AWS Transit Gateway

Amazon VPC

Amazon VPC: AWS Transit Gateway

Table of Contents

Apa itu AWS Transit Gateway untuk Amazon VPC?

AWS Transit Gateway adalah hub transit jaringan yang digunakan untuk menghubungkan virtual private cloud (VPC) dan jaringan lokal. Saat infrastruktur cloud Anda berkembang secara global, peering antar wilayah menghubungkan gateway transit bersama-sama menggunakan Infrastruktur Global. AWS Semua lalu lintas jaringan antara pusat AWS data secara otomatis dienkripsi pada lapisan fisik.

Untuk informasi selengkapnya, lihat web AWS Transit Gateway.

Konsep gerbang transit

Berikut ini adalah konsep kunci untuk gateway transit:

- Lampiran - Anda dapat melampirkan yang berikut:
  - Satu atau lebih VPC
  - Alat SD-WAN/third-party jaringan Connect
  - AWS Direct Connect Gerbang
  - Koneksi mengintip dengan gateway transit lain
  - Koneksi VPN ke gateway transit
  - Konsentrator VPN ke gateway transit
  - Titik akhir Client VPN ke gateway transit
  - Lampiran fungsi jaringan. Untuk informasi selengkapnya, lihat the section called “Lampiran fungsi jaringan”.
- Transit Gateway Maximum Transmission Unit (MTU) — Unit transmisi maksimum (MTU) dari koneksi jaringan adalah ukuran, dalam byte, dari paket terbesar yang diizinkan yang dapat dilewatkan melalui koneksi. Semakin besar MTU suatu koneksi, semakin banyak data yang dapat dilewatkan dalam satu paket tunggal. Gateway transit mendukung MTU 8500 byte untuk lalu lintas antara VPC, Direct Connect Transit Gateway Connect, dan lampiran peering (lampiran peering intra-wilayah, antar-wilayah, dan Cloud WAN). Lalu lintas melalui koneksi VPN dapat memiliki MTU 1500 byte.
- Kontrol enkripsi — Gateway transit dapat dikonfigurasi untuk mendukung kontrol Enkripsi, yang memberlakukan enkripsi dalam transit untuk semua lalu lintas pada VPC yang terpasang pada gateway transit. Ketika kontrol Enkripsi diaktifkan, gateway transit dapat dilampirkan ke VPC

dengan kontrol Enkripsi diberlakukan. Fitur ini memastikan bahwa semua lalu lintas yang mengalir melalui gateway transit dienkripsi, memberikan keamanan yang ditingkatkan untuk komunikasi jaringan Anda.

- Tabel rute gerbang transit — Gateway transit memiliki tabel rute default dan secara opsional dapat memiliki tabel rute tambahan. Tabel rute mencakup rute dinamis dan statis yang menentukan hop berikutnya berdasarkan alamat IP tujuan paket. Target rute ini bisa berupa lampiran gateway transit apa pun. Secara default, lampiran gateway transit dikaitkan dengan tabel rute gateway transit default.
- Asosiasi - Setiap lampiran dikaitkan dengan tepat satu tabel rute. Setiap tabel rute dapat dikaitkan dengan nol hingga banyak lampiran.
- Propagasi rute — VPC, koneksi VPN, atau gateway Direct Connect dapat secara dinamis menyebarkan rute ke tabel rute gateway transit. Dengan lampiran Connect, rute disebarkan ke tabel rute gateway transit secara default. Dengan VPC, Anda harus membuat rute statis untuk mengirim lalu lintas ke gateway transit. Dengan koneksi VPN, rute disebarkan dari gateway transit ke router lokal Anda menggunakan Border Gateway Protocol (BGP). Dengan gateway Direct Connect, awalan yang diizinkan berasal dari router lokal Anda menggunakan BGP. Dengan lampiran peering, Anda harus membuat rute statis di tabel rute gateway transit untuk menunjuk ke lampiran peering.

Cara memulai dengan gateway transit

Gunakan sumber daya berikut untuk membantu Anda membuat dan menggunakan gateway transit.

- Cara kerja gateway transit
- Memulai dengan gateway transit
- Praktik terbaik desain

Bekerja dengan gateway transit

Anda dapat membuat, mengakses, dan mengelola gateway transit menggunakan salah satu antarmuka berikut:

- Konsol Manajemen AWS— Menyediakan antarmuka web yang dapat Anda gunakan untuk mengakses gateway transit Anda.

- AWS Command Line Interface (AWS CLI) - Menyediakan perintah untuk serangkaian AWS layanan yang luas, termasuk Amazon VPC, dan didukung di Windows, macOS, dan Linux. Untuk informasi selengkapnya, lihat AWS Command Line Interface.
- AWS SDK — Menyediakan operasi API khusus bahasa dan menangani banyak detail koneksi, seperti menghitung tanda tangan, menangani percobaan ulang permintaan, dan menangani kesalahan. Untuk informasi selengkapnya, lihat AWS SDK.
- Kueri API — Menyediakan tindakan API tingkat rendah yang Anda hubungi menggunakan permintaan HTTPS. Menggunakan Query API adalah cara paling langsung untuk mengakses Amazon VPC, tetapi aplikasi Anda harus menangani detail tingkat rendah seperti membuat hash untuk menandatangani permintaan, dan menangani kesalahan. Untuk informasi selengkapnya, lihat Referensi API Amazon EC2.

Harga

Anda dikenakan biaya per jam untuk setiap lampiran pada gateway transit, dan Anda dikenakan biaya untuk jumlah lalu lintas yang diproses di gateway transit. Secara default, biaya pemrosesan data dialokasikan ke akun yang memiliki lampiran sumber. Anda dapat menggunakan alokasi biaya fleksibel untuk menyesuaikan bagaimana biaya ini dialokasikan berdasarkan kebutuhan organisasi Anda. Untuk informasi selengkapnya, lihat harga AWS Transit Gateway danAlokasi biaya yang fleksibel.

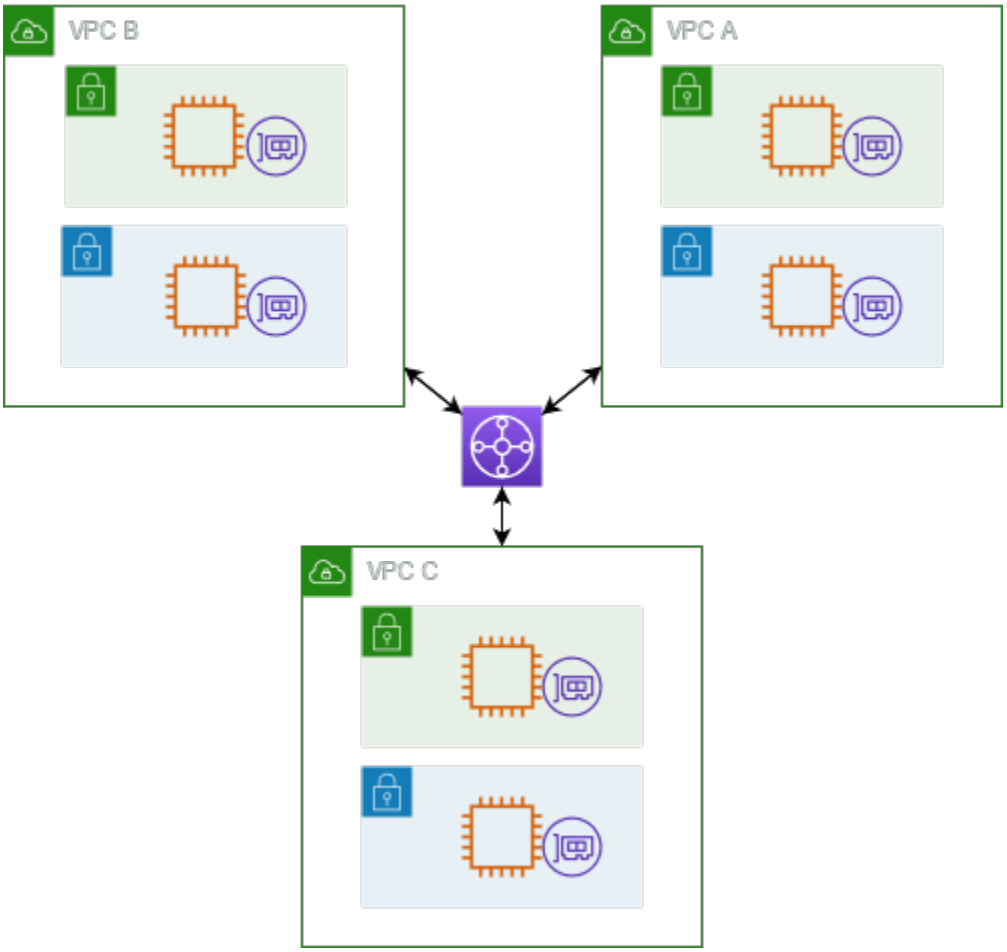
Cara kerja AWS Transit Gateway

Di AWS Transit Gateway, gateway transit bertindak sebagai router virtual Regional untuk lalu lintas yang mengalir antara virtual private cloud (VPC) dan jaringan lokal. Gateway transit menskalakan secara elastis berdasarkan volume lalu lintas jaringan. Routing melalui gateway transit beroperasi pada lapisan 3, di mana paket dikirim ke lampiran next-hop tertentu, berdasarkan alamat IP tujuan.

Topik

Contoh diagram arsitektur

Diagram berikut menunjukkan gateway transit dengan tiga lampiran VPC. Tabel rute untuk masing-masing VPC ini mencakup rute lokal dan rute yang mengirim lalu lintas yang ditujukan untuk dua VPC lainnya ke gateway transit.



Berikut ini adalah contoh tabel rute gateway transit default untuk lampiran yang ditunjukkan pada diagram sebelumnya. Blok CIDR untuk setiap VPC merambat ke tabel rute. Oleh karena itu, setiap lampiran dapat merutekan paket ke dua lampiran lainnya.

Destinasi	Target	Jenis rute
VPC A CIDR	*Attachment for VPC A*	diperbanyak
VPC B CIDR	*Attachment for VPC B*	diperbanyak
VPC C CIDR	*Attachment for VPC C*	diperbanyak

Lampiran sumber daya

Lampiran gateway transit adalah sumber dan tujuan paket. Anda dapat melampirkan sumber daya berikut ke gateway transit Anda:

- Satu atau lebih VPC AWS Transit Gateway menggunakan elastic network interface dalam subnet VPC, yang kemudian digunakan oleh gateway transit untuk merutekan lalu lintas ke dan dari subnet yang dipilih. Anda harus memiliki setidaknya satu subnet untuk setiap Availability Zone, yang kemudian memungkinkan lalu lintas untuk mencapai sumber daya di setiap subnet zona itu. Selama pembuatan lampiran, sumber daya dalam Availability Zone tertentu dapat mencapai gateway transit hanya jika subnet diaktifkan dalam zona yang sama. Jika tabel rute subnet menyertakan rute ke gateway transit, lalu lintas hanya diteruskan ke gateway transit jika gateway transit memiliki lampiran di subnet dari Availability Zone yang sama.
- Satu atau lebih koneksi VPN
- Satu atau lebih Konsentrator VPN
- Satu atau lebih AWS Direct Connect gateway
- Satu atau beberapa lampiran Transit Gateway Connect
- Satu atau lebih koneksi peering gateway transit

Perutean Multipath Biaya Sama

AWS Transit Gateway mendukung perutean Equal Cost Multipath (ECMP) untuk sebagian besar lampiran. Untuk lampiran VPN, Anda dapat mengaktifkan atau menonaktifkan dukungan ECMP menggunakan konsol saat membuat atau memodifikasi gateway transit. Untuk semua jenis lampiran lainnya, pembatasan ECMP berikut berlaku:

- VPC - VPC tidak mendukung ECMP karena blok CIDR tidak dapat tumpang tindih. Misalnya, Anda tidak dapat melampirkan VPC dengan CIDR 10.1.0. 0/16 dengan VPC kedua menggunakan CIDR yang sama ke gateway transit, dan kemudian mengatur perutean untuk memuat keseimbangan lalu lintas di antara mereka.
- VPN - Ketika opsi dukungan ECMP VPN dinonaktifkan, gateway transit menggunakan metrik internal untuk menentukan jalur yang disukai jika terjadi awalan yang sama di beberapa jalur. Untuk informasi selengkapnya tentang mengaktifkan atau menonaktifkan ECMP untuk lampiran VPN, lihat. the section called “Transit gateway”
- AWS Transit Gateway Connect - AWS Transit Gateway Connect attachment secara otomatis mendukung ECMP.
- AWS Direct Connect AWS Direct Connect Gateway - Lampiran Gateway secara otomatis mendukung ECMP di beberapa lampiran Direct Connect Gateway ketika awalan jaringan, panjang awalan, dan AS_PATH persis sama.

- Transit gateway peering - Transit gateway peering tidak mendukung ECMP karena tidak mendukung perutean dinamis dan Anda juga tidak dapat mengonfigurasi rute statis yang sama terhadap dua target yang berbeda.
- Konsentrator VPN - Konsentrator VPN tidak mendukung ECMP.

> **Note**
>
> - BGP Multipath AS-Path Relax tidak didukung, jadi Anda tidak dapat menggunakan ECMP melalui Nomor Sistem Otonomi (ASN) yang berbeda.
> - ECMP tidak didukung antara jenis lampiran yang berbeda. Misalnya, Anda tidak dapat mengaktifkan ECMP antara VPN dan lampiran VPC. Sebaliknya, rute gateway transit dievaluasi dan lalu lintas diarahkan sesuai dengan rute yang dievaluasi. Untuk informasi selengkapnya, lihat the section called “Urutan evaluasi rute”.
> - Gateway Direct Connect tunggal mendukung ECMP di beberapa antarmuka virtual transit. Oleh karena itu, kami menyarankan Anda mengatur dan menggunakan hanya satu gateway Direct Connect dan untuk tidak mengatur dan menggunakan beberapa gateway untuk memanfaatkan ECMP. Untuk informasi selengkapnya tentang gateway Direct Connect dan antarmuka virtual publik, lihat Bagaimana cara mengatur koneksi atau Active/Active Direct Active/Passive Connect AWS dari antarmuka virtual publik? .

Zona Ketersediaan

Saat Anda melampirkan VPC ke gateway transit, Anda harus mengaktifkan satu atau beberapa Availability Zone untuk digunakan oleh gateway transit untuk merutekan lalu lintas ke sumber daya di subnet VPC. Untuk mengaktifkan setiap Availability Zone, Anda menentukan persis satu subnet. Gateway transit menempatkan antarmuka jaringan di subnet itu menggunakan satu alamat IP dari subnet. Setelah Anda mengaktifkan Availability Zone dengan menentukan subnet, lalu lintas dapat dialihkan ke semua subnet di Availability Zone tersebut, bukan hanya yang Anda tentukan. Namun, hanya sumber daya yang berada di Availability Zones di mana ada lampiran gateway transit yang dapat mencapai gateway transit.

Jika lalu lintas bersumber dari Availability Zone dimana lampiran tujuan tidak ada, AWS Transit Gateway akan secara internal merutekan lalu lintas tersebut ke Availability Zone acak di mana lampiran tersebut ada. Tidak ada biaya gerbang transit tambahan untuk jenis lalu lintas Zona Ketersediaan Lintas ini.

Kami menyarankan Anda mengaktifkan beberapa Availability Zone untuk memastikan ketersediaan.

Menggunakan dukungan mode alat

Jika Anda berencana untuk mengonfigurasi alat jaringan stateful di VPC, Anda dapat mengaktifkan dukungan mode alat untuk lampiran VPC tempat alat berada. Ini memastikan bahwa gateway transit menggunakan Availability Zone yang sama untuk lampiran VPC tersebut selama masa arus lalu lintas antara sumber dan tujuan. Ini juga memungkinkan gateway transit untuk mengirim lalu lintas ke Availability Zone apa pun di VPC, selama ada asosiasi subnet di zona itu. Untuk informasi selengkapnya, lihat Contoh: Peralatan di VPC layanan bersama.

Perutean

Gateway transit Anda merutekan paket IPv4 dan IPv6 di antara lampiran menggunakan tabel rute gateway transit. Anda dapat mengonfigurasi tabel rute ini untuk menyebarkan rute dari tabel rute untuk VPC terlampir, koneksi VPN, dan gateway Direct Connect. Anda juga dapat menambahkan rute statis ke tabel rute gateway transit. Ketika sebuah paket berasal dari satu lampiran, itu dirutekan ke lampiran lain menggunakan rute yang cocok dengan alamat IP tujuan.

Untuk lampiran peering gateway transit, hanya rute statis yang didukung.

Topik perutean

- Tabel rute
- Asosiasi tabel rute
- Perbanyakan rute
- Rute untuk lampiran peering
- Urutan evaluasi rute

Tabel rute

Gateway transit Anda secara otomatis dilengkapi dengan tabel rute default. Secara default, tabel rute ini adalah tabel rute asosiasi default dan tabel rute propagasi default. Jika Anda menonaktifkan propagasi rute dan asosiasi tabel rute, AWS tidak akan membuat tabel rute default untuk gateway transit. Namun, jika propagasi rute atau asosiasi tabel rute diaktifkan, AWS maka buat tabel rute default.

Anda dapat membuat tabel rute tambahan untuk gateway transit Anda. Ini memungkinkan Anda untuk mengisolasi subset lampiran. Setiap lampiran dapat dikaitkan dengan satu tabel rute. Lampiran dapat menyebarkan rutenya ke satu atau beberapa tabel rute.

Anda dapat membuat rute blackhole di tabel rute gateway transit Anda yang menurunkan lalu lintas yang cocok dengan rute.

Saat Anda melampirkan VPC ke gateway transit, Anda harus menambahkan rute ke tabel rute subnet Anda agar lalu lintas dapat dirutekan melalui gateway transit. Untuk informasi selengkapnya, lihat Perutean untuk Gateway Transit di Panduan Pengguna Amazon VPC.

Asosiasi tabel rute

Anda dapat mengaitkan lampiran gateway transit dengan satu tabel rute. Setiap tabel rute dapat dikaitkan dengan nol hingga banyak lampiran dan dapat meneruskan paket ke lampiran lainnya.

Perbanyakan rute

Setiap lampiran dilengkapi dengan rute yang dapat dipasang di satu atau lebih tabel rute gateway transit. Ketika lampiran disebarkan ke tabel rute gateway transit, rute ini dipasang di tabel rute. Anda tidak dapat memfilter pada rute yang diiklankan.

Untuk lampiran VPC, blok CIDR dari VPC disebarkan ke tabel rute gateway transit.

Saat perutean dinamis digunakan dengan lampiran VPN, lampiran VPN Concentrator, atau lampiran gateway Direct Connect, Anda dapat menyebarkan rute yang dipelajari dari router lokal melalui BGP ke salah satu tabel rute gateway transit.

Ketika perutean dinamis digunakan dengan lampiran VPN atau lampiran Konsentrator VPN, rute dalam tabel rute yang terkait dengan lampiran VPN atau lampiran Konsentrator VPN diiklankan ke gateway pelanggan melalui BGP.

Untuk lampiran Connect, rute dalam tabel rute yang terkait dengan lampiran Connect diiklankan ke peralatan virtual pihak ketiga, seperti SD-WAN peralatan, yang berjalan dalam VPC melalui BGP.

Untuk lampiran gateway Direct Connect, interaksi awalan yang diizinkan mengontrol rute mana yang diiklankan ke jaringan pelanggan. AWS

Ketika rute statis dan rute yang disebarkan memiliki tujuan yang sama, rute statis memiliki prioritas yang lebih tinggi, sehingga rute yang disebarkan tidak termasuk dalam tabel rute. Jika Anda menghapus rute statis, rute propagasi yang tumpang tindih disertakan dalam tabel rute.

Rute untuk lampiran peering

Anda dapat mengintip dua gateway transit, dan mengarahkan lalu lintas di antara mereka. Untuk melakukan ini, Anda membuat lampiran peering pada gateway transit Anda, dan menentukan gateway transit peer yang digunakan untuk membuat koneksi peering. Anda kemudian membuat rute statis di tabel rute gateway transit Anda untuk merutekan lalu lintas ke lampiran peering gateway transit. Lalu lintas yang diarahkan ke gateway peer transit kemudian dapat diarahkan ke lampiran VPC dan VPN untuk gateway peer transit.

Untuk informasi selengkapnya, lihat Contoh: Gateway transit peered.

Urutan evaluasi rute

Rute gateway transit dievaluasi dengan urutan sebagai berikut:

- Rute paling spesifik untuk alamat tujuan.
- Untuk rute dengan CIDR yang sama, tetapi dari jenis lampiran yang berbeda, prioritas rute adalah sebagai berikut:
  - Rute statis (misalnya, rute statis Site-to-Site VPN)
  - Daftar awalan rute referensi
  - VPC-propagated rute
  - Rute yang disebarkan oleh gateway Direct Connect
  - Connect-propagated Rute Transit Gateway
  - Site-to-Site VPN melalui Connect-propagated rute Langsung pribadi
  - Site-to-Site VPN-propagated rute
  - Site-to-Site VPN-Concentrator rute yang diperbanyak
  - Rute yang disebarkan oleh Client VPN
  - Rute yang disebarkan oleh rekan Transit Gateway (Cloud WAN)

Beberapa lampiran mendukung iklan rute melalui BGP. Untuk rute dengan CIDR yang sama, dan dari jenis lampiran yang sama, prioritas rute dikendalikan oleh atribut BGP:

- Panjang jalur AS yang lebih pendek
- Nilai MED yang lebih rendah
- eBGP melalui rute iBGP lebih disukai, jika lampiran mendukungnya

> **Important**
>
> - AWS tidak dapat menjamin urutan prioritas rute yang konsisten untuk rute BGP dengan CIDR, tipe lampiran, dan atribut BGP yang sama seperti yang tercantum di atas.
> - Untuk rute yang diiklankan ke gateway transit tanpa MED, AWS Transit Gateway akan menetapkan nilai default berikut:
>   - 0 untuk rute masuk yang diiklankan di lampiran Direct Connect.
>   - 100 untuk rute masuk yang diiklankan di lampiran VPN dan Connect.

AWS Transit Gateway hanya menampilkan rute pilihan. Rute cadangan hanya akan muncul di tabel rute gateway transit jika rute yang sebelumnya aktif tidak lagi diiklankan — misalnya, jika Anda mengiklankan rute yang sama melalui gateway Direct Connect dan melalui Site-to-Site VPN. AWS Transit Gateway hanya akan menampilkan rute yang diterima dari rute gateway Direct Connect, yang merupakan rute pilihan. Site-to-Site VPN, yang merupakan rute cadangan, hanya akan ditampilkan ketika gateway Direct Connect tidak lagi diiklankan.

Perbedaan tabel rute VPC dan transit gateway

Evaluasi tabel rute berbeda antara apakah Anda menggunakan tabel rute VPC atau tabel rute gateway transit.

Contoh berikut menunjukkan tabel rute VPC. Rute lokal VPC memiliki prioritas tertinggi, diikuti oleh rute yang paling spesifik. Ketika rute statis dan rute yang disebarkan memiliki tujuan yang sama, rute statis memiliki prioritas yang lebih tinggi.

Destinasi	Target	Prioritas
10.0.0. 0/16	lokal	1
192.168.0. 0/16	pcx-12345	2
172.31.0. 0/16	vgw-12345 (statis) atau tgw-12345 (statis)	2
172.31.0. 0/16	vgw-12345 (diperbanyak)	3

Destinasi	Target	Prioritas
0.0.0. 0/0	igw-12345	4

Contoh berikut menunjukkan tabel rute gateway transit. Jika Anda lebih suka lampiran Direct Connect gateway ke lampiran VPN, gunakan koneksi BGP VPN dan sebarkan rute di tabel rute gateway transit.

Destinasi	Lampiran (Target)	Tipe sumber daya	Jenis rute	Prioritas
10.0.0. 0/16	tgw-attach-123 | vpc-1234	VPC	Statis atau diperbanyak	1
192.168.0. 0/16	tgw-lampiran-789 | vpn-5678	VPN	Statis	2
172.31.0. 0/16	tgw-attach-456 | dxgw_id	Direct Connect pintu gerbang	Diperbanyak	3
172.31.0. 0/16	tgw-attach-789 | tgw-connect-peer-123	Hubungkan	Diperbanyak	4
172.31.0. 0/16	tgw-lampiran-789 | vpn-5678	VPN	Diperbanyak	5

Lampiran fungsi jaringan

Lampiran fungsi jaringan adalah sumber daya yang menghubungkan fungsi keamanan jaringan — misalnya, AWS Network Firewall lampiran — langsung ke gateway transit Anda. Ini menghilangkan kebutuhan untuk membuat dan mengelola VPC inspeksi secara manual.

Dengan lampiran fungsi jaringan:

- AWS secara otomatis membuat dan mengelola infrastruktur yang mendasarinya
- Lalu lintas dapat diperiksa saat mengalir melalui gateway transit Anda
- Kebijakan keamanan diterapkan secara konsisten di seluruh jaringan Anda

- Anda dapat mengarahkan lalu lintas melalui firewall menggunakan aturan perutean sederhana
- Lampiran berfungsi di beberapa Availability Zone untuk ketersediaan tinggi

Integrasi ini menyederhanakan keamanan jaringan dengan memungkinkan Anda untuk melampirkan firewall langsung ke gateway transit Anda daripada membuat konfigurasi routing yang kompleks dan mengelola endpoint terpisah melalui VPC terpisah.

AWS Network Firewall integrasi

AWS Network Firewall integrasi memungkinkan Anda untuk menghubungkan firewall dalam bentuk grup Gateway Load Balancer Endpoints, satu per Availability Zone, dalam VPC buffer yang dikelola layanan. Lampiran Network Firewall dibuat dengan mode alat diaktifkan secara otomatis. Ini menghilangkan kebutuhan untuk mengelola VPC inspeksi secara eksplisit.

Dengan integrasi Network Firewall, Anda tidak perlu lagi membuat dan mengelola VPC inspeksi untuk penerapan Network Firewall Anda. Alih-alih memilih VPC dan subnet saat membuat firewall, Anda langsung memilih Transit Gateway, dan AWS secara otomatis menyediakan dan mengelola semua sumber daya yang diperlukan di belakang layar. Anda akan melihat lampiran fungsi jaringan gateway transit baru daripada titik akhir firewall individual.

Untuk skenario lintas akun, Transit Gateway dapat RAM-shared dari pemilik Transit Gateway ke akun pemilik Network Firewall, yang memungkinkan salah satu akun untuk mengelola lampiran firewall. Setelah firewall dan lampiran Anda siap, Anda cukup memodifikasi tabel rute Transit Gateway Anda untuk mengirim lalu lintas ke lampiran untuk diperiksa.

> **Note**
>
> - Transit Gateway hanya mendukung perutean statis pada lampiran Network Firewall.
> - Third-party Firewall tidak didukung.

Untuk informasi selengkapnya tentang firewall dan lampiran, lihat Lampiran fungsi jaringan gateway Transit.

Contoh skenario gateway transit

Berikut ini adalah kasus penggunaan umum untuk gateway transit. Gateway transit Anda tidak terbatas pada kasus penggunaan ini.

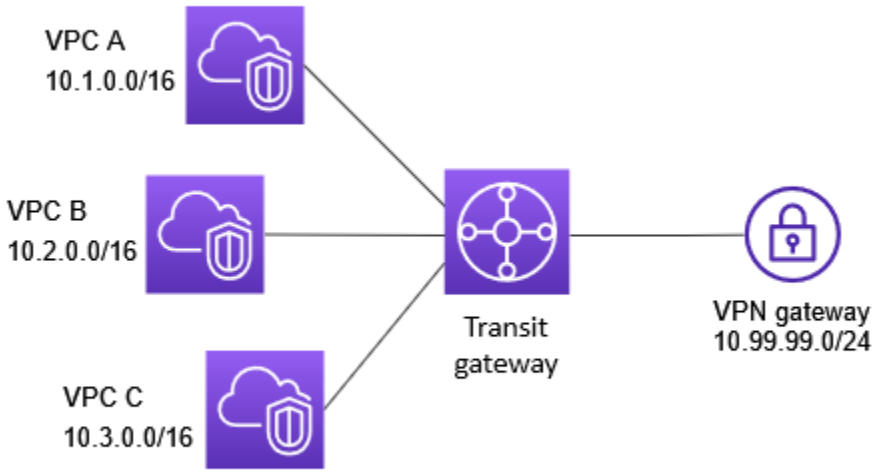
Contoh: Router terpusat

Anda dapat mengonfigurasi gateway transit Anda sebagai router terpusat yang menghubungkan semua VPC, AWS Direct Connect, dan koneksi Site-to-Site VPN Anda. Dalam skenario ini, semua lampiran dikaitkan dengan tabel rute default gateway transit dan disebarkan ke tabel rute default gateway transit. Oleh karena itu, semua lampiran dapat merutekan paket satu sama lain, dengan gateway transit berfungsi sebagai router IP layer 3 sederhana.

Daftar Isi

Ikhtisar

Diagram berikut menunjukkan komponen kunci konfigurasi untuk skenario ini. Dalam skenario ini, ada tiga lampiran VPC dan satu lampiran Site-to-Site VPN ke gateway transit. Paket dari subnet di VPC A, VPC B, dan VPC C yang ditujukan untuk subnet di VPC lain atau untuk koneksi VPN rute pertama melalui gateway transit.



Sumber daya

Buat sumber daya berikut untuk skenario ini:

- Tiga VPC. Untuk informasi selengkapnya, lihat Membuat VPC di Panduan Pengguna Amazon VPC.
- Transit gateway. Untuk informasi selengkapnya, lihat the section called “Membuat transit gateway”.
- Tiga lampiran VPC di gateway transit. Untuk informasi selengkapnya, lihat the section called “Buat lampiran VPC”.
- Lampiran Site-to-Site VPN di gateway transit. Blok CIDR untuk setiap VPC merambat ke tabel rute gateway transit. Ketika koneksi VPN habis, sesi BGP dibuat dan Site-to-Site VPN CIDR menyebar ke tabel rute gateway transit dan CIDR VPC ditambahkan ke tabel BGP gateway pelanggan. Untuk informasi selengkapnya, lihat the section called “Buat lampiran gateway transit ke VPN”.

  Pastikan Anda meninjau persyaratan untuk perangkat gateway pelanggan Anda di Panduan AWS Site-to-Site VPN Pengguna.

Perutean

Setiap VPC memiliki tabel rute dan ada tabel rute untuk gateway transit.

Tabel rute VPC

Setiap VPC memiliki tabel rute dengan 2 entri. Entri pertama adalah entri default untuk perutean IPv4 lokal di VPC; entri ini mengaktifkan instans-instans di dalam VPC ini untuk berkomunikasi satu sama lain. Entri kedua merutekan semua lalu lintas subnet IPv4 lainnya ke gateway transit. Tabel berikut menunjukkan rute VPC A.

Tujuan	Target
10.1.0. 0/16	lokal
0.0.0. 0/0	tgw-id

Tabel rute gateway transit

Berikut ini adalah contoh tabel rute default untuk lampiran yang ditunjukkan pada diagram sebelumnya, dengan propagasi rute diaktifkan.

Tujuan	Target	Jenis rute
10.1.0. 0/16	*Attachment for VPC A*	diperbanyak
10.2.0. 0/16	*Attachment for VPC B*	diperbanyak
10.3.0. 0/16	*Attachment for VPC C*	diperbanyak
10.99.99. 0/24	*Attachment for VPN connection*	diperbanyak

Tabel BGP gateway pelanggan

Tabel BGP gateway pelanggan berisi CIDR VPC berikut.

- 10.1.0. 0/16
- 10.2.0. 0/16

- 10.3.0. 0/16

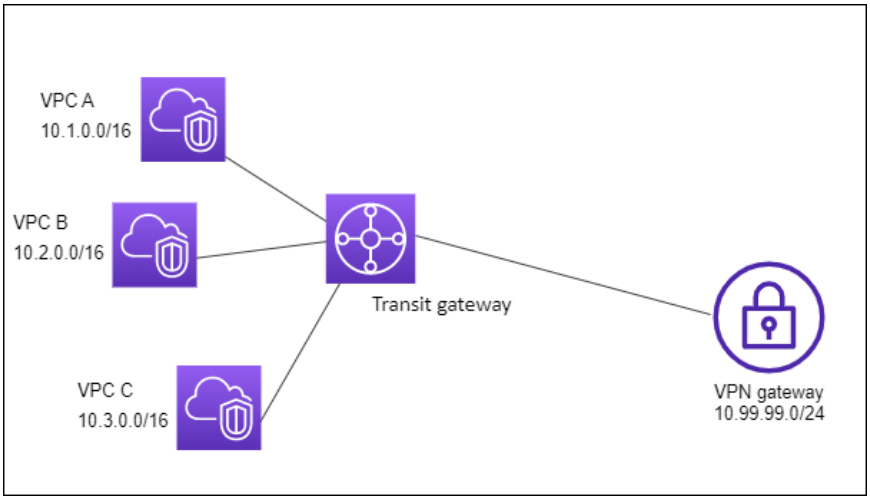
Contoh: VPC terisolasi

Anda dapat mengkonfigurasi transit gateway Anda sebagai beberapa router terisolasi. Hal ini mirip dengan menggunakan beberapa transit gateway, tetapi memberikan lebih banyak fleksibilitas dalam kasus di mana rute dan lampiran mungkin berubah. Dalam skenario ini, setiap router terisolasi memiliki tabel rute tunggal. Semua lampiran yang terkait dengan router terisolasi menyebar dan dikaitkan dengan tabel rutenya. Lampiran yang terkait dengan satu router terisolasi dapat merutekan paket satu sama lain, tetapi tidak dapat merutekan paket ke atau menerima paket dari lampiran untuk router lain yang terisolasi.

Daftar Isi

Ikhtisar

Diagram berikut menunjukkan komponen kunci konfigurasi untuk skenario ini. Paket dari VPC A, VPC B, dan VPC C rute ke gateway transit. Paket dari subnet di VPC A, VPC B, dan VPC C yang memiliki internet sebagai rute tujuan pertama melalui gateway transit dan kemudian rute ke koneksi VPN (jika tujuan Site-to-Site berada dalam jaringan itu). Paket dari satu VPC yang memiliki tujuan subnet di VPC lain, misalnya dari 10.1.0.0 hingga 10.2.0.0, rute melalui gateway transit, di mana mereka diblokir karena tidak ada rute untuk mereka di tabel rute gateway transit.



Sumber daya

Buat sumber daya berikut untuk skenario ini:

- Tiga VPC. Untuk informasi selengkapnya, lihat Membuat VPC di Panduan Pengguna Amazon VPC.
- Transit gateway. Untuk informasi selengkapnya, lihat the section called “Membuat transit gateway”.
- Tiga lampiran pada gateway transit untuk tiga VPC. Untuk informasi selengkapnya, lihat the section called “Buat lampiran VPC”.
- Lampiran Site-to-Site VPN di gateway transit. Untuk informasi selengkapnya, lihat the section called “Buat lampiran gateway transit ke VPN”. Pastikan Anda meninjau persyaratan untuk perangkat gateway pelanggan Anda di Panduan AWS Site-to-Site VPN Pengguna.

Ketika koneksi VPN habis, sesi BGP dibuat dan VPN CIDR menyebar ke tabel rute gateway transit dan CIDR VPC ditambahkan ke tabel BGP gateway pelanggan.

Perutean

Setiap VPC memiliki tabel rute, dan gateway transit memiliki dua tabel rute — satu untuk VPC dan satu untuk koneksi VPN.

Tabel rute VPC A, VPC B, dan VPC C

Setiap VPC memiliki tabel rute dengan 2 entri. Entri pertama adalah entri default untuk routing IPv4 lokal di VPC. Entri ini memungkinkan instance dalam VPC ini untuk berkomunikasi satu sama lain. Entri kedua merutekan semua lalu lintas subnet IPv4 lainnya ke gateway transit. Tabel berikut menunjukkan rute VPC A.

Tujuan	Target
10.1.0. 0/16	lokal
0.0.0. 0/0	tgw-id

Tabel rute transit gateway

Skenario ini menggunakan satu tabel rute untuk VPC dan satu tabel rute untuk koneksi VPN.

Lampiran VPC dikaitkan dengan tabel rute berikut, yang memiliki rute propagasi untuk lampiran VPN.

Tujuan	Target	Jenis rute
10.99.99. 0/24	*Attachment for VPN connection*	diperbanyak

Lampiran VPN dikaitkan dengan tabel rute berikut, yang telah menyebarkan rute untuk setiap lampiran VPC.

Tujuan	Target	Jenis rute
10.1.0. 0/16	*Attachment for VPC A*	diperbanyak
10.2.0. 0/16	*Attachment for VPC B*	diperbanyak
10.3.0. 0/16	*Attachment for VPC C*	diperbanyak

Untuk informasi selengkapnya tentang menyebarkan rute dalam tabel rute gateway transit, lihatAktifkan propagasi rute ke tabel rute gateway transit di AWS Transit Gateway.

Tabel BGP gateway pelanggan

Tabel BGP gateway pelanggan berisi CIDR VPC berikut.

- 10.1.0. 0/16
- 10.2.0. 0/16
- 10.3.0. 0/16

Contoh: VPC terisolasi dengan layanan bersama

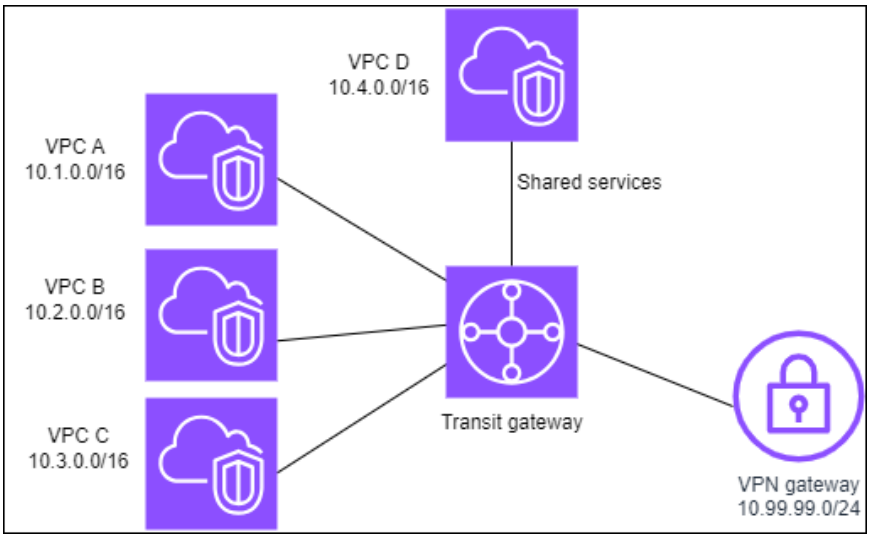
Anda dapat mengonfigurasi gateway transit Anda sebagai beberapa router terisolasi yang menggunakan layanan bersama. Hal ini mirip dengan menggunakan beberapa transit gateway, tetapi memberikan lebih banyak fleksibilitas dalam kasus di mana rute dan lampiran mungkin berubah.

Dalam skenario ini, setiap router terisolasi memiliki tabel rute tunggal. Semua lampiran yang terkait dengan router terisolasi menyebar dan dikaitkan dengan tabel rutenya. Lampiran yang terkait dengan satu router terisolasi dapat merutekan paket satu sama lain, tetapi tidak dapat merutekan paket ke atau menerima paket dari lampiran untuk router lain yang terisolasi. Lampiran dapat merutekan paket ke atau menerima paket dari layanan bersama. Anda dapat menggunakan skenario ini ketika Anda memiliki grup yang perlu diisolasi, tetapi menggunakan layanan bersama, misalnya sistem produksi.

Daftar Isi

Ikhtisar

Diagram berikut menunjukkan komponen kunci konfigurasi untuk skenario ini. Paket dari subnet di VPC A, VPC B, dan VPC C yang memiliki internet sebagai tujuan, rute pertama melalui gateway transit dan kemudian rute ke gateway pelanggan untuk VPN. Site-to-Site Paket dari subnet di VPC A, VPC B, atau VPC C yang memiliki tujuan subnet di rute VPC A, VPC B, atau VPC C melalui gateway transit, di mana mereka diblokir karena tidak ada rute untuk mereka di tabel rute gateway transit. Paket dari VPC A, VPC B, dan VPC C yang memiliki VPC D sebagai rute tujuan melalui gateway transit dan kemudian ke VPC D.



Sumber daya

Buat sumber daya berikut untuk skenario ini:

- Empat VPC. Untuk informasi selengkapnya, lihat Membuat VPC di Panduan Pengguna Amazon VPC.
- Transit gateway. Untuk informasi selengkapnya, lihat Membuat gateway transit.
- Empat lampiran di gateway transit, satu per VPC. Untuk informasi selengkapnya, lihat the section called “Buat lampiran VPC”.
- Lampiran Site-to-Site VPN di gateway transit. Untuk informasi selengkapnya, lihat the section called “Buat lampiran gateway transit ke VPN”.

  Pastikan Anda meninjau persyaratan untuk perangkat gateway pelanggan Anda di Panduan AWS Site-to-Site VPN Pengguna.

Ketika koneksi VPN habis, sesi BGP dibuat dan VPN CIDR menyebar ke tabel rute gateway transit dan CIDR VPC ditambahkan ke tabel BGP gateway pelanggan.

- Setiap VPC terisolasi dikaitkan dengan tabel rute terisolasi dan disebarkan ke tabel rute bersama.
- Setiap VPC layanan bersama dikaitkan dengan tabel rute bersama dan disebarkan ke kedua tabel rute.

Perutean

Setiap VPC memiliki tabel rute, dan gateway transit memiliki dua tabel rute — satu untuk VPC dan satu untuk koneksi VPN dan layanan bersama VPC.

VPC A, VPC B, VPC C, dan VPC D tabel rute

Setiap VPC memiliki tabel rute dengan dua entri. Entri pertama adalah entri default untuk perutean lokal di VPC; entri ini mengaktifkan instans-instans di VPC ini untuk berkomunikasi satu sama lain. Entri kedua merutekan semua lalu lintas subnet IPv4 lainnya ke gateway transit.

Tujuan	Target
10.1.0. 0/16	lokal
0.0.0. 0/0	*transit gateway ID*

Tabel rute transit gateway

Skenario ini menggunakan satu tabel rute untuk VPC dan satu tabel rute untuk koneksi VPN.

Lampiran VPC A, B, dan C dikaitkan dengan tabel rute berikut, yang memiliki rute propagasi untuk lampiran VPN dan rute propagasi untuk lampiran untuk VPC D.

Tujuan	Target	Jenis rute
10.99.99. 0/24	*Attachment for VPN connection*	diperbanyak
10.4.0. 0/16	*Attachment for VPC D*	diperbanyak

Lampiran VPN dan lampiran VPC (VPC D) layanan bersama dikaitkan dengan tabel rute berikut, yang memiliki entri yang mengarah ke masing-masing lampiran VPC. Hal ini memungkinkan komunikasi ke VPC dari koneksi VPN dan layanan bersama VPC.

Tujuan	Target	Jenis rute
10.1.0. 0/16	*Attachment for VPC A*	diperbanyak
10.2.0. 0/16	*Attachment for VPC B*	diperbanyak
10.3.0. 0/16	*Attachment for VPC C*	diperbanyak

Untuk informasi selengkapnya, lihat Aktifkan propagasi rute ke tabel rute gateway transit di AWS Transit Gateway.

Tabel BGP gateway pelanggan

Tabel BGP gateway pelanggan berisi CIDR untuk keempat VPC.

Contoh: Gateway transit peered

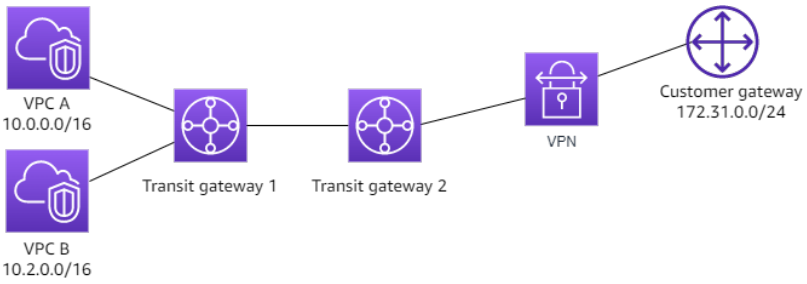
Anda dapat membuat koneksi peering gateway transit antara gateway transit. Anda kemudian dapat merutekan lalu lintas di antara lampiran untuk masing-masing gateway transit. Dalam skenario ini, lampiran VPC dan VPN dikaitkan dengan tabel rute default gateway transit, dan mereka menyebar ke

tabel rute default gateway transit. Setiap tabel rute gateway transit memiliki rute statis yang menunjuk ke lampiran peering gateway transit.

Daftar Isi

Ikhtisar

Diagram berikut menunjukkan komponen kunci konfigurasi untuk skenario ini. Transit gateway 1 memiliki dua lampiran VPC, dan transit gateway 2 memiliki satu Site-to-Site lampiran VPN. Paket dari subnet di VPC A dan VPC B yang memiliki internet sebagai rute tujuan pertama melalui transit gateway 1, kemudian transit gateway 2, dan kemudian rute ke koneksi VPN.



Sumber daya

Buat sumber daya berikut untuk skenario ini:

- Dua VPC. Untuk informasi selengkapnya, lihat Membuat VPC di Panduan Pengguna Amazon VPC.
- Dua gerbang transit. Mereka bisa berada di Wilayah yang sama atau di Wilayah yang berbeda. Untuk informasi selengkapnya, lihat the section called “Membuat transit gateway”.
- Dua lampiran VPC pada gateway transit pertama. Untuk informasi selengkapnya, lihat the section called “Buat lampiran VPC”.
- Lampiran Site-to-Site VPN pada gateway transit kedua. Untuk informasi selengkapnya, lihat the section called “Buat lampiran gateway transit ke VPN”. Pastikan Anda meninjau persyaratan untuk perangkat gateway pelanggan Anda di Panduan AWS Site-to-Site VPN Pengguna.
- Lampiran mengintip gateway transit antara dua gateway transit. Untuk informasi selengkapnya, lihat Lampiran mengintip gateway transit di AWS Transit Gateway.

Saat Anda membuat lampiran VPC, CIDR untuk setiap VPC menyebar ke tabel rute untuk gateway transit 1. Ketika koneksi VPN habis, tindakan berikut terjadi:

- Sesi BGP didirikan
- Site-to-Site VPN CIDR merambat ke tabel rute untuk gateway transit 2
- CIDR VPC ditambahkan ke tabel BGP gateway pelanggan

Perutean

Setiap VPC memiliki tabel rute dan setiap gateway transit memiliki tabel rute.

Tabel rute VPC A dan VPC B

Setiap VPC memiliki tabel rute dengan 2 entri. Entri pertama adalah entri default untuk routing IPv4 lokal di VPC. Entri default ini memungkinkan sumber daya dalam VPC ini untuk berkomunikasi satu sama lain. Entri kedua merutekan semua lalu lintas subnet IPv4 lainnya ke gateway transit. Tabel berikut menunjukkan rute VPC A.

Tujuan	Target
10.0.0. 0/16	lokal
0.0.0. 0/0	tgw-1-id

Tabel rute transit gateway

Berikut ini adalah contoh tabel rute default untuk transit gateway 1, dengan propagasi rute diaktifkan.

Tujuan	Target	Jenis rute
10.0.0. 0/16	*Attachment ID for VPC A*	diperbanyak
10.2.0. 0/16	*Attachment ID for VPC B*	diperbanyak

Tujuan	Target	Jenis rute
0.0.0. 0/0	*Attachment ID for peering connection*	statis

Berikut ini adalah contoh tabel rute default untuk transit gateway 2, dengan propagasi rute diaktifkan.

Tujuan	Target	Jenis rute
172.31.0. 0/24	*Attachment ID for VPN connection*	diperbanyak
10.0.0. 0/16	*Attachment ID for peering connection*	statis
10.2.0. 0/16	*Attachment ID for peering connection*	statis

Tabel BGP gateway pelanggan

Tabel BGP gateway pelanggan berisi CIDR VPC berikut.

- 10.0.0. 0/16
- 10.2.0. 0/16

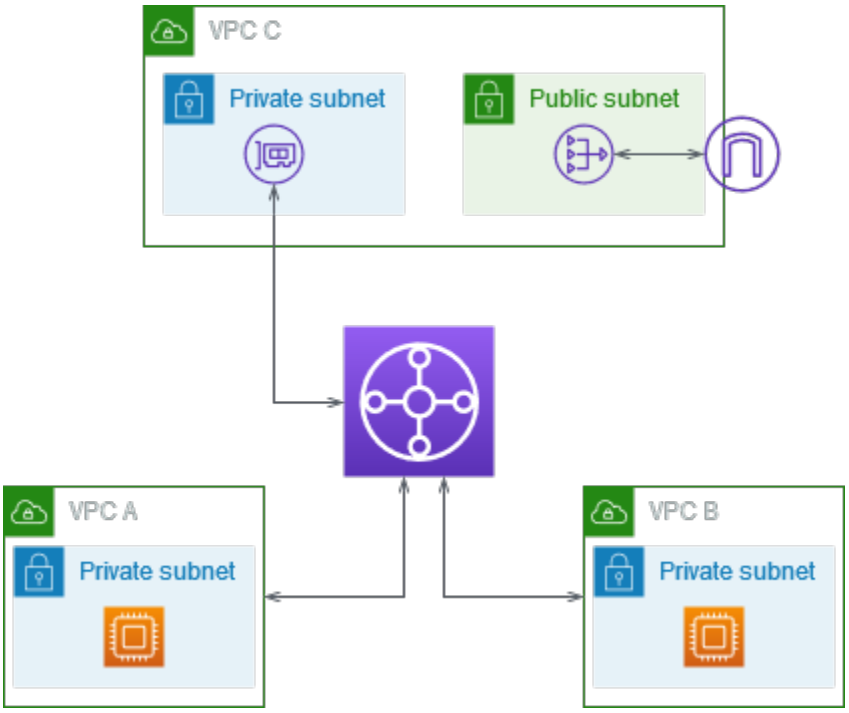
Contoh: Perutean keluar terpusat ke internet

Anda dapat mengonfigurasi gateway transit untuk merutekan lalu lintas internet keluar dari VPC tanpa gateway internet ke VPC yang berisi gateway NAT dan gateway internet.

