AWS Transit Gateway

Amazon VPC

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon VPC: AWS Transit Gateway

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara para pelanggan, atau dengan cara apa pun yang menghina atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan properti dari masing-masing pemilik, yang mungkin berafiliasi, terkait dengan, atau disponsori oleh Amazon, atau tidak.

Table of Contents

Apa yang dimaksud dengan gateway transit? 1
Konsep gateway transit 1
Cara memulai dengan gateway transit 2
Bekerja dengan gateway transit 2
Harga 3
Cara kerja gateway transit 4
Diagram arsitektur 4
Lampiran sumber daya 5
Perutean Multipath Biaya Sama 6
Zona Ketersediaan 7
Perutean 8
Tabel rute 8
Asosiasi tabel rute 9
Perbanyakan rute 9
Rute untuk lampiran peering 9
Urutan evaluasi rute 10
Mulai 13
Prasyarat 13
Langkah 1: Buat transit gateway 13
Langkah 2: Lampirkan VPC Anda ke transit gateway Anda 14
Langkah 3: Tambahkan rute antara gateway transit dan VPC Anda 15
Langkah 4: Uji transit gateway 16
Langkah 5: Hapus transit gateway 16
Praktik terbaik desain 17
Contoh kasus penggunaan 18
Router terpusat 18
Gambaran Umum 18
Sumber daya 19
Perutean 19
VPC Terisolasi 21
Gambaran Umum 21
Sumber daya 22
Perutean 22
VPC terisolasi dengan layanan bersama 24

Gambaran Umum ... 24
Sumber daya ... 25
Perutean ... 26
Mengintip ... 27
Gambaran Umum ... 27
Sumber daya ... 28
Perutean ... 29
Perutean keluar terpusat ... 30
Gambaran Umum ... 30
Sumber daya ... 31
Perutean ... 32
Alat VPC ... 34
Ikhtisar ... 35
Peralatan stateful dan mode alat ... 37
Perutean ... 38
Bekerja dengan gateway transit ... 41
Transit gateway ... 41
Membuat transit gateway ... 42
Lihat gateway transit Anda ... 44
Menambahkan atau mengedit tag untuk gateway transit ... 45
Ubah gateway transit ... 45
Bagikan gateway transit ... 46
Terima pembagian sumber daya ... 46
Terima lampiran bersama ... 47
Hapus gateway transit ... 47
Lampiran VPC ... 48
Siklus hidup lampiran VPC ... 49
Buat lampiran gateway transit ke VPC ... 52
Ubah lampiran VPC Anda ... 53
Ubah tag lampiran VPC Anda ... 53
Lihat lampiran VPC Anda ... 54
Hapus lampiran VPC ... 54
Memecahkan masalah lampiran VPC ... 55
Lampiran VPN ... 55
Buat lampiran gateway transit ke VPN ... 56
Lihat lampiran VPN Anda ... 57

Lampiran ke gateway Direct Connect 57
Lampiran Peering 58
Buat lampiran peering 59
Menerima atau menolak permintaan lampiran peering 60
Menambahkan rute ke tabel rute gateway transit 60
Lihat lampiran koneksi peering gateway transit Anda 61
Hapus lampiran peering 62
Pertimbangan Keikutsertaan AWS Wilayah 62
Connect attachment dan Connect peer 63
Connect rekan-rekan 64
Persyaratan dan pertimbangan 67
Membuat lampiran Connect 68
Buat rekan Connect (terowongan GRE) 69
Melihat lampiran Connect dan Connect peer 70
Ubah lampiran Connect dan Connect peer tag 70
Hapus rekan Connect 71
Menghapus lampiran Connect 71
Tabel rute transit gateway 72
Buat tabel rute gateway transit 72
Lihat tabel rute gateway transit 72
Kaitkan tabel rute gateway transit 73
Menghapus asosiasi untuk tabel rute gateway transit 73
Menyebarkan rute ke tabel rute gateway transit 74
Nonaktifkan propagasi rute 74
Buat rute statis 75
Hapus rute statis 76
Ganti rute statis 76
Ekspor tabel rute ke Amazon S3 77
Menghapus tabel rute gateway transit 78
Refiks daftar prefiks 79
Tabel kebijakan gateway transit 81
Membuat tabel kebijakan gateway transit 82
Menghapus tabel kebijakan gateway transit 82
Multicast di gateway transit 83
Konsep multicast 1
Pertimbangan 84

Multicast dengan Windows Server 85
Perutean multicast 86
Bekerja dengan multicast 88
Bagikan gateway transit Anda 107
Batalkan pembagian gateway transit 108
Subnet bersama 108
Log Aliran Transit Gateway 110
Catatan Log Aliran Transit Gateway 111
Format default 112
Format kustom 112
Bidang yang tersedia 112
Harga Log Aliran Transit Gateway 118
Publikasikan ke CloudWatch Log 118
Peran IAM untuk menerbitkan log alur ke CloudWatch Log 119
Izin bagi pengguna IAM untuk meneruskan peran 121
Buat log alur yang diterbitkan ke CloudWatch Log 122
Proses catatan log alur di CloudWatch Log 123
Terbitkan ke Amazon S3 124
Berkas log alur 125
Kebijakan IAM untuk prinsipal IAM yang menerbitkan log alur ke Amazon S3 127
Izin bucket Amazon S3 untuk log alur 128
Kebijakan kunci yang diperlukan untuk digunakan dengan SSE-KMS 129
Izin file berkas log Amazon S3 130
Membuat log alur yang menerbitkan ke Amazon S3 130
Catatan log alur proses di Amazon S3 132
Publikasikan ke Kinesis Data Firehose 132
Peran IAM untuk pengiriman lintas akun 133
Membuat log alur yang diterbitkan ke Firehose 137
Bekerja dengan log alur 139
Mengontrol penggunaan log alur 139
Membuat log alur 140
Melihat log alur 140
Menambahkan atau menghapus tag untuk log alur 140
Melihat catatan log alur 141
Cari catatan log alur 142
Menghapus log alur 143

Ikhtisar dan batasan API dan CLI 144
Pantau gateway transit Anda 146
CloudWatch metrik 147
Metrik gerbang transit 147
Dimensi metrik untuk gateway transit 149
CloudTrail log 149
Informasi gateway transit di CloudTrail 149
Memahami entri file log gateway transit 150
Manajemen identitas dan akses 153
Contoh kebijakan untuk mengelola gateway transit 153
Contoh kebijakan untuk mengelola Manajer AWS Jaringan 155
Peran terkait layanan 156
Transit Gateway 156
Kebijakan yang dikelola AWS 157
AWSVPCTransitGatewayServiceRolePolicy 158
Pembaruan kebijakan 158
ACL jaringan 159
Subnet yang sama untuk instans EC2 dan asosiasi gateway transit 159
Subnet berbeda untuk instans EC2 dan asosiasi gateway transit 159
Praktik Terbaik 160
Kuota 161
Umum 161
Perutean 161
Lampiran gateway transit 162
Bandwidth 162
AWS Direct Connect gerbang 164
Unit transmisi maksimum (MTU) 164
Multicast 165
Network Manager 166
Sumber daya kuota tambahan 166
Riwayat dokumen 167
..... clxx

Apa yang dimaksud dengan gateway transit?

Gateway transit adalah hub transit jaringan yang dapat Anda gunakan untuk menghubungkan cloud pribadi virtual (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 antar pusat AWS data secara otomatis dienkripsi pada lapisan fisik.

Untuk informasi selengkapnya, lihat AWS Transit Gateway.

Konsep gateway transit

Berikut ini adalah konsep kunci untuk gateway transit:

- Lampiran - Anda dapat melampirkan yang berikut:
  - Satu atau lebih VPC
  - Alat jaringan Connect SD-WAN/Pihak Ketiga
  - AWS Direct ConnectGateway
  - Koneksi peering dengan gateway transit lain
  - Koneksi VPN ke gateway transit
- Transit gateway Unit Transmisi Maksimum (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, Transit Gateway ConnectAWS Direct Connect, dan lampiran peering. Lalu lintas melalui koneksi VPN dapat memiliki MTU 1500 byte.
- Tabel rute gateway 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. 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 ke banyak lampiran.
- Propagasi rute - Gateway VPC, koneksi VPN, atau 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
- Mulai
- Praktik terbaik desain

Bekerja dengan gateway transit

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

- AWS Management Console- Menyediakan antarmuka web yang dapat Anda gunakan untuk mengakses gateway transit Anda.
- AWSCommand Line Interface (AWS CLI) — Menyediakan perintah untuk serangkaian AWS layanan yang luas, termasuk Amazon VPC, dan didukung pada Windows, macOS, dan Linux. Untuk informasi selengkapnya, lihat AWS Command Line Interface.
- AWSSDK — 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 SDK AWS.
- 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 menghasilkan hash untuk menandatangani permintaan, dan menangani kesalahan. Untuk informasi selengkapnya, lihat Referensi API Amazon EC2.

Harga

Anda dikenai biaya per jam untuk setiap lampiran di gateway transit, dan Anda dikenai biaya untuk jumlah lalu lintas yang diproses di gateway transit. Untuk informasi selengkapnya, lihat harga AWS Transit Gateway.

Cara kerja gateway transit

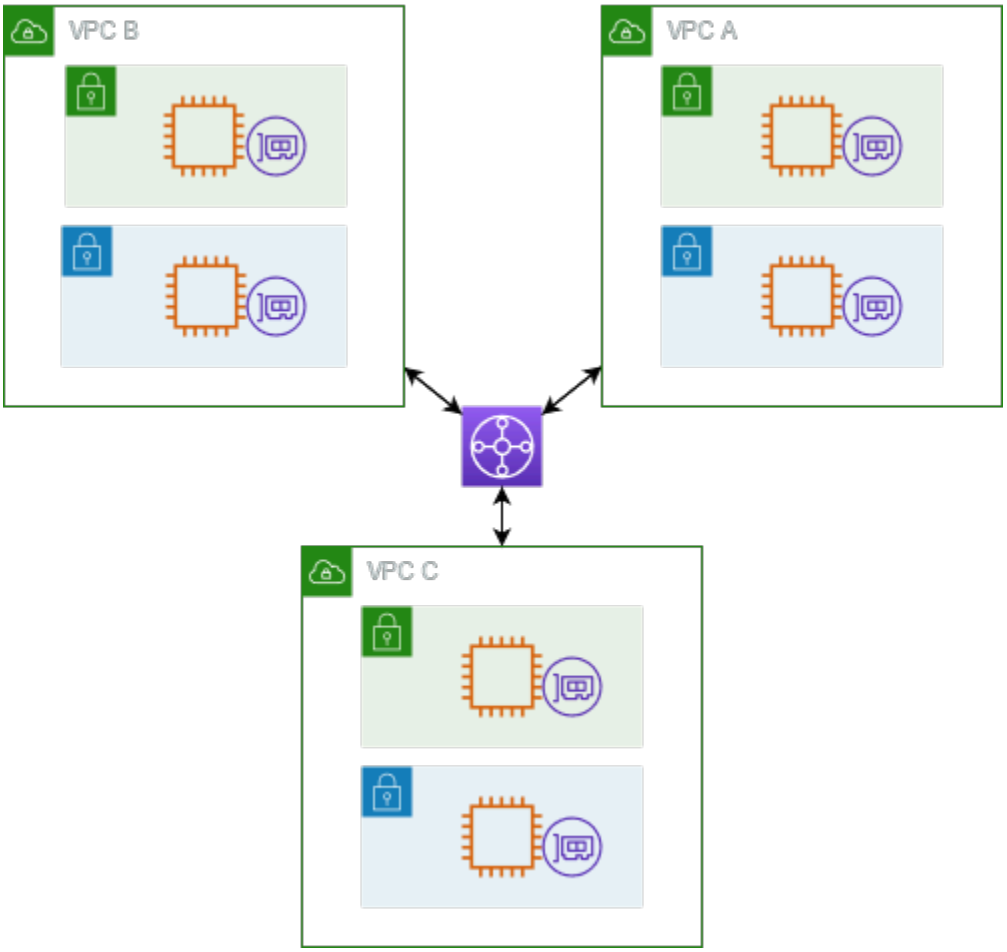
Gateway transit bertindak sebagai router virtual Regional untuk lalu lintas yang mengalir antara virtual private cloud (VPC) dan jaringan lokal. Gateway transit menskalakan secara elastis berdasarkan volume lalu lintas jaringan. Routing melalui gateway transit beroperasi pada lapisan 3, di mana paket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

Daftar Isi

- Diagram arsitektur
- Lampiran sumber daya
- Perutean Multipath Biaya Sama
- Zona Ketersediaan
- Perutean

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.

Tujuan	Target	Jenis rute
VPC KE CIDR	*Lampiran untuk VPC A*	diperbanyak
VPC B CIDR	*Lampiran untuk VPC B*	diperbanyak
VPC C CIDR	*Lampiran untuk 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 AWS Direct Connect gateway
- Satu atau beberapa lampiran Transit Gateway Connect
- Satu atau lebih koneksi peering gateway transit
- Lampiran gateway transit dapat menjadi sumber dan tujuan paket

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.

> **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 Active/Active atau Active/Passive Direct Connect dari antarmuka virtual publik? AWS .

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, lalu lintas dapat dialihkan ke semua subnet di VPC, bukan hanya subnet atau Availability Zone yang ditentukan. 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: Appliance 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.

Daftar Isi

- 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. Atau, jika Anda menonaktifkan propagasi rute dan asosiasi tabel rute, AWS tidak akan membuat tabel rute default untuk gateway transit.

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 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, rute dalam tabel rute yang terkait dengan lampiran 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 peralatan SD-WAN, 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: Gerbang transit sejawat.

Urutan evaluasi rute

Rute gateway transit dievaluasi dengan urutan sebagai berikut:

- Rute paling spesifik untuk alamat tujuan.
- Untuk rute dengan alamat IP tujuan yang sama tetapi target yang berbeda, prioritas rute adalah sebagai berikut:
  - Rute statis (misalnya, rute statis Site-to-Site VPN)
  - Daftar awalan rute referensi
  - Rute yang disebarkan VPC
  - Rute propagasi gateway Direct Connect
  - Transit Gateway Connect rute yang disebarkan
  - Rute propagasi pribadi Site-to-Site VPN
  - Rute yang disebarkan VPN publik situs-ke-situs
  - Transit Gateway mengintip rute yang disebarkan (Cloud WAN)

Transit Gateway hanya menampilkan rute pilihan. Rute cadangan hanya akan muncul di tabel rute Transit Gateway jika rute tersebut 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.

Tujuan	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
0.0.0.0/0	igw-12345	4

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

Tujuan	Lampiran (Target)	Jenis 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	AWS Direct Connect pintu gerbang	Diperbanyak	3
172.31.0.0/16	tgw-attach-789 | -123 tgw-connect-peer	Hubungkan	Diperbanyak	4

Tujuan	Lampiran (Target)	Jenis sumber daya	Jenis rute	Prioritas
172.31.0.0/16	tgw-lampiran-789 | vpn-5678	VPN	Diperbanyak	5

Memulai dengan gateway transit

Tugas-tugas berikut membantu Anda mempelajari transit gateway. Anda akan membuat gateway transit dan kemudian menghubungkan dua VPC Anda menggunakan gateway transit.

