Logs mengumpulkan data tentang lalu lintas IP yang menuju dan dari VPC Anda ke dalam catatan log, menggabungkan catatan tersebut ke dalam file log, dan kemudian menerbitkan file log ke bucket Amazon S3 dengan interval 5 menit. Beberapa file dapat dipublikasikan dan setiap file log mungkin berisi beberapa atau semua catatan log aliran untuk lalu lintas IP yang direkam dalam 5 menit sebelumnya.

Dalam Amazon S3, bidang Terakhir diubah untuk berkas log alur menunjukkan tanggal dan waktu di mana file diunggah ke Amazon S3 bucket. Ini lebih lambat dari stempel waktu dalam nama file, dan berbeda dengan jumlah waktu yang dibutuhkan untuk mengunggah file ke bucket Amazon S3.

Format file log

Anda dapat menentukan salah satu format berikut untuk file log. Setiap file dikompresi menjadi satu file Gzip.

- Teks — Teks biasa. Ini adalah format default.
- Parket - Apache Parquet adalah format data kolumnar. Kueri pada data dalam format Parket 10 hingga 100 kali lebih cepat dibandingkan dengan kueri pada data dalam teks biasa. Data dalam format Parket dengan kompresi Gzip membutuhkan ruang penyimpanan 20 persen lebih sedikit daripada teks biasa dengan kompresi Gzip.

> **Note**
>
> Jika data dalam format Parket dengan kompresi Gzip kurang dari 100 KB per periode agregasi, menyimpan data dalam format Parket mungkin memakan lebih banyak ruang daripada teks biasa dengan kompresi Gzip karena persyaratan memori file Parket.

Opsi file 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 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 untuk prinsipal IAM yang menerbitkan log alur ke Amazon S3

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.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource": "*"
    }
  ]
}
```

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",
                "s3:ListBucket"
            ],
            "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 untuk *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 Akun AWS ARN individual. 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.

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 (ACL) untuk mengelola akses ke berkas log yang dibuat oleh log alur. Secara default, pemilik bucket

memiliki izin `FULL_CONTROL` pada setiap file berkas log. Pemilik pengiriman log, jika berbeda dari pemilik bucket, tidak memiliki izin. Akun pengiriman log memiliki izin `READ` dan `WRITE`. Untuk informasi selengkapnya, lihat Ikhtisar Daftar Kontrol Akses (ACL) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

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 VPC Anda.

Untuk membuat log aliran menggunakan konsol

1. Lakukan salah satu hal berikut ini:
   - Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/. Di panel navigasi, pilih Antarmuka Jaringan. Pilih kotak centang untuk antarmuka jaringan.
   - Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Pada panel navigasi, pilih VPC Anda. Pilih kotak centang untuk VPC.
   - Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Di panel navigasi, pilih Pengguna. Pilih kotak centang untuk subnet.
2. Pilih 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.
   - Parket - Apache Parquet adalah format data kolumnar. Kueri pada data dalam format Parket 10 hingga 100 kali lebih cepat dibandingkan dengan kueri pada data dalam teks biasa. Data dalam format Parket 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 menerbitkan ke Amazon S3 menggunakan alat baris perintah

Gunakan salah satu perintah berikut:

- create-flow-logs (AWS CLI)
- New-EC2FlowLogs (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}'
```

Melihat catatan log alur

Anda dapat melihat catatan log alur menggunakan konsol Amazon S3. Setelah Anda membuat log alur, mungkin perlu beberapa menit agar dapat terlihat di konsol.

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, awalan//account_id AWSLogs / vpcflowlogs/ wilayah/tahun/bulan/hari /.*
4. Pilih kotak centang di sebelah nama file, lalu pilih Unduh.

Catatan log alur proses di Amazon S3

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.

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.

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

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 membuat kebijakan, tentukan VPC, antarmuka jaringan, atau subnet yang Anda pantau dengan kunci kondisi. `iam:AssociatedResourceARN`

```
{
  "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.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Dari akun sumber, gunakan prosedur berikut untuk membuat peran.

Untuk membuat peran akun sumber

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Kebijakan.
3. Pilih Buat kebijakan.
4. Pada halaman Buat kebijakan, lakukan hal berikut:
   a. PilihJSON.
   b. Ganti isi jendela ini dengan kebijakan izin di awal bagian ini.
   c. Pilih Selanjutnya.
   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 Selanjutnya.

```
"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.

```
{
  "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.

```
{
  "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. PilihJSON.
    b. Ganti isi jendela ini dengan kebijakan izin di awal bagian ini.
    c. Pilih Selanjutnya.

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 Selanjutnya.

```
"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 dipublikasikan ke Amazon Data Firehose

Anda dapat membuat log alur untuk VPC, subnet, atau antarmuka jaringan.

Prasyarat

- Buat aliran pengiriman Amazon Data Firehose tujuan. Gunakan Direct Put sebagai sumbernya. Untuk informasi selengkapnya, lihat Membuat aliran pengiriman Amazon Data Firehose.
- Jika Anda memublikasikan log alur ke akun lain, buat peran IAM yang diperlukan, seperti yang dijelaskan dalamthe section called “Peran IAM untuk pengiriman lintas akun”.

Untuk membuat log alur yang diterbitkan ke Amazon Data Firehose

1. Lakukan salah satu hal berikut ini:
   - Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/. Di panel navigasi, pilih Antarmuka Jaringan. Pilih kotak centang untuk antarmuka jaringan.
   - Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Pada panel navigasi, pilih VPC Anda. Pilih kotak centang untuk VPC.

- Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Di panel navigasi, pilih Pengguna. Pilih kotak centang untuk subnet.

2. Pilih 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 peran IAM, tentukan peran yang diperlukan (lihatthe section called “Peran IAM untuk pengiriman lintas akun”).
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 alat baris perintah

Gunakan salah satu perintah berikut:

- create-flow-logs (AWS CLI)

- New-EC2FlowLogs (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
```

Catatan log alur proses di Amazon Data Firehose

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 virtual private cloud (VPC) yang merupakan pembicara teratas atau mengidentifikasi alamat IP dengan koneksi TCP yang paling sering ditolak.

Opsi

- Anda dapat merampingkan dan mengotomatiskan integrasi log aliran VPC Anda dengan Athena 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
- Hasilkan 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 hal berikut ini:
    - Buka konsol Amazon VPC. Di panel navigasi, pilih VPC Anda dan kemudian pilih VPC Anda.

- Buka konsol Amazon VPC. Di panel navigasi, pilih Subnet, lalu pilih subnet Anda.
- Buka konsol Amazon EC2. Di panel navigasi, pilih Antarmuka Jaringan, lalu pilih antarmuka jaringan Anda.

2. Pada tab Log Alur, pilih log alur yang menerbitkan ke Amazon S3 dan kemudian pilih Tindakan, Hasilkan Integrasi Athena.
3. Tentukan frekuensi beban partisi. Jika Anda memilih Tidak ada, Anda harus menentukan tanggal mulai dan akhir partisi, menggunakan tanggal yang ada di masa lalu. Jika Anda memilih Harian, Mingguan, atau Bulanan, tanggal mulai dan akhir partisi bersifat opsional. Jika Anda tidak menentukan tanggal mulai dan 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 basis data adalah vpcflowlogsathenadatabase<flow-logs-subscription-id>.
- Athena workgroup. Nama workgroup adalah <flow-log-subscription-id><partition-load-frequency><start-date><end-date>workgroup
- Sebuah tabel Athena dipartisi yang sesuai dengan catatan log alur Anda. Nama tabel adalah <flow-log-subscription-id><partition-load-frequency><start-date><end-date>.
- Satu set Athena bernama kueri. Untuk informasi selengkapnya, lihat Kueri yang ditentukan sebelumnya.
- Fungsi Lambda yang memuat partisi baru ke tabel pada jadwal yang ditentukan (harian, mingguan, atau bulanan).
- IAM role yang memberikan izin untuk menjalankan fungsi Lambda.

Hasilkan 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 template. CloudFormation

```
aws ec2 get-flow-logs-integration-template --cli-input-json file://config.json
```

Berikut ini adalah contoh file `config.json`.

```
{
    "FlowLogId": "fl-12345678901234567",
    "ConfigDeliveryS3DestinationArn": "arn:aws:s3:::my-flow-logs-athena-integration/
templates/",
    "IntegrateServices": {
        "AthenaIntegrations": [
            {
                "IntegrationResultS3DestinationArn": "arn:aws:s3:::my-flow-logs-
analysis/athena-query-results/",
                "PartitionLoadFrequency": "monthly",
                "PartitionStartDate": "2021-01-01T00:00:00",
                "PartitionEndDate": "2021-12-31T00:00:00"
            }
        ]
    }
}
```

Gunakan perintah create-stack berikut untuk membuat tumpukan menggunakan template yang dihasilkan. CloudFormation

```
aws cloudformation create-stack --stack-name my-vpc-flow-logs --template-body file://
my-cloudformation-template.json
```

Menjalankan kueri yang sudah ditentukan sebelumnya

CloudFormation Template yang dihasilkan menyediakan serangkaian kueri standar 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.

- VpcFlowLogsAcceptedLalu Lintas — Koneksi TCP yang diizinkan berdasarkan grup keamanan dan ACL jaringan Anda.
- VpcFlowLogsAdminPortTraffic10 alamat IP teratas dengan lalu lintas terbanyak, seperti yang dicatat oleh aplikasi yang melayani permintaan pada port administratif.
- VpcFlowLogsipv4Traffic — Total byte lalu lintas IPv4 dicatat.
- VpcFlowLogsipv6Traffic — Total byte lalu lintas IPv6 yang direkam.
- VpcFlowLogsRejectedTCPTraffic — Koneksi TCP yang ditolak berdasarkan grup keamanan atau ACL jaringan Anda.
- VpcFlowLogsRejectedLalu lintas — Lalu lintas yang ditolak berdasarkan grup keamanan atau ACL jaringan Anda.
- VpcFlowLogsSshRdpTrafficLalu lintas SSH dan RDP.
- VpcFlowLogsTopPembicara — 50 alamat IP dengan lalu lintas terbanyak yang tercatat.
- VpcFlowLogsTopTalkersPacketLevel — 50 alamat IP tingkat paket dengan lalu lintas terbanyak yang tercatat.
- VpcFlowLogsTopTalkingInstances— ID dari 50 instance dengan lalu lintas terbanyak yang tercatat.
- VpcFlowLogsTopTalkingSubnets— ID dari 50 subnet dengan lalu lintas terbanyak yang tercatat.
- VpcFlowLogsTopTCPTraffic — Semua lalu lintas TCP direkam untuk alamat IP sumber.

- VpcFlowLogsTotalBytesTransferred— 50 pasang alamat IP sumber dan tujuan dengan byte terbanyak yang 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

Masalah

Catatan log alur Anda tidak lengkap, atau tidak lagi diterbitkan.

Penyebab

Mungkin ada masalah saat mengirimkan log aliran ke grup CloudWatch log Log.

Solusi

Dalam konsol Amazon EC2 atau konsol Amazon VPC, pilih tab log alur untuk sumber daya yang relevan. Untuk informasi selengkapnya, lihat Melihat log aliran. Tabel log alur menampilkan kesalahan dalam kolom Status. Atau, gunakan perintah describe-flow-logs, dan periksa nilai yang dikembalikan dalam bidang `DeliverLogsErrorMessage`. Salah satu kesalahan berikut mungkin ditampilkan:

- `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 CloudWatchService Quotas di CloudWatch Panduan 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 konsol Amazon VPC atau Amazon EC2 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.

Kesalahan 'LogDestinationNotFoundPengecualian' atau 'Akses Ditolak untuk' 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.

CloudWatch metrik untuk VPC Anda

Amazon VPC menerbitkan data tentang VPC Anda ke Amazon CloudWatch. Anda dapat mengambil statistik tentang VPC Anda sebagai kumpulan data deret waktu yang diurutkan, yang dikenal sebagai metrik. Anggap metrik sebagai variabel untuk memantau dan data tersebut sebagai nilai variabel tersebut dari waktu ke waktu ke waktu ke waktu ke waktu ke waktu ke waktu ke waktu ke waktu ke waktu ke waktu ke waktu ke waktu ke waktu ke Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

Daftar Isi

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 kuota NAU atau peered NAU untuk VPC Anda, Anda tidak dapat meluncurkan instans EC2 baru atau menyediakan sumber daya baru, seperti Network Load Balancers, endpoint 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 berisi VPC.

Anda dapat menggunakan metrik ini untuk memahami tingkat pertumbuhan VPC Anda, memperkirakan kapan VPC Anda akan mencapai batas ukurannya, atau membuat alarm saat ambang batas ukuran dilintasi.

`AWS/EC2`Namespace mencakup metrik berikut untuk memantau NAU.

Metrik	Deskripsi
`NetworkAddressUsage`	Jumlah NAU per VPC. Kriteria pelaporan • Setiap 24 jam. Dimensi • Nama:`Per-VPC Metrics`, Nilai: ID VPC.
`NetworkAddressUsagePeered`	Jumlah NAU untuk VPC dan semua VPC yang diintip. Kriteria pelaporan

Metrik	Deskripsi
	• Setiap 24 jam. Dimensi • Nama:`Per-VPC Metrics`, Nilai: ID VPC.

`AWS/Usage`Namespace mencakup metrik berikut untuk memantau NAU.

Metrik	Deskripsi
`ResourceCount`	Jumlah NAU per VPC. Kriteria pelaporan • Setiap 24 jam. Dimensi • Nama:`Service`, Nilai:`EC2` • Nama:`Type`, Nilai:`Resource` • Nama:`Resource`, Nilai: ID VPC. • Nama:`Class`, Nilai:`NetworkAddressUsage`
`ResourceCount`	Jumlah NAU untuk VPC dan semua VPC yang diintip. Kriteria pelaporan • Setiap 24 jam. Dimensi • Nama:`Service`, Nilai:`EC2` • Nama:`Type`, Nilai:`Resource`

Metrik	Deskripsi
	• Nama:`Resource`, Nilai: ID VPC. • Nama:`Class`, Nilai:`NetworkAddressUsagePeered`
`ResourceCount`	Tampilan gabungan penggunaan NAU di seluruh VPC. Kriteria pelaporan • Setiap 24 jam. Dimensi • Nama:`Service`, Nilai:`EC2` • Nama:`Type`, Nilai:`Resource` • Nama:`Resource`, Nilai:`VPC` • Nama:`Class`, Nilai:`NetworkAddressUsage`
`ResourceCount`	Tampilan gabungan penggunaan NAU di seluruh VPC yang diintip. Kriteria pelaporan • Setiap 24 jam. Dimensi • Nama:`Service`, Nilai:`EC2` • Nama:`Type`, Nilai:`Resource` • Nama:`Resource`, Nilai:`VPC` • Nama:`Class`, Nilai:`NetworkAddressUsagePeered`

Mengaktifkan pemantauan NAU

Untuk melihat metrik NAU CloudWatch, Anda harus terlebih dahulu mengaktifkan pemantauan pada setiap VPC untuk memantau.

Untuk mengaktifkan pemantauan NAU

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih VPC Anda.
3. Pilih kotak centang untuk VPC.
4. Pilih Tindakan, Edit pengaturan VPC.
5. Lakukan salah satu dari berikut:

    - Untuk mengaktifkan pemantauan, pilih Pengaturan 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 pemantauan menggunakan baris perintah

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

Contoh CloudWatch alarm NAU

Anda dapat menggunakanAWS CLI perintah dan contoh berikut `.json` untuk membuat CloudWatch alarm Amazon dan notifikasi SNS yang melacak pemanfaatan NAU VPC dengan 50.000 NAU sebagai ambang batas. Sampel ini mengharuskan Anda membuat sebuah 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"
}
```

Keamanan di 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 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 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

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 kredensyal 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 sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Amazon VPC atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan

supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Privasi lalu lintas antar jaringan di Amazon VPC

Amazon Virtual Private Cloud menyediakan fitur yang dapat Anda gunakan untuk meningkatkan dan memantau keamanan untuk virtual private cloud (VPC) Anda:

- Grup keamanan: Grup keamanan memungkinkan lalu lintas masuk dan keluar tertentu pada tingkat sumber daya (seperti instans EC2). Saat meluncurkan instance, Anda dapat mengaitkannya dengan satu atau beberapa grup keamanan. Setiap instans di VPC Anda bisa menjadi milik grup keamanan yang berbeda. Jika Anda tidak menentukan grup keamanan saat meluncurkan instance, instans secara otomatis dikaitkan dengan grup keamanan default untuk VPC-nya. Untuk informasi selengkapnya, lihat Grup keamanan.
- Daftar kontrol akses jaringan (ACL): ACL jaringan mengizinkan atau menolak lalu lintas masuk dan keluar tertentu di tingkat subnet. Untuk informasi selengkapnya, lihat Kontrol lalu lintas ke subnet menggunakan ACL 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.
- Mirroring lalu lintas: Anda dapat menyalin lalu lintas jaringan dari antarmuka jaringan elastis dari instans Amazon EC2. Anda kemudian dapat mengirim lalu lintas ke peralatan 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

- 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 kredensyal 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 kredensyal yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center),

autentikasi masuk tunggal perusahaan Anda, dan kredensyal 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 kredensyal Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani permintaan AWS API di 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 Menggunakan autentikasi multi-faktor (MFA) dalam AWS 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 memiliki grup yang bernama IAMAdmins dan memberikan izin ke 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 Kapan harus membuat pengguna IAM (bukan peran) 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. Anda dapat mengambil peran IAM untuk sementara AWS Management Console dengan beralih peran. 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 Menggunakan peran IAM 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 Membuat 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 Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.

- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Sebagai contoh, ketika Anda memanggil 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 Membuat 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 kredensyal sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial

sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan dalam instans Amazon EC2 dalam Panduan Pengguna IAM.

Untuk mempelajari kapan waktunya menggunakan IAM role atau pengguna IAM, lihat Kapan harus membuat IAM role (sebagai ganti pengguna) dalam 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 Membuat kebijakan IAM 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 Memilih 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 (ACL)

Daftar kontrol akses (ACL) mengendalikan prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, lihat Gambaran umum daftar kontrol akses (ACL) dalam Panduan Developer Amazon Simple Storage Service.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang 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 (SCP) — SCP 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 di organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) 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 Organisasi dan SCP, lihat Cara kerja SCP dalam Panduan Pengguna AWS Organizations .
- 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

- Kunci syarat
- kebijakan berbasis sumber daya Amazon VPC
- Otorisasi berdasarkan tanda
- Peran IAM

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan tindakan yang diizinkan atau ditolak. Untuk beberapa tindakan, Anda dapat menentukan sumber daya dan syarat apakah suatu tindakan diizinkan atau ditolak. Amazon VPC men-support tindakan, sumber daya, dan kunci syarat tertentu. Untuk mempelajari semua elemen yang Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan IAM JSON dalam Panduan Pengguna IAM.

Tindakan

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. 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 sebuah kebijakan untuk memberikan izin pelaksanaan operasi terkait.

Amazon VPC berbagi namespace API dengan Amazon EC2. Tindakan kebijakan di Amazon VPC menggunakan prefiks berikut ini sebelum tindakan: `ec2:`. Misalnya, untuk memberikan izin 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 Amazon VPC, lihat Tindakan yang ditentukan oleh Amazon EC2 di Referensi Otorisasi Layanan.

Sumber daya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. 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 VPC di Wilayah tertentu milik akun tertentu, gunakan wildcard (*).

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/*"
```

Beberapa tindakan Amazon VPC, seperti membuat sumber daya, tidak dapat dilakukan pada sumber daya tertentu. Dalam kasus tersebut, Anda harus menggunakan wildcard (*).

```
"Resource": "*"
```

Banyak tindakan API Amazon EC2 yang melibatkan beberapa sumber daya. Untuk menentukan beberapa sumber daya dalam satu pernyataan tunggal, pisahkan ARN dengan koma.

```
"Resource": [
      "resource1",
      "resource2"
]
```

Untuk melihat daftar jenis sumber daya Amazon VPC dan ARNnya, 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 tag yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat Elemen kebijakan IAM: variabel dan tag 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 tindakan Amazon EC2 mendukung kunci syarat `aws:RequestedRegion` dan `ec2:Region`. Untuk informasi selengkapnya, lihat Contoh: Membatasi akses ke Wilayah tertentu.