Daftar Isi

Ikhtisar

Diagram berikut menunjukkan komponen kunci konfigurasi untuk skenario ini. Anda memiliki aplikasi di VPC A dan VPC B yang hanya membutuhkan akses internet keluar. Anda mengonfigurasi VPC C dengan gateway NAT publik dan gateway internet, dan subnet pribadi untuk lampiran VPC. Connect semua VPC ke gateway transit. Konfigurasikan perutean sehingga lalu lintas internet keluar dari VPC A dan VPC B melintasi gateway transit ke VPC C. Gateway NAT di VPC C merutekan lalu lintas ke gateway internet.



Sumber daya

Buat sumber daya berikut untuk skenario ini:

- Tiga VPC dengan rentang alamat IP yang tidak identik atau tumpang tindih. Untuk informasi selengkapnya, lihat Membuat VPC di Panduan Pengguna Amazon VPC.
- VPC A dan VPC B masing-masing memiliki subnet pribadi dengan instans EC2.
- VPC C memiliki yang berikut:
  - Gateway internet yang terpasang pada VPC. Untuk informasi selengkapnya, lihat Membuat dan melampirkan gateway internet di Panduan Pengguna Amazon VPC.
  - Subnet publik dengan gateway NAT. Untuk informasi selengkapnya, lihat Membuat gateway NAT di Panduan Pengguna Amazon VPC.

  - Subnet pribadi untuk lampiran gateway transit. Subnet pribadi harus berada di Availability Zone yang sama dengan subnet publik.
- Satu gerbang transit. Untuk informasi selengkapnya, lihat the section called “Membuat transit gateway”.
- Tiga lampiran VPC di gateway transit. Blok CIDR untuk setiap VPC merambat ke tabel rute gateway transit. Untuk informasi selengkapnya, lihat the section called “Buat lampiran VPC”. Untuk VPC C, Anda harus membuat lampiran menggunakan subnet pribadi. Jika Anda membuat lampiran menggunakan subnet publik, lalu lintas instance dirutekan ke gateway internet, tetapi gateway internet menurunkan lalu lintas karena instans tidak memiliki alamat IP publik. Dengan menempatkan lampiran di subnet pribadi, lalu lintas diarahkan ke gateway NAT, dan gateway NAT mengirimkan lalu lintas ke gateway internet menggunakan alamat IP Elastisnya sebagai alamat IP sumber.

Perutean

Ada tabel rute untuk setiap VPC dan tabel rute untuk gateway transit.

Tabel rute

- Tabel rute untuk VPC A
- Tabel rute untuk VPC B
- Tabel rute untuk VPC C
- Tabel rute gateway transit

Tabel rute untuk VPC A

Berikut ini adalah contoh tabel rute. Entri pertama memungkinkan instance di VPC untuk berkomunikasi satu sama lain. Entri kedua merutekan semua lalu lintas subnet IPv4 lainnya ke gateway transit.

Tujuan	Target
VPC A CIDR	lokal
0.0.0. 0/0	*transit-gateway-id*

Tabel rute untuk VPC B

Berikut ini adalah contoh tabel rute. Entri pertama memungkinkan instance di VPC untuk berkomunikasi satu sama lain. Entri kedua merutekan semua lalu lintas subnet IPv4 lainnya ke gateway transit.

Tujuan	Target
VPC B CIDR	lokal
0.0.0. 0/0	*transit-gateway-id*

Tabel rute untuk VPC C

Konfigurasikan subnet dengan gateway NAT sebagai subnet publik dengan menambahkan rute ke gateway internet. Biarkan subnet lainnya sebagai subnet pribadi.

Berikut ini adalah contoh tabel rute untuk subnet publik. Entri pertama memungkinkan instance di VPC untuk berkomunikasi satu sama lain. Entri kedua dan ketiga merutekan lalu lintas untuk VPC A dan VPC B ke gateway transit. Entri yang tersisa merutekan semua lalu lintas subnet IPv4 lainnya ke gateway internet.

Tujuan	Target
VPC C CIDR	lokal
VPC A CIDR	*transit-gateway-id*
VPC B CIDR	*transit-gateway-id*
0.0.0. 0/0	*internet-gateway-id*

Berikut ini adalah contoh tabel rute untuk subnet pribadi. Entri pertama memungkinkan instance di VPC untuk berkomunikasi satu sama lain. Entri kedua merutekan semua lalu lintas subnet IPv4 lainnya ke gateway NAT.

Tujuan	Target
VPC C CIDR	lokal
0.0.0. 0/0	*nat-gateway-id*

Tabel rute gateway transit

Berikut ini adalah contoh tabel rute gateway transit. Blok CIDR untuk setiap VPC merambat ke tabel rute gateway transit. Rute statis mengirimkan lalu lintas internet keluar ke VPC C. Anda dapat secara opsional mencegah komunikasi antar-VPC dengan menambahkan rute blackhole untuk setiap CIDR VPC.

CIDR	Lampiran	Jenis rute
VPC A CIDR	*Attachment for VPC A*	diperbanyak
VPC B CIDR	*Attachment for VPC B*	diperbanyak
VPC C CIDR	*Attachment for VPC C*	diperbanyak
0.0.0. 0/0	*Attachment for VPC C*	statis

Contoh: Peralatan di VPC layanan bersama

Anda dapat mengonfigurasi alat (seperti alat keamanan) di VPC layanan bersama. Semua lalu lintas yang diarahkan antara lampiran gateway transit pertama kali diperiksa oleh alat di VPC layanan bersama. Saat mode alat diaktifkan, gateway transit memilih antarmuka jaringan tunggal di VPC alat, menggunakan algoritme hash aliran, untuk mengirim lalu lintas selama masa pakai aliran. Gateway transit menggunakan antarmuka jaringan yang sama untuk lalu lintas kembali. Ini memastikan bahwa lalu lintas dua arah dirutekan secara simetris—itu dirutekan melalui Availability Zone yang sama di attachment VPC selama masa pakai aliran. Jika Anda memiliki beberapa gateway transit dalam arsitektur Anda, setiap gateway transit mempertahankan afinitas sesinya sendiri, dan setiap gateway transit dapat memilih antarmuka jaringan yang berbeda.

Anda harus menghubungkan tepat satu gateway transit ke VPC alat untuk menjamin kelengketan aliran. Menghubungkan beberapa gateway transit ke satu VPC alat tidak menjamin kelengketan aliran karena gateway transit tidak berbagi informasi status aliran satu sama lain.

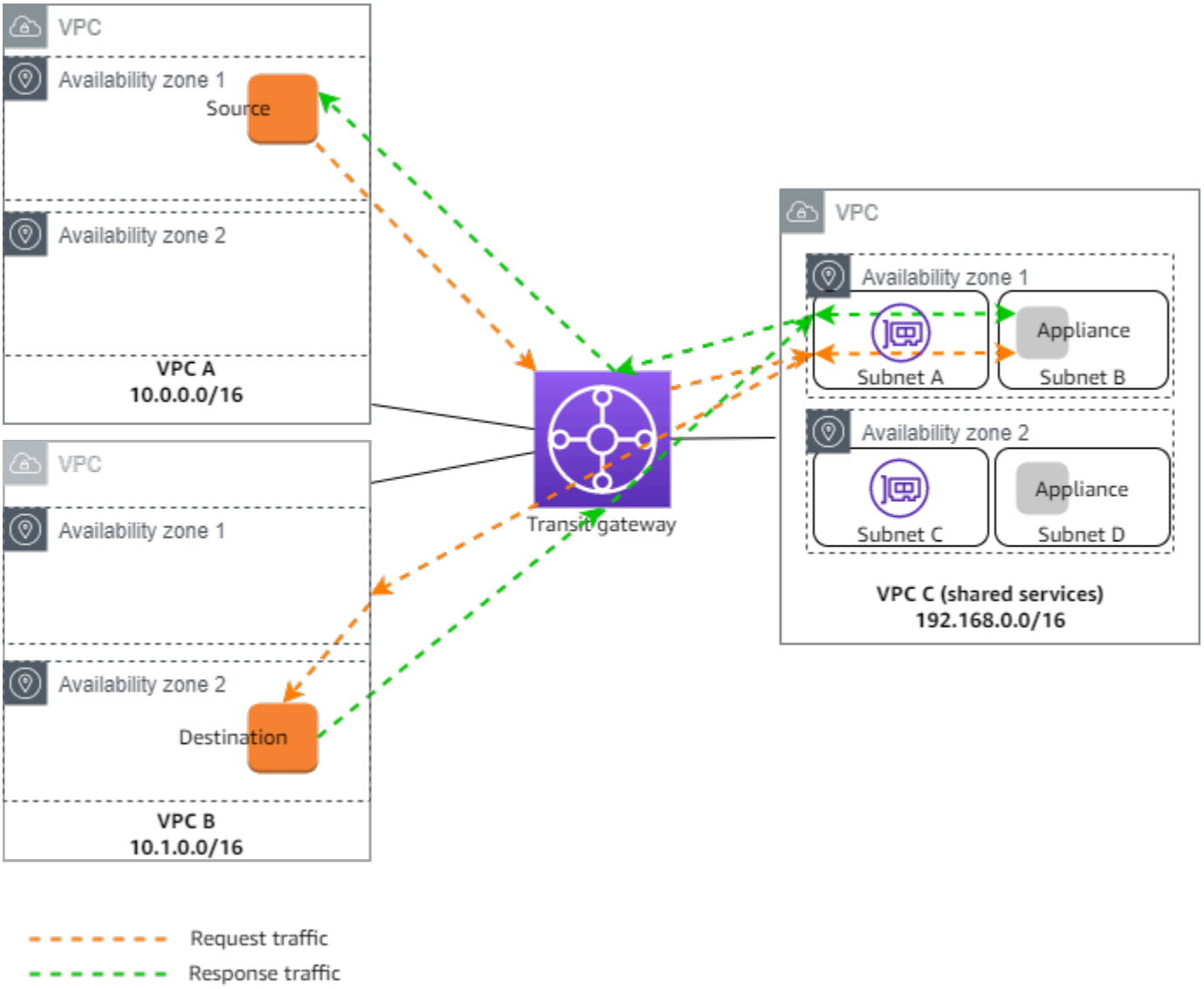
⚠ Important

- Lalu lintas dalam mode alat dirutekan dengan benar selama lalu lintas sumber dan tujuan datang ke VPC terpusat (VPC Inspeksi) dari lampiran gateway transit yang sama. Lalu lintas dapat turun jika sumber dan tujuan berada di dua lampiran gateway transit yang berbeda. Lalu lintas dapat turun jika VPC terpusat menerima lalu lintas dari gateway yang berbeda - misalnya, gateway Internet - dan kemudian mengirimkan lalu lintas itu ke lampiran gateway transit setelah pemeriksaan.
- Mengaktifkan mode alat pada lampiran yang ada dapat memengaruhi rute lampiran saat ini karena lampiran dapat mengalir melalui Availability Zone apa pun. Saat mode alat tidak diaktifkan, lalu lintas disimpan ke Availability Zone yang berasal.

Daftar Isi

Ikhtisar

Diagram berikut menunjukkan komponen kunci konfigurasi untuk skenario ini. Gateway transit memiliki tiga lampiran VPC. VPC C adalah VPC layanan bersama. Lalu lintas antara VPC A dan VPC B diarahkan ke gateway transit, kemudian diarahkan ke alat keamanan di VPC C untuk diperiksa sebelum diarahkan ke tujuan akhir. Alat ini adalah alat stateful, oleh karena itu lalu lintas permintaan dan respons diperiksa. Untuk ketersediaan tinggi, ada alat di setiap Availability Zone di VPC C.



Anda membuat sumber daya berikut untuk skenario ini:

- Tiga VPC. Untuk informasi selengkapnya, lihat Membuat VPC di Panduan Pengguna Amazon VPC.
- Transit gateway. Untuk informasi selengkapnya, lihat the section called “Membuat transit gateway”.
- Tiga lampiran VPC - satu untuk masing-masing VPC. Untuk informasi selengkapnya, lihat the section called “Buat lampiran VPC”.

  Untuk setiap lampiran VPC, tentukan subnet di setiap Availability Zone. Untuk VPC layanan bersama, ini adalah subnet tempat lalu lintas diarahkan ke VPC dari gateway transit. Dalam contoh sebelumnya, ini adalah subnet A dan C.

Untuk lampiran VPC untuk VPC C, aktifkan dukungan mode alat sehingga lalu lintas respons dialihkan ke Availability Zone yang sama di VPC C sebagai lalu lintas sumber.

Konsol VPC Amazon mendukung mode alat. Anda juga dapat menggunakan Amazon VPC API, AWS SDK, mode AWS CLI untuk mengaktifkan alat, atau. CloudFormationMisalnya, tambahkan `--options ApplianceModeSupport=enable` ke perintah create-transit-gateway-vpc-attachment atau modify-transit-gateway-vpc-attachment.

> **Note**
>
> Kelengketan aliran dalam mode alat dijamin hanya untuk lalu lintas sumber dan tujuan yang berasal dari VPC Inspeksi.

Peralatan stateful dan mode alat

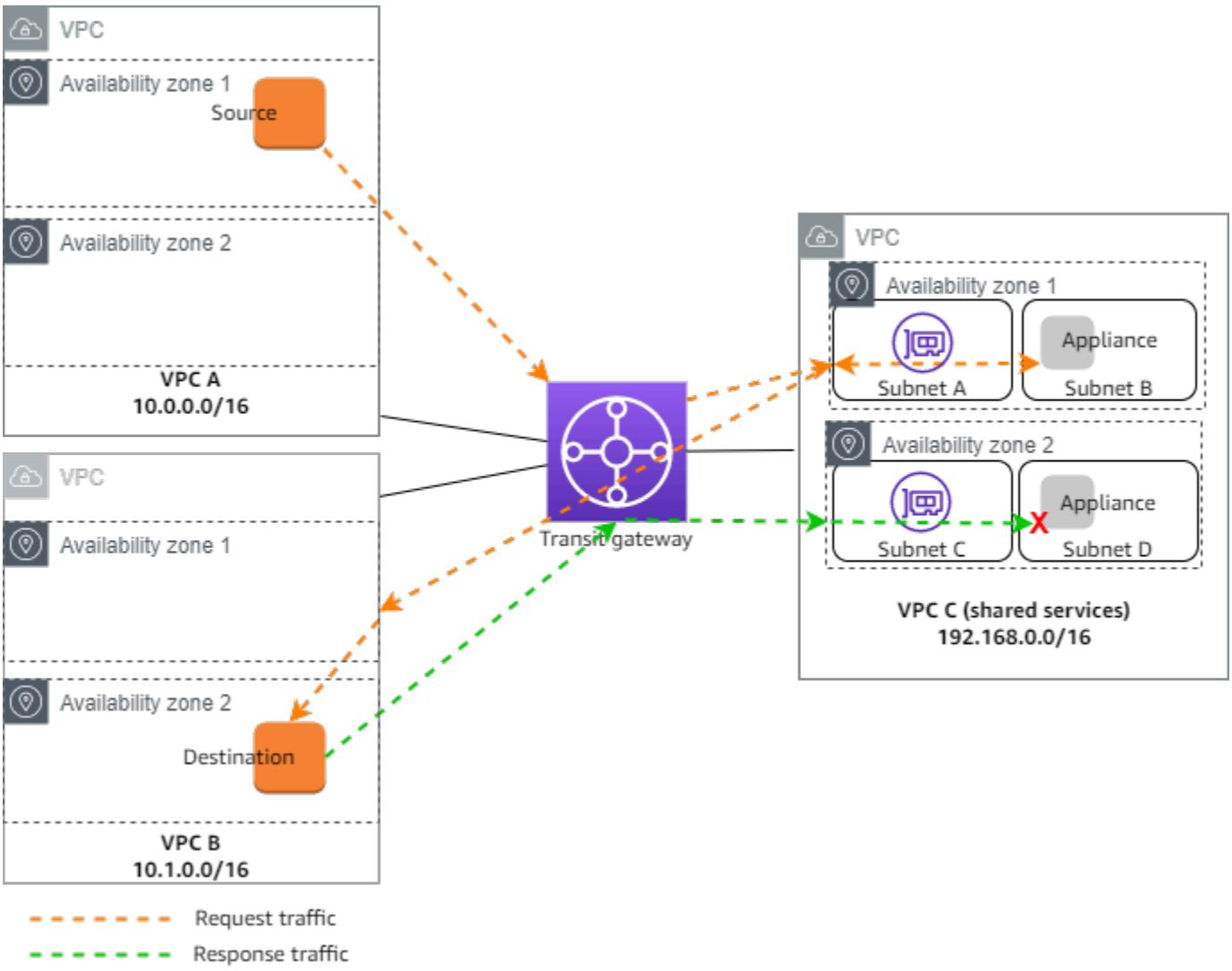
Jika lampiran VPC Anda menjangkau beberapa Availability Zone dan Anda memerlukan lalu lintas antara host sumber dan tujuan untuk dialihkan melalui alat yang sama untuk pemeriksaan stateful, aktifkan dukungan mode alat untuk lampiran VPC tempat alat berada.

Untuk informasi lebih lanjut, lihat Arsitektur inspeksi terpusat di AWS blog.

Perilaku saat mode alat tidak diaktifkan

Ketika mode alat tidak diaktifkan, gateway transit mencoba untuk menjaga lalu lintas dirutekan antara lampiran VPC di Availability Zone asal hingga mencapai tujuannya. Lalu lintas melintasi Availability Zone di antara lampiran hanya jika ada kegagalan Availability Zone atau jika tidak ada subnet yang terkait dengan lampiran VPC di Availability Zone tersebut.

Diagram berikut menunjukkan arus lalu lintas saat dukungan mode alat tidak diaktifkan. Lalu lintas respons yang berasal dari Availability Zone 2 di VPC B dialihkan oleh gateway transit ke Availability Zone yang sama di VPC C. Oleh karena itu lalu lintas dijatuhkan, karena alat di Availability Zone 2 tidak mengetahui permintaan asli dari sumber di VPC A.



Perutean

Setiap VPC memiliki satu atau lebih tabel rute dan gateway transit memiliki dua tabel rute.

Tabel rute VPC

VPC A dan VPC B

VPC A dan B memiliki tabel rute dengan 2 entri. Entri pertama adalah entri default untuk routing IPv4 lokal di VPC. Entri default ini memungkinkan sumber daya dalam VPC ini untuk berkomunikasi satu sama lain. Entri kedua merutekan semua lalu lintas subnet IPv4 lainnya ke gateway transit. Berikut ini adalah tabel rute untuk VPC A.

Tujuan	Target

Tujuan	Target
10.0.0. 0/16	lokal
0.0.0. 0/0	tgw-id

VPC C

Layanan bersama VPC (VPC C) memiliki tabel rute yang berbeda untuk setiap subnet. Subnet A digunakan oleh gateway transit (Anda menentukan subnet ini saat Anda membuat lampiran VPC). Tabel rute untuk subnet A merutekan semua lalu lintas ke alat di subnet B.

Tujuan	Target
192.168.0. 0/16	lokal
0.0.0. 0/0	alat-eni-id

Tabel rute untuk subnet B (yang berisi alat) merutekan lalu lintas kembali ke gateway transit.

Destinasi	Target
192.168.0. 0/16	lokal
0.0.0. 0/0	tgw-id

Tabel rute transit gateway

Gateway transit ini menggunakan satu tabel rute untuk VPC A dan VPC B, dan satu tabel rute untuk VPC layanan bersama (VPC C).

Lampiran VPC A dan VPC B dikaitkan dengan tabel rute berikut. Tabel rute merutekan semua lalu lintas ke VPC C.

Destinasi	Target	Jenis rute
0.0.0. 0/0	*Attachment ID for VPC C*	statis

Lampiran VPC C dikaitkan dengan tabel rute berikut. Ini merutekan lalu lintas ke VPC A dan VPC B.

Destinasi	Target	Jenis rute
10.0.0. 0/16	*Attachment ID for VPC A*	diperbanyak
10.1.0. 0/16	*Attachment ID for VPC B*	diperbanyak

Tutorial: Memulai AWS Transit Gateway

Tutorial berikut membantu Anda menjadi akrab dengan gateway transit di AWS Transit Gateway. Tugas-tugas dalam tutorial berikut memandu Anda melalui pembuatan gateway transit dan kemudian menghubungkan dua dari Anda VPCs menggunakan gateway transit itu. Anda dapat membuat gateway transit menggunakan konsol VPC Amazon atau menggunakan. AWS CLI

Tugas

- Tutorial: Membuat Gateway AWS Transit menggunakan Konsol VPC Amazon
- Tutorial: Buat Gateway AWS Transit menggunakan baris AWS perintah

Tutorial: Membuat Gateway AWS Transit menggunakan Konsol VPC Amazon

Dalam tutorial ini, Anda akan belajar cara menggunakan Konsol VPC Amazon untuk membuat gateway transit dan menghubungkan dua VPCs ke sana. Anda akan membuat gateway transit, melampirkan keduanya VPCs, dan kemudian mengonfigurasi rute yang diperlukan untuk mengaktifkan komunikasi antara gateway transit dan rute Anda VPCs.

Prasyarat

- Untuk menunjukkan contoh sederhana menggunakan gateway transit, buat dua VPCs di Wilayah yang sama. Tidak VPCs bisa identik atau tumpang tindih CIDRs. Luncurkan satu EC2 instans Amazon di setiap VPC. Untuk informasi selengkapnya, lihat Membuat VPC di Panduan Pengguna Amazon VPC dan Luncurkan instance di Panduan Pengguna Amazon. EC2
- Anda tidak dapat memiliki rute identik yang menunjuk ke dua yang berbeda VPCs. Gateway transit tidak menyebarkan VPC CIDRs yang baru dilampirkan jika rute yang identik ada di tabel rute gateway transit.
- Verifikasi bahwa Anda memiliki izin yang diperlukan untuk bekerja dengan gateway transit. Untuk informasi selengkapnya, lihat Identitas dan manajemen akses di AWS Transit Gateway.
- Anda tidak dapat melakukan ping antar host jika Anda belum menambahkan aturan ICMP ke masing-masing grup keamanan host. Untuk informasi selengkapnya, lihat Mengonfigurasi aturan grup keamanan di Panduan Pengguna Amazon VPC.

Langkah-langkah

Langkah 1: Buat transit gateway

Ketika Anda membuat transit gateway, kita membuat tabel rute transit gateway default dan menggunakannya sebagai tabel rute pengaitan default dan tabel rute propagasi default.

Untuk membuat gateway transit

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di pemilih Region, pilih Wilayah yang Anda gunakan saat membuat. VPCs
3. Pada panel navigasi, pilih Transit Gateways.
4. Pilih Buat gateway transit.
5. (Opsional) Untuk tag Nama, masukkan nama untuk gateway transit. Ini membuat tag dengan “Nama” sebagai kunci dan nama yang Anda tentukan sebagai nilai.
6. (Opsional) Untuk Deskripsi, masukkan deskripsi untuk gateway transit.
7. Di Konfigurasikan bagian gateway transit, lakukan hal berikut:

    1. Untuk Amazon side Autonomous System Number (ASN), masukkan ASN pribadi untuk gateway transit Anda. Ini harus menjadi ASN untuk AWS sisi sesi Border Gateway Protocol (BGP).

        Kisarannya dari 64512 hingga 65534 untuk 16-bit. ASNs

        Kisarannya dari 4200000000 hingga 4294967294 untuk 32-bit. ASNs

        Jika Anda memiliki penyebaran Multi-wilayah, kami sarankan Anda menggunakan ASN unik untuk setiap gateway transit Anda.
    2. (Opsional) Pilih apakah akan mengaktifkan salah satu dari berikut ini:
        - Dukungan DNS untuk VPCs melekat pada gateway transit ini.

- Dukungan ECMP VPN untuk koneksi VPN yang terpasang pada gateway transit.
- Asosiasi tabel rute default, yang secara otomatis mengaitkan lampiran gateway transit dengan tabel rute default gateway transit ini.
- Perambatan tabel rute default, yang secara otomatis menyebarkan lampiran tabel rute ke tabel rute default gateway transit ini.
- Dukungan multicast, yang memungkinkan Anda membuat domain multicast di gateway transit ini.

8. (Opsional) Di bagian opsi Configure-cross-account berbagi, pilih apakah akan menerima lampiran bersama secara otomatis. Jika diaktifkan, lampiran diterima secara otomatis. Jika tidak, Anda harus menerima atau menolak permintaan lampiran.
9. (Opsional) Di bagian blok CIDR gateway Transit, tambahkan blok CIDR ukuran /24 atau lebih besar untuk IPv4 alamat atau/64 blok atau blok CIDR yang lebih besar untuk alamat. IPv6 Anda dapat mengaitkan rentang alamat IP publik atau pribadi apa pun, kecuali alamat dalam rentang 169.254.0.0/16, dan rentang yang tumpang tindih dengan alamat untuk lampiran VPC dan jaringan lokal.

   > **Note**
   >
   > Blok CIDR gateway transit digunakan jika Anda mengonfigurasi lampiran Connect (GRE) atau PrivateIP. VPNs Transit Gateway menetapkan IPs untuk titik akhir Tunnel (GRE/PrivateIP VPN) dari rentang ini.

10. (Opsional) Tambahkan tag nilai kunci ke gateway transit ini untuk membantu mengidentifikasinya lebih lanjut.
    1. Pilih Tambahkan tanda baru.
    2. Masukkan nama Kunci dan Nilai terkait.
    3. Pilih Tambahkan tag baru untuk menambahkan tag tambahan, atau lewati ke langkah berikutnya.
11. Pilih Buat gateway transit. Saat gateway dibuat, status awal gateway transit adalah`pending`.

Langkah 2: Lampirkan VPCs ke gateway transit Anda

Tunggu hingga gateway transit yang Anda buat di bagian sebelumnya ditampilkan sebagai tersedia sebelum melanjutkan dengan membuat lampiran. Buat lampiran untuk setiap VPC.

Konfirmasikan bahwa Anda telah membuat dua VPCs dan meluncurkan EC2 instance di masing-masing, seperti yang dijelaskan dalamPrasyarat.

Buat lampiran gateway transit ke VPC

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Lampiran Transit Gateway.
3. Pilih Buat lampiran gateway transit.
4. (Opsional) Untuk tag Nama, masukkan nama untuk lampiran.
5. Untuk ID gateway Transit, pilih gateway transit yang akan digunakan untuk lampiran.
6. Untuk jenis Lampiran, pilih VPC.
7. Pilih apakah akan mengaktifkan dukungan DNS. Untuk latihan ini, jangan aktifkan IPv6 dukungan.
8. Untuk ID VPC, pilih VPC yang dilampirkan pada transit gateway.
9. Untuk Subnet IDs, pilih satu subnet untuk setiap Availability Zone yang akan digunakan oleh gateway transit untuk merutekan lalu lintas. Anda harus memilih setidaknya satu subnet. Anda hanya dapat memilih satu subnet per Availability Zone.
10. Pilih Buat lampiran gateway transit.

Setiap lampiran selalu dikaitkan dengan tepat satu tabel rute. Tabel rute dapat dikaitkan dengan nol hingga banyak lampiran. Untuk menentukan rute yang akan dikonfigurasi, tentukan kasus penggunaan untuk gateway transit Anda, lalu konfigurasikan rute. Untuk informasi selengkapnya, lihat the section called “Contoh skenario gateway transit”.

Langkah 3: Tambahkan rute antara gateway transit dan Anda VPCs

Sebuah tabel rute mencakup rute dinamis dan statis yang menentukan hop berikutnya untuk terkait VPCs berdasarkan alamat IP tujuan paket. Konfigurasikan rute yang memiliki tujuan untuk rute non-lokal dan target ID lampiran gateway transit. Untuk informasi selengkapnya, lihat Perutean untuk gateway transit di Panduan Pengguna Amazon VPC.

Untuk menambahkan rute ke tabel rute VPC

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Tabel Rute.
3. Pilih tabel rute yang terkait dengan VPC Anda.

4. Pilih Rute, kemudian pilih Edit rute.
5. Pilih Tambahkan rute.
6. Di dalam kolom Tujuan, masukkan maukkan rentang alamat IP tujuan. Untuk Target, pilih Transit Gateway, lalu pilih ID gateway transit.
7. Pilih Simpan perubahan.

Langkah 4: Uji gateway transit

Anda dapat mengonfirmasi bahwa gateway transit berhasil dibuat dengan menghubungkan ke EC2 instans Amazon di setiap VPC, dan kemudian mengirim data di antara mereka, seperti perintah ping. Untuk informasi selengkapnya, lihat Connect ke EC2 instans Anda di Panduan EC2 Pengguna Amazon.

Langkah 5: Hapus gateway transit

Ketika Anda tidak lagi membutuhkan gateway transit, Anda dapat menghapusnya.

Anda tidak dapat menghapus gateway transit yang memiliki lampiran sumber daya. Jika Anda mencoba menghapus gateway transit dengan lampiran, Anda akan diminta untuk menghapus lampiran tersebut terlebih dahulu sebelum Anda dapat menghapus gateway transit. Segera setelah gateway transit dihapus, Anda berhenti menimbulkan biaya untuk itu.

Untuk menghapus gateway transit Anda

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Transit Gateways.
3. Pilih gateway transit, lalu pilih Tindakan, Hapus gateway transit.
4. Masuk **`delete`** dan pilih Hapus.

   Status gateway transit di halaman gateway Transit adalah Menghapus. Setelah dihapus, gateway transit dihapus dari halaman.

Tutorial: Buat Gateway AWS Transit menggunakan baris AWS perintah

Dalam tutorial ini, Anda akan belajar bagaimana menggunakan AWS CLI untuk membuat gateway transit dan menghubungkan dua VPCs untuk itu. Anda akan membuat gateway transit, melampirkan keduanya VPCs, dan kemudian mengonfigurasi rute yang diperlukan untuk mengaktifkan komunikasi antara gateway transit dan rute Anda VPCs.

Prasyarat

Sebelum Anda mulai, pastikan Anda memiliki:

- AWS CLI diinstal dan dikonfigurasi dengan izin yang sesuai. Jika Anda belum AWS CLI menginstal, lihat Dokumentasi Antarmuka Baris AWS Perintah.
- Tidak VPCs bisa identik atau tumpang tindih CIDRs. Untuk informasi selengkapnya, lihat Membuat VPC di Panduan Pengguna Amazon VPC.
- Satu instans EC2 di setiap VPC. Untuk langkah-langkah meluncurkan instans EC2 ke dalam VPC, lihat Meluncurkan instance di Panduan Pengguna Amazon EC2.
- Grup keamanan dikonfigurasi untuk memungkinkan lalu lintas ICMP antar instance. Untuk langkah-langkah mengontrol lalu lintas menggunakan grup keamanan, lihat Mengontrol lalu lintas ke AWS sumber daya Anda menggunakan grup keamanan di Panduan Pengguna Amazon VPC.
- Izin IAM yang sesuai untuk bekerja dengan gateway transit. Untuk memeriksa izin IAM gateway transit, lihat Identitas dan manajemen akses di Gateway AWS Transit dalam Panduan.AWS Transit Gateway

Langkah-langkah

Langkah 1: Buat transit gateway

Saat Anda membuat gateway transit, AWS buat tabel rute gateway transit default dan menggunakannya sebagai tabel rute asosiasi default dan tabel rute propagasi default. Berikut ini menunjukkan contoh `create-transit-gateway` permintaan di `us-west-2` Wilayah. Tambahan `options` diteruskan dalam permintaan. Untuk informasi selengkapnya tentang `create-transit-gateway` perintah, termasuk daftar opsi yang dapat Anda berikan dalam permintaan, lihat create-transit-gateway.

```
aws ec2 create-transit-gateway \
  --description "My Transit Gateway" \
  --region us-west-2
```

Respons kemudian menunjukkan bahwa gateway transit telah dibuat. Sebagai tanggapan, `Options` yang dikembalikan adalah semua nilai default.

```
{
    "TransitGateway": {
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "TransitGatewayArn": "arn:aws:ec2:us-west-2:123456789012:transit-gateway/
tgw-1234567890abcdef0",
        "State": "pending",
        "OwnerId": "123456789012",
        "Description": "My Transit Gateway",
        "CreationTime": "2025-06-23T17:39:33+00:00",
        "Options": {
            "AmazonSideAsn": 64512,
            "AutoAcceptSharedAttachments": "disable",
            "DefaultRouteTableAssociation": "enable",
            "AssociationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
            "DefaultRouteTablePropagation": "enable",
            "PropagationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
            "VpnEcmpSupport": "enable",
            "DnsSupport": "enable",
            "SecurityGroupReferencingSupport": "disable",
            "MulticastSupport": "disable"
        }
    }
}
```

> **Note**
>
> Perintah ini mengembalikan informasi tentang gateway transit baru Anda, termasuk ID-nya. Catat ID gateway transit (`tgw-1234567890abcdef0`) karena Anda akan membutuhkannya di langkah selanjutnya.

Langkah 2: Verifikasi status ketersediaan gateway transit

Saat Anda membuat gateway transit, itu ditempatkan dalam `pending` keadaan. Status akan berubah dari pending menjadi tersedia secara otomatis, tetapi sampai itu terjadi Anda tidak dapat melampirkan apa pun VPCs hingga status berubah. Untuk memverifikasi status, jalankan `describe-transit-gatweways` perintah menggunakan ID gateway transit yang baru dibuat bersama dengan opsi filter. `filters`Opsi menggunakan `Name=state` dan `Values=available` berpasangan. Perintah kemudian mencari untuk memverifikasi apakah status gateway transit Anda dalam keadaan tersedia. Jika ya, responsnya menunjukkan`"State": "available"`. Jika dalam keadaan lain maka itu belum tersedia untuk digunakan. Tunggu beberapa menit sebelum menjalankan perintah.

Untuk informasi selengkapnya tentang `describe-transit-gateways` perintah, lihat describe-transit-gateways.

```
aws ec2 describe-transit-gateways \
  --transit-gateway-ids tgw-1234567890abcdef0 \
  --filters Name=state,Values=available
```

Tunggu hingga status gateway transit berubah dari `pending` ke `available` sebelum melanjutkan. Dalam tanggapan berikut, `State` telah berubah menjadi`available`.

```
{
    "TransitGateways": [
        {
            "TransitGatewayId": "tgw-1234567890abcdef0",
            "TransitGatewayArn": "arn:aws:ec2:us-west-2:123456789012:transit-gateway/
tgw-1234567890abcdef0",
            "State": "available",
            "OwnerId": "123456789012",
            "Description": "My Transit Gateway",
            "CreationTime": "2022-04-20T19:58:25+00:00",
```

```
            "Options": {
                "AmazonSideAsn": 64512,
                "AutoAcceptSharedAttachments": "disable",
                "DefaultRouteTableAssociation": "enable",
                "AssociationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
                "DefaultRouteTablePropagation": "enable",
                "PropagationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
                "VpnEcmpSupport": "enable",
                "DnsSupport": "enable",
                "SecurityGroupReferencingSupport": "disable",
                "MulticastSupport": "disable"
            },
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "example-transit-gateway"
                }
            ]
        }
    ]
}
```

Langkah 3: Lampirkan VPCs ke gateway transit Anda

Setelah gateway transit Anda tersedia, buat lampiran untuk setiap VPC menggunakan. `create-transit-gateway-vpc-attachment` Anda harus memasukkan`transit-gateway-id`,`vpc-id`, dan`subnet-ids`.

Untuk informasi selengkapnya tentang `create-transit-vpc attachment` perintah, lihat create-transit-gateway-vpc-attachment.

Dalam contoh berikut, perintah dijalankan dua kali, sekali untuk setiap VPC.

Untuk VPC pertama jalankan yang berikut ini menggunakan yang pertama `vpc_id` dan: `subnet-ids`

```
aws ec2 create-transit-gateway-vpc-attachment \
  --transit-gateway-id tgw-1234567890abcdef0 \
  --vpc-id vpc-1234567890abcdef0 \
  --subnet-ids subnet-1234567890abcdef0
```

Tanggapan menunjukkan keterikatan yang berhasil. Lampiran dibuat dalam `pending` keadaan. Tidak perlu mengubah status ini karena berubah menjadi `available` status secara otomatis. Ini mungkin memakan waktu beberapa menit.

```
{
    "TransitGatewayVpcAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-1234567890abcdef0",
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "VpcId": "vpc-1234567890abcdef0",
        "VpcOwnerId": "123456789012",
        "State": "pending",
        "SubnetIds": [
            "subnet-1234567890abcdef0",
            "subnet-abcdef1234567890"
        ],
        "CreationTime": "2025-06-23T18:35:11+00:00",
        "Options": {
            "DnsSupport": "enable",
            "SecurityGroupReferencingSupport": "enable",
            "Ipv6Support": "disable",
            "ApplianceModeSupport": "disable"
        }
    }
}
```

Untuk VPC kedua, jalankan perintah yang sama seperti di atas menggunakan yang kedua `vpc_id` dan: `subnet-ids`

```
aws ec2 create-transit-gateway-vpc-attachment \
  --transit-gateway-id tgw-1234567890abcdef0 \
  --vpc-id vpc-abcdef1234567890 \
  --subnet-ids subnet-abcdef01234567890
```

Respons untuk perintah ini juga menunjukkan lampiran yang berhasil, dengan lampiran saat ini dalam `pending` keadaan.

```
{
    {
    "TransitGatewayVpcAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-abcdef1234567890",
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "VpcId": "vpc-abcdef1234567890",
```

```
        "VpcOwnerId": "123456789012",
        "State": "pending",
        "SubnetIds": [
            "subnet-fedcba0987654321",
            "subnet-0987654321fedcba"
        ],
        "CreationTime": "2025-06-23T18:42:56+00:00",
        "Options": {
            "DnsSupport": "enable",
            "SecurityGroupReferencingSupport": "enable",
            "Ipv6Support": "disable",
            "ApplianceModeSupport": "disable"
        }
    }
}
```

Langkah 4: Verifikasi bahwa lampiran gateway transit tersedia

Lampiran gateway transit dibuat dalam `pending` keadaan awal. Anda tidak akan dapat menggunakan lampiran ini di rute Anda sampai status berubah. `available` Ini terjadi secara otomatis. Gunakan `describe-transit-gateways` perintah, bersama dengan`transit-gateway-id`, untuk memeriksa`State`. Untuk informasi selengkapnya tentang `describe-transit-gateways` perintah, lihat describe-transit-gateways.

Jalankan perintah berikut untuk memeriksa status. Dalam contoh ini, bidang opsional `Name` dan `Values` filter diteruskan dalam permintaan:

```
aws ec2 describe-transit-gateway-vpc-attachments \
  --filters Name=transit-gateway-id,Values=tgw-1234567890abcdef0
```

Tanggapan berikut menunjukkan bahwa kedua lampiran dalam suatu `available` keadaan:

```
{
    "TransitGatewayVpcAttachments": [
        {
            "TransitGatewayAttachmentId": "tgw-attach-1234567890abcdef0",
            "TransitGatewayId": "tgw-1234567890abcdef0",
            "VpcId": "vpc-1234567890abcdef0",
            "VpcOwnerId": "123456789012",
            "State": "available",
            "SubnetIds": [
```

```
                "subnet-1234567890abcdef0",
                "subnet-abcdef1234567890"
            ],
            "CreationTime": "2025-06-23T18:35:11+00:00",
            "Options": {
                "DnsSupport": "enable",
                "SecurityGroupReferencingSupport": "enable",
                "Ipv6Support": "disable",
                "ApplianceModeSupport": "disable"
            },
            "Tags": []
        },
        {
            "TransitGatewayAttachmentId": "tgw-attach-abcdef1234567890",
            "TransitGatewayId": "tgw-1234567890abcdef0",
            "VpcId": "vpc-abcdef1234567890",
            "VpcOwnerId": "123456789012",
            "State": "available",
            "SubnetIds": [
                "subnet-fedcba0987654321",
                "subnet-0987654321fedcba"
            ],
            "CreationTime": "2025-06-23T18:42:56+00:00",
            "Options": {
                "DnsSupport": "enable",
                "SecurityGroupReferencingSupport": "enable",
                "Ipv6Support": "disable",
                "ApplianceModeSupport": "disable"
            },
            "Tags": []
        }
    ]
}
```

Langkah 5: Tambahkan rute antara gateway transit Anda dan VPCs

Konfigurasikan rute di setiap tabel rute VPC untuk mengarahkan lalu lintas ke VPC lain melalui gateway transit menggunakan `create-route` perintah bersama dengan untuk `transit-gateway-id` setiap tabel rute VPC. Dalam contoh berikut, perintah dijalankan dua kali, sekali untuk setiap tabel rute. Permintaan termasuk`route-table-id`,`destination-cidr-block`, dan `transit-gateway-id` untuk setiap rute VPC yang Anda buat.

Untuk informasi selengkapnya tentang `create-route` perintah, lihat create-route.

Untuk tabel rute VPC pertama jalankan perintah berikut:

```
aws ec2 create-route \
  --route-table-id rtb-1234567890abcdef0 \
  --destination-cidr-block 10.2.0.0/16 \
  --transit-gateway-id tgw-1234567890abcdef0
```

Untuk tabel rute VPC kedua jalankan perintah berikut. Rute ini menggunakan `route-table-id` dan `destination-cidr-block` berbeda dari VPC pertama. Namun, karena Anda hanya menggunakan satu gateway transit, hal yang sama `transit-gateway-id` digunakan.

```
aws ec2 create-route \
  --route-table-id rtb-abcdef1234567890 \
  --destination-cidr-block 10.1.0.0/16 \
  --transit-gateway-id tgw-1234567890abcdef0
```

Respons kembali `true` untuk setiap rute, menunjukkan rute telah dibuat.

```
{
    "Return": true
}
```

> **Note**
>
> Ganti blok CIDR tujuan dengan blok CIDR Anda yang sebenarnya. VPCs

Langkah 6: Uji gateway transit

Anda dapat mengonfirmasi bahwa gateway transit berhasil dibuat dengan menghubungkan ke instans EC2 di satu VPC dan melakukan ping instance di VPC lainnya, lalu menjalankan perintah. `ping`

1. Connect ke instans EC2 Anda di VPC pertama menggunakan SSH atau EC2 Instance Connect
2. Ping alamat IP pribadi instans EC2 di VPC kedua:

   ```
   ping 10.2.0.50
   ```

> **Note**
>
> Ganti `10.2.0.50` dengan alamat IP pribadi sebenarnya dari instans EC2 Anda di VPC kedua.

Jika ping berhasil, gateway transit Anda dikonfigurasi dengan benar dan merutekan lalu lintas di antara Anda VPCs.

Langkah 7: Hapus lampiran gateway transit dan gateway transit

Ketika Anda tidak lagi membutuhkan gateway transit, Anda dapat menghapusnya. Pertama, Anda harus menghapus semua lampiran. Jalankan `delete-transit-gateway-vpc-attachment` perintah, menggunakan `transit-gateway-attachment-id` untuk setiap lampiran. Setelah menjalankan perintah, gunakan `delete-transit-gateway` untuk menghapus gateway transit. Untuk hal berikut, hapus dua lampiran VPC dan gateway transit tunggal yang dibuat pada langkah sebelumnya.

> **Important**
>
> Anda akan berhenti mengeluarkan biaya setelah menghapus semua lampiran gateway transit.

1. Hapus lampiran VPC menggunakan perintah. `delete-transit-gateway-vpc-attachment` Untuk informasi selengkapnya tentang `delete-transit-gateway-vpc-attachment` perintah, lihat delete-transit-gateway-vpc-attachment.

   Untuk lampiran pertama, jalankan perintah berikut:

   ```
   aws ec2 delete-transit-gateway-vpc-attachment \
     --transit-gateway-attachment-id tgw-attach-1234567890abcdef0
   ```

   Tanggapan hapus untuk lampiran VPC pertama mengembalikan yang berikut:

   ```
   {
       "TransitGatewayVpcAttachment": {
           "TransitGatewayAttachmentId": "tgw-attach-1234567890abcdef0",
   ```

```
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "VpcId": "vpc-abcdef1234567890",
        "VpcOwnerId": "123456789012",
        "State": "deleting",
        "CreationTime": "2025-06-23T18:42:56+00:00"
    }
}
```

Jalankan `delete-transit-gateway-vpc-attachment` perintah untuk lampiran kedua:

```
aws ec2 delete-transit-gateway-vpc-attachment \
  --transit-gateway-attachment-id tgw-attach-abcdef1234567890
```

Tanggapan hapus untuk lampiran VPC kedua mengembalikan yang berikut:

```
The response returns:
{
    "TransitGatewayVpcAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-abcdef1234567890",
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "VpcId": "vpc-abcdef1234567890",
        "VpcOwnerId": "123456789012",
        "State": "deleting",
        "CreationTime": "2025-06-23T18:42:56+00:00"
    }
}
```

2. Lampiran berada dalam `deleting` keadaan sampai dihapus. Setelah dihapus, Anda kemudian dapat menghapus gateway transit. Gunakan `delete-transit-gateway` perintah bersama dengan`transit-gateway-id`. Untuk informasi selengkapnya tentang `delete-transit-gateway` perintah, lihat delete-transit-gateway.

   Contoh berikut menghapus `My Transit Gateway` yang Anda buat pada langkah pertama di atas:

```
aws ec2 delete-transit-gateway \
  --transit-gateway-id tgw-1234567890abcdef0
```

Berikut ini menunjukkan respons terhadap permintaan, yang mencakup ID dan nama gateway transit yang dihapus, bersama dengan opsi asli yang ditetapkan untuk gateway transit saat dibuat.


```
{
    "TransitGateway": {
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "TransitGatewayArn": "arn:aws:ec2:us-west-2:123456789012:transit-gateway/
tgw-1234567890abcdef0",
        "State": "deleting",
        "OwnerId": "123456789012",
        "Description": "My Transit Gateway",
        "CreationTime": "2025-06-23T17:39:33+00:00",
        "Options": {
            "AmazonSideAsn": 64512,
            "AutoAcceptSharedAttachments": "disable",
            "DefaultRouteTableAssociation": "enable",
            "AssociationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
            "DefaultRouteTablePropagation": "enable",
            "PropagationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
            "VpnEcmpSupport": "enable",
            "DnsSupport": "enable",
            "SecurityGroupReferencingSupport": "disable",
            "MulticastSupport": "disable"
        },
        "Tags": [
            {
                "Key": "Name",
                "Value": "example-transit-gateway"
            }
        ]
    }
}
```


Kesimpulan

Anda telah berhasil membuat gateway transit, melampirkan dua VPCs padanya, mengonfigurasi perutean di antara mereka, dan konektivitas terverifikasi. Contoh sederhana ini menunjukkan fungsionalitas dasar AWS Transit Gateways. Untuk skenario yang lebih kompleks, seperti

menghubungkan ke jaringan lokal atau menerapkan konfigurasi perutean yang lebih maju, lihat Panduan Gateway AWS Transit.

AWS Praktik terbaik desain Transit Gateway

Berikut ini adalah praktik terbaik untuk desain gateway transit Anda:

- Gunakan subnet terpisah untuk setiap lampiran VPC gateway transit. Untuk setiap subnet, gunakan CIDR kecil, misalnya/28, sehingga Anda memiliki lebih banyak alamat untuk EC2 sumber daya. Saat Anda menggunakan subnet terpisah, Anda dapat mengonfigurasi yang berikut:
  - Jaga agar jaringan masuk dan keluar yang ACLs terkait dengan subnet gateway transit tetap terbuka.
  - Tergantung pada arus lalu lintas Anda, Anda dapat menerapkan jaringan ACLs ke subnet beban kerja Anda.
- Buat satu jaringan ACL dan kaitkan dengan semua subnet yang terkait dengan gateway transit. Jaga agar ACL jaringan tetap terbuka di arah masuk dan keluar.
- Kaitkan tabel rute VPC yang sama dengan semua subnet yang terkait dengan gateway transit, kecuali desain jaringan Anda memerlukan beberapa tabel rute VPC (misalnya, VPC kotak tengah yang merutekan lalu lintas melalui beberapa gateway NAT).
- Gunakan Site-to-Site koneksi VPN Border Gateway Protocol (BGP). Jika perangkat gateway pelanggan Anda atau firewall untuk koneksi mendukung multipath, aktifkan fitur tersebut.
- Aktifkan propagasi rute untuk lampiran Direct Connect gateway dan lampiran BGP VPN Site-to-Site.
- Saat bermigrasi dari VPC mengintip untuk menggunakan gateway transit. Ketidakcocokan ukuran MTU antara pengintip VPC dan gateway transit dapat mengakibatkan beberapa paket jatuh untuk lalu lintas asimetris. Perbarui keduanya secara VPCs bersamaan untuk menghindari paket jumbo jatuh karena ketidakcocokan ukuran.
- Anda tidak memerlukan gateway transit tambahan untuk ketersediaan tinggi, karena gateway transit sangat tersedia berdasarkan desain.
- Batasi jumlah tabel rute gateway transit kecuali desain Anda memerlukan beberapa tabel rute gateway transit.
- Untuk redundansi, gunakan gerbang transit tunggal di setiap Wilayah untuk pemulihan bencana.
- Untuk penerapan dengan beberapa gateway transit, kami menyarankan Anda menggunakan Nomor Sistem Otonom (ASN) unik untuk setiap gateway transit Anda. Anda juga dapat menggunakan peering antar wilayah. Untuk informasi selengkapnya, lihat Membangun jaringan global menggunakan AWS Transit Gateway peering Antar Wilayah.