Tugas

- Prasyarat
- Langkah 1: Buat transit gateway
- Langkah 2: Lampirkan VPC Anda ke transit gateway Anda
- Langkah 3: Tambahkan rute antara gateway transit dan VPC Anda
- Langkah 4: Uji transit gateway
- Langkah 5: Hapus transit gateway

Prasyarat

- Untuk mendemonstrasikan contoh sederhana menggunakan gateway transit, buat dua VPC di Wilayah yang sama. VPC tidak dapat memiliki CIDR yang tumpang tindih. Peluncuran satu instans Amazon EC2 di setiap VPC. Untuk informasi selengkapnya, lihat Memulai dengan Amazon VPC dalam Panduan Pengguna Amazon VPC.
- Anda tidak dapat memiliki rute identik yang menunjuk ke dua VPC yang berbeda. Gateway transit tidak menyebarkan CIDR dari VPC yang baru dilampirkan jika rute identik ada di tabel rute gateway transit.
- Verifikasi bahwa Anda memiliki izin yang diperlukan untuk bekerja dengan transit gateway. Untuk informasi selengkapnya, lihat Manajemen identitas dan akses untuk gateway transit Anda.
- Anda tidak dapat melakukan ping di antara host jika Anda belum menambahkan aturan ICMP ke masing-masing grup keamanan host. Untuk informasi selengkapnya, lihat Bekerja dengan grup keamanan di Panduan Pengguna Amazon VPC.

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 menciptakantag transit gateway

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di pemilih Wilayah, pilih Wilayah yang Anda gunakan saat membuat VPC.
3. Pada panel navigasi, pilih Gateway Transit.
4. Pilih Buat gateway transit.
5. (Opsional) Untuk tag Nama, masukkan nama untuk transit gateway. Ini menciptakantag Nama" sebagai kunci dan nama yang Anda tentakantag nilai.
6. (Opsional) Untuk Deskripsi, masukkan deskripsi untuk transit gateway.
7. Untuk Amazon side Autonomous System Number (ASN), masukkan ASN pribadi untuk gateway transit Anda. Ini harus ASN untukAWS sisi sesi Border Gateway Protocol (BGP).

   Rentangnya adalah dari 64512 hingga 65534 untuk ASN 16-bit.

   Kisarannya dari 4200000000 hingga 4294967294 untuk ASN 32-bit.

   Jika Anda memiliki penerapan Multi-wilayah, kami sarankan Anda menggunakan ASN unik untuk setiap gateway transit Anda.
8. (Opsional) Anda dapat mengubah pengaturan default jika Anda perlu menonaktifkan dukungan DNS, atau jika Anda tidak ingin tabel rute asosiasi default atau tabel rute propagasi default.
9. Pilih Buat gateway transit. Ketika gateway dibuat, keadaan awal gateway transit adalah`pending`.

Langkah 2: Lampirkan VPC Anda ke transit gateway 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 VPC dan meluncurkan instans EC2 di masing-masing, seperti yang dijelaskan dalamPrasyarat.

Buat transit gateway attachment ke VPC

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. (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 dukungan IPv6.
8. Untuk ID VPC, pilih VPC yang dilampirkan pada transit gateway.
9. Untuk ID Subnet, pilih satu subnet untuk setiap Availability Zone yang akan digunakan oleh gateway transit untuk mengarahkan 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, putuskan kasus penggunaan untuk gateway transit Anda, lalu konfigurasikan rute. Untuk informasi selengkapnya, lihat Contoh kasus penggunaan.

Langkah 3: Tambahkan rute antara gateway transit dan VPC Anda

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

Untuk menambahkan rute ke tabel rute VPC

1. Buka konsol Amazon VPC 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 transit gateway.
7. Pilih Save changes (Simpan perubahan).

Langkah 4: Uji transit gateway

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

Langkah 5: Hapus transit gateway

Bila Anda tidak lagi memerlukan gateway transit gateway, Anda dapat menghapusnya.

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

Untuk menghapus gateway transit

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

   Status gateway transit pada halaman gateway Transit adalah Menghapus. Setelah dihapus transit gateway dihapus dari halaman.

Praktik terbaik desain gerbang transit

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 sumber daya EC2. Saat Anda menggunakan subnet terpisah, Anda dapat mengonfigurasi yang berikut:
  - Biarkan ACL jaringan masuk dan keluar yang terkait dengan subnet gateway transit tetap terbuka.
  - Bergantung pada arus lalu lintas Anda, Anda dapat menerapkan ACL jaringan 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 koneksi VPN Site-to-Site Border Gateway Protocol (BGP). Jika perangkat gateway pelanggan Anda atau firewall untuk koneksi mendukung multipath, aktifkan fitur tersebut.
- Aktifkan propagasi rute untuk lampiran AWS Direct Connect gateway dan lampiran VPN Site-to-Site BGP.
- 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 kedua VPC secara 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 Otonomi (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.

Contoh kasus penggunaan untuk gateway transit

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

Contoh

- Contoh: Router terpusat
- Contoh: VPC terisolasi
- Contoh: VPC terisolasi dengan layanan bersama
- Contoh: Gerbang transit sejawat
- Contoh: Perutean keluar terpusat ke internet
- Contoh: Appliance di VPC layanan bersama

Contoh: Router terpusat

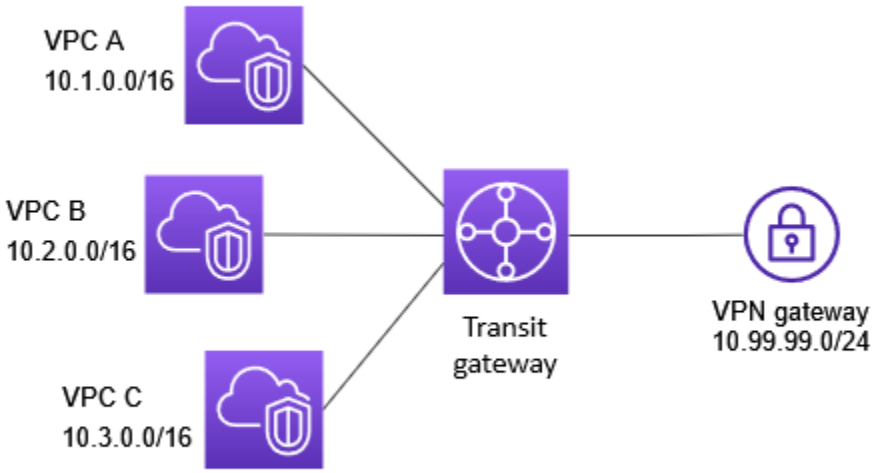
Anda dapat mengonfigurasi gateway transit Anda sebagai router terpusat yang menghubungkan semua VPC Anda,AWS Direct Connect, dan koneksi VPN Site-to-Site. Dalam skenario ini, semua lampiran dikaitkan dengan tabel rute default gateway transit dan disebarkan ke tabel rute default gateway transit. Oleh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

Daftar Isi

- Gambaran Umum
- Sumber daya
- Perutean

Gambaran Umum

Diagram berikut menunjukkan komponen kunci konfigurasi untuk skenario ini. Dalam skenario ini, ada tiga lampiran VPC dan satu lampiran VPN Site-to-Site 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 tentang membuat VPC, 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 gateway transit ke VPC”.
- Lampiran VPN Site-to-Site di gateway transit. Blok CIDR untuk setiap VPC merambat ke tabel rute gateway transit. Ketika koneksi VPN habis, sesi BGP dibuat dan CIDR VPN Site-to-Site 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	*Lampiran untuk VPC A*	diperbanyak
10.2.0.0/16	*Lampiran untuk VPC B*	diperbanyak
10.3.0.0/16	*Lampiran untuk VPC C*	diperbanyak
10.99.99.0/24	*Lampiran untuk koneksi VPN*	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

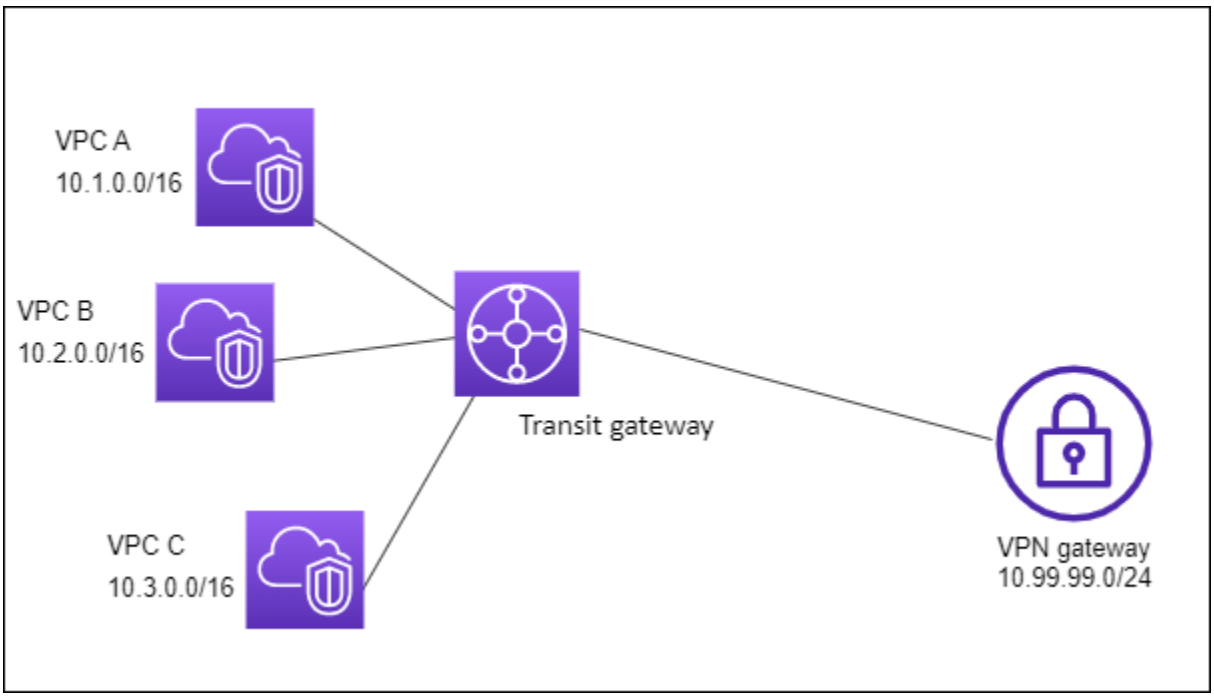
Anda dapat mengkonfigurasi transit gateway Anda sebagai beberapa router terisolasi. Hal ini mirip dengan menggunakan beberapa transit gateway, tetapi memberikan lebih banyak fleksibilitas dalam kasus di mana rute dan lampiran mungkin berubah. Dalam skenario ini, setiap router terisolasi memiliki tabel 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

- Gambaran Umum
- Sumber daya
- Perutean

Gambaran Umum

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 Site-to-Site VPN (jika tujuan 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 tentang membuat VPC, 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 gateway transit ke VPC”.
- Lampiran VPN Site-to-Site 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	*Lampiran untuk koneksi VPN*	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	*Lampiran untuk VPC A*	diperbanyak
10.2.0.0/16	*Lampiran untuk VPC B*	diperbanyak
10.3.0.0/16		diperbanyak

Tujuan	Target	Jenis rute
	Lampiran untuk VPC C	

Untuk informasi selengkapnya tentang menyebarkan rute dalam tabel rute gateway transit, lihatMenyebarkan rute ke tabel rute gateway transit.

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.

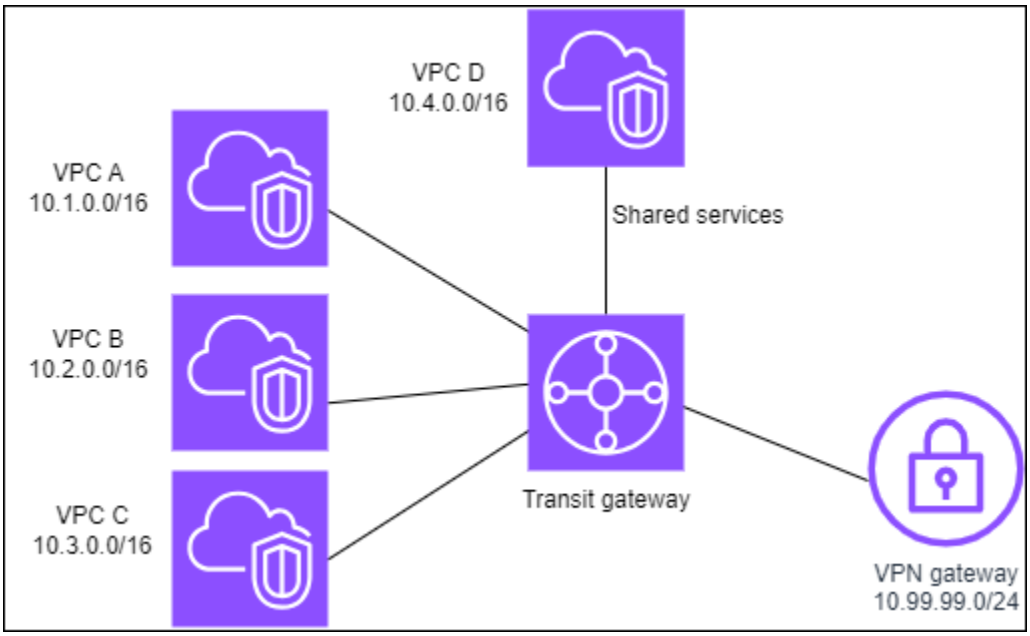
Daftar Isi

- Gambaran Umum
- Sumber daya
- Perutean

Gambaran Umum

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 Site-to-Site VPN. 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 tentang membuat VPC, 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 gateway transit ke VPC”.
- Lampiran VPN Site-to-Site pada 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 dalam 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	*ID gerbang transit*

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	*Lampiran untuk koneksi VPN*	diperbanyak
10.4.0.0/16	*Lampiran untuk 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	*Lampiran untuk VPC A*	diperbanyak
10.2.0.0/16	*Lampiran untuk VPC B*	diperbanyak
10.3.0.0/16	*Lampiran untuk VPC C*	diperbanyak

Untuk informasi selengkapnya, lihat Menyebarkan rute ke tabel rute gateway transit.

Tabel BGP gateway pelanggan

Tabel BGP gateway pelanggan berisi CIDR untuk keempat VPC.