Amazon VPC menentukan pengaturan kunci syaratnya sendiri dan juga men-support penggunaan beberapa kunci syarat global. Untuk melihat daftar kunci kondisi Amazon VPC, lihat Kunci kondisi untuk Amazon EC2 di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya 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 prinsipal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya 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 Menandai sumber daya selama pembuatan dan Kontrol akses ke sumber daya EC2 menggunakan tag sumber daya di Panduan Pengguna Amazon EC2.

Untuk melihat contoh kebijakan berbasis identitas untuk membatasi akses ke sumber daya berdasarkan tag pada sumber daya tersebut, lihat Meluncurkan instans ke VPC tertentu.

Peran IAM

Peran IAM adalah entitas di dalam Anda Akun AWS yang memiliki izin khusus.

Gunakan kredensial sementara

Anda dapat menggunakan kredensial sementara untuk masuk dengan gabungan, menjalankan IAM role, atau menjalankan peran lintas akun. Anda memperoleh kredensyal keamanan sementara dengan memanggil operasi AWS STS API seperti AssumeRoleatau GetFederation Token.

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 tertaut layanan.

Transit Gateway men-support peran yang tertaut dengan layanan.

Peran layanan

Fitur ini memungkinkan layanan untuk menerima peran layanan atas nama Anda. Peran ini mengizinkan layanan untuk mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Peran layanan muncul di akun IAM Anda dan dimiliki oleh akun tersebut. Ini berarti administrator IAM dapat mengubah izin untuk peran ini. Namun, melakukan hal itu dapat merusak fungsionalitas layanan.

Amazon VPC men-support peran layanan untuk log alur. Saat 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

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 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 Mengonfigurasi akses API yang dilindungi MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan dalam 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.

```
{
    "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 VPC, 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.

```
{
   "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 tag`Purpose=Test`. Kebijakan ini juga menetapkan bahwa peran hanya dapat menghapus gateway internet yang memiliki tag. `Purpose=Test` Peran tidak dapat bekerja dengan tabel rute atau gateway internet yang tidak memiliki tag ini.

```
{
    "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 untuk mengelola aturan masuk dan keluar untuk grup keamanan apa pun dengan tag. `Stack=test` Pernyataan kedua membutuhkan peran untuk menandai grup keamanan apa pun yang mereka buat dengan tag`Stack=Test`. Pernyataan ketiga memungkinkan peran untuk membuat tag saat membuat

grup keamanan. Pernyataan keempat memungkinkan peran untuk melihat 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.

```
{
    "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"
                },
                "ForAllValues: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.

```
{
  "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.

```
{
   "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 AMI yang memiliki tag ""`department=dev`.

```
{
   "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/*"
         ]
      }
   ]
}
```

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
- Layanan titik akhir VPC dan titik akhir VPC
- Kebijakan titik akhir VPC
- VPC mengintip
- AWS Wavelength

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 (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah Amazon VPC men-support fitur-fitur ini, lihat Bagaimana cara Amazon VPC bekerja sama dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya 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 penggunaan kebijakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya dalam 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, pemutakhiran 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 AWS kebijakan yang dikelola dalam Panduan Pengguna IAM.

AWS kebijakan terkelola: AmazonVPC FullAccess

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 AmazonVPC FullAccess di Referensi Kebijakan Terkelola.AWS

AWS kebijakan terkelola: Akses AmazonVPC ReadOnly

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 ReadOnlyAkses AmazonVPC di Referensi Kebijakan Terkelola.AWS

AWS kebijakan terkelola: Operasi AmazonVPC CrossAccount NetworkInterface

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 CrossAccountNetworkInterfaceOperasi AmazonVPC di Referensi Kebijakan Terkelola.AWS

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 “AmazonVPC FullAccess” — Pembaruan ke kebijakan yang sudah ada	Menambahkan GetSecurityGroupsForVpc tindakan, yang memungkinkan Anda mendapatkan grup keamanan yang dapat digunakan di VPC Anda.	Februari 8, 2024
the section called “Akses AmazonVPC ReadOnly” – 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 “Operasi AmazonVPC CrossAccount NetworkInterface” – Pembaruan ke kebijakan yang ada	Ditambahkan AssignIpv6Addresses dan UnassignIpv6Addresses tindakan, yang memungkinkan Anda untuk mengelola alamat IPv6 yang	25 September 2023

Perubahan	Deskripsi	Tanggal
	terkait dengan antarmuka jaringan.	
the section called “Akses AmazonVPC ReadOnly” – Pembaruan ke kebijakan yang ada	Menambahkan DescribeSecurityGroupRules tindakan, yang memungkinkan Anda untuk melihat aturan grup keamanan.	2 Agustus 2021
the section called “AmazonVPC FullAccess” – 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 “AmazonVPC FullAccess” – Pembaruan ke kebijakan yang ada	Tindakan tambahan untuk gateway operator, kumpulan IPv6, gateway lokal, dan tabel rute gateway lokal.	23 Juni 2021
the section called “Akses AmazonVPC ReadOnly” – Pembaruan ke kebijakan yang ada	Tindakan tambahan untuk gateway operator, kumpulan IPv6, 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 VPC yang terpisah untuk melakukan isolasi terhadap infrastruktur berdasarkan beban kerja atau entitas organisasi.

subnet adalah serangkaian alamat IP di VPC. Saat Anda meluncurkan instans, Anda meluncurkan instans tersebut ke dalam subnet dalam VPC Anda. Gunakan subnet untuk melakukan isolasi terhadap jenjang-jenjang aplikasi Anda (misalnya web, aplikasi, dan basis data) dalam satu VPC. Gunakan subnet privat untuk instans Anda jika instan tersebut tidak dapat diakses secara langsung dari internet.

Anda dapat menggunakan AWS PrivateLinkuntuk 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 instans EC2:

- Gunakan grup keamanan sebagai mekanisme utama untuk mengontrol akses jaringan ke VPC Anda. Bila perlu, gunakan ACL jaringan untuk menyediakan kontrol jaringan butir kasar tanpa kewarganegaraan. Grup keamanan lebih fleksibel daripada ACL jaringan, karena kemampuan mereka untuk melakukan penyaringan paket stateful dan membuat aturan yang merujuk pada kelompok keamanan lainnya. ACL jaringan dapat efektif sebagai kontrol sekunder (misalnya, untuk

menolak subset lalu lintas tertentu) atau sebagai rel penjaga subnet tingkat tinggi. Juga, karena ACL jaringan berlaku untuk seluruh subnet, mereka dapat digunakan seolah-olah defense-in-depth instance pernah diluncurkan tanpa grup keamanan yang benar.

- Gunakan subnet privat untuk instans Anda jika instan tersebut tidak dapat diakses secara langsung dari internet. Gunakan host bastion atau gateway NAT untuk akses internet dari instance di subnet pribadi.
- Konfigurasikan tabel rute subnet dengan rute jaringan minimum untuk mendukung persyaratan konektivitas Anda.
- Pertimbangkan untuk menggunakan grup keamanan tambahan atau antarmuka jaringan untuk mengontrol dan meng-audit lalu lintas pengelolaan instans Amazon EC2 secara terpisah dari lalu lintas aplikasi reguler. Oleh karena itu, Anda dapat menerapkan kebijakan IAM khusus untuk kontrol perubahan, sehingga lebih mudah untuk mengaudit perubahan 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 VPC Anda. Untuk informasi selengkapnya, lihat Opsi Konektivitas Network-to-Amazon VPC.
- Gunakan Log Aliran VPC untuk memantau lalu lintas yang menjangkau instans Anda.
- Gunakan AWS Security Hub untuk memeriksa aksesibilitas jaringan yang tidak disengaja pada instans Anda.
- Gunakan AWS Network Firewalluntuk melindungi subnet di VPC Anda dari ancaman jaringan umum.

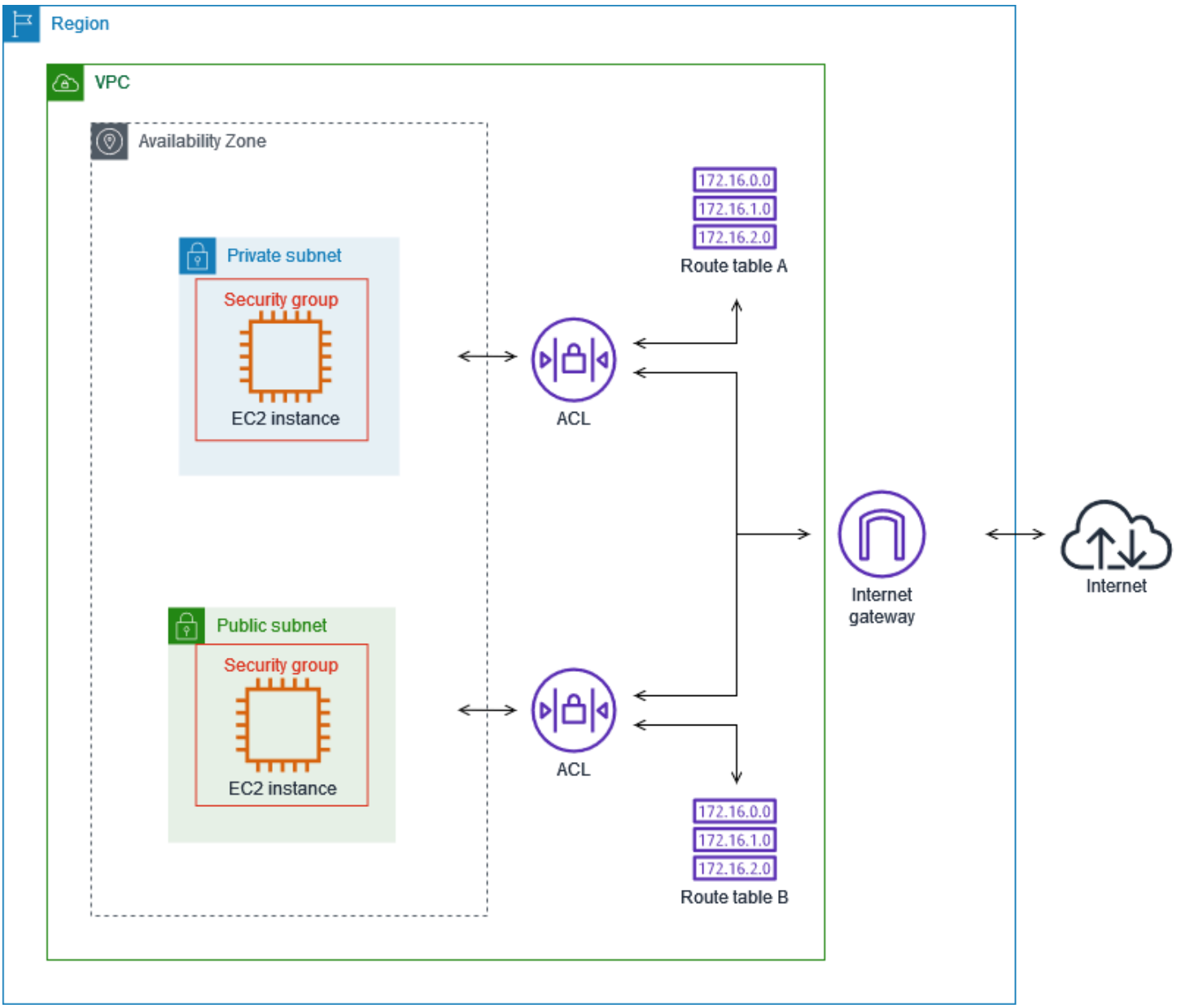
Membandingkan grup keamanan dan ACL jaringan

Tabel berikut merangkum dasar perbedaan antara grup keamanan dan ACL jaringan.

Grup keamanan	ACL jaringan
Beroperasi pada tingkat instans	Beroperasi pada tingkat subnet
Berlaku untuk sebuah instance hanya jika dikaitkan dengan instance	Berlaku untuk semua instance yang digunakan di subnet terkait (menyediakan lapisan

Grup keamanan	ACL jaringan
	pertahanan tambahan jika aturan grup keamanan terlalu permisif)
Mendukung hanya mengizinkan aturan	Mendukung mengizinkan aturan dan menolak aturan
Mengevaluasi semua aturan sebelum memutuskan apakah akan mengizinkan lalu lintas	Mengevaluasi aturan secara berurutan, dimulai dengan aturan bernomor terendah, ketika memutuskan apakah akan mengizinkan lalu lintas
Stateful: Lalu lintas kembali diperbolehkan, terlepas dari aturannya	Stateless: Lalu lintas pengembalian harus secara eksplisit diizinkan oleh aturan

Diagram berikut menggambarkan lapisan keamanan yang disediakan oleh grup keamanan dan ACL jaringan. Sebagai contoh, lalu lintas dari gateway internet dirutekan ke subnet yang sesuai menggunakan rute dalam tabel perutean. Aturan ACL jaringan yang terkait dengan kontrol subnet yang lalu lintas diperbolehkan untuk subnet. Aturan grup keamanan yang terkait dengan kontrol instans yang lalu lintasnya diizinkan untuk instans tersebut.



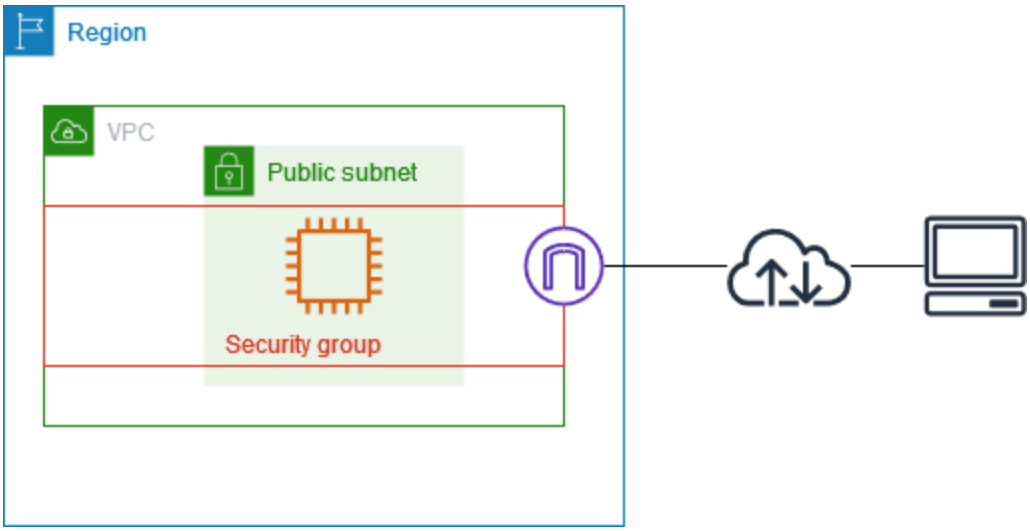
Anda dapat mengamankan instans Anda hanya menggunakan grup keamanan. Namun, Anda dapat menambahkan ACL jaringan sebagai lapisan pertahanan tambahan. Untuk informasi selengkapnya, lihat Contoh: Kontrol akses ke instans dalam subnet.

Kontrol lalu lintas ke 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 instans EC2, grup ini mengontrol lalu lintas masuk dan keluar untuk instans 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 instance EC2. Grup keamanan ditugaskan ke instance. Grup keamanan bertindak sebagai firewall virtual. Satu-satunya lalu lintas yang mencapai instance adalah lalu lintas yang diizinkan oleh aturan grup keamanan. Misalnya, jika grup keamanan berisi aturan yang 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

Harga

Tidak ada biaya tambahan untuk menggunakan grup keamanan.