Bekerja dengan AWS Transit Gateway

Anda dapat bekerja dengan gateway transit menggunakan konsol VPC Amazon atau. AWS CLI Untuk informasi tentang mengaktifkan dan mengelola dukungan Enkripsi untuk gateway transit Anda, lihatthe section called “Dukungan Enkripsi”.

Topik

Gateway transit bersama

Anda dapat menggunakan AWS Resource Access Manager (RAM) untuk berbagi gateway transit lampiran VPC di seluruh akun atau di seluruh organisasi Anda. AWS Organizations RAM harus diaktifkan dan sumber daya dibagikan dengan organisasi. Untuk informasi selengkapnya, lihat Mengaktifkan berbagi sumber daya AWS Organizations di Panduan AWS RAM Pengguna.

Pertimbangan-pertimbangan

Pertimbangkan hal berikut ketika Anda ingin berbagi gateway transit.

- AWS Site-to-Site VPN Lampiran harus dibuat di AWS akun yang sama yang memiliki gateway transit.
- Lampiran ke gateway Direct Connect menggunakan asosiasi gateway transit dan dapat berada di AWS akun yang sama dengan gateway Direct Connect, atau yang berbeda dari gateway Direct Connect.

Secara default, pengguna tidak memiliki izin untuk membuat atau memodifikasi AWS RAM sumber daya. Untuk memungkinkan pengguna membuat atau memodifikasi sumber daya dan melakukan tugas, Anda harus membuat kebijakan IAM yang memberikan izin untuk menggunakan sumber daya dan tindakan API tertentu. Anda kemudian melampirkan kebijakan tersebut ke pengguna IAM atau grup yang memerlukan izin tersebut.

Hanya pemilik sumber daya yang dapat melakukan operasi berikut:

- Buat berbagi sumber daya.
- Perbarui pembagian sumber daya.
- Lihat pembagian sumber daya.
- Lihat sumber daya yang dibagikan oleh akun Anda, di semua pembagian sumber daya.
- Lihat kepala sekolah dengan siapa Anda berbagi sumber daya Anda, di semua pembagian sumber daya. Melihat kepala sekolah dengan siapa Anda berbagi memungkinkan Anda untuk menentukan siapa yang memiliki akses ke sumber daya bersama Anda.
- Hapus pembagian sumber daya.
- Jalankan semua gateway transit, lampiran gateway transit, dan API tabel rute gateway transit.

Anda dapat melakukan operasi berikut pada sumber daya yang dibagikan dengan Anda:

- Terima, atau tolak undangan berbagi sumber daya.
- Lihat pembagian sumber daya.
- Lihat sumber daya bersama yang dapat Anda akses.
- Lihat daftar semua prinsipal yang berbagi sumber daya dengan Anda. Anda dapat melihat sumber daya dan sumber daya mana yang telah mereka bagikan dengan Anda.
- Dapat menjalankan `DescribeTransitGateways` API.
- Jalankan API yang membuat dan mendeskripsikan lampiran, misalnya `CreateTransitGatewayVpcAttachment` dan`DescribeTransitGatewayVpcAttachments`, di VPC mereka.

- Tinggalkan bagian sumber daya.

Ketika gateway transit dibagikan dengan Anda, Anda tidak dapat membuat, memodifikasi, atau menghapus tabel rute gateway transit, atau propagasi dan asosiasi tabel rute gateway transit.

Saat Anda membuat gateway transit, gateway transit, dibuat di Availability Zone yang dipetakan ke akun Anda dan independen dari akun lain. Saat gateway transit dan entitas lampiran berada di akun yang berbeda, gunakan ID Availability Zone untuk mengidentifikasi Availability Zone secara unik dan konsisten. Misalnya, use1-az1 adalah ID AZ untuk Wilayah us-east-1 dan memetakan ke lokasi yang sama di setiap akun. AWS

Batalkan berbagi gateway transit

Jika pemilik saham membatalkan pembagian gateway transit, aturan berikut berlaku:

- Lampiran gateway transit tetap berfungsi.
- Akun bersama tidak dapat menggambarkan gateway transit.
- Pemilik gateway transit, dan pemilik saham dapat menghapus lampiran gateway transit.

Ketika gateway transit tidak dibagikan dengan AWS akun lain, atau jika AWS akun yang digunakan bersama gateway transit dihapus dari organisasi, gateway transit itu sendiri tidak akan terpengaruh.

Subnet bersama

Pemilik VPC dapat melampirkan gateway transit ke subnet VPC bersama. Peserta tidak bisa. Lalu lintas dari sumber daya peserta dapat menggunakan lampiran tergantung pada rute yang diatur pada subnet VPC bersama oleh pemilik VPC.

Untuk informasi selengkapnya, lihat Berbagi VPC Anda dengan akun lain di Panduan Pengguna Amazon VPC.

Gerbang transit di AWS Transit Gateway

Gateway transit memungkinkan Anda untuk melampirkan VPCs dan koneksi VPN dan merutekan lalu lintas di antara mereka. Gateway transit berfungsi di seberang Akun AWS, dan Anda dapat menggunakannya AWS RAM untuk berbagi gateway transit Anda dengan akun lain. Setelah Anda berbagi gateway transit dengan yang lain Akun AWS, pemilik akun dapat melampirkannya VPCs ke

gateway transit Anda. Pengguna dari kedua akun ini dapat menghapus lampiran VPC tersebut kapan saja.

Anda dapat mengaktifkan multicast pada gateway transit, lalu membuat domain multicast gateway transit yang memungkinkan lalu lintas multicast dikirim dari sumber multicast Anda untuk anggota grup multicast melalui lampiran VPC yang Anda kaitkan dengan domain.

Setiap lampiran VPC atau VPN dikaitkan dengan satu tabel rute. Tabel rute itu memutuskan lompatan berikutnya untuk lalu lintas yang berasal dari lampiran sumber daya itu. Tabel rute di dalam gateway transit memungkinkan untuk keduanya IPv4 atau IPv6 CIDRs dan target. Targetnya adalah VPCs dan koneksi VPN. Saat Anda melampirkan VPC atau membuat koneksi VPN di gateway transit, lampiran dikaitkan dengan tabel rute default gateway transit.

Anda dapat membuat tabel rute tambahan di dalam gateway transit, dan mengubah asosiasi VPC atau VPN ke tabel rute ini. Ini memungkinkan Anda untuk mengelompokkan jaringan Anda. Misalnya, Anda dapat mengaitkan pengembangan VPCs dengan satu tabel rute dan produksi VPCs dengan tabel rute yang berbeda. Ini memungkinkan Anda untuk membuat jaringan terisolasi di dalam gateway transit yang mirip dengan virtual routing dan forwarding (VRFs) di jaringan tradisional.

Transit gateway mendukung perutean dinamis dan statis antara koneksi terpasang VPCs dan VPN. Anda dapat mengaktifkan atau menonaktifkan propagasi rute untuk setiap lampiran. Lampiran VPN Concentrator hanya mendukung perutean BGP (dinamis). Lampiran peering gateway transit hanya mendukung perutean statis. Anda dapat mengarahkan rute dalam tabel rute gateway transit ke lampiran peering untuk merutekan lalu lintas antara gateway transit peered.

Anda dapat secara opsional mengaitkan satu atau lebih IPv4 atau blok IPv6 CIDR dengan gateway transit Anda. Anda menentukan alamat IP dari blok CIDR saat membuat peer Transit Gateway Connect untuk lampiran Transit Gateway Connect. Anda dapat mengaitkan rentang alamat IP publik atau pribadi apa pun, kecuali alamat dalam `169.254.0.0/16` rentang tersebut, dan rentang yang tumpang tindih dengan alamat untuk lampiran VPC dan jaringan lokal. Untuk informasi selengkapnya tentang IPv4 dan pemblokiran IPv6 CIDR, lihat Pengalamatan IP di Panduan Pengguna Amazon VPC.

Tugas

- Buat gateway transit di AWS Transit Gateway
- Lihat informasi gateway transit di AWS Transit Gateway
- Kelola tag gateway transit di AWS Transit Gateway
- Ubah gateway transit di AWS Transit Gateway

- Menerima pembagian sumber daya AWS Transit Gateway menggunakan AWS Resource Access Manager konsol
- Menerima lampiran bersama di AWS Transit Gateway
- Menghapus gateway transit di AWS Transit Gateway
- Dukungan Enkripsi untuk AWS Transit Gateway

Buat gateway transit di AWS Transit Gateway

Ketika Anda membuat transit gateway, kita membuat tabel rute transit gateway default dan menggunakannya sebagai tabel rute pengaitan default dan tabel rute propagasi default. Jika Anda memilih untuk tidak membuat tabel rute gateway transit default, Anda dapat membuatnya nanti. Untuk informasi selengkapnya tentang rute dan tabel rute, lihat???.

> **Note**
>
> Jika Anda ingin mengaktifkan dukungan Enkripsi pada gateway transit, Anda tidak dapat mengaktifkannya saat membuat gateway. Setelah Anda membuat gateway transit, dan itu dalam keadaan tersedia, Anda kemudian dapat memodifikasinya untuk mengaktifkan dukungan Enkripsi. Untuk informasi selengkapnya, lihat the section called “Dukungan Enkripsi”.

Untuk membuat gateway transit menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Transit Gateways.
3. Pilih Buat gateway transit.
4. Untuk tag Nama, secara opsional masukkan nama untuk gateway transit. Tag nama dapat membuatnya lebih mudah untuk mengidentifikasi gateway tertentu dari daftar gateway. Saat Anda menambahkan tag Nama, tag dibuat dengan kunci Nama dan dengan nilai yang sama dengan nilai yang Anda masukkan.
5. Untuk Deskripsi, secara opsional masukkan deskripsi untuk gateway transit.
6. Untuk Amazon side Autonomous System Number (ASN), tinggalkan nilai default untuk menggunakan ASN default atau masukkan ASN pribadi untuk gateway transit Anda. Ini harus menjadi ASN untuk AWS sisi sesi Border Gateway Protocol (BGP).

Rentangnya adalah 64512 hingga 65534 untuk ASN 16-bit.

Kisarannya adalah 4200000000 hingga 4294967294 untuk ASN 32-bit.

Jika Anda memiliki penyebaran Multi-wilayah, kami sarankan Anda menggunakan ASN unik untuk setiap gateway transit Anda.

7. Untuk dukungan DNS, pilih opsi ini jika Anda memerlukan VPC untuk menyelesaikan nama host DNS IPv4 publik ke alamat IPv4 pribadi saat ditanyakan dari instance di VPC lain yang dilampirkan ke gateway transit.
8. Untuk dukungan Referensi Grup Keamanan, aktifkan fitur ini untuk mereferensikan grup keamanan di seluruh VPC yang dilampirkan ke gateway transit. Untuk informasi selengkapnya tentang referensi grup keamanan, lihatthe section called “Referensi kelompok keamanan”.
9. Untuk dukungan VPN ECMP, pilih opsi ini jika Anda memerlukan dukungan perutean Equal Cost Multipath (ECMP) antara terowongan VPN. Jika koneksi mengiklankan CIDR yang sama, lalu lintas didistribusikan secara merata di antara mereka.

   Ketika Anda memilih opsi ini, BGP ASN yang diiklankan, maka atribut BGP seperti, harus sama. AS-path

   > **Note**
   >
   > Untuk menggunakan ECMP, Anda harus membuat koneksi VPN yang menggunakan perutean dinamis. Koneksi VPN yang menggunakan perutean statis tidak mendukung ECMP.

10. Untuk asosiasi tabel rute default, pilih opsi ini untuk secara otomatis mengaitkan lampiran gateway transit dengan tabel rute default untuk gateway transit.
11. Untuk propagasi tabel rute default, pilih opsi ini untuk secara otomatis menyebarkan lampiran gateway transit ke tabel rute default untuk gateway transit.
12. (Opsional) Untuk menggunakan gateway transit sebagai router untuk lalu lintas multicast, pilih Dukungan multicast.
13. (Opsional) Di bagian opsi Configure-cross-account berbagi, pilih apakah akan menerima lampiran bersama secara otomatis. Jika diaktifkan, lampiran diterima secara otomatis. Jika tidak, Anda harus menerima atau menolak permintaan lampiran.

Untuk Auto accept shared attachment, pilih opsi ini untuk secara otomatis menerima lampiran lintas akun.

14. (Opsional) Untuk blok CIDR gateway Transit, tentukan satu atau beberapa blok CIDR IPv4 atau IPv6 untuk gateway transit Anda.

    Anda dapat menentukan blok CIDR ukuran /24 atau lebih besar (misalnya, /23 atau /22) untuk IPv4, atau blok CIDR ukuran /64 atau lebih besar (misalnya, /63 atau/62) untuk IPv6. Anda dapat mengaitkan rentang alamat IP publik atau pribadi apa pun, kecuali untuk alamat di 169.254.0.0/16 rentang, dan rentang yang tumpang tindih dengan alamat untuk lampiran VPC dan jaringan lokal Anda.

    > **Note**
    >
    > Blok CIDR gateway transit digunakan jika Anda mengonfigurasi lampiran Connect (GRE), VPN PrivateIP, atau lampiran Client VPN. Transit Gateway menetapkan IP untuk lampiran Tunnel endpoint (GRE/PrivateIP VPN) dan Client VPN dari rentang ini.

15. Pilih Buat gateway transit.

Untuk membuat gateway transit menggunakan AWS CLI

Gunakan perintah create-transit-gateway.

Lihat informasi gateway transit di AWS Transit Gateway

Lihat salah satu gateway transit Anda.

Untuk melihat gateway transit menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Transit Gateways. Detail untuk gateway transit ditampilkan di bawah daftar gateway di halaman.

Untuk melihat gateway transit menggunakan AWS CLI

Gunakan perintah describe-transit-gateways.

Kelola tag gateway transit di AWS Transit Gateway

Tambahkan tag ke sumber daya Anda untuk membantu mengatur dan mengidentifikasi sumber daya tersebut, misalnya berdasarkan tujuan, pemilik, atau lingkungan. Anda dapat menambahkan beberapa tag ke setiap gateway transit. Kunci tag harus unik untuk setiap gateway transit. Jika Anda menambahkan tag dengan kunci yang sudah dikaitkan dengan gateway transit, itu akan memperbarui nilai tag tersebut. Untuk informasi selengkapnya, lihat Menandai EC2 Sumber Daya Amazon Anda.

Tambahkan tag ke gateway transit menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Transit Gateways.
3. Pilih gateway transit yang ingin Anda tambahkan atau edit tag.
4. Pilih tab Tag di bagian bawah halaman.
5. Pilih Kelola tanda.
6. Pilih Tambahkan tag baru.
7. Masukkan Kunci dan Nilai untuk tag.
8. Pilih Simpan.

Ubah gateway transit di AWS Transit Gateway

Anda dapat mengubah opsi konfigurasi untuk gateway transit. Saat Anda memodifikasi gateway transit, setiap lampiran gateway transit yang ada tidak mengalami gangguan layanan apa pun.

Anda tidak dapat mengubah gateway transit yang telah dibagikan dengan Anda.

Anda tidak dapat menghapus blok CIDR untuk gateway transit jika salah satu alamat IP saat ini digunakan untuk rekan Connect.

> **Note**
>
> Gateway transit yang mengaktifkan Dukungan Enkripsi dapat dilampirkan VPCs dengan Kontrol Enkripsi di monitor atau mode Terapkan, atau VPCs yang tidak mengaktifkan Kontrol Enkripsi. VPCs yang memiliki Encryption Controls dalam mode Enforce HANYA dapat dilampirkan ke Transit Gateways yang mengaktifkan Encryption Support.

Untuk informasi selengkapnya, lihat the section called “Dukungan Enkripsi”.

Untuk memodifikasi gateway transit

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Transit Gateways.
3. Pilih gateway transit untuk dimodifikasi.
4. Pilih Tindakan, Ubah gateway transit.
5. Ubah opsi sesuai kebutuhan, dan pilih Ubah gateway transit.

Untuk memodifikasi gateway transit Anda menggunakan AWS CLI

Gunakan perintah modify-transit-gateway.

Menerima pembagian sumber daya AWS Transit Gateway menggunakan AWS Resource Access Manager konsol

Jika Anda ditambahkan ke pembagian sumber daya, Anda menerima undangan untuk bergabung dengan pembagian sumber daya. Anda harus menerima pembagian sumber daya melalui konsol AWS Resource Access Manager (AWS RAM) sebelum dapat mengakses sumber daya bersama.

Untuk menerima pembagian sumber daya

1. Buka AWS RAM konsol di https://console.aws.amazon.com/ram/.
2. Di panel navigasi, pilih Dibagikan dengan saya, Berbagi sumber daya.
3. Pilih bagian sumber daya.
4. Pilih Terima pembagian sumber daya.
5. Untuk melihat gateway transit bersama, buka halaman Transit Gateways di konsol VPC Amazon.

Menerima lampiran bersama di AWS Transit Gateway

Jika Anda tidak mengaktifkan fungsionalitas Auto accept shared attachment saat membuat gateway transit, Anda harus secara manual menerima lampiran lintas akun (bersama) menggunakan Konsol VPC Amazon atau CLI. AWS

Untuk menerima lampiran bersama secara manual

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Lampiran Transit Gateway.
3. Pilih lampiran gateway transit yang menunggu penerimaan.
4. Pilih Tindakan, Terima lampiran gateway transit.

Untuk menerima lampiran bersama menggunakan AWS CLI

Gunakan perintah accept-transit-gateway-vpc-attachment.

Menghapus gateway transit di AWS Transit Gateway

Anda tidak dapat menghapus gateway transit dengan lampiran yang ada. Anda harus menghapus semua lampiran sebelum dapat menghapus gateway transit.

Untuk menghapus gateway transit menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pilih gateway transit untuk dihapus.
3. Pilih Tindakan, Hapus gateway transit. Masuk **`delete`** dan pilih Hapus untuk mengonfirmasi penghapusan.

Untuk menghapus gateway transit menggunakan AWS CLI

Gunakan perintah delete-transit-gateway.

Dukungan Enkripsi untuk AWS Transit Gateway

Kontrol Enkripsi memungkinkan Anda untuk mengaudit status enkripsi arus lalu lintas di VPC Anda dan kemudian menerapkan enkripsi dalam perjalanan untuk semua lalu lintas dalam VPC. Ketika Kontrol Enkripsi VPC dalam mode penegakan, semua Antarmuka Jaringan Elastis (ENI) dalam VPC tersebut akan dibatasi untuk dilampirkan hanya ke instans yang mampu enkripsi AWS Nitro; dan hanya AWS layanan yang mengenkripsi data dalam perjalanan yang akan diizinkan untuk dilampirkan ke Kontrol Enkripsi yang diberlakukan VPC. Untuk informasi lebih lanjut tentang Kontrol Enkripsi VPC, silakan lihat dokumentasi ini.

Dukungan Enkripsi Transit Gateway dan Kontrol Enkripsi VPC

Dukungan Enkripsi pada Transit Gateway memungkinkan Anda untuk menerapkan enkripsi dalam transit untuk lalu lintas antara VPC yang dilampirkan ke Gateway Transit. Anda perlu mengaktifkan Encryption Support secara manual di Transit Gateway menggunakan perintah modify-transit-gateway untuk mengenkripsi lalu lintas antar VPC. Setelah diaktifkan, semua lalu lintas akan melintasi 100% tautan terenkripsi antara VPC yang berada dalam mode Menegakkan (tanpa pengecualian) melalui Transit Gateway. Anda juga dapat menghubungkan VPC yang tidak mengaktifkan Kontrol Enkripsi, atau berada dalam mode Monitor melalui Transit Gateway yang mengaktifkan Dukungan Enkripsi. Dalam skenario ini Transit Gateway dijamin untuk mengenkripsi lalu lintas hingga lampiran Transit Gateway di VPC yang tidak berjalan dalam mode penegakan. Di luar itu, itu tergantung pada contoh lalu lintas dikirim ke dalam VPC yang tidak berjalan dalam mode penegakan.

Anda hanya dapat menambahkan dukungan enkripsi ke gateway transit yang ada dan tidak saat Anda membuatnya. Saat Transit Gateway bertransisi ke status Encryption Support Enabled, tidak akan ada downtime pada Transit Gateway atau lampiran. Migrasi mulus dan transparan tanpa lalu lintas yang dijatuhkan. Untuk langkah-langkah untuk memodifikasi gateway transit untuk menambahkan Encryption Support, lihatUbah gateway transit.

Persyaratan

Sebelum mengaktifkan dukungan enkripsi pada gateway transit, pastikan bahwa:

- Gateway transit tidak memiliki lampiran Connect
- Gerbang transit tidak memiliki lampiran Peering
- Gateway transit tidak memiliki lampiran Network Firewall
- Gateway transit tidak memiliki lampiran VPN Concentrator
- Gateway transit tidak memiliki lampiran Client VPN
- Gateway transit tidak mengaktifkan referensi grup keamanan
- Gateway transit tidak mengaktifkan fitur Multicast

Status Dukungan Enkripsi

Gateway transit dapat memiliki salah satu status enkripsi berikut:

- mengaktifkan - Gateway transit sedang dalam proses mengaktifkan dukungan enkripsi. Proses ini bisa memakan waktu hingga 14 hari untuk menyelesaikannya.

- diaktifkan - Dukungan enkripsi diaktifkan pada gateway transit. Anda dapat membuat lampiran VPC dengan Kontrol Enkripsi diberlakukan.
- menonaktifkan - Gateway transit sedang dalam proses menonaktifkan dukungan Enkripsi.
- dinonaktifkan - Dukungan enkripsi dinonaktifkan pada gateway transit.

Aturan lampiran Transit Gateway

Jika gateway transit mengaktifkan dukungan Enkripsi, aturan lampiran berikut berlaku:

- Saat status enkripsi gateway transit diaktifkan atau dinonaktifkan, Anda dapat membuat lampiran Direct Connect, lampiran VPN, dan lampiran VPC yang tidak dalam mode Encryption Control yang diberlakukan atau ditegakkan.
- Saat status enkripsi gateway transit diaktifkan, Anda dapat membuat lampiran VPC, Direct Connect, lampiran VPN, dan lampiran VPC dalam mode Kontrol Enkripsi apa pun.
- Ketika status enkripsi gateway transit dinonaktifkan, Anda tidak dapat membuat lampiran VPC baru dengan kontrol Enkripsi diberlakukan.
- Connect attachment, lampiran Peering, lampiran Network Firewall, lampiran VPN Concentrator, lampiran Client VPN, referensi grup keamanan, dan fitur multicast tidak didukung dengan Encryption Support.

Mencoba membuat lampiran yang tidak kompatibel akan gagal dengan kesalahan API.

Lampiran Amazon VPC di Transit Gateway AWS

Lampiran Amazon Virtual Private Cloud (VPC) ke gateway transit memungkinkan Anda merutekan lalu lintas ke dan dari satu atau beberapa subnet VPC. Saat Anda melampirkan VPC ke gateway transit, Anda harus menentukan satu subnet dari setiap Availability Zone yang akan digunakan oleh gateway transit untuk merutekan lalu lintas. Subnet yang ditentukan berfungsi sebagai titik masuk dan keluar untuk lalu lintas gateway transit. Lalu lintas hanya dapat mencapai sumber daya di subnet lain dalam Availability Zone yang sama jika subnet lampiran gateway transit memiliki rute yang sesuai yang dikonfigurasi dalam tabel rute mereka yang menunjuk ke subnet target.

Batas

- Saat Anda melampirkan VPC ke gateway transit, sumber daya apa pun di Availability Zones yang tidak memiliki lampiran gateway transit tidak dapat mencapai gateway transit.

> **Note**
>
> Dalam Availability Zones yang memiliki lampiran gateway transit, lalu lintas hanya diteruskan ke gateway transit dari subnet tertentu yang terkait dengan lampiran. Jika ada rute ke gateway transit dalam tabel rute subnet, lalu lintas diteruskan ke gateway transit hanya ketika gateway transit memiliki lampiran di subnet di Availability Zone yang sama dan tabel rute subnet lampiran berisi rute yang sesuai ke tujuan yang dituju lalu lintas dalam VPC.

- Gateway transit tidak mendukung resolusi DNS untuk nama DNS kustom dari VPCs pengaturan terlampir menggunakan zona host pribadi di Amazon Route 53. Untuk mengonfigurasi resolusi nama untuk zona host pribadi untuk semua yang VPCs dilampirkan ke gateway transit, lihat Manajemen DNS terpusat cloud hybrid dengan Amazon Route 53 dan AWS Transit Gateway.
- Gateway transit tidak mendukung perutean antara VPCs dengan identik CIDRs, atau jika CIDR dalam rentang tumpang tindih dengan CIDR dalam VPC terlampir. Jika Anda melampirkan VPC ke gateway transit dan CIDR-nya identik dengan, atau tumpang tindih dengan, CIDR dari VPC lain yang sudah terpasang ke gateway transit, rute untuk VPC yang baru dilampirkan tidak disebarkan ke tabel rute gateway transit.
- Anda tidak dapat membuat lampiran untuk subnet VPC yang berada di Zona Lokal. Namun, Anda dapat mengonfigurasi jaringan Anda sehingga subnet di Zona Lokal dapat terhubung ke gateway transit melalui Availability Zone induk. Untuk informasi selengkapnya, lihat Menghubungkan subnet Zona Lokal ke gateway transit.
- Anda tidak dapat membuat lampiran gateway transit menggunakan subnet IPv6 -only. Subnet lampiran gateway transit juga harus mendukung IPv4 alamat.
- Gateway transit harus memiliki setidaknya satu lampiran VPC sebelum gateway transit dapat ditambahkan ke tabel rute.

Persyaratan tabel rute untuk lampiran VPC

Lampiran VPC gateway transit memerlukan konfigurasi tabel rute tertentu agar berfungsi dengan baik:

- Tabel rute subnet lampiran: Subnet yang terkait dengan lampiran gateway transit harus memiliki entri tabel rute untuk tujuan apa pun dalam VPC yang harus dapat dijangkau melalui gateway transit. Ini termasuk rute ke subnet lain, gateway internet, gateway NAT, dan titik akhir VPC.

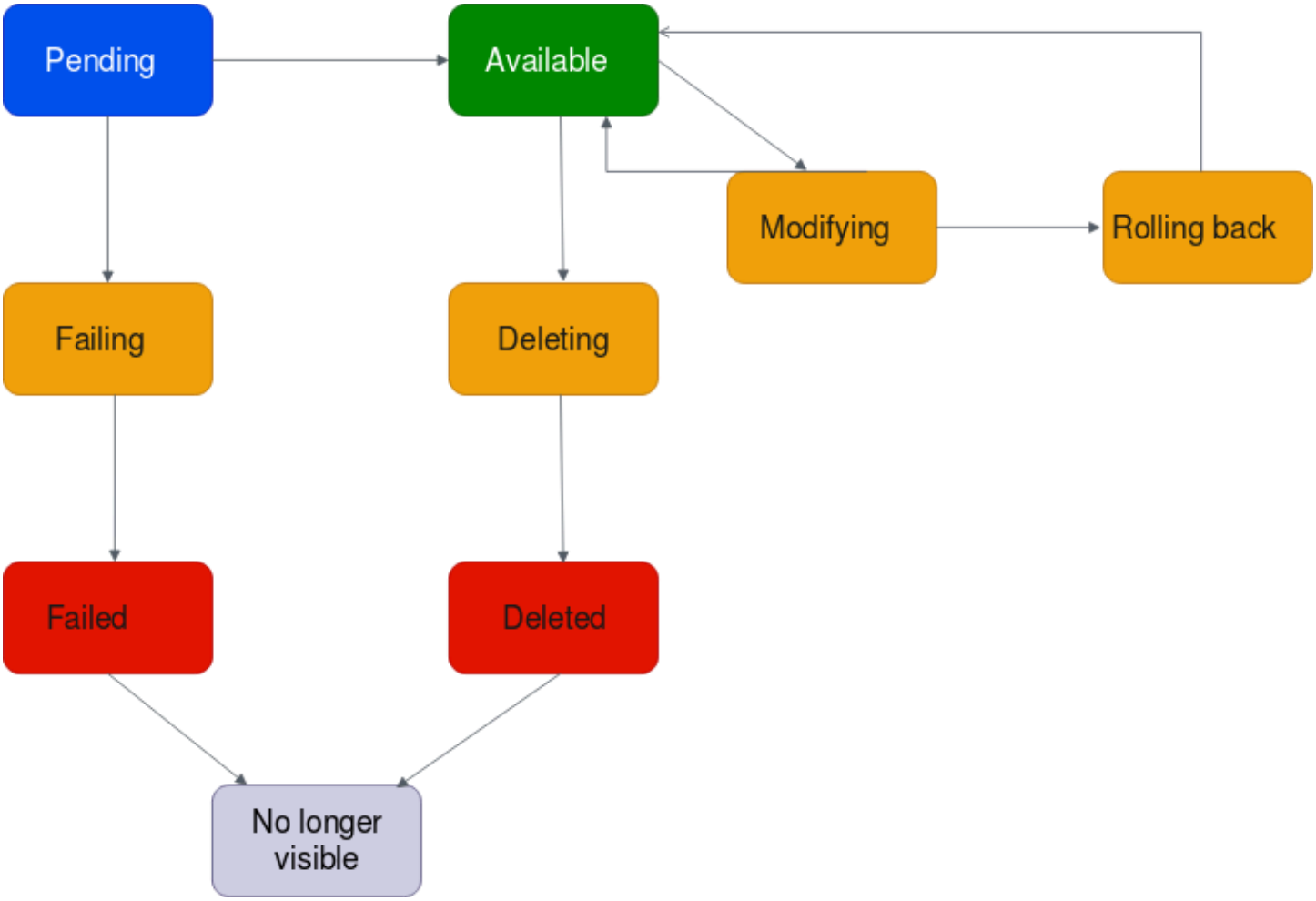
- Tabel rute subnet target: Subnet yang berisi sumber daya yang perlu berkomunikasi melalui gateway transit harus memiliki rute yang menunjuk kembali ke gateway transit untuk mengembalikan lalu lintas ke tujuan eksternal.
- Lalu lintas VPC lokal: Lampiran gateway transit tidak secara otomatis mengaktifkan komunikasi antar subnet dalam VPC yang sama. Aturan perutean VPC standar berlaku, dan rute lokal (VPC CIDR) harus ada dalam tabel rute untuk komunikasi intra-VPC.

> **Note**
>
> Memiliki rute yang dikonfigurasi dalam subnet non-lampiran dalam Availability Zone yang sama tidak memungkinkan arus lalu lintas. Hanya subnet spesifik yang terkait dengan lampiran gateway transit yang dapat berfungsi sebagai entry/exit titik untuk lalu lintas gateway transit.

Siklus hidup lampiran VPC

Lampiran VPC melewati berbagai tahap, dimulai saat permintaan dimulai. Pada setiap tahap, mungkin ada tindakan yang dapat Anda lakukan, dan pada akhir siklus hidupnya, lampiran VPC tetap terlihat di Amazon Virtual Private Cloud Console dan di API atau output baris perintah, untuk jangka waktu tertentu.

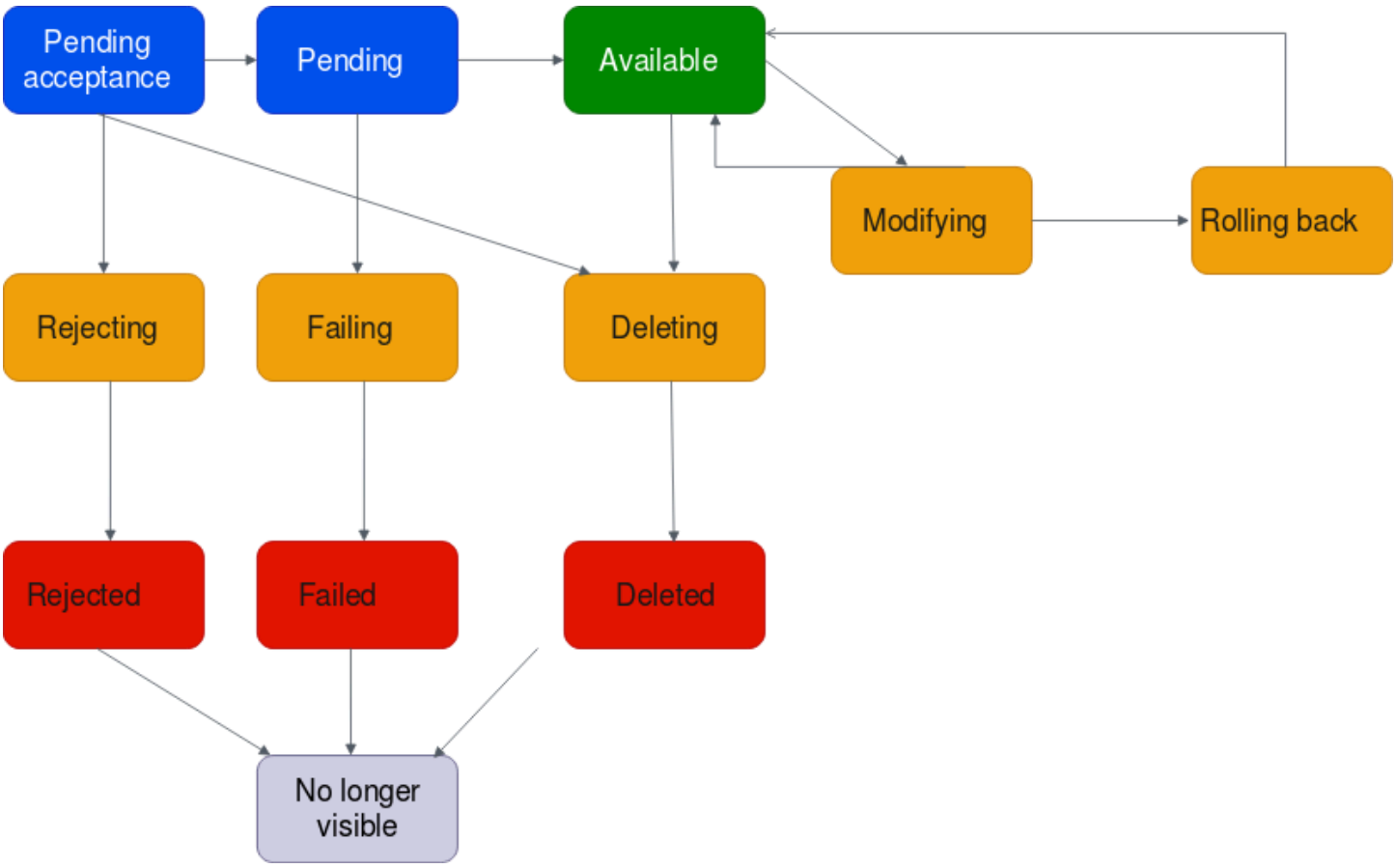
Diagram berikut menunjukkan status yang dapat dilalui lampiran dalam satu konfigurasi akun, atau konfigurasi lintas akun yang mengaktifkan Auto accept shared attachment.



- Tertunda: Permintaan untuk lampiran VPC telah dimulai dan sedang dalam proses penyediaan. Pada tahap ini, lampiran bisa gagal, atau bisa pergi ke`available`.
- Gagal: Permintaan untuk lampiran VPC gagal. Pada tahap ini, lampiran VPC masuk ke. `failed`
- Gagal: Permintaan untuk lampiran VPC telah gagal. Sementara dalam keadaan ini, itu tidak dapat dihapus. Lampiran VPC yang gagal tetap terlihat selama 2 jam, dan kemudian tidak lagi terlihat.
- Tersedia: Lampiran VPC tersedia, dan lalu lintas dapat mengalir antara VPC dan gateway transit. Pada tahap ini, lampiran dapat pergi ke`modifying`, atau pergi ke`deleting`.
- Menghapus: Lampiran VPC yang sedang dalam proses dihapus. Pada tahap ini, lampiran bisa masuk ke`deleted`.
- Dihapus: Lampiran `available` VPC telah dihapus. Saat dalam keadaan ini, lampiran VPC tidak dapat dimodifikasi. Lampiran VPC tetap terlihat selama 2 jam, dan kemudian tidak lagi terlihat.
- Memodifikasi: Permintaan telah dibuat untuk memodifikasi properti lampiran VPC. Pada tahap ini, lampiran dapat pergi ke`available`, atau pergi ke`rolling back`.

- Memutar kembali: Permintaan modifikasi lampiran VPC tidak dapat diselesaikan, dan sistem membatalkan perubahan apa pun yang dibuat. Pada tahap ini, lampiran bisa masuk `keavailable`.

Diagram berikut menunjukkan status yang dapat dilalui lampiran dalam konfigurasi lintas akun yang menonaktifkan Auto accept shared attachment.



- Penerimaan tertunda: Permintaan lampiran VPC sedang menunggu penerimaan. Pada tahap ini, lampiran dapat pergi ke`pending`, ke`rejecting`, atau ke`deleting`.
- Menolak: Lampiran VPC yang sedang dalam proses ditolak. Pada tahap ini, lampiran bisa masuk ke`rejected`.
- Ditolak: Lampiran `pending acceptance` VPC telah ditolak. Saat dalam keadaan ini, lampiran VPC tidak dapat dimodifikasi. Lampiran VPC tetap terlihat selama 2 jam, dan kemudian tidak lagi terlihat.
- Tertunda: Lampiran VPC telah diterima dan sedang dalam proses penyediaan. Pada tahap ini, lampiran bisa gagal, atau bisa pergi ke`available`.
- Gagal: Permintaan untuk lampiran VPC gagal. Pada tahap ini, lampiran VPC masuk ke. `failed`

- Gagal: Permintaan untuk lampiran VPC telah gagal. Sementara dalam keadaan ini, itu tidak dapat dihapus. Lampiran VPC yang gagal tetap terlihat selama 2 jam, dan kemudian tidak lagi terlihat.
- Tersedia: Lampiran VPC tersedia, dan lalu lintas dapat mengalir antara VPC dan gateway transit. Pada tahap ini, lampiran dapat pergi ke`modifying`, atau pergi ke`deleting`.
- Menghapus: Lampiran VPC yang sedang dalam proses dihapus. Pada tahap ini, lampiran bisa masuk ke`deleted`.
- Dihapus: Lampiran `available` atau `pending acceptance` VPC telah dihapus. Saat dalam keadaan ini, lampiran VPC tidak dapat dimodifikasi. Lampiran VPC tetap terlihat 2 jam, dan kemudian tidak lagi terlihat.
- Memodifikasi: Permintaan telah dibuat untuk memodifikasi properti lampiran VPC. Pada tahap ini, lampiran dapat pergi ke`available`, atau pergi ke`rolling back`.
- Memutar kembali: Permintaan modifikasi lampiran VPC tidak dapat diselesaikan, dan sistem membatalkan perubahan apa pun yang dibuat. Pada tahap ini, lampiran bisa masuk ke`available`.

Mode alat

Jika Anda berencana untuk mengonfigurasi alat jaringan stateful di VPC, Anda dapat mengaktifkan dukungan mode alat untuk lampiran VPC tempat alat berada saat Anda membuat lampiran. Ini memastikan bahwa AWS Transit Gateway menggunakan Availability Zone yang sama untuk lampiran VPC tersebut selama masa arus lalu lintas antara sumber dan tujuan. Ini juga memungkinkan gateway transit untuk mengirim lalu lintas ke Availability Zone apa pun di VPC selama ada asosiasi subnet di zona itu. Meskipun mode alat hanya didukung pada lampiran VPC, aliran jaringan dapat berasal dari jenis lampiran gateway transit lainnya, termasuk lampiran VPC, VPN, dan Connect. Mode alat juga berfungsi untuk arus jaringan yang memiliki sumber dan tujuan di berbagai tempat Wilayah AWS. Alur jaringan berpotensi diseimbangkan kembali di berbagai Availability Zone jika Anda awalnya tidak mengaktifkan mode alat tetapi kemudian mengedit konfigurasi lampiran untuk mengaktifkannya. Anda dapat mengaktifkan atau menonaktifkan mode alat menggunakan konsol atau baris perintah atau API.

Mode alat di AWS Transit Gateway mengoptimalkan perutean lalu lintas dengan mempertimbangkan Zona Ketersediaan sumber dan tujuan saat menentukan jalur melalui VPC mode alat. Pendekatan ini meningkatkan efisiensi dan mengurangi latensi. Perilaku bervariasi tergantung pada konfigurasi spesifik dan pola lalu lintas. Berikut ini adalah contoh skenario.

Skenario 1: Perutean Lalu Lintas Intra-Availability Zone melalui VPC Appliance

Ketika lalu lintas mengalir dari Availability Zone sumber us-east-1a ke Availability Zone tujuan us-east-1a, dengan lampiran VPC Mode Appliance di us-east-1a dan us-east-1b, Transit Gateway memilih antarmuka jaringan dari us-east-1a dalam VPC alat. Availability Zone ini dipertahankan selama seluruh durasi arus lalu lintas antara sumber dan tujuan.

Skenario 2: Perutean Lalu Lintas Zona Antar-Ketersediaan melalui VPC Peralatan

Untuk lalu lintas yang mengalir dari Availability Zone sumber us-east-1a ke Availability Zone tujuan us-east-1b, dengan lampiran VPC Mode Appliance di us-east-1a dan us-east-1b, Transit Gateway menggunakan algoritme hash aliran untuk memilih us-east-1a atau us-east-1b di VPC alat. Availability Zone yang dipilih digunakan secara konsisten selama masa pakai aliran.

Skenario 3: Merutekan lalu lintas melalui VPC alat tanpa data Availability Zone

Ketika lalu lintas berasal dari Availability Zone sumber us-east-1a ke tujuan tanpa informasi Availability Zone (misalnya, lalu lintas terikat internet), dengan lampiran VPC Mode Appliance di us-east-1a dan us-east-1b, Transit Gateway memilih antarmuka jaringan dari us-east-1a dalam VPC alat.

Skenario 4: Merutekan lalu lintas melalui VPC alat di Availability Zone yang berbeda dari sumber atau tujuan

Ketika lalu lintas mengalir dari Availability Zone sumber us-east-1a ke Availability Zone tujuan us-east-1b, dengan lampiran VPC Mode Appliance di Availability Zone yang berbeda misalnya us-east-1c dan us-east-1d, Transit Gateway menggunakan algoritme hash aliran untuk memilih us-east-1c atau us-east-1d di VPC alat. Availability Zone yang dipilih digunakan secara konsisten selama masa pakai aliran.

> **Note**
>
> Mode alat hanya didukung untuk lampiran VPC. Pastikan propagasi rute diaktifkan untuk tabel rute yang terkait dengan lampiran VPC alat.

Referensi kelompok keamanan

Anda dapat menggunakan fitur ini untuk menyederhanakan manajemen grup keamanan dan kontrol instance-to-instance lalu lintas lintas VPCs yang dilampirkan ke gateway transit yang sama.

Anda dapat mereferensikan silang grup keamanan hanya dalam aturan masuk. Aturan keamanan keluar tidak mendukung referensi grup keamanan. Tidak ada biaya tambahan yang terkait dengan mengaktifkan atau menggunakan referensi grup keamanan.

Dukungan referensi grup keamanan dapat dikonfigurasi untuk gateway transit dan lampiran VPC gateway transit dan hanya akan berfungsi jika telah diaktifkan untuk gateway transit dan lampiran VPC-nya.

Batasan

Batasan berikut berlaku saat menggunakan referensi grup keamanan dengan lampiran VPC.

- Referensi grup keamanan tidak didukung di seluruh koneksi peering gateway transit. Keduanya VPCs harus dilampirkan ke gateway transit yang sama.
- Referensi grup keamanan tidak didukung untuk lampiran VPC di zona ketersediaan use1-az3.
- Referensi grup keamanan tidak didukung untuk titik PrivateLink akhir. Sebaiknya gunakan aturan keamanan berbasis IP CIDR sebagai alternatif.
- Referensi grup keamanan berfungsi untuk Elastic File System (EFS) selama aturan grup keamanan allow all egress dikonfigurasi untuk antarmuka EFS di VPC.
- Untuk konektivitas Zona Lokal melalui gateway transit, hanya Local Zones berikut yang didukung: us-east-1-atl-2a, us-east-1-dfw-2a, us-east-1-iah-2a, us-west-2-lax-1a, us-west-2-lax-1b, us-east-1-mia-2a, us-east-1-chi-2a, dan us-west-2-phx-2a.
- Sebaiknya nonaktifkan fitur ini di tingkat attachment VPC VPCs dengan subnet di Local Zones, Outposts, dan AWS Wavelength Zones yang tidak didukung AWS , karena dapat menyebabkan gangguan layanan.
- Jika Anda memiliki VPC inspeksi, maka referensi grup keamanan melalui gateway transit tidak berfungsi di seluruh Load AWS Balancer Gateway atau Network Firewall. AWS

Tugas

- Buat lampiran VPC di AWS Transit Gateway
- Memodifikasi lampiran VPC di AWS Transit Gateway
- Ubah tag lampiran VPC di AWS Transit Gateway
- Lihat lampiran VPC di AWS Transit Gateway
- Menghapus lampiran VPC di AWS Transit Gateway
- Perbarui AWS Transit Gateway aturan masuk grup keamanan

- Identifikasi AWS Transit Gateway kelompok keamanan yang direferensikan
- Hapus aturan grup AWS Transit Gateway keamanan basi
- Memecahkan masalah pembuatan lampiran VPC Gateway AWS Transit

Buat lampiran VPC di AWS Transit Gateway

Untuk membuat lampiran VPC menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Lampiran Transit Gateway.
3. Pilih Buat lampiran gateway transit.
4. Untuk tag Nama, secara opsional masukkan nama untuk lampiran gateway transit.
5. Untuk ID gateway Transit, pilih gateway transit untuk lampiran. Anda dapat memilih gateway transit yang Anda miliki atau gateway transit yang dibagikan dengan Anda.
6. Untuk jenis Lampiran, pilih VPC.
7. Pilih apakah akan mengaktifkan dukungan mode Dukungan DNS, IPv6Support, dan Appliance.

   Jika mode alat dipilih, arus lalu lintas antara sumber dan tujuan menggunakan Availability Zone yang sama untuk lampiran VPC selama masa pakai aliran tersebut.
8. Pilih apakah akan mengaktifkan dukungan Referensi Grup Keamanan. Aktifkan fitur ini untuk mereferensikan grup keamanan di seluruh yang VPCs dilampirkan ke gateway transit. Untuk informasi selengkapnya tentang referensi grup keamanan, lihatthe section called “Referensi kelompok keamanan”.
9. Pilih apakah akan mengaktifkan IPv6Support.
10. Untuk ID VPC, pilih VPC yang dilampirkan pada transit gateway.

    VPC ini harus memiliki setidaknya satu subnet yang terkait dengannya.
11. Untuk Subnet IDs, pilih satu subnet untuk setiap Availability Zone yang akan digunakan oleh gateway transit untuk merutekan lalu lintas. Anda harus memilih setidaknya satu subnet. Anda hanya dapat memilih satu subnet per Availability Zone.
12. Pilih Buat lampiran gateway transit.

Untuk membuat lampiran VPC menggunakan AWS CLI

Gunakan perintah create-transit-gateway-vpc-attachment.

Memodifikasi lampiran VPC di AWS Transit Gateway

Untuk memodifikasi lampiran VPC Anda menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Lampiran Transit Gateway.
3. Pilih lampiran VPC, lalu pilih Tindakan, Ubah lampiran gateway transit.
4. Aktifkan atau nonaktifkan salah satu dari berikut ini:
   - Dukungan DNS
   - IPv6 dukungan
   - Dukungan mode alat
5. Untuk menambah atau menghapus subnet dari lampiran, pilih atau kosongkan kotak centang dengan ID Subnet yang ingin Anda tambahkan atau hapus.

   > **Note**
   >
   > Menambahkan atau memodifikasi subnet lampiran VPC dapat memengaruhi lalu lintas data saat lampiran dalam keadaan modifikasi.

6. Untuk dapat mereferensikan grup keamanan di seluruh yang VPCs dilampirkan ke gateway transit, pilih dukungan Referensi Grup Keamanan. Untuk informasi selengkapnya tentang referensi grup keamanan, lihatthe section called “Referensi kelompok keamanan”.

   > **Note**
   >
   > Jika Anda menonaktifkan referensi grup keamanan untuk gateway transit yang ada, itu akan dinonaktifkan pada semua lampiran VPC.

7. Pilih Ubah lampiran gateway transit.

Untuk memodifikasi lampiran VPC Anda menggunakan AWS CLI

Gunakan perintah modify-transit-gateway-vpc-attachment.

Ubah tag lampiran VPC di AWS Transit Gateway

Untuk memodifikasi tag lampiran VPC Anda menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Lampiran Transit Gateway.
3. Pilih lampiran VPC, lalu pilih Tindakan, Kelola tag.
4. [Menambahkan tanda] Pilih Tambahkan tanda baru dan lakukan hal berikut:
   - Untuk Kunci, masukkan nama kunci.
   - Untuk Nilai, masukkan nilai kunci.
5. [Hapus tag] Di samping tag, pilih Hapus.
6. Pilih Simpan.

Tag lampiran VPC hanya dapat dimodifikasi menggunakan konsol.