Contoh: Gerbang transit sejawat

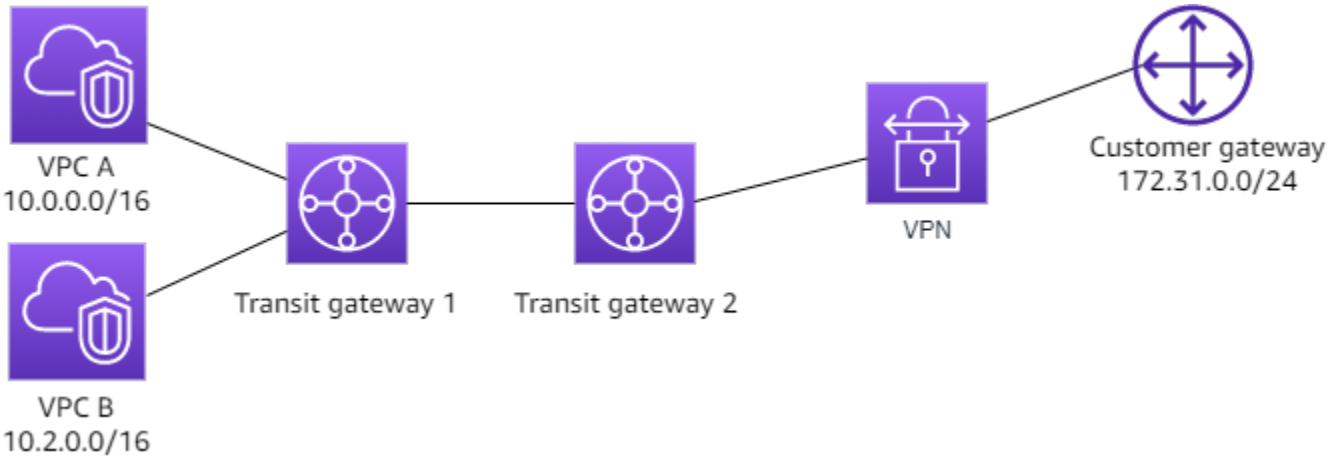
Anda dapat membuat koneksi peering gateway transit antara gateway transit. Anda kemudian dapat merutekan lalu lintas di antara lampiran untuk masing-masing gateway transit. Dalam skenario ini, lampiran VPC dan VPN dikaitkan dengan tabel rute default gateway transit, dan mereka menyebar ke tabel rute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

Daftar Isi

- Gambaran Umum
- Sumber daya
- Perutean

Gambaran Umum

Diagram berikut menunjukkan komponen kunci konfigurasi untuk skenario ini. Transit gateway 1 memiliki dua lampiran VPC, dan transit gateway 2 memiliki satu lampiran VPN Site-to-Site. 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 tentang membuat VPC, 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 gateway transit ke VPC”.
- Lampiran VPN Site-to-Site 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 transit gateway peering.

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
- CIDR VPN Site-to-Site menyebar 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	*ID Lampiran untuk VPC A*	diperbanyak
10.2.0.0/16	*ID Lampiran untuk VPC B*	diperbanyak
0.0.0.0/0	*ID lampiran untuk koneksi peering*	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	*ID lampiran untuk koneksi VPN*	diperbanyak
10.0.0.0/16	*ID lampiran untuk koneksi peering*	statis
10.2.0.0/16	*ID lampiran untuk koneksi peering*	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

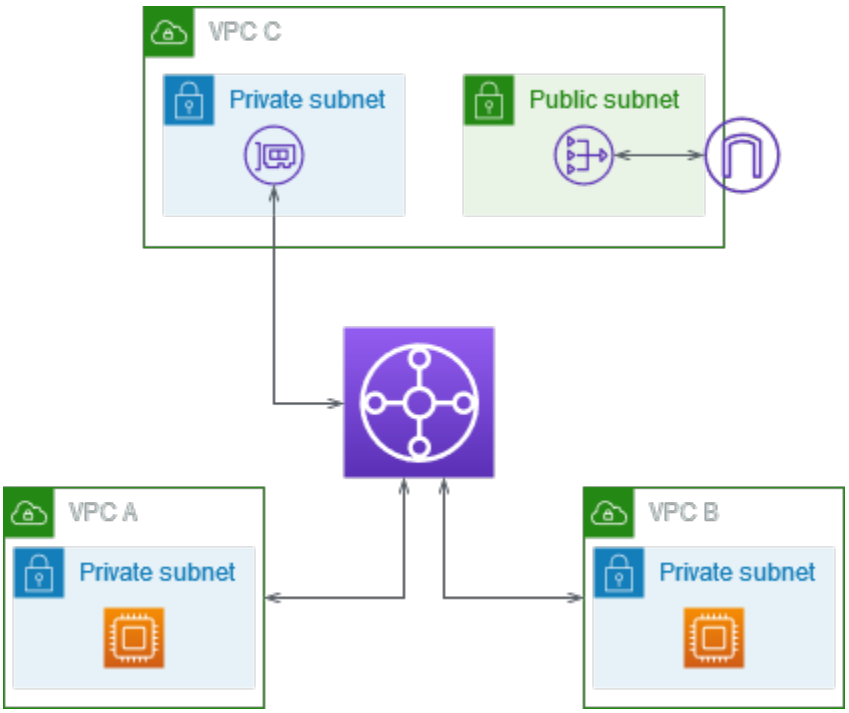
Anda dapat mengonfigurasi gateway transit untuk merutekan lalu lintas internet keluar dari VPC tanpa gateway internet ke VPC yang berisi gateway NAT dan gateway internet.

Daftar Isi

- Gambaran Umum
- Sumber daya
- Perutean

Gambaran Umum

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 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 gateway transit ke 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 KE 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

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 KE 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 KE CIDR	*Lampiran untuk VPC A*	diperbanyak
VPC B CIDR	*Lampiran untuk VPC B*	diperbanyak
VPC C CIDR	*Lampiran untuk VPC C*	diperbanyak
0.0.0.0/0	*Lampiran untuk VPC C*	statis

Contoh: Appliance 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

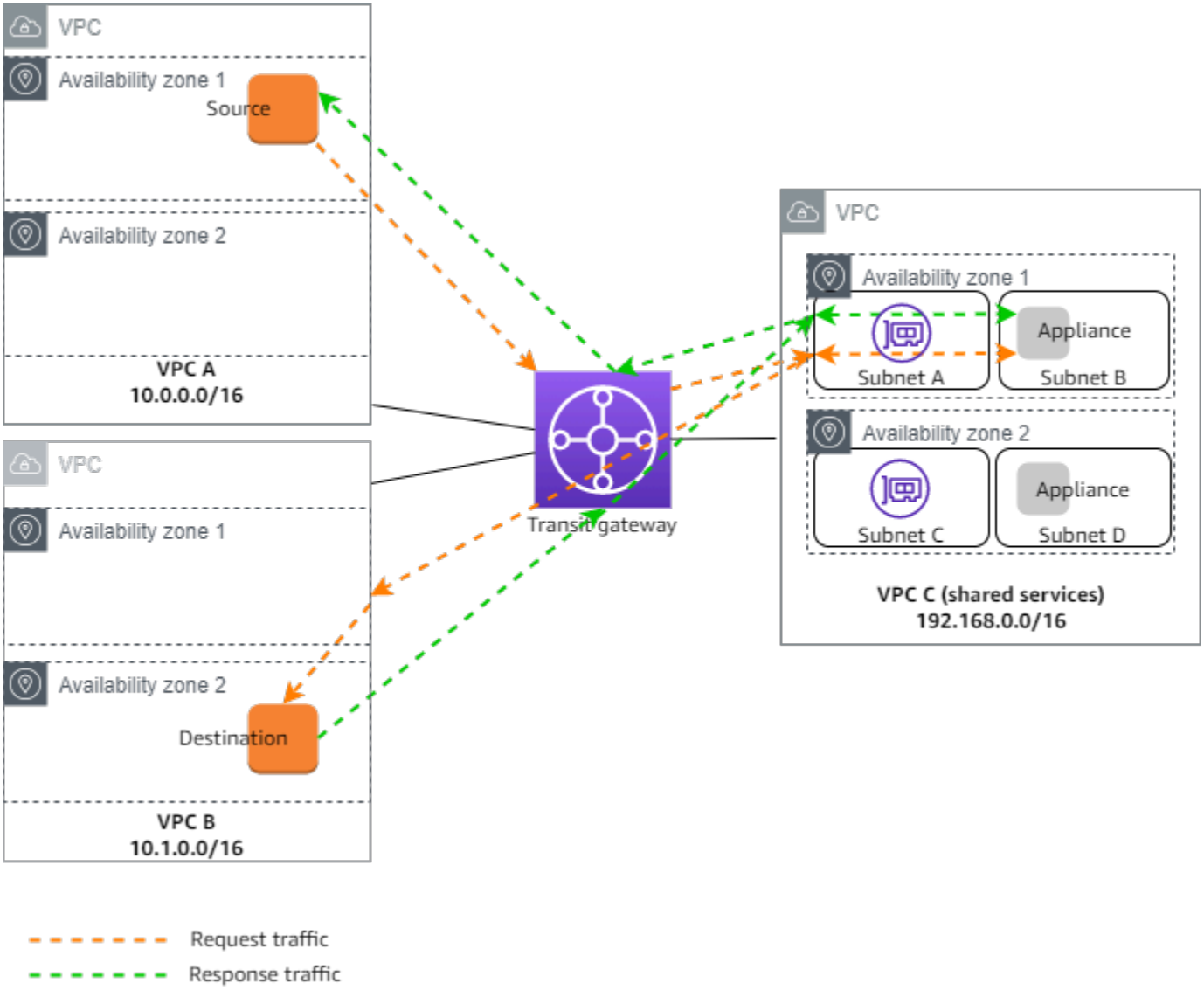
- Lalu lintas dalam mode alat dialihkan dengan benar selama lalu lintas sumber dan tujuan datang ke VPC terpusat (VPC Inspeksi) dari lampiran gateway transit yang sama. Lalu lintas dapat turun jika sumber dan tujuan masuk dari dua lampiran gateway transit yang berbeda. Mode alat tidak berlaku untuk lalu lintas yang memasuki jaringan melalui VPN.
- 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
- Peralatan stateful dan mode alat
- Perutean

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 tentang membuat VPC, lihat Membuat VPC di Panduan Pengguna Amazon Virtual Private Cloud.
- 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 gateway transit ke 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. AWS CloudFormation Misalnya, 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

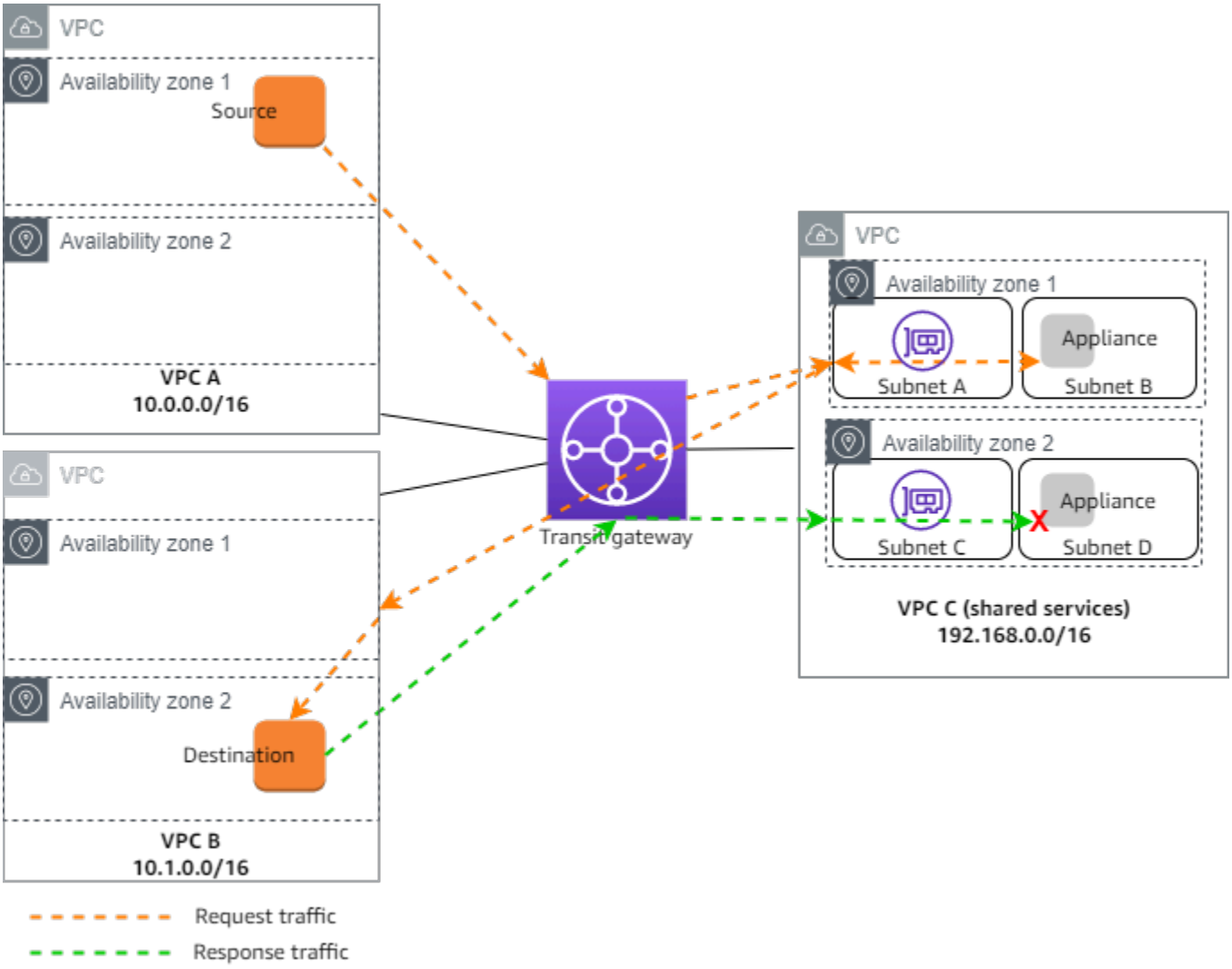
Jika lampiran VPC Anda menjangkau beberapa Availability Zone dan Anda memerlukan lalu lintas antara host sumber dan tujuan untuk dialihkan melalui alat yang sama untuk pemeriksaan stateful, aktifkan dukungan mode alat untuk lampiran VPC tempat alat berada.

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
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	appliance-eni-id

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

Tujuan	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.