Dasar-dasar grup keamanan

- Anda dapat menetapkan grup keamanan hanya untuk sumber daya yang dibuat di VPC yang sama dengan grup keamanan. Anda dapat menetapkan beberapa grup keamanan ke 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 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)
  - Metadata instans Amazon EC2
  - Titik akhir metadata tugas Amazon ECS
  - Aktivasi lisensi untuk instance Windows
  - Layanan Amazon Time Sync
  - Alamat IP yang dicadangkan 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

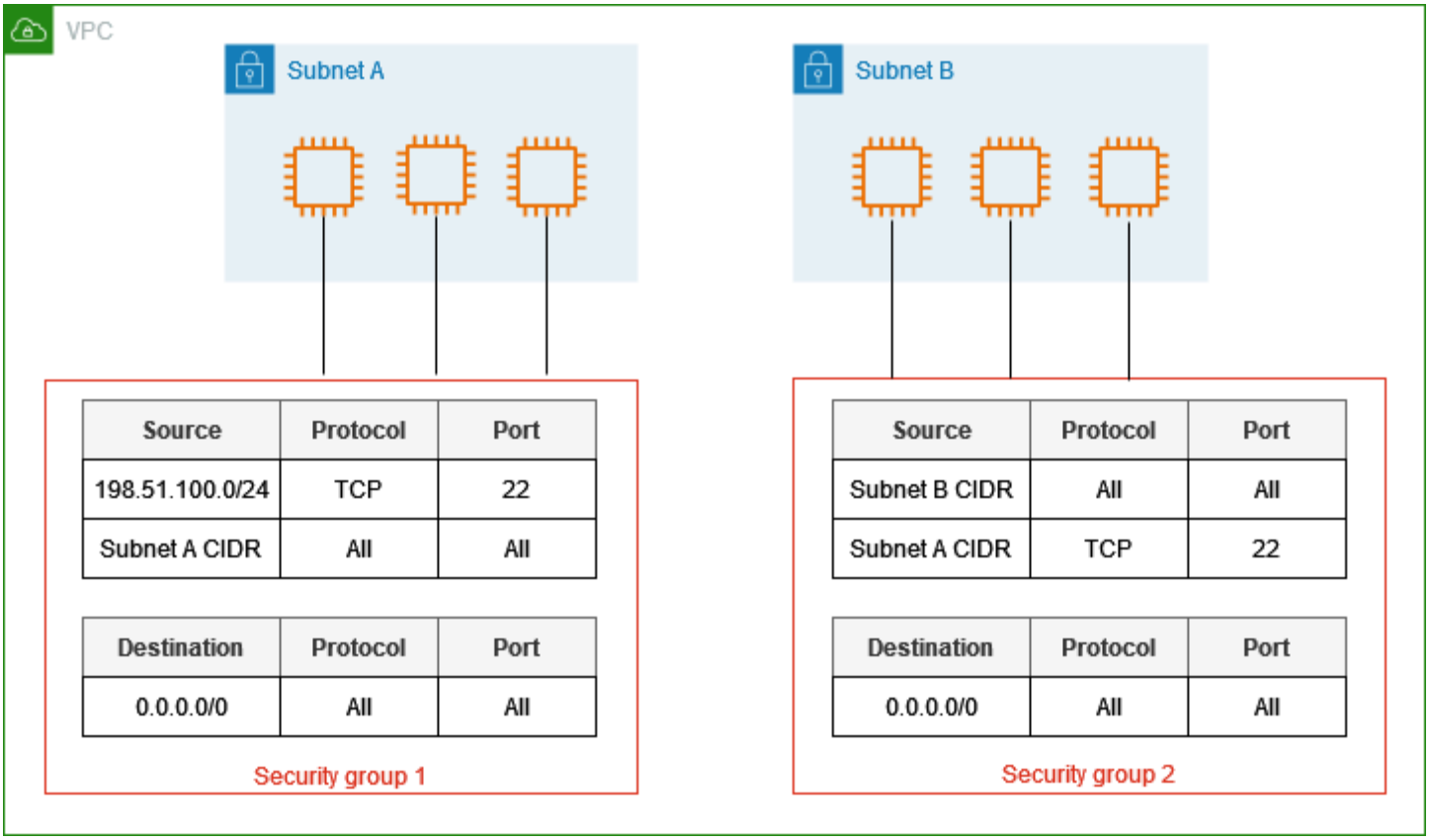
- Otorisasi hanya prinsipal IAM tertentu untuk membuat dan memodifikasi grup keamanan.

- 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 instans EC2 Anda, otorisasi hanya rentang alamat IP tertentu. Jika Anda menentukan 0.0.0.0/0 (IPv4) dan: :/ (IPv6), ini memungkinkan siapa pun 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 ACL jaringan dengan aturan yang mirip dengan grup keamanan Anda, untuk menambahkan lapisan keamanan tambahan ke VPC Anda. Untuk informasi lebih lanjut tentang perbedaan antara grup keamanan dan ACL jaringan, lihat Membandingkan grup keamanan dan ACL jaringan.

Contoh grup keamanan

Diagram berikut menunjukkan VPC dengan dua 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-aturan tersebut juga mengontrol lalu lintas ke luar yang diperbolehkan untuk meninggalkannya.

Anda dapat menambahkan atau menghapus aturan untuk sebuah grup keamanan (juga disebut sebagai memberikan otorisasi atau mencabut akses masuk atau keluar). Suatu aturan berlaku baik untuk lalu lintas masuk (ingress) atau lalu lintas keluar (egress). Anda dapat memberikan akses ke sumber atau tujuan tertentu.

Daftar Isi

- Bekerja dengan aturan kelompok keamanan
- Contoh aturan
- Memecahkan masalah jangkauan

Dasar-dasar 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. Dampak dari beberapa perubahan aturan dapat bergantung pada cara pelacakan lalu lintas yang digunakan. Untuk informasi selengkapnya, lihat Pelacakan koneksi di Panduan Pengguna Amazon EC2.
- Saat Anda membuat aturan grup keamanan, AWS tetapkan 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 Resolverdi 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

- Protocol: Protokol yang akan diizinkan. Protokol yang paling umum adalah 6 (TCP), 17 (UDP), dan 1 (ICMP).

- Port range: Untuk TCP, UDP, atau protokol kustom, ada rentang port yang diizinkan. Anda dapat menentukan satu nomor port (misalnya, 22), atau rentang nomor port (misalnya, `7000-8000`).
- Tipe dan kode ICMP: Untuk ICMP, jenis dan kode ICMP. Sebagai contoh, gunakan tipe 8 untuk ICMP Echo Request atau tipe 128 untuk ICMPv6 Echo Request.
- Source or destination: Sumber (aturan ke dalam) atau tujuan (aturan ke luar) untuk lalu lintas yang akan diizinkan. Tentukan satu dari yang berikut ini:
  - Satu alamat IPv4. Anda harus menggunakan panjang awalan `/32`. Sebagai contoh, `203.0.113.1/32`.
  - Satu alamat IPv6. Anda harus menggunakan panjang awalan `/128`. Sebagai contoh, `2001:db8:1234:1a00::123/128`.
  - Rentang alamat IPv4, dalam notasi blok CIDR. Sebagai contoh, `203.0.113.0/24`.
  - Rentang alamat IPv6, dalam notasi blok CIDR. Sebagai contoh, `2001:db8:1234:1a00::/64`.
  - ID daftar awalan. Sebagai contoh, `pl-1234abc1234abc123`. Untuk informasi selengkapnya, lihat the section called “Daftar prefiks terkelola”.
  - ID grup keamanan. Misalnya, `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 ._-:/()#,@[]+=;{}!$*.

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
sg-0abcdef1234567890	TCP	22

Saat mereferensikan grup keamanan dalam aturan grup keamanan, perhatikan hal berikut:

- Kedua grup keamanan harus memiliki VPC yang sama atau VPC peered.
- Tidak ada aturan dari grup keamanan yang direferensikan ditambahkan ke grup keamanan yang mereferensikannya.
- Untuk aturan masuk, instans EC2 yang terkait dengan grup keamanan dapat menerima lalu lintas masuk dari alamat IP pribadi instans EC2 yang terkait dengan grup keamanan yang direferensikan.
- Untuk aturan keluar, instans EC2 yang terkait dengan grup keamanan dapat mengirim lalu lintas keluar ke alamat IP pribadi instans EC2 yang terkait dengan grup keamanan yang direferensikan.

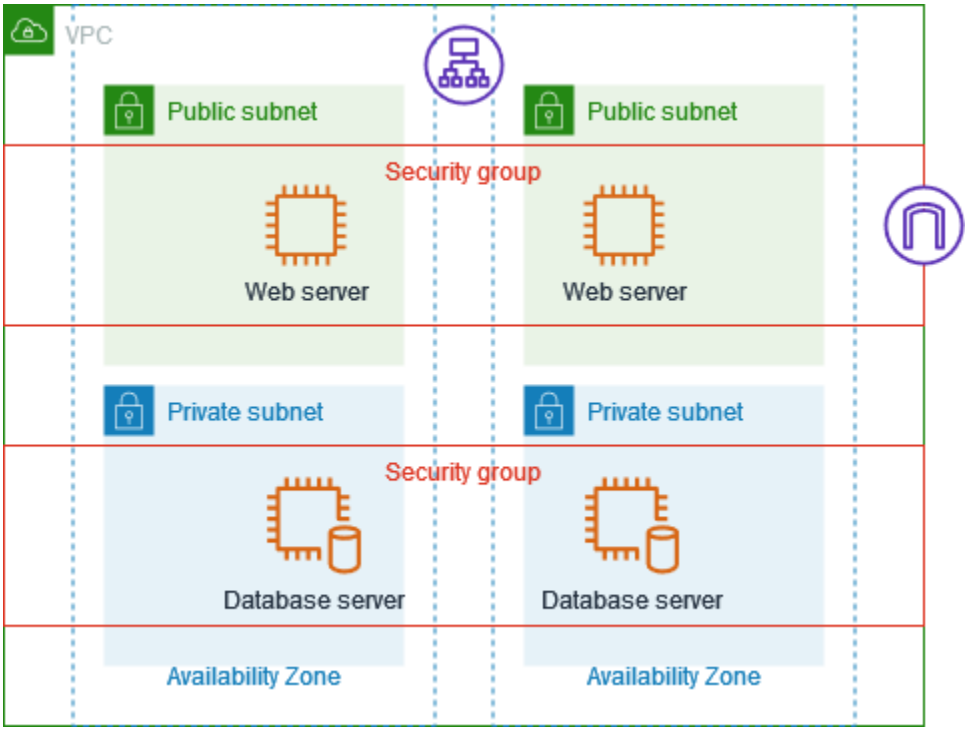
Batasan

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.

Jika grup keamanan di VPC bersama dihapus, atau jika 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. Untuk informasi selengkapnya, lihat Bekerja dengan aturan grup keamanan basi di Panduan Peering VPC Amazon.

Bekerja dengan aturan kelompok keamanan

Tugas-tugas berikut menunjukkan cara bekerja dengan aturan grup keamanan.

Izin yang diperlukan

- Mengelola aturan grup keamanan

Tugas

- Menambahkan aturan ke grup keamanan
- Memperbarui aturan-aturan grup keamanan
- Menandai aturan grup keamanan
- Menghapus aturan grup keamanan

Menambahkan aturan ke grup keamanan

Saat Anda menambahkan aturan ke grup keamanan, aturan baru secara otomatis diterapkan ke sumber daya apa pun yang terkait dengan grup keamanan.

Jika Anda memiliki koneksi peering VPC, Anda dapat merujuk grup keamanan dari VPC peer sebagai sumber atau tujuan dalam aturan grup keamanan Anda. Untuk informasi selengkapnya, lihat Memperbarui grup keamanan Anda untuk merujuk grup keamanan VPC peer dalam Panduan Peering Amazon VPC.

Untuk informasi tentang izin yang diperlukan untuk mengelola aturan grup keamanan, lihat Mengelola aturan grup keamanan.

> **Warning**
>
> Jika Anda memilih di mana-mana-IPv4, Anda mengizinkan lalu lintas dari semua alamat IPv4. Jika Anda memilih di mana-mana-IPv6, Anda mengizinkan lalu lintas dari semua alamat IPv6. Saat Anda menambahkan aturan untuk port 22 (SSH) atau 3389 (RDP), otorisasi hanya rentang alamat IP tertentu untuk mengakses instans Anda.

Untuk menambahkan aturan menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Grup keamanan.
3. Memilih grup keamanan.
4. Pilih Tindakan, Edit aturan masuk atau Tindakan, Edit aturan keluar.
5. Untuk setiap aturan, pilih Tambahkan aturan dan lakukan hal berikut.

   a. Untuk Jenis, pilih jenis protokol yang diperbolehkan.

      - Untuk TCP atau UDP, Anda harus memasukkan rentang port yang diperbolehkan.
      - 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 dikonfigurasi secara otomatis.

   b. Untuk tipe Sumber (aturan masuk) atau Jenis tujuan (aturan keluar), lakukan salah satu hal berikut untuk mengizinkan lalu lintas:

      - Pilih Kustom dan kemudian masukkan alamat IP dalam notasi CIDR, blok CIDR, grup keamanan lainnya, atau daftar awalan.
      - Pilih Anywhere-IPv4 untuk mengizinkan lalu lintas dari alamat IPv4 apa pun (aturan masuk) atau untuk mengizinkan lalu lintas mencapai semua alamat IPv4 (aturan keluar). Ini secara otomatis menambahkan aturan untuk blok CIDR IPv4 0.0.0.0/0.
      - Pilih Anywhere-IPv6 untuk mengizinkan lalu lintas dari alamat IPv6 apa pun (aturan masuk) atau untuk mengizinkan lalu lintas mencapai semua alamat IPv6 (aturan keluar). Ini secara otomatis menambahkan aturan untuk blok CIDR: :/0 IPv6.
      - Pilih My IP untuk mengizinkan lalu lintas hanya dari (aturan masuk) atua ke (aturan keluar) alamat IPv4 publik komputer lokal Anda.

   c. (Opsional) Untuk Deskripsi, sebutkan deskripsi singkat untuk aturan.

6. Pilih Simpan aturan.

Untuk menambahkan aturan ke grup keamanan menggunakan AWS CLI

Gunakan perintah authorize-security-group-ingress dan authorize-security-group-egress.

Memperbarui aturan-aturan grup keamanan

Saat Anda memperbarui aturan, aturan yang diperbarui secara otomatis diterapkan ke sumber daya apa pun yang terkait dengan grup keamanan.

Untuk informasi tentang izin yang diperlukan untuk mengelola aturan grup keamanan, lihat Mengelola aturan grup keamanan.

Untuk memperbarui aturan menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Grup keamanan.
3. Memilih grup keamanan.
4. Pilih Tindakan, Edit aturan masuk atau Tindakan, Edit aturan keluar.
5. Perbarui aturan seperti yang diperlukan.
6. Pilih Simpan aturan.

Untuk memperbarui aturan grup keamanan menggunakan AWS CLI

Gunakan perintah modify-security-group-rules, update-security-group-rule-descriptions-ingress, dan update-security-group-rule-descriptions-egress.

Menandai aturan grup keamanan

Tambahkan tag ke sumber daya Anda untuk membantu mengatur dan mengidentifikasi sumber daya tersebut, misalnya berdasarkan tujuan, pemilik, atau lingkungan. Anda dapat menambahkan tag ke aturan grup keamanan. Kunci tag harus unik untuk masing-masing aturan grup keamanan. Jika Anda menambahkan tag dengan kunci yang sudah terkait dengan grup target, maka nilai tag tersebut akan diperbarui.

Untuk menandai aturan menggunakan konsol

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

2. Pada panel navigasi, pilih Grup keamanan.
3. Pilih grup keamanan.
4. Pada tab Inbound rules (Aturan ke dalam) atau Outbound rules (Aturan ke luar), pilih kotak centang untuk aturan dan kemudian pilih Manage tandas (Kelola tanda).
5. Halaman Kelola tanda akan menampilkan tanda yang ditetapkan ke aturan tersebut. Untuk menambahkan tanda, pilih Add tanda (Tambahkan tanda) dan masukkan kunci dan nilai tanda. Untuk menghapus tanda, pilih Remove (Hapus) yang ada di samping tanda yang ingin Anda hapus.
6. Pilih Save changes (Simpan perubahan).

Untuk menandai aturan menggunakan AWS CLI

Gunakan perintah create-tags.

Menghapus aturan grup keamanan

Saat Anda menghapus sebuah aturan dari sebuah grup keamanan, perubahan secara otomatis diterapkan pada setiap instans yang terkait dengan grup keamanan.

Untuk menghapus grup keamanan menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Grup keamanan.
3. Memilih grup keamanan.
4. Pilih Tindakan, lalu pilih Edit aturan masuk untuk menghapus aturan masuk atau Edit aturan keluar untuk menghapus aturan keluar.
5. Pilih tombol Hapus di sebelah aturan yang akan dihapus.
6. Pilih Simpan aturan. Atau, pilih Pratinjau perubahan, tinjau perubahan Anda, dan pilih Konfirmasi.

Untuk menghapus aturan grup keamanan menggunakan AWS CLI

Gunakan perintah revoke-security-group-ingress dan revoke-security-group-egress.

Contoh aturan

Server web

Berikut ini adalah contoh aturan untuk grup keamanan untuk server web Anda. Server web dapat menerima lalu lintas HTTP dan HTTPS dari semua alamat IPv4 dan IPv6 dan mengirim lalu lintas SQL atau MySQL ke server database Anda.

> **Warning**
>
> Ketika Anda menambahkan aturan untuk port 22 (SSH) atau 3389 (RDP) sehingga Anda dapat mengakses instans EC2 Anda, kami sarankan Anda hanya mengotorisasi rentang alamat IP tertentu. Jika Anda menentukan 0.0.0.0/0 (IPv4) dan: :/ (IPv6), ini memungkinkan siapa pun untuk mengakses instance Anda dari alamat IP apa pun menggunakan protokol yang ditentukan.

Jalur masuk

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
Rentang alamat IPv4 publik dari jaringan Anda	TCP	22	(Opsional) Memungkinkan akses SSH masuk dari alamat IP IPv4 di jaringan Anda

Sumber	Protokol	Rentang Port	Deskripsi
Rentang alamat IPv6 jaringan Anda	TCP	22	(Opsional) Memungkinkan akses SSH masuk dari alamat IP IPv6 di jaringan Anda
Rentang alamat IPv4 publik dari jaringan Anda	TCP	3389	(Opsional) Memungkinkan akses RDP masuk dari alamat IP IPv4 di jaringan Anda
Rentang alamat IPv6 jaringan Anda	TCP	3389	(Opsional) Memungkinkan akses RDP masuk dari alamat IP IPv6 di jaringan Anda
ID grup keamanan ini	Semua	Semua	(Opsional) Memungkinkan lalu lintas masuk dari server lain yang terkait dengan grup keamanan ini

Jalur keluar

Tujuan	Protokol	Rentang Port	Deskripsi
ID grup keamanan untuk instance yang menjalankan Microsoft SQL Server	TCP	1433	Memungkinkan akses Microsoft SQL Server keluar
ID grup keamanan untuk instance yang menjalankan MySQL	TCP	3306	Memungkinkan akses MySQL keluar

Server basis data

Server database memerlukan aturan yang memungkinkan protokol spesifik masuk, seperti MySQL atau Microsoft SQL Server. Sebagai contoh, lihat Aturan server database di Panduan Pengguna Amazon EC2. Untuk informasi selengkapnya tentang grup keamanan untuk instans DB Amazon RDS, lihat Mengendalikan akses dengan grup keamanan di Panduan Pengguna Amazon RDS.

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 grup keamanan yang hilang atau salah konfigurasi.

Untuk informasi selengkapnya, lihat Panduan Reachability Analyzer.

Grup keamanan default untuk VPC Anda

VPC default Anda dan VPC apa pun 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 instans EC2, 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 default untuk grup keamanan default.