Lihat lampiran VPC di AWS Transit Gateway

Untuk melihat lampiran VPC Anda menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Lampiran Transit Gateway.
3. Di kolom Jenis sumber daya, cari VPC. Ini adalah lampiran VPC.
4. Pilih lampiran untuk melihat detailnya.

Untuk melihat lampiran VPC Anda menggunakan AWS CLI

Gunakan perintah describe-transit-gateway-vpc-attachments.

Menghapus lampiran VPC di AWS Transit Gateway

Untuk menghapus lampiran VPC menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Lampiran Transit Gateway.
3. Pilih lampiran VPC.

4. Pilih Tindakan, Hapus lampiran gateway transit.
5. Saat diminta, masukkan **`delete`** dan pilih Hapus.

Untuk menghapus lampiran VPC menggunakan AWS CLI

Gunakan perintah delete-transit-gateway-vpc-attachment.

Perbarui AWS Transit Gateway aturan masuk grup keamanan

Anda dapat memperbarui salah satu aturan grup keamanan masuk yang terkait dengan gateway transit. Anda dapat memperbarui aturan grup keamanan menggunakan konsol Konsol VPC Amazon atau dengan menggunakan baris perintah atau API. Untuk informasi selengkapnya tentang referensi grup keamanan, lihatthe section called “Referensi kelompok keamanan”.

Untuk memperbarui aturan 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, Edit aturan masuk untuk mengubah aturan masuk.
4. Untuk menambahkan aturan, pilih Tambahkan aturan dan tentukan jenis, protokol, dan rentang port. Untuk Sumber (aturan masuk), masukkan ID grup keamanan di VPC yang terhubung ke gateway transit.

   > **Note**
   >
   > Grup keamanan dalam VPC yang terhubung ke gateway transit tidak ditampilkan secara otomatis.

5. Untuk mengedit aturan yang ada, ubah nilainya (misalnya, sumber atau deskripsi).
6. Untuk menghapus aturan, pilih Hapus di sebelah aturan.
7. Pilih Simpan aturan.

Untuk memperbarui aturan inbound menggunakan baris perintah

- authorize-security-group-ingress (AWS CLI)
- Grant-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)

- Revoke-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)
- revoke-security-group-ingress (AWS CLI)

Identifikasi AWS Transit Gateway kelompok keamanan yang direferensikan

Untuk menentukan apakah grup keamanan Anda direferensikan dalam aturan grup keamanan di VPC yang dilampirkan ke gateway transit yang sama, gunakan salah satu perintah berikut.

- describe-security-group-references (AWS CLI)
- Get-EC2SecurityGroupReference (AWS Tools for Windows PowerShell)

Hapus aturan grup AWS Transit Gateway keamanan basi

Aturan grup keamanan basi adalah aturan yang mereferensikan grup keamanan yang dihapus dalam VPC yang sama atau di VPC yang dilampirkan ke gateway transit yang sama. Bila aturan grup keamanan menjadi kedaluwarsa, aturan grup tidak secara otomatis terhapus dari grup keamanan Anda—Anda harus menghapusnya secara manual.

Anda dapat melihat dan menghapus aturan grup keamanan kedaluwarsa untuk VPC menggunakan konsol Amazon VPC.

Untuk melihat dan menghapus aturan grup keamanan yang kedaluwarsa

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Grup keamanan.
3. Pilih Tindakan, Kelola aturan kedaluwarsa.
4. Untuk VPC, pilih VPC dengan aturan kedaluwarsa.
5. Pilih Sunting.
6. Pilih tombol Hapus di samping aturan yang ingin Anda hapus. Pilih Tinjau perubahan, Simpan aturan.

Untuk mendeskripsikan aturan grup keamanan basi Anda menggunakan baris perintah

- describe-stale-security-groups (AWS CLI)
- Get-EC2StaleSecurityGroup (AWS Tools for Windows PowerShell)

Setelah mengidentifikasi aturan grup keamanan basi, Anda dapat menghapusnya menggunakan revoke-security-group-egressperintah revoke-security-group-ingressatau.

Memecahkan masalah pembuatan lampiran VPC Gateway AWS Transit

Topik berikut dapat membantu Anda memecahkan masalah yang mungkin Anda miliki saat membuat lampiran VPC.

Masalah

Lampiran VPC gagal.

Penyebab

Penyebabnya mungkin salah satu dari berikut ini:

1. Pengguna yang membuat lampiran VPC tidak memiliki izin yang benar untuk membuat peran terkait layanan.
2. Ada masalah pelambatan karena terlalu banyak permintaan IAM, misalnya yang Anda gunakan CloudFormation untuk membuat izin dan peran.
3. Akun memiliki peran terkait layanan, dan peran terkait layanan telah dimodifikasi.
4. Gerbang transit tidak ada di `available` negara bagian.

Solusi

Tergantung pada penyebabnya, coba yang berikut ini:

1. Verifikasi bahwa pengguna memiliki izin yang benar untuk membuat peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran terkait layanan dalam Panduan Pengguna IAM. Setelah pengguna memiliki izin, buat lampiran VPC.
2. Buat lampiran VPC secara manual. Untuk informasi selengkapnya, lihat the section called “Buat lampiran VPC”.
3. Verifikasi bahwa peran terkait layanan memiliki izin yang benar. Untuk informasi selengkapnya, lihat the section called “Gateway transit”.
4. Verifikasi bahwa gateway transit berada di `available` negara bagian. Lihat informasi yang lebih lengkap di the section called “Lihat gateway transit”.

AWS Lampiran fungsi jaringan Transit Gateway

Anda dapat membuat lampiran fungsi jaringan untuk menghubungkan gateway transit Anda secara langsung ke AWS Network Firewall. Ini menghilangkan kebutuhan untuk membuat dan mengelola inspeksi VPCs.

Dengan lampiran firewall, AWS secara otomatis menyediakan dan mengelola semua sumber daya yang diperlukan di belakang layar. Anda akan melihat lampiran gateway transit baru daripada titik akhir firewall individual. Ini menyederhanakan proses penerapan inspeksi lalu lintas jaringan terpusat.

Sebelum Anda dapat menggunakan lampiran firewall, Anda harus terlebih dahulu membuat lampiran di AWS Network Firewall. Untuk langkah-langkah membuat lampiran, lihat Memulai AWS Network Firewall Manajemen di Panduan AWS Network Firewall Pengembang Setelah firewall dibuat, Anda dapat melihat lampiran di konsol Transit Gateway di bawah bagian Lampiran. Lampiran akan terdaftar dengan jenis fungsi Jaringan.

Topik

- Menerima atau menolak lampiran fungsi jaringan AWS Transit Gateway
- Lihat lampiran fungsi jaringan AWS Transit Gateway
- Rutekan lalu lintas melalui lampiran fungsi jaringan AWS Transit Gateway

Menerima atau menolak lampiran fungsi jaringan AWS Transit Gateway

Anda dapat menggunakan konsol Amazon VPC atau AWS Network Firewall CLI atau API untuk menerima atau menolak lampiran fungsi jaringan gateway transit, termasuk lampiran Network Firewall. Jika Anda adalah pemilik gateway transit dan seseorang telah membuat lampiran firewall ke gateway transit Anda dari akun lain, Anda harus menerima atau menolak permintaan lampiran.

Untuk menerima atau menolak lampiran fungsi jaringan menggunakan Network Firewall CLI, lihat *AcceptNetworkFirewallTransitGatewayAttachment* *RejectNetworkFirewallTransitGatewayAttachment* APIs atau di AWS Network Firewall Referensi API.

Menerima atau menolak lampiran fungsi jaringan menggunakan konsol

Gunakan konsol Amazon VPC untuk menerima atau menolak lampiran fungsi jaringan gateway transit.

Untuk menerima atau menolak lampiran fungsi jaringan menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Transit Gateways.
3. Pilih Lampiran gateway Transit.
4. Pilih lampiran dengan status Penerimaan tertunda dan jenis fungsi Jaringan.
5. Pilih Tindakan, lalu pilih Terima lampiran atau Tolak lampiran.
6. Di kotak dialog konfirmasi, pilih Terima atau Tolak.

Jika Anda menerima lampiran, itu menjadi aktif dan firewall dapat memeriksa lalu lintas. Jika Anda menolak lampiran, itu memasuki status ditolak dan pada akhirnya akan dihapus.

Lihat lampiran fungsi jaringan AWS Transit Gateway

Anda dapat melihat lampiran fungsi jaringan, termasuk AWS Network Firewall lampiran Anda, menggunakan Konsol VPC Amazon atau konsol Manajer Jaringan untuk mendapatkan representasi visual dari topologi jaringan Anda.

Melihat lampiran fungsi jaringan menggunakan konsol Network Manager

Anda dapat melihat lampiran fungsi jaringan menggunakan konsol Network Manager.

Untuk melihat lampiran firewall di Network Manager

1. Buka konsol Network Manager di https://console.aws.amazon.com/networkmanager/rumah/.
2. Buat jaringan global di Network Manager jika Anda belum memilikinya.
3. Daftarkan gateway transit Anda dengan Network Manager.
4. Di bawah Jaringan Global, pilih jaringan global tempat lampiran berada.
5. Di panel navigasi, pilih Gateway transit.
6. Pilih gateway transit yang ingin Anda lihat lampirannya.
7. Pilih tampilan pohon topologi. Lampiran Network Firewall muncul dengan ikon fungsi jaringan.
8. Untuk melihat detail tentang lampiran firewall tertentu, pilih gateway transit di tampilan topologi, lalu pilih tab Fungsi jaringan.

Konsol Network Manager menyediakan informasi terperinci tentang lampiran firewall Anda, termasuk statusnya, gateway transit terkait, dan Availability Zones.

Melihat lampiran fungsi jaringan menggunakan konsol Amazon VPC Console

Gunakan konsol VPC untuk melihat daftar jenis lampiran gateway transit Anda.

Untuk melihat jenis lampiran gateway transit menggunakan konsol VPC

- Lihat Lihat lampiran VPC.

Rutekan lalu lintas melalui lampiran fungsi jaringan AWS Transit Gateway

Setelah membuat lampiran fungsi jaringan, Anda perlu memperbarui tabel rute gateway transit Anda untuk mengirim lalu lintas melalui firewall untuk diperiksa menggunakan Konsol VPC Amazon atau dengan menggunakan CLI. Untuk langkah-langkah memperbarui asosiasi tabel rute gateway transit, lihatKaitkan tabel rute gateway transit.

Rutekan lalu lintas melalui lampiran firewall menggunakan konsol

Gunakan konsol Amazon VPC Console untuk merutekan lalu lintas melalui lampiran fungsi jaringan gateway transit.

Untuk merutekan lalu lintas melalui lampiran fungsi jaringan menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Transit Gateways.
3. Pilih tabel rute gerbang Transit.
4. Pilih tabel rute yang ingin Anda ubah.
5. Pilih Tindakan, lalu pilih Buat rute statis.
6. Untuk CIDR, masukkan blok CIDR tujuan untuk rute tersebut.
7. Untuk Lampiran, pilih lampiran fungsi jaringan. Misalnya, ini mungkin AWS Network Firewall lampiran.
8. Pilih Buat rute statis.

> **Note**
>
> Hanya rute statis yang didukung.

Lalu lintas yang cocok dengan blok CIDR di tabel rute Anda sekarang akan dikirim ke lampiran firewall untuk diperiksa sebelum diteruskan ke tujuan akhirnya.

Rutekan lalu lintas melalui lampiran fungsi jaringan menggunakan CLI atau API

Gunakan baris perintah atau API untuk merutekan lampiran fungsi jaringan gateway transit.

Untuk merutekan lalu lintas melalui lampiran fungsi jaringan menggunakan baris perintah atau API

- Gunakan `create-transit-gateway-route`.

  Misalnya, permintaan mungkin untuk merutekan lampiran firewall jaringan:

```
aws ec2 create-transit-gateway-route \
  --transit-gateway-route-table-id tgw-rtb-0123456789abcdef0 \
  --destination-cidr-block 0.0.0.0/0 \
  --transit-gateway-attachment-id tgw-attach-0123456789abcdef0
```

  Output kemudian kembali:

```
{
  "Route": {
    "DestinationCidrBlock": "0.0.0.0/0",
    "TransitGatewayAttachments": [
      {
        "ResourceId": "network-firewall",
        "TransitGatewayAttachmentId": "tgw-attach-0123456789abcdef0",
        "ResourceType": "network-function"
      }
    ],
    "Type": "static",
    "State": "active"
  }
}
```

Lalu lintas yang cocok dengan blok CIDR di tabel rute Anda sekarang akan dikirim ke lampiran firewall untuk diperiksa sebelum diteruskan ke tujuan akhirnya.

AWS Site-to-Site VPN lampiran di AWS Transit Gateway

Anda dapat menghubungkan lampiran Site-to-Site VPN ke gateway AWS transit di Transit Gateway, yang memungkinkan Anda menghubungkan VPC dan jaringan lokal. Rute dinamis dan statis didukung, serta IPv4 dan IPv6.

Persyaratan

- Melampirkan koneksi VPN ke gateway transit Anda mengharuskan Anda menentukan gateway pelanggan VPN, yang memiliki persyaratan perangkat tertentu. Sebelum membuat lampiran Site-to-Site VPN, tinjau persyaratan gateway pelanggan untuk memastikan bahwa gateway Anda diatur dengan benar. Untuk informasi selengkapnya tentang persyaratan ini, termasuk contoh file konfigurasi gateway, lihat Persyaratan untuk perangkat gateway pelanggan Site-to-Site VPN Anda di Panduan AWS Site-to-Site VPN Pengguna.
- Untuk VPN statis, Anda juga harus terlebih dahulu menambahkan rute statis ke tabel rute gateway transit. Rute statis dalam tabel rute gateway transit yang menargetkan lampiran VPN tidak difilter oleh Site-to-Site VPN karena ini memungkinkan arus lalu lintas keluar yang tidak diinginkan saat menggunakan VPN. BGP-based Untuk langkah-langkah untuk menambahkan rute statis ke tabel rute gateway transit, lihatBuat rute statis.

Anda dapat membuat, melihat, atau menghapus lampiran Site-to-Site VPN gateway transit menggunakan konsol VPC Amazon atau menggunakan CLI AWS .

Tugas

- Buat lampiran gateway transit ke VPN di AWS Transit Gateway
- Lihat lampiran VPN di AWS Transit Gateway
- Hapus lampiran VPN di AWS Transit Gateway

Buat lampiran gateway transit ke VPN di AWS Transit Gateway

Untuk membuat lampiran VPN menggunakan konsol tersebut

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Lampiran Transit Gateway.
3. Pilih Buat lampiran gateway transit.

4. Untuk ID gateway Transit, pilih gateway transit untuk lampiran. Anda dapat memilih gateway transit yang Anda miliki.
5. Untuk Jenis lampiran, mohon untuk memilih VPN.
6. Untuk Gateway Pelanggan, lakukan salah satu dari hal-hal berikut:
   - Untuk menggunakan gateway pelanggan yang sudah ada, pilih Yang sudah ada, dan kemudian pilih gateway untuk digunakan.

     Jika gateway pelanggan Anda berada di belakang perangkat terjemahan alamat jaringan (NAT) yang diaktifkan untuk NAT traversal (NAT-T), gunakan alamat IP publik perangkat NAT Anda, dan sesuaikan aturan firewall Anda untuk membuka blokir port UDP 4500.
   - Untuk membuat gateway pelanggan, pilih Baru, lalu untuk Alamat IP, ketik alamat IP publik statis dan BGP ASN.

     Untuk Opsi perutean, pilih apakah akan menggunakan Dinamis atau Statis. Untuk informasi selengkapnya, lihat Opsi Perutean Site-to-Site VPN di Panduan AWS Site-to-Site VPN Pengguna.
7. Untuk Opsi Tunnel, masukkan rentang CIDR dan kunci yang telah dibagikan sebelumnya untuk terowongan Anda. Untuk informasi selengkapnya, lihat arsitektur Site-to-Site VPN.
8. Pilih Buat lampiran gateway transit.

Untuk membuat lampiran VPN menggunakan AWS CLI

Gunakan perintah create-vpn-connection.

Lihat lampiran VPN di AWS Transit Gateway

Untuk melihat lampiran VPN Anda menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Lampiran Transit Gateway.
3. Di kolom Jenis sumber daya, cari VPN. Ini adalah lampiran VPN.
4. Pilih lampiran untuk melihat detailnya atau menambahkan tag.

Untuk melihat lampiran VPN Anda menggunakan AWS CLI

Gunakan perintah describe-transit-gateway-attachments.

Hapus lampiran VPN di AWS Transit Gateway

Untuk menghapus lampiran VPN menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Lampiran Transit Gateway.
3. Pilih lampiran VPN.
4. Pilih ID sumber daya koneksi VPN untuk menavigasi ke halaman Koneksi VPN.
5. Pilih Tindakan, Hapus.
6. Saat diminta konfirmasi, pilih Hapus.

Untuk menghapus lampiran VPN menggunakan AWS CLI

Gunakan perintah delete-vpn-connection.

Lampiran Konsentrator VPN di AWS Transit Gateway

AWS Site-to-Site VPN Concentrator adalah fitur baru yang menyederhanakan konektivitas multi-situs untuk perusahaan terdistribusi. VPN Concentrator cocok untuk pelanggan yang perlu menghubungkan 25+ situs jarak jauh AWS, dengan setiap situs membutuhkan bandwidth rendah (di bawah 100 Mbps).

Bagaimana VPN Concentrator bekerja

Konsentrator VPN muncul sebagai satu lampiran pada gateway transit Anda, tetapi dapat menampung beberapa koneksi Site-to-Site VPN.

Lalu lintas dari semua koneksi VPN di Concentrator dirutekan melalui lampiran gateway transit yang sama, memungkinkan Anda menerapkan kebijakan perutean dan aturan keamanan yang konsisten di semua situs yang terhubung. Concentrator terintegrasi secara mulus dengan tabel rute gateway transit, memungkinkan Anda untuk mengontrol arus lalu lintas antara situs jarak jauh Anda dan lampiran lainnya seperti VPCs, koneksi VPN lainnya, dan koneksi peering.

Manfaat Konsentrator VPN

- Optimalisasi biaya: Mengurangi biaya dengan mengkonsolidasikan beberapa koneksi VPN bandwidth rendah ke dalam satu lampiran gateway transit, terutama bermanfaat ketika masing-masing situs tidak memerlukan kapasitas lampiran VPN penuh.

- Manajemen yang disederhanakan: Kelola beberapa koneksi situs jarak jauh melalui lampiran terpadu sambil mempertahankan kontrol dan pemantauan koneksi VPN individual.
- Perutean yang konsisten: Menerapkan kebijakan perutean terpadu di semua situs yang terhubung melalui asosiasi tabel rute gateway transit tunggal.
- Arsitektur yang dapat diskalakan: Hubungkan hingga 100 situs jarak jauh menggunakan satu Konsentrator, dengan dukungan hingga 5 Konsentrator per gateway transit.
- Fitur VPN standar: Setiap koneksi VPN mendukung kemampuan keamanan, pemantauan, dan perutean yang sama dengan koneksi Site-to-Site VPN standar.

Persyaratan dan batasan

- Hanya perutean BGP: Konsentrator VPN hanya mendukung perutean BGP (dinamis). Perutean statis tidak didukung saat peluncuran.
- Persyaratan gateway pelanggan: Setiap situs jarak jauh memerlukan gateway pelanggan yang mendukung perutean BGP. Sebelum membuat koneksi VPN pada Konsentrator, tinjau persyaratan gateway pelanggan dalam Persyaratan untuk perangkat gateway pelanggan Site-to-Site VPN Anda di Panduan AWS Site-to-Site VPN Pengguna.
- Pertimbangan kinerja: Setiap koneksi VPN pada Konsentrator dirancang untuk bandwidth maksimum 100 Mbps. Untuk persyaratan bandwidth yang lebih tinggi, pertimbangkan untuk menggunakan lampiran VPN gateway transit standar.

Anda dapat membuat, melihat, atau menghapus lampiran Konsentrator VPN menggunakan konsol AWS VPC atau CLI. AWS Koneksi VPN individual pada Concentrator dikelola melalui koneksi VPN standar APIs dan antarmuka konsol.

Tugas

- Buat lampiran Konsentrator VPN di AWS Transit Gateway
- Lihat lampiran Konsentrator VPN di AWS Transit Gateway
- Hapus lampiran Konsentrator VPN di AWS Transit Gateway

Buat lampiran Konsentrator VPN di AWS Transit Gateway

Prasyarat

- Anda harus memiliki gateway transit yang ada di akun Anda.

Untuk membuat lampiran VPN Concentrator menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Konsentrator Site-to-Site VPN.
3. Pilih Buat Konsentrator Site-to-Site VPN.
4. (Opsional) Untuk tag Nama, masukkan nama untuk Konsentrator Site-to-Site VPN Anda.
5. Untuk gateway Transit, pilih gateway transit yang ada.
6. (Opsional) Untuk menambahkan tag tambahan, pilih Tambahkan tag baru dan tentukan kunci dan nilai untuk setiap tag.
7. Pilih Buat Konsentrator Site-to-Site VPN.

Setelah Anda membuat lampiran VPN Concentrator, itu muncul dalam daftar lampiran dengan jenis sumber daya VPN Concentrator dan status awal Pending. Saat lampiran sudah siap, status berubah menjadi Tersedia. Anda kemudian dapat membuat koneksi Site-to-Site VPN pada Concentrator ini.

Untuk membuat lampiran VPN Concentrator menggunakan AWS CLI

Gunakan perintah create-vpn-concentrator.

Untuk membuat koneksi VPN pada Konsentrator VPN menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Koneksi Site-to-Site VPN.
3. Pilih Buat koneksi VPN.
4. Untuk Jenis Gateway Target, pilih Konsentrator Site-to-Site VPN.
5. Untuk Site-to-Site VPN Concentrator, pilih VPN Concentrator tempat Anda ingin membuat koneksi VPN.
6. Untuk Gateway Pelanggan, lakukan salah satu dari hal-hal berikut:
   - Untuk menggunakan gateway pelanggan yang sudah ada, pilih Yang sudah ada, dan kemudian pilih gateway untuk digunakan. Pastikan gateway pelanggan mendukung perutean BGP.
   - Untuk membuat gateway pelanggan, pilih Baru. Untuk Alamat IP, masukkan alamat IP publik statis untuk perangkat gateway pelanggan Anda. Untuk BGP ASN, masukkan Border Gateway Protocol (BGP) Autonomous System Number (ASN) untuk gateway pelanggan Anda.

Jika gateway pelanggan Anda berada di belakang perangkat translasi alamat jaringan (NAT) yang telah diaktifkan untuk NAT traversal (NAT-T), maka gunakan alamat IP publik pada perangkat NAT Anda, dan sesuaikan aturan firewall Anda untuk membuka blokir UDP port 4500.

7. Untuk opsi Routing, Dynamic (membutuhkan BGP) dipilih secara otomatis. VPN Concentrator hanya mendukung perutean dinamis dengan BGP.
8. Untuk penyimpanan kunci yang telah dibagikan sebelumnya, pilih Standard atau Secrets Manager.
9. Untuk bandwidth Tunnel, Standar dipilih secara otomatis. VPN Concentrator hanya mendukung bandwidth terowongan standar.
10. Untuk Tunnel di dalam versi IP, pilih salah satu IPv4atau IPv6.
11. (Opsional) Pilih Aktifkan akselerasi untuk meningkatkan kinerja terowongan VPN.
12. (Opsional) Untuk CIDR IPv4 jaringan lokal, sediakan rentang IPv4 CIDR.
13. (Opsional) Untuk CIDR IPv4 jaringan jarak jauh, sediakan rentang IPv4 CIDR.
14. Untuk Jenis Alamat IP Luar, Anda dapat memilih Publik IPv4 atau IPv6alamat.
15. (Opsional) Untuk Opsi Tunnel, Anda dapat mengonfigurasi pengaturan terowongan seperti di dalam alamat IP terowongan dan kunci yang telah dibagikan sebelumnya. Untuk informasi selengkapnya, lihat arsitektur Site-to-Site VPN di Panduan AWS Site-to-Site VPN Pengguna.
16. (Opsional) Untuk menambahkan tag tambahan, pilih Tambahkan tag baru dan tentukan kunci dan nilai untuk setiap tag.
17. Pilih Buat koneksi VPN.

Koneksi VPN muncul dalam daftar koneksi VPN dengan ID Konsentrator VPN di kolom ID Transit Gateway dan status awal Pending. Ketika koneksi VPN siap, status berubah menjadi Tersedia.

Untuk membuat koneksi VPN pada Konsentrator VPN menggunakan AWS CLI

Gunakan create-vpn-connectionperintah dan tentukan ID Konsentrator VPN menggunakan `--vpn-concentrator-id` parameter.

Lihat lampiran Konsentrator VPN di AWS Transit Gateway

Untuk melihat lampiran VPN Concentrator Anda menggunakan konsol

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

2. Pada panel navigasi, pilih Lampiran Transit Gateway.
3. Di kolom Jenis sumber daya, cari VPN Concentrator. Ini adalah lampiran VPN Concentrator.
4. Pilih lampiran untuk melihat detailnya.

Untuk melihat koneksi VPN pada Konsentrator VPN menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Koneksi Site-to-Site VPN.
3. Dalam daftar koneksi VPN, identifikasi koneksi yang menampilkan ID Konsentrator VPN di kolom ID Transit Gateway. Ini adalah koneksi VPN yang dihosting di Konsentrator VPN.
4. Pilih koneksi VPN untuk melihat detailnya.

Untuk melihat lampiran VPN Concentrator Anda menggunakan AWS CLI

Gunakan describe-vpn-concentratorperintah untuk melihat detail VPN Concentrator, atau gunakan describe-transit-gateway-attachmentsperintah dengan filter untuk jenis `vpn-concentrator` sumber daya.

Untuk melihat koneksi VPN pada Konsentrator VPN menggunakan AWS CLI

Gunakan describe-vpn-connectionsperintah dengan filter `vpn-concentrator-id` untuk melihat koneksi VPN yang terkait dengan Konsentrator tertentu.

Hapus lampiran Konsentrator VPN di AWS Transit Gateway

Prasyarat

- Semua koneksi VPN pada Konsentrator VPN harus dihapus sebelum Anda dapat menghapus lampiran Concentrator.
- Pastikan bahwa Anda telah memperbarui konfigurasi perutean Anda untuk memperhitungkan penghapusan Konsentrator VPN dan koneksi VPN yang terkait.

Untuk menghapus koneksi VPN pada Konsentrator VPN menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Koneksi Site-to-Site VPN.

3. Identifikasi koneksi VPN yang terkait dengan Konsentrator VPN Anda dengan mencari ID Konsentrator VPN di kolom ID Transit Gateway.
4. Pilih koneksi VPN yang ingin Anda hapus.
5. Pilih Tindakan, Hapus.
6. Saat diminta konfirmasi, pilih Hapus.
7. Ulangi langkah 4-6 untuk setiap koneksi VPN yang terkait dengan Konsentrator VPN.

Untuk menghapus lampiran VPN Concentrator menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Lampiran Transit Gateway.
3. Pilih lampiran VPN Concentrator yang ingin Anda hapus. Pastikan tidak ada koneksi VPN yang terkait dengan Konsentrator ini.
4. Pilih Tindakan, Hapus lampiran.
5. Saat diminta konfirmasi, pilih Hapus.

Lampiran VPN Concentrator memasuki status Menghapus dan akan dihapus dari akun Anda. Proses ini mungkin memakan waktu beberapa menit untuk menyelesaikannya.

Untuk menghapus koneksi VPN pada Konsentrator VPN menggunakan AWS CLI

Gunakan delete-vpn-connectionperintah untuk setiap koneksi VPN yang terkait dengan Konsentrator VPN.

Untuk menghapus lampiran VPN Concentrator menggunakan AWS CLI

Gunakan delete-vpn-concentratorperintah setelah semua koneksi VPN dihapus.

Lampiran Client VPN di AWS Transit Gateway

Saat Anda mengaitkan titik akhir Client VPN dengan gateway transit, lampiran Client VPN dibuat secara otomatis, memungkinkan Anda untuk merutekan lalu lintas antara VPC, jaringan lokal, dan titik akhir Client VPN. AWS Transit Gateway mendukung lampiran Client VPN lintas akun, memungkinkan akun yang digunakan bersama gateway transit untuk membuat lampiran Client VPN mereka sendiri.

Setelah titik akhir Client VPN dikaitkan dengan gateway transit, Anda dapat melihat lampiran di konsol Gateway Transit di bawah lampiran gateway Transit. Lampiran akan dicantumkan dengan jenis Client VPN.

Persyaratan dan batasan

- Gateway transit Anda harus memiliki blok CIDR IPv4 atau IPv6 yang ditetapkan sebelum Anda dapat membuat lampiran Client VPN.
- Propagasi tabel rute harus diaktifkan untuk lampiran Client VPN untuk memungkinkan lalu lintas antara titik akhir Client VPN dan gateway transit Anda. Lihat Aktifkan propagasi rute.

Tugas

- Buat lampiran Client VPN di AWS Transit Gateway
- Lihat lampiran Client VPN di AWS Transit Gateway
- Menghapus lampiran Client VPN di AWS Transit Gateway
- Menerima atau menolak lampiran Client VPN di AWS Transit Gateway

Buat lampiran Client VPN di AWS Transit Gateway

Prasyarat

- Anda harus memiliki gateway transit yang ada di akun Anda.
- Gateway transit Anda harus memiliki blok CIDR IPv4 atau IPv6 yang ditetapkan.

Lampiran Client VPN dibuat secara otomatis saat Anda mengaitkan titik akhir Client VPN dengan gateway transit.

Untuk membuat lampiran Client VPN menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih titik akhir Client VPN.
3. Pilih Create Client VPN endpoint.
4. Pilih Transit Gateway sebagai jenis asosiasi dan masukkan ID Gateway Transit yang akan digunakan.
5. Pilih Create Client VPN endpoint.

Setelah Anda membuat lampiran Client VPN, itu muncul dalam daftar lampiran dengan jenis sumber daya Client VPN dan status awal Pending. Saat lampiran sudah siap, status berubah menjadi Tersedia. Jika gateway transit berada di akun yang berbeda, status lampiran menunggu penerimaan sampai pemilik gateway transit menerimanya.

Untuk informasi selengkapnya tentang membuat titik akhir Client VPN, lihat Memulai dengan AWS Client VPN.

Untuk membuat lampiran Client VPN menggunakan AWS CLI

Gunakan perintah create-client-vpn-endpoint.

Lihat lampiran Client VPN di AWS Transit Gateway

Untuk melihat lampiran Client VPN Anda menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Transit gateway.
3. Pilih Lampiran gateway Transit.
4. Di kolom Jenis sumber daya, cari Client VPN.
5. Pilih lampiran untuk melihat detailnya.

Untuk melihat lampiran Client VPN Anda menggunakan AWS CLI

Gunakan perintah describe-transit-gateway-attachments dengan filter untuk tipe sumber daya. `client-vpn`

Menghapus lampiran Client VPN di AWS Transit Gateway

Untuk menghapus lampiran Client VPN menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Transit gateway.
3. Pilih Lampiran gateway Transit.
4. Pilih lampiran Client VPN yang ingin Anda hapus.
5. Pilih Tindakan, Hapus lampiran gateway transit.
6. Ketika diminta konfirmasi, masukkan **`delete`** lalu pilih Hapus.

Lampiran Client VPN memasuki status Menghapus dan akan dihapus dari akun Anda. Proses ini mungkin membutuhkan waktu untuk menyelesaikannya.

Untuk menghapus lampiran Client VPN menggunakan AWS CLI

Gunakan perintah delete-transit-gateway-client-vpn-attachment.

Menerima atau menolak lampiran Client VPN di AWS Transit Gateway

Jika titik akhir Client VPN di akun lain membuat lampiran ke gateway transit Anda, Anda harus menerima atau menolak permintaan lampiran sebelum lalu lintas dapat mengalir.

Untuk menerima atau menolak lampiran Client VPN menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Transit gateway.
3. Pilih Lampiran gateway Transit.
4. Pilih lampiran dengan status penerimaan Tertunda dan jenis Client VPN.
5. Pilih Tindakan, lalu pilih Terima lampiran atau Tolak lampiran.
6. Di kotak dialog konfirmasi, pilih Terima atau Tolak.

Jika Anda menerima lampiran, lampiran menjadi aktif dan AWS Transit Gateway akan mulai memproses lalu lintas ke dan dari titik akhir Client VPN. Jika Anda menolak lampiran, itu memasuki status ditolak dan pada akhirnya akan dihapus.

Untuk menerima lampiran Client VPN menggunakan AWS CLI

Gunakan perintah accept-transit-gateway-client-vpn-attachment.

Untuk menolak lampiran Client VPN menggunakan AWS CLI

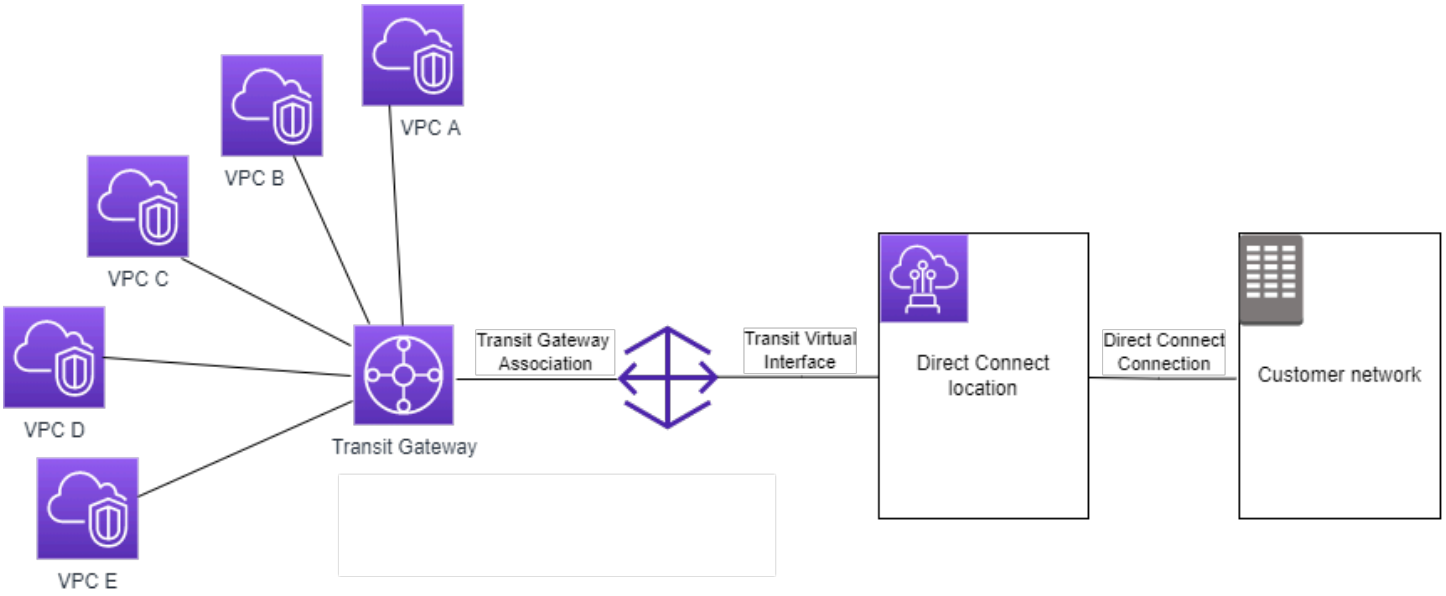
Gunakan perintah reject-transit-gateway-client-vpn-attachment.

Lampiran gateway transit ke gateway Direct Connect di AWS Transit Gateway

Lampirkan gateway transit ke gateway Direct Connect menggunakan antarmuka virtual transit. Konfigurasi ini menawarkan manfaat sebagai berikut. Anda dapat:

- Kelola satu koneksi untuk beberapa VPCs atau VPNs yang berada di Wilayah yang sama.
- Iklankan awalan dari lokal ke AWS dan dari ke lokal. AWS

Diagram berikut menggambarkan bagaimana gateway Direct Connect memungkinkan Anda membuat satu koneksi ke koneksi Direct Connect yang VPCs dapat Anda gunakan.



Solusinya melibatkan komponen berikut:

- Transit gateway.
- Sebuah gateway Direct Connect.
- Keterkaitan antara gateway Direct Connect dan transit gateway.
- Antarmuka virtual transit yang terlampir ke gateway Direct Connect.

Untuk informasi tentang mengonfigurasi gateway Direct Connect dengan gateway transit, lihat Asosiasi gateway transit di Panduan Pengguna.AWS Direct Connect

Lampiran mengintip gateway transit di AWS Transit Gateway

Anda dapat mengintip gateway transit intra-wilayah dan antar wilayah, dan merutekan lalu lintas di antara mereka, yang mencakup dan lalu lintas. IPv4 IPv6 Untuk melakukan ini, buat lampiran peering di gateway transit Anda, dan tentukan gateway transit. Gateway peer transit dapat berada di akun Anda atau dapat dari akun lain. Anda juga dapat meminta lampiran peering dari akun Anda sendiri ke gateway transit di akun lain.

Setelah Anda membuat permintaan lampiran peering, pemilik gateway transit sejawat (juga disebut sebagai gateway transit penerima) harus menerima permintaan tersebut. Untuk merutekan lalu lintas antar gateway transit, tambahkan rute statis ke tabel rute gateway transit yang menunjuk ke lampiran peering gateway transit.

Kami merekomendasikan penggunaan unik ASNs untuk setiap gateway transit peered untuk memanfaatkan kemampuan propagasi rute masa depan.

Transit gateway peering tidak mendukung penyelesaian nama host IPv4 DNS publik atau pribadi ke IPv4 alamat pribadi di kedua VPCs sisi lampiran peering gateway transit menggunakan di Wilayah lain. Amazon Route 53 Resolver Untuk informasi lebih lanjut tentang Resolver Route 53, lihat Apa itu Resolver Route 53? di Panduan Pengembang Amazon Route 53.

Inter-Region gateway peering menggunakan infrastruktur jaringan yang sama dengan VPC peering. Oleh karena itu lalu lintas dienkripsi menggunakan enkripsi AES-256 pada lapisan jaringan virtual saat bergerak antar Wilayah. Lalu lintas juga dienkripsi menggunakan enkripsi AES-256 pada lapisan fisik ketika melintasi tautan jaringan yang berada di luar kendali fisik. AWS Akibatnya, lalu lintas dienkripsi ganda pada tautan jaringan di luar kendali fisik. AWS Dalam Wilayah yang sama, lalu lintas dienkripsi pada lapisan fisik hanya ketika melintasi tautan jaringan yang berada di luar kendali fisik. AWS

Untuk informasi tentang Wilayah mana yang mendukung lampiran peering gateway transit, lihat Gateway AWS Transit. FAQs

Pertimbangan Keikutsertaan AWS Wilayah

Anda dapat menginjak gateway transit melintasi batas Wilayah keikutsertaan. Untuk informasi tentang Wilayah ini, dan cara ikut serta, lihat Mengelola AWS Wilayah. Pertimbangkan hal-hal berikut saat Anda menggunakan peering gateway transit di Wilayah ini:

- Anda dapat mengintip ke Wilayah keikutsertaan selama akun yang menerima lampiran peering telah memilih Wilayah tersebut.
- Terlepas dari status keikutsertaan Wilayah, AWS bagikan data akun berikut dengan akun yang menerima lampiran peering:
  - Akun AWS ID
  - ID gerbang transit
  - Kode Wilayah
- Saat Anda menghapus lampiran gateway transit, data akun di atas akan dihapus.

- Kami menyarankan Anda menghapus lampiran peering gateway transit sebelum Anda memilih keluar dari Wilayah. Jika Anda tidak menghapus lampiran peering, lalu lintas mungkin terus melewati lampiran dan Anda terus dikenakan biaya. Jika Anda tidak menghapus lampiran, Anda dapat memilih kembali, dan kemudian menghapus lampiran.
- Secara umum, gateway transit memiliki model pengirim membayar. Dengan menggunakan lampiran peering gateway transit melintasi batas pilihan, Anda mungkin dikenakan biaya di Wilayah yang menerima lampiran, termasuk Wilayah yang belum Anda pilih. Untuk informasi selengkapnya, lihat Harga AWS Transit Gateway.

Tugas

- Buat lampiran peering di AWS Transit Gateway
- Menerima atau menolak permintaan lampiran peering di AWS Transit Gateway
- Menambahkan rute ke tabel rute gateway transit menggunakan AWS Transit Gateway
- Menghapus lampiran peering di AWS Transit Gateway

Buat lampiran peering di AWS Transit Gateway

Sebelum Anda mulai, pastikan Anda memiliki ID gateway transit yang ingin Anda lampirkan. Jika gateway transit ada di gerbang lain Akun AWS, pastikan Anda memiliki Akun AWS ID pemilik gateway transit. Setelah Anda membuat lampiran peering, pemilik gateway transit penerima harus menerima atau menolak permintaan lampiran.

Untuk membuat lampiran peering menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Lampiran Transit Gateway.
3. Pilih Buat lampiran gateway transit.
4. Untuk ID gateway Transit, pilih gateway transit untuk lampiran. Anda dapat memilih gateway transit yang Anda miliki. Gateway transit yang dibagikan dengan Anda tidak tersedia untuk mengintip.
5. Untuk jenis Lampiran, pilih Koneksi Peering.
6. Secara opsional masukkan tag nama untuk lampiran.
7. Untuk Akun, lakukan salah satu hal berikut:

    - Jika gateway transit ada di akun Anda, pilih Akun saya.

- Jika gateway transit berbeda Akun AWS, pilih Akun lain. Untuk ID Akun, masukkan ID Akun AWS .

8. Untuk Wilayah, pilih Wilayah tempat gateway transit berada.
9. Untuk Transit gateway (penerima), masukkan ID gateway transit yang ingin Anda lampirkan.
10. Pilih Buat lampiran gateway transit.

Untuk membuat lampiran peering menggunakan AWS CLI

Gunakan perintah create-transit-gateway-peering-attachment.

Menerima atau menolak permintaan lampiran peering di AWS Transit Gateway

Saat dibuat, lampiran peering gateway transit secara otomatis dibuat dalam `pendingAcceptance` status dan tetap dalam status ini tanpa batas hingga diterima atau ditolak. Untuk mengaktifkan lampiran peering, pemilik gateway transit penerima harus menerima permintaan lampiran peering, meskipun kedua gateway transit berada di akun yang sama. Terima permintaan lampiran peering dari Wilayah tempat gateway transit penerima berada. Atau, jika Anda menolak lampiran peering, Anda harus menolak permintaan dari Wilayah tempat gateway transit penerima berada.

Untuk menerima permintaan lampiran peering menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Lampiran Transit Gateway.
3. Pilih lampiran peering gateway transit yang menunggu penerimaan.
4. Pilih Tindakan, Terima lampiran gateway transit.
5. Tambahkan rute statis ke tabel rute gateway transit. Untuk informasi selengkapnya, lihat the section called “Buat rute statis”.

Untuk menolak permintaan lampiran peering menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Lampiran Transit Gateway.
3. Pilih lampiran peering gateway transit yang menunggu penerimaan.
4. Pilih Tindakan, Tolak lampiran gateway transit.

Untuk menerima atau menolak lampiran peering menggunakan AWS CLI

Gunakan perintah accept-transit-gateway-peering-attachment dan reject-transit-gateway-peering-attachment.

Menambahkan rute ke tabel rute gateway transit menggunakan AWS Transit Gateway

Untuk merutekan lalu lintas antara gateway transit peered, Anda harus menambahkan rute statis ke tabel rute gateway transit yang menunjuk ke lampiran peering gateway transit. Pemilik gateway transit penerima juga harus menambahkan rute statis ke tabel rute gateway transit mereka.

Untuk membuat rute statis menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Tabel Rute Transit Gateway.
3. Pilih tabel rute untuk membuat rute.
4. Pilih Tindakan, Buat rute statis.
5. Pada halaman Buat rute statis, masukkan blok CIDR untuk membuat rute. Misalnya, tentukan blok CIDR dari VPC yang dilampirkan ke gateway transit sejawat.
6. Pilih lampiran peering untuk rute tersebut.
7. Pilih Buat rute statis.

Untuk membuat rute statis menggunakan AWS CLI

Gunakan perintah create-transit-gateway-route.

> **Important**
>
> Setelah Anda membuat rute, lampiran peering gateway transit harus sudah dikaitkan dengan tabel rute gateway transit. Lihat informasi yang lebih lengkap di the section called “Kaitkan tabel rute gateway transit”.

Menghapus lampiran peering di AWS Transit Gateway

Anda dapat menghapus lampiran peering gateway transit. Pemilik salah satu gateway transit dapat menghapus lampiran.

Untuk menghapus lampiran peering menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Lampiran Transit Gateway.
3. Pilih lampiran peering gateway transit.
4. Pilih Tindakan, Hapus lampiran gateway transit.
5. Masuk **`delete`** dan pilih Hapus.

Untuk menghapus lampiran peering menggunakan AWS CLI

Gunakan perintah delete-transit-gateway-peering-attachment.

Hubungkan lampiran dan Connect peer di AWS Transit Gateway

Anda dapat membuat lampiran Transit Gateway Connect untuk membuat sambungan antara gateway transit dan peralatan virtual pihak ketiga (seperti SD-WAN peralatan) yang berjalan di VPC. Lampiran Connect mendukung protokol terowongan Generic Routing Encapsulation (GRE) untuk kinerja tinggi, dan Border Gateway Protocol (BGP) untuk perutean dinamis. Setelah membuat lampiran Connect, Anda dapat membuat satu atau beberapa terowongan GRE (juga disebut sebagai rekan Transit Gateway Connect) pada lampiran Connect untuk menghubungkan gateway transit dan alat pihak ketiga. Anda membuat dua sesi BGP di atas terowongan GRE untuk bertukar informasi perutean.

> **Important**
>
> Rekan Transit Gateway Connect terdiri dari dua sesi peering BGP yang berakhir pada infrastruktur yang dikelola. AWS Dua sesi peering BGP memberikan redundansi pesawat routing, memastikan bahwa kehilangan satu sesi peering BGP tidak memengaruhi operasi perutean Anda. Informasi routing yang diterima dari kedua sesi BGP diakumulasikan untuk rekan Connect yang diberikan. Dua sesi peering BGP juga melindungi terhadap operasi AWS infrastruktur apa pun seperti pemeliharaan rutin, penambalan, peningkatan perangkat keras, dan penggantian. Jika rekan Connect Anda beroperasi tanpa sesi peering BGP ganda yang direkomendasikan yang dikonfigurasi untuk redundansi, mungkin mengalami kehilangan konektivitas sesaat selama operasi infrastruktur. AWS Kami sangat menyarankan Anda mengonfigurasi kedua sesi peering BGP pada rekan Connect Anda. Jika Anda telah mengonfigurasi beberapa rekan Connect untuk mendukung ketersediaan tinggi di sisi

alat, sebaiknya Anda mengonfigurasi kedua sesi peering BGP pada masing-masing rekan Connect Anda.

Lampiran Connect menggunakan VPC yang ada atau lampiran Direct Connect sebagai mekanisme transportasi yang mendasarinya. Ini disebut sebagai lampiran transportasi. Gateway transit mengidentifikasi paket GRE yang cocok dari alat pihak ketiga sebagai lalu lintas dari lampiran Connect. Ini memperlakukan paket lain, termasuk paket GRE dengan sumber atau informasi tujuan yang salah, sebagai lalu lintas dari lampiran transportasi.

> **Note**
>
> Untuk menggunakan lampiran Direct Connect sebagai mekanisme transportasi, Anda harus terlebih dahulu mengintegrasikan Direct Connect dengan AWS Transit Gateway. Untuk langkah-langkah membuat integrasi ini, lihat Mengintegrasikan SD-WAN perangkat dengan AWS Transit Gateway dan Direct Connect.

Connect peer

Connect peer (GRE tunnel) terdiri dari komponen-komponen berikut.

Di dalam blok CIDR (alamat BGP)

Alamat IP bagian dalam yang digunakan untuk peering BGP. Anda harus menentukan blok CIDR /29 dari `169.254.0.0/16` rentang untuk IPv4. Anda dapat secara opsional menentukan blok CIDR /125 dari `fd00::/8` rentang untuk IPv6. Blok CIDR berikut dicadangkan dan tidak dapat digunakan:

- 169.254.0. 0/29
- 169.254.1. 0/29
- 169.254.2. 0/29
- 169.254.3. 0/29
- 169.254.4. 0/29
- 169.254.5. 0/29
- 169.254.169. 248/29

Anda harus mengonfigurasi alamat pertama dari rentang IPv4 pada alat sebagai alamat IP BGP. Saat Anda menggunakan IPv6, jika blok CIDR di dalam Anda adalah fd00: :/125, maka Anda harus mengonfigurasi alamat pertama dalam rentang ini (fd00: :1) pada antarmuka terowongan alat.

Alamat BGP harus unik di semua terowongan di gateway transit.

Alamat IP rekan

Alamat IP rekan (alamat IP luar GRE) di sisi alat rekan Connect. Ini bisa berupa alamat IP apa saja. Alamat IP dapat berupa alamat IPv4 atau IPv6, tetapi harus merupakan keluarga alamat IP yang sama dengan alamat gateway transit.

Alamat gateway transit

Alamat IP peer (alamat IP luar GRE) di sisi gateway transit rekan Connect. Alamat IP harus ditentukan dari blok CIDR gateway transit, dan harus unik di seluruh lampiran Connect pada gateway transit. Jika Anda tidak menentukan alamat IP, kami menggunakan alamat pertama yang tersedia dari blok CIDR gateway transit.