Tujuan	Target	Jenis rute
0.0.0.0/0	*ID Lampiran untuk VPC C*	statis

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

Tujuan	Target	Jenis rute
10.0.0.0/16	*ID Lampiran untuk VPC A*	diperbanyak
10.1.0.0/16	*ID Lampiran untuk VPC B*	diperbanyak

Bekerja dengan gateway transit

Anda dapat bekerja dengan gateway transit menggunakan konsol VPC Amazon atau. AWS CLI

Daftar Isi

- Transit gateway
- Lampiran gateway transit ke VPC
- Lampiran Transit gateway VPN
- Lampiran gateway transit ke gateway Direct Connect
- Lampiran transit gateway peering
- Lampiran Transit Gateway Connect dan rekan Transit Gateway Connect
- Tabel rute transit gateway
- Tabel kebijakan gateway transit
- Multicast di gateway transit

Transit gateway

Gateway transit memungkinkan Anda untuk melampirkan koneksi VPC dan 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 melampirkan VPC mereka ke gateway transit Anda. Pengguna dari kedua akun dapat menghapus lampuran tersebut kapan saja.

Anda dapat mengaktifkan multicast pada gateway transit, lalu membuat domain multicast gateway transit yang mengizinkan 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 IPv4 atau IPv6 CIDR dan target. Targetnya adalah koneksi VPC dan 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 VPC pengembangan dengan satu tabel rute dan VPC produksi dengan tabel rute yang berbeda. Ini memungkinkan Anda untuk membuat jaringan terisolasi di dalam gateway transit yang mirip dengan virtual routing and forwarding (VRF) di jaringan tradisional.

Transit gateway mendukung perutean dinamis dan statis antara VPC terpasang dan koneksi VPN. Anda dapat mengaktifkan atau menonaktifkan propagasi rute untuk setiap lampiran. Lampiran peering gateway transit hanya mendukung perutean statis. Namun, Anda tidak dapat menambahkan rute statis yang menunjuk ke peering antara dua gateway transit di Wilayah yang sama.

Anda dapat secara opsional mengaitkan satu atau lebih blok CIDR IPv4 atau IPv6 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 blok IPv4 dan IPv6 CIDR, lihat VPC dan subnet di Panduan Pengguna Amazon VPC.

Tugas

- Membuat transit gateway
- Lihat gateway transit Anda
- Menambahkan atau mengedit tag untuk gateway transit
- Ubah gateway transit
- Bagikan gateway transit
- Terima pembagian sumber daya
- Terima lampiran bersama
- Hapus gateway transit

Membuat 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???.

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 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, atribut BGP seperti AS-path, dan komunitas untuk preferensi harus sama.

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

9. Untuk asosiasi tabel rute default, pilih opsi ini untuk secara otomatis mengaitkan lampiran gateway transit dengan tabel rute default untuk gateway transit.
10. Untuk propagasi tabel rute default, pilih opsi ini untuk secara otomatis menyebarkan lampiran gateway transit ke tabel rute default untuk gateway transit.
11. (Opsional) Untuk menggunakan gateway transit sebagai router untuk lalu lintas multicast, pilih Dukungan multicast.
12. Untuk Auto accept shared attachment, pilih opsi ini untuk secara otomatis menerima lampiran lintas akun.
13. (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 alamat dalam rentang 169.254.0.0/16, dan rentang yang tumpang tindih dengan alamat untuk lampiran VPC dan jaringan lokal.
14. Pilih Buat gateway transit.

Untuk membuat gateway transit menggunakan AWS CLI

Gunakan perintah create-transit-gateway.

Lihat gateway transit Anda

Untuk melihat gateway transit Anda menggunakan konsol

1. Buka konsol Amazon VPC 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 Anda menggunakan AWS CLI

Gunakan perintah describe-transit-gateways.

Menambahkan atau mengedit tag untuk gateway transit

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 Sumber Daya Amazon EC2 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 akan ditambahkan atau diedit 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

Anda dapat memodifikasi opsi konfigurasi untuk gateway transit Anda. Saat Anda memodifikasi gateway transit, opsi yang dimodifikasi hanya diterapkan ke lampiran gateway transit baru. Lampiran gateway transit Anda yang ada tidak dimodifikasi dan tidak melihat 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.

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.

Bagikan gateway transit

Anda dapat menggunakan AWS RAM untuk berbagi gateway transit di seluruh akun atau di seluruh organisasi Anda di AWS Organizations. Gunakan prosedur berikut untuk berbagi gateway transit yang Anda miliki.

Anda harus mengaktifkan pembagian sumber daya dari akun pengelolaan organisasi Anda. Untuk informasi tentang mengaktifkan berbagi sumber daya, lihat Mengaktifkan Berbagi dengan AWS Organizations di Panduan AWS RAM Pengguna.

Untuk berbagi gateway transit

1. Buka AWS RAM konsol di https://console.aws.amazon.com/ram/.
2. Pilih Buat berbagi sumber daya.
3. Di bawah Nama, ketik nama deskriptif untuk berbagi sumber daya.
4. Untuk Pilih jenis sumber daya, pilih Gateway Transit. Pilih gateway transit.
5. (Opsional) Untuk Prinsipal, tambahkan prinsipal ke pembagian sumber daya. Untuk masing-masing Akun AWS, OU, atau organisasi, tentukan ID-nya dan pilih Tambah.

   Untuk Izinkan akun eksternal, pilih apakah akan mengizinkan berbagi sumber daya ini dengan Akun AWS yang berada di luar organisasi Anda.
6. (Opsional) Di bawah Tag, ketikkan kunci tag dan pasangan nilai tag untuk setiap tag. Tag ini diterapkan pada pembagian sumber daya tetapi tidak ke gateway transit.
7. Pilih Buat berbagi sumber daya.

Terima pembagian sumber daya

Jika Anda ditambahkan ke pembagian sumber daya, Anda menerima undangan untuk bergabung dengan pembagian sumber daya. Anda harus menerima pembagian sumber daya sebelum dapat mengakses sumber daya bersama.

Untuk menerima pembagian sumber daya

1. Buka AWS RAM konsol di https://console.aws.amazon.com/ram/.
2. Pada 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.

Terima lampiran bersama

Jika Anda tidak mengaktifkan fungsionalitas Auto accept shared attachment saat membuat gateway transit, Anda harus menerima lampiran lintas akun (bersama) secara manual.

Untuk menerima lampiran bersama secara manual

1. Buka konsol Amazon VPC 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.

Hapus gateway transit

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.

Lampiran gateway transit ke 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. Menentukan satu subnet dari Availability Zone memungkinkan lalu lintas untuk mencapai sumber daya di setiap subnet di Availability Zone tersebut.

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. 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.
- Sumber daya dalam VPC yang dilampirkan ke gateway transit tidak dapat mengakses grup keamanan dari VPC yang berbeda yang juga dilampirkan ke gateway transit yang sama.
- Gateway transit tidak mendukung resolusi DNS untuk nama DNS kustom dari VPC terlampir yang disiapkan menggunakan zona host pribadi di Amazon Route 53. Untuk mengonfigurasi resolusi nama untuk zona host pribadi untuk semua VPC yang dilampirkan ke gateway transit, lihat Manajemen DNS terpusat dari cloud hybrid dengan Amazon Route 53 dan Transit Gateway AWS.
- Gateway transit tidak mendukung perutean antara VPC dengan CIDR yang identik. Jika Anda melampirkan VPC ke gateway transit dan CIDR-nya identik 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 khusus IPv6. Subnet lampiran gateway transit juga harus mendukung alamat IPv4.
- Gateway transit harus memiliki setidaknya satu lampiran VPC sebelum gateway transit dapat ditambahkan ke tabel rute.

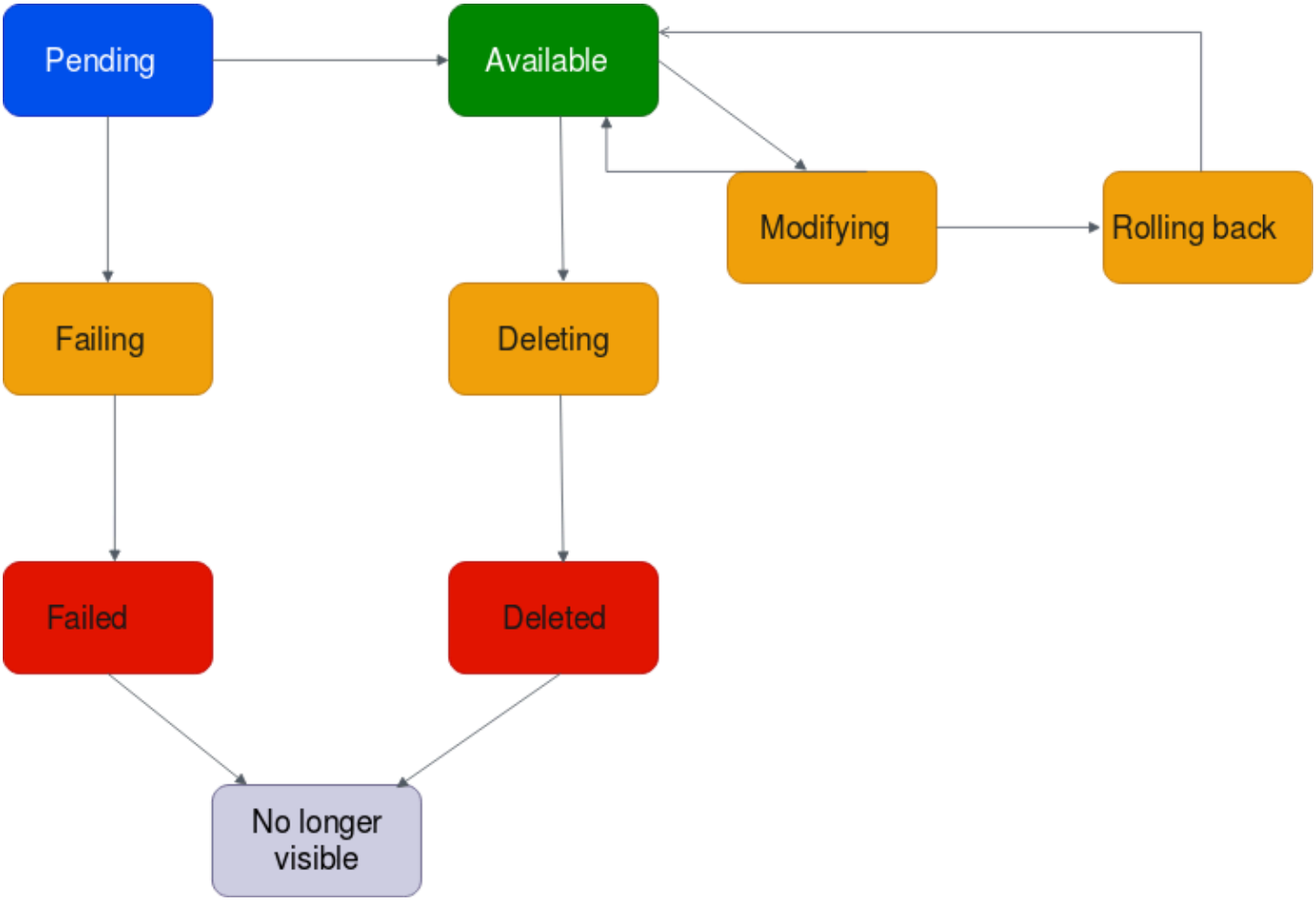
Daftar Isi

- Siklus hidup lampiran VPC
- Buat lampiran gateway transit ke VPC
- Ubah lampiran VPC Anda
- Ubah tag lampiran VPC Anda
- Lihat lampiran VPC Anda
- Hapus lampiran VPC
- Memecahkan masalah pembuatan lampiran VPC

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.

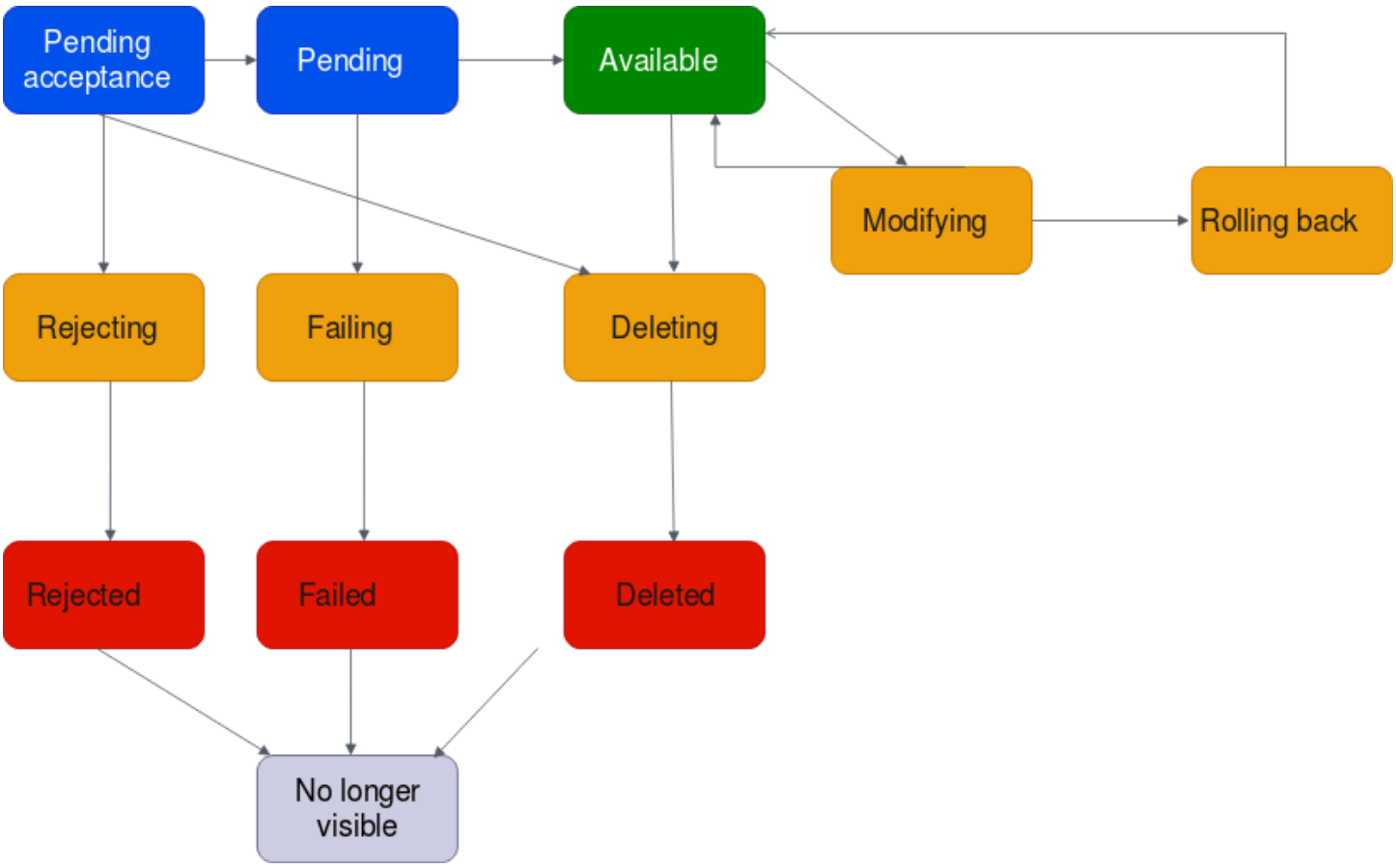
Diagram berikut menunjukkan status yang dapat dilalui lampiran dalam satu konfigurasi akun, atau konfigurasi lintas akun yang mengaktifkan Auto accept shared attachment.