Jalur masuk

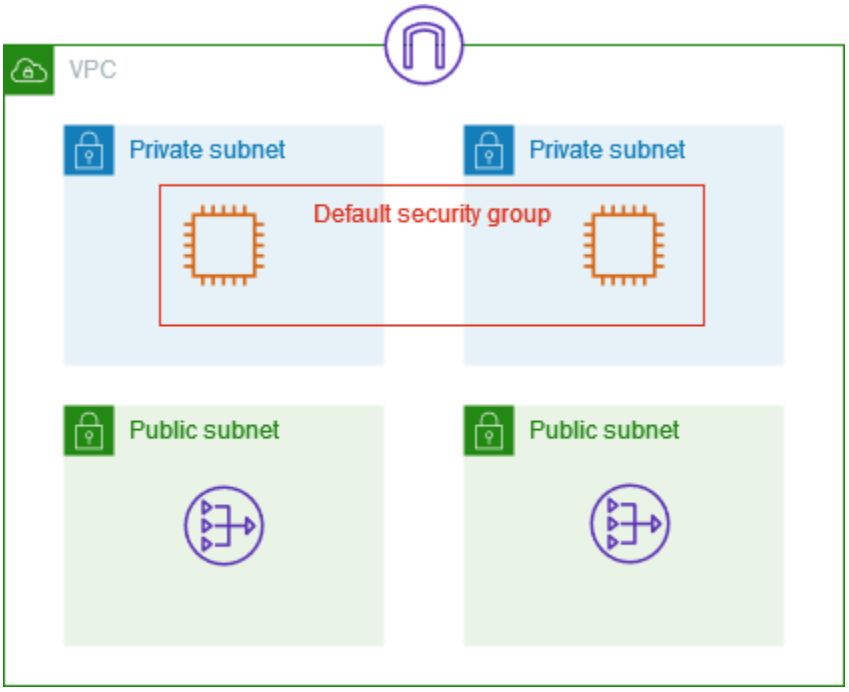
Sumber	Protokol	Rentang Port	Deskripsi
sg-1234567890abcdef0	Semua	Semua	Mengizinkan lalu lintas jalur masuk dari semua sumber daya yang ditetapkan untuk grup keamanan ini. Sumbernya adalah ID dari grup keamanan ini.

Jalur keluar

Tujuan	Protokol	Rentang Port	Deskripsi
0.0.0.0/0	Semua	Semua	Mengizinkan semua lalu lintas IPv4 ke luar.
::/0	Semua	Semua	Mengizinkan semua lalu lintas IPv6 ke luar. Aturan ini ditambahkan hanya jika VPC Anda memiliki blok CIDR IPv6 yang dikaitkan.

Contoh

Diagram berikut menunjukkan VPC dengan grup keamanan default, gateway internet, dan gateway NAT. Keamanan default hanya berisi aturan defaultnya, dan dikaitkan dengan dua instans EC2 yang berjalan di VPC. Dalam skenario ini, setiap instance dapat menerima lalu lintas masuk dari instance lain 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.



Cara menggunakan grup keamanan

Tugas-tugas berikut menunjukkan cara bekerja dengan grup keamanan.

Tugas

- Membuat grup keamanan
- Menampilkan grup keamanan Anda
- Menandai grup keamanan Anda
- Menghapus grup keamanan
- Kelola grup keamanan menggunakan Firewall Manager

Izin yang diperlukan

Sebelum memulai, pastikan Anda memiliki izin yang diperlukan.

- Mengelola grup keamanan
- Mengelola aturan grup keamanan

Aturan grup keamanan mengontrol lalu lintas masuk yang diizinkan untuk mencapai sumber daya yang terkait dengan grup keamanan. Untuk informasi selengkapnya tentang aturan grup keamanan, lihatAturan-aturan grup keamanan.

Membuat grup keamanan

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.

Untuk membuat grup keamanan menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Grup keamanan.
3. Pilih Buat grup keamanan.
4. Masukkan nama dan deskripsi untuk grup keamanan tersebut. Anda tidak dapat mengubah nama dan deskripsi grup keamanan setelah dibuat.
5. Dari VPC, pilih VPC. Grup keamanan hanya dapat digunakan di VPC yang dibuatnya.
6. Anda dapat menambahkan aturan-aturan grup keamanan sekarang, atau Anda dapat menambahkannya nanti. Untuk informasi selengkapnya, lihat Menambahkan aturan ke grup keamanan.
7. Anda dapat menambahkan tanda sekarang, atau Anda dapat menambahkannya nanti. Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.
8. Pilih Create security group (Buat grup keamanan).

Setelah membuat grup keamanan, Anda mungkin ingin melakukan salah satu hal berikut:

- Tetapkan grup keamanan ke instans EC2 saat Anda meluncurkan instans atau mengubah grup keamanan yang saat ini ditetapkan ke instans. Untuk informasi selengkapnya, lihat Meluncurkan instans atau Mengubah grup keamanan di Panduan Pengguna Amazon EC2.
- Tambahkan aturan grup keamanan. Aturan grup keamanan mengontrol lalu lintas masuk yang diizinkan untuk mencapai sumber daya yang terkait dengan grup keamanan. Untuk informasi selengkapnya tentang aturan grup keamanan, lihatBekerja dengan aturan kelompok keamanan.

Untuk membuat grup keamanan menggunakan AWS CLI

Gunakan perintah create-security-group.

Menampilkan grup keamanan Anda

Anda dapat melihat informasi tentang grup keamanan Anda sebagai berikut.

Untuk memperbarui grup keamanan menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Grup keamanan.
3. Grup keamanan Anda terdaftar. Untuk melihat detail untuk suatu grup keamanan tertentu, termasuk aturan masuk dan keluar, pilih grup keamanan tersebut. Untuk informasi selengkapnya tentang memperbarui aturan grup keamanan, lihatMemperbarui aturan-aturan grup keamanan.

Untuk melihat semua grup keamanan Anda di seluruh Wilayah

Buka konsol Amazon EC2 Global View di https://console.aws.amazon.com/ec2globalview/home. Untuk informasi selengkapnya, lihat Daftar dan filter sumber daya menggunakan Tampilan Global Amazon EC2 di Panduan Pengguna Amazon EC2.

Untuk melihat grup keamanan Anda menggunakan AWS CLI

Gunakan perintah describe-security-groups dan describe-security-group-rules.

Menandai grup keamanan Anda

Tambahkan tag ke sumber daya Anda untuk membantu mengatur dan mengidentifikasi sumber daya tersebut, misalnya berdasarkan tujuan, pemilik, atau lingkungan. Anda dapat menambahkan tag ke grup keamanan Anda. Kunci tag harus unik untuk setiap grup keamanan. Jika Anda menambahkan tag dengan kunci yang sudah terkait dengan aturan, maka nilai tag tersebut akan diperbarui.

Untuk menandai grup keamanan menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Grup keamanan.
3. Pilih kotak centang untuk grup keamanan.
4. Pilih Tindakan, Kelola tag. Halaman Kelola tag menampilkan tag yang ditetapkan ke grup keamanan.
5. Untuk menambahkan tag, pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag. Untuk menghapus tanda, pilih Remove (Hapus) yang ada di samping tanda yang akan dihapus.
6. Pilih Simpan perubahan.

Untuk menandai grup keamanan menggunakan AWS CLI

Gunakan perintah create-tags.

Menghapus grup keamanan

Anda dapat menghapus grup keamanan hanya jika tidak terkait dengan sumber daya apa pun. Anda tidak dapat menghapus grup keamanan default.

Jika menggunakan konsol tersebut, Anda dapat menghapus lebih dari satu grup keamanan sekaligus. Jika menggunakan baris perintah atau API, Anda hanya dapat menghapus satu grup keamanan dalam satu waktu.

Untuk menghapus grup keamanan menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Grup keamanan.
3. Pilih grup keamanan lalu pilih Tindakan, Hapus Grup Keamanan.
4. Saat diminta konfirmasi, pilih Hapus.

Untuk menghapus grup keamanan menggunakan AWS CLI

Gunakan perintah delete-security-group.

Kelola grup keamanan menggunakan Firewall Manager

AWS Firewall Manager menyederhanakan administrasi grup keamanan dan tugas pemeliharaan Anda di beberapa akun dan sumber daya. Dengan Firewall Manager, Anda dapat mengonfigurasi dan mengaudit grup keamanan untuk organisasi Anda dari satu akun administrator pusat. Firewall Manager secara otomatis menerapkan aturan dan perlindungan di seluruh akun dan sumber daya, bahkan saat Anda menambahkan sumber daya baru. Firewall Manager sangat berguna ketika Anda ingin melindungi seluruh organisasi Anda, atau jika Anda sering menambahkan sumber daya baru yang ingin Anda lindungi dari akun administrator pusat.

Anda dapat menggunakan Firewall Manager untuk mengelola grup keamanan secara terpusat dengan cara berikut:

- Mengkonfigurasi grup keamanan dasar umum di seluruh organisasi: Anda dapat menggunakan kebijakan grup keamanan umum untuk menyediakan pengelompokan grup keamanan untuk akun dan sumber daya di seluruh organisasi Anda. Anda menentukan di mana dan bagaimana menerapkan kebijakan di organisasi Anda.

- Mengaudit grup keamanan yang ada di organisasi Anda: Anda dapat menggunakan kebijakan grup keamanan audit untuk memeriksa aturan yang ada yang digunakan dalam grup keamanan organisasi Anda. Anda dapat menjangkau kebijakan untuk meng-audit semua akun, akun tertentu, atau sumber daya yang ditandai dalam organisasi Anda. Firewall Manager secara otomatis mendeteksi akun dan sumber daya baru dan mengauditnya. Anda dapat membuat aturan audit untuk menetapkan pengaman yang berupa aturan grup keamanan untuk pemberian izin atau pelarangan dalam organisasi Anda, dan untuk memeriksa grup keamanan yang tidak digunakan atau tumpang tindih.
- Mendapatkan laporan tentang sumber daya yang tidak sesuai dan memperbaikinya: Anda bisa mendapatkan laporan dan peringatan untuk sumber daya yang tidak sesuai untuk data awal Anda dan meng-audit kebijakan. Anda juga dapat mengatur alur kerja perbaikan otomatis untuk memulihkan sumber daya yang tidak sesuai yang terdeteksi oleh Firewall Manager.

Untuk mempelajari selengkapnya tentang menggunakan Firewall Manager untuk mengelola grup keamanan Anda, lihat sumber daya berikut di panduan AWS Firewall Manager pengembang:

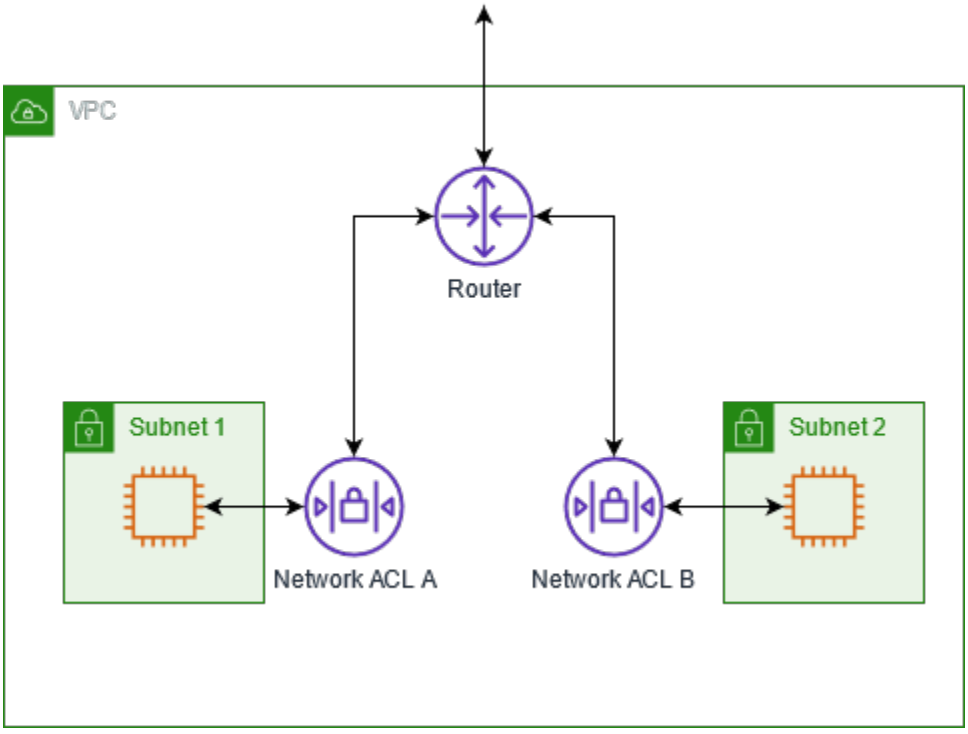
- AWS Firewall Manager prasyarat
- Memulai AWS Firewall Manager kebijakan grup keamanan Amazon VPC
- Bagaimana kebijakan kelompok keamanan bekerja di AWS Firewall Manager
- Kasus penggunaan kebijakan grup keamanan

Kontrol lalu lintas ke subnet menggunakan ACL jaringan

Network Access Control List (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 ACL jaringan.

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 ACL jaringan, lihatMembandingkan grup keamanan dan ACL jaringan.

Daftar Isi

Dasar-dasar ACL jaringan

Berikut ini adalah hal-hal dasar yang perlu Anda ketahui tentang ACL jaringan:

- VPC Anda secara otomatis dilengkapi dengan ACL jaringan default yang dapat diubah. Secara default, mengizinkan semua lalu lintas IPv4 masuk dan keluar dan, jika mengizinkan, lalu lintas IPv6.
- Anda dapat membuat ACL jaringan khusus dan mengaitkannya dengan subnet untuk mengizinkan atau menolak lalu lintas masuk atau keluar tertentu di tingkat subnet.
- Setiap subnet di VPC Anda harus dihubungkan dengan sebuah ACL jaringan. Jika Anda tidak benar-benar menghubungkan subnet dengan ACL jaringan, subnet secara otomatis dihubungkan ke ACL jaringan default.
- 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.
- ACL jaringan memiliki aturan masuk dan aturan keluar. 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.
- NACL tidak memiliki 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 instans EC2, respons secara otomatis diizinkan terlepas dari aturan grup keamanan keluar.
- ACL jaringan tidak 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 di Panduan Pengembang Amazon Route 53.
- ACL jaringan tidak dapat memblokir lalu lintas ke Layanan Metadata Instans (IMDS). Untuk mengelola akses ke IMDS, lihat Mengonfigurasi opsi metadata instans di Panduan Pengguna Amazon EC2.
- ACL jaringan tidak memfilter lalu lintas yang ditujukan ke dan dari berikut ini:

  - Layanan Nama Domain Amazon (DNS)
  - Protokol Konfigurasi Host Dinamis (DHCP)
  - Metadata instans Amazon EC2
  - Titik akhir metadata tugas Amazon ECS
  - Aktivasi lisensi untuk instance Windows
  - Layanan Amazon Time Sync
  - Alamat IP yang dicadangkan yang digunakan oleh router VPC default
- Ada kuota (juga dikenal sebagai batas) untuk jumlah ACL jaringan per VPC dan jumlah aturan per ACL jaringan. Untuk informasi selengkapnya, lihat Kuota Amazon VPC.

Aturan ACL Jaringan

Anda dapat menambahkan atau menghapus aturan dari ACL jaringan default, atau membuat ACL jaringan tambahan untuk VPC Anda. Ketika Anda menambahkan atau menghapus aturan dari ACL jaringan, perubahan secara otomatis diterapkan ke subnet yang terhubung dengannya.

Berikut ini adalah bagian-bagian dari aturan ACL jaringan:

- Nomor aturan. Aturan dievaluasi mulai dari aturan bernomor terendah. Setelah aturan cocok dengan lalu lintas, aturan tersebut langsung diterapkan terlepas dari apakah ada aturan bernomor lebih tinggi yang mungkin bertentangan dengan itu.
- Jenis. Jenis lalu lintas; misalnya, SSH. Anda juga dapat menentukan semua lalu lintas atau rentang kustom.
- Protokol. Anda dapat menetapkan protokol manapun yang memiliki nomor protokol standar. Untuk informasi selengkapnya, lihat Nomor Protokol. Jika Anda menetapkan ICMP sebagai protokol, Anda dapat menetapkan satu atau semua jenis dan kode ICMP.
- Rentang port. Listening port atau rentang port untuk lalu lintas. Misalnya, 80 untuk lalu lintas HTTP.
- Sumber. [Aturan masuk saja] Sumber lalu lintas (rentang CIDR).
- Tujuan. [Aturan keluar saja] Tujuan untuk lalu lintas (rentang CIDR).
- Izinkan/Tolak. Apakah mengizinkan atau menolak lalu lintas yang ditentukan.

Jika Anda menambahkan aturan menggunakan alat baris perintah atau API Amazon EC2, rentang CIDR secara otomatis diubah ke bentuk kanonisnya. Misalnya, jika Anda menetapkan

`100.68.0.18/18` untuk rentang CIDR, kami membuat aturan dengan rentang CIDR `100.68.0.0/18`.

ACL jaringan default

ACL jaringan default dikonfigurasi untuk mengizinkan semua lalu lintas mengalir masuk dan keluar dari subnet yang terhubung dengannya. Setiap jaringan ACL juga menyertakan aturan yang nomor aturannya adalah tanda bintang (*). Aturan ini memastikan bahwa jika sebuah paket tidak cocok dengan aturan bernomor lainnya, maka paket ditolak. Anda tidak dapat mengubah atau menghapus aturan ini.

Berikut ini adalah contoh ACL jaringan default untuk VPC yang hanya mendukung IPv4.

Masuk

Aturan #	Tipe	Protokol	Rentang port	Sumber	Izinkan/Tolak
100	Semua lalu lintas IPv4	Semua	Semua	0.0.0.0/0	IZINKAN
*	Semua lalu lintas IPv4	Semua	Semua	0.0.0.0/0	MENOLAK

Keluar

Aturan #	Tipe	Protokol	Rentang Port	Tujuan	Izinkan/Tolak
100	Semua lalu lintas IPv4	Semua	Semua	0.0.0.0/0	IZINKAN
*	Semua lalu lintas IPv4	Semua	Semua	0.0.0.0/0	MENOLAK

Jika Anda membuat VPC dengan blok CIDR IPv6 atau jika Anda mengaitkan blok CIDR IPv6 dengan VPC yang ada, kami secara otomatis menambahkan aturan yang mengizinkan semua lalu lintas IPv6 mengalir masuk dan keluar dari subnet Anda. Kami juga menambahkan aturan yang memiliki nomor aturan bertanda bintang yang memastikan bahwa paket ditolak jika tidak cocok dengan aturan bernomor lainnya. Anda tidak dapat mengubah atau menghapus aturan ini. Berikut ini adalah contoh ACL jaringan default untuk VPC yang mendukung IPv4 dan IPv6.

> **Note**
>
> Jika Anda telah mengubah aturan masuk ACL jaringan default Anda, kami tidak secara otomatis menambahkan `ALLOW` aturan untuk lalu lintas IPv6 masuk saat Anda mengaitkan blok IPv6 dengan VPC Anda. Demikian pula, jika Anda telah memodifikasi aturan keluar, kami tidak secara otomatis menambahkan `ALLOW` aturan untuk lalu lintas IPv6 keluar.