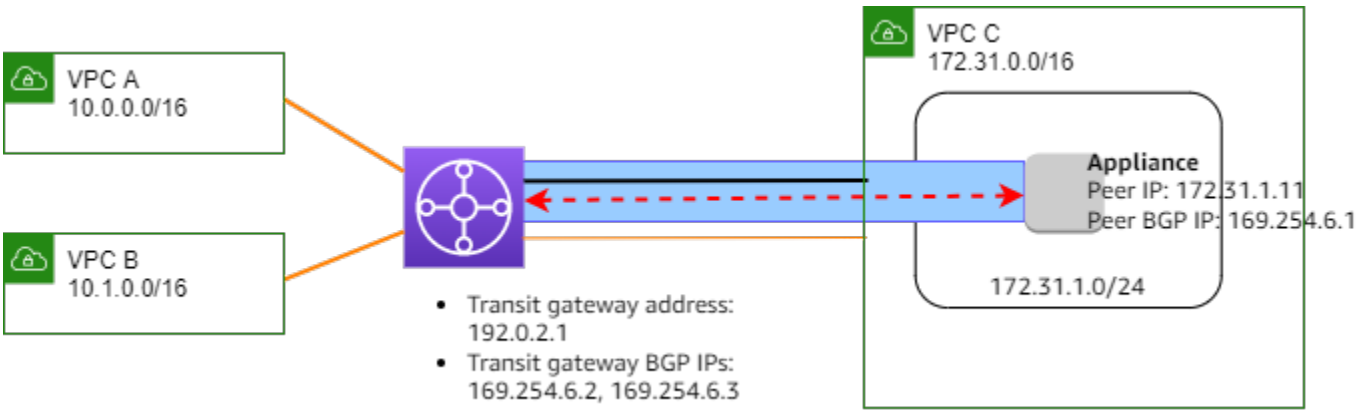
Anda dapat menambahkan blok CIDR gateway transit saat membuat atau memodifikasi gateway transit.

Alamat IP dapat berupa alamat IPv4 atau IPv6, tetapi harus merupakan keluarga alamat IP yang sama dengan alamat IP rekan.

Alamat IP peer dan alamat gateway transit digunakan untuk mengidentifikasi terowongan GRE secara unik. Anda dapat menggunakan kembali salah satu alamat di beberapa terowongan, tetapi tidak keduanya di terowongan yang sama.

Transit Gateway Connect untuk peering BGP hanya mendukung Multiprotocol BGP (MP-BGP), di mana pengalamatan IPv4 Unicast diperlukan untuk juga membuat sesi BGP untuk IPv6 Unicast. Anda dapat menggunakan alamat IPv4 dan IPv6 untuk alamat IP luar GRE.

Contoh berikut menunjukkan lampiran Connect antara gateway transit dan alat di VPC.



Komponen diagram	Deskripsi
	Lampiran VPC
	Lampiran Connect
	Terowongan GRE (Connect peer)
	Sesi mengintip BGP

Pada contoh sebelumnya, lampiran Connect dibuat pada lampiran VPC yang ada (lampiran transport). Rekan Connect dibuat pada lampiran Connect untuk membuat sambungan ke alat di VPC. Alamat gateway transit adalah`192.0.2.1`, dan kisaran alamat BGP adalah. `169.254.6.0/29` Alamat IP pertama dalam range (`169.254.6.1`) dikonfigurasi pada alat sebagai alamat IP BGP peer.

Tabel rute subnet untuk VPC C memiliki rute yang mengarahkan lalu lintas yang ditujukan untuk blok CIDR gateway transit ke gateway transit.

Destinasi	Target
172.31.0. 0/16	Lokal:
192.0.2. 0/24	tgw-id

Persyaratan dan pertimbangan

Berikut ini adalah persyaratan dan pertimbangan untuk lampiran Connect.

- Untuk informasi tentang Regions yang mendukung lampiran Connect, lihat FAQ AWS Transit Gateways.
- Alat pihak ketiga harus dikonfigurasi untuk mengirim dan menerima lalu lintas melalui terowongan GRE ke dan dari gateway transit menggunakan lampiran Connect.
- Alat pihak ketiga harus dikonfigurasi untuk menggunakan BGP untuk pembaruan rute dinamis dan pemeriksaan kesehatan.
- Jenis BGP berikut didukung:
  - Exterior BGP (eBGP): Digunakan untuk menghubungkan ke router yang berada dalam sistem otonom yang berbeda dari gateway transit. Jika Anda menggunakan eBGP, Anda harus mengonfigurasi ebgp-multihop dengan nilai time-to-live (TTL) 2.
  - Interior BGP (iBGP): Digunakan untuk menghubungkan ke router yang berada dalam sistem otonom yang sama dengan gateway transit. Gateway transit tidak akan menginstal rute dari rekan IBGP (alat pihak ketiga), kecuali rute tersebut berasal dari peer eBGP dan harus memiliki konfigurasi next-hop-self. Rute yang diiklankan oleh alat pihak ketiga melalui pengintip IBGP harus memiliki ASN.
  - MP-BGP (ekstensi multiprotocol untuk BGP): Digunakan untuk mendukung beberapa jenis protokol, seperti keluarga alamat IPv4 dan IPv6.
- BGP keep-alive timeout default adalah 10 detik dan timer tahan default adalah 30 detik.
- IPv6 BGP peering tidak didukung; hanya IPv4-based BGP peering yang didukung. Awalan IPv6 dipertukarkan melalui peering IPv4 BGP menggunakan. MP-BGP
- Deteksi Penerusan Dua Arah (BFD) tidak didukung.
- Restart anggun BGP tidak didukung.
- Saat Anda membuat peer gateway transit, jika Anda tidak menentukan nomor ASN peer, kami memilih nomor ASN gateway transit. Ini berarti bahwa alat dan gateway transit Anda akan berada dalam sistem otonom yang sama dengan melakukan IBGP.
- Connect peer menggunakan AS-PATH atribut BGP adalah rute pilihan ketika Anda memiliki dua rekan Connect.

  Untuk menggunakan perutean multi-jalur (ECMP) biaya sama antara beberapa peralatan, Anda harus mengonfigurasi alat untuk mengiklankan awalan yang sama ke gateway transit dengan atribut BGP yang sama. AS-PATH Agar gateway transit memilih semua jalur ECMP yang

tersedia, AS-PATH dan Autonomous System Number (ASN) harus cocok. Gateway transit dapat menggunakan ECMP antara rekan Connect untuk lampiran Connect yang sama atau antara lampiran Connect pada gateway transit yang sama. Gateway transit tidak dapat menggunakan ECMP antara kedua rekan BGP redundan yang ditetapkan oleh rekan tunggal untuk itu.

- Dengan lampiran Connect, rute disebarkan ke tabel rute gateway transit secara default.
- Rute statis tidak didukung.
- Konfigurasikan terowongan GRE MTU menjadi lebih kecil dari antarmuka eksternal MTU dengan mengurangi overhead header GRE (4 byte) dan header IP luar (20 byte). Misalnya, jika antarmuka eksternal MTU Anda adalah 1500 byte, atur terowongan GRE MTU ke 1476 byte (1500 - 4 - 20 = 1476) untuk mencegah fragmentasi paket.

Tugas

- Membuat lampiran Connect di AWS Transit Gateway
- Buat rekan Connect di AWS Transit Gateway
- Lihat lampiran Connect dan Connect peer di AWS Transit Gateway
- Ubah lampiran Connect dan Connect peer tag di AWS Transit Gateway
- Menghapus rekan Connect di AWS Transit Gateway
- Menghapus lampiran Connect di AWS Transit Gateway

Membuat lampiran Connect di AWS Transit Gateway

Untuk membuat lampiran Connect, Anda harus menentukan lampiran yang ada sebagai lampiran transport. Anda dapat menentukan lampiran VPC atau lampiran Direct Connect sebagai lampiran transport.

Untuk membuat lampiran Connect menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Lampiran gateway transit.
3. Pilih Buat lampiran gateway transit.
4. (Opsional) Untuk tag Nama, tentukan tag nama untuk lampiran.
5. Untuk ID gateway Transit, pilih gateway transit untuk lampiran.
6. Untuk jenis Lampiran, pilih Connect.
7. Untuk ID lampiran Transport, pilih ID lampiran yang ada (lampiran transport).

8. Pilih Buat lampiran gateway transit.

Untuk membuat lampiran Connect menggunakan AWS CLI

Gunakan perintah create-transit-gateway-connect.

Buat rekan Connect di AWS Transit Gateway

Anda dapat membuat Connect peer (GRE tunnel) untuk lampiran Connect yang ada. Sebelum Anda mulai, pastikan Anda telah mengonfigurasi blok CIDR gateway transit. Anda dapat mengonfigurasi blok CIDR gateway transit saat membuat atau memodifikasi gateway transit.

Saat Anda membuat rekan Connect, Anda harus menentukan alamat IP luar GRE di sisi alat rekan Connect.

Untuk membuat Connect peer menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Lampiran gateway transit.
3. Pilih lampiran Connect, dan pilih Actions, Create connect peer.
4. (Opsional) Untuk tag Nama, tentukan tag nama untuk rekan Connect.
5. (Opsional) Untuk Alamat GRE gateway Transit, tentukan alamat IP luar GRE untuk gateway transit. Secara default, alamat pertama yang tersedia dari blok CIDR gateway transit digunakan.
6. Untuk alamat Peer GRE, tentukan alamat IP luar GRE untuk sisi alat dari rekan Connect.
7. Untuk blok BGP Inside CIDR IPv4, tentukan rentang IPv4 alamat dalam yang digunakan untuk peering BGP. Tentukan blok CIDR /29 dari rentang. `169.254.0.0/16`
8. (Opsional) Untuk BGP Di dalam blok CIDR IPv6, tentukan rentang IPv6 alamat dalam yang digunakan untuk pengintip BGP. Tentukan blok CIDR /125 dari rentang. `fd00::/8`
9. (Opsional) Untuk Peer ASN, tentukan Nomor Sistem Otonomi Border Gateway Protocol (BGP) (ASN) untuk alat. Anda dapat menggunakan ASN yang sudah ada yang ditetapkan ke jaringan Anda. Jika Anda tidak memilikinya, Anda dapat menggunakan ASN pribadi dalam rentang 64512—65534 (ASN 16-bit) atau 4200000000—4294967294 (ASN 32-bit).

   Defaultnya adalah ASN yang sama dengan gateway transit. Jika Anda mengonfigurasi ASN Peer agar berbeda dari gateway transit ASN (eBGP), Anda harus mengonfigurasi ebgp-multihop dengan nilai (TTL) 2. time-to-live
10. Pilih Create connect peer.

Untuk membuat Connect peer menggunakan AWS CLI

Gunakan perintah create-transit-gateway-connect-peer.

Lihat lampiran Connect dan Connect peer di AWS Transit Gateway

Lihat lampiran Connect dan Connect peer Anda.

Untuk melihat lampiran Connect dan Connect peer menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Lampiran gateway transit.
3. Pilih lampiran Connect.
4. Untuk melihat Connect peer untuk lampiran, pilih tab Connect Peers.

Untuk melihat lampiran Connect dan Connect peer menggunakan AWS CLI

Gunakan perintah describe-transit-gateway-connectsand describe-transit-gateway-connect-peers.

Ubah lampiran Connect dan Connect peer tag di AWS Transit Gateway

Anda dapat memodifikasi tag untuk lampiran Connect Anda.

Untuk mengubah tag lampiran Connect menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Lampiran Transit Gateway.
3. Pilih lampiran Connect, lalu pilih Actions, Manage tags.
4. Untuk menambahkan tag, pilih Tambahkan tag baru dan tentukan nama kunci dan nilai kunci.
5. Untuk menghapus sebuah tag, pilih Hapus.
6. Pilih Simpan.

Anda dapat memodifikasi tag untuk rekan Connect Anda.

Untuk mengubah tag rekan Connect menggunakan konsol

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

2. Di panel navigasi, pilih Lampiran Transit Gateway.
3. Pilih lampiran Connect, lalu pilih Connect peer.
4. Pilih Connect peer dan kemudian pilih Actions, Manage tags.
5. Untuk menambahkan tag, pilih Tambahkan tag baru dan tentukan nama kunci dan nilai kunci.
6. Untuk menghapus sebuah tag, pilih Hapus.
7. Pilih Simpan.

Untuk mengubah lampiran Connect dan Connect peer tag menggunakan AWS CLI

Gunakan perintah buat-tanda dan hapus-tanda.

Menghapus rekan Connect di AWS Transit Gateway

Jika Anda tidak lagi membutuhkan rekan Connect, Anda dapat menghapusnya.

Untuk menghapus rekan Connect menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Lampiran gateway transit.
3. Pilih lampiran Connect.
4. Di tab Connect Peers, pilih Connect peer dan pilih Actions, Delete connect peer.

Untuk menghapus rekan Connect menggunakan AWS CLI

Gunakan perintah delete-transit-gateway-connect-peer.

Menghapus lampiran Connect di AWS Transit Gateway

Jika Anda tidak lagi memerlukan lampiran Connect, Anda dapat menghapusnya. Anda harus terlebih dahulu menghapus semua rekan Connect untuk lampiran.

Untuk menghapus lampiran Connect menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Lampiran gateway transit.
3. Pilih lampiran Connect, dan pilih Actions, Delete transit gateway attachment.

4. Masuk **`delete`** dan pilih Hapus.

Untuk menghapus lampiran Connect menggunakan AWS CLI

Gunakan perintah delete-transit-gateway-connect.

Tabel rute gerbang transit di AWS Transit Gateway

Gunakan tabel rute gateway transit untuk mengonfigurasi perutean untuk lampiran gateway transit Anda. Tabel rute adalah tabel yang berisi aturan yang mengarahkan bagaimana lalu lintas jaringan Anda dirutekan antara VPC dan VPN Anda. Setiap rute dalam tabel berisi rentang alamat IP untuk tujuan yang ingin Anda kirimi lalu lintas.

Tabel rute gateway transit memungkinkan Anda untuk mengaitkan tabel dengan lampiran gateway transit. Lampiran VPC, VPN, VPN Concentrator, Client VPN, Direct Connect gateway, Peering, dan Connect semuanya didukung. Saat dikaitkan, rute untuk lampiran ini disebarkan dari lampiran ke tabel rute gateway transit target. Lampiran dapat disebarkan ke beberapa tabel rute.

Selain itu Anda dapat membuat dan mengelola rute statis dengan tabel rute. Misalnya, Anda mungkin memiliki rute statis yang digunakan sebagai rute cadangan jika terjadi gangguan jaringan yang memengaruhi rute dinamis apa pun.

Tugas

- Buat tabel rute gateway transit di AWS Transit Gateway
- Lihat tabel rute gateway transit menggunakan AWS Transit Gateway
- Kaitkan tabel rute gateway transit di AWS Transit Gateway
- Menghapus asosiasi untuk tabel rute gateway transit di AWS Transit Gateway
- Aktifkan propagasi rute ke tabel rute gateway transit di AWS Transit Gateway
- Nonaktifkan propagasi rute di AWS Transit Gateway
- Buat rute statis di AWS Transit Gateway
- Menghapus rute statis di AWS Transit Gateway
- Ganti rute statis di AWS Transit Gateway
- Ekspor tabel rute ke Amazon S3 di AWS Transit Gateway
- Menghapus tabel rute gateway transit di AWS Transit Gateway

- Buat referensi daftar awalan tabel rute di AWS Transit Gateway
- Ubah referensi daftar awalan di AWS Transit Gateway
- Hapus referensi daftar awalan di AWS Transit Gateway

Buat tabel rute gateway transit di AWS Transit Gateway

Untuk membuat tabel rute gateway transit menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Tabel Rute Transit Gateway.
3. Pilih Buat tabel rute gateway transit.
4. (Opsional) Untuk tag Nama, ketikkan nama untuk tabel rute gateway transit. Ini membuat tag dengan kunci tag “Nama”, di mana nilai tag adalah nama yang Anda tentukan.
5. Untuk ID gateway Transit, pilih gateway transit untuk tabel rute.
6. Pilih Buat tabel rute gateway transit.

Untuk membuat tabel rute gateway transit menggunakan AWS CLI

Gunakan perintah create-transit-gateway-route-table.

Lihat tabel rute gateway transit menggunakan AWS Transit Gateway

Untuk melihat tabel rute gateway transit Anda menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Tabel Rute Transit Gateway.
3. (Opsional) Untuk menemukan tabel rute atau kumpulan tabel tertentu, masukkan semua atau sebagian nama, kata kunci, atau atribut di bidang filter.
4. Pilih kotak centang untuk tabel rute, atau pilih ID-nya, untuk menampilkan informasi tentang asosiasi, propagasi, rute, dan tag.

Untuk melihat tabel rute gateway transit Anda menggunakan AWS CLI

Gunakan perintah describe-transit-gateway-route-tables.

Untuk melihat rute untuk tabel rute gateway transit menggunakan AWS CLI

Gunakan perintah search-transit-gateway-routes.

Untuk melihat propagasi rute untuk tabel rute gateway transit menggunakan AWS CLI

Gunakan perintah get-transit-gateway-route-table-propagations.

Untuk melihat asosiasi untuk tabel rute gateway transit menggunakan AWS CLI

Gunakan perintah get-transit-gateway-route-table-associations.

Kaitkan tabel rute gateway transit di AWS Transit Gateway

Anda dapat mengaitkan tabel rute gateway transit dengan lampiran gateway transit.

Untuk mengaitkan tabel rute gateway transit menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Tabel Rute Transit Gateway.
3. Pilih tabel rute.
4. Di bagian bawah halaman, pilih tab Asosiasi.
5. Pilih Buat asosiasi.
6. Pilih lampiran yang akan diasosiasikan dan kemudian pilih Buat asosiasi.

Untuk mengaitkan tabel rute gateway transit menggunakan AWS CLI

Gunakan perintah associate-transit-gateway-route-table.

Menghapus asosiasi untuk tabel rute gateway transit di AWS Transit Gateway

Anda dapat memisahkan tabel rute gateway transit dari lampiran gateway transit.

Untuk memisahkan tabel rute gateway transit menggunakan konsol

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

3. Pilih tabel rute.
4. Di bagian bawah halaman, pilih tab Asosiasi.
5. Pilih lampiran untuk memisahkan dan kemudian pilih Hapus asosiasi.
6. Saat diminta konfirmasi, pilih Hapus asosiasi.

Untuk memisahkan tabel rute gateway transit menggunakan AWS CLI

Gunakan perintah disassociate-transit-gateway-route-table.

Aktifkan propagasi rute ke tabel rute gateway transit di AWS Transit Gateway

Gunakan propagasi rute untuk menambahkan rute dari lampiran ke tabel rute.

Untuk menyebarkan rute ke tabel rute lampiran gateway transit

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Tabel Rute Transit Gateway.
3. Pilih tabel rute untuk membuat propagasi.
4. Pilih Tindakan, Buat propagasi.
5. Pada halaman Buat propagasi, pilih lampiran.
6. Pilih Buat propagasi.

Untuk mengaktifkan propagasi rute menggunakan AWS CLI

Gunakan perintah enable-transit-gateway-route-table-propagation.

Nonaktifkan propagasi rute di AWS Transit Gateway

Hapus rute yang disebarkan dari lampiran tabel rute.

Untuk menonaktifkan propagasi rute menggunakan konsol

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

3. Pilih tabel rute untuk menghapus propagasi dari.
4. Di bagian bawah halaman, pilih tab Propagasi.
5. Pilih lampiran dan kemudian pilih Hapus propagasi.
6. Saat diminta konfirmasi, pilih Hapus propagasi.

Untuk menonaktifkan propagasi rute menggunakan AWS CLI

Gunakan perintah disable-transit-gateway-route-table-propagation.

Buat rute statis di AWS Transit Gateway

Buat rute statis untuk lampiran peering VPC, VPN, atau gateway transit, atau Anda dapat membuat rute lubang hitam yang menurunkan lalu lintas yang cocok dengan rute tersebut.

Rute statis dalam tabel rute gateway transit yang menargetkan lampiran VPN tidak difilter oleh Site-to-Site VPN. Ini mungkin memungkinkan arus lalu lintas keluar yang tidak diinginkan saat menggunakan VPN berbasis BGP.

Untuk membuat rute statis menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Tabel Rute Transit Gateway.
3. Pilih tabel rute untuk membuat rute.
4. Pilih Tindakan, Buat rute statis.
5. Pada halaman Buat rute statis, masukkan blok CIDR untuk membuat rute, lalu pilih Aktif.
6. Pilih lampiran untuk rute.
7. Pilih Buat rute statis.

Untuk membuat rute blackhole menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Tabel Rute Transit Gateway.
3. Pilih tabel rute untuk membuat rute.
4. Pilih Tindakan, Buat rute statis.

5. Pada halaman Buat rute statis, masukkan blok CIDR untuk membuat rute, lalu pilih Blackhole.
6. Pilih Buat rute statis.

Untuk membuat rute statis atau rute lubang hitam menggunakan AWS CLI

Gunakan perintah create-transit-gateway-route.

Menghapus rute statis di AWS Transit Gateway

Hapus rute statis dari tabel rute gateway transit.

Untuk menghapus rute statis menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Tabel Rute Transit Gateway.
3. Pilih tabel rute untuk menghapus rute, dan pilih Rute.
4. Pilih rute yang akan dihapus.
5. Pilih Hapus rute statis.
6. Di kotak konfirmasi, pilih Hapus rute statis.

Untuk menghapus rute statis menggunakan AWS CLI

Gunakan perintah delete-transit-gateway-route.

Ganti rute statis di AWS Transit Gateway

Ganti rute statis dalam tabel rute gateway transit dengan rute statis yang berbeda.

Untuk mengganti rute statis menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Tabel Rute Transit Gateway.
3. Pilih rute yang ingin Anda ganti di tabel rute.
4. Di bagian detail, pilih tab Rute.
5. Pilih Tindakan, Ganti rute statis.
6. Untuk Type, pilih Active atau Blackhole.

7. Dari drop-down Pilih lampiran, pilih gateway transit yang akan menggantikan yang sekarang di tabel rute.
8. Pilih Ganti rute statis.

Untuk mengganti rute statis menggunakan AWS CLI

Gunakan perintah replace-transit-gateway-route.

Ekspor tabel rute ke Amazon S3 di AWS Transit Gateway

Anda dapat mengekspor rute di tabel rute gateway transit ke bucket Amazon S3. Rute disimpan ke bucket Amazon S3 yang ditentukan dalam file JSON.

Untuk mengekspor tabel rute gateway transit menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Tabel Rute Transit Gateway.
3. Pilih tabel rute yang mencakup rute yang akan diekspor.
4. Pilih Tindakan, rute Ekspor.
5. Pada halaman Export routes, untuk nama bucket S3, ketikkan nama bucket S3.
6. Untuk memfilter rute yang diekspor, tentukan parameter filter di bagian Filter halaman.
7. Pilih rute Ekspor.

Untuk mengakses rute yang diekspor, buka konsol Amazon S3 https://console.aws.amazon.com/s3/di, dan arahkan ke bucket yang Anda tentukan. Nama file termasuk Akun AWS ID, AWS Wilayah, ID tabel rute, dan stempel waktu. Pilih file dan pilih Unduh. Berikut ini adalah contoh file JSON yang berisi informasi tentang dua rute yang disebarkan untuk lampiran VPC.

```
{
  "filter": [
    {
      "name": "route-search.subnet-of-match",
      "values": [
        "0.0.0.0/0",
        "::/0"
      ]
    }
  ],
```

```
  "routes": [
    {
      "destinationCidrBlock": "10.0.0.0/16",
      "transitGatewayAttachments": [
        {
          "resourceId": "vpc-0123456abcd123456",
          "transitGatewayAttachmentId": "tgw-attach-1122334455aabbcc1",
          "resourceType": "vpc"
        }
      ],
      "type": "propagated",
      "state": "active"
    },
    {
      "destinationCidrBlock": "10.2.0.0/16",
      "transitGatewayAttachments": [
        {
          "resourceId": "vpc-abcabc123123abca",
          "transitGatewayAttachmentId": "tgw-attach-6677889900aabbcc7",
          "resourceType": "vpc"
        }
      ],
      "type": "propagated",
      "state": "active"
    }
  ]
}
```


Menghapus tabel rute gateway transit di AWS Transit Gateway

Untuk menghapus tabel rute gateway transit menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Tabel Rute Transit Gateway.
3. Pilih tabel rute yang akan dihapus.
4. Pilih Tindakan, Hapus tabel rute gateway transit.
5. Masuk **`delete`** dan pilih Hapus untuk mengonfirmasi penghapusan.

Untuk menghapus tabel rute gateway transit menggunakan AWS CLI

Gunakan perintah delete-transit-gateway-route-table.

Buat referensi daftar awalan tabel rute di AWS Transit Gateway

Anda dapat mereferensikan daftar awalan di tabel rute gateway transit Anda. Daftar awalan adalah satu set dari satu atau beberapa entri blok CIDR yang Anda tentukan dan kelola. Anda dapat menggunakan daftar awalan untuk menyederhanakan pengelolaan alamat IP yang Anda referensikan dalam sumber daya Anda untuk merutekan lalu lintas jaringan. Misalnya, jika Anda sering menentukan tujuan yang sama CIDRs di beberapa tabel rute gateway transit, Anda dapat mengelolanya CIDRs dalam satu daftar awalan, alih-alih berulang kali mereferensikan hal yang sama CIDRs di setiap tabel rute. Jika Anda perlu menghapus blok CIDR tujuan, Anda dapat menghapus entri dari daftar awalan alih-alih menghapus rute dari setiap tabel rute yang terpengaruh.

Saat Anda membuat referensi daftar awalan di tabel rute gateway transit Anda, setiap entri dalam daftar awalan direpresentasikan sebagai rute dalam tabel rute gateway transit Anda.

Untuk informasi selengkapnya tentang daftar awalan, lihat Daftar awalan di Panduan Pengguna Amazon VPC.

Untuk membuat referensi daftar awalan menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Tabel Rute Transit Gateway.
3. Pilih tabel rute gateway transit.
4. Pilih Tindakan, Buat referensi daftar awalan.
5. Untuk ID daftar Awalan, pilih ID dari daftar awalan.
6. Untuk Jenis, pilih apakah lalu lintas ke daftar awalan ini harus diizinkan (Aktif) atau dijatuhkan (Blackhole).
7. Untuk ID lampiran gateway Transit, pilih ID lampiran yang akan mengarahkan lalu lintas.
8. Pilih Buat referensi daftar awalan.

Untuk membuat referensi daftar awalan menggunakan AWS CLI

Gunakan perintah create-transit-gateway-prefix-list-reference.

Ubah referensi daftar awalan di AWS Transit Gateway

Anda dapat mengubah referensi daftar awalan dengan mengubah lampiran yang dialihkan lalu lintas, atau menunjukkan apakah akan menghentikan lalu lintas yang cocok dengan rute.

Anda tidak dapat mengubah rute individual untuk daftar awalan di tab Rute. Untuk mengubah entri dalam daftar awalan, gunakan layar Daftar Awalan Terkelola. Untuk informasi selengkapnya, lihat Memodifikasi daftar awalan di Panduan Pengguna Amazon VPC.

Untuk mengubah referensi daftar awalan menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Tabel Rute Transit Gateway.
3. Pilih tabel rute gateway transit.
4. Di panel bawah, pilih Referensi daftar awalan.
5. Pilih referensi daftar awalan, dan pilih Ubah referensi.
6. Untuk Jenis, pilih apakah lalu lintas ke daftar awalan ini harus diizinkan (Aktif) atau dijatuhkan (Blackhole).
7. Untuk ID lampiran gateway Transit, pilih ID lampiran yang akan mengarahkan lalu lintas.
8. Pilih Ubah referensi daftar awalan.

Untuk memodifikasi referensi daftar awalan menggunakan AWS CLI

Gunakan perintah modify-transit-gateway-prefix-list-reference.

Hapus referensi daftar awalan di AWS Transit Gateway

Jika Anda tidak lagi memerlukan referensi daftar awalan, Anda dapat menghapusnya dari tabel rute gateway transit Anda. Menghapus referensi tidak menghapus daftar awalan.

Untuk menghapus referensi daftar awalan menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Tabel Rute Transit Gateway.
3. Pilih tabel rute gateway transit.
4. Pilih referensi daftar awalan, dan pilih Hapus referensi.
5. Pilih Hapus referensi.

Untuk memodifikasi referensi daftar awalan menggunakan AWS CLI

Gunakan perintah delete-transit-gateway-prefix-list-reference.

Tabel kebijakan gateway transit di AWS Transit Gateway

Perutean dinamis gateway transit menggunakan tabel kebijakan untuk merutekan lalu lintas jaringan untuk AWS Cloud WAN. Tabel berisi aturan kebijakan untuk mencocokkan lalu lintas jaringan dengan atribut kebijakan, lalu memetakan lalu lintas yang cocok dengan aturan ke tabel rute target.

Anda dapat menggunakan perutean dinamis untuk gateway transit untuk secara otomatis bertukar informasi perutean dan jangkauan dengan tipe gateway transit peered. Berbeda dengan rute statis, lalu lintas dapat diarahkan di sepanjang jalur yang berbeda berdasarkan kondisi jaringan, seperti kegagalan jalur atau kemacetan. Perutean dinamis juga menambahkan lapisan keamanan ekstra karena lebih mudah untuk merutekan ulang lalu lintas jika terjadi pelanggaran atau serangan jaringan.

> **Note**
>
> Tabel kebijakan gateway transit saat ini hanya didukung di Cloud WAN saat membuat koneksi peering gateway transit. Saat membuat koneksi peering, Anda dapat mengaitkan tabel itu dengan koneksi. Asosiasi kemudian mengisi tabel secara otomatis dengan aturan kebijakan.
> Untuk informasi selengkapnya tentang koneksi peering di Cloud WAN, lihat Peerings di Panduan Pengguna AWS Cloud WAN.

Tugas

- Membuat tabel kebijakan gateway transit di AWS Transit Gateway
- Menghapus tabel kebijakan gateway transit di AWS Transit Gateway

Membuat tabel kebijakan gateway transit di AWS Transit Gateway

Untuk membuat tabel kebijakan gateway transit menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Tabel kebijakan gateway transit.
3. Pilih Buat tabel kebijakan gateway transit.
4. (Opsional) Untuk tag Nama, masukkan nama untuk tabel kebijakan gateway transit. Ini menciptakan tag, di mana nilai tag adalah nama yang Anda tentukan.

5. Untuk ID gateway Transit, pilih gateway transit untuk tabel kebijakan.
6. Pilih Buat tabel kebijakan gateway transit.

Untuk membuat tabel kebijakan gateway transit menggunakan AWS CLI

Gunakan perintah create-transit-gateway-policy-table.

Menghapus tabel kebijakan gateway transit di AWS Transit Gateway

Menghapus tabel kebijakan gateway transit. Ketika tabel dihapus, semua aturan kebijakan dalam tabel tersebut akan dihapus.

Untuk menghapus tabel kebijakan gateway transit menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Tabel kebijakan gateway transit.
3. Pilih tabel kebijakan gateway transit yang akan dihapus.
4. Pilih Tindakan, lalu pilih Hapus tabel kebijakan.
5. Konfirmasikan bahwa Anda ingin menghapus tabel.

Untuk menghapus tabel kebijakan gateway transit menggunakan AWS CLI

Gunakan perintah delete-transit-gateway-policy-table.

Multicast di Transit Gateway AWS

Multicast adalah protokol komunikasi yang digunakan untuk mengirimkan satu aliran data ke beberapa komputer penerima secara bersamaan. Transit Gateway mendukung perutean lalu lintas multicast antara subnet yang terpasang VPCs, dan berfungsi sebagai router multicast untuk instance pengiriman lalu lintas yang ditujukan untuk beberapa instance penerima.

Topik

- Daftarkan sumber dengan grup multicast di AWS Transit Gateway
- Daftarkan anggota dengan grup multicast di AWS Transit Gateway
- Deregister sumber dari grup multicast di Transit Gateway AWS
- Membatalkan pendaftaran anggota dari grup multicast di Transit Gateway AWS
- Lihat grup multicast di AWS Transit Gateway
- Siapkan multicast untuk Windows Server di AWS Transit Gateway
- Contoh: Mengelola konfigurasi IGMP menggunakan AWS Transit Gateway
- Contoh: Mengelola konfigurasi sumber statis di AWS Transit Gateway
- Contoh: Mengelola konfigurasi anggota grup statis di AWS Transit Gateway

Konsep multicast

Berikut ini adalah konsep kunci untuk multicast:

- Domain multicast — Memungkinkan segmentasi jaringan multicast ke dalam domain yang berbeda, dan membuat gateway transit bertindak sebagai beberapa router multicast. Anda menentukan keanggotaan domain multicast di tingkat subnet.
- Grup multicast - Mengidentifikasi sekumpulan host yang akan mengirim dan menerima lalu lintas multicast yang sama. Grup multicast diidentifikasi oleh alamat IP grup. Keanggotaan grup multicast didefinisikan oleh antarmuka jaringan elastis individu yang melekat pada instance. EC2
- Internet Group Management Protocol (IGMP) — Protokol internet yang memungkinkan host dan router mengelola keanggotaan grup multicast secara dinamis. Domain multicast IGMP berisi host yang menggunakan protokol IGMP untuk bergabung, meninggalkan, dan mengirim pesan. AWS mendukung IGMPv2 protokol dan domain multicast keanggotaan grup IGMP dan statis (berbasis API).

- Sumber multicast — Sebuah elastic network interface yang terkait dengan EC2 instance yang didukung yang dikonfigurasi secara statis untuk mengirim lalu lintas multicast. Sumber multicast hanya berlaku untuk konfigurasi sumber statis.

  Domain multicast sumber statis berisi host yang tidak menggunakan protokol IGMP untuk bergabung, meninggalkan, dan mengirim pesan. Anda menggunakan AWS CLI untuk menambahkan sumber dan anggota grup. Sumber yang ditambahkan secara statis mengirimkan lalu lintas multicast dan anggota menerima lalu lintas multicast.

- Anggota grup multicast — Sebuah elastic network interface yang terkait dengan EC2 instance yang didukung yang menerima lalu lintas multicast. Grup multicast memiliki beberapa anggota grup. Dalam konfigurasi keanggotaan grup sumber statis, anggota grup multicast hanya dapat menerima lalu lintas. Dalam konfigurasi grup IGMP, anggota dapat mengirim dan menerima lalu lintas.

Pertimbangan

- Transit gateway multicast mungkin tidak cocok untuk perdagangan frekuensi tinggi atau aplikasi yang peka terhadap kinerja. Kami sangat menyarankan Anda meninjau kuota Multicast untuk batasannya. Hubungi akun Anda atau tim Arsitek Solusi untuk tinjauan terperinci tentang persyaratan kinerja Anda.
- Untuk informasi tentang Wilayah yang didukung, lihat AWS Transit Gateway FAQs.
- Anda harus membuat gateway transit baru untuk mendukung multicast.
- Keanggotaan grup multicast dikelola menggunakan atau AWS CLI, Amazon Virtual Private Cloud Console atau IGMP.
- Subnet hanya dapat berada dalam satu domain multicast.
- Jika Anda menggunakan instance non-Nitro, Anda harus menonaktifkan kotak centang Source/Dest. Untuk informasi tentang menonaktifkan pemeriksaan, lihat Mengubah pemeriksaan sumber atau tujuan di EC2 Panduan Pengguna Amazon.
- Instance non-Nitro tidak bisa menjadi pengirim multicast.
- Perutean multicast tidak didukung over Direct Connect, Site-to-Site VPN, lampiran peering, atau lampiran Connect gateway transit.
- Gateway transit tidak mendukung fragmentasi paket multicast. Paket multicast yang terfragmentasi dijatuhkan. Untuk informasi selengkapnya, lihat Unit transmisi maksimum (MTU).
- Saat startup, host IGMP mengirimkan beberapa JOIN pesan IGMP untuk bergabung dengan grup multicast (biasanya 2 hingga 3 percobaan ulang). Jika semua JOIN pesan IGMP hilang, host tidak akan menjadi bagian dari grup multicast gateway transit. Dalam skenario seperti itu, Anda perlu memicu kembali JOIN pesan IGMP dari host menggunakan metode khusus aplikasi.
- Keanggotaan grup dimulai dengan penerimaan IGMPv2 JOIN pesan oleh gateway transit dan diakhiri dengan penerimaan IGMPv2 LEAVE pesan. Gerbang transit melacak host yang berhasil bergabung dengan grup. Sebagai router multicast cloud, gateway transit mengeluarkan IGMPv2 QUERY pesan ke semua anggota setiap dua menit. Setiap anggota mengirimkan IGMPv2 JOIN pesan sebagai tanggapan, yang merupakan cara anggota memperbarui keanggotaan mereka. Jika anggota gagal membalas tiga pertanyaan berturut-turut, gateway transit akan menghapus

keanggotaan ini dari semua grup yang bergabung. Namun, ia terus mengirimkan kueri ke anggota ini selama 12 jam sebelum secara permanen menghapus anggota dari to-be-queried daftarnya. IGMPv2 LEAVEPesan eksplisit segera dan permanen menghapus host dari pemrosesan multicast lebih lanjut.

- Gerbang transit melacak host yang berhasil bergabung dengan grup. Jika terjadi pemadaman gateway transit, gateway transit terus mengirim data multicast ke host selama tujuh menit (420 detik) setelah pesan IGMP terakhir yang berhasil. JOIN Gateway transit terus mengirim kueri keanggotaan ke host hingga 12 jam atau sampai menerima LEAVE pesan IGMP dari host.
- Gateway transit mengirimkan paket kueri keanggotaan ke semua anggota IGMP sehingga dapat melacak keanggotaan grup multicast. IP sumber dari paket kueri IGMP ini adalah 0.0.0.0/32, dan IP tujuan adalah 224.0.0.1/32 dan protokolnya adalah 2. Konfigurasi grup keamanan Anda pada host IGMP (instance), dan ACLs konfigurasi apa pun pada subnet host harus mengizinkan pesan protokol IGMP ini.
- Ketika sumber dan tujuan multicast berada di VPC yang sama, Anda tidak dapat menggunakan referensi grup keamanan untuk mengatur grup keamanan tujuan untuk menerima lalu lintas dari grup keamanan sumber.
- Untuk grup dan sumber multicast statis, AWS Transit Gateway secara otomatis menghapus grup statis dan sumber ENIs yang tidak ada lagi. Ini dilakukan dengan secara berkala mengasumsikan peran terkait layanan Transit Gateway untuk dijelaskan ENIs dalam akun.
- Hanya dukungan multicast statis. IPv6 Multicast dinamis tidak.

Perutean multicast

Ketika Anda mengaktifkan multicast pada gateway transit, ia bertindak sebagai router multicast. Saat Anda menambahkan subnet ke domain multicast, kami mengirim semua lalu lintas multicast ke gateway transit yang terkait dengan domain multicast tersebut.

Jaringan ACLs

Aturan ACL jaringan beroperasi di tingkat subnet. Mereka berlaku untuk lalu lintas multicast, karena gateway transit berada di luar subnet. Untuk informasi selengkapnya, lihat Jaringan ACLs di Panduan Pengguna VPC Amazon.

Untuk lalu lintas multicast Internet Group Management Protocol (IGMP), berikut ini adalah aturan masuk minimum. Host jarak jauh adalah host yang mengirimkan lalu lintas multicast.

Jenis	Protokol	Sumber	Deskripsi
Protokol Kustom	IGMP (2)	0.0.0.0/32	Kueri IGMP
Protokol UDP Kustom	UDP	Alamat IP host jarak jauh	Lalu lintas multicast masuk

Berikut ini adalah aturan keluar minimum untuk IGMP.

Jenis	Protokol	Tujuan	Deskripsi
Protokol Kustom	IGMP (2)	224.0.0.2/32	IGMP pergi
Protokol Kustom	IGMP (2)	Alamat IP grup multicast	IGMP bergabung
Protokol UDP Kustom	UDP	Alamat IP grup multicast	Lalu lintas multicast keluar

Grup keamanan

Aturan grup keamanan beroperasi pada tingkat instans. Mereka dapat diterapkan pada lalu lintas multicast masuk dan keluar. Perilakunya sama dengan lalu lintas unicast. Untuk semua instance anggota grup, Anda harus mengizinkan lalu lintas masuk dari sumber grup. Untuk informasi selengkapnya, lihat Grup keamanan di Panduan Pengguna Amazon VPC.

Untuk lalu lintas multicast IGMP, Anda harus memiliki aturan masuk berikut minimal. Host jarak jauh adalah host yang mengirimkan lalu lintas multicast. Anda tidak dapat menentukan grup keamanan sebagai sumber aturan masuk UDP.

Jenis	Protokol	Sumber	Deskripsi
Protokol Kustom	2	0.0.0.0/32	Kueri IGMP
Protokol UDP Kustom	UDP	Alamat IP host jarak jauh	Lalu lintas multicast masuk

Untuk lalu lintas multicast IGMP, Anda harus memiliki aturan keluar berikut minimal.

Jenis	Protokol	Tujuan	Deskripsi
Protokol Kustom	2	224.0.0.2/32	IGMP pergi
Protokol Kustom	2	Alamat IP grup multicast	IGMP bergabung
Protokol UDP Kustom	UDP	Alamat IP grup multicast	Lalu lintas multicast keluar

Domain multicast di Transit Gateway AWS

Domain multicast memungkinkan segmentasi jaringan multicast ke dalam domain yang berbeda. Untuk mulai menggunakan multicast dengan gateway transit, buat domain multicast, dan kemudian kaitkan subnet dengan domain.

Atribut domain multicast

Tabel berikut merinci atribut domain multicast. Anda tidak dapat mengaktifkan kedua atribut secara bersamaan.

Atribut	Deskripsi
`Igmpv2Support` (AWS CLI) IGMPv2 dukungan (konsol)	Atribut ini menentukan bagaimana anggota grup bergabung atau meninggalkan grup multicast. Ketika atribut ini dinonaktifkan, Anda harus menambahkan anggota grup ke domain secara manual. Aktifkan atribut ini jika setidaknya satu anggota menggunak an protokol IGMP. Anggota bergabung dengan grup multicast dengan salah satu cara berikut: • Anggota yang mendukung IGMP menggunakan `JOIN` dan `LEAVE` pesan.

Atribut	Deskripsi
	• Anggota yang tidak mendukung IGMP harus ditambahkan atau dihapus dari grup menggunakan konsol VPC Amazon atau. AWS CLI Jika Anda mendaftarkan anggota grup multicast, Anda juga harus membatalkan pendaftaran mereka. Gateway transit mengabaikan `LEAVE` pesan IGMP yang dikirim oleh anggota grup yang ditambahkan secara manual.
`StaticSourcesSupport` (AWS CLI) Dukungan sumber statis (konsol)	Atribut ini menentukan apakah ada sumber multicast statis untuk grup. Ketika atribut ini diaktifkan, Anda harus menambahkan sumber untuk domain multicast menggunakan register-transit-gateway-multicast -group-sources. Hanya sumber multicast yang dapat mengirim lalu lintas multicast. Ketika atribut ini dinonaktifkan, tidak ada sumber multicast yang ditunjuk. Setiap instance yang ada di subnet yang terkait dengan domain multicast dapat mengirim lalu lintas multicast, dan anggota grup menerima lalu lintas multicast.

Buat domain multicast IGMP di Transit Gateway AWS

Jika Anda belum melakukannya, tinjau atribut domain multicast yang tersedia. Untuk informasi selengkapnya, lihat the section called “Domain multicast”.

Untuk membuat domain multicast IGMP menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Transit Gateway Multicast.
3. Pilih Buat domain multicast gateway transit.
4. Untuk tag Nama, masukkan nama untuk domain.
5. Untuk ID gateway Transit, pilih gateway transit yang memproses lalu lintas multicast.
6. Untuk IGMPv2 dukungan, pilih kotak centang.

7. Untuk dukungan sumber statis, kosongkan kotak centang.
8. Untuk secara otomatis menerima asosiasi subnet lintas akun untuk domain multicast ini, pilih Terima otomatis asosiasi bersama.
9. Pilih Buat domain multicast gateway transit.

Untuk membuat domain multicast IGMP menggunakan AWS CLI

Gunakan perintah create-transit-gateway-multicast-domain.

```
aws ec2 create-transit-gateway-multicast-domain --transit-gateway-
id tgw-0xexampleid12345 --options StaticSourcesSupport=disable,Igmpv2Support=enable
```

Buat domain multicast sumber statis di AWS Transit Gateway

Jika Anda belum melakukannya, tinjau atribut domain multicast yang tersedia. Untuk informasi selengkapnya, lihat the section called “Domain multicast”.

Untuk membuat domain multicast statis menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Transit Gateway Multicast.
3. Pilih Buat domain multicast gateway transit.
4. Untuk tag Nama, masukkan nama untuk mengidentifikasi domain.
5. Untuk ID gateway Transit, pilih gateway transit yang memproses lalu lintas multicast.
6. Untuk IGMPv2 dukungan, kosongkan kotak centang.
7. Untuk dukungan sumber statis, pilih kotak centang.
8. Untuk secara otomatis menerima asosiasi subnet lintas akun untuk domain multicast ini, pilih Terima otomatis asosiasi bersama.
9. Pilih Buat domain multicast gateway transit.

Untuk membuat domain multicast statis menggunakan AWS CLI

Gunakan perintah create-transit-gateway-multicast-domain.

```
aws ec2 create-transit-gateway-multicast-domain --transit-gateway-
id tgw-0xexampleid12345 --options StaticSourcesSupport=enable,Igmpv2Support=disable
```

Mengaitkan lampiran dan subnet VPC dengan domain multicast di Transit Gateway AWS

Gunakan prosedur berikut untuk mengaitkan lampiran VPC dengan domain multicast. Saat Anda membuat asosiasi, Anda kemudian dapat memilih subnet untuk disertakan dalam domain multicast.

Sebelum memulai, Anda harus membuat lampiran VPC di gateway transit Anda. Untuk informasi selengkapnya, lihat Lampiran Amazon VPC di Transit Gateway AWS.

Untuk mengaitkan lampiran VPC dengan domain multicast menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Transit Gateway Multicast.
3. Pilih domain multicast, lalu pilih Actions, Create Association.
4. Untuk Pilih lampiran yang akan diasosiasikan, pilih lampiran gateway transit.
5. Untuk Pilih subnet untuk diasosiasikan, pilih subnet yang akan disertakan dalam domain multicast.
6. Pilih Buat asosiasi.

Untuk mengaitkan lampiran VPC dengan domain multicast menggunakan AWS CLI

Gunakan perintah associate-transit-gateway-multicast-domain.

Putuskan hubungan subnet dari domain multicast di Transit Gateway AWS

Gunakan prosedur berikut untuk memisahkan subnet dari domain multicast.

Untuk memisahkan subnet menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Transit Gateway Multicast.
3. Pilih domain multicast.
4. Pilih tab Asosiasi.
5. Pilih subnet, lalu pilih Actions, Delete Association.

Untuk memisahkan subnet menggunakan AWS CLI

Gunakan perintah disassociate-transit-gateway-multicast-domain.

Lihat asosiasi domain multicast di AWS Transit Gateway

Lihat domain multicast Anda untuk memverifikasi bahwa domain tersebut tersedia, dan bahwa domain tersebut berisi subnet dan lampiran yang sesuai.

Untuk melihat domain multicast menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Transit Gateway Multicast.
3. Pilih domain multicast.
4. Pilih tab Asosiasi.

Untuk melihat domain multicast menggunakan AWS CLI

Gunakan perintah describe-transit-gateway-multicast-domains.

Tambahkan tag ke domain multicast di AWS Transit Gateway

Tambahkan tag ke sumber daya Anda untuk membantu mengatur dan mengidentifikasi sumber daya tersebut, misalnya berdasarkan tujuan, pemilik, atau lingkungan. Anda dapat menambahkan beberapa tag ke setiap domain multicast. Kunci tag harus unik untuk setiap domain multicast. Jika Anda menambahkan tag dengan kunci yang sudah dikaitkan dengan domain multicast, itu memperbarui nilai tag tersebut. Untuk informasi selengkapnya, lihat Menandai EC2 Sumber Daya Amazon Anda.

Untuk menambahkan tag ke domain multicast menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Transit Gateway Multicast.
3. Pilih domain multicast.
4. Pilih Tindakan, Kelola tag.
5. Untuk setiap tag, pilih Tambahkan tag baru dan masukkan Kunci dan Nilai untuk tag.
6. Pilih Simpan.

Untuk menambahkan tag ke domain multicast menggunakan AWS CLI

Gunakan perintah create-tags.

Menghapus domain multicast di AWS Transit Gateway

Gunakan prosedur berikut untuk menghapus domain multicast.

Untuk menghapus domain multicast menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Transit Gateway Multicast.
3. Pilih domain multicast, lalu pilih Actions, Delete multicast domain.
4. Saat diminta konfirmasi, masukkan **`delete`**, lalu pilih Hapus.

Untuk menghapus domain multicast menggunakan AWS CLI

Gunakan perintah delete-transit-gateway-multicast-domain.

Domain multicast bersama di Transit Gateway AWS

Dengan berbagi domain multicast, pemilik domain multicast dapat berbagi domain dengan AWS akun lain di dalam organisasinya atau di seluruh organisasi. AWS Organizations Sebagai pemilik domain multicast, Anda dapat membuat dan mengelola domain multicast secara terpusat. Setelah dibagikan, pengguna tersebut dapat melakukan operasi berikut pada domain multicast bersama:

- Mendaftarkan dan membatalkan pendaftaran anggota grup atau sumber grup di domain multicast
- Kaitkan subnet dengan domain multicast, dan pisahkan subnet dari domain multicast

Pemilik domain multicast dapat berbagi domain multicast dengan:

- AWS akun di dalam organisasinya atau di seluruh organisasi di AWS Organizations
- Unit organisasi di dalam organisasinya di AWS Organizations
- Seluruh organisasinya di AWS Organizations
- AWS akun di luar AWS Organizations.