- 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 ke `available`.

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`, `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`.

Buat lampiran gateway transit ke VPC

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 DNS, Dukungan IPv6, dan dukungan mode 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. Untuk ID VPC, pilih VPC yang dilampirkan pada transit gateway.

   VPC ini harus memiliki setidaknya satu subnet yang terkait dengannya.

9. Untuk ID Subnet, 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.

Untuk membuat lampiran VPC menggunakan AWS CLI

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

Ubah lampiran VPC Anda

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. Untuk mengaktifkan dukungan DNS, pilih dukungan DNS.
5. Untuk menambahkan subnet ke lampiran, di sebelah subnet, pilih kotak.

   Menambahkan atau memodifikasi subnet lampiran VPC dapat memengaruhi lalu lintas data saat lampiran dalam keadaan modifikasi.
6. Pilih Ubah lampiran gateway transit.

Untuk memodifikasi lampiran VPC Anda menggunakan AWS CLI

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

Ubah tag lampiran VPC Anda

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 Anda

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.

Hapus lampiran VPC

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.

Memecahkan masalah pembuatan lampiran VPC

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 AWS 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 melalui konsol atau API. Untuk informasi selengkapnya, lihat the section called “Buat lampiran gateway transit ke VPC”.
3. Verifikasi bahwa peran terkait layanan memiliki izin yang benar. Untuk informasi selengkapnya, lihat the section called “Transit Gateway”.
4. Verifikasi bahwa gateway transit berada di `available` negara bagian. Untuk informasi selengkapnya, lihat the section called “Lihat gateway transit Anda”.

Lampiran Transit gateway VPN

Untuk melampirkan koneksi VPN ke gateway transit Anda, Anda harus menentukan gateway pelanggan. Untuk informasi selengkapnya tentang persyaratan untuk perangkat gateway pelanggan,

lihat Persyaratan untuk perangkat gateway pelanggan Anda di Panduan AWS Site-to-Site VPN Pengguna.

Untuk VPN statis, tambahkan rute statis ke tabel rute gateway transit.

Buat lampiran gateway transit ke VPN

Untuk membuat lampiran VPN menggunakan konsol tersebut

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.
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 translasi alamat jaringan (NAT) yang telah diaktifkan untuk NAT traversal (NAT-T), maka gunakan alamat IP publik perangkat NAT Anda, dan sesuaikan aturan firewall Anda untuk membuka blokir UDP port 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 VPN Site-to-Site di Panduan Pengguna.AWS Site-to-Site VPN
7. Untuk Opsi Tunnel, masukkan rentang CIDR dan kunci yang telah dibagikan sebelumnya untuk terowongan Anda. Untuk informasi selengkapnya, lihat Arsitektur VPN Site-to-Site.
8. Pilih Buat lampiran gateway transit.

Untuk membuat lampiran VPN menggunakan AWS CLI

Gunakan perintah create-vpn-connection.

Lihat lampiran VPN Anda

Untuk melihat lampiran VPN 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 VPN. Ini adalah lampiran VPN.
4. Pilih lampiran untuk melihat detailnya atau menambahkan tag.

Untuk melihat lampiran VPN Anda menggunakan AWS CLI

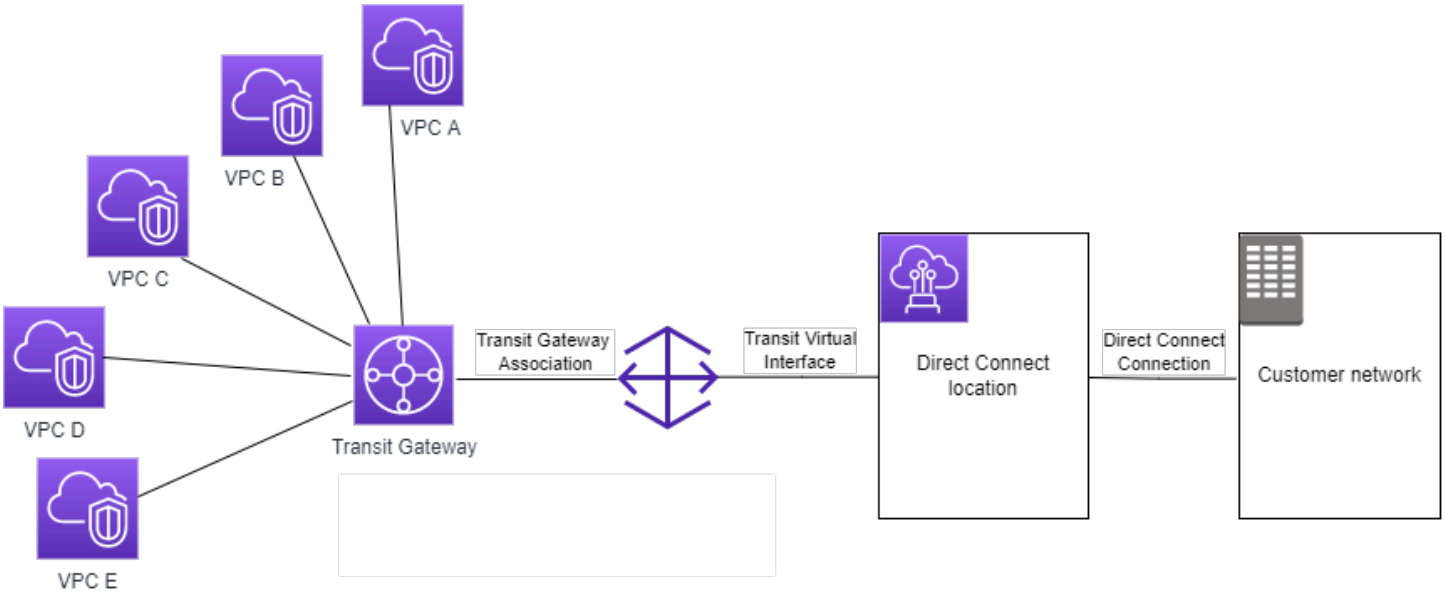
Gunakan perintah describe-transit-gateway-attachments.

Lampiran gateway transit ke gateway Direct Connect

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

- Mengelola satu koneksi untuk beberapa VPC atau VPN yang berada di Wilayah yang sama.
- Mengiklankan prefiks dari on-premise ke AWS dan dari AWSke on-premise.

Diagram berikut menggambarkan bagaimana gateway Direct Connect memungkinkan Anda membuat satu koneksi ke koneksi Direct Connect yang dapat digunakan oleh semua VPC Anda.



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 transit gateway peering

Anda dapat mengintip gateway transit intra-wilayah dan antar wilayah, dan merutekan lalu lintas di antara mereka, yang mencakup lalu lintas IPv4 dan IPv6. Untuk melakukan ini, buat lampiran peering di gateway transit Anda, dan tentukan gateway transit. Transit gateway peer dapat berada di akun Anda atau Akun AWS berbeda.

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 ASN unik untuk setiap gateway transit peered untuk memanfaatkan kemampuan propagasi rute masa depan.

Transit gateway peering tidak mendukung penyelesaian nama host DNS IPv4 publik atau pribadi ke alamat IPv4 pribadi di seluruh VPC di kedua 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 FAQ AWSTransit Gateways.

Buat lampiran peering

Sebelum Anda mulai, pastikan Anda memiliki ID gateway transit yang ingin Anda lampirkan. Jika gateway transit ada di gerbang lainAkun AWS, pastikan Anda memiliki Akun AWS ID pemilik gateway transit.

Setelah Anda membuat lampiran peering, pemilik transit gateway penerima harus menerima 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 atau gateway transit yang dibagikan dengan Anda.
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 berbedaAkun 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

Untuk mengaktifkan lampiran peering, pemilik gateway transit penerima harus menerima permintaan lampiran peering. Ini diperlukan bahkan jika kedua gateway transit berada di akun yang sama. Lampiran mengintip harus di `pendingAcceptance` negara bagian. Terima permintaan lampiran peering dari Wilayah tempat gateway transit penerima berada.

Atau, Anda dapat menolak permintaan koneksi peering apa pun yang Anda terima yang ada di negara bagian`pendingAcceptance`. 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

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 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. 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, kaitkan tabel rute gateway transit dengan lampiran peering gateway transit. Untuk informasi selengkapnya, lihat the section called “Kaitkan tabel rute gateway transit”.

Lihat lampiran koneksi peering gateway transit Anda

Anda dapat melihat lampiran peering gateway transit Anda dan informasi tentang mereka.

Untuk melihat lampiran peering 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 Peering. Ini adalah lampiran mengintip.
4. Pilih lampiran untuk melihat detailnya.

Untuk melihat lampiran peering gateway transit Anda menggunakan AWS CLI

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

Hapus lampiran peering

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.

Pertimbangan Keikutsertaan AWS Wilayah

Anda dapat mengintip gateway transit melintasi batas Wilayah keikutsertaan. Untuk informasi tentang Wilayah ini, dan cara ikut serta, lihat Mengelola AWS Wilayah di Referensi Umum Amazon Web. 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:
  - ID Akun AWS
  - 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.

Lampiran Transit Gateway Connect dan rekan Transit Gateway Connect

Anda dapat membuat lampiran Transit Gateway Connect untuk membuat koneksi antara gateway transit dan peralatan virtual pihak ketiga (seperti peralatan SD-WAN) 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 agar 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 untuk membuat integrasi ini, lihat Mengintegrasikan perangkat SD-WAN dengan AWS Transit Gateway dan. AWS Direct Connect

Daftar Isi

- Connect rekan-rekan
- Persyaratan dan pertimbangan
- Membuat lampiran Connect
- Buat rekan Connect (terowongan GRE)
- Melihat lampiran Connect dan Connect peer
- Ubah lampiran Connect dan Connect peer tag
- Hapus rekan Connect
- Menghapus lampiran Connect

Connect rekan-rekan

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.

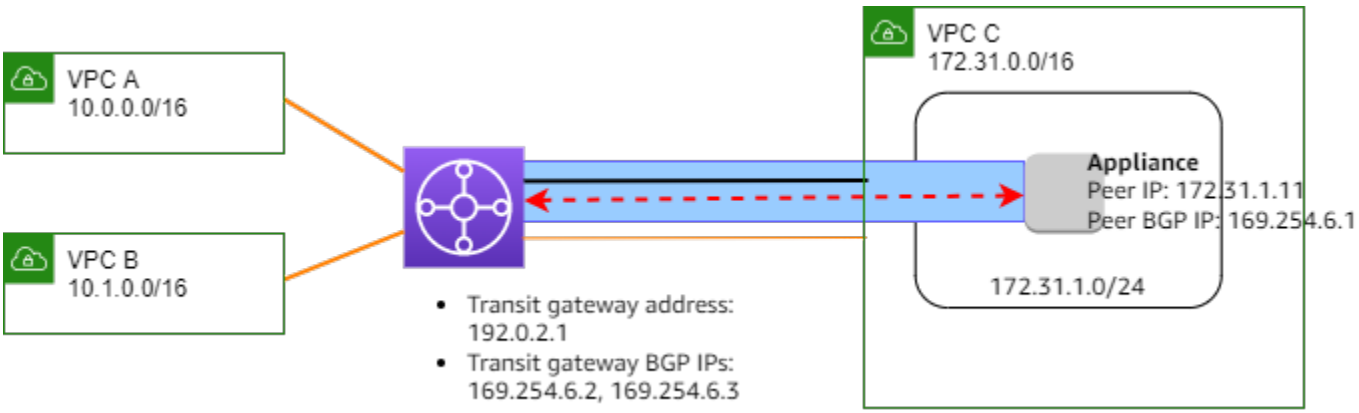
Anda dapat menambahkan blok CIDR gateway transit saat membuat atau memodifikasi gateway transit.

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.

Tujuan	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 AWSTransit 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 mengkonfigurasi 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 rekan eBGP dan seharusnya telah dikonfigurasi. 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.
- Peering IPv6 BGP tidak didukung; hanya peering BGP berbasis IPv4 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.
- Rekan Connect menggunakan atribut BGP AS-PATH adalah rute yang disukai 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 AS-PATH yang sama. 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 di 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.
- Pastikan antarmuka eksternal alat pihak ketiga Anda (sumber terowongan) Unit Transmisi Maksimum (MTU)
  - cocok dengan MTU antarmuka terowongan GRE, atau
  - harus lebih besar dari antarmuka terowongan GRE.

Membuat lampiran Connect

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 (terowongan GRE)

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 dari 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 alamat IPv4 di dalam yang digunakan untuk peering BGP. Tentukan blok CIDR /29 dari rentang. `169.254.0.0/16`
8. (Opsional) Untuk blok BGP Inside CIDR IPv6, tentukan kisaran alamat IPv6 di dalam yang digunakan untuk peering 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.

Melihat lampiran Connect dan Connect peer

Anda dapat melihat lampiran Connect dan Connect peer.

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

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.

Hapus rekan Connect

Jika Anda tidak lagi membutuhkan Connect peer, 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

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 Amazon VPC 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 transit gateway

Gunakan tabel rute gateway transit untuk mengonfigurasi perutean untuk lampiran gateway transit Anda.

Buat tabel rute gateway transit

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

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

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

Untuk mengaitkan 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 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

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 dipisahkan 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.

Menyebarkan rute ke tabel rute gateway transit

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

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

Anda dapat membuat 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 VPN Site-to-Site. 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.

Hapus rute statis

Anda dapat menghapus rute statis dari tabel rute gateway transit.

Untuk menghapus 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 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

Anda dapat mengganti 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

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 Amazon VPC 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 di https://console.aws.amazon.com/s3/, 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

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.

Refiks daftar prefiks

Anda dapat mereferensikan daftar awalan di tabel rute gateway transit Anda. Sebuah daftar prefiks adalah satu set dari satu atau lebih entri blok CIDR. Sebuah daftar prefiks adalah satu set dari satu atau lebih entri blok CIDR. Anda dapat menggunakan daftar awalan untuk menyederhanakan pengelolaan alamat IP yang Anda referensi dalam sumber daya Anda untuk merutekan lalu lintas jaringan. Misalnya, jika Anda sering menentukan CIDR tujuan yang sama di beberapa tabel rute gateway transit, Anda dapat mengelola CIDR tersebut dalam daftar awalan tunggal, alih-alih berulang kali mereferensikan CIDR yang sama 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.

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

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

Membuat referensi daftar prefiks

Anda dapat membuat daftar prefiks ke daftar prefiks dalam tabel rute transit gateway.

Untuk membuat referensi daftar prefiks menggunakan konsol ini

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 transit gateway.
4. Pilih Tindakan, Buat referensi daftar awalan.
5. Untuk ID daftar prefiks, pilih ID dari daftar prefiks.
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 merutekan lalu lintas.
8. Memilih Buat referensi daftar awalan.