Masuk

Aturan #	Tipe	Protokol	Rentang port	Sumber	Izinkan/Tolak
100	Semua lalu lintas IPv4	Semua	Semua	0.0.0.0/0	IZINKAN
101	Semua lalu lintas IPv6	Semua	Semua	::/0	IZINKAN
*	Semua Lalu lintas	Semua	Semua	0.0.0.0/0	MENOLAK
*	Semua lalu lintas IPv6	Semua	Semua	::/0	TOLAK

Keluar

Aturan #	Tipe	Protokol	Rentang Port	Tujuan	Izinkan/Tolak
100	Semua Lalu lintas	Semua	Semua	0.0.0.0/0	IZINKAN
101	Semua lalu lintas IPv6	Semua	Semua	::/0	IZINKAN
*	Semua Lalu lintas	Semua	Semua	0.0.0.0/0	MENOLAK
*	Semua lalu lintas IPv6	Semua	Semua	::/0	TOLAK

ACL Jaringan kustom

Contoh berikut menunjukkan ACL jaringan kustom untuk VPC yang mendukung IPv4 saja. Ini termasuk aturan masuk yang memungkinkan lalu lintas HTTP dan HTTPS (100 dan 110). Ada aturan keluar yang sesuai yang memungkinkan respons terhadap lalu lintas masuk (140), yang mencakup port fana 32768-65535. Untuk informasi lebih lanjut tentang cara memilih rentang port ephemeral yang sesuai, lihat Ephemeral port.

ACL jaringan juga mencakup aturan masuk yang mengizinkan lalu lintas SSH dan RDP ke subnet. Aturan keluar 120 memungkinkan respons untuk meninggalkan subnet.

ACL jaringan memiliki aturan keluar (100 dan 110) yang mengizinkan lalu lintas HTTP dan HTTPS keluar dari subnet. Ada aturan masuk yang sesuai yang memungkinkan respons terhadap lalu lintas keluar (140), yang mencakup port fana 32768-65535.

Setiap ACL jaringan mencakup aturan default yang nomor aturannya bertanda bintang. Aturan ini memastikan bahwa jika sebuah paket tidak cocok dengan aturan lainnya, maka paket ditolak. Anda tidak dapat mengubah atau menghapus aturan ini.

masuk

Aturan #	Tipe	Protokol	Rentang port	Sumber	Izinkan/Tolak	Komentar
100	HTTP	TCP	80	0.0.0.0/0	IZINKAN	Mengizinkan akses jalur masuk HTTP dari alamat IPv4 apa pun.
110	HTTPS	TCP	443	0.0.0.0/0	IZINKAN	Mengizinkan akses jalur masuk HTTPS dari alamat IPv4 apa pun.
120	SSH	TCP	22	192.0.2.0/24	IZINKAN	Mengizinkan lalu lintas SSH masuk dari rentang alamat IPv4 publik jaringan rumah Anda (melalui gateway internet).

Aturan #	Tipe	Protokol	Rentang port	Sumber	Izinkan/Tolak	Komentar
130	RDP	TCP	3389	192.0.2.0/24	IZINKAN	Mengizinkan lalu lintas RDP masuk ke server web dari rentang alamat IPv4 publik jaringan rumah Anda (melalui gateway internet).
140	TCP Kustom	TCP	32768-65535	0.0.0.0/0	IZINKAN	Mengizinkan lalu lintas IPv4 kembali masuk dari internet (yaitu, untuk permintaan yang berasal dari subnet). Rentang ini hanya contoh.
*	Semua Lalu lintas	Semua	Semua	0.0.0.0/0	MENOLAK	Menolak semua lalu lintas IPv4 masuk yang belum ditangani oleh aturan sebelumnya (tidak dapat diubah).

Keluar

Aturan #	Tipe	Protokol	Rentang Port	Tujuan	Izinkan/Tolak	Komentar
100	HTTP	TCP	80	0.0.0.0/0	IZINKAN	Mengizinkan lalu lintas HTTP IPv4 keluar dari subnet ke internet.

Aturan #	Tipe	Protokol	Rentang Port	Tujuan	Izinkan/Tolak	Komentar
110	HTTPS	TCP	443	0.0.0.0/0	IZINKAN	Mengizinkan lalu lintas HTTPS IPv4 keluar dari subnet ke internet.
120	SSH	TCP	1024-65535	192.0.2.0/24	IZINKAN	Memungkinkan lalu lintas SSH pengembalian keluar ke rentang alamat IPv4 publik jaringan rumah Anda (melalui gateway internet).
140	TCP Kustom	TCP	32768-65535	0.0.0.0/0	IZINKAN	Mengizinkan respon jalur keluar IPv4 untuk klien di internet (misalnya, melayani halaman web untuk orang-orang yang mengunjungi server web di subnet). Rentang ini adalah contoh saja.
*	Semua Lalu lintas	Semua	Semua	0.0.0.0/0	MENOLAK	Menolak semua lalu lintas IPv4 keluar yang belum ditangani oleh aturan sebelumnya (tidak dapat diubah).

Ketika paket datang ke subnet, kami mengevaluasinya terhadap aturan masuk ACL yang dikaitkan dengan subnet tersebut (mulai dari bagian atas daftar aturan, terus ke bawah). Berikut adalah

pelaksanaan evaluasi jika paket ditujukan untuk port HTTPS (443). Paket tidak cocok aturan pertama dievaluasi (aturan 100). Ini tidak cocok dengan aturan kedua (110), yang mengizinkan paket ke subnet. Jika paket telah ditujukan untuk port 139 (NetBIOS), itu tidak cocok salah satu aturan, dan aturan * akhirnya menolak paket.

Anda mungkin ingin menambahkan aturan Tolak dalam situasi di mana Anda sah perlu membuka berbagai port, tetapi ada port tertentu dalam rentang tersebut yang ingin Anda tolak. Pastikan untuk menempatkan aturan Tolak sebelumnya dalam tabel daripada aturan yang mengizinkan berbagai lalu lintas port.

Anda menambahkan aturan Izinkan tergantung pada kasus penggunaan Anda. Misalnya, Anda dapat menambahkan aturan yang mengizinkan TCP keluar dan akses UDP pada port 53 untuk resolusi DNS. Untuk setiap aturan yang Anda tambahkan, pastikan bahwa ada aturan masuk atau keluar sesuai yang mengizinkan lalu lintas respon.

Contoh berikut menunjukkan ACL jaringan kustom untuk VPC yang memiliki blok CIDR IPv6 terkait. ACL jaringan ini mencakup aturan untuk semua lalu lintas HTTP dan HTTPS IPv6. Dalam hal ini, aturan baru dimasukkan di antara aturan yang ada untuk lalu lintas IPv4. Anda juga dapat menambahkan aturan sebagai aturan nomor yang lebih tinggi setelah aturan IPv4. Lalu lintas IPv4 dan IPv6 terpisah, dan karena itu tidak ada aturan untuk lalu lintas IPv4 berlaku untuk lalu lintas IPv6.

Masuk

Aturan #	Tipe	Protokol	Rentang port	Sumber	Izinkan/Tolak	Komentar
100	HTTP	TCP	80	0.0.0.0/0	IZINKAN	Mengizinkan lalu lintas HTTP masuk dari alamat IPv4 apa pun.
105	HTTP	TCP	80	::/0	IZINKAN	Mengizinkan lalu lintas HTTP masuk dari alamat IPv6 apa pun.
110	HTTPS	TCP	443	0.0.0.0/0	IZINKAN	Mengizinkan lalu lintas HTTP masuk

Aturan #	Tipe	Protokol	Rentang port	Sumber	Izinkan/Tolak	Komentar
						dari alamat IPv4 apa pun.
115	HTTPS	TCP	443	::/0	IZINKAN	Mengizinkan akses HTTPS masuk dari alamat IPv6 apa pun.
120	SSH	TCP	22	192.0.2.0/24	IZINKAN	Mengizinkan lalu lintas SSH masuk dari rentang alamat IPv4 publik jaringan rumah Anda (melalui gateway internet).
130	RDP	TCP	3389	192.0.2.0/24	IZINKAN	Mengizinkan lalu lintas RDP masuk ke server web dari rentang alamat IPv4 publik jaringan rumah Anda (melalui gateway internet).
140	TCP Kustom	TCP	32768-65535	0.0.0.0/0	IZINKAN	Mengizinkan lalu lintas IPv4 kembali masuk dari internet (yaitu, untuk permintaan yang berasal dari subnet). Rentang ini hanya contoh.

Aturan #	Tipe	Protokol	Rentang port	Sumber	Izinkan/Tolak	Komentar
145	TCP Kustom	TCP	32768-65535	::/0	IZINKAN	Mengizinkan lalu lintas IPv6 kembali masuk dari internet (yaitu, untuk permintaan yang berasal dari subnet). Rentang ini adalah contoh saja.
*	Semua Lalu lintas	Semua	Semua	0.0.0.0/0	MENOLAK	Menolak semua lalu lintas IPv4 masuk yang belum ditangani oleh aturan sebelumnya (tidak dapat diubah).
*	Semua lalu lintas	Semua	Semua	::/0	TOLAK	Menolak semua lalu lintas IPv6 masuk yang belum ditangani oleh aturan sebelumnya (tidak dapat diubah).

Keluar

Aturan #	Tipe	Protokol	Rentang Port	Tujuan	Izinkan/Tolak	Komentar
100	HTTP	TCP	80	0.0.0.0/0	IZINKAN	Mengizinkan lalu lintas HTTP IPv4 keluar dari subnet ke internet.

Aturan #	Tipe	Protokol	Rentang Port	Tujuan	Izinkan/Tolak	Komentar
105	HTTP	TCP	80	::/0	IZINKAN	Mengizinkan lalu lintas HTTP IPv6 keluar dari subnet ke internet.
110	HTTPS	TCP	443	0.0.0.0/0	IZINKAN	Mengizinkan lalu lintas HTTPS IPv4 keluar dari subnet ke internet.
115	HTTPS	TCP	443	::/0	IZINKAN	Mengizinkan lalu lintas HTTPS IPv6 keluar dari subnet ke internet.
140	TCP Kustom	TCP	32768-65535	0.0.0.0/0	IZINKAN	Mengizinkan respon jalur keluar IPv4 untuk klien di internet (misalnya, melayani halaman web untuk orang-orang yang mengunjungi server web di subnet). Rentang ini adalah contoh saja.

Aturan #	Tipe	Protokol	Rentang Port	Tujuan	Izinkan/Tolak	Komentar
145	TCP Kustom	TCP	32768-65535	::/0	IZINKAN	Mengizinkan respon IPv6 keluar untuk klien di internet (misalnya, melayani halaman web untuk orang-orang yang mengunjungi server web di subnet). Rentang ini adalah contoh saja.
*	Semua Lalu lintas	Semua	Semua	0.0.0.0/0	MENOLAK	Menolak semua lalu lintas IPv4 keluar belum ditangani oleh aturan sebelumnya (tidak dapat diubah).
*	Semua lalu lintas	Semua	Semua	::/0	TOLAK	Menolak semua lalu lintas jalur keluar IPv6 yang belum ditangani oleh aturan sebelumnya (tidak dapat dimodifikasi).

ACL jaringan khusus dan layanan lainnya AWS

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 lebih lanjut tentang aturan ACL jaringan yang disarankan untuk

penyeimbang beban dan instans backend Anda, lihat ACL rangkaian untuk penyeimbang beban dalam VPC di Panduan Pengguna untuk Classic Load Balancer.

Ephemeral port

Contoh ACL jaringan di bagian sebelumnya menggunakan rentang ephemeral port 32768-65535. Namun, Anda mungkin ingin menggunakan rentang yang berbeda untuk ACL jaringan Anda tergantung pada jenis klien yang Anda gunakan atau yang berkomunikasi dengan Anda.

Klien yang menginisiasi permintaan memilih rentang ephemeral port. Rentang bervariasi tergantung pada sistem operasi klien.

- Banyak kernel Linux (termasuk kernel Amazon Linux) menggunakan port 32768-61000.
- Permintaan yang berasal dari Elastic Load Balancing menggunakan port 1024-65535.
- Sistem operasi Windows melalui Windows Server 2003 menggunakan port 1025-5000.
- Windows Server 2008 dan versi yang lebih baru menggunakan port 49152-65535.
- Gateway NAT menggunakan port 1024-65535.
- AWS Lambda fungsi menggunakan port 1024-65535.

Sebagai contoh, jika permintaan datang ke server web di VPC Anda dari klien Windows 10 di internet, ACL jaringan Anda harus memiliki aturan keluar untuk mengaktifkan lalu lintas yang ditujukan untuk port 49152-65535.

Jika instans dalam VPC klien menginisiasi permintaan, ACL jaringan Anda harus memiliki aturan masuk untuk mengaktifkan lalu lintas yang ditujukan untuk ephemeral port khusus untuk jenis instans ini (Amazon Linux, Windows Server 2008, dan sebagainya).

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.

Path MTU Discovery

Path MTU Discovery digunakan untuk menentukan jalur MTU antara dua perangkat. Jalur MTU adalah ukuran paket maksimum yang didukung pada jalur antara host asal dan host penerima.

Untuk IPv4, 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: `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set` (Tipe 3, Kode 4). Ini menginstruksikan host transmisi untuk membagi muatan menjadi beberapa paket yang lebih kecil, dan kemudian mentrasmisikannya kembali.

Protokol IPv6 tidak mendukung fragmentasi dalam jaringan. 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 mentrasmisikannya kembali.

Jika unit transmisi maksimum (MTU) antar host di subnet Anda berbeda, atau instans Anda berkomunikasi dengan rekan-rekan melalui internet, Anda harus menambahkan aturan ACL jaringan berikut, baik masuk maupun keluar. Hal ini memastikan bahwa Path MTU Discovery dapat berfungsi dengan benar dan mencegah kehilangan paket. Pilih Aturan ICMP Kustom untuk jenis tersebut dan Tujuan yang Tidak Dapat Dihubungi, fragmentasi yang diperlukan, dan bendera DF yang ditetapkan untuk rentang port tersebut (tipe 3, kode 4). Jika Anda menggunakan traceroute, tambahkan juga aturan berikut: pilih Aturan ICMP Kustom untuk jenis ini dan Waktu Terlampaui, Transit kedaluwarsa TTL untuk rentang port ini (tipe 11, kode 0). Untuk informasi selengkapnya, lihat Unit transmisi maksimum jaringan (MTU) untuk instans EC2 Anda di Panduan Pengguna Amazon EC2.

Bekerja dengan ACL jaringan

Tugas-tugas berikut menunjukkan kepada Anda tentang cara bekerja dengan ACL jaringan menggunakan konsol Amazon VPC.

Tugas

- Menentukan pengaitan ACL jaringan
- Membuat ACL jaringan
- Menambah dan menghapus aturan
- Mengaitkan subnet dengan ACL jaringan
- Melepaskan ACL jaringan dari subnet
- Mengubah ACL jaringan subnet
- Menghapus ACL jaringan

- gambaran umum API dan perintah
- Kelola ACL jaringan menggunakan Firewall Manager

Menentukan pengaitan ACL jaringan

Anda dapat menggunakan konsol Amazon VPC untuk menentukan ACL jaringan yang terkait dengan subnet. ACL jaringan dapat dikaitkan dengan lebih dari satu subnet, sehingga Anda juga dapat menentukan subnet yang terkait dengan ACL jaringan.

Untuk menentukan ACL jaringan mana yang dikaitkan dengan subnet

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

   ACL jaringan yang terkait dengan subnet dicantumkan dalam tab ACL Jaringan, bersama dengan aturan ACL jaringan.

Untuk menentukan subnet mana yang dikaitkan dengan ACL jaringan

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih ACL Jaringan. Kolom Dikaitkan Dengan menunjukkan jumlah subnet terkait untuk setiap ACL jaringan.
3. Pilih ACL jaringan.
4. Di panel rincian, pilih Pengaitan Subnet untuk menampilkan subnet yang terkait dengan ACL jaringan.

Membuat ACL jaringan

Anda dapat membuat ACL jaringan kustom untuk VPC Anda. Secara default, ACL jaringan yang Anda buat memblokir semua lalu lintas masuk dan keluar sampai Anda menambahkan aturan, dan tidak terkait dengan subnet sampai Anda secara eksplisit mengaitkannya dengan satu subnet.

Untuk membuat ACL jaringan

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih ACL Jaringan.
3. Pilih Buat ACL Jaringan.

4. Di kotak dialog Buat ACL Jaringan, Anda dapat memberi nama ACL jaringan Anda, dan memilih ID VPC Anda dari daftar VPC. Kemudian, pilih Ya, Buat.

Menambah dan menghapus aturan

Ketika Anda menambahkan atau menghapus aturan dari ACL, subnet yang terkait dengan ACL tunduk pada perubahan tersebut. Anda tidak harus mengakhiri dan meluncurkan kembali instans di subnet. Perubahan berlaku setelah beberapa saat.

> **Important**
>
> Berhati-hatilah jika Anda menambahkan dan menghapus aturan secara bersamaan. Aturan ACL jaringan menentukan jenis lalu lintas jaringan mana yang dapat masuk atau keluar dari VPC Anda. Jika Anda menghapus aturan masuk atau keluar dan kemudian menambahkan entri baru lebih dari yang diizinkan di Kuota Amazon VPC, entri yang dipilih untuk dihapus akan dihapus dan entri baru tidak akan ditambahkan. Hal ini dapat menyebabkan masalah konektivitas yang tidak terduga dan secara tidak sengaja mencegah akses ke dan dari VPC Anda.

Jika Anda menggunakan API Amazon EC2 atau alat baris perintah, Anda tidak dapat mengubah aturan. Anda hanya dapat menambahkan dan menghapus aturan. Jika Anda menggunakan konsol Amazon VPC, Anda dapat mengubah entri untuk aturan yang ada. Konsol tersebut menghapus aturan yang ada dan menambahkan aturan baru untuk Anda. Jika Anda perlu mengubah urutan aturan di ACL, Anda harus menambahkan aturan baru dengan nomor aturan baru, dan kemudian menghapus aturan semula.

Untuk menambahkan aturan ke ACL jaringan

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih ACL Jaringan.
3. Di panel rincian, pilih tab Aturan Masuk atau Aturan Keluar, tergantung pada jenis aturan yang Anda perlu tambahkan, dan kemudian pilih Edit.
4. Di Aturan #, masukkan nomor aturan (misalnya, 100). Nomor aturan tidak boleh yang sudah digunakan dalam ACL jaringan. Kami memproses aturan secara berurutan, dimulai 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.