  Untuk berbagi domain multicast dengan AWS akun di luar Organisasi Anda, Anda harus membuat pembagian sumber daya menggunakan AWS Resource Access Manager, lalu pilih Izinkan berbagi dengan siapa pun saat memilih Prinsipal untuk berbagi domain multicast. Untuk informasi

selengkapnya tentang membuat pembagian sumber daya, lihat Membuat bagian sumber daya AWS RAM di Panduan AWS RAM Pengguna

Daftar Isi

Prasyarat untuk berbagi domain multicast

- Untuk berbagi domain multicast, Anda harus memilikinya di akun Anda AWS . Anda tidak dapat berbagi domain multicast yang telah dibagikan dengan Anda.
- Untuk berbagi domain multicast dengan organisasi Anda atau unit organisasi di AWS Organizations, Anda harus mengaktifkan berbagi dengan. AWS Organizations Untuk informasi selengkapnya, lihat Mengaktifkan Berbagi dengan AWS Organizations di Panduan AWS RAM Pengguna.

Layanan terkait

Berbagi domain multicast terintegrasi dengan AWS Resource Access Manager ().AWS RAM AWS RAM adalah layanan yang memungkinkan Anda untuk berbagi AWS sumber daya Anda dengan AWS akun apa pun atau melalui AWS Organizations. Dengan AWS RAM, Anda dapat berbagi sumber daya yang Anda miliki dengan membuat berbagi sumber daya. Pembagian sumber daya menentukan sumber daya untuk dibagikan, dan pengguna yang akan dibagikan. Konsumen dapat berupa AWS akun individu, atau unit organisasi atau seluruh organisasi di dalamnya AWS Organizations.

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

Izin domain multicast bersama

Izin untuk pemilik

Pemilik bertanggung jawab untuk mengelola domain multicast dan anggota serta lampiran yang mereka daftarkan atau kaitkan dengan domain. Pemilik dapat mengubah atau mencabut akses bersama kapan saja. Mereka dapat menggunakan AWS Organizations untuk melihat, memodifikasi, dan menghapus sumber daya yang dibuat konsumen pada domain multicast bersama.

Izin untuk konsumen

Pengguna domain multicast bersama dapat melakukan operasi berikut pada domain multicast bersama dengan cara yang sama seperti pada domain multicast yang mereka buat:

- Mendaftarkan dan membatalkan pendaftaran anggota grup atau sumber grup di domain multicast
- Kaitkan subnet dengan domain multicast, dan pisahkan subnet dari domain multicast

Konsumen bertanggung jawab untuk mengelola sumber daya yang mereka buat di domain multicast bersama.

Pelanggan tidak dapat melihat atau memodifikasi sumber daya yang dimiliki oleh konsumen lain atau oleh pemilik domain multicast, dan mereka tidak dapat memodifikasi domain multicast yang dibagikan dengan mereka.

Tagihan dan pengukuran

Tidak ada biaya tambahan untuk berbagi domain multicast baik untuk pemilik, atau konsumen.

Kuota

Domain multicast bersama diperhitungkan terhadap kuota domain multicast pemilik dan pengguna bersama.

Bagikan sumber daya di seluruh Availability Zone di AWS Transit Gateway

Untuk memastikan bahwa sumber daya didistribusikan di seluruh Availability Zone untuk suatu Wilayah, AWS Transit Gateway secara independen memetakan Availability Zone ke nama untuk setiap akun. Hal ini dapat menyebabkan perbedaan penamaan Zona Ketersediaan di seluruh 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 mengidentifikasi lokasi domain multicast Anda relatif terhadap akun Anda, Anda harus menggunakan ID Availability Zone (ID AZ). ID AZ adalah pengidentifikasi unik dan konsisten untuk Availability Zone di semua AWS akun. Misalnya, `use1-az1` adalah ID AZ untuk `us-east-1` Wilayah dan itu adalah lokasi yang sama di setiap AWS akun.

Untuk melihat AZ IDs untuk Availability Zones di akun Anda

1. Buka AWS RAM konsol di https://console.aws.amazon.com/ram/rumah.
2. AZ IDs untuk Wilayah saat ini ditampilkan di panel ID AZ Anda di sisi kanan layar.

Bagikan domain multicast di AWS Transit Gateway

Ketika pemilik berbagi domain multicast dengan Anda, Anda dapat melakukan hal berikut:

- Mendaftarkan dan membatalkan pendaftaran anggota grup atau sumber grup
- Mengaitkan dan memisahkan subnet

> **Note**
>
> Untuk berbagi domain multicast, Anda harus menambahkannya ke berbagi sumber daya. Berbagi sumber daya adalah AWS RAM sumber daya yang memungkinkan Anda berbagi sumber daya di seluruh AWS akun. Pembagian sumber daya menentukan sumber daya yang akan dibagikan, dan konsumen yang akan berbagi dengan mereka. Saat Anda membagikan domain multicast menggunakan domain Amazon Virtual Private Cloud Console, Anda menambahkannya ke pembagian sumber daya yang ada. Untuk menambahkan domain multicast ke pembagian sumber daya baru, Anda harus terlebih dahulu membuat pembagian sumber daya menggunakan konsol.AWS RAM
>
> Jika Anda adalah bagian dari organisasi AWS Organizations dan berbagi dalam organisasi Anda diaktifkan, konsumen di organisasi Anda secara otomatis diberikan akses ke domain multicast bersama. Jika tidak, konsumen menerima undangan untuk bergabung dengan pembagian sumber daya dan diberikan akses ke domain multicast bersama setelah menerima undangan.

Anda dapat berbagi domain multicast yang Anda miliki menggunakan Amazon Virtual Private Cloud konsol, AWS RAM konsol, atau. AWS CLI

Untuk berbagi domain multicast yang Anda miliki menggunakan *Amazon Virtual Private Cloud Console

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Domain Multicast.
3. Pilih domain multicast Anda, lalu pilih Actions, Share multicast domain.
4. Pilih berbagi sumber daya Anda dan pilih Bagikan domain multicast.

Untuk berbagi domain multicast yang Anda miliki menggunakan konsol AWS RAM

Lihat Membuat Sumber Daya Bersama di Panduan Pengguna AWS RAM .

Untuk berbagi domain multicast yang Anda miliki menggunakan AWS CLI

Gunakan perintah create-resource-share.

Membatalkan berbagi domain multicast bersama di Transit Gateway AWS

Ketika domain multicast bersama tidak dibagikan, hal berikut terjadi pada sumber daya domain multicast konsumen:

- Subnet konsumen dipisahkan dari domain multicast. Subnet tetap ada di akun konsumen.
- Sumber grup konsumen dan anggota grup dipisahkan dari domain multicast, dan kemudian dihapus dari akun konsumen.

Untuk membatalkan berbagi domain multicast, Anda harus menghapusnya dari pembagian sumber daya. Anda dapat melakukan ini dari AWS RAM konsol atau AWS CLI.

Untuk membatalkan berbagi domain multicast bersama yang Anda miliki, Anda harus menghapusnya dari pembagian sumber daya. Anda dapat melakukan ini menggunakan Amazon Virtual Private Cloud, AWS RAM konsol, atau AWS CLI.

Untuk membatalkan berbagi domain multicast bersama yang Anda miliki menggunakan *Amazon Virtual Private Cloud Console

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Domain Multicast.
3. Pilih domain multicast Anda, lalu pilih Actions, Stop sharing.

Untuk membatalkan berbagi domain multicast bersama yang Anda miliki menggunakan konsol AWS RAM

Lihat Memperbarui Sumber Daya Bersama di Panduan Pengguna AWS RAM .

Untuk membatalkan berbagi domain multicast bersama yang Anda miliki menggunakan AWS CLI

Gunakan perintah disassociate-resource-share.

Identifikasi domain multicast bersama di AWS Transit Gateway

Pemilik dan konsumen dapat mengidentifikasi domain multicast bersama menggunakan dan Amazon Virtual Private Cloud AWS CLI

Untuk mengidentifikasi domain multicast bersama menggunakan *Amazon Virtual Private Cloud Console

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Domain Multicast.
3. Pilih domain multicast Anda.
4. Pada halaman Detail Domain Transit Multicast, lihat ID Pemilik untuk mengidentifikasi ID AWS akun domain multicast.

Untuk mengidentifikasi domain multicast bersama menggunakan AWS CLI

Gunakan perintah describe-transit-gateway-multicast-domains. Perintah mengembalikan domain multicast yang Anda miliki dan domain multicast yang dibagikan dengan Anda. `OwnerId`menunjukkan ID AWS akun pemilik domain multicast.

Daftarkan sumber dengan grup multicast di AWS Transit Gateway

> **Note**
>
> Prosedur ini hanya diperlukan ketika Anda telah mengatur atribut dukungan sumber Statis untuk mengaktifkan.

Gunakan prosedur berikut untuk mendaftarkan sumber dengan grup multicast. Sumbernya adalah antarmuka jaringan yang mengirimkan lalu lintas multicast.

Anda memerlukan informasi berikut sebelum menambahkan sumber:

- ID domain multicast
- IDs Antarmuka jaringan sumber
- Alamat IP grup multicast

Untuk mendaftarkan sumber menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Transit Gateway Multicast.
3. Pilih domain multicast, lalu pilih Tindakan, Tambahkan sumber grup.
4. Untuk alamat IP Grup, masukkan blok IPv4 CIDR atau blok IPv6 CIDR untuk ditetapkan ke domain multicast.
5. Di bawah Pilih antarmuka jaringan, pilih antarmuka jaringan pengirim multicast.
6. Pilih Tambahkan sumber.

Untuk mendaftarkan sumber menggunakan AWS CLI

Gunakan perintah register-transit-gateway-multicast-group-sources.

Daftarkan anggota dengan grup multicast di AWS Transit Gateway

Gunakan prosedur berikut untuk mendaftarkan anggota grup dengan grup multicast.

Anda memerlukan informasi berikut sebelum menambahkan anggota:

- ID dari domain multicast
- IDs Antarmuka jaringan anggota grup
- Alamat IP grup multicast

Untuk mendaftarkan anggota menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Transit Gateway Multicast.
3. Pilih domain multicast, lalu pilih Tindakan, Tambahkan anggota grup.

4. Untuk alamat IP Grup, masukkan blok IPv4 CIDR atau blok IPv6 CIDR untuk ditetapkan ke domain multicast.
5. Di bawah Pilih antarmuka jaringan, pilih antarmuka jaringan penerima multicast.
6. Pilih Tambahkan anggota.

Untuk mendaftarkan anggota menggunakan AWS CLI

Gunakan perintah register-transit-gateway-multicast-group-members.

Deregister sumber dari grup multicast di Transit Gateway AWS

Anda tidak perlu mengikuti prosedur ini kecuali Anda menambahkan sumber secara manual ke grup multicast.

Untuk menghapus sumber menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Transit Gateway Multicast.
3. Pilih domain multicast.
4. Pilih tab Grup.
5. Pilih sumber, lalu pilih Hapus sumber.

Untuk menghapus sumber menggunakan AWS CLI

Gunakan perintah deregister-transit-gateway-multicast-group-sources.

Membatalkan pendaftaran anggota dari grup multicast di Transit Gateway AWS

Anda tidak perlu mengikuti prosedur ini kecuali Anda menambahkan anggota secara manual ke grup multicast.

Untuk membatalkan pendaftaran anggota menggunakan konsol

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

3. Pilih domain multicast.
4. Pilih tab Grup.
5. Pilih anggota, lalu pilih Hapus anggota.

Untuk membatalkan pendaftaran anggota menggunakan AWS CLI

Gunakan perintah deregister-transit-gateway-multicast-group-members.

Lihat grup multicast di AWS Transit Gateway

Anda dapat melihat informasi tentang grup multicast Anda untuk memverifikasi bahwa anggota ditemukan menggunakan protokol. IGMPv2 Jenis anggota (di konsol), atau `MemberType` (dalam AWS CLI) menampilkan IGMP saat AWS ditemukan anggota dengan protokol.

Untuk melihat grup multicast menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Transit Gateway Multicast.
3. Pilih domain multicast.
4. Pilih tab Grup.

Untuk melihat grup multicast menggunakan AWS CLI

Gunakan perintah search-transit-gateway-multicast-groups.

Contoh berikut menunjukkan bahwa protokol IGMP menemukan anggota grup multicast.

```
aws ec2 search-transit-gateway-multicast-groups --transit-gateway-multicast-domain tgw-mcast-domain-000fb24d04EXAMPLE
{
    "MulticastGroups": [
        {
            "GroupIpAddress": "224.0.1.0",
            "TransitGatewayAttachmentId": "tgw-attach-0372e72386EXAMPLE",
            "SubnetId": "subnet-0187aff814EXAMPLE",
            "ResourceId": "vpc-0065acced4EXAMPLE",
            "ResourceType": "vpc",
            "NetworkInterfaceId": "eni-03847706f6EXAMPLE",
```

```
            "MemberType": "igmp"
        }
    ]
}
```

Siapkan multicast untuk Windows Server di AWS Transit Gateway

Anda harus melakukan langkah-langkah tambahan saat menyiapkan multicast untuk bekerja dengan gateway transit di Windows Server 2019 atau 2022. Untuk mengatur ini, Anda harus menggunakan PowerShell, dan menjalankan perintah berikut:

Untuk mengatur multicast untuk Windows Server menggunakan PowerShell

1. Ubah Windows Server untuk digunakan IGMPv2 alih-alih IGMPv3 untuk TCP/IP tumpukan:

   ```
   PS C:\> New-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services
   \Tcpip\Parameters -Name IGMPVersion -PropertyType DWord -Value 3
   ```

   > **Note**
   >
   > `New-ItemProperty`adalah indeks properti yang menentukan versi IGMP. Karena IGMP v2 adalah versi yang didukung untuk multicast, properti `Value` harus. `3` Alih-alih mengedit registri Windows Anda dapat menjalankan perintah berikut untuk mengatur versi IGMP ke 2. :
   > `Set-NetIPv4Protocol -IGMPVersion Version2`

2. Windows Firewall menurunkan sebagian besar lalu lintas UDP secara default. Pertama-tama Anda harus memeriksa profil koneksi mana yang digunakan untuk multicast:

   ```
   PS C:\> Get-NetConnectionProfile | Select-Object NetworkCategory

   NetworkCategory
   ---------------
            Public
   ```

3. Perbarui profil koneksi dari langkah sebelumnya untuk memungkinkan akses ke port UDP yang diperlukan:

   ```
   PS C:\> Set-NetFirewallProfile -Profile Public -Enabled False
   ```

4. Reboot EC2 instance.

5. Uji aplikasi multicast Anda untuk memastikan lalu lintas mengalir seperti yang diharapkan.

Contoh: Mengelola konfigurasi IGMP menggunakan AWS Transit Gateway

Contoh ini menunjukkan setidaknya satu host yang menggunakan protokol IGMP untuk lalu lintas multicast. AWS secara otomatis membuat grup multicast ketika menerima `JOIN` pesan IGMP dari sebuah instance, dan kemudian menambahkan instance sebagai anggota dalam grup ini. Anda juga dapat menambahkan host non-IGMP secara statis sebagai anggota ke grup menggunakan. AWS CLI Setiap contoh yang ada di subnet yang terkait dengan domain multicast dapat mengirim lalu lintas, dan anggota grup menerima lalu lintas multicast.

Gunakan langkah-langkah berikut untuk menyelesaikan konfigurasi:

1. Buat sebuah VPC. Untuk informasi selengkapnya, lihat Membuat VPC di Panduan Pengguna Amazon VPC.
2. Buat subnet di VPC. Untuk informasi selengkapnya, lihat Membuat subnet di Panduan Pengguna Amazon VPC.
3. Buat gateway transit yang dikonfigurasi untuk lalu lintas multicast. Untuk informasi selengkapnya, lihat the section called “Membuat transit gateway”.
4. Buat lampiran VPC. Untuk informasi selengkapnya, lihat the section called “Buat lampiran VPC”.
5. Buat domain multicast yang dikonfigurasi untuk dukungan IGMP. Untuk informasi selengkapnya, lihat the section called “Buat domain multicast IGMP”.

   Gunakan pengaturan berikut:

   - Aktifkan IGMPv2 dukungan.
   - Nonaktifkan dukungan sumber statis.
6. Buat asosiasi antara subnet di lampiran VPC gateway transit dan domain multicast. Untuk mengetahui informasi selengkapnya, lihat the section called “Mengaitkan lampiran dan subnet VPC dengan domain multicast”.
7. Versi IGMP default untuk EC2 adalah. IGMPv3 Anda perlu mengubah versi untuk semua anggota grup IGMP. Anda dapat menjalankan perintah berikut:

   ```
   sudo sysctl net.ipv4.conf.eth0.force_igmp_version=2
   ```
8. Tambahkan anggota yang tidak menggunakan protokol IGMP ke grup multicast. Lihat informasi yang lebih lengkap di the section called “Daftarkan anggota dengan grup multicast”.

Contoh: Mengelola konfigurasi sumber statis di AWS Transit Gateway

Contoh ini secara statis menambahkan sumber multicast ke grup. Host tidak menggunakan protokol IGMP untuk bergabung atau meninggalkan grup multicast. Anda perlu menambahkan anggota grup secara statis yang menerima lalu lintas multicast.

Gunakan langkah-langkah berikut untuk menyelesaikan konfigurasi:

1. Buat sebuah VPC. Untuk informasi selengkapnya, lihat Membuat VPC di Panduan Pengguna Amazon VPC.
2. Buat subnet di VPC. Untuk informasi selengkapnya, lihat Membuat subnet di Panduan Pengguna Amazon VPC.
3. Buat gateway transit yang dikonfigurasi untuk lalu lintas multicast. Untuk informasi selengkapnya, lihat the section called “Membuat transit gateway”.
4. Buat lampiran VPC. Untuk informasi selengkapnya, lihat the section called “Buat lampiran VPC”.
5. Buat domain multicast yang dikonfigurasi tanpa dukungan IGMP, dan dukungan untuk menambahkan sumber secara statis. Untuk informasi selengkapnya, lihat the section called “Buat domain multicast sumber statis”.

   Gunakan pengaturan berikut:

   - Nonaktifkan IGMPv2 dukungan.
   - Untuk menambahkan sumber secara manual, aktifkan dukungan Sumber statis.

     Sumber adalah satu-satunya sumber daya yang dapat mengirim lalu lintas multicast saat atribut diaktifkan. Jika tidak, setiap instance yang ada di subnet yang terkait dengan domain multicast dapat mengirim lalu lintas multicast, dan anggota grup menerima lalu lintas multicast.
6. Buat asosiasi antara subnet di lampiran VPC gateway transit dan domain multicast. Untuk mengetahui informasi selengkapnya, lihat the section called “Mengaitkan lampiran dan subnet VPC dengan domain multicast”.
7. Jika Anda mengaktifkan dukungan sumber statis, tambahkan sumber ke grup multicast. Untuk informasi selengkapnya, lihat the section called “Daftarkan sumber dengan grup multicast”.
8. Tambahkan anggota ke grup multicast. Lihat informasi yang lebih lengkap di the section called “Daftarkan anggota dengan grup multicast”.

Contoh: Mengelola konfigurasi anggota grup statis di AWS Transit Gateway

Contoh ini menunjukkan secara statis menambahkan anggota multicast ke grup. Host tidak dapat menggunakan protokol IGMP untuk bergabung atau meninggalkan grup multicast. Setiap instance yang ada di subnet yang terkait dengan domain multicast dapat mengirim lalu lintas multicast, dan anggota grup menerima lalu lintas multicast.

Gunakan langkah-langkah berikut untuk menyelesaikan konfigurasi:

1. Buat sebuah VPC. Untuk informasi selengkapnya, lihat Membuat VPC di Panduan Pengguna Amazon VPC.
2. Buat subnet di VPC. Untuk informasi selengkapnya, lihat Membuat subnet di Panduan Pengguna Amazon VPC.
3. Buat gateway transit yang dikonfigurasi untuk lalu lintas multicast. Untuk informasi selengkapnya, lihat the section called “Membuat transit gateway”.
4. Buat lampiran VPC. Untuk informasi selengkapnya, lihat the section called “Buat lampiran VPC”.
5. Buat domain multicast yang dikonfigurasi tanpa dukungan IGMP, dan dukungan untuk menambahkan sumber secara statis. Untuk informasi selengkapnya, lihat the section called “Buat domain multicast sumber statis”.

   Gunakan pengaturan berikut:

   - Nonaktifkan IGMPv2 dukungan.
   - Nonaktifkan dukungan sumber statis.
6. Buat asosiasi antara subnet di lampiran VPC gateway transit dan domain multicast. Untuk mengetahui informasi selengkapnya, lihat the section called “Mengaitkan lampiran dan subnet VPC dengan domain multicast”.
7. Tambahkan anggota ke grup multicast. Lihat informasi yang lebih lengkap di the section called “Daftarkan anggota dengan grup multicast”.

Alokasi biaya yang fleksibel

Secara default, transit gateway menggunakan model alokasi biaya berbasis pengirim di mana biaya pemrosesan data dialokasikan ke akun yang memiliki lampiran sumber. Anda dapat membuat kebijakan pengukuran khusus yang menentukan akun mana yang harus dibebankan berdasarkan properti arus lalu lintas seperti jenis lampiran, ID lampiran tertentu, atau alamat jaringan.

Kebijakan pengukuran terdiri dari aturan terurut yang dievaluasi dari nomor aturan terendah hingga tertinggi. Ketika lalu lintas cocok dengan aturan, akun yang ditentukan dibebankan sesuai dengan konfigurasi aturan. Anda dapat menentukan pemilik akun untuk mengalokasikan biaya dari opsi berikut:

- Pemilik lampiran sumber - Biaya dialokasikan ke akun yang memiliki lampiran sumber (perilaku default)
- Pemilik lampiran tujuan - Biaya dialokasikan ke akun yang memiliki lampiran tujuan
- Pemilik Transit Gateway - Biaya dialokasikan ke akun yang memiliki gateway transit

Alokasi Biaya Fleksibel memungkinkan manajemen biaya yang lebih baik untuk organisasi yang menggunakan arsitektur jaringan terpusat, memungkinkan biaya dialokasikan ke unit bisnis atau pemilik aplikasi yang sesuai terlepas dari topologi jaringan.

> **Note**
>
> Alokasi Biaya Fleksibel memungkinkan alokasi penggunaan pengukuran yang fleksibel dan pada gilirannya biaya untuk pemilik akun pilihan Anda. Namun, implikasi pajak untuk AWS akun dapat bervariasi secara signifikan berdasarkan lokasi geografis, pola penggunaan, dan faktor lainnya. Harap tinjau implikasi penagihan, pajak, dan manajemen biaya untuk akun di AWS Organisasi Anda sebelum mengaktifkan fitur ini. Referensi: Apa itu AWS Billing and Cost Management?

Kebijakan pengukuran

Kebijakan pengukuran memungkinkan Anda mengonfigurasi aturan alokasi biaya untuk gateway transit Anda untuk mengontrol akun mana yang dikenakan biaya untuk pemrosesan data dan biaya transfer berdasarkan properti arus lalu lintas. Fitur ini memungkinkan manajemen biaya dan kemampuan chargeback yang lebih baik untuk organisasi yang menggunakan arsitektur jaringan terpusat.

Kebijakan pengukuran terdiri dari yang berikut:

- Kebijakan pengukuran - Kontainer konfigurasi keseluruhan yang berisi Aturan Kebijakan Pengukuran. Saat dibuat, ini berisi satu entri kebijakan pengukuran default yang dikonfigurasi untuk mengisi daya semua lalu lintas ke pemilik lampiran sumber. Setiap gateway transit hanya dapat memiliki satu kebijakan pengukuran.

- Entri kebijakan pengukuran - Aturan individual dalam kebijakan pengukuran yang menentukan kriteria pencocokan spesifik dan penggunaan akun untuk meteran. Setiap entri menyertakan nomor aturan untuk urutan evaluasi, kondisi pencocokan lalu lintas (seperti jenis lampiran sumber dan tujuan, ID lampiran, blok CIDR, port, dan protokol), dan pemilik akun mana yang dikenakan biaya untuk lalu lintas yang cocok. Kebijakan dapat berisi hingga 50 entri, dievaluasi dalam urutan dari nomor aturan terendah hingga tertinggi.

  Anda dapat mengalokasikan penggunaan pengukuran untuk salah satu dari berikut ini:

  - Pemilik lampiran sumber: Mengalokasikan penggunaan pengukuran ke akun yang memiliki lampiran tempat lalu lintas berasal (perilaku default)
  - Pemilik lampiran tujuan: Mengalokasikan penggunaan pengukuran ke akun yang memiliki lampiran tempat lalu lintas berakhir, dan
  - pemilik gateway transit: Mengalokasikan penggunaan pengukuran ke akun yang memiliki gateway transit.
- Lampiran Middlebox - (Opsional) Lampiran gateway transit yang ditunjuk yang merutekan lalu lintas melalui peralatan jaringan untuk inspeksi keamanan, penyeimbangan beban, atau fungsi jaringan lainnya. Penggunaan data untuk lampiran middlebox yang melintasi lalu lintas diukur ke pemilik akun yang ditentukan dalam kebijakan pengukuran. Anda dapat menentukan maksimal 10 lampiran middlebox. Jenis lampiran middlebox yang didukung adalah Network Function (AWS Network Firewall), lampiran VPC dan VPN.

Cara kerja kebijakan pengukuran

Secara default, transit gateway menggunakan model alokasi biaya berbasis pengirim di mana biaya pemrosesan data diukur ke akun yang memiliki lampiran sumber. Dengan kebijakan pengukuran, Anda dapat membuat aturan khusus untuk mengukur penggunaan secara fleksibel berdasarkan properti arus lalu lintas berikut:

- Jenis lampiran sumber dan tujuan (VPC, VPN, Client VPN, Direct Connect Gateway, Peering, Network Function, dan VPN Concentrator)
- ID lampiran sumber dan tujuan
- Alamat IP sumber dan tujuan, rentang Port dan protokol

Kebijakan pengukuran terdiri dari aturan terurut yang dievaluasi dari nomor aturan terendah hingga tertinggi. Ketika lalu lintas cocok dengan aturan, akun yang ditentukan dibebankan sesuai dengan

pengaturan akun terukur aturan. Kebijakan pengukuran membahas beberapa skenario organisasi umum:

- Alokasi biaya lingkungan hibrid: Alokasikan biaya untuk data yang masuk AWS dari lokal melalui Direct Connect Gateway ke pemilik akun VPC tujuan, bukan pemilik akun admin TI pusat.
- Arsitektur inspeksi terpusat: Alokasikan biaya untuk aplikasi individu atau pemilik akun VPC daripada tim keamanan pusat untuk melintasi lalu lintas melalui VPC inspeksi.
- Application-based chargeback: Alokasikan semua biaya penggunaan data untuk beban kerja ke pemilik VPC terlepas dari arah lalu lintas.
- Alokasi biaya klien: Alokasikan biaya data ke akun klien saat mereka membuat lampiran ke gateway transit Anda.

Lampiran Middlebox

Kebijakan pengukuran gateway transit mendukung lampiran Middlebox yang memungkinkan Anda mengalokasikan biaya pemrosesan data secara fleksibel untuk lalu lintas jaringan yang dirutekan melalui peralatan middlebox seperti firewall jaringan dan penyeimbang beban. Contoh lampiran middlebox adalah lampiran Fungsi Jaringan ke AWS Network Firewall atau lampiran VPC yang merutekan lalu lintas ke peralatan keamanan pihak ketiga dalam VPC. Lalu lintas antara lampiran gateway transit sumber dan tujuan melintasi lampiran middlebox ini untuk kasus penggunaan pemeriksaan keamanan yang khas. Anda dapat menentukan kebijakan pengukuran untuk mengalokasikan penggunaan pemrosesan data secara fleksibel pada lampiran middlebox ke lampiran sumber asli, lampiran tujuan akhir, atau pemilik akun gateway transit. Untuk lampiran Fungsi Jaringan, biaya pemrosesan data AWS Network Firewall juga dialokasikan ke akun terukur.

Alokasi Biaya Fleksibel - Jenis penggunaan pengukuran

Alokasi biaya yang fleksibel melalui kebijakan pengukuran berlaku untuk jenis penggunaan data berikut:

- Penggunaan Pemrosesan Data gateway transit pada lampiran VPC, VPN, Client VPN, Konsentrator VPN, dan Direct Connect
- Penggunaan Transfer Data Client VPN Out pada lampiran Client VPN
- Site-to-site Penggunaan Transfer Data VPN Keluar pada lampiran VPN
- Penggunaan Direct Connect Data Transfer Out pada lampiran Direct Connect.
- Penggunaan transfer data pada lampiran peering TGW

- Gateway transit Penggunaan pemrosesan data pada lampiran Fungsi Jaringan
- AWS penggunaan pemrosesan data firewall jaringan (NFW) pada lampiran Fungsi Jaringan.

Alokasi biaya yang fleksibel tidak berlaku untuk penggunaan lampiran per jam dan penggunaan pemrosesan data multicast. Untuk lampiran Transit Gateway Connect, kebijakan pengukuran dapat ditentukan untuk lampiran VPC transport atau Direct Connect yang mendasarinya. Untuk lampiran Private IP VPN, kebijakan pengukuran dapat ditentukan untuk lampiran transport Direct Connect yang mendasarinya.

Pertimbangan dan batasan

Pertimbangkan hal berikut saat menerapkan kebijakan pengukuran untuk gateway transit Anda.

Izin

- Hanya pemilik gateway transit yang dapat membuat, memodifikasi, atau menghapus kebijakan pengukuran.
- Pengaturan alokasi biaya berlaku di tingkat gateway transit.
- Pemilik lampiran tidak dapat mengganti pengaturan alokasi biaya yang dikonfigurasi oleh pemilik gateway transit.

Pengintip Transit Gateway

Saat lalu lintas melintasi koneksi peering gateway transit:

- Setiap gateway transit menerapkan kebijakan pengukuran sendiri secara independen.
- Biaya data dialokasikan secara terpisah oleh setiap gateway transit berdasarkan kebijakan lokalnya.
- Lalu lintas dapat dianggap sebagai dua arus terpisah: keterikatan sumber untuk mengintip, dan mengintip ke lampiran tujuan.

Integrasi Cloud WAN

Ketika gateway transit dilampirkan ke jaringan inti Cloud WAN:

- Biaya transfer data gateway transit pada koneksi peering dialokasikan sesuai dengan kebijakan pengukuran gateway transit.

- Kebijakan pengukuran tidak didukung pada jaringan inti Cloud WAN.

Dampak kinerja

- Kebijakan pengukuran tidak memperkenalkan latensi jalur data tambahan.
- Kebijakan pengukuran tidak berdampak pada bandwidth maksimum per lampiran.
- Tidak ada perubahan pada kemampuan berbagi sumber daya gateway transit.

Integrasi penagihan

- Tag alokasi biaya terus bekerja dengan kebijakan pengukuran untuk mengatur biaya berdasarkan unit bisnis.
- Kebijakan pengukuran menentukan akun mana yang mengeluarkan biaya, sementara tag alokasi biaya membantu mengkategorikan biaya tersebut.
- Perubahan kebijakan pengukuran akan berlaku pada akhir jam penagihan berikutnya.

Dukungan IPv6

Kebijakan pengukuran didukung untuk lalu lintas IPv4 dan IPv6. Pencocokan blok CIDR dalam entri kebijakan berfungsi dengan kedua keluarga alamat.

Dukungan lampiran Middlebox

- Kebijakan pengukuran Middlebox mengasumsikan lalu lintas antara sumber asli dan lampiran tujuan disematkan melalui lampiran kotak tengah yang ditentukan (contoh inspeksi timur-barat untuk lalu lintas). VPC-to-VPC Oleh karena itu jaringan 5-tuple (source/destination IP, source/destination port, dan protokol) untuk aliran yang masuk dan keluar dari lampiran kotak tengah harus cocok. Aliran dengan kesalahan kecocokan 5 tupel pada lampiran kotak tengah (misalnya transformasi NAT dalam VPC inspeksi) diperlakukan sebagai aliran lampiran tujuan sumber biasa (sebagai lawan dari aliran lampiran kotak tengah).
- Semua aliran egress-only pada lampiran middlebox (misalnya lalu lintas utara-selatan ke internet melalui IGW dalam VPC inspeksi) diperlakukan sebagai aliran tujuan sumber biasa (sebagai lawan dari aliran lampiran kotak tengah).
- Untuk lampiran Fungsi Jaringan saat firewall AWS Jaringan menjatuhkan paket, semua penggunaan pemrosesan data dibebankan kembali ke akun pengirim terlepas dari konfigurasi kebijakan pengukuran.

Membuat kebijakan pengukuran AWS Transit Gateway

Untuk mengaktifkan kebijakan pengukuran, Anda harus membuat kebijakan pengukuran untuk gateway transit dan mengonfigurasi entri kebijakan yang menentukan cara penggunaan pengukuran dialokasikan. Kebijakan pengukuran menetapkan kerangka kerja dan pengaturan default, sementara entri kebijakan berisi aturan khusus yang menentukan akun mana yang diukur berdasarkan karakteristik lalu lintas.

Entri kebijakan pengukuran berfungsi sebagai aturan terurut yang diterapkan secara berurutan dari nomor aturan terendah hingga tertinggi untuk lalu lintas yang mengalir melalui gateway transit Anda. Setiap entri mendefinisikan kriteria pencocokan seperti jenis lampiran sumber dan tujuan, blok CIDR, protokol, dan rentang port, bersama dengan akun yang harus diukur untuk mencocokkan lalu lintas. Ketika arus lalu lintas cocok dengan beberapa entri, entri dengan nomor aturan terendah diutamakan. Jika tidak ada entri yang cocok dengan alur tertentu, akun terukur default yang ditentukan dalam kebijakan akan dikenakan biaya.

Setelah membuat kebijakan, Anda harus menambahkan entri kebijakan untuk menerapkan logika alokasi biaya. Untuk langkah-langkah membuat entri kebijakan pengukuran, lihatBuat entri kebijakan pengukuran.

Membuat kebijakan pengukuran menggunakan konsol

Buat kebijakan untuk menentukan aturan alokasi biaya yang fleksibel untuk penggunaan data gateway transit. Secara default, semua aliran diukur ke pemilik lampiran sumber. Buat entri untuk menagih aliran jaringan tertentu ke akun yang berbeda.

Untuk membuat kebijakan pengukuran

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Kebijakan pengukuran.
3. Pilih Buat kebijakan pengukuran.
4. Untuk ID gateway Transit pilih gateway transit yang ingin Anda buat kebijakan pengukuran.
5. (Opsional) Untuk lampiran Middlebox IDs, pilih satu atau lebih lampiran middlebox. Secara default, penggunaan data diukur ke pemilik middlebox. Dukungan lampiran Middlebox memungkinkan kebijakan pengukuran diterapkan untuk lalu lintas melintasi lampiran middlebox. Lampiran tambahan dapat ditambahkan nanti.
6. (Opsional) Di bagian Tag, tambahkan tag untuk membantu Anda mengidentifikasi dan mengatur kebijakan pengukuran Anda:

a. Pilih Tambahkan tag baru.
b. Masukkan tag Key dan opsional tag Nilai.
c. Pilih Tambahkan tag baru untuk menambahkan tag tambahan, atau lewati ke langkah berikutnya. Anda dapat menambahkan hingga 50 tanda.

7. Pilih Buat kebijakan pengukuran gateway transit.

> **Note**
>
> Akun terukur default adalah pemilik lampiran sumber, dan setelah membuat kebijakan pengukuran, Anda dapat menambahkan entri yang menentukan akun mana yang dikenakan biaya berdasarkan properti arus lalu lintas, dengan mencatat bahwa entri kebijakan default (yang merupakan entri terakhir) tidak dapat diubah atau dihapus seperti entri kebijakan lainnya.

Buat kebijakan pengukuran menggunakan AWS CLI

Kebijakan pengukuran menentukan perilaku alokasi biaya default dan pengaturan global untuk gateway transit Anda. Gunakan create-transit-gateway-metering-policy.

Parameter yang diperlukan:

- `--transit-gateway-id`- ID gateway transit untuk membuat kebijakan

Parameter opsional:

- `--middle-box-attachment-ids`- Id lampiran gateway transit yang didukung untuk ditambahkan ke kebijakan sebagai middlebox
- `--tag-specifications`- tag untuk kebijakan pengukuran

Untuk membuat kebijakan pengukuran menggunakan AWS CLI

1. Jalankan create-transit-gateway-metering-policy perintah untuk membuat kebijakan pengukuran baru dengan lampiran middlebox opsional.

```
aws ec2 create-transit-gateway-metering-policy \
```

```
    --transit-gateway-id tgw-07a5946195a67dc47 \
    --middle-box-attachment-ids \
    tgw-attach-0123456789abcdef0 \
    tgw-attach-0abc123def456789a \
    --tag-specifications \
    '[{ "ResourceType": "transit-gateway-metering-policy", \
    "Tags": [ { "Key": "Env", "Value": "Prod" } ] }]'
```

Perintah ini membuat kebijakan pengukuran untuk gateway transit yang ditentukan dengan lampiran dan tag middlebox yang disediakan.

2. Perintah mengembalikan output berikut ketika kebijakan berhasil dibuat:

```
{
    "TransitGatewayMeteringPolicy": {
        "TransitGatewayMeteringPolicyId": "tgw-mp-042d444564d4b2da7",
        "TransitGatewayId": "tgw-07a5946195a67dc47",
        "MiddleboxAttachmentIds":  ["tgw-attach-0123456789abcdef0",
        "tgw-attach-0abc123def456789a"],
        "State": "pending",
        "UpdateEffectiveAt": "2025-11-05T21:00:00.000Z",
        "Tags": [{"Key": "Env","Value": "Prod"}]
    }
}
```

Perhatikan ID kebijakan pengukuran yang ditampilkan dalam respons untuk digunakan dalam perintah berikutnya. describe-transit-gateway-metering-policiesperintah dapat digunakan untuk mendapatkan kebijakan pengukuran yang terkait dengan gateway transit.

Kelola AWS kebijakan pengukuran Transit Gateway

Setelah membuat kebijakan pengukuran, Anda dapat mengelolanya dengan melihat setelan saat ini, mengubah opsi konfigurasi, atau menghapus kebijakan saat tidak diperlukan lagi. Operasi manajemen memungkinkan Anda untuk menambah atau menghapus lampiran middlebox saat persyaratan jaringan Anda berubah. Anda hanya dapat membuat atau menghapus entri kebijakan. Jika Anda perlu mengubah aturan yang ada, Anda dapat menghapus entri dan membuat yang baru dengan konfigurasi yang dimodifikasi. Semua operasi manajemen memerlukan izin pemilik gateway transit dan berlaku setelah dua jam penagihan.

Manajemen kebijakan pengukuran yang efektif sangat penting untuk menjaga alokasi biaya yang akurat seiring perkembangan arsitektur jaringan Anda. Organizations sering perlu menyesuaikan kebijakan mereka ketika unit bisnis berubah, aplikasi baru dikerahkan, atau topologi jaringan dimodifikasi. Misalnya pengaturan dukungan metering middlebox mungkin memerlukan pembaruan ketika arsitektur keamanan firewall berubah atau ketika layanan inspeksi baru diperkenalkan ke jalur lalu lintas.

Modifikasi kebijakan mendukung berbagai skenario operasional termasuk perubahan pola lalu lintas musiman, aktivitas merger dan akuisisi, dan pembaruan persyaratan kepatuhan. Saat mengelola kebijakan, pertimbangkan dampaknya terhadap pengaturan penagihan yang ada dan komunikasikan perubahan kepada pemangku kepentingan yang terkena dampak sebelum implementasi.

Tinjauan kebijakan reguler membantu memastikan bahwa alokasi biaya tetap selaras dengan tujuan bisnis dan struktur organisasi. Praktik terbaik termasuk mendokumentasikan perubahan kebijakan, menguji modifikasi di lingkungan non-produksi bila memungkinkan, dan berkoordinasi dengan tim keuangan untuk memahami implikasi penagihan. Selain itu, pertimbangkan waktu perubahan kebijakan untuk meminimalkan gangguan pada siklus penagihan bulanan dan proses pelaporan keuangan.

Topik

Mengedit kebijakan pengukuran AWS Transit Gateway

Edit kebijakan pengukuran yang ada untuk memodifikasi konfigurasi lampiran middlebox. Modifikasi kebijakan berlaku pada jam penagihan berikutnya dan berlaku untuk semua arus lalu lintas future melalui gateway transit Anda.

Mengedit kebijakan pengukuran menggunakan konsol

Gunakan konsol untuk mengubah setelan kebijakan pengukuran yang ada untuk gateway transit Anda.

Untuk mengedit kebijakan pengukuran yang ada menggunakan konsol

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

3. Pilih kebijakan pengukuran yang ingin Anda ubah dengan memilih ID kebijakannya
4. Ubah setelan kebijakan yang tersedia di bawah Tindakan. Konsol hanya mengizinkan menambah dan menghapus lampiran kotak Tengah.

    - Lampiran Middlebox - Menambahkan atau menghapus lampiran gateway transit yang harus diperlakukan sebagai middlebox untuk penagihan khusus.

Mengedit kebijakan pengukuran menggunakan AWS CLI

Gunakan modify-transit-gateway-metering-policy perintah untuk melihat dan memodifikasi kebijakan pengukuran.

Parameter yang diperlukan untuk memodifikasi operasi:

- `--transit-gateway-metering-policy-id`- ID kebijakan pengukuran untuk memodifikasi
- `--add-middle-box-attachment-ids`atau `--remove-middle-box-attachment-ids` - Id lampiran gateway transit yang didukung untuk ditambahkan atau dihapus dari kebijakan sebagai middlebox

Untuk melihat dan mengedit kebijakan pengukuran menggunakan CLI AWS

1. (Opsional) Lihat kebijakan pengukuran yang ada menggunakan describe-transit-gateway-metering-policies perintah untuk melihat pengaturan konfigurasi saat ini:

    ```
    aws ec2 describe-transit-gateway-metering-policies
    ```

    Perintah ini menampilkan semua kebijakan pengukuran di akun Anda, menampilkan statusnya saat ini, dan lampiran diaktifkan sebagai middlebox untuk setiap kebijakan pengukuran.
2. Ubah kebijakan pengukuran menggunakan modify-transit-gateway-metering-policy perintah untuk memperbarui opsi konfigurasi:

    ```
    aws ec2 modify-transit-gateway-metering-policy \
        --transit-gateway-metering-policy-id tgw-mp-042d444564d4b2da7 \
        --add-middle-box-attachment-ids tgw-attach-0123456789abcdef1  \
        --remove-middle-box-attachment-ids tgw-attach-0abc123def456789a
    ```

    Perintah ini memodifikasi kebijakan pengukuran dengan menambahkan and/or menghapus lampiran middlebox.

3. Perintah mengembalikan output berikut ketika kebijakan berhasil dimodifikasi:

```
{
    "TransitGatewayMeteringPolicy": {
        "TransitGatewayMeteringPolicyId": "tgw-mp-042d444564d4b2da7",
        "TransitGatewayId": "tgw-07a5946195a67dc47",
        "MiddleboxAttachmentIds":  ["tgw-attach-0123456789abcdef0",
        "tgw-attach-0123456789abcdef1"],
        "State": "modifying",
        "UpdateEffectiveAt": "2025-11-05T21:00:00.000Z"
    }
}
```

Perubahan dapat memakan waktu hingga dua jam penagihan untuk diterapkan.

Menghapus kebijakan pengukuran AWS Transit Gateway

Hapus kebijakan pengukuran saat tidak lagi diperlukan untuk strategi alokasi biaya gateway transit Anda. Menghapus kebijakan mengembalikan alokasi biaya ke model berbasis pengirim default di mana biaya pemrosesan data dan transfer data dialokasikan ke akun yang memiliki lampiran sumber. Semua entri kebijakan yang terkait dengan kebijakan pengukuran yang dihapus juga akan dihapus.

Menghapus kebijakan pengukuran menggunakan konsol

Gunakan konsol untuk menghapus kebijakan pengukuran yang tidak lagi diperlukan.

Untuk menghapus kebijakan pengukuran menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Kebijakan pengukuran.
3. Pilih kebijakan yang ingin Anda hapus dengan memilih ID kebijakannya.
4. Pilih Tindakan, lalu Hapus.
5. Konfirmasikan penghapusan dengan mengetikkan **`delete`** dialog konfirmasi.
6. Pilih Hapus.

> **Important**
>
> Menghapus kebijakan pengukuran tidak dapat diubah. Semua entri kebijakan dan pengaturan konfigurasi akan dihapus secara permanen, dan alokasi biaya akan kembali ke model berbasis pengirim default.

Menghapus kebijakan pengukuran menggunakan AWS CLI

Gunakan delete-transit-gateway-metering-policy perintah untuk menghapus kebijakan pengukuran secara terprogram.

Persyaratan:

- Izin pemilik gateway transit

Parameter yang diperlukan:

- `--transit-gateway-metering-policy-id`- ID kebijakan pengukuran yang akan dihapus

Untuk melihat dan menghapus kebijakan pengukuran menggunakan CLI AWS

1. (Opsional) Lihat kebijakan pengukuran yang ada menggunakan describe-transit-gateway-metering-policies perintah untuk melihat pengaturan konfigurasi saat ini:

   ```
   aws ec2 describe-transit-gateway-metering-policies
   ```

   Perintah ini mengembalikan semua kebijakan pengukuran di akun Anda, menunjukkan status dan konfigurasinya saat ini.
2. Menghapus kebijakan pengukuran menggunakan delete-transit-gateway-metering-policy perintah untuk menghapus kebijakan secara permanen:

   ```
   aws ec2 delete-transit-gateway-metering-policy \
       --transit-gateway-metering-policy-id tgw-mp-042d444564d4b2da7
   ```

   Perintah ini secara permanen menghapus kebijakan pengukuran yang ditentukan dan semua entri terkait. Alokasi biaya akan kembali ke model berbasis pengirim default untuk semua arus lalu lintas future. Perubahan ini juga membutuhkan waktu 2 jam penagihan untuk diterapkan.

3. Perintah mengembalikan output berikut ketika kebijakan berhasil dihapus:

```
{
    "TransitGatewayMeteringPolicy": {
        "TransitGatewayMeteringPolicyId": "tgw-mp-042d444564d4b2da7",
        "TransitGatewayId": "tgw-07a5946195a67dc47",
        "MiddleboxAttachmentIds":  ["tgw-attach-0123456789abcdef0",
        "tgw-attach-0123456789abcdef1"],
        "State": "deleting",
        "UpdateEffectiveAt": "2025-11-05T21:00:00.000Z"
    }
}
```

Respons mengonfirmasi bahwa kebijakan sedang dihapus dengan `deleting` status saat penghapusan diproses di seluruh infrastruktur gateway transit.

Buat sebuah AWS Entri kebijakan pengukuran Transit Gateway

Secara default, semua aliran diukur ke pemilik lampiran sumber. Untuk mengukur aliran tertentu ke akun yang berbeda, buat entri kebijakan individual yang menentukan akun mana yang dikenakan biaya berdasarkan properti arus lalu lintas.

Entri kebijakan pengukuran berfungsi sebagai aturan bersyarat yang dievaluasi secara berurutan berdasarkan nomor aturannya saat lalu lintas mengalir melalui gateway transit Anda. Setiap entri bertindak sebagai pernyataan “jika-maka”: jika lalu lintas cocok dengan kriteria yang ditentukan (seperti jenis lampiran sumber, blok CIDR tujuan, atau protokol), maka bebankan biaya pada akun yang ditunjuk. Sistem mengevaluasi entri dari nomor aturan terendah ke tertinggi, dan entri pencocokan pertama menentukan akun penagihan untuk arus lalu lintas tersebut.

Entri mendukung berbagai kriteria pencocokan termasuk jenis lampiran (VPC, VPN, Client VPN, Direct Connect Gateway, Peering, Network Function, dan VPN Concentrator), ID lampiran spesifik, blok CIDR sumber dan tujuan, jenis protokol, dan rentang port. Anda dapat menggabungkan beberapa kriteria dalam satu entri untuk membuat aturan penargetan yang tepat. Misalnya, Anda dapat membuat entri yang cocok dengan semua lalu lintas HTTPS (port 443) dari lampiran VPC ke rentang CIDR tujuan tertentu dan membebankan biaya aliran tersebut ke akun tim keamanan. Jika tidak ada entri yang cocok dengan arus lalu lintas tertentu, akun terukur default yang ditentukan dalam kebijakan pengukuran induk akan dikenakan biaya, memastikan semua lalu lintas ditagih dengan benar. Membuat entri membutuhkan waktu 2 jam penagihan untuk diterapkan.

> **Important**
>
> - Rencanakan nomor aturan dengan hati-hati - Tinggalkan celah (mis., 10, 20, 30) untuk memungkinkan penyisipan masa depan
> - Uji entri dengan kondisi yang kurang spesifik terlebih dahulu sebelum menambahkan aturan yang lebih ketat
> - Gunakan kondisi pencocokan tertentu untuk menghindari penagihan yang tidak diinginkan

Membuat entri kebijakan pengukuran menggunakan konsol

Kebijakan pengukuran menentukan perilaku alokasi biaya default dan pengaturan global untuk gateway transit Anda.