Untuk membuat referensi daftar prefiks menggunakanAWS CLI

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

Lihat referensi daftar prefiks Lihat referensi daftar prefiks Lihat

Anda dapat melihat referensi daftar awalan di tabel rute gateway transit Anda. Anda juga dapat melihat setiap entri dalam daftar awalan sebagai rute individual di tabel rute gateway transit Anda. Jenis rute untuk rute daftar awalan adalah`propagated`.

Untuk melihat referensi daftar prefiks menggunakan konsol ini

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 transit gateway.
4. Di panel bawah, pilih Referensi daftar awalan. Referensi daftar awalan tercantum.
5. Pilih Rute. Setiap entri daftar awalan terdaftar sebagai rute dalam tabel rute.

Untuk melihat referensi daftar awalan menggunakanAWS CLI

Gunakan perintah get-transit-gateway-prefix-list-references.

Memodifiks referensi daftar prefiks

Anda dapat memodifikasi referensi daftar awalan dengan mengubah lampiran yang dirutekan lalu lintas, atau menunjukkan apakah akan menjatuhkan lalu lintas yang cocok dengan rute.

Anda tidak dapat mengubah rute individu untuk daftar awalan di tab Rute. Untuk memodifikasi entri dalam daftar awalan, gunakan daftar awalan terkelola layar. Untuk informasi selengkapnya, lihat Memodifikasi daftar awalan di Panduan Pengguna Amazon VPC.

Untuk mengubah referensi daftar prefiks menggunakan konsol ini

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 transit gateway.
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 merutekan lalu lintas.
8. Pilih Ubah referensi daftar awalan.

Untuk mengubah referensi daftar prefiks menggunakanAWS CLI

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

Menghapus referensi daftar prefiks

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

Untuk menghapus referensi daftar prefiks menggunakan konsol ini

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 transit gateway.
4. Pilih referensi daftar awalan, dan pilih Hapus referensi.
5. Pilih Hapus referensi.

Untuk menghapus referensi daftar prefiks menggunakanAWS CLI

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

Tabel kebijakan gateway transit

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.

Membuat tabel kebijakan gateway transit

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

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 gateway transit

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 VPC yang terpasang, dan berfungsi sebagai router multicast untuk instance pengiriman lalu lintas yang ditujukan untuk beberapa instance penerima.

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 ditentukan oleh antarmuka jaringan elastis individu yang melekat pada instans 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 protokol IGMPv2 dan domain multicast keanggotaan grup IGMP dan statis (berbasis API).

- Sumber multicast — Sebuah elastic network interface yang terkait dengan instans EC2 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 instans EC2 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

- Untuk informasi tentang Wilayah yang didukung, lihat FAQ AWS Transit Gateway.
- 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 pemeriksaan Source/Dest. Untuk informasi tentang menonaktifkan pemeriksaan, lihat Mengubah pemeriksaan sumber atau tujuan di Panduan Pengguna Amazon EC2 untuk Instans Linux.
- Instance non-Nitro tidak bisa menjadi pengirim multicast.
- Perutean multicast tidak didukung melalui, AWS 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 JOIN pesan IGMPv2 oleh gateway transit dan diakhiri dengan penerimaan pesan LEAVE IGMPv2. Gerbang transit melacak host yang berhasil bergabung dengan grup. Sebagai router multicast cloud, gateway transit mengeluarkan QUERY pesan IGMPv2 ke semua anggota setiap dua menit. Setiap anggota mengirimkan JOIN pesan IGMPv2 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. LEAVEPesan IGMPv2 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 konfigurasi ACL 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, Amazon VPC Transit Gateways secara otomatis menghapus grup statis dan sumber untuk ENI yang sudah tidak ada lagi. Ini dilakukan dengan secara berkala mengasumsikan peran terkait layanan Transit Gateway untuk menggambarkan ENI di akun.
- Hanya multicast statis yang mendukung IPv6. Multicast dinamis tidak.

Multicast dengan Windows Server

Anda harus melakukan langkah-langkah tambahan saat menyiapkan multicast untuk bekerja dengan gateway transit di Windows Server 2019 atau 2022. Menggunakan PowerShell, jalankan perintah berikut:

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

```
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 instance EC2.
5. Uji aplikasi multicast Anda untuk memastikan lalu lintas mengalir seperti yang diharapkan.

Perutean multicast

Saat 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.

ACL jaringan

Aturan ACL jaringan beroperasi pada tingkat subnet. Mereka berlaku untuk lalu lintas multicast, karena gateway transit berada di luar subnet. Untuk informasi lebih lanjut, lihatACL jaringandi dalamPanduan Pengguna Amazon VPC.

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

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

Berikut ini adalah aturan keluar minimum untuk IGMP.

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

Grup keamanan

Aturan grup keamanan beroperasi di tingkat instans. Mereka dapat diterapkan pada lalu lintas multicast masuk dan keluar. Perilakunya sama dengan lalu lintas unicast. Untuk semua instans anggota grup, Anda harus mengizinkan lalu lintas masuk dari sumber grup. Untuk informasi lebih lanjut, lihatGrup keamanandi dalamPanduan Pengguna Amazon VPC.

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

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

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

Tipe	Protokol	Tujuan	Deskripsi
Protokol Kustom	2	224.0.0.2/32	Cuti IGMP
Protokol Kustom	2	Alamat IP grup multicast	IGMP bergabung

Tipe	Protokol	Tujuan	Deskripsi
Protokol UDP Khusus	UDP	Alamat IP grup multicast	Lalu lintas multicast keluar

Bekerja dengan multicast

Anda dapat mengonfigurasi multicast di gateway transit menggunakan konsol VPC Amazon atau. AWS CLI

Sebelum Anda membuat domain multicast, Anda perlu tahu apakah host Anda menggunakan protokol Internet Group Management Protocol (IGMP) untuk lalu lintas multicast.

Daftar Isi

- Atribut domain multicast
- Mengelola konfigurasi IGMP
- Mengelola konfigurasi sumber statis
- Mengelola konfigurasi anggota grup statis
- Mengelola domain multicast
- Mengelola grup multicast
- Bekerja dengan domain multicast bersama

Atribut domain multicast

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

Atribut	Deskripsi
`Igmpv2Support` (AWS CLI) Dukungan IGMPv2 (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.

Atribut	Deskripsi
	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. • 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.

Mengelola konfigurasi IGMP

Ketika Anda memiliki 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 tentang membuat VPC, lihat Membuat VPC di Panduan Pengguna Amazon VPC.
2. Buat subnet di VPC. Untuk informasi selengkapnya tentang membuat subnet, lihat Membuat subnet di VPC Anda 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 gateway transit ke VPC”.
5. Buat domain multicast yang dikonfigurasi untuk dukungan IGMP. Untuk informasi selengkapnya, lihat the section called “Membuat domain multicast IGMP”.

   Gunakan pengaturan berikut:

   - Aktifkan dukungan IGMPv2.
   - Nonaktifkan dukungan sumber statis.
6. Buat asosiasi antara subnet di lampiran VPC gateway transit dan domain multicast. Untuk 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. Untuk informasi selengkapnya, lihat the section called “Mendaftarkan anggota dengan grup multicast”.

Mengelola konfigurasi sumber statis

Dalam konfigurasi ini, Anda perlu menambahkan sumber multicast secara statis dalam 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 tentang membuat VPC, lihat Membuat VPC di Panduan Pengguna Amazon VPC.
2. Buat subnet di VPC. Untuk informasi selengkapnya tentang membuat subnet, lihat Membuat subnet di VPC Anda 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 gateway transit ke VPC”.
5. Buat domain multicast yang dikonfigurasi tanpa dukungan IGMP, dan dukungan untuk menambahkan sumber secara statis. Untuk informasi selengkapnya, lihat the section called “Membuat domain multicast sumber statis”.

   Gunakan pengaturan berikut:

   - Nonaktifkan dukungan IGMPv2.
   - 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 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 “Mendaftarkan sumber dengan grup multicast”.
8. Tambahkan anggota ke grup multicast. Untuk informasi selengkapnya, lihat the section called “Mendaftarkan anggota dengan grup multicast”.

Mengelola konfigurasi anggota grup statis

Dalam konfigurasi ini, Anda perlu menambahkan anggota multicast secara statis 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 tentang membuat VPC, lihat Membuat VPC di Panduan Pengguna Amazon VPC.
2. Buat subnet di VPC. Untuk informasi selengkapnya tentang membuat subnet, lihat Membuat subnet di VPC Anda 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 gateway transit ke VPC”.
5. Buat domain multicast yang dikonfigurasi tanpa dukungan IGMP, dan dukungan untuk menambahkan sumber secara statis. Untuk informasi selengkapnya, lihat the section called “Membuat domain multicast sumber statis”.

   Gunakan pengaturan berikut:

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

Mengelola domain multicast

Untuk mulai menggunakan multicast dengan gateway transit, buat domain multicast, dan kemudian kaitkan subnet dengan domain tersebut.

Daftar Isi

- Membuat domain multicast IGMP
- Membuat domain multicast sumber statis
- Mengaitkan lampiran dan subnet VPC dengan domain multicast
- Melihat asosiasi domain multicast Anda
- Memutuskan subnet dari domain multicast

- Menambahkan tag ke domain multicast
- Menghapus domain multicast

Membuat domain multicast IGMP

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

Console

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 dukungan IGMPv2, 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.

Command line

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
```

Membuat domain multicast sumber statis

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

Console

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 dukungan IGMPv2, 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.

Command line

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

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 gateway transit ke VPC.

Console

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.

Command line

Untuk mengaitkan lampiran VPC dengan domain multicast menggunakan AWS CLI

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

Melihat asosiasi domain multicast Anda

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

Console

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.

Command line

Untuk melihat domain multicast menggunakan AWS CLI

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

Memutuskan subnet dari domain multicast

Gunakan prosedur berikut untuk memisahkan subnet dari domain multicast.

Console

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.

Command line

Untuk memisahkan subnet menggunakan AWS CLI

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

Menambahkan tag ke domain multicast

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 Sumber Daya Amazon EC2 Anda.

Console

Untuk menambahkan tag ke 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 Tindakan, Kelola tag.
5. Untuk setiap tag, pilih Tambahkan tag baru dan masukkan Kunci dan Nilai untuk tag.
6. Pilih Simpan.

Command line

Untuk menambahkan tag ke domain multicast menggunakan AWS CLI

Gunakan perintah create-tags.

Menghapus domain multicast

Gunakan prosedur berikut untuk menghapus domain multicast.

Console

Untuk menghapus 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, Delete multicast domain.
4. Saat diminta konfirmasi, masukkan **`delete`**, lalu pilih Hapus.

Command line

Untuk menghapus domain multicast menggunakan AWS CLI

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

Mengelola grup multicast

Daftar Isi

- Mendaftarkan sumber dengan grup multicast
- Mendaftarkan anggota dengan grup multicast
- Menderegistrasi sumber dari grup multicast
- Membatalkan pendaftaran anggota dari grup multicast
- Melihat grup multicast Anda

Mendaftarkan sumber dengan grup multicast

> **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 dari domain multicast
- ID antarmuka jaringan sumber
- Alamat IP grup multicast

Console

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.

Command line

Untuk mendaftarkan sumber menggunakan AWS CLI

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

Mendaftarkan anggota dengan grup multicast

Gunakan prosedur berikut untuk mendaftarkan anggota grup dengan grup multicast.

Anda memerlukan informasi berikut sebelum menambahkan anggota:

- ID dari domain multicast
- ID antarmuka jaringan anggota grup
- Alamat IP grup multicast

Console

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.

Command line

Untuk mendaftarkan anggota menggunakan AWS CLI

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

Menderegistrasi sumber dari grup multicast

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

Console

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.

Command line

Untuk menghapus sumber menggunakan AWS CLI

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

Membatalkan pendaftaran anggota dari grup multicast

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

Console

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.

Command line

Untuk membatalkan pendaftaran anggota menggunakan AWS CLI

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

Melihat grup multicast Anda

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.

Console

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.