5. Pilih aturan dari daftar Jenis. Misalnya, untuk menambahkan aturan untuk HTTP, pilih HTTP. Untuk menambahkan aturan untuk mengizinkan semua lalu lintas TCP, pilih Semua TCP. Untuk beberapa opsi ini (misalnya, HTTP), kami mengisikan port untuk Anda. Untuk menggunakan protokol yang tidak terdaftar, pilih Aturan Protokol Kustom.
6. (Opsional) Jika Anda membuat aturan protokol kustom, pilih nomor dan nama protokol dari daftar Protokol. Untuk informasi selengkapnya, lihat Daftar Nomor Protokol IANA.
7. (Opsional) Jika protokol yang Anda pilih memerlukan nomor port, masukkan nomor port atau rentang port yang dipisahkan oleh tanda hubung (misalnya, 49152-65535).
8. Di bidang Sumber atau Tujuan (tergantung pada apakah ini adalah aturan masuk atau keluar), masukkan rentang CIDR yang terhadapnya berlaku aturan tersebut.
9. Dari daftar Izinkan/Tolak, pilih IZINKAN untuk mengizinkan lalu lintas yang ditentukan atau TOLAK untuk menolak lalu lintas yang ditentukan.
10. (Opsional) Untuk menambahkan aturan lain, pilih Tambahkan aturan lain, dan ulangi langkah 4 sampai 9 sesuai kebutuhan.
11. Jika Anda sudah selesai, pilih Simpan.

Untuk menghapus aturan dari ACL jaringan

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih ACL Jaringan, dan kemudian pilih ACL jaringan.
3. Di panel rincian, pilih tab Aturan Masuk atau Aturan Keluar, kemudian pilih Edit. Pilih Hapus untuk aturan yang ingin Anda hapus, kemudian pilih Simpan.

Mengaitkan subnet dengan ACL jaringan

Untuk menerapkan aturan ACL jaringan untuk subnet tertentu, Anda harus mengaitkan subnet tersebut dengan ACL jaringan. Anda dapat menghubungkan ACL jaringan dengan beberapa subnet. Namun, suatu subnet dapat dikaitkan dengan hanya satu ACL jaringan. Setiap subnet yang tidak terkait dengan ACL tertentu dikaitkan dengan ACL jaringan default secara default.

Untuk mengaitkan subnet dengan ACL jaringan

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih ACL Jaringan, dan kemudian pilih ACL jaringan.
3. Di panel rincian, pada tab Pengaitan Subnet, pilih Edit. Pilih kotak centang Pengaitan untuk mengaitkan subnet dengan ACL jaringan, dan kemudian pilih Simpan.

Melepaskan ACL jaringan dari subnet

Anda dapat melepaskan ACL jaringan dari subnet. Ketika subnet telah dilepaskan dari ACL jaringan kustom, maka subnet akan secara otomatis terkait dengan ACL jaringan default.

Untuk melepaskan subnet dari ACL jaringan

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih ACL Jaringan, dan kemudian pilih ACL jaringan.
3. Di panel rincian, pilih tab Pengaitan Subnet.
4. Pilih Edit, kemudian batalkan pilihan kotak centang Pengaitan untuk subnet tersebut. Pilih Simpan.

Mengubah ACL jaringan subnet

Anda dapat mengubah ACL jaringan yang terkait dengan suatu subnet. Misalnya, ketika Anda membuat suatu subnet, awalnya subnet tersebut dikaitkan dengan ACL jaringan default. Anda mungkin ingin mengaitkannya dengan ACL jaringan kustom yang telah Anda buat.

Setelah mengubah ACL jaringan subnet, Anda tidak harus mengakhiri dan meluncurkan kembali instans di subnet tersebut. Perubahan berlaku setelah beberapa saat.

Untuk mengubah pengaitan ACL jaringan subnet

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Subnet, lalu pilih subnet.
3. Pilih tab ACL Jaringan, lalu pilih Edit.
4. Dari daftar Ubah ke, pilih ACL jaringan yang akan dikaitkan dengan subnet tersebut, dan kemudian pilih Simpan.

Menghapus ACL jaringan

Anda dapat menghapus ACL jaringan hanya jika tidak ada subnet yang terkait dengannya. Anda tidak dapat menghapus ACL jaringan default.

Untuk menghapus ACL jaringan

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih ACL Jaringan.
3. Pilih ACL jaringan, lalu pilih Hapus.
4. Di kotak dialog konfirmasi, pilih Ya, Hapus.

gambaran umum API dan perintah

Anda dapat melakukan tugas yang dijelaskan di halaman ini menggunakan baris perintah atau API. Untuk informasi selengkapnya tentang antarmuka baris perintah dan daftar API yang tersedia, lihat Bekerja dengan Amazon VPC.

Membuat ACL jaringan untuk VPC anda

- create-network-acl (AWS CLI)
- New-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Menjelaskan satu atau beberapa ACL jaringan Anda

- describe-network-acls (AWS CLI)
- Get-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Menambahkan aturan ke ACL jaringan

- create-network-acl-entry (AWS CLI)
- New-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Menghapus aturan dari ACL jaringan

- delete-network-acl-entry (AWS CLI)
- Remove-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Mengganti aturan yang ada di ACL jaringan

- mengganti-acl jaringan (AWS CLI)
- Set-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Mengganti pengaitan ACL jaringan

- replace-network-acl-association (AWS CLI)
- Set-EC2NetworkAclAssociation (AWS Tools for Windows PowerShell)

Menghapus ACL jaringan

- delete-network-acl (AWS CLI)
- Remove-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Kelola ACL jaringan 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 ACL jaringan 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 ACL jaringan untuk subnet dalam lingkup, dan Anda dapat mengonfigurasi Firewall Manager untuk secara otomatis memulihkan ACL jaringan yang tidak sesuai, agar sesuai.

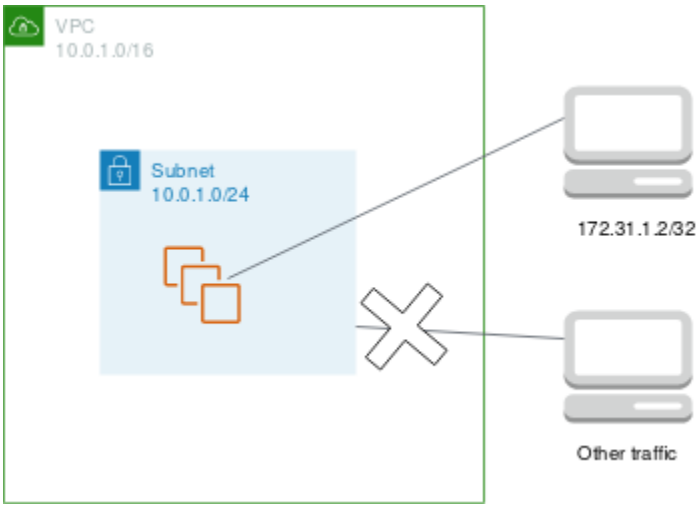
Untuk mempelajari selengkapnya tentang menggunakan Firewall Manager untuk mengelola ACL jaringan Anda, lihat sumber daya berikut di panduan AWS Firewall Manager pengembang:

- AWS Firewall Manager prasyarat
- Memulai dengan AWS Firewall Manager kebijakan ACL jaringan Amazon VPC

- Kebijakan daftar kontrol akses jaringan (ACL) Amazon Virtual Private Cloud

Contoh: Kontrol akses ke instans dalam subnet

Dalam contoh ini, instans di subnet Anda dapat berkomunikasi satu sama lain, dan dapat diakses dari komputer jarak jauh yang terpercaya. Komputer jarak jauh tersebut mungkin berupa komputer di jaringan lokal Anda atau instans di subnet atau VPC yang berbeda. Anda menggunakannya untuk terhubung ke instans Anda untuk melakukan tugas-tugas administratif. Aturan grup keamanan dan aturan ACL jaringan Anda mengizinkan akses dari alamat IP komputer jarak jauh Anda (172.31.1.2/32). Semua lalu lintas lain dari internet atau jaringan lain ditolak. Skenario ini memberi Anda fleksibilitas untuk mengubah grup keamanan atau aturan grup keamanan untuk instans Anda, dan membuat ACL jaringan sebagai lapisan backup untuk pertahanan.



Berikut ini adalah contoh grup keamanan yang terkait dengan instans. Grup keamanan bersifat stateful. Oleh karena itu Anda tidak memerlukan aturan yang mengizinkan respon terhadap lalu lintas masuk.

Ke dalam

Tipe protokol	Protokol	Rentang port	Sumber	Komentar
Semua lalu lintas	Semua	Semua	sg-123456 7890abcdef0	Semua instans yang terkait dengan grup keamanan ini dapat berkomuni

Tipe protokol	Protokol	Rentang port	Sumber	Komentar
				kasi satu sama lain.
SSH	TCP	22	172.31.1.2/32	Mengizinkan akses SSH masuk dari komputer jarak jauh Anda.

Ke luar

Jenis protokol	Protokol	Rentang Port	Tujuan	Komentar
Semua lalu lintas	Semua	Semua	sg-123456 7890abcdef0	Semua instans yang terkait dengan grup keamanan ini dapat berkomuni kasi satu sama lain.

Berikut ini adalah contoh ACL jaringan untuk mengaitkan dengan subnet untuk instans. Aturan ACL jaringan berlaku untuk semua instans di subnet. ACL jaringan bersifat stateless. Oleh karena itu, Anda memerlukan aturan yang mengizinkan respon terhadap lalu lintas masuk.

Masuk

Aturan #	Tipe	Protokol	Rentang port	Sumber	Izinkan/Tolak	Komentar
100	SSH	TCP	22	172.31.1.2/32	IZINKAN	Mengizinkan lalu lintas masuk dari

Aturan #	Tipe	Protokol	Rentang port	Sumber	Izinkan/Tolak	Komentar
						komputer jarak jauh.
*	Semua lalu lintas	Semua	Semua	0.0.0.0/0	TOLAK	Menolak semua lalu lintas masuk lainnya.

Keluar

Aturan #	Tipe	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 keluar lainnya.

Jika Anda secara tidak sengaja membuat aturan grup keamanan Anda terlalu permisif, ACL jaringan dalam hal ini terus mengizinkan akses hanya dari alamat IP yang ditentukan. Misalnya, grup keamanan berikut berisi aturan yang memungkinkan akses SSH masuk dari alamat IP apa pun. Namun, jika Anda mengaitkan grup keamanan ini dengan instans di subnet yang menggunakan ACL jaringan, hanya instans lain dalam subnet dan komputer jarak jauh Anda yang dapat mengakses instans ini, karena aturan ACL jaringan menolak lalu lintas masuk lain ke subnet tersebut.

Ke dalam

Tipe	Protokol	Rentang port	Sumber	Komentar
Semua lalu lintas	Semua	Semua	sg-123456 7890abcdef0	Semua instans yang terkait dengan grup keamanan ini dapat berkomuni kasi satu sama lain.
SSH	TCP	22	0.0.0.0/0	Mengizinkan akses SSH dari alamat IP mana pun.

Ke luar

Tipe	Protokol	Rentang Port	Tujuan	Komentar
Semua lalu lintas	Semua	Semua	0.0.0.0/0	Mengizinkan semua lalu lintas keluar.

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.

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.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur AWS Global.

Anda dapat mengonfigurasi VPC Anda untuk memenuhi persyaratan ketahanan untuk beban kerja Anda. Untuk informasi selengkapnya, lihat berikut ini:

- Memahami pola ketahanan dan 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:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.

- Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

  > **Note**
  >
  > Tidak semua memenuhi Layanan AWS syarat HIPAA. Untuk informasi selengkapnya, lihat Referensi Layanan yang Memenuhi 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 yang 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 ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

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. Untuk informasi selengkapnya, lihat Amazon VPC aktif. AWS
- Gunakan grup keamanan untuk mengontrol lalu lintas ke instans EC2 di subnet Anda. Untuk informasi selengkapnya, lihat Grup keamanan.
- Gunakan ACL jaringan untuk mengontrol lalu lintas masuk dan keluar di tingkat subnet. Untuk informasi selengkapnya, lihat Kontrol lalu lintas ke subnet menggunakan ACL 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 VPC kami. 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 dasar 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 FAQ Keamanan dan Pemfilteran di Amazon VPC.

Gunakan Amazon VPC dengan yang lain Layanan AWS

Anda dapat menggunakan Amazon VPC dengan yang lain Layanan AWS untuk membangun solusi yang memenuhi kebutuhan Anda.

Daftar Isi

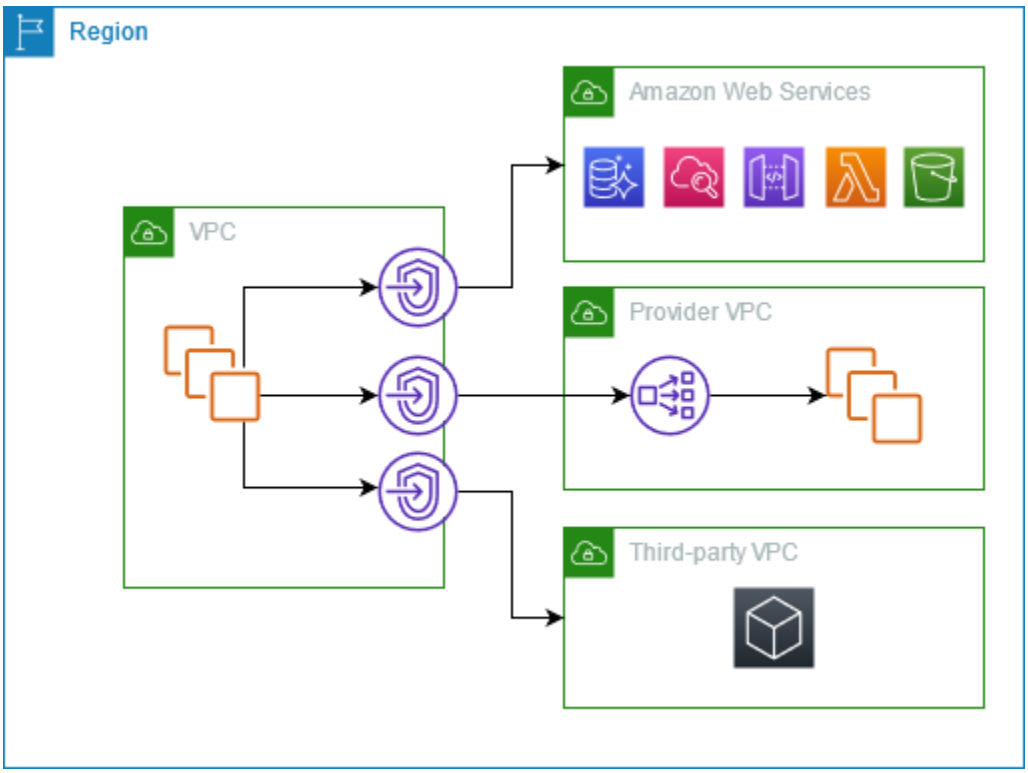
Connect VPC Anda ke layanan menggunakanAWS PrivateLink

AWS PrivateLinkmenetapkan konektivitas privat antara virtual private cloud (VPC) dan layanan yang didukungLayanan AWS, dihostingAkun AWS olehAWS Marketplace layanan yang didukung. Anda tidak perlu menggunakan gateway internet, perangkat NAT,AWS Direct Connect koneksi, atauAWS Site-to-Site VPN koneksi untuk berkomunikasi dengan layanan.

Untuk menggunakanAWS PrivateLink, buat endpoint VPC di VPC Anda, tentukan nama layanan dan subnet. Ini membuat elastic network interface dalam subnet yang berfungsi sebagai titik masuk untuk lalu lintas ditujukan ke layanan yang didukung.

Anda dapat membuat VPC endpoint Anda sendiri, yang didukung oleh AWS PrivateLink dan memungkinkan pelanggan AWS lainnya mengakses layanan Anda.

Diagram berikut menunjukkan kasus penggunaan umum untukAWS PrivateLink. VPC di sebelah kiri memiliki beberapa instans EC2 dalam subnet pribadi dan tiga titik akhir VPC antarmuka. Endpoint VPC paling atas terhubung ke sebuahLayanan AWS. Endpoint VPC tengah terhubung ke layanan yang dihosting oleh yang lainAkun AWS (layanan endpoint VPC). Endpoint VPC bawah terhubung ke layananAWS Marketplace mitra.



Untuk informasi selengkapnya, lihat AWS PrivateLink.

Filter lalu lintas jaringan menggunakanAWS Network Firewall

Anda dapat mem-filter lalu lintas jaringan di perimeter VPC Anda menggunakan AWS Network Firewall. Network Firewall adalah stateful, dikelola, jaringan firewall dan deteksi intrusi dan layanan pencegahan. Untuk informasi selengkapnya, lihat Panduan Developer AWS Network Firewall.

Anda menerapkan Network Firewall dengan sumber daya AWS 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. Hal ini juga mendefinisikan pengatura n tingkat tinggi seperti konfigurasi pencatatan firewall dan penandaan pada sumber daya firewall AWS.

Sumber daya Network Firewall	Deskripsi
	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 hal perilaku dan fungsinya untuk daftar kontrol akses (ACL) 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 Network Firewall secara terpusat di seluruh akun dan aplikasi Anda di AWS Organizations. Anda dapat mengelola firewall untuk beberapa akun menggunakan satu akun di Firewall Manager. Untuk informasi selengkapnya, lihat AWS Firewall Manager di Panduan Developer AWS WAF, AWS Firewall Manager, dan AWS Shield Advanced.

Filter DNS Firewall

Dengan DNS Firewall, Anda menentukan aturan penyaringan nama domain di grup aturan yang Anda kaitkan dengan VPC Anda. 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 sumber daya AWS 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 penyaringan, kemudian mengaitkan grup aturan dengan satu atau lebih VPC dari Amazon VPC. Ketika Anda mengaitkan grup aturan dengan VPC, Anda mengaktifkan penyaringan DNS Firewall untuk VPC. Kemudian, ketika Resolver menerima kueri DNS untuk VPC yang memiliki grup aturan yang terkait dengannya, Resolver meneruskan kueri tersebut ke DNS Firewall untuk disaring. Setiap aturan dalam grup aturan menentukan satu daftar domain dan tindakan yang akan dilakukan terhadap kueri DNS yang domainnya sesuai dengan spesifikasi domain dalam daftar. Anda dapat mengizink an, memblokir, atau memperingatkan adanya kueri yang cocok. Anda juga dapat menentukan respon kustom untuk kueri yang diblokir. Untuk informasi lebih lanjut, lihat: Grup aturan dan aturan dalam Route 53 Resolver DNS Firewall.
Daftar domain	Daftar domain adalah seperangkat spesifikasi domain yang dapat digunakan kembali yang Anda gunakan dalam aturan DNS Firewall, di dalam grup aturan. 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 di AWS Organizations. Anda dapat mengelola firewall untuk beberapa akun menggunakan satu akun di Firewall Manager. Untuk informasi selengkapnya, lihat AWS Firewall Manager di Panduan Developer AWS WAF, AWS Firewall Manager, dan AWS Shield Advanced.

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

Berikut ini adalah contoh konfigurasi untuk virtual private cloud (VPC) 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 VPC Anda satu sama lain, lihatKonfigurasi peering VPCdiPanduan Peering Amazon VPC.
- Untuk menghubungkan VPC Anda ke jaringan Anda sendiri, lihatArsitektur VPN situs-ke-situsdiAWS Site-to-Site VPNPanduan Pengguna.
- Untuk menghubungkan VPC Anda satu sama lain dan ke jaringan Anda sendiri, lihatContoh gerbang transitdiGerbang Transit Amazon VPC.