Untuk membuat entri kebijakan pengukuran menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Kebijakan pengukuran.
3. Pilih tautan ID kebijakan pengukuran untuk melihat detailnya.
4. Pilih tab Entri kebijakan pengukuran.
5. Pilih Buat entri kebijakan pengukuran.
6. Nomor aturan kebijakan -Ini harus berupa nomor unik (1- 32.766) yang menentukan urutan evaluasi. Angka yang lebih rendah memiliki prioritas yang lebih tinggi.
7. Akun terukur - Pilih salah satu jenis akun berikut yang akan dikenakan biaya untuk pencocokan arus lalu lintas:
   a. Pemilik Lampiran Sumber
   b. Pemilik Lampiran Tujuan
   c. Pemilik Lampiran Transit Gateway
8. (Opsional) Pilih Ketentuan aturan - Kondisi opsional ini menentukan kriteria untuk mencocokkan lalu lintas tertentu:
   - Jenis lampiran sumber atau ID - Filter berdasarkan jenis lampiran (VPC, VPN, Client VPN, Direct Connect Gateway, Peering, Network Function, dan VPN Concentrator) atau ID.
   - Jenis lampiran tujuan atau ID - Filter berdasarkan jenis lampiran tujuan atau ID

- Blok CIDR Sumber - Cocokkan lalu lintas dari rentang IP tertentu
- Blok CIDR tujuan - Cocokkan lalu lintas dengan rentang IP tertentu
- Rentang port sumber - Cocokkan port sumber tertentu
- Rentang port tujuan - Cocokkan port tujuan tertentu
- Protokol - Filter berdasarkan protokol untuk aturan (1, 6, 17, dll.)

9. Pilih Buat entri kebijakan pengukuran untuk menyimpan konfigurasi.

Buat entri kebijakan pengukuran menggunakan AWS CLI

Entri kebijakan menentukan aturan khusus untuk alokasi biaya berdasarkan karakteristik lalu lintas. Aturan dievaluasi secara berurutan dari nomor aturan terendah hingga tertinggi.

Parameter yang diperlukan:

- `--transit-gateway-metering-policy-id`- ID kebijakan pengukuran untuk menambahkan entri ke
- `--policy-rule-number`- Nomor unik (1-32.766) yang menentukan urutan evaluasi
- `--metered-account`- Jenis pembayar (sumber-lampiran-pemilik/tujuan-lampiran-pemilik /transit-gateway-pemilik)

Parameter opsional:

Parameter opsional ini yang menentukan kriteria agar sesuai dengan lalu lintas tertentu:

- `--source-transit-gateway-attachment-id`- ID lampiran gateway transit sumber.
- `--source-transit-gateway-attachment-type`- Jenis lampiran gateway transit sumber.
- `--source-cidr-block`- Blok CIDR sumber untuk aturan.
- `--source-port-range`- Rentang port sumber untuk aturan.
- `--destination-transit-gateway-attachment-id`- ID lampiran gateway transit tujuan.
- `--destination-transit-gateway-attachment-type`- Jenis lampiran gateway transit tujuan.
- `--destination-cidr-block`- Blok CIDR tujuan untuk aturan.
- `--destination-port-range`- Rentang port tujuan untuk aturan.
- `--protocol`- Nomor protokol untuk aturan

Untuk membuat entri kebijakan pengukuran menggunakan AWS CLI

1. Gunakan create-transit-gateway-metering-policy-entry perintah untuk membuat entri kebijakan baru yang merutekan lalu lintas VPC ke akun terukur tertentu:

```
aws ec2 create-transit-gateway-metering-policy-entry \
    --transit-gateway-metering-policy-id tgw-mp-042d444564d4b2da7 \
    --policy-rule-number 100 \
    --destination-transit-gateway-attachment-type vpc \
    --metered-account destination-attachment-owner
```

   Perintah ini membuat entri kebijakan dengan nomor aturan 100 yang cocok dengan lalu lintas yang ditujukan untuk lampiran VPC dan menagih pemilik lampiran tujuan untuk alur tersebut.

2. Perintah mengembalikan output berikut ketika entri berhasil dibuat:

```
{
    "TransitGatewayMeteringPolicyEntry": {
        "MeteredAccount": "destination-attachment-owner",
        "MeteringPolicyRule": {
            "DestinationTransitGatewayAttachmentType": "vpc"
        },
        "PolicyRuleNumber": 100,
        "State": "available",
        "UpdateEffectiveAt": "2025-11-06T02:00:00.000Z"
    }
}
```

   Respons mengonfirmasi entri dibuat dengan status “tersedia” saat sedang diaktifkan di seluruh infrastruktur gateway transit.

Menghapus entri kebijakan pengukuran AWS Transit Gateway

Hapus entri kebijakan pengukuran ketika aturan alokasi biaya tertentu tidak lagi diperlukan untuk arus lalu lintas jaringan Anda. Penghapusan entri membantu menyederhanakan manajemen kebijakan dengan menghapus aturan yang sudah ketinggalan zaman atau tidak perlu sambil mempertahankan struktur kebijakan secara keseluruhan. Saat Anda menghapus entri, lalu lintas yang sebelumnya cocok dengan aturan yang dihapus akan dievaluasi terhadap entri yang tersisa dalam urutan nomor aturan, atau kembali ke perilaku kebijakan default jika tidak ada entri lain yang cocok.

Sebelum menghapus entri, pertimbangkan dampaknya pada pengaturan penagihan saat ini dan arus lalu lintas. Setelah dihapus, perubahan membutuhkan waktu hingga 2 jam penagihan untuk menjadi efektif dan tidak dapat dibatalkan, jadi koordinasikan perubahan dengan pemilik akun dan tim keuangan yang terpengaruh. Tinjau entri yang tersisa untuk memastikan cakupan lalu lintas yang tepat dan alokasi penagihan setelah penghapusan. Urutan evaluasi aturan untuk entri yang tersisa tetap tidak berubah, mempertahankan perilaku alokasi biaya yang dapat diprediksi untuk arus lalu lintas yang berkelanjutan.

⚠ Important

- Penghapusan tidak dapat diubah
- Lalu lintas yang sebelumnya cocok dengan entri ini akan dievaluasi ulang terhadap entri yang tersisa
- Tinjau entri yang tersisa untuk memastikan cakupan lalu lintas yang tepat

Menghapus entri kebijakan pengukuran menggunakan konsol

Gunakan konsol untuk menghapus entri kebijakan melalui antarmuka intuitif yang menyediakan dialog konfirmasi untuk mencegah penghapusan yang tidak disengaja.

Untuk menghapus entri kebijakan menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Kebijakan pengukuran.
3. Pilih kebijakan pengukuran yang berisi entri yang ingin Anda hapus.
4. Pilih entri yang ingin Anda hapus dan pilih Hapus.
5. Dalam dialog konfirmasi, tinjau detail entri dan ketik **`delete`** untuk mengonfirmasi penghapusan.
6. Pilih Hapus untuk menghapus entri secara permanen.

Menghapus entri kebijakan pengukuran menggunakan AWS CLI

Gunakan delete-transit-gateway-metering-policy-entry perintah untuk menghapus entri kebijakan secara terprogram.

Persyaratan:

- Izin pemilik gateway transit
- ID kebijakan pengukuran yang valid dan nomor aturan entri

Parameter yang diperlukan:

- `--transit-gateway-metering-policy-id`- ID kebijakan pengukuran
- `--policy-rule-number`- Nomor aturan entri yang akan dihapus

Untuk melihat dan menghapus entri kebijakan menggunakan CLI AWS

1. (Opsional) Lihat entri kebijakan yang ada menggunakan get-transit-gateway-metering-policy-entries perintah untuk melihat pengaturan konfigurasi saat ini:

   ```
   aws ec2 get-transit-gateway-metering-policy-entries \
       --transit-gateway-metering-policy-id tgw-mp-0123456789abcdefg
   ```

   Perintah ini mengembalikan semua entri untuk kebijakan yang ditentukan, menampilkan nomor aturan, kriteria yang cocok, dan akun terukur.
2. Hapus entri kebijakan menggunakan delete-transit-gateway-metering-policy-entry perintah untuk menghapus entri secara permanen:

   ```
   aws ec2 delete-transit-gateway-metering-policy-entry \
       --transit-gateway-metering-policy-id tgw-mp-0123456789abcdefg \
       --policy-rule-number 100
   ```

   Perintah ini secara permanen menghapus entri yang ditentukan dari kebijakan. Lalu lintas yang sebelumnya cocok dengan entri ini akan segera dievaluasi ulang terhadap entri yang tersisa atau kembali ke perilaku kebijakan default.
3. Perintah mengembalikan output berikut ketika entri berhasil dihapus:

   ```
   {
       "TransitGatewayMeteringPolicyEntry": [
           {
               "PolicyRuleNumber": 100,
               "MeteredAccount": "destination-attachment-owner",
               "UpdateEffectiveAt": "2024-01-01T01:00:00+00:00",
               "state": "deleted",
               "MeteringPolicyRule": {
   ```

```
                "DestinationTransitGatewayAttachmentType": "vpc"
            }
        }
}
```

Respons mengonfirmasi entri sedang dihapus dengan status “dihapus” saat penghapusan diproses di seluruh infrastruktur gateway transit.

Kelola AWS lampiran middlebox kebijakan pengukuran Transit Gateway

Kebijakan pengukuran gateway transit mendukung lampiran Middlebox yang memungkinkan Anda mengalokasikan biaya pemrosesan data secara fleksibel untuk lalu lintas jaringan yang dirutekan melalui peralatan middlebox seperti firewall jaringan dan penyeimbang beban. Contoh lampiran middlebox adalah lampiran Fungsi Jaringan ke AWS Network Firewall atau lampiran VPC yang merutekan lalu lintas ke peralatan keamanan pihak ketiga dalam VPC. Lalu lintas antara lampiran gateway transit sumber dan tujuan melintasi lampiran middlebox ini untuk kasus penggunaan pemeriksaan keamanan yang khas. Anda dapat menentukan kebijakan pengukuran untuk mengalokasikan penggunaan pemrosesan data secara fleksibel pada lampiran middlebox ke lampiran sumber asli, lampiran tujuan akhir, atau pemilik akun gateway transit. Untuk lampiran Fungsi Jaringan, biaya pemrosesan data AWS Network Firewall juga dialokasikan ke akun terukur.

Lampiran gateway transit yang ditunjuk yang merutekan lalu lintas melalui peralatan jaringan untuk pemeriksaan keamanan, penyeimbangan beban, atau fungsi jaringan lainnya. Penggunaan data untuk lampiran middlebox yang melintasi lalu lintas diukur ke pemilik akun yang ditentukan dalam kebijakan pengukuran. Anda dapat menentukan maksimal 10 lampiran middlebox. Jenis lampiran middlebox yang didukung adalah Network Function (AWS Network Firewall), lampiran VPC dan VPN.

Topik

- Tambahkan lampiran middlebox kebijakan pengukuran AWS Transit Gateway
- Hapus AWS lampiran middlebox kebijakan pengukuran Transit Gateway

Tambahkan lampiran middlebox kebijakan pengukuran AWS Transit Gateway

Anda dapat menambahkan lampiran middlebox untuk mengintegrasikan peralatan jaringan ke dalam kebijakan pengukuran Transit Gateway Anda. Ini memungkinkan Anda untuk merutekan lalu lintas tertentu melalui peralatan keamanan, penyeimbang beban, atau fungsi jaringan lainnya sambil mempertahankan kontrol alokasi biaya granular.

Important

- Pastikan peralatan middlebox dikonfigurasi dan dapat diakses dengan benar
- Uji perutean lalu lintas sebelum mendaftar ke beban kerja produksi
- Pantau kinerja middlebox untuk menghindari pengenalan latensi
- Konfigurasikan perilaku failover yang sesuai untuk ketersediaan tinggi

Tambahkan lampiran middlebox menggunakan konsol

Untuk menambahkan entri lampiran middlebox

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Kebijakan pengukuran.
3. Pilih tautan ID kebijakan pengukuran untuk melihat detailnya.
4. Pilih tab lampiran Middlebox.
5. Pilih Tambahkan.
6. Saat diminta, Pilih lampiran middlebox IDs yang harus diperlakukan sebagai middlebox untuk penagihan khusus. Anda dapat memilih hingga 10 lampiran middlebox.
7. Pilih Tambahkan lampiran middlebox untuk menyimpan konfigurasi.

Tambahkan lampiran middlebox menggunakan AWS CLI

Gunakan modify-transit-gateway-metering-policy perintah untuk menambahkan lampiran.

Sebelum Anda mulai, pastikan Anda memiliki parameter yang diperlukan berikut:

- `--transit-gateway-metering-policy-id`- ID kebijakan pengukuran yang ada
- `--add-middle-box-attachment-ids`- Satu atau lebih lampiran IDs untuk ditambahkan ke kebijakan (untuk menambahkan lampiran)

Untuk menambahkan lampiran middlebox ke kebijakan yang ada menggunakan CLI AWS

1. Dalam contoh berikut, modify-transit-gateway-metering-policy digunakan untuk menambahkan empat lampiran middlebox ke kebijakan pengukuran yang ada. Perintah menambahkan lampiran yang ditentukan IDs ke daftar yang ada tanpa menghapus lampiran saat ini:

```
aws ec2 modify-transit-gateway-metering-policy \
    --transit-gateway-metering-policy-id tgw-mp-0123456789abcdefg \
    --add-middle-box-attachment-ids tgw-attach-0bdc681c211bf71f3 tgw-
attach-0987654321fedcba0 tgw-attach-0456789012345abcd tgw-attach-0fedcba0987654321
```

2. Dalam contoh respons berikut, keluaran JSON menunjukkan konfigurasi kebijakan yang diperbarui dengan keempat lampiran middlebox yang sekarang disertakan:

```
{
    "TransitGatewayMeteringPolicy": {
        "TransitGatewayMeteringPolicyId": "tgw-mp-0123456789abcdefg",
        "TransitGatewayId": "tgw-0ecec6433f4bfe55a",
        "MiddleBoxAttachmentIds": [
            "tgw-attach-0bdc681c211bf71f3",
            "tgw-attach-0987654321fedcba0",
            "tgw-attach-0456789012345abcd",
            "tgw-attach-0fedcba0987654321"
        ],
        "State": "available",
        "UpdateEffectiveAt": "2024-09-05T16:00:00.000Z"
    }
}
```

Hapus AWS lampiran middlebox kebijakan pengukuran Transit Gateway

Secara default, biaya pengukuran dikaitkan dengan pemilik lampiran middlebox. Namun, Anda dapat memodifikasi tugas ini untuk memastikan biaya dialokasikan dengan benar ke sumber atau tujuan lalu lintas yang sebenarnya. Anda dapat menambah atau menghapus hingga 10 lampiran middlebox total untuk kebijakan pengukuran.

Hapus lampiran middlebox menggunakan konsol

Gunakan konsol Amazon VPC untuk menghapus lampiran middlebox dari konfigurasi kebijakan pengukuran Anda.

Untuk menghapus lampiran middlebox

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Gateway transit, Kebijakan pengukuran.

3. Pilih kebijakan pengukuran yang ingin Anda ubah.
4. Pilih tab lampiran Middlebox.
5. Pilih hingga 10 lampiran middlebox untuk dihapus dari kebijakan pengukuran.
6. Pilih Hapus.
7. Saat diminta, Anda dapat memperbarui lampiran middlebox yang Anda pilih untuk dihapus. Lalu lintas melalui lampiran yang dihapus akan diukur ke pemilik lampiran middlebox.
8. Pilih Hapus lampiran middlebox.

Hapus lampiran middlebox menggunakan AWS CLI

Gunakan modify-transit-gateway-metering-policy perintah untuk menghapus lampiran.

Sebelum Anda mulai, pastikan Anda memiliki parameter yang diperlukan berikut:

- `--transit-gateway-metering-policy-id`- ID kebijakan pengukuran yang ada
- `--remove-middle-box-attachment-ids`- Satu atau lebih lampiran IDs untuk dihapus dari kebijakan (untuk menghapus lampiran)

Untuk menghapus lampiran middlebox dari kebijakan yang ada menggunakan CLI AWS

1. Dalam contoh berikut, modify-transit-gateway-metering-policy digunakan untuk menghapus dua lampiran middlebox tertentu dari kebijakan pengukuran yang ada. Perintah hanya menghapus lampiran yang ditentukan IDs sambil mempertahankan lampiran yang tersisa:

```
aws ec2 modify-transit-gateway-metering-policy \
    --transit-gateway-metering-policy-id tgw-mp-0123456789abcdefg \
    --remove-middle-box-attachment-ids tgw-attach-0456789012345abcd tgw-
attach-0fedcba0987654321
```

2. Dalam contoh respons berikut, keluaran JSON menunjukkan konfigurasi kebijakan yang diperbarui dengan lampiran yang ditentukan dihapus dan lampiran yang tersisa masih aktif:

```
{
    "TransitGatewayMeteringPolicy": {
        "TransitGatewayMeteringPolicyId": "tgw-mp-0123456789abcdefg",
        "TransitGatewayId": "tgw-0ecec6433f4bfe55a",
        "MiddleBoxAttachmentIds": [
            "tgw-attach-0bdc681c211bf71f3",
```

```
            "tgw-attach-0987654321fedcba0"
        ],
        "State": "available",
        "UpdateEffectiveAt": "2024-09-05T16:00:00.000Z"
    }
}
```

AWS Log Aliran Transit Gateway

Transit Gateway Flow Logs adalah fitur AWS Transit Gateway yang memungkinkan Anda menangkap informasi tentang lalu lintas IP yang menuju dan dari gateway transit Anda. Data log aliran dapat dipublikasikan ke Amazon CloudWatch Logs, Amazon S3, atau Firehose. Setelah membuat log alur, Anda dapat mengambil dan melihat datanya di tujuan yang dipilih. 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. Log Aliran Transit Gateway menangkap informasi yang hanya terkait dengan gateway transit, yang dijelaskan dalam. the section called “Catatan Log Aliran Transit Gateway” Jika Anda ingin menangkap informasi tentang lalu lintas IP yang pergi ke dan dari antarmuka jaringan di VPC Anda, gunakan VPC Flow Logs. Lihat Mencatat lalu lintas IP menggunakan Log Aliran VPC di Panduan Pengguna Amazon VPC untuk informasi selengkapnya.

> **Note**
>
> Untuk membuat log aliran gateway transit, Anda harus menjadi pemilik gateway transit. Jika Anda bukan pemiliknya, pemilik gateway transit harus memberi Anda izin.

Data log aliran untuk gateway transit yang dipantau dicatat sebagai catatan log aliran, yang merupakan peristiwa log yang terdiri dari bidang yang menggambarkan arus lalu lintas. Untuk informasi selengkapnya, lihat Catatan Log Aliran Transit Gateway.

Untuk membuat log alur, Anda menentukan:

- Sumber daya untuk membuat log alur
- Tujuan publikasi data log alur Anda

Setelah Anda membuat log alur, dibutuhkan beberapa menit untuk mulai mengumpulkan dan menerbitkan data ke tujuan yang dipilih. Log aliran tidak menangkap aliran log waktu nyata untuk gateway transit Anda.

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, dan tidak ada catatan log aliran baru yang dibuat atau dipublikasikan ke CloudWatch Log atau Amazon S3. Menghapus log aliran tidak menghapus catatan log aliran yang ada atau aliran log (untuk CloudWatch Log) atau objek file log (untuk Amazon S3) untuk gateway transit. Untuk menghapus aliran log yang ada, gunakan konsol CloudWatch Log. Untuk menghapus objek file berkas log yang ada, gunakan konsol Amazon S3. Setelah Anda menghapus log alur, perlu beberapa menit untuk menghentikan pengumpulan data. Untuk informasi selengkapnya, lihat Menghapus catatan Log Aliran AWS Transit Gateway.

Anda dapat membuat log aliran untuk gateway transit yang dapat mempublikasikan data ke CloudWatch Log, Amazon S3, atau Amazon Data Firehose. Untuk informasi selengkapnya, lihat berikut ini:

- Membuat Log Aliran yang memublikasikan ke CloudWatch Log
- Buat Log Aliran yang diterbitkan ke Amazon S3
- Membuat Log Aliran yang dipublikasikan ke Firehose

Batasan

Batasan berikut berlaku untuk Log Aliran Transit Gateway:

- Lalu lintas multicast tidak didukung.
- Lampiran Connect tidak didukung. Semua log aliran Connect muncul di bawah lampiran transport dan karenanya harus diaktifkan pada gateway transit atau lampiran Connect transport.
- Log Aliran Transit Gateway mendukung maksimum 250 langganan per sumber daya per akun. Untuk membuat langganan tambahan pada sumber daya yang telah mencapai batas ini, Anda harus terlebih dahulu menghapus langganan yang ada.

Catatan Log Aliran Transit Gateway

Catatan log aliran mewakili aliran jaringan di gateway transit Anda. Setiap catatan adalah string dengan bidang yang dipisahkan oleh spasi. Catatan mencakup nilai untuk berbagai komponen arus lalu lintas, 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

Format default

Dengan format default, catatan log aliran mencakup semua bidang versi 2 hingga versi 6, dalam urutan yang ditunjukkan pada tabel bidang yang tersedia. Anda tidak dapat menyesuaikan atau mengubah format default. Untuk menangkap bidang tambahan atau subset bidang yang berbeda, tentukan format kustom sebagai gantinya.

Format kustom

Dengan format kustom, Anda menentukan bidang yang disertakan dalam catatan log alur dan urutannya. Hal ini memungkinkan Anda untuk membuat flow log yang khusus 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 aliran gateway transit. Kolom Versi menunjukkan versi bidang mana yang diperkenalkan.

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	Menunjukkan versi di mana bidang diperkenalkan. Format default mencakup 2 bidang semua versi, dalam urutan yang sama sebagaimana yang tercantum di tabel. Tipe data parket: INT_32	2
resource-type	Jenis sumber daya tempat langganan dibuat. Untuk Log Aliran Transit Gateway, ini akan terjadiTransitGateway. Jenis data parket: STRING	6
account-id	Akun AWS ID pemilik gateway transit sumber. Jenis data parket: STRING	2
tgw-id	ID gateway transit tempat lalu lintas direkam. Jenis data parket: STRING	6
tgw-attachment-id	ID lampiran gateway transit tempat lalu lintas direkam. Jenis data parket: STRING	6
tgw-src-vpc-account-id	Akun AWS ID untuk lalu lintas sumber VPC. Jenis data parket: STRING	6
tgw-dst-vpc-account-id	Akun AWS ID untuk lalu lintas VPC tujuan. Jenis data parket: STRING	6
tgw-src-vpc-id	ID VPC sumber untuk gateway transit Jenis data parket: STRING	6
tgw-dst-vpc-id	ID VPC tujuan untuk gateway transit. Jenis data parket: STRING	6
tgw-src-subnet-id	ID subnet untuk lalu lintas sumber gateway transit.	6

Bidang	Deskripsi	Versi
	Jenis data parket: STRING	
tgw-dst-subnet-id	ID subnet untuk lalu lintas tujuan gateway transit. Jenis data parket: STRING	6
tgw-src-eni	ID lampiran gateway transit sumber ENI untuk aliran. Jenis data parket: STRING	6
tgw-dst-eni	ID lampiran gateway transit tujuan ENI untuk aliran. Jenis data parket: STRING	6
tgw-src-az-id	ID Availability Zone yang berisi gateway transit sumber yang lalu lintasnya direkam. Jika lalu lintas berasal dari sublokasi, catatan akan menampilkan simbol '-' untuk bidang ini. Jenis data parket: STRING	6
tgw-dst-az-id	ID Availability Zone yang berisi gateway transit tujuan yang lalu lintas dicatat. Jenis data parket: STRING	6
tgw-pair-attachment-id	Bergantung pada arah aliran, ini adalah ID lampiran keluar atau masuknya aliran. Jenis data parket: STRING	6
srcaddr	Alamat sumber untuk lalu lintas masuk. Jenis data parket: STRING	2
dstaddr	Alamat tujuan untuk lalu lintas keluar. Jenis data parket: STRING	2

Bidang	Deskripsi	Versi
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 dikirim atau diterima pada gateway transit. 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 dikirim atau diterima pada gateway transit. Tipe data parket: INT_64	2

Bidang	Deskripsi	Versi
log-status	Status log aliran: • OK — Data masuk secara normal ke tujuan yang dipilih. • NODATA — Tidak ada lalu lintas jaringan ke atau dari antarmuka jaringan selama interval agregasi. • SKIPDATA — Beberapa catatan log aliran dilewati selama interval agregasi. Ini mungkin karena kendala kapasitas internal, atau kesalahan internal. Jenis data parket: STRING	2
type	Jenis lalu lintas. Nilai yang mungkin adalah IPv4 | IPv6 | EFA. Untuk informasi selengkapnya, lihat Adaptor Kain Elastis di Panduan Pengguna Amazon EC2. Jenis data parket: STRING	3
packets-lost-no-route	Paket hilang karena tidak ada rute yang ditentukan. Tipe data parket: INT_64	6
packets-lost-blackhole	Paket hilang karena lubang hitam. Tipe data parket: INT_64	6
packets-lost-mtu-exceeded	Paket hilang karena ukurannya melebihi MTU. Tipe data parket: INT_64	6
packets-lost-ttl-expired	Paket hilang karena berakhirnya time-to-live. Tipe data parket: INT_64	6

Bidang	Deskripsi	Versi
tcp-flags	Nilai bitmask untuk bendera TCP berikut: • FIN — 1 • SYN — 2 • RST — 4 • PSH — 8 • ACK — 16 • SYN-ACK — 18 • URG — 32 **Important** Ketika entri log aliran hanya terdiri dari paket ACK, nilai flag adalah 0, bukan 16. Untuk informasi umum tentang bendera TCP (seperti arti bendera seperti FIN, SYN, dan ACK), lihat Struktur segmen TCP di Wikipedia. Bendera TCP dapat OR-ed selama interval agregasi. Untuk koneksi singkat, bendera mungkin ditetapkan pada baris yang sama dalam catatan log aliran, misalnya, 19 untuk SYN-ACK dan FIN, dan 3 untuk SYN dan FIN. Tipe data parket: INT_32	3
region	Wilayah yang berisi gateway transit tempat lalu lintas dicatat. Jenis data parket: STRING	4
flow-direction	Arah aliran sehubungan dengan gateway transit. Kemungkinan nilai adalah: ingress | egress. Jenis data parket: STRING	5

Bidang	Deskripsi	Versi
pkt-src-aws-service	Nama subset alamat IP berkisar srcaddr jika alamat IP sumber adalah untuk AWS layanan. 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_H EALTHCHECKS ROUTE53_HEALTHCHECKS_PUBLISHING | ROUTE53_RESOLVER | S3 | | WORKSPACES_GATEWAYS Jenis data parket: STRING	5
pkt-dst-aws-service	Nama subset alamat IP berkisar untuk 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

Mengontrol penggunaan log alur

Secara default, pengguna tidak memiliki izin untuk bekerja dengan log aliran. Anda dapat membuat kebijakan pengguna yang memberi pengguna izin untuk membuat, mendeskripsikan, dan menghapus log aliran. Untuk informasi selengkapnya, lihat Pemberian Izin Pengguna IAM yang Diperlukan untuk Sumber Daya Amazon EC2 dalam Referensi API Amazon EC2.

Berikut ini adalah contoh kebijakan yang memberikan izin penuh kepada pengguna untuk membuat, menjelaskan, dan menghapus log alur.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteFlowLogs",
```

```
        "ec2:CreateFlowLogs",
        "ec2:DescribeFlowLogs"
      ],
      "Resource": "*"
    }
  ]
}
```

Beberapa konfigurasi peran dan izin IAM tambahan diperlukan, tergantung apakah Anda memublikasikan ke CloudWatch Log atau Amazon S3. Untuk informasi selengkapnya, lihat AWS Catatan Log Aliran Transit Gateway di CloudWatch Log Amazon dan AWS Catatan Log Aliran Transit Gateway di Amazon S3.

Harga Log Aliran Transit Gateway

Biaya konsumsi data dan penyimpanan untuk log vended berlaku saat Anda mempublikasikan log aliran gateway transit. Untuk informasi selengkapnya tentang harga saat menerbitkan log terjual, buka CloudWatch Harga Amazon, lalu di bawah Tingkat berbayar, pilih Log dan temukan Log Terjual.

Membuat atau memperbarui peran IAM untuk Log Aliran AWS Transit Gateway

Anda dapat memperbarui peran yang ada atau menggunakan prosedur berikut untuk membuat peran baru untuk digunakan dengan log aliran menggunakan AWS Identity and Access Management konsol.

Untuk membuat IAM role untuk log alur

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Dalam panel navigasi, pilih Roles (Peran), lalu Create role (Buat peran).
3. Untuk Pilih tipe entitas tepercaya, pilih Layanan AWS . Untuk Kasus penggunaan, pilih EC2. Pilih Berikutnya.
4. Pada halaman Tambahkan izin, pilih Berikutnya: Tag dan tambahkan tag secara opsional. Pilih Berikutnya.
5. Pada Nama, tinjau, dan buat halaman masukkan nama untuk peran Anda dan berikan Deskripsi secara opsional. Pilih Buat peran.

6. Pilih nama peran Anda. Untuk Menambahkan izin, pilih Buat kebijakan sebaris, lalu pilih tab JSON.
7. Salin kebijakan pertama dari Peran IAM untuk menerbitkan log alur ke CloudWatch Log dan tempel di window. Pilih Tinjau kebijakan.
8. Masukkan nama untuk kebijakan Anda dan pilih Buat kebijakan.
9. Pilih nama peran Anda. Untuk Hubungan kepercayaan, pilih Edit hubungan kepercayaan. Dalam dokumen kebijakan yang ada, ubah layanan dari `ec2.amazonaws.com` ke `vpc-flow-logs.amazonaws.com`. Pilih Perbarui Kebijakan Kepercayaan.
10. Pada halaman Ringkasan, perhatikan ARN untuk peran Anda. Anda perlu ARN ini ketika Anda membuat log alur Anda.

AWS Catatan Log Aliran Transit Gateway di CloudWatch Log Amazon

Log aliran dapat mempublikasikan data log aliran langsung ke Amazon CloudWatch.

Saat dipublikasikan ke CloudWatch Log, data log aliran dipublikasikan ke grup log, dan setiap gateway transit 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 gateway transit yang sama hadir dalam satu atau lebih log aliran dalam grup log yang sama, ia memiliki satu aliran 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.

Biaya konsumsi data dan arsip untuk log penjual berlaku saat Anda mempublikasikan log aliran ke Log. CloudWatch Untuk informasi selengkapnya, lihat CloudWatch Harga Amazon.

Di CloudWatch Log, bidang stempel waktu sesuai dengan waktu mulai yang ditangkap dalam catatan log aliran. Bidang IngestionTime menyediakan tanggal dan waktu ketika catatan log aliran diterima oleh Log. CloudWatch Stempel waktu lebih lambat dari waktu akhir yang ditangkap dalam catatan log aliran.

Untuk informasi selengkapnya tentang CloudWatch Log, lihat Log yang dikirim ke CloudWatch Log di Panduan Pengguna CloudWatch Log Amazon.

Daftar Isi

- Izin bagi pengguna IAM untuk meneruskan peran
- Membuat catatan Log Aliran AWS Transit Gateway yang diterbitkan ke Amazon CloudWatch Logs
- Lihat catatan Log Aliran AWS Transit Gateway di Amazon CloudWatch
- Memproses catatan Log Aliran AWS Transit Gateway di CloudWatch Log Amazon

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 Anda Akun AWS.

Kebijakan IAM yang dilampirkan ke IAM role Anda harus menyertakan setidaknya izin berikut.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource": "*"
    }
  ]
}
```

Juga memastikan bahwa peran Anda memiliki hubungan kepercayaan yang memungkinkan layanan log alur untuk menjalankan peran.

JSON

```
{
```

```
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Kami menyarankan Anda menggunakan kunci syarat `aws:SourceAccount` dan `aws:SourceArn` untuk melindungi diri Anda dari masalah wakil yang membingungkan. Misalnya, Anda dapat menambahkan blok kondisi berikut ke kebijakan kepercayaan sebelumnya. Akun sumber adalah pemilik log aliran dan sumber ARN adalah ARN log aliran. Jika Anda tidak mengetahui ID log alur, Anda dapat mengganti bagian ARN tersebut dengan wildcard (*) dan kemudian memperbarui kebijakan setelah Anda membuat log alur.

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:region:account_id:vpc-flow-log/flow-log-id"
    }
}
```

Izin bagi pengguna IAM untuk meneruskan peran

Pengguna juga harus memiliki izin untuk menggunakan tindakan `iam:PassRole` untuk IAM role yang terkait dengan log alur.

JSON

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

```
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/flow-log-role-name"
        }
    ]
}
```

Membuat catatan Log Aliran AWS Transit Gateway yang diterbitkan ke Amazon CloudWatch Logs

Anda dapat membuat log aliran untuk gateway transit. Jika Anda melakukan langkah-langkah ini sebagai pengguna IAM, pastikan bahwa Anda memiliki izin untuk menggunakan Tindakan `iam:PassRole`. Untuk informasi selengkapnya, lihat Izin bagi pengguna IAM untuk meneruskan peran.

Anda dapat membuat log CloudWatch aliran Amazon menggunakan Konsol VPC Amazon atau CLI AWS .

Untuk membuat log aliran gateway transit menggunakan konsol

1. Masuk ke Konsol Manajemen AWS dan buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Gateway transit.
3. Pilih kotak centang untuk satu atau beberapa gateway transit dan pilih Tindakan, Buat log alur.
4. Untuk Tujuan, pilih Kirim ke CloudWatch Log.
5. Untuk grup log Tujuan, pilih nama grup log tujuan saat ini.

   > **Note**
   >
   > Jika grup log tujuan belum ada, memasukkan nama baru di bidang ini akan membuat grup log tujuan baru.

6. Untuk peran IAM, tentukan nama peran yang memiliki izin untuk menerbitkan log ke CloudWatch Log.
7. 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.

8. (Opsional) Pilih Tambahkan tag baru untuk menerapkan tag ke log alur.
9. Pilih Buat log alur.

Untuk membuat log alur menggunakan baris perintah

Gunakan salah satu perintah berikut ini.

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

AWS CLI Contoh berikut membuat log aliran yang menangkap informasi gateway transit. Log aliran dikirim ke grup log di Log yang disebut`my-flow-logs`, di CloudWatch akun 123456789101, menggunakan peran IAM. `publishFlowLogs`

```
aws ec2 create-flow-logs --resource-type TransitGateway --resource-ids
 tgw-1a2b3c4d --log-group-name my-flow-logs --deliver-logs-permission-arn
 arn:aws:iam::123456789101:role/publishFlowLogs
```

Lihat catatan Log Aliran AWS Transit Gateway di Amazon CloudWatch

Anda dapat melihat catatan log alur menggunakan konsol CloudWatch Log atau konsol Amazon S3, tergantung pada jenis tujuan yang dipilih. Mungkin perlu beberapa menit setelah Anda membuat log alur agar dapat terlihat di konsol.

Untuk melihat catatan log alur yang dipublikasikan ke CloudWatch Log

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, pilih Log, dan pilih grup log yang berisi log alur Anda. Daftar aliran log untuk setiap gateway transit ditampilkan.
3. Pilih aliran log yang berisi ID gateway transit yang ingin Anda lihat catatan log aliran. Lihat informasi yang lebih lengkap di Catatan Log Aliran Transit Gateway.

Memproses catatan Log Aliran AWS Transit Gateway di CloudWatch Log Amazon

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 Membuat metrik dari peristiwa log menggunakan filter di Panduan CloudWatch Pengguna Amazon.

Contoh: Membuat filter CloudWatch metrik dan alarm untuk log aliran

Dalam contoh ini, Anda memiliki log alur untuk `tgw-123abc456bca`. 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 perintah berikut.

```
[version, resource_type, account_id,tgw_id="tgw-123abc456bca”, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr= "10.0.0.1", dstaddr,
 srcport=“80”, dstport, protocol=“6”, packets, bytes,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
```

5. Untuk Pilih data log yang akan diuji, pilih aliran log untuk gateway transit Anda. (Opsional) Untuk melihat baris data log yang cocok dengan pola filter, pilih Pola uji. Saat Anda siap, pilih Berikutnya.
6. Masukkan nama filter, namespace metrik, dan nama metrik. Tetapkan nilai metrik ke**1**. Setelah selesai, pilih Berikutnya dan kemudian pilih Buat filter metrik.
7. Pada panel navigasi, pilih Alarm, Semua alarm.

8. Pilih Buat alarm.
9. Pilih namespace untuk filter metrik yang Anda buat.

   Diperlukan waktu beberapa menit hingga metrik baru ditampilkan di konsol.
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 pun, pilih Greater/Equal dan masukkan **10** untuk ambang batas.
    - Untuk konfigurasi tambahan, Datapoint untuk alarm, biarkan default. **1**
12. Untuk Pemberitahuan, pilih topik SNS yang ada, atau pilih Buat topik baru untuk membuat topik baru. Pilih Berikutnya.
13. Masukkan nama dan deskripsi untuk alarm dan pilih Berikutnya.
14. Setelah selesai mengonfigurasi alarm, pilih Buat alarm.

AWS Catatan Log Aliran Transit Gateway di 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 aliran untuk semua gateway transit yang dipantau dipublikasikan ke serangkaian objek file log yang disimpan di bucket.

Biaya konsumsi data dan arsip diterapkan oleh Amazon CloudWatch untuk log vended saat Anda memublikasikan log aliran ke Amazon S3. Untuk informasi selengkapnya tentang CloudWatch harga untuk log penjual, buka CloudWatchHarga Amazon, pilih Log, lalu temukan Log Terjual.

Untuk membuat bucket Amazon S3 untuk digunakan dengan flow log, lihat Membuat bucket di Panduan Pengguna Amazon S3.

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.

Daftar Isi

Berkas log alur

VPC Flow Logs adalah fitur yang mengumpulkan catatan log aliran, mengkonsolidasikannya ke dalam file log, dan kemudian menerbitkan file log ke bucket Amazon S3 dengan interval 5 menit. Setiap file berkas log berisi catatan log alur untuk lalu lintas IP yang dicatat dalam lima menit sebelumnya.

Ukuran file maksimum untuk berkas log adalah 75 MB. File berkas log mencapai batas ukuran file dalam periode 5 menit, log alur berhenti menambahkan catatan log alur kepadanya. Kemudian menerbitkan log alur ke bucket Amazon S3, dan membuat file berkas log baru.

Di Amazon S3, bidang terakhir yang dimodifikasi untuk file log alur menunjukkan tanggal dan waktu saat file diunggah ke bucket Amazon S3. 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.

Opsi berkas log

Anda dapat secara opsional menentukan opsi berikut.

- Awalan S3 yang kompatibel dengan HIVE - Aktifkan awalan yang kompatibel dengan HIVE alih-alih mengimpor partisi ke alat yang kompatibel dengan HIVE Anda. Sebelum Anda menjalankan kueri, gunakan MSCK REPAIR TABLE perintah.
- Partisi per jam - Jika Anda memiliki volume log yang besar dan biasanya menargetkan kueri ke jam tertentu, Anda bisa mendapatkan hasil yang lebih cepat dan menghemat biaya kueri dengan mempartisi log setiap jam.

Struktur ember S3 file log

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

Secara default, file dikirim ke lokasi berikut.

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

Jika Anda mengaktifkan awalan S3 yang kompatibel dengan HIVE, file akan dikirim ke lokasi berikut.

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/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/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 aliran yang dibuat oleh Akun AWS 123456789012, untuk sumber daya di us-east-1 Wilayah, June 20, 2018 pada at16:20 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
```

Kebijakan IAM untuk prinsipal IAM yang menerbitkan log alur ke Amazon S3

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

JSON

```
{
  "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 baru yang dibuat secara otomatis ini ditambahkan ke kebijakan asli.

Jika tidak, pemilik bucket harus menambahkan kebijakan ini ke bucket, menentukan Akun AWS ID pembuat log aliran, atau pembuatan log alur gagal. Untuk informasi selengkapnya, lihat Kebijakan Bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:us-east-1:123456789012:*"
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": [
                "s3:GetBucketAcl"
            ],
            "Resource": "arn:aws:s3:::bucket_name",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:us-east-1:123456789012:*"
                }
            }
        }
    ]
}
```

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

- Awalan default

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

- Awalan S3 yang kompatibel dengan HIVE

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

Sebagai praktik terbaik, kami menyarankan Anda memberikan izin ini kepada prinsipal layanan pengiriman log, bukan individu Akun AWS ARNs. Ini juga merupakan praktik terbaik untuk menggunakan kunci `aws:SourceAccount` dan `aws:SourceArn` kondisi untuk melindungi dari masalah wakil yang membingungkan. Akun sumber adalah pemilik log aliran dan sumber ARN adalah ARN wildcard (*) dari layanan log.

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). Untuk informasi selengkapnya, lihat Melindungi data menggunakan enkripsi sisi server di Panduan Pengguna Amazon S3.

Dengan SSE-KMS, Anda dapat menggunakan kunci terkelola atau kunci yang AWS dikelola pelanggan. Dengan kunci AWS terkelola, Anda tidak dapat menggunakan pengiriman lintas akun. Log alur dikirim dari akun pengiriman log, sehingga Anda harus memberikan akses untuk pengiriman lintas akun. Untuk memberikan akses lintas akun ke bucket S3 Anda, gunakan kunci terkelola

pelanggan dan tentukan Nama Sumber Daya Amazon (ARN) kunci terkelola pelanggan saat Anda mengaktifkan enkripsi bucket. Untuk informasi selengkapnya, lihat Menentukan enkripsi sisi server dengan AWS KMS di Panduan Pengguna Amazon S3.

Bila Anda menggunakan SSE-KMS dengan kunci terkelola pelanggan, Anda harus menambahkan yang berikut ini ke kebijakan kunci untuk kunci Anda (bukan kebijakan bucket untuk bucket S3 Anda), sehingga VPC Flow Logs dapat menulis ke bucket S3 Anda.

> **Note**
>
> Menggunakan S3 Bucket Keys memungkinkan Anda menghemat biaya permintaan AWS Key Management Service (AWS KMS) dengan mengurangi permintaan Anda ke AWS KMS Encrypt, GenerateDataKey, dan Decrypt operasi melalui penggunaan kunci tingkat ember. Secara desain, permintaan berikutnya yang memanfaatkan kunci tingkat ember ini tidak menghasilkan permintaan AWS KMS API atau memvalidasi akses terhadap kebijakan kunci. AWS KMS

```
{
    "Sid": "Allow Transit Gateway Flow Logs to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "delivery.logs.amazonaws.com"
        ]
    },
   "Action": [
       "kms:Encrypt",
       "kms:Decrypt",
       "kms:ReEncrypt*",
       "kms:GenerateDataKey*",
       "kms:DescribeKey"
    ],
    "Resource": "*"
}
```

Izin file berkas log Amazon S3

Selain kebijakan bucket yang diperlukan, Amazon S3 menggunakan daftar kontrol akses (ACLs) untuk mengelola akses ke file log yang dibuat oleh log alur. Secara default, pemilik bucket memiliki

izin `FULL_CONTROL` pada setiap file berkas log. Pemilik pengiriman log, jika berbeda dari pemilik bucket, tidak memiliki izin. Akun pengiriman log memiliki izin `READ` dan `WRITE`. Untuk informasi selengkapnya, lihat Ringkasan daftar kontrol akses (ACL) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Buat peran akun sumber AWS Transit Gateway Flow Logs untuk Amazon S3

Dari akun sumber, buat peran sumber di AWS Identity and Access Management konsol.

Untuk membuat peran akun sumber

1. Masuk ke Konsol Manajemen AWS dan 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:
    1. PilihJSON.
    2. Ganti isi jendela ini dengan kebijakan izin di awal bagian ini.
    3. Pilih Berikutnya: Tag dan Berikutnya: Tinjau.
    4. Masukkan nama untuk kebijakan Anda dan deskripsi opsional, lalu pilih Buat kebijakan.
5. Di panel navigasi, pilih Peran.
6. Pilih Buat peran.
7. Untuk jenis entitas Tepercaya, pilih Kebijakan kepercayaan khusus. Untuk kebijakan kepercayaan kustom, ganti `"Principal": {},` dengan yang berikut ini, yang menentukan layanan pengiriman log. Pilih Berikutnya.

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

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

Membuat catatan Log Aliran AWS Transit Gateway yang diterbitkan ke Amazon S3

Setelah membuat dan mengonfigurasi bucket Amazon S3, Anda dapat membuat log aliran untuk gateway transit. Anda dapat membuat log aliran Amazon S3 menggunakan Konsol VPC Amazon atau CLI. AWS

Untuk membuat log aliran gateway transit yang diterbitkan ke Amazon S3 menggunakan konsol

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Gateway transit atau Lampiran gateway Transit.
3. Pilih kotak centang untuk satu atau beberapa gateway transit atau lampiran gateway transit.
4. Pilih Tindakan, Buat log alur.
5. Konfigurasikan pengaturan log aliran. Untuk informasi selengkapnya, lihat Untuk mengonfigurasi setelan log alur.

Untuk mengkonfigurasi pengaturan log aliran menggunakan konsol

1. Untuk Tujuan, pilih Kirim ke ember S3.
2. 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.
3. 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.

4. 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.
5. (Opsional) Untuk menggunakan awalan S3 yang kompatibel dengan HIVE, pilih awalan S3 yang kompatibel dengan HIVE, Aktifkan.
6. (Opsional) Untuk mempartisi log aliran Anda per jam, pilih Setiap 1 jam (60 menit).
7. (Opsional) Untuk menambahkan tag ke log aliran, pilih Tambahkan tag baru dan tentukan kunci dan nilai tag.
8. Pilih Buat log alur.

Untuk membuat log alur yang menerbitkan ke Amazon S3 menggunakan alat baris perintah

Gunakan salah satu perintah berikut ini.

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

AWS CLI Contoh berikut membuat log aliran yang menangkap semua lalu lintas gateway transit untuk `tgw-00112233344556677` VPC dan mengirimkan log aliran ke bucket Amazon S3 yang dipanggil. `flow-log-bucket` Parameter `--log-format` menentukan format kustom untuk catatan log alur.

```
aws ec2 create-flow-logs --resource-type TransitGateway --resource-ids
 tgw-00112233344556677 --log-destination-type s3 --log-destination arn:aws:s3:::flow-
log-bucket/my-custom-flow-logs/'
```

Lihat catatan Aliran AWS Transit Gateway di Amazon S3

Untuk melihat catatan log alur yang diterbitkan ke Amazon S3

1. Buka konsol Amazon S3 di. https://console.aws.amazon.com/s3/
2. Untuk Nama bucket, pilih bucket tempat tujuan penerbitan log alur.

3. Untuk Nama, pilih kotak centang di sebelah file log. Di halaman gambaran umum, pilih Unduh.

Catatan Log Aliran AWS Transit Gateway yang Diproses 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.

AWS Transit Gateway, catatan Log Aliran di Amazon Data Firehose

Topik

Log aliran dapat mempublikasikan data log aliran langsung ke Firehose. Anda dapat memilih untuk mempublikasikan log alur ke akun yang sama dengan monitor sumber daya atau ke akun lain.

Prasyarat

Saat memublikasikan ke Firehose, data flow log dipublikasikan ke aliran pengiriman Firehose, dalam format teks biasa. Anda harus terlebih dahulu membuat aliran pengiriman Firehose. Untuk langkah-langkah membuat aliran pengiriman, lihat Membuat Aliran Pengiriman Firehose Data Amazon di Panduan Pengembang Amazon Data Firehose.

Harga

Biaya konsumsi dan pengiriman standar berlaku. Untuk informasi selengkapnya, buka CloudWatch Harga Amazon, pilih Log dan temukan Log Terjual.

Peran IAM untuk pengiriman lintas akun

Saat memublikasikan ke Kinesis 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 aliran ke Firehose, Anda harus membuat peran IAM di akun sumber dan peran IAM di akun tujuan.

Peran

- Peran akun sumber
- Peran akun tujuan

Peran akun sumber

Di akun sumber, buat peran yang memberikan izin berikut. Dalam contoh ini, nama perannya adalah`mySourceRole`, tetapi Anda dapat memilih nama yang berbeda untuk peran ini. Pernyataan terakhir memungkinkan peran dalam akun tujuan untuk mengambil peran ini. Pernyataan kondisi memastikan bahwa peran ini diteruskan hanya ke layanan pengiriman log, dan hanya saat memantau sumber daya yang ditentukan. Saat Anda membuat kebijakan, tentukan VPCs, antarmuka jaringan, atau subnet yang Anda pantau dengan kunci kondisi. `iam:AssociatedResourceARN`

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::111122223333:role/mySourceRole",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "delivery.logs.amazonaws.com"
                },
                "StringLike": {
                    "iam:AssociatedResourceARN": [
                        "arn:aws:ec2:us-east-1:source-account:transit-gateway/
tgw-0fb8421e2da853bf"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:ListLogDeliveries",
```

```
                "logs:GetLogDelivery"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::111122223333:role/
AWSLogDeliveryFirehoseCrossAccountRole"
        }
    ]
}
```

Pastikan bahwa peran ini memiliki kebijakan kepercayaan berikut, yang memungkinkan layanan pengiriman log untuk mengambil peran tersebut.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Peran akun tujuan

Di akun tujuan, buat peran dengan nama yang dimulai dengan AWSLogDeliveryFirehoseCrossAccountRole. Peran ini harus memberikan izin berikut.

JSON

```
{
```

```
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
          "iam:CreateServiceLinkedRole",
          "firehose:TagDeliveryStream"
      ],
      "Resource": "*"
    }
  ]
}
```

Pastikan peran ini memiliki kebijakan kepercayaan berikut, yang memungkinkan peran yang Anda buat di akun sumber untuk mengambil peran ini.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/mySourceRole"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Buat peran akun sumber AWS Transit Gateway Flow Logs untuk Amazon Data Firehose

Dari akun sumber, buat peran sumber di AWS Identity and Access Management konsol.