Command line

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"
        }
    ]
}
```

Bekerja dengan domain multicast bersama

Dengan berbagi domain multicast, pemilik domain multicast dapat berbagi domain denganAWS akun lain di dalam organisasinya atau di seluruh organisasiAWS Organizations. Sebagai pemilik domain multicast, Anda dapat membuat dan mengelola domain multicast secara terpusat. Konsumen dapat melakukan operasi berikut pada domain multicast bersama:

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

Pemilik domain multicast dapat berbagi domain multicast dengan:

- AWSakun di dalam organisasinya atau lintas organisasi diAWS Organizations
- Sebuah unit organisasi di dalam organisasi di AWS Organizations
- Seluruh organisasi di AWS Organizations
- AWSrekening di luarAWS Organizations.

  Untuk berbagi domain multicast denganAWS akun di luar Organisasi, Anda harus membuat berbagi sumber daya menggunakanAWS Resource Access Manager, dan kemudian memilih Izinkan berbagi dengan siapa pun saat memilih Prinsipal untuk berbagi domain multicast. Untuk informasi selengkapnya tentang cara membuat berbagi sumber daya, lihat Membuat berbagi sumber dayaAWS RAM di dalam PanduanAWS RAM Pengguna

Daftar Isi

- Prasyarat untuk membagikan domain multicast
- Layanan terkait
- Berbagi di seluruh Availability Zone
- Berbagi domain multicast
- Membatalkan berbagi domain multicast bersama
- Mengidentifikasi domain multicast bersama
- Izin domain multicast bersama
- Penagihan dan pengukuran
- Quotas

Prasyarat untuk membagikan domain multicast

- Untuk membagikan domain multicast, Anda harus memilikinya diAWS akun Anda. Anda tidak dapat membagikan domain multicast yang telah dibagikan dengan Anda.
- Untuk membagikan domain multicast dengan organisasi atau unit organisasi Anda diAWS Organizations, Anda harus mengaktifkan pembagian denganAWS Organizations. Untuk informasi

selengkapnya, lihat Mengaktifkan Berbagi denganAWS Organizations di PanduanAWS RAM Pengguna.

Layanan terkait

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

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

Berbagi di seluruh Availability Zone

Untuk memastikan bahwa sumber daya didistribusikan di seluruh Availability Zone untuk suatu Wilayah, kami secara independen memetakan Availability Zone ke nama untuk setiap akun. Hal ini dapat menyebabkan perbedaan penamaan Availability Zone di seluruh akun. Misalnya, Availability Zone `us-east-1a` untuk akun AWS Anda mungkin tidak memiliki lokasi yang sama karena `us-east-1a` untuk akun AWS lainnya.

Untuk mengidentifikasi lokasi domain multicast Anda yang terkait dengan akun Anda, Anda harus menggunakan ID Availability Zone (AZ ID). ID AZ adalah pengenal unik dan konsisten untuk Availability Zone di semua akun AWS. Misalnya, `use1-az1` adalah ID AZ untuk Wilayah `us-east-1` dan lokasinya sama di setiap akun AWS.

Untuk melihat ID AZ untuk Availability Zone di akun Anda

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

Berbagi domain multicast

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

- Mendaftar dan membatalkan pendaftaran anggota grup atau sumber grup
- Associate dan memisahkan subnet

Untuk membagikan domain multicast, Anda harus menambahkannya ke pembagian sumber daya. Berbagi sumber daya adalah sumber daya AWS RAM yang memungkinkan Anda berbagi sumber daya di seluruh akun AWS. Pembagian sumber daya menentukan sumber daya untuk dibagikan, dan konsumen dengan siapa mereka berbagi. Saat Anda berbagi domain multicast menggunakanAmazon 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 AWS RAMkonsol.

Jika Anda adalah bagian dari sebuah organisasi diAWS Organizations dan berbagi dalam organisasi Anda diaktifkan, maka 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 tersebut.

Anda dapat membagikan domain multicast yang Anda miliki menggunakanAmazon Virtual Private Cloud ConsoleAWS RAM konsol, atauAWS CLI.

Untuk membagikan domain multicast yang Anda miliki menggunakanAmazon Virtual Private Cloud Console

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

Untuk membagikan domain multicast yang Anda miliki menggunakanAWS RAM konsol

Lihat Membuat Berbagi Sumber Daya di Panduan Pengguna.AWS RAM

Untuk membagikan domain multicast yang Anda miliki menggunakanAWS CLI

Gunakan perintah create-resource-share.

Membatalkan berbagi domain multicast bersama

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

- Subnet konsumen dipisahkan dari domain multicast. Subnet tetap berada di akun konsumen.

- Sumber grup konsumen dan anggota grup dipisahkan dari domain multicast, dan kemudian dihapus dari akun konsumen.

Untuk membatalkan pembagian pembagian domain multicast, Anda harus menghapusnya dari pembagian sumber daya. Anda dapat melakukan ini dariAWS RAM konsol atauAWS CLI.

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

Untuk membatalkan pembagian pembagian domain multicast bersama yang Anda miliki menggunakanAmazon Virtual Private Cloud Console

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

Untuk membatalkan pembagian pembagian domain multicast bersama yang Anda miliki menggunakanAWS RAM konsol

Lihat Memperbarui Berbagi Sumber Daya di Panduan Pengguna.AWS RAM

Untuk membatalkan pembagian pembagian domain multicast bersama yang Anda miliki menggunakanAWS CLI

Gunakan perintah disassociate-resource-share.

Mengidentifikasi domain multicast bersama

Pemilik dan konsumen dapat mengidentifikasi domain multicast bersama menggunakanAmazon Virtual Private Cloud ConsoleAWS CLI

Untuk mengidentifikasi domain multicast bersama menggunakanAmazon Virtual Private Cloud Console

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

4. Pada halaman Detail Domain Multicast Transit, lihat ID Pemilik untuk mengidentifikasi IDAWS akun domain multicast.

Untuk mengidentifikasi domain multicast bersama menggunakanAWS CLI

Gunakan perintah describe-transit-gateway-multicast-domains. Perintah menampilkan domain multicast yang Anda miliki dan domain multicast yang dibagikan dengan Anda. `OwnerId`menampilkan IDAWS akun pemilik domain multicast.

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 menggunakanAWS Organizations untuk melihat, memodifikasi, dan menghapus sumber daya yang dibuat konsumen pada domain multicast bersama.

Izin untuk konsumen

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

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

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

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

Penagihan dan pengukuran

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

Quotas

Domain multicast bersama diperhitungkan dalam kuota domain multicast pemilik dan konsumen.

Pertimbangan berbagi gateway transit

Anda dapat menggunakanAWSResource Access Manager (RAM) untuk berbagi gateway transit untuk lampiran VPC di seluruh akun atau di seluruh organisasiAWS Organizations. RAM harus diaktifkan dan sumber daya dibagikan dengan organisasi. Untuk informasi lebih lanjut, lihatAktifkan berbagi sumber daya denganAWS OrganizationsdiAWS RAMPanduan Pengguna.

Pertimbangkan hal berikut ketika Anda ingin berbagi gateway transit.

- SebuahAWS Site-to-Site VPNlampiran harus dibuat dalam hal yang samaAWSakun yang memiliki gateway transit.
- Lampiran ke gateway Direct Connect menggunakan asosiasi gateway transit dan dapat berada di jalur yang samaAWSakun sebagai gateway Direct Connect, atau yang berbeda dari gateway Direct Connect.

Secara default, pengguna tidak memiliki izin untuk membuat atau memodifikasiAWS RAMsumber 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-timur-1 dan memetakan ke lokasi yang sama di setiapAWSakun.

Batalkan pembagian 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 yang lainAWSakun, atau jikaAWSakun 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 lebih lanjut, lihatBagikan VPC Anda dengan akun laindiPanduan Pengguna Amazon VPC.

Mencatat lalu lintas jaringan menggunakan Log Aliran Transit Gateway

Transit Gateway Flow Logs adalah fitur 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, atau 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. Untuk informasi selengkapnya, lihat Membuat log alur.

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 log alur.

Daftar Isi

- Catatan Log Aliran Transit Gateway
- Harga Log Aliran Transit Gateway
- Buat log alur yang diterbitkan ke CloudWatch Log
- Membuat log alur yang menerbitkan ke Amazon S3
- Publikasikan log aliran ke Firehose
- Bekerja dengan Log Aliran Transit Gateway

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
- Format kustom
- Bidang yang tersedia

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. Ini bisa TransitGateway atauTransitGatewayAttachment.	6

Bidang	Deskripsi	Versi
	Jenis data parket: STRING	
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. Jenis data parket: STRING	6
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

Bidang	Deskripsi	Versi
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
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_64	2

Bidang	Deskripsi	Versi
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
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 untuk Instans Linux. Jenis data parket: STRING	3

Bidang	Deskripsi	Versi
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 kedaluwarsa. 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 pendek, bendera mungkin diatur pada baris yang sama dalam catatan log alur, misalnya, 19 untuk SYN-ACK dan FIN, dan 3 untuk SYN dan FIN. 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 antarmuka di mana lalu lintas ditangkap. 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_HEALTHCHECKS | 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

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.

Buat log alur yang diterbitkan ke CloudWatch Log

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

- Peran IAM untuk menerbitkan log alur ke CloudWatch Log
- Izin bagi pengguna IAM untuk meneruskan peran
- Buat log alur yang diterbitkan ke CloudWatch Log
- Proses catatan log alur di CloudWatch Log

Peran IAM untuk menerbitkan log alur ke CloudWatch Log

Peran IAM yang terkait dengan log alur Anda harus memiliki izin yang cukup untuk 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.

```
{
  "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.

```
{
  "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"
    }
}
```

Membuat atau memperbarui peran IAM untuk log alur

Anda dapat memperbarui peran yang ada atau menggunakan prosedur berikut untuk membuat peran baru untuk digunakan dengan log alur.

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, buka, dan buat halaman masukkan nama untuk peran Anda dan secara opsional berikan Deskripsi. 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.

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.

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

Buat log alur yang diterbitkan ke CloudWatch Log

Anda dapat membuat log 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.

Untuk membuat log aliran gateway transit menggunakan konsol

1. Masuk ke AWS Management Console 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-EC2FlowLogs (AWS Tools for Windows PowerShell)

- CreateFlowLogs (Amazon EC2 Query API)

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
```

Proses catatan log alur di CloudWatch Log

Anda dapat bekerja dengan catatan log alur seperti yang Anda lakukan dengan peristiwa log lainnya yang dikumpulkan oleh CloudWatch Log. Untuk informasi selengkapnya tentang memantau data log dan filter metrik, lihat Mencari dan Memfilter Data Log di Panduan CloudWatch Pengguna Amazon.

Contoh: Membuat filter CloudWatch metrik dan alarm untuk log aliran

Dalam contoh ini, Anda memiliki log alur untuk `eni-1a2b3c4d`. Anda ingin membuat alarm yang memperingatkan Anda jika ada 10 percobaan penolakan atau lebih untuk terkoneksi ke instans Anda melalui TCP port 22 (SSH) dalam jangka waktu 1 jam. Pertama, Anda harus membuat filter metrik yang sesuai dengan pola lalu lintas yang untuknya harus membuat alarm. Setelah itu, Anda dapat membuat alarm untuk filter metrik.

Untuk membuat filter metrik untuk lalu lintas SSH yang ditolak dan membuat alarm untuk filter

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, pilih Log, Grup log.
3. Pilih kotak centang untuk grup log, lalu pilih Tindakan, Buat filter metrik.
4. Untuk Pola Filter, masukkan 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 ke 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.

Membuat log alur yang menerbitkan ke Amazon S3

Arus log dapat menerbitkan data log alur ke Amazon S3.

Ketika menerbitkan ke Amazon S3, data log alur diterbitkan ke bucket Amazon S3 yang ada yang Anda tentukan. Catatan log 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 Layanan Penyimpanan Sederhana Amazon.

Untuk informasi selengkapnya tentang pencatatan beberapa akun, lihat Pencatatan Pusat dalam Perpustakaan Solusi AWS .

Untuk informasi selengkapnya tentang CloudWatch Log, lihat Log yang dikirim ke Amazon S3 di Panduan Pengguna Amazon CloudWatch Logs.

Daftar Isi

- Berkas log alur
- Kebijakan IAM untuk prinsipal IAM yang menerbitkan log alur ke Amazon S3
- Izin bucket Amazon S3 untuk log alur
- Kebijakan kunci yang diperlukan untuk digunakan dengan SSE-KMS
- Izin file berkas log Amazon S3
- Membuat log alur yang menerbitkan ke Amazon S3
- Catatan log alur proses di Amazon S3

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 berkas 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 di16:20 UTC. File berisi catatan log aliran dengan waktu akhir antara 16:20:00 dan16:24:59.

```
123456789012_vpcflowlogs_us-east-1_fl-1234abcd_20180620T1620Z_fe123456.log.gz
```

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.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
        ],
      "Resource": "*"
    }
  ]
}
```

Izin bucket Amazon S3 untuk log alur

Objek dan bucket Amazon S3 secara default bersifat privat. Hanya pemilik bucket yang bisa mengakses bucket dan objek yang tersimpan di dalamnya. Namun, pemilik bucket dapat memberikan akses kepada sumber daya dan pengguna lain dengan menulis kebijakan akses.

Jika pengguna yang membuat log alur memiliki bucket `PutBucketPolicy` dan memiliki serta `GetBucketPolicy` izin untuk bucket, kami secara otomatis melampirkan kebijakan berikut ke bucket. Kebijakan ini akan menggantikan kebijakan yang sebelumnya sudah melekat pada bucket.

Jika tidak, pemilik bucket harus menambahkan kebijakan ini ke bucket, menentukan Akun AWS ID pembuat log aliran, atau pembuatan log alur gagal. Untuk informasi selengkapnya, lihat Menggunakan kebijakan bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

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

```
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:account_id:*"
                }
            }
        }
    ]
}
```

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

- Awalan default

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

- Awalan S3 yang kompatibel dengan HIVE

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

Sebagai praktik terbaik, sebaiknya Anda memberikan izin ini kepada prinsipal layanan pengiriman log, bukan Akun AWS ARN individual. Ini juga merupakan praktik terbaik untuk menggunakan kunci `aws:SourceAccount` dan `aws:SourceArn` kondisi untuk melindungi dari masalah wakil yang membingungkan. Akun sumber adalah pemilik log aliran dan sumber ARN adalah ARN wildcard (*) dari layanan log.

Kebijakan kunci yang diperlukan untuk digunakan dengan SSE-KMS

Anda dapat melindungi data di bucket Amazon S3 dengan mengaktifkan Enkripsi Sisi Server dengan Amazon S3-Managed Keys (SSE-S3) atau Enkripsi Sisi Server dengan Kunci KMS (SSE-KMS). 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 yang dikelola 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.

```
{
    "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 (ACL) untuk mengelola akses ke berkas log yang dibuat oleh log alur. Secara default, pemilik bucket memiliki izin `FULL_CONTROL` pada setiap file berkas log. Pemilik pengiriman log, jika berbeda dari pemilik bucket, tidak memiliki izin. Akun pengiriman log memiliki izin `READ` dan `WRITE`. Untuk informasi selengkapnya, lihat Ikhtisar Daftar Kontrol Akses (ACL) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Membuat log alur yang menerbitkan ke Amazon S3

Setelah membuat dan mengonfigurasi bucket Amazon S3, Anda dapat membuat log aliran untuk gateway transit.

Untuk membuat log aliran gateway transit yang diterbitkan ke Amazon S3 menggunakan konsol

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 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-EC2FlowLogs (AWS Tools for Windows PowerShell)
- CreateFlowLogs (Amazon EC2 Query API)

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/'
```

Catatan log alur proses di Amazon S3

Berkas log dikompresi. Jika Anda membuka berkas log menggunakan konsol Amazon S3, berkas log akan didekompresi dan catatan log alur ditampilkan. Jika Anda mengunduh berkas, Anda harus mendekompresi mereka untuk melihat catatan log alur.

Publikasikan log aliran ke Firehose

Topik

- Peran IAM untuk pengiriman lintas akun
- Membuat log alur yang diterbitkan ke Firehose

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.

Penetapan 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 membuat kebijakan, tentukan VPC, antarmuka jaringan, atau subnet yang Anda pantau dengan kunci kondisi. `iam:AssociatedResourceARN`

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

```
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::source-account:role/mySourceRole",
      "Condition": {
          "StringEquals": {
              "iam:PassedToService": "delivery.logs.amazonaws.com"
          },
          "StringLike": {
              "iam:AssociatedResourceARN": [
                  "arn:aws:ec2:region:source-account: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::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole"
    }
  ]
}
```

Pastikan bahwa peran ini memiliki kebijakan kepercayaan berikut, yang memungkinkan layanan pengiriman log untuk mengambil peran tersebut.

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

```
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Dari akun sumber, gunakan prosedur berikut untuk membuat peran.

Untuk membuat peran akun sumber

1. Masuk ke AWS Management Console 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 kustom. Untuk kebijakan kepercayaan kustom, ganti `"Principal": {},` dengan yang berikut ini, yang menentukan layanan pengiriman log. Pilih Berikutnya.

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

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

Peran akun tujuan

Di akun tujuan, buat peran dengan nama yang dimulai dengan AWSLogsDeliveryFirehoseCrossAccountRole. Peran ini harus memberikan izin berikut.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
          "iam:CreateServiceLinkedRole",
          "firehose:TagDeliveryStream"
      ],
      "Resource": "*"
    }
  ]
}
```

Pastikan peran ini memiliki kebijakan kepercayaan berikut, yang memungkinkan peran yang Anda buat di akun sumber untuk mengambil peran ini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::source-account:role/mySourceRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Dari akun tujuan, gunakan prosedur berikut untuk membuat peran.