Sumber daya tambahan

- Memahami pola ketahanan dan trade-off(AWSBlog Arsitektur)
- Rencanakan topologi jaringan Anda(AWSKerangka yang Dirancang dengan Baik)
- Opsi Konektivitas Cloud Pribadi Virtual Amazon(AWSWhitepaper)

Contoh: VPC untuk lingkungan pengujian

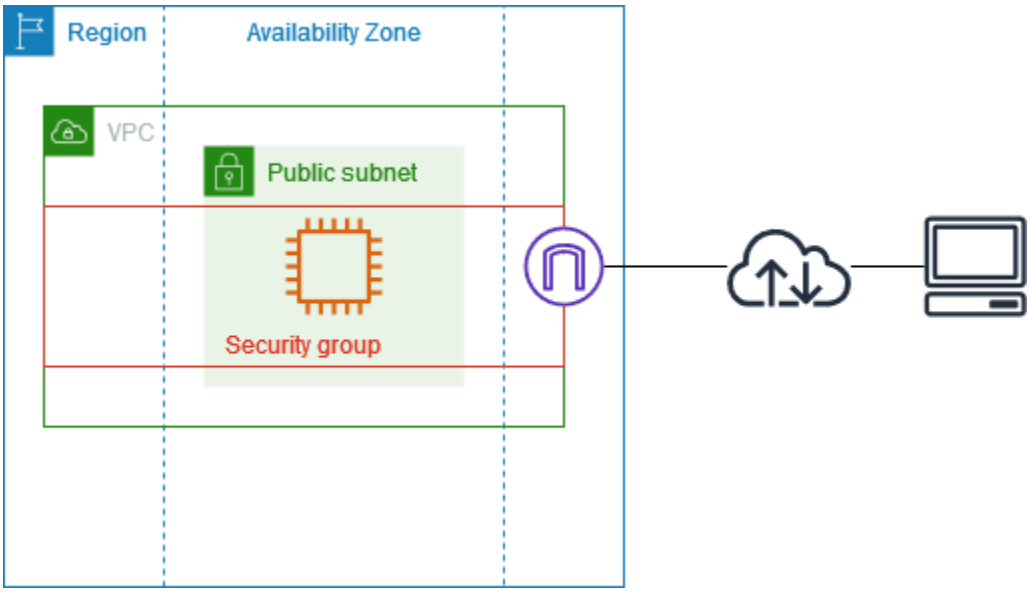
Contoh ini menunjukkan cara membuat VPC yang dapat Anda gunakan sebagai pengembangan atau lingkungan pengujian. Karena VPC ini tidak dimaksudkan untuk digunakan dalam produksi, tidak perlu untuk menyebarkan server Anda di beberapa Availability Zone. Untuk menjaga biaya dan kompleksitasnya tetap rendah, Anda dapat menerapkan server Anda dalam satu Availability Zone.

Daftar Isi

- Men-deploy aplikasi Anda
- Uji konfigurasi Anda
- Bersihkan

Gambaran Umum

Diagram berikut memberikan gambaran umum mengenai sumber daya yang termasuk dalam contoh ini. VPC memiliki subnet publik di Availability Zone tunggal dan gateway internet. Server adalah contoh EC2 yang berjalan di subnet publik. Grup keamanan untuk instans memungkinkan lalu lintas SSH dari komputer Anda sendiri, ditambah lalu lintas lain yang secara khusus diperlukan untuk pengembangan atau aktivitas pengujian Anda.



Perutean

Saat Anda membuat VPC ini dengan menggunakan konsol Amazon VPC, kami membuat tabel rute untuk subnet publik dengan rute lokal dan rute ke gateway internet. Berikut ini adalah contoh tabel rute dengan rute untuk IPv4 dan IPv6. Jika Anda membuat subnet IPv4 saja, bukan subnet tumpukan ganda, tabel rute Anda hanya memiliki rute IPv4.

Tujuan	Target
10.0.0.0/16	lokal
2001:db 8:1234:1 a00: :56	lokal

Tujuan	Target
0.0.0.0/0	*id*
::/0	*id*

Keamanan

Untuk konfigurasi contoh ini, Anda harus membuat grup keamanan untuk instans Anda yang memungkinkan lalu lintas yang dibutuhkan aplikasi Anda. Misalnya, Anda mungkin perlu menambahkan aturan yang memungkinkan lalu lintas SSH dari komputer atau lalu lintas HTTP dari jaringan Anda.

Berikut ini adalah contoh aturan masuk untuk grup keamanan, dengan aturan untuk IPv4 dan IPv6. Jika Anda membuat subnet khusus IPv4, bukan subnet tumpukan ganda, Anda hanya perlu aturan untuk IPv4.

Jalur masuk

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
Rentang alamat IPv4 publik dari jaringan Anda	TCP	22	(Opsional) Memungkinkan akses SSH masuk dari alamat IP IPv4 di jaringan Anda

Sumber	Protokol	Rentang Port	Deskripsi
Rentang alamat IPv6 dari jaringan Anda	TCP	22	(Opsional) Memungkinkan akses SSH masuk dari alamat IP IPv6 di jaringan Anda
Rentang alamat IPv4 publik dari jaringan Anda	TCP	3389	(Opsional) Memungkinkan akses RDP masuk dari alamat IP IPv4 di jaringan Anda
Rentang alamat IPv6 dari jaringan Anda	TCP	3389	(Opsional) Memungkinkan akses RDP masuk dari alamat IP IPv6 di jaringan Anda

Buat VPC

Gunakan prosedur berikut untuk membuat VPC dengan subnet publik di satu Availability Zone. Konfigurasi ini cocok untuk lingkungan pengembangan atau pengujian.

Untuk membuat VPC

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di dasbor, pilih Buat VPC.
3. Agar Sumber Daya dapat dibuat, pilih VPC dan lainnya.
4. Konfigurasikan VPC
    a. Untuk Pembuatan otomatis tag nama, masukkan nama untuk VPC.
    b. Untuk blok CIDR IPv4, Anda dapat menyimpan saran default, atau 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 alamat IPv6, pilih blok CIDR IPv6, blok CIDR IPv6 yang disediakan Amazon.
5. Konfigurasikan subnet
    a. Untuk Jumlah Availability Zone, pilih 1. Anda dapat menyimpan Availability Zone default, atau sebagai alternatif Anda dapat memperluas Sesuaikan AZ 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 blok CIDR Customize subnet dan masukkan blok CIDR. Untuk informasi selengkapnya, lihat the section called “Blok CIDR subnet”.
6. Untuk gateway NAT, pertahankan nilai default, None.
7. Untuk endpoint VPC, pilih None. Endpoint gateway VPC 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.

Men-deploy aplikasi Anda

Ada berbagai cara untuk menyebarkan instans EC2. Misalnya:

- Penuntun instans peluncuran Amazon EC2
- Amazon EC2 Auto Scaling
- AWS CloudFormation
- Amazon Elastic Container Service (Amazon ECS)

Setelah Anda menerapkan instans EC2, Anda dapat terhubung ke instans, menginstal perangkat lunak yang Anda butuhkan untuk aplikasi Anda, dan kemudian membuat gambar untuk penggunaan di future. Untuk informasi selengkapnya, lihat Membuat AMI Linux atau Membuat AMI Windows dalam dokumentasi Amazon EC2. Atau, Anda dapat menggunakan EC2 Image Builder untuk membuat dan mengelola Amazon Machine Image (AMI) Anda.

Uji konfigurasi Anda

Setelah Anda selesai men-deploy aplikasi Anda, Anda dapat mengujinya. Jika Anda tidak dapat terhubung ke instans EC2, 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 lebih lanjut, lihat Panduan Reachability Analyzer.

Bersihkan

Setelah Anda selesai dengan konfigurasi ini, Anda dapat menghapusnya. Sebelum Anda dapat menghapus VPC, Anda harus menghentikan instans Anda. Untuk informasi selengkapnya, lihat the section called “Hapus VPC Anda”.

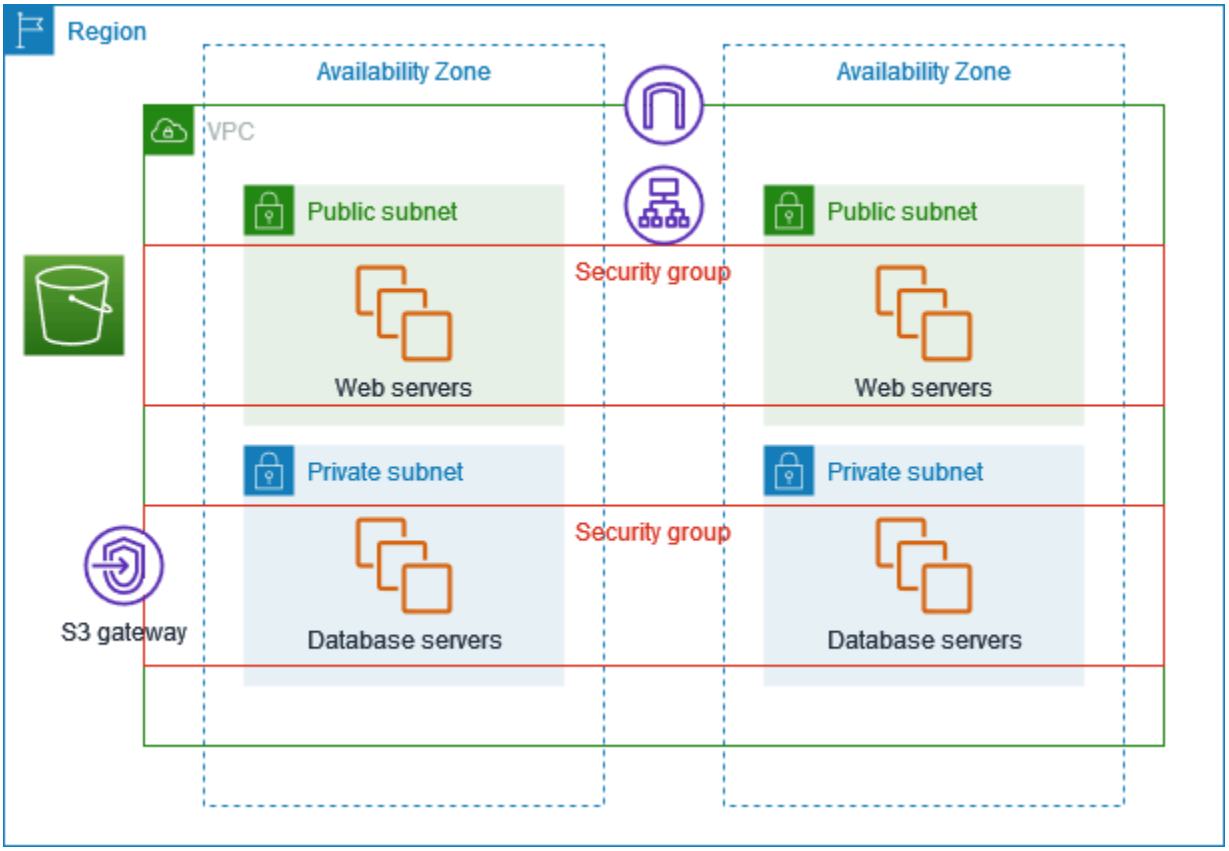
Contoh: VPC untuk server web dan database

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

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 IPv4 dan IPv6. Jika Anda membuat subnet khusus IPv4 alih-alih subnet tumpukan ganda, tabel rute Anda hanya memiliki rute IPv4.

Tujuan	Target
10.0.0.0/16	lokal
2001:db 8:1234:1 a00: :/56	lokal
0.0.0.0/0	*igw-id*
::/0	*igw-id*

Berikut ini adalah contoh tabel rute untuk subnet pribadi, dengan rute lokal untuk IPv4 dan IPv6. Jika Anda membuat subnet khusus IPv4, tabel rute Anda hanya memiliki rute IPv4. Rute terakhir mengirimkan lalu lintas yang ditujukan untuk Amazon S3 ke titik akhir VPC gateway.

Tujuan	Target
10.0.0.0/16	lokal
2001:db 8:1234:1 a00: :/56	lokal
s3-awalan-daftar-id	*s3-gateway-id*

Keamanan

Untuk konfigurasi contoh ini, Anda membuat grup keamanan untuk penyeimbang beban, grup keamanan untuk server web, dan grup keamanan untuk server database.

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.

Jalur masuk

Sumber	Protokol	Rentang Port	Deskripsi
ID grup keamanan untuk penyeimbang beban	TCP	80	Memungkinkan akses HTTP masuk dari penyeimbang beban

Sumber	Protokol	Rentang Port	Deskripsi
ID grup keamanan untuk penyeimbang beban	TCP	443	Memungkinkan akses HTTPS masuk dari penyeimbang beban
Rentang alamat IPv4 publik dari jaringan Anda	TCP	22	(Opsional) Memungkinkan akses SSH masuk dari alamat IP IPv4 di jaringan Anda
Rentang alamat IPv6 jaringan Anda	TCP	22	(Opsional) Memungkinkan akses SSH masuk dari alamat IP IPv6 di jaringan Anda
Rentang alamat IPv4 publik dari jaringan Anda	TCP	3389	(Opsional) Memungkinkan akses RDP masuk dari alamat IP IPv4 di jaringan Anda
Rentang alamat IPv6 jaringan Anda	TCP	3389	(Opsional) Memungkinkan akses RDP masuk dari alamat IP IPv6 di jaringan Anda

Jalur keluar

Tujuan	Protokol	Rentang Port	Deskripsi
ID grup keamanan untuk instance yang menjalankan Microsoft SQL Server	TCP	1433	Memungkinkan akses Microsoft SQL Server keluar ke server database
ID grup keamanan untuk instance yang menjalankan MySQL	TCP	3306	Memungkinkan akses MySQL keluar ke server database

Server basis data

Aturan grup keamanan berikut memungkinkan server database menerima permintaan baca dan tulis dari server web.

Jalur masuk

Sumber	Protokol	Rentang Port	Komentar
ID grup keamanan server web	TCP	1433	Memungkinkan akses Microsoft SQL Server masuk dari server web
ID grup keamanan server web	TCP	3306	Memungkinkan akses MySQL Server masuk dari server web

Jalur keluar

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.

Buat VPC

Gunakan prosedur berikut untuk membuat VPC dengan subnet publik dan subnet pribadi di dua Availability Zones.

Untuk membuat VPC

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di dasbor, pilih Buat VPC.

3. Agar Sumber Daya dapat dibuat, pilih VPC dan lainnya.
4. Konfigurasikan VPC:
   a. Biarkan pembuatan otomatis tag Nama dipilih untuk membuat tag Nama untuk sumber daya VPC atau hapus untuk menyediakan tag Nama Anda sendiri untuk sumber daya VPC.
   b. Untuk blok IPv4 CIDR, Anda dapat menyimpan saran default, atau sebagai alternatif Anda dapat memasukkan blok CIDR yang diperlukan oleh aplikasi atau jaringan Anda. Untuk informasi selengkapnya, lihat the section called “Blok VPC CIDR”.
   c. (Opsional) Jika aplikasi Anda berkomunikasi dengan menggunakan alamat IPv6, pilih blok IPv6 CIDR, blok CIDR IPv6 yang disediakan Amazon.
   d. Pilih opsi Sewa. Opsi ini menentukan apakah instans EC2 yang Anda luncurkan ke VPC akan berjalan pada perangkat keras yang dibagikan dengan perangkat keras lain Akun AWS atau pada perangkat keras yang didedikasikan untuk penggunaan Anda saja. Jika Anda memilih penyewaan VPC yang `Default` akan menjadi, instans EC2 yang diluncurkan ke VPC ini akan menggunakan atribut penyewaan yang ditentukan saat Anda meluncurkan instance. Untuk informasi selengkapnya, lihat Meluncurkan instance menggunakan parameter yang ditentukan 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`
5. Konfigurasikan subnet:
   a. Untuk Jumlah Availability Zone, pilih 2, sehingga Anda dapat meluncurkan instans di dua Availability Zone untuk meningkatkan ketahanan.
   b. Untuk Jumlah subnet publik, pilih 2.
   c. Untuk Jumlah subnet pribadi, pilih 2.
   d. Anda dapat menyimpan blok CIDR default untuk subnet, atau sebagai alternatif Anda dapat memperluas Kustomisasi subnet blok CIDR dan memasukkan blok CIDR. Untuk informasi selengkapnya, lihat the section called “Blok 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.

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 instans EC2 untuk server web Anda. Ada berbagai cara untuk menerapkan instans EC2. Sebagai contoh:

- Wisaya instans peluncuran Amazon EC2
- AWS CloudFormation
- Amazon Elastic Container Service (Amazon ECS)

Untuk meningkatkan ketersediaan, Anda dapat menggunakan Auto Scaling Amazon EC2 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 instans EC2 untuk server database Anda, atau salah satu jenis database kami yang dibuat khusus. Untuk informasi selengkapnya, lihat Database tentang AWS: Cara memilih.

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.

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”.