Untuk membuat peran akun sumber

1. Masuk ke Konsol Manajemen AWS dan 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:
    1. PilihJSON.
    2. Ganti isi jendela ini dengan kebijakan izin di awal bagian ini.
    3. Pilih Berikutnya: Tag dan Berikutnya: Tinjau.
    4. Masukkan nama untuk kebijakan Anda dan deskripsi opsional, lalu pilih Buat kebijakan.
5. Di panel navigasi, pilih Peran.
6. Pilih Buat peran.
7. Untuk jenis entitas Tepercaya, pilih Kebijakan kepercayaan khusus. Untuk kebijakan kepercayaan kustom, ganti `"Principal": {},` dengan yang berikut ini, yang menentukan layanan pengiriman log. Pilih Berikutnya.

    ```
    "Principal": {
       "Service": "delivery.logs.amazonaws.com"
    },
    ```
8. Pada halaman Tambahkan izin, pilih kotak centang untuk kebijakan yang Anda buat sebelumnya dalam prosedur ini, lalu pilih Berikutnya.
9. Masukkan nama untuk peran Anda dan berikan deskripsi secara opsional.
10. Pilih Buat peran.

Buat peran akun tujuan AWS Transit Gateway Flow Logs untuk Amazon Data Firehose

Dari akun tujuan, buat peran tujuan di AWS Identity and Access Management konsol.

Untuk membuat peran akun tujuan

1. Masuk ke Konsol Manajemen AWS dan 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:
    1. PilihJSON.
    2. Ganti isi jendela ini dengan kebijakan izin di awal bagian ini.
    3. Pilih Berikutnya: Tag dan Berikutnya: Tinjau.
    4. 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 kustom, ganti `"Principal": {},` dengan yang berikut ini, yang menentukan layanan pengiriman log. Pilih Berikutnya.

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

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

Membuat catatan Log Aliran AWS Transit Gateway yang diterbitkan ke Amazon Data Firehose

Buat Log Aliran Transit Gateway yang dipublikasikan ke Amazon Data Firehose. Sebelum Anda dapat membuat log alur, pastikan bahwa Anda telah menyiapkan peran akun IAM sumber dan tujuan untuk pengiriman lintas akun dan bahwa Anda telah membuat aliran pengiriman Firehose. Untuk informasi selengkapnya, lihat Log Aliran Firehose Data Amazon. Anda dapat membuat log aliran Firehose menggunakan Konsol VPC Amazon atau CLI. AWS

Untuk membuat log aliran gateway transit yang diterbitkan ke Firehose menggunakan konsol

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

2. Di panel navigasi, pilih Gateway transit atau Lampiran gateway Transit.
3. Pilih kotak centang untuk satu atau beberapa gateway transit atau lampiran gateway transit.
4. Pilih Tindakan, Buat log alur.
5. Untuk Tujuan pilih Kirim ke Sistem Pengiriman Firehose.
6. Untuk Firehose Delivery Stream ARN, pilih ARN dari aliran pengiriman yang Anda buat di mana log aliran akan dipublikasikan.
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. (Opsional) Untuk menambahkan tag ke log aliran, pilih Tambahkan tag baru dan tentukan kunci dan nilai tag.
9. Pilih Buat log alur.

Untuk membuat log alur yang diterbitkan ke Firehose menggunakan alat baris perintah

Gunakan salah satu perintah berikut:

- create-flow-logs(AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

Contoh AWS CLI berikut membuat log aliran yang menangkap informasi gateway transit dan mengirimkan log aliran ke aliran pengiriman Firehose yang ditentukan.

```
aws ec2 create-flow-logs \
                --resource-type TransitGateway \
                --resource-ids tgw-1a2b3c4d \
                --log-destination-type kinesis-data-firehose \
                --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream:flowlogs_stream
```

Contoh AWS CLI berikut membuat log aliran yang menangkap informasi gateway transit dan mengirimkan log aliran ke aliran pengiriman Firehose yang berbeda dari akun sumber.

```
aws ec2 create-flow-logs  \
  --resource-type TransitGateway \
```

```
  --resource-ids gw-1a2b3c4d \
  --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
```

Membuat dan mengelola Log Aliran AWS Transit Gateway menggunakan APIs atau CLI

Anda dapat melakukan tugas yang dijelaskan di halaman ini menggunakan baris perintah.

Keterbatasan berikut berlaku saat menggunakan create-flow-logsperintah:

- `--resource-ids`memiliki batasan maksimum 25 `TransitGateway` atau jenis `TransitGatewayAttachment` sumber daya.
- `--traffic-type`bukan bidang wajib secara default. Kesalahan dikembalikan jika Anda menyediakan ini untuk jenis sumber daya gateway transit. Batas ini hanya berlaku untuk jenis sumber daya gateway transit.
- `--max-aggregation-interval`memiliki nilai default`60`, dan merupakan satu-satunya nilai yang diterima untuk jenis sumber daya gateway transit. Kesalahan dikembalikan jika Anda mencoba meneruskan nilai lainnya. Batas ini hanya berlaku untuk jenis sumber daya gateway transit.
- `--resource-type`mendukung dua jenis sumber daya baru, `TransitGateway` dan`TransitGatewayAttachment`.
- `--log-format`menyertakan semua bidang log untuk jenis sumber daya gateway transit jika Anda tidak menyetel bidang mana yang ingin Anda sertakan. Ini hanya berlaku untuk jenis sumber daya gateway transit.

Membuat log alur

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

Deskripsikan log alur

- describe-flow-logs (AWS CLI)

- Get-EC2FlowLog (AWS Tools for Windows PowerShell)

Melihat catatan log alur Anda (log acara)

- get-log-events (AWS CLI)
- Dapatkan- CWLLog Acara (AWS Tools for Windows PowerShell)

Menghapus log alur

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

Lihat catatan Log Aliran AWS Transit Gateway

Lihat informasi tentang log aliran gateway transit Anda melalui Amazon VPC. Saat Anda memilih sumber daya, semua log aliran untuk sumber daya tersebut dicantumkan. Informasi yang ditampilkan termasuk ID log alur, konfigurasi log alur, dan informasi tentang status log alur.

Untuk melihat informasi tentang log aliran untuk gateway transit

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Gateway transit atau Lampiran gateway Transit.
3. Pilih gateway transit atau lampiran gateway transit dan pilih Flow Logs. Informasi tentang log alur ditampilkan pada tab. Kolom Jenis tujuan menunjukkan tempat tujuan penerbitan log.

Mengelola tag Log Aliran AWS Transit Gateway

Anda dapat menambahkan atau menghapus tag untuk log alur di konsol Amazon EC2 dan Amazon VPC.

Untuk menambah atau menghapus tag untuk log aliran gateway transit

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Gateway transit atau Lampiran gateway Transit.
3. Pilih gateway transit atau lampiran gateway transit
4. Pilih Kelola Tag untuk log alur yang diperlukan.

5. Untuk menambahkan tag baru, pilih Buat Tag. Untuk menghapus sebuah tag, pilih tombol hapus (x).
6. Pilih Simpan.

Cari catatan Log Aliran AWS Transit Gateway

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. Pada panel navigasi, pilih Log, lalu pilih Grup log.
3. Pilih grup log yang berisi log alur Anda. Daftar aliran log untuk setiap gateway transit ditampilkan.
4. Pilih aliran log individual jika Anda mengetahui gateway transit yang Anda cari. Atau, pilih Cari Grup Log untuk mencari seluruh grup log. Ini mungkin memakan waktu lama jika ada banyak gateway transit di grup log Anda, atau tergantung pada rentang waktu yang Anda pilih.
5. Untuk Filter peristiwa, masukkan string berikut. Ini mengasumsikan bahwa catatan log alur menggunakan format default.

```
[version, resource_type, account_id,tgw_id, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr, dstaddr, srcport, dstport,
 protocol, packets, bytes,start,end, log_status, type,packets_lost_no_route,
 packets_lost_blackhole, packets_lost_mtu_exceeded, packets_lost_ttl_expired,
 tcp_flags,region, flow_direction, pkt_src_aws_service, pkt_dst_aws_service]
```

6. Ubah filter sesuai kebutuhan dengan menentukan nilai untuk bidang. Contoh berikut adalah filter berdasarkan alamat IP sumber tertentu.

```
[version, resource_type, account_id,tgw_id, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr= 10.0.0.1, dstaddr,
 srcport, dstport, protocol, packets, bytes,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
```

```
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
[version, resource_type, account_id,tgw_id, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr= 10.0.2.*, dstaddr,
 srcport, dstport, protocol, packets, bytes,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
```

Contoh berikut menyaring dengan transit gateway ID tgw-123abc456bca, port tujuan, dan jumlah byte.

```
[version, resource_type, account_id,tgw_id=tgw-123abc456bca, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr, dstaddr, srcport, dstport =
 80 || dstport = 8080, protocol, packets, bytes >= 500,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
```

Menghapus catatan Log Aliran AWS Transit Gateway

Anda dapat menghapus log aliran gateway transit menggunakan konsol Amazon VPC.

Prosedur ini menonaktifkan layanan log alur untuk sumber daya. Menghapus log aliran tidak menghapus aliran log yang ada dari Log atau file CloudWatch log dari Amazon S3. Data log alur yang ada harus dihapus menggunakan konsol layanan masing-masing. Selain itu, menghapus log alur yang diterbitkan ke Amazon S3 tidak akan menghapus kebijakan bucket dan daftar kontrol akses file log (). ACLs

Untuk menghapus log aliran gateway transit

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Gateway transit.
3. Pilih ID gateway Transit.
4. Di bagian Flow logs, pilih flow log yang ingin Anda hapus.

5. Pilih Tindakan, lalu pilih Hapus log aliran.
6. Konfirmasikan bahwa Anda ingin menghapus alur dengan memilih Hapus.

Metrik dan peristiwa di AWS Transit Gateway

Anda dapat menggunakan fitur-fitur berikut untuk memantau gateway transit Anda, menganalisis pola lalu lintas, dan memecahkan masalah dengan gateway transit Anda.

CloudWatch metrik

Anda dapat menggunakan Amazon CloudWatch untuk mengambil statistik tentang titik data untuk gateway transit Anda sebagai kumpulan data deret waktu yang diurutkan, yang dikenal sebagai metrik. Anda dapat menggunakan metrik ini untuk memverifikasi bahwa sistem Anda bekerja sesuai harapan. Untuk informasi selengkapnya, lihat CloudWatch metrik dalam AWS Transit Gateway.

Log Aliran Transit Gateway

Anda dapat menggunakan Log Aliran Transit Gateway untuk menangkap informasi terperinci tentang lalu lintas jaringan di gateway transit Anda. Untuk informasi selengkapnya, lihat Log Aliran Transit Gateway.

Log Aliran VPC

Anda dapat menggunakan VPC Flow Logs untuk menangkap informasi terperinci tentang lalu lintas yang menuju dan dari VPCs yang dilampirkan ke gateway transit Anda. Untuk informasi selengkapnya, lihat Log Alur VPC di Panduan Pengguna Amazon VPC.

CloudTrail log

Anda dapat menggunakan AWS CloudTrail untuk menangkap informasi terperinci tentang panggilan yang dilakukan ke API gateway transit dan menyimpannya sebagai file log di Amazon S3. Anda dapat menggunakan CloudTrail log ini untuk menentukan panggilan mana yang dilakukan, alamat IP sumber dari mana panggilan itu berasal, siapa yang melakukan panggilan, kapan panggilan dilakukan, dan sebagainya. Untuk informasi selengkapnya, lihat CloudTrail log.

CloudWatch Acara menggunakan Network Manager

Anda dapat menggunakan AWS Network Manager untuk meneruskan peristiwa ke CloudWatch, dan kemudian merutekan peristiwa tersebut ke fungsi atau aliran target. Network Manager menghasilkan peristiwa untuk perubahan topologi, pembaruan perutean, dan pembaruan status, yang semuanya dapat digunakan untuk mengingatkan Anda tentang perubahan di gateway transit Anda. Untuk informasi selengkapnya, lihat Memantau jaringan global Anda dengan CloudWatch Peristiwa di Panduan Pengguna Jaringan AWS Global untuk Gateway Transit.

CloudWatch metrik dalam AWS Transit Gateway

Amazon VPC menerbitkan titik data ke Amazon CloudWatch untuk gateway transit dan lampiran gateway transit Anda. CloudWatchmemungkinkan Anda untuk mengambil statistik tentang titik-titik data tersebut sebagai kumpulan data deret waktu yang diurutkan, yang dikenal sebagai metrik. Anggap metrik sebagai variabel untuk memantau, dan titik data sebagai nilai variabel tersebut dari waktu ke waktu. Setiap titik data memiliki timestamp terkait dan pengukuran unit opsional.

Anda dapat menggunakan metrik untuk memverifikasi bahwa sistem Anda bekerja sesuai harapan. Misalnya, Anda dapat membuat CloudWatch alarm untuk memantau metrik tertentu dan memulai tindakan (seperti mengirim pemberitahuan ke alamat email) jika metrik berada di luar rentang yang Anda anggap dapat diterima.

Amazon VPC mengukur dan mengirimkan metriknya ke CloudWatch dalam interval 60 detik.

Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

Daftar Isi

Metrik gerbang transit

Namespace `AWS/TransitGateway` mencakup metrik berikut.

Semua metrik selalu dilaporkan. Nilai-nilai mereka tergantung pada lalu lintas melalui gateway transit. Lihat Dimensi metrik gerbang transit untuk dimensi yang didukung.

Metrik	Deskripsi
`BytesDropCountBlackhole`	Jumlah byte turun karena cocok dengan rute. `blackhole` Statistics: Satu-satunya statistik yang bermakna adalah `Sum`.
`BytesDropCountNoRoute`	Jumlah byte turun karena tidak cocok dengan rute. Statistics: Satu-satunya statistik yang bermakna adalah `Sum`.

Metrik	Deskripsi
BytesIn	Jumlah byte yang diterima oleh gateway transit. Statistics: Satu-satunya statistik yang bermakna adalah Sum.
BytesOut	Jumlah byte yang dikirim dari gateway transit. Statistics: Satu-satunya statistik yang bermakna adalah Sum.
PacketsIn	Jumlah paket yang diterima oleh gateway transit. Statistics: Satu-satunya statistik yang bermakna adalah Sum.
PacketsOut	Jumlah paket yang dikirim oleh gateway transit. Statistics: Satu-satunya statistik yang bermakna adalah Sum.
PacketDropCountBlackhole	Jumlah paket turun karena cocok dengan rute. blackhole Statistics: Satu-satunya statistik yang bermakna adalah Sum.
PacketDropCountNoRoute	Jumlah paket turun karena tidak cocok dengan rute. Statistics: Satu-satunya statistik yang bermakna adalah Sum.
PacketDropCountTTLExpired	Jumlah paket turun karena TTL kedaluwarsa. Statistics: Satu-satunya statistik yang bermakna adalah Sum.

Metrik tingkat lampiran dan zona ketersediaan

Metrik berikut tersedia untuk lampiran gateway transit. Semua metrik lampiran dipublikasikan ke akun pemilik gateway transit. Metrik lampiran individual juga dipublikasikan ke akun pemilik lampiran. Pemilik lampiran hanya dapat melihat metrik untuk lampiran mereka sendiri. Untuk informasi selengkapnya tentang jenis lampiran yang didukung, lihatthe section called “Lampiran sumber daya”.

Metrik zona ketersediaan tersedia untuk diaktifkan untuk zona ketersediaan (AZs) pada lampiran gateway transit. Hanya lampiran VPC yang mendukung metrik per-AZ. Semua metrik tingkat AZ dipublikasikan ke akun pemilik gateway transit. Metrik AZ individual untuk lampiran juga

dipublikasikan ke akun pemilik lampiran. Pemilik lampiran hanya dapat melihat metrik per-AZ untuk lampiran mereka sendiri.

Semua metrik selalu dilaporkan. Nilai-nilai mereka tergantung pada lalu lintas yang and/or keluar dari lampiran gateway transit. Lihat Dimensi metrik gerbang transit untuk dimensi yang didukung.

Metrik	Deskripsi
`BytesDropCountBlackhole`	Jumlah byte turun karena cocok dengan `blackhole` rute pada lampiran gateway transit. Statistics: Satu-satunya statistik yang bermakna adalah `Sum`.
`BytesDropCountNoRoute`	Jumlah byte turun karena tidak cocok dengan rute pada lampiran gateway transit. Statistics: Satu-satunya statistik yang bermakna adalah `Sum`.
`BytesIn`	Jumlah byte yang diterima oleh gateway transit dari lampiran. Statistics: Satu-satunya statistik yang bermakna adalah `Sum`.
`BytesOut`	Jumlah byte yang dikirim dari gateway transit ke lampiran. Statistics: Satu-satunya statistik yang bermakna adalah `Sum`.
`PacketsIn`	Jumlah paket yang diterima oleh gateway transit dari lampiran. Statistics: Satu-satunya statistik yang bermakna adalah `Sum`.
`PacketsOut`	Jumlah paket yang dikirim oleh gateway transit ke lampiran. Statistics: Satu-satunya statistik yang bermakna adalah `Sum`.
`PacketDropCountBlackhole`	Jumlah paket turun karena cocok dengan `blackhole` rute pada lampiran gateway transit. Statistics: Satu-satunya statistik yang bermakna adalah `Sum`.
`PacketDropCountNoRoute`	Jumlah paket turun karena tidak cocok dengan rute.

Metrik	Deskripsi
	Statistics: Satu-satunya statistik yang bermakna adalah `Sum`.
`PacketDropCountTTLExpired`	Jumlah paket turun karena TTL kedaluwarsa. Statistics: Satu-satunya statistik yang bermakna adalah `Sum`.

Dimensi metrik gerbang transit

Filter data metrik gateway transit menggunakan dimensi berikut:

Dimensi	Deskripsi
`TransitGateway`	Memfilter data metrik dengan gateway transit.
`TransitGatewayAttachment`	Memfilter data metrik dengan lampiran gateway transit.
`TransitGateway` , `AvailabilityZone`	Memfilter data metrik berdasarkan gateway transit dan zona ketersediaan.
`TransitGatewayAttachment` , `AvailabilityZone`	Memfilter data metrik dengan lampiran gateway transit dan zona ketersediaan.

Log panggilan AWS Transit Gateway API menggunakan AWS CloudTrail

AWS Transit Gateway; terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau Layanan AWS. CloudTrail menangkap semua panggilan API untuk Transit Gateway sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari konsol Transit Gateway dan panggilan kode ke operasi Transit Gateway API. Dengan

menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke Transit Gateway, alamat IP dari mana permintaan dibuat, kapan dibuat, dan detail tambahan.

Setiap entri peristiwa atau log berisi informasi tentang entitas yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut hal ini:

- Baik permintaan tersebut dibuat dengan kredensial pengguna root atau pengguna.
- Apakah permintaan dibuat atas nama pengguna IAM Identity Center.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan tersebut dibuat oleh Layanan AWS lain.

CloudTrail aktif di Anda Akun AWS ketika Anda membuat akun dan Anda secara otomatis memiliki akses ke riwayat CloudTrail Acara. Riwayat CloudTrail Acara menyediakan catatan yang dapat dilihat, dapat dicari, dapat diunduh, dan tidak dapat diubah dari 90 hari terakhir dari peristiwa manajemen yang direkam dalam file. Wilayah AWS Untuk informasi selengkapnya, lihat Bekerja dengan riwayat CloudTrail Acara di Panduan AWS CloudTrail Pengguna. Tidak ada CloudTrail biaya untuk melihat riwayat Acara.

Untuk catatan acara yang sedang berlangsung dalam 90 hari Akun AWS terakhir Anda, buat jejak atau penyimpanan data acara CloudTrailDanau.

CloudTrail jalan setapak

Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Semua jalur yang dibuat menggunakan Konsol Manajemen AWS Multi-region. Anda dapat membuat jalur Single-region atau Multi-region dengan menggunakan. AWS CLI Membuat jejak Multi-wilayah disarankan karena Anda menangkap aktivitas Wilayah AWS di semua akun Anda. Jika Anda membuat jejak wilayah Tunggal, Anda hanya dapat melihat peristiwa yang dicatat di jejak. Wilayah AWS Untuk informasi selengkapnya tentang jejak, lihat Membuat jejak untuk Anda Akun AWS dan Membuat jejak untuk organisasi di Panduan AWS CloudTrail Pengguna.

Anda dapat mengirimkan satu salinan acara manajemen yang sedang berlangsung ke bucket Amazon S3 Anda tanpa biaya CloudTrail dengan membuat jejak, namun, ada biaya penyimpanan Amazon S3. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga. Untuk informasi tentang harga Amazon S3, lihat Harga Amazon S3.

CloudTrail Menyimpan data acara danau

CloudTrail Lake memungkinkan Anda menjalankan kueri berbasis SQL pada acara Anda. CloudTrail Lake mengonversi peristiwa yang ada dalam format JSON berbasis baris ke format Apache ORC. ORC adalah format penyimpanan kolumnar yang dioptimalkan untuk pengambilan data dengan cepat. Peristiwa digabungkan ke dalam penyimpanan data peristiwa, yang merupakan kumpulan peristiwa yang tidak dapat diubah berdasarkan kriteria yang Anda pilih dengan menerapkan pemilih acara tingkat lanjut. Penyeleksi yang Anda terapkan ke penyimpanan data acara mengontrol peristiwa mana yang bertahan dan tersedia untuk Anda kueri. Untuk informasi lebih lanjut tentang CloudTrail Danau, lihat Bekerja dengan AWS CloudTrail Danau di Panduan AWS CloudTrail Pengguna.

CloudTrail Penyimpanan data acara danau dan kueri menimbulkan biaya. Saat Anda membuat penyimpanan data acara, Anda memilih opsi harga yang ingin Anda gunakan untuk penyimpanan data acara. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa, dan periode retensi default dan maksimum untuk penyimpanan data acara. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga.

Acara manajemen Transit Gateway

Acara manajemen memberikan informasi tentang operasi manajemen yang dilakukan pada sumber daya di Anda Akun AWS. Ini juga dikenal sebagai operasi bidang kontrol. Secara default, CloudTrail mencatat peristiwa manajemen.

AWS Transit Gateway mencatat semua operasi pesawat kontrol Transit Gateway sebagai peristiwa manajemen. Untuk daftar operasi pesawat kontrol Gateway AWS Transit yang dicatat oleh Gateway Transit CloudTrail, lihat tindakan AWS Transit Gateway di Referensi API Amazon EC2.

Contoh acara Transit Gateway

Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang operasi API yang diminta, tanggal dan waktu operasi, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, sehingga peristiwa tidak muncul dalam urutan tertentu.

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah

jejak tumpukan yang diurutkan dari panggilan API publik, sehingga file tersebut tidak muncul dalam urutan tertentu.

File log menyertakan peristiwa untuk semua panggilan API untuk AWS akun Anda, bukan hanya panggilan API gateway transit. Anda dapat menemukan panggilan ke API gateway transit dengan memeriksa `eventSource` elemen dengan nilai`ec2.amazonaws.com`. Untuk melihat catatan tindakan tertentu, seperti `CreateTransitGateway`, periksa elemen `eventName` dengan nama tindakan.

Berikut ini adalah contoh catatan CloudTrail log untuk API gateway transit untuk pengguna yang membuat gateway transit menggunakan konsol. Anda dapat mengidentifikasi konsol menggunakan `userAgent` elemen. Anda dapat mengidentifikasi panggilan API yang diminta menggunakan `eventName` elemen. Informasi tentang pengguna (`Alice`) dapat ditemukan di elemen `userIdentity`.

Example Contoh: CreateTransitGateway

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2018-11-15T05:25:50Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateTransitGateway",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "console.ec2.amazonaws.com",
    "requestParameters": {
        "CreateTransitGatewayRequest": {
            "Options": {
                "DefaultRouteTablePropagation": "enable",
                "AutoAcceptSharedAttachments": "disable",
                "DefaultRouteTableAssociation": "enable",
                "VpnEcmpSupport": "enable",
                "DnsSupport": "enable"
            },
```

```
            "TagSpecification": {
                "ResourceType": "transit-gateway",
                "tag": 1,
                "Tag": {
                    "Value": "my-tgw",
                    "tag": 1,
                    "Key": "Name"
                }
            }
        }
    },
    "responseElements": {
        "CreateTransitGatewayResponse": {
            "xmlns": "http://ec2.amazonaws.com/doc/2016-11-15/",
            "requestId": "a07c1edf-c201-4e44-bffb-3ce90EXAMPLE",
            "transitGateway": {
                "tagSet": {
                    "item": {
                        "value": "my-tgw",
                        "key": "Name"
                    }
                },
                "creationTime": "2018-11-15T05:25:50.000Z",
                "transitGatewayId": "tgw-0a13743bd6c1f5fcb",
                "options": {
                    "propagationDefaultRouteTableId": "tgw-rtb-0123cd602be10b00a",
                    "amazonSideAsn": 64512,
                    "defaultRouteTablePropagation": "enable",
                    "vpnEcmpSupport": "enable",
                    "autoAcceptSharedAttachments": "disable",
                    "defaultRouteTableAssociation": "enable",
                    "dnsSupport": "enable",
                    "associationDefaultRouteTableId": "tgw-rtb-0123cd602be10b00a"
                },
                "state": "pending",
                "ownerId": 123456789012
            }
        }
    },
    "requestID": "a07c1edf-c201-4e44-bffb-3ce90EXAMPLE",
    "eventID": "e8fa575f-4964-4ab9-8ca4-6b5b4EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
```

```
}
```

Identitas dan manajemen akses di AWS Transit Gateway

AWS menggunakan kredensi keamanan untuk mengidentifikasi Anda dan memberi Anda akses ke sumber daya Anda AWS . Anda dapat menggunakan fitur AWS Identity and Access Management (IAM) untuk memungkinkan pengguna, layanan, dan aplikasi lain menggunakan AWS sumber daya Anda sepenuhnya atau dengan cara yang terbatas, tanpa membagikan kredensil keamanan Anda.

Secara default, pengguna IAM tidak memiliki izin untuk membuat, melihat, atau memodifikasi AWS sumber daya. Untuk mengizinkan pengguna mengakses sumber daya seperti gateway transit, dan untuk melakukan tugas, Anda harus membuat kebijakan IAM yang memberikan izin kepada pengguna untuk menggunakan sumber daya spesifik dan tindakan API yang mereka perlukan, lalu lampirkan kebijakan tersebut ke grup tempat pengguna tersebut berada. Saat Anda melampirkan kebijakan ke pengguna atau grup pengguna, kebijakan itu mengizinkan atau menolak izin pengguna untuk melakukan tugas yang ditentukan pada sumber daya yang ditentukan.

Untuk bekerja dengan gateway transit, salah satu kebijakan AWS terkelola berikut mungkin memenuhi kebutuhan Anda:

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

Contoh kebijakan untuk mengelola gateway transit

Berikut ini adalah contoh kebijakan IAM untuk bekerja dengan gateway transit.

Buat gateway transit dengan tag yang diperlukan

Contoh berikut memungkinkan pengguna untuk membuat gateway transit. Kunci `aws:RequestTag` kondisi mengharuskan pengguna untuk menandai gateway transit dengan tag`stack=prod`. Kunci `aws:TagKeys` kondisi menggunakan `ForAllValues` pengubah untuk menunjukkan bahwa hanya kunci yang `stack` diizinkan dalam permintaan (tidak ada tag lain yang dapat ditentukan). Jika pengguna tidak meneruskan tag khusus ini saat mereka membuat gateway transit, atau jika mereka tidak menentukan tag sama sekali, permintaan gagal.

Pernyataan kedua menggunakan kunci syarat `ec2:CreateAction` untuk memungkinkan para pengguna membuat tanda hanya dalam konteks `CreateTransitGateway`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCreateTaggedTGWs",
            "Effect": "Allow",
            "Action": "ec2:CreateTransitGateway",
            "Resource": "arn:aws:ec2:us-east-1:123456789012:transit-gateway/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/stack": "prod"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "stack"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:123456789012:transit-gateway/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateTransitGateway"
                }
            }
        }
    ]
}
```

Bekerja dengan tabel rute gateway transit

Contoh berikut memungkinkan pengguna untuk membuat dan menghapus tabel rute gateway transit untuk gateway transit tertentu saja (`tgw-11223344556677889`). Pengguna juga dapat membuat dan mengganti rute di tabel rute gateway transit apa pun, tetapi hanya untuk lampiran yang memiliki tag`network=new-york-office`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteTransitGatewayRouteTable",
                "ec2:CreateTransitGatewayRouteTable"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1:123456789012:transit-gateway/
tgw-11223344556677889",
                "arn:aws:ec2:*:*:transit-gateway-route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGatewayRoute",
                "ec2:ReplaceTransitGatewayRoute"
            ],
            "Resource": "arn:aws:ec2:*:*:transit-gateway-attachment/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/network": "new-york-office"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGatewayRoute",
                "ec2:ReplaceTransitGatewayRoute"
            ],
            "Resource": "arn:aws:ec2:*:*:transit-gateway-route-table/*"
```

```
        }
    ]
}
```

Gunakan peran terkait layanan untuk gateway transit di AWS Transit Gateway

Amazon VPC menggunakan peran terkait layanan untuk izin yang diperlukan untuk memanggil layanan lain AWS atas nama Anda. Untuk informasi selengkapnya, lihat Service-linkedperan dalam Panduan Pengguna IAM.

Peran terkait layanan gateway transit

Amazon VPC menggunakan peran terkait layanan untuk izin yang diperlukan untuk memanggil AWS layanan lain atas nama Anda saat Anda bekerja dengan gateway transit.

Izin yang diberikan oleh peran tertaut layanan

Amazon VPC menggunakan peran terkait layanan yang diberi nama AWSServiceRoleForVPCTransitGatewayuntuk memanggil tindakan berikut atas nama Anda saat Anda bekerja dengan gateway transit:

- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:DeleteNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2:AssignIpv6Addresses`
- `ec2:UnAssignIpv6Addresses`

AWSServiceRoleForVPCTransitGatewayPeran tersebut mempercayai layanan berikut untuk mengambil peran:

- `transitgateway.amazonaws.com`

AWSServiceRoleForVPCTransitGatewaymenggunakan kebijakan terkelolaAWSVPCTransitGatewayServiceRolePolicy.

Anda harus mengonfigurasi izin agar entitas IAM (seperti pengguna, grup, atau peran) dapat membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat izin Service-linked peran di Panduan Pengguna IAM.

Membuat peran terkait layanan

Anda tidak perlu membuat peran AWSServiceRoleForVPCTransitGateway secara manual. Amazon VPC membuat peran ini untuk Anda saat Anda melampirkan VPC di akun Anda ke gateway transit.

Mengedit peran terkait layanan

Anda dapat mengedit deskripsi AWSServiceRoleForVPCTransitGatewaymenggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit deskripsi peran terkait layanan di Panduan Pengguna IAM.

Menghapus peran terkait layanan

Jika Anda tidak perlu lagi menggunakan gateway transit, kami sarankan Anda menghapusnya. AWSServiceRoleForVPCTransitGateway

Anda dapat menghapus peran terkait layanan ini hanya setelah Anda menghapus semua lampiran VPC gateway transit di akun Anda. AWS Ini memastikan bahwa Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses lampiran VPC Anda.

Anda dapat menggunakan konsol IAM, CLI IAM, atau API IAM untuk menghapus peran terkait layanan . Untuk informasi selengkapnya, lihat Menghapus peran terkait layanan di Panduan Pengguna IAM.

Setelah Anda menghapus AWSServiceRoleForVPCTransitGateway, Amazon VPC membuat peran lagi jika Anda melampirkan VPC di akun Anda ke gateway transit.

AWS kebijakan terkelola untuk gateway transit di AWS Transit Gateway

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 Kebijakan terkelola AWS dalam Panduan Pengguna IAM.

Untuk bekerja dengan gateway transit, salah satu kebijakan AWS terkelola berikut mungkin memenuhi kebutuhan Anda:

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

AWS kebijakan terkelola: AWSVPCTransitGatewayServiceRolePolicy

Kebijakan ini melekat pada peran AWSServiceRoleForVPCTransitGateway. Hal ini memungkinkan Amazon VPC untuk membuat dan mengelola sumber daya untuk lampiran gateway transit Anda.

Untuk melihat izin kebijakan ini, lihat AWSVPCTransitGatewayServiceRolePolicydi Referensi Kebijakan AWS Terkelola.

Pembaruan gateway transit ke AWS kebijakan terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk gateway transit sejak Amazon VPC mulai melacak perubahan ini pada Maret 2021.

Ubah	Deskripsi	Date
Amazon VPC mulai melacak perubahan	Amazon VPC mulai melacak perubahan pada kebijakan yang AWS dikelola.	1 Maret 2021

ACL jaringan untuk gateway transit di AWS Transit Gateway

Network Access Control List (NACL) adalah lapisan keamanan opsional.

Aturan Network Access Control List (NACL) diterapkan secara berbeda, tergantung pada skenario:

- the section called “Subnet yang sama untuk instans EC2 dan asosiasi gateway transit”
- the section called “Subnet berbeda untuk instans EC2 dan asosiasi gateway transit”

Subnet yang sama untuk instans EC2 dan asosiasi gateway transit

Pertimbangkan konfigurasi di mana Anda memiliki instans EC2 dan asosiasi gateway transit di subnet yang sama. ACL jaringan yang sama digunakan untuk lalu lintas dari instans EC2 ke gateway transit dan lalu lintas dari gateway transit ke instans.

Aturan NACL diterapkan sebagai berikut untuk lalu lintas dari instance ke gateway transit:

- Aturan keluar menggunakan alamat IP tujuan untuk evaluasi.
- Aturan masuk menggunakan alamat IP sumber untuk evaluasi.

Aturan NACL diterapkan sebagai berikut untuk lalu lintas dari gateway transit ke instance:

- Aturan keluar tidak dievaluasi.
- Aturan masuk tidak dievaluasi.

Subnet berbeda untuk instans EC2 dan asosiasi gateway transit

Pertimbangkan konfigurasi di mana Anda memiliki instans EC2 dalam satu subnet dan asosiasi gateway transit di subnet yang berbeda, dan setiap subnet dikaitkan dengan ACL jaringan yang berbeda.

Aturan ACL jaringan diterapkan sebagai berikut untuk subnet instans EC2:

- Aturan keluar menggunakan alamat IP tujuan untuk mengevaluasi lalu lintas dari instance ke gateway transit.
- Aturan masuk menggunakan alamat IP sumber untuk mengevaluasi lalu lintas dari gateway transit ke instance.

Aturan NACL diterapkan sebagai berikut untuk subnet gateway transit:

- Aturan keluar menggunakan alamat IP tujuan untuk mengevaluasi lalu lintas dari gateway transit ke instance.
- Aturan keluar tidak digunakan untuk mengevaluasi lalu lintas dari instance ke gateway transit.
- Aturan masuk menggunakan alamat IP sumber untuk mengevaluasi lalu lintas dari instance ke gateway transit.
- Aturan masuk tidak digunakan untuk mengevaluasi lalu lintas dari gateway transit ke instans.

Praktik Terbaik

Gunakan subnet terpisah untuk setiap lampiran VPC gateway transit. Untuk setiap subnet, gunakan CIDR kecil, misalnya /28, sehingga Anda memiliki lebih banyak alamat untuk sumber daya EC2. Saat Anda menggunakan subnet terpisah, Anda dapat mengonfigurasi yang berikut:

- Biarkan NACL masuk dan keluar yang terkait dengan subnet gateway transit tetap terbuka.
- Tergantung pada arus lalu lintas Anda, Anda dapat menerapkan NACL ke subnet beban kerja Anda.

Untuk informasi selengkapnya tentang cara kerja lampiran VPC, lihat. the section called “Lampiran sumber daya”

AWS Kuota Transit Gateway

Anda Akun AWS memiliki kuota berikut (sebelumnya disebut sebagai batas) yang terkait dengan gateway transit. Kecuali dinyatakan lain, setiap kuota bersifat khusus per Wilayah.

Konsol Service Quotas memberikan informasi tentang kuota untuk akun Anda. Anda dapat menggunakan konsol Service Quotas untuk melihat kuota default dan meminta peningkatan kuota untuk kuota yang dapat disesuaikan. Untuk informasi selengkapnya, lihat Meminta peningkatan kuota di Panduan Pengguna Service Quotas.

Jika kuota yang dapat disesuaikan belum tersedia di Service Quotas, Anda dapat membuka kasus dukungan.

Umum

Nama	Default	Dapat disesuaikan
Transit gateway per akun	5	Ya
Blok CIDR per gerbang transit	5	Tidak

Blok CIDR digunakan dalam the section called “Connect attachment dan Connect peer” fitur ini.

Perutean

Nama	Default	Dapat disesuaikan
Tabel rute gerbang transit per gateway transit	20	Ya
Total rute gabungan (dinamis dan statis) di semua tabel rute untuk satu gateway transit	10.000	Hubungi Solutions Architect (SA) atau Technical Account Manager (TAM) Anda untuk bantuan lebih lanjut.

Nama	Default	Dapat disesuaikan
Rute dinamis yang diiklankan dari alat router virtual ke rekan Connect	1.000	Hubungi Solutions Architect (SA) atau Technical Account Manager (TAM) Anda untuk bantuan lebih lanjut.
Rute yang diiklankan dari rekan Connect di gateway transit ke alat router virtual	5.000	Tidak
Rute statis untuk awalan ke lampiran tunggal	1	Tidak

Rute yang diiklankan berasal dari tabel rute yang terkait dengan lampiran Connect.

Lampiran gateway transit

Gateway transit tidak dapat memiliki lebih dari satu lampiran VPC ke VPC yang sama.

Nama	Default	Dapat disesuaikan
Lampiran per transit gateway	5.000	Ya
Transit gateway untuk VPC	5	Tidak
Lampiran peering per transit gateway	50	Ya
Lampiran peering yang tertunda per transit gateway	10	Ya
Mengintip lampiran antara dua gateway transit atau antara satu gateway transit dan tepi jaringan inti Cloud WAN (CNE)	1	Tidak
Connect peer (terowongan GRE) untuk lampiran Connect	4	Tidak

Nama	Default	Dapat disesuaikan
Konsentrator VPN per gerbang transit	5	Tidak
Koneksi VPN untuk Konsentrator VPN	100	Tidak

Bandwidth

Ada banyak faktor yang dapat mempengaruhi bandwidth yang direalisasikan melalui koneksi Site-to-Site VPN, termasuk namun tidak terbatas pada: ukuran paket, bauran lalu lintas (TCP/UDP), kebijakan pembentukan atau pelambatan pada jaringan perantara, cuaca internet, dan persyaratan aplikasi tertentu. Untuk lampiran VPC, gateway, atau lampiran Direct Connect gateway transit peered, kami akan mencoba memberikan bandwidth tambahan di luar nilai default.

Nama	Default	Dapat disesuaikan
Bandwidth per lampiran VPC per Availability Zone	Hingga 100 Gbps setiap arah (yaitu, masuknya 100 Gbps dan jalan keluar 100 Gbps)	Hubungi Solutions Architect (SA) atau Technical Account Manager (TAM) Anda untuk bantuan lebih lanjut.
Paket per detik per lampiran VPC gateway transit per Availability Zone	Hingga 7.500.000	Hubungi Solutions Architect (SA) atau Technical Account Manager (TAM) Anda untuk bantuan lebih lanjut.
Bandwidth untuk Direct Connect gateway atau koneksi gateway transit peered per Availability Zone yang tersedia di Wilayah	Hingga 100 Gbps setiap arah (yaitu, masuknya 100 Gbps dan jalan keluar 100 Gbps)	Hubungi Solutions Architect (SA) atau Technical Account Manager (TAM) Anda untuk bantuan lebih lanjut.

Nama	Default	Dapat disesuaikan
Paket per detik per lampiran gateway transit (Direct Connect dan lampiran peering) per Availability Zone yang tersedia di Wilayah	Hingga 7.500.000	Hubungi Solutions Architect (SA) atau Technical Account Manager (TAM) Anda untuk bantuan lebih lanjut.
Bandwidth maksimum per Connect peer (terowongan GRE) untuk lampiran Connect	Hingga 5 Gbps	Tidak
Paket maksimum per detik per Connect peer	Hingga 300.000	Tidak

Anda dapat menggunakan perutean multipath berbiaya sama (ECMP) untuk mendapatkan bandwidth VPN yang lebih tinggi dengan menggabungkan beberapa terowongan VPN. Untuk menggunakan ECMP, koneksi VPN harus dikonfigurasi untuk perutean dinamis. ECMP tidak didukung pada koneksi VPN yang menggunakan perutean statis.

Anda dapat membuat hingga 4 rekan Connect per lampiran Connect (total bandwidth hingga 20 Gbps per lampiran Connect), selama lampiran transport (VPC Direct Connect atau) yang mendasarinya mendukung bandwidth yang diperlukan. Anda dapat menggunakan ECMP untuk mendapatkan bandwidth yang lebih tinggi dengan menskalakan secara horizontal di beberapa rekan Connect dari lampiran Connect yang sama atau di beberapa lampiran Connect pada gateway transit yang sama. Gateway transit tidak dapat menggunakan ECMP antara rekan BGP dari rekan Connect yang sama.

Untuk batas bandwidth dan paket dengan terowongan VPN, silakan merujuk ke bandwidth dan throughput VPN.

Direct Connect gerbang

Nama	Default	Dapat disesuaikan
Direct Connect gateway per gerbang transit	20	Tidak
Gerbang transit per gerbang Direct Connect	6	Tidak

Unit transmisi maksimum (MTU)

- MTU koneksi jaringan adalah ukuran, dalam byte, dari paket terbesar yang diizinkan yang dapat dilewatkan melalui koneksi. Semakin besar MTU suatu koneksi, semakin banyak data yang dapat dilewatkan dalam satu paket tunggal. Gateway transit mendukung MTU 8500 byte untuk lalu lintas antara VPCs, Transit Direct Connect Gateway Connect, dan lampiran peering (lampiran intra wilayah, antar-wilayah, dan Cloud WAN peering). Lalu lintas melalui koneksi VPN dapat memiliki MTU 1500 byte.
- Saat bermigrasi dari pengintipan VPC untuk menggunakan gateway transit, ketidakcocokan ukuran MTU antara pengintipan VPC dan gateway transit dapat mengakibatkan beberapa paket lalu lintas asimetris turun. Perbarui keduanya secara VPCs bersamaan untuk menghindari paket jumbo jatuh karena ketidakcocokan ukuran.
- Gateway transit memberlakukan penjepitan Ukuran Segmen Maksimum (MSS) untuk semua paket. Untuk informasi selengkapnya, lihat RFC879.
- Untuk detail tentang kuota Site-to-Site VPN untuk MTU, lihat Unit transmisi maksimum (MTU) di Panduan Pengguna.AWS Site-to-Site VPN
- Transit gateway mendukung Path MTU Discovery (PMTUD) untuk masuknya lalu lintas pada lampiran VPC dan Connect. Transit gateway menghasilkan ICMPv4 paket `FRAG_NEEDED` for dan `Packet Too Big (PTB)` untuk ICMPv6 paket. Transit gateway tidak mendukung PMTUD pada lampiran VPN Site-to-site, Direct Connect, dan Peering. Untuk informasi selengkapnya tentang Path MTU Discovery, lihat Path MTU Discovery di Panduan Pengguna Amazon VPC

Multicast

> **Note**
>
> Transit gateway multicast mungkin tidak cocok untuk perdagangan frekuensi tinggi atau aplikasi yang peka terhadap kinerja. Kami sangat menyarankan Anda meninjau batas multicast berikut. Hubungi akun Anda atau tim Arsitek Solusi untuk tinjauan terperinci tentang persyaratan kinerja Anda.

Nama	Default	Dapat disesuaikan
Domain multicast per transit gateway	20	Hubungi Solutions Architect (SA) atau Technical Account Manager (TAM) Anda untuk bantuan lebih lanjut.
Antarmuka jaringan multicast per gateway transit	10.000	Hubungi Solutions Architect (SA) atau Technical Account Manager (TAM) Anda untuk bantuan lebih lanjut.
Asosiasi domain multicast per VPC	20	Hubungi Solutions Architect (SA) atau Technical Account Manager (TAM) Anda untuk bantuan lebih lanjut.
Anggota dan sumber grup statis dan IGMPv2 multicast per gateway transit	10.000	Tidak
Anggota grup statis dan IGMPv2 multicast per grup multicast gateway transit	100	Tidak
Throughput multicast maksimum per aliran	1 Gbps	Tidak
Throughput multicast agregat maksimum per Availability Zone	20 Gbps	Tidak
Paket maksimum per detik per aliran (kurang dari 10 penerima)	75.000	Tidak

Nama	Default	Dapat disesuaikan
Paket maksimum per detik per aliran (lebih besar dari 10 penerima)	15.000	Tidak
Paket agregat maksimum per detik (kurang dari 10 penerima)	2.500.000	Tidak
Paket agregat maksimum per detik (lebih besar dari 10 penerima)	500.000	Tidak

AWS Manajer Jaringan

Nama	Default	Dapat disesuaikan
Jaringan global per Akun AWS	5	Ya
Perangkat per jaringan global	200	Ya
Tautan per jaringan global	200	Ya
Situs per jaringan global	200	Ya
Koneksi per jaringan global	500	Tidak

Sumber daya kuota tambahan

Untuk informasi selengkapnya, lihat berikut ini:

- Site-to-Site Kuota VPN di AWS Site-to-Site VPN Panduan Pengguna
- Kuota VPC Amazon di Panduan Pengguna Amazon VPC
- Kuota Direct Connect dalam Panduan Pengguna AWS Direct Connect

Riwayat dokumen untuk gateway transit

Tabel berikut menjelaskan rilis untuk gateway transit.

Perubahan	Deskripsi	Tanggal
Lampiran Client VPN	Buat lampiran Client VPN untuk menghubungkan gateway transit ke titik akhir Client VPN.	April 20, 2026
Alokasi Biaya Fleksibel	Konfigurasikan kebijakan alokasi biaya yang fleksibel untuk mengontrol bagaimana pemrosesan data dan biaya transfer dialokasikan di seluruh organisasi Anda.	November 20, 2025
Dukungan Enkripsi untuk gateway transit	Mengelola Dukungan Enkripsi di gateway transit untuk menerapkan enkripsi dalam transit untuk semua lalu lintas.	November 20, 2025
Lampiran fungsi jaringan	Buat lampiran fungsi jaringan untuk menghubungkan gateway transit langsung ke AWS Network Firewall.	Juni 16, 2025
Dukungan referensi kelompok keamanan	Anda sekarang dapat mereferensikan grup keamanan di seluruh VPC yang dilampirkan ke gateway transit.	September 25, 2024
AWS Kuota Transit Gateway	Batas bandwidth ditambahkan.	Agustus 14, 2023
AWS Log Aliran Transit Gateway	Transit Gateways sekarang mendukung Log Aliran Transit	14 Juli 2022

	Gateway, memungkinkan Anda memantau dan mencatat lalu lintas jaringan antar gateway transit.	
Tabel kebijakan gateway transit	Gunakan tabel kebijakan untuk menyiapkan perutean dinamis untuk gateway transit agar secara otomatis bertukar informasi perutean dan jangkauan dengan tipe gateway transit peered.	Juli 13, 2022
Panduan Pengguna Manajer Jaringan	Network Manager dibuat sebagai panduan mandiri, dan tidak lagi disertakan sebagai bagian dari Panduan Pengguna AWS Transit Gateway.	2 Desember 2021
Lampiran Peering	Anda dapat membuat koneksi peering dengan gateway transit di Wilayah yang sama.	1 Desember 2021
Transit Gateway Connect	Anda dapat membuat koneksi antara gateway transit dan peralatan virtual pihak ketiga yang berjalan di VPC.	10 Desember 2020
Mode alat	Anda dapat mengaktifkan mode alat pada lampiran VPC untuk memastikan bahwa lalu lintas dua arah mengalir melalui Availability Zone yang sama untuk lampiran.	29 Oktober 2020

Referensi daftar awalan	Anda dapat mereferensikan daftar awalan di tabel rute gateway transit Anda.	24 Agustus 2020
Ubah gateway transit	Anda dapat memodifikasi opsi konfigurasi untuk gateway transit Anda.	24 Agustus 2020
CloudWatch metrik untuk lampiran gateway transit	Anda dapat melihat CloudWatch metrik untuk setiap lampiran gateway transit.	6 Juli 2020
Penganalisis Rute Manajer Jaringan	Anda dapat menganalisis rute dalam tabel rute gateway transit Anda di jaringan global Anda.	4 Mei 2020
Lampiran Peering	Anda dapat membuat koneksi peering dengan gateway transit di Wilayah lain.	3 Desember 2019
Dukungan multicast	Transit Gateway mendukung perutean lalu lintas multicast antara subnet VPC yang terpasang dan berfungsi sebagai router multicast untuk instance pengiriman lalu lintas yang ditujukan untuk beberapa instance penerima.	3 Desember 2019
AWS Manajer Jaringan	Anda dapat memvisual isasikan dan memantau jaringan global Anda yang dibangun di sekitar gateway transit.	3 Desember 2019

AWS Direct Connect dukungan	Anda dapat menggunakan Direct Connect gateway untuk menghubungkan Direct Connect koneksi Anda melalui antarmuka virtual transit ke VPC atau VPN yang terpasang pada gateway transit Anda.	27 Maret 2019
Rilis awal	Rilis ini memperkenalkan gateway transit.	26 November 2018

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.