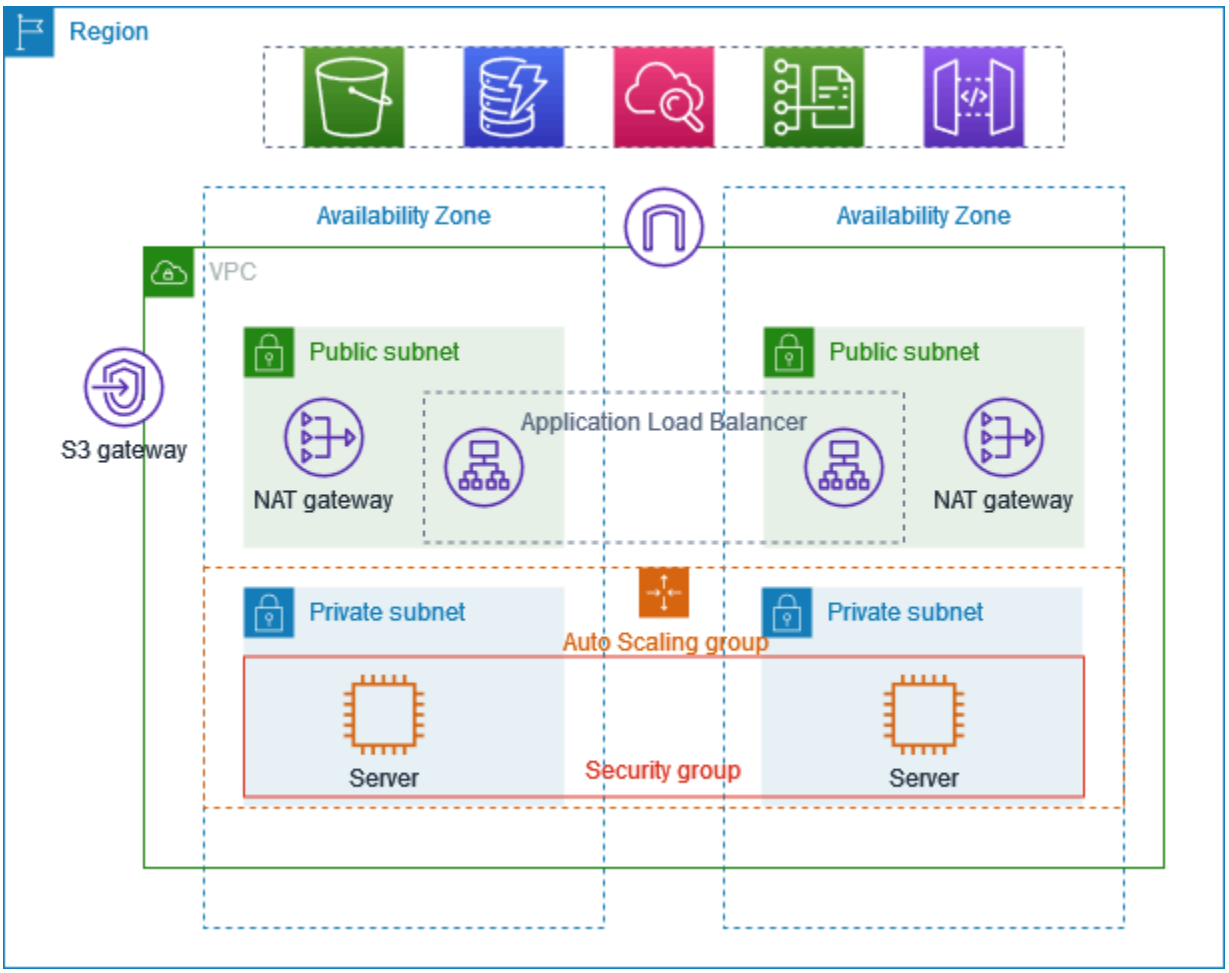
Contoh: VPC dengan server di subnet pribadi dan NAT

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

Diagram berikut memberikan gambaran umum mengenai sumber daya yang disertakan dalam contoh ini. VPC memiliki subnet publik dan subnet pribadi di dua Availability Zone. Setiap subnet publik berisi gateway NAT dan node load balancer. Server berjalan di subnet pribadi, diluncurkan dan diakhiri dengan menggunakan grup Auto Scaling, dan menerima lalu lintas dari penyeimbang muatan. Server dapat terhubung ke internet dengan menggunakan gateway NAT. Server dapat terhubung ke Amazon S3 dengan menggunakan titik akhir gateway VPC.



Perutean

Saat Anda membuat VPC ini dengan menggunakan konsol Amazon VPC, kami membuat tabel rute untuk subnet publik dengan rute lokal dan rute ke gateway internet. Kami juga membuat tabel rute untuk subnet pribadi dengan rute lokal, dan rute ke gateway NAT, gateway internet khusus egres, dan titik akhir gateway VPC.

Berikut ini adalah contoh tabel rute untuk subnet publik, dengan rute untuk IPv4 dan IPv6. Jika Anda membuat subnet khusus IPv4, bukan subnet tumpukan ganda, tabel rute Anda hanya mencakup rute IPv4.

Tujuan	Target
10.0.0.0/16	lokal
2001:db 8:1234:1 a00: :/56	lokal

Tujuan	Target
0.0.0.0/0	*id*
::/0	*id*

Berikut ini adalah contoh tabel rute untuk salah satu subnet pribadi, dengan rute untuk IPv4 dan IPv6. Jika Anda membuat subnet IPv4 saja, tabel rute hanya mencakup rute IPv4. Rute terakhir mengirimkan lalu lintas yang ditujukan untuk Amazon S3 ke titik akhir gateway VPC.

Tujuan	Target
10.0.0.0/16	lokal
2001:db 8:1234:1 a00: :/56	lokal
0.0.0.0/0	*nat-gateway-id*
::/0	*eigw-id*
s3-prefix-list-id	*s3-gateway-id*

Keamanan

Berikut ini adalah contoh aturan yang mungkin Anda buat untuk grup keamanan yang Anda kaitkan dengan server Anda. Grup keamanan harus mengizinkan lalu lintas dari penyeimbang beban melalui port dan protokol listener. Ini juga harus mengizinkan lalu lintas pemeriksaan kondisi.

Jalur masuk

Sumber	Protokol	Rentang Port	Comments
ID grup keamanan penyeimbang beban	*protokol pendengar*	*port pendengar*	Mengizinkan lalu lintas masuk dari penyeimbang beban di port listener

Sumber	Protokol	Rentang Port	Comments
ID grup keamanan penyeimbang beban	*protokol pemeriksaan kesehatan*	*port pemeriksaan kesehatan*	Memungkinkan lalu lintas pemeriksaan kesehatan masuk dari penyeimbang muatan

Buat VPC

Gunakan prosedur berikut untuk membuat VPC dengan subnet publik dan subnet privat di dua Availability Zone, dan gateway NAT di setiap Availability Zone.

Untuk membuat VPC

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di dasbor, pilih Buat VPC.
3. Agar Sumber Daya dapat dibuat, pilih VPC dan lainnya.
4. Konfigurasikan VPC
    a. Untuk Pembuatan otomatis tag nama, masukkan nama untuk VPC.
    b. Untuk blok CIDR IPv4, Anda dapat menyimpan saran default, atau sebagai alternatif Anda dapat memasukkan blok CIDR yang diperlukan oleh aplikasi atau jaringan Anda.
    c. Jika aplikasi Anda berkomunikasi dengan menggunakan alamat IPv6, pilih Blok CIDR IPv6, Blok CIDR IPv6 yang disediakan Amazon.
5. Konfigurasikan subnet
    a. Untuk Jumlah Availability Zone, pilih 2, sehingga Anda dapat meluncurkan instans 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 blok CIDR Customize subnet dan masukkan 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 alamat IPv6, untuk gateway internet Egress saja, pilih Ya.
8. Untuk endpoint 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 menyimpan default jika Anda mungkin menggunakan bucket S3 di masa future. Jika Anda memilih Tidak Ada, Anda selalu dapat menambahkan titik akhir gateway VPC nanti.
9. Untuk opsi DNS, hapus Aktifkan nama host DNS.
10. Pilih Buat VPC.

Men-deploy aplikasi Anda

Idealnya, Anda telah selesai menguji server Anda di lingkungan pengembangan atau pengujian, dan membuat skrip atau gambar yang akan Anda gunakan untuk menerapkan aplikasi Anda dalam produksi.

Anda dapat menggunakan Amazon EC2 Auto Scaling untuk menerapkan server di beberapa Availability Zone dan mempertahankan kapasitas server minimum yang diperlukan oleh aplikasi Anda.

Untuk meluncurkan instans dengan menggunakan grup Auto Scaling

1. Buat template peluncuran untuk menentukan informasi konfigurasi yang diperlukan untuk meluncurkan instans EC2 Anda dengan menggunakan Amazon EC2 Auto Scaling. Untukstep-by-step petunjuk arah, lihat Buat templat peluncuran untuk grup Auto Scaling Amazon EC2 Auto Scaling Panduan Pengguna Auto Scaling Amazon EC2.
2. Buat grup Auto Scaling, yang merupakan kumpulan instans EC2 dengan ukuran minimum, maksimum, dan diinginkan. Untukstep-by-step petunjuk arah, lihat Buat grup Auto Scaling Auto Scaling Amazon EC2 Auto Scaling Panduan Pengguna Auto Scaling Amazon EC2.
3. Buat penyeimbang beban, yang mendistribusikan lalu lintas secara merata di seluruh instans di grup Auto Scaling, dan melampirkan load balancer ke grup Auto Scaling Anda. Untuk informasi selengkapnya, lihat Panduan Pengguna Elastic Load Balancing dan Gunakan Elastic Load Balancing dalam Panduan Pengguna Auto Scaling Amazon EC2 Auto Scaling.

Uji konfigurasi Anda

Setelah Anda selesai men-deploy aplikasi, 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.

Bersihkan

Setelah Anda selesai dengan konfigurasi ini, Anda dapat menghapusnya. Sebelum Anda dapat menghapus VPC, Anda harus menghapus grup Auto Scaling, menghentikan instans Anda, menghapus gateway NAT, dan menghapus load balancer. Untuk informasi selengkapnya, lihat the section called “Hapus VPC Anda”.

Kuota Amazon VPC

Tabel berikut mencantumkan kuota, yang 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
VPC per Wilayah	5	Ya	Penambahan kuota ini menambah kuota pada gateway internet per Wilayah dengan jumlah yang sama. Anda dapat meningkatkan batas ini sehingga Anda dapat memiliki ratusan VPC per Wilayah.
Subnet per VPC	200	Ya	
Blok CIDR IPv4 per VPC	5	Ya (hingga 50)	Blok CIDR primer ini dan semua blok CIDR sekunder dihitung terhadap kuota ini.
blok CIDR IPv6 per VPC	5	Ya (hingga 50)	Jumlah CIDR yang dapat Anda alokasikan ke satu VPC.

DNS

Setiap instans EC2 dapat mengirim 1024 paket per detik per antarmuka jaringan ke Route 53 Resolver (khususnya alamat.2, seperti 10.0.0.2 dan 169.254.169.253). Kuota ini tidak dapat dinaikkan jumlahnya. Jumlah kueri DNS per detik yang didukung oleh Route 53 Resolver bervariasi 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 VPC individual dan Akun AWS VPC bersama.
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 VPC per Region. Anda dapat melampirkan hanya satu gateway internet egress untuk satu VPC pada suatu waktu.
Gateway internet per Wilayah	5	Ya	Untuk meningkatkan kuota ini, tingkatkan kuota VPC per Region.

Nama	Default	Dapat disesuaikan	Komentar
			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 dipending,, active dan negara bagian. deleting
Kuota alamat IP pribadi per gateway NAT	8	Tidak	
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 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

Nama	Default	Dapat disesuaikan	Komentar
			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.

ACL jaringan

Nama	Default	Dapat disesuaikan	Komentar
ACL jaringan per VPC	200	Ya	Anda dapat mengaitkan satu jaringan ACL untuk satu atau lebih subnet di VPC.

Nama	Default	Dapat disesuaikan	Komentar
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 VPC individual dan Akun AWS VPC bersama. Batas ini diberlakukan per Availability Zone (AZ). Jika, misalnya, antarmuka jaringan dalam tiga AZ, masing-masing AZ akan memiliki batas 5.000 dan Wilayah akan memiliki batas 15.000.

Tabel rute

Nama	Default	Dapat disesuaikan	Komentar
Tabel rute per VPC	200	Ya	Tabel rute utama dihitung terhadap kuota ini. Perhatikan bahwa jika Anda meminta 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 disebarkan)	50	Ya	Anda dapat menambah kuota ini hingga maksimum 1.000; namun, performa jaringan mungkin terkena dampaknya. Kuota ini diberlakukan secara terpisah untuk rute IPv4 dan rute IPv6. Jika Anda memiliki lebih dari 125 rute, kami sarankan Anda memberikan nomor halaman panggilan untuk menggambarkan tabel rute Anda untuk performa yang lebih baik.
Rute yang disebarkan per tabel rute	100	Tidak	Jika Anda memerlukan prefiks tambahan, iklankan rute default.

Grup keamanan

Nama	Default	Dapat disesuaikan	Komentar
Grup keamanan VPC per Wilayah	2.500	Ya	Kuota ini berlaku untuk VPC individual dan Akun AWS VPC bersama. Jika Anda menambah kuota ini hingga lebih dari 5.000 grup keamanan di Wilayah, kami sarankan agar Anda melakukan pemberian nomor panggilan untuk menjelaskan grup keamanan Anda agar memiliki performa yang lebih baik.
Aturan masuk atau keluar per grup keamanan	60	Ya	Kuota ini diberlakukan secara terpisah untuk aturan masuk dan keluar. Untuk akun dengan kuota default 60 aturan, grup keamanan dapat memiliki 60 aturan masuk dan 60 aturan keluar. Selain itu, kuota ini diberlakukan secara terpisah untuk aturan IPv4 dan aturan IPv6. Untuk akun dengan kuota default 60 aturan, grup keamanan dapat memiliki 60 aturan masuk untuk lalu lintas IPv4 dan 60 aturan masuk untuk lalu lintas IPv6. Untuk informasi selengkapnya, lihat the section called “Ukuran grup keamanan”. Perubahan kuota berlaku untuk aturan masuk dan keluar. Kuota ini yang dikalikan dengan kuota untuk grup keamanan per antarmuka jaringan tidak dapat lebih dari 1.000.

Nama	Default	Dapat disesuaikan	Komentar
Grup keamanan per antarmuka jaringan	5	Ya (hingga 16)	Kuota ini dikalikan dengan kuota untuk aturan per grup keamanan tidak boleh melebihi 1.000.

Pembagian VPC

Semua kuota VPC standar berlaku untuk 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 CIDR 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 VPC peered intra-wilayahnya. VPC yang diintip di berbagai Wilayah tidak berkontribusi pada nomor ini.

Amazon EC2 API throttling

Untuk informasi selengkapnya tentang Amazon EC2 throttling, lihat Throttling Permintaan API dalam Referensi API 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
- Kuota Site-to-Site VPN dalam Panduan Pengguna AWS Site-to-Site VPN
- Kuota Pencerminan Lalu Lintas di Panduan Pencerminan 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
Waktu sewa yang disukai IPv6	Anda sekarang dapat memilih seberapa sering instance yang berjalan dengan IPv6 yang ditetapkan untuk itu melewati perpanjangan sewa DHCPv6.	Februari 20, 2024
AWS pembaruan kebijakan terkelola	Amazon VPC memperbarui AmazonVPCFullAccess dan AmazonVPCReadOnlyAccess mengelola kebijakan.	Februari 8, 2024
AWS pembaruan kebijakan terkelola	Amazon VPC memperbar ui kebijakan AmazonVPC CrossAccountNetworkInterfac eOperations terkelola.	25 September 2023
EC2-Classic tidak digunakan lagi	Dengan EC2-Classic, instans EC2 berjalan dalam jaringan datar tunggal yang dibagikan dengan pelanggan lain. Amazon VPC menggantikan EC2-Classic. Dengan Amazon VPC, instans Anda berjalan di cloud pribadi virtual (VPC) yang secara logis terisolasi untuk Anda. Akun AWS	31 Juli 2023
Tambahkan alamat IPv4 sekunder ke gateway NAT	Anda dapat menambahkan alamat IPv4 pribadi sekunder ke gateway NAT publik dan pribadi. Alamat IPv4 sekunder	31 Januari 2023

	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.	
Menyelaraskan dengan praktik terbaik IAM	Panduan yang diperbarui untuk menyelaraskan dengan praktik terbaik IAM. Untuk informasi selengkapnya, 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
Konfigurasi router gateway default IPv6	Tiga alamat IPv6 sekarang dicadangkan untuk digunakan oleh router VPC default.	11 November 2022
Mentransfer alamat IP Elastis	Anda sekarang dapat mentransfer alamat IP 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.	September 8, 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 blok CIDR IPv6	Anda dapat mengaitkan hingga lima blok CIDR IPv6 ke VPC.	12 Mei 2022
Reorganisasi	Reorganisasi umum Panduan Pengguna Amazon Virtual Private Cloud ini.	Januari 2, 2022
NAT gateway IPv6 ke IPv4	Gateway NAT mendukung terjemahan alamat jaringan dari IPv6 ke IPv4, yang dikenal sebagai NAT64.	24 November 2021
Subnet khusus IPv6 di VPC	Anda dapat membuat subnet khusus IPv6 di mana Anda dapat meluncurkan instans EC2 khusus IPv6.	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 Global Amazon EC2	Amazon EC2 Global View memungkinkan Anda melihat VPC, 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 blok IPv4 atau IPv6 CIDR dari subnet di VPC Anda.	Agustus 30, 2021
ID sumber daya dan dukungan penandaan untuk aturan grup keamanan	Anda dapat merujuk ke aturan grup keamanan berdasarkan ID sumber daya. Anda dapat menambahkan tanda ke aturan grup keamanan.	7 Juli 2021

Gateway NAT pribadi	Anda dapat menggunakan gateway NAT pribadi untuk komunikasi pribadi outbound-only antar VPC atau antara VPC dan jaringan on-premise Anda.	10 Juni 2021
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
Peningkatan 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 mengkonfigurasi grup perbatasan jaringan untuk VPC Anda dari Amazon Virtual Private Cloud Console.	22 Januari 2020
Nama DNS pribadi	Anda dapat mengakses layanan AWS PrivateLink berbasis pribadi dari dalam VPC Anda menggunakan nama DNS Pribadi.	6 Januari 2020
Tabel rute gateway	Anda dapat mengaitkan tabel rute dengan gateway dan rute masuk lalu lintas VPC rute inbound ke antarmuka jaringan tertentu di VPC Anda.	3 Desember 2019
Peningkatan log aliran	Anda dapat menentukan format kustom untuk log alur Anda dan memilih bidang mana yang akan dikembalikan dalam catatan log alur.	11 September 2019
Berbagi VPC	Anda dapat berbagi subnet yang berada di VPC yang sama dengan beberapa akun di organisasi yang 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 menambahk an deskripsi ke aturan grup keamanan.	31 Agustus 2017
Blok CIDR IPv4 sekunder untuk VPC Anda	Anda dapat menambahkan beberapa blok CIDR IPv4 untuk VPC Anda.	29 Agustus 2017
Pulihkan alamat IP Elastis	Jika Anda merilis alamat IP Elastis Anda, Anda dapat memulihkannya.	11 Agustus 2017
Buat VPC default	Anda dapat membuat VPC default baru jika Anda menghapus VPC default yang ada.	27 Juli 2017
Dukungan IPv6	Anda dapat mengaitkan sebuah blok CIDR IPv6 dengan VPC Anda dan menetapkan alamat IPv6 ke sumber daya di VPC Anda.	1 Desember 2016
Dukungan resolusi DNS untuk rentang alamat IP non-RFC 1918	Server DNS Amazon sekarang dapat mengubah nama host DNS pribadi ke alamat IP pribadi untuk semua ruang alamat.	24 Oktober 2016

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, yang memungkinkan komunikasi antara instans EC2-Classic dan instans di VPC Anda menggunakan alamat IP privat.	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 mengaktif kan nama host DNS.	11 Maret 2013
VPC Dimana-mana	Menambahkan dukungan untuk VPC di lima AWS Wilayah, VPC di beberapa Availability Zone, beberapa VPC per AWS akun, dan beberapa koneksi VPN per VPC.	3 Agustus 2011
Instans Khusus	Instans Khusus adalah instans Amazon EC2 yang diluncurk an dalam VPC Anda yang menjalankan perangkat keras yang didedikasikan untuk satu pelanggan.	27 Maret 2011

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.