Untuk membuat peran akun tujuan

1. Masuk ke AWS Management Console 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 kustom. 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 log alur yang diterbitkan ke Firehose

Untuk membuat log aliran gateway transit yang dipublikasikan ke Firehose menggunakan konsol

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 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-EC2FlowLogs (AWS Tools for Windows PowerShell)
- CreateFlowLogs (Amazon EC2 Query API)

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
```

Bekerja dengan Log Aliran Transit Gateway

Anda dapat bekerja dengan Log Aliran Transit Gateway menggunakan konsol Amazon EC2, Amazon VPC,, dan CloudWatch Amazon S3.

Tugas

- Mengontrol penggunaan log alur
- Membuat log alur
- Melihat log alur
- Menambahkan atau menghapus tag untuk log alur
- Melihat catatan log alur
- Cari catatan log alur
- Menghapus log alur
- Ikhtisar dan batasan API dan CLI

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.

```
{
  "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. Lihat informasi yang lebih lengkap di Buat log alur yang diterbitkan ke CloudWatch Log dan Membuat log alur yang menerbitkan ke Amazon S3.

Membuat log alur

Anda dapat membuat log aliran untuk gateway transit yang dapat mempublikasikan data ke CloudWatch Log, Amazon S3, atau Firehose.

Untuk informasi selengkapnya, lihat hal berikut:

- Buat log alur yang diterbitkan ke CloudWatch Log
- Membuat log alur yang menerbitkan ke Amazon S3
- Membuat log alur yang diterbitkan ke Firehose

Melihat log alur

Anda dapat melihat informasi tentang log alur di konsol VPC Amazon dengan melihat tab Flow Logs untuk sumber daya tertentu. 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 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 dan pilih Flow Logs. Informasi tentang log alur ditampilkan pada tab. Parameter kolom Jenis tujuan menunjukkan tujuan tempat penerbitan log alur.

Menambahkan atau menghapus tag untuk log alur

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.

Melihat catatan log alur

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. Untuk informasi selengkapnya, lihat Catatan Log Aliran Transit Gateway.

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 samping file berkas log. Di halaman gambaran umum, pilih Unduh.

Cari catatan log alur

Anda dapat mencari catatan log alur yang dipublikasikan ke CloudWatch Log menggunakan konsol CloudWatch Log. Anda dapat menggunakan filter metrik untuk menyaring catatan log alur. Catatan log alur adalah ruang yang dibatasi.

Untuk mencari catatan log alur menggunakan konsol CloudWatch Log

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. 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 log alur

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, penghapusan log alur yang menerbitkan ke Amazon S3 tidak menghapus kebijakan bucket dan daftar kontrol akses (ACL) file berkas log.

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.

Ikhtisar dan batasan API dan CLI

Anda dapat melakukan tugas yang dijelaskan di halaman ini menggunakan baris perintah atau API.

Batasan berikut berlaku saat menggunakan `CreateFlowLogs` API atau `create-flow-logs`CLI:

- `--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)
- CreateFlowLogs (Amazon EC2 Query API)

Deskripsikan log alur

- describe-flow-logs (AWS CLI)
- Get-EC2FlowLog (AWS Tools for Windows PowerShell)
- DescribeFlowLogs (Amazon EC2 Query API)

Melihat catatan log alur Anda (log acara)

- get-log-events (AWS CLI)

- LogEventDapatkan-CWL ()AWS Tools for Windows PowerShell
- GetLogEvents(CloudWatchAPI)

Menghapus log alur

- delete-flow-logs (AWS CLI)
- Remove-EC2FlowLog (AWS Tools for Windows PowerShell)
- DeleteFlowLogs (Amazon EC2 Query API)

Pantau gateway transit Anda

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 untuk gateway transit Anda.

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 VPC yang dilampirkan ke gateway transit Anda. Untuk informasi selengkapnya, lihat Log VPC Flow 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 Logging API memanggil gateway transit Anda menggunakan AWS CloudTrail.

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 untuk gateway transit Anda

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
- Dimensi metrik untuk gateway transit

Metrik gerbang transit

Namespace `AWS/TransitGateway` mencakup metrik berikut.

Metrik	Deskripsi
`BytesDropCountBlackhole`	Jumlah byte turun karena cocok dengan rute. `blackhole`
`BytesDropCountNoRoute`	Jumlah byte turun karena tidak cocok dengan rute.
`BytesIn`	Jumlah byte yang diterima oleh gateway transit.
`BytesOut`	Jumlah byte yang dikirim dari gateway transit.
`PacketsIn`	Jumlah paket yang diterima oleh gateway transit.

Metrik	Deskripsi
PacketsOut	Jumlah paket yang dikirim oleh gateway transit.
PacketDropCountBlackhole	Jumlah paket turun karena cocok dengan rute. blackhole
PacketDropCountNoRoute	Jumlah paket turun karena tidak cocok dengan rute.

Metrik tingkat lampiran

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	Deskripsi
BytesDropCountBlackhole	Jumlah byte turun karena cocok dengan blackhole rute pada lampiran gateway transit.
BytesDropCountNoRoute	Jumlah byte turun karena tidak cocok dengan rute pada lampiran gateway transit.
BytesIn	Jumlah byte yang diterima oleh gateway transit dari lampiran.
BytesOut	Jumlah byte yang dikirim dari gateway transit ke lampiran.
PacketsIn	Jumlah paket yang diterima oleh gateway transit dari lampiran.
PacketsOut	Jumlah paket yang dikirim oleh gateway transit ke lampiran.
PacketDropCountBlackhole	Jumlah paket turun karena cocok dengan blackhole rute pada lampiran gateway transit.
PacketDropCountNoRoute	Jumlah paket turun karena tidak cocok dengan rute pada lampiran gateway transit.

Dimensi metrik untuk gateway transit

Untuk memfilter metrik gateway transit Anda, gunakan dimensi berikut.

Dimensi	Deskripsi
`TransitGateway`	Memfilter data metrik dengan gateway transit.
`TransitGatewayAttachment`	Memfilter data metrik dengan lampiran gateway transit.

Logging API memanggil gateway transit Anda menggunakan AWS CloudTrail

AWS CloudTrailadalah layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan. CloudTrail menangkap semua panggilan API gateway transit sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari AWS Management Console dan panggilan kode ke operasi API gateway transit. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk acara untuk gateway transit. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan apa yang dibuat ke API gateway transit, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk informasi selengkapnya tentang API gateway transit, lihat tindakan AWS Transit Gateway di Referensi API Amazon EC2.

Untuk informasi selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

Informasi gateway transit di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Ketika aktivitas terjadi melalui API gateway transit, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Peristiwa. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun AWS Anda. Untuk informasi selengkapnya, lihat Melihat Acara dengan Riwayat CloudTrail Acara.

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk peristiwa untuk API gateway transit, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di dalam konsol tersebut, jejak diterapkan ke semua Wilayah . Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat yang berikut:

- Ikhtisar untuk Membuat Jejak
- CloudTrail Layanan dan Integrasi yang Didukung
- Mengonfigurasi Notifikasi Amazon SNS untuk CloudTrail
- Menerima File CloudTrail Log dari Beberapa Wilayah dan Menerima File CloudTrail Log dari Beberapa Akun

Semua panggilan ke tindakan gateway transit dicatat oleh CloudTrail. Misalnya, panggilan ke `CreateTransitGateway` tindakan menghasilkan entri dalam file CloudTrail log.

Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut:

- Baik permintaan tersebut dibuat dengan kredensial pengguna root atau AWS Identity and Access Management.
- Baik permintaan tersebut dibuat dengan kredensial keamanan sementara untuk peran atau pengguna gabungan.
- Bahwa permintaan dibuat oleh layanan AWS lain.

Untuk informasi lain, lihat Elemen userIdentity CloudTrail .

Memahami entri file log gateway transit

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, jadi 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"
}
```

Manajemen identitas dan akses untuk gateway transit Anda

AWS menggunakan kredensial keamanan untuk mengidentifikasi dan memberi Anda akses menuju AWS sumber daya Anda. Anda dapat menggunakan fitur AWS Identity and Access Management (IAM) untuk memungkinkan pengguna, layanan, dan aplikasi lain untuk menggunakan sumber daya AWS sepenuhnya atau dengan cara yang terbatas, tanpa berbagi kredensial keamanan Anda.

Secara default, pengguna IAM tidak memiliki izin untuk membuat, melihat, atau memodifikasi sumber daya AWS. 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:

- AmazonEC2 FullAccess
- AmazonEC2 ReadOnlyAccess
- 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`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCreateTaggedTGWs",
            "Effect": "Allow",
            "Action": "ec2:CreateTransitGateway",
            "Resource": "arn:aws:ec2:region:account-id:transit-gateway/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/stack": "prod"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "stack"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account-id: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`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteTransitGatewayRouteTable",
                "ec2:CreateTransitGatewayRouteTable"
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id: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/*"
        }
    ]
}
```

Contoh kebijakan untuk mengelola Manajer AWS Jaringan

Misalnya kebijakan, lihat Contoh kebijakan untuk mengelola Manajer Jaringan di Panduan Pengguna Jaringan AWS Global untuk Gateway Transit.

Gunakan peran terkait layanan untuk gateway transit Anda

Amazon VPC menggunakan peran terkait layanan untuk izin yang diperlukan untuk memanggil layanan lain AWS atas nama Anda. Untuk informasi lebih lanjut, lihat Menggunakan peran terkait layanan 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 untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran tertaut layanan dalam Panduan Pengguna IAM.

Membuat peran tertaut 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.

Agar Amazon VPC dapat membuat peran terkait layanan atas nama Anda, Anda harus memiliki izin yang diperlukan. Untuk informasi selengkapnya, lihat Izin peran tertaut layanan dalam Panduan Pengguna IAM.

Mengedit peran tertaut layanan

Anda dapat mengedit deskripsi AWSServiceRoleForVPCTransitGatewaymenggunakan IAM. Untuk informasi lebih lanjut, lihat Mengedit peran terkait layanan dalam Panduan Pengguna IAM.

Hapus peran tertaut 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, IAM CLI, atau IAM API untuk menghapus peran tertaut layanan. Untuk informasi selengkapnya, lihat Menghapus peran tertaut layanan dalam Panduan Pengguna IAM.

Setelah Anda menghapus AWSServiceRoleForVPCTransitGateway, Amazon VPC membuat peran lagi jika Anda melampirkan VPC di akun Anda ke gateway transit.

AWSkebijakan terkelola untuk gateway transit

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola olehAWS. AWSKebijakan 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 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. AWSkemungkinan 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:

- AmazonEC2 FullAccess
- AmazonEC2 ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

AWSkebijakan 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 kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk gateway transit sejak Amazon VPC mulai melacak perubahan ini pada Maret 2021.

Perubahan	Deskripsi	Tanggal
Amazon VPC mulai melacak perubahan	Amazon VPC mulai melacak perubahan pada kebijakan AWS terkelolanya.	1 Maret 2021

Bagaimana Network ACL bekerja dengan gateway transit

Daftar kontrol akses jaringan (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 outbound 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 instance.

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:

- Jaga agar NACL masuk dan keluar yang terkait dengan subnet gateway transit tetap terbuka.
- Bergantung pada arus lalu lintas Anda, Anda dapat menerapkan NACL ke subnet beban kerja Anda.

Untuk informasi selengkapnya tentang cara kerja lampiran VPC, lihatthe section called “Lampiran sumber daya”.

Kuota untuk gateway transit Anda

Anda Akun AWS memiliki kuota berikut (sebelumnya disebut sebagai batas) yang terkait dengan gateway transit. Kecuali dinyatakan sebaliknya, setiap kuota unik untuk suatu 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	Ya
Rute dinamis yang diiklankan dari alat router virtual ke rekan Connect	1.000	Ya
Rute yang diiklankan dari rekan Connect di gateway transit ke alat router virtual	5.000	Tidak

Nama	Default	Dapat disesuaikan
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	Tidak
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

Bandwidth

Ada banyak faktor yang dapat memengaruhi bandwidth terealisasi melalui koneksi VPN Site-to-Site, 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 AWS 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	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 AWS Direct Connect gateway atau koneksi gateway transit peered per Availability Zone yang tersedia di Wilayah	Hingga 100 Gbps	Hubungi Solutions Architect (SA) atau Technical Account Manager (TAM) Anda untuk bantuan lebih lanjut.
Paket per detik per lampiran gateway transit (AWS 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 terowongan VPN	Hingga 1,25 Gbps	Tidak
Paket maksimum per detik per terowongan VPN	Hingga 140.000	Tidak
Bandwidth maksimum per Connect peer (terowongan GRE) untuk lampiran Connect	Hingga 5 Gbps	Tidak

Nama	Default	Dapat disesuaikan
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 AWS 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.

AWS Direct Connect gerbang

Nama	Default	Dapat disesuaikan
AWS Direct Connect gateway per gerbang transit	20	Tidak
Gerbang transit per gerbang AWS 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 VPC, AWS Direct Connect Transit Gateway Connect, dan lampiran 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 kedua VPC secara bersamaan untuk menghindari paket jumbo jatuh karena ketidakcocokan ukuran.
- Paket dengan ukuran lebih besar dari 8500 byte yang tiba di gateway transit dijatuhkan.
- Gateway transit tidak menghasilkan FRAG_NEEDED untuk paket ICMPv4, atau Packet Too Big (PTB) untuk paket ICMPv6. Oleh karena itu, Path MTU Discovery (PMTUD) tidak didukung.
- Gateway transit memberlakukan penjepitan Ukuran Segmen Maksimum (MSS) untuk semua paket. Untuk informasi lebih lanjut, lihat RFC879.
- Untuk detail tentang kuota VPN Site-to-Site untuk MTU, lihat Unit transmisi maksimum (MTU) di Panduan Pengguna.AWS Site-to-Site VPN

Multicast

Nama	Default	Dapat disesuaikan
Domain multicast per transit gateway	20	Ya
Antarmuka jaringan multicast per gateway transit	10.000	Ya
Asosiasi domain multicast per VPC	20	Ya
Sumber per grup multicast transit gateway	1	Ya
Anggota dan sumber grup multicast statis dan IGMPv2 per gateway transit	10.000	Tidak
Anggota grup multicast statis dan IGMPv2 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

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 hal berikut:

- Kuota Site-to-Site VPN dalam Panduan Pengguna AWS Site-to-Site VPN
- Kuota VPC Amazon di Panduan Pengguna Amazon VPC
- Kuota AWS Direct Connect dalam Panduan Pengguna AWS Direct Connect

Riwayat dokumen untuk gateway transit

Tabel berikut menjelaskan rilis untuk gateway transit.

Perubahan	Deskripsi	Tanggal
AWSKuota Transit Gateway	Batas bandwidth ditambahkan.	Agustus 14, 2023
AWSLog Aliran Transit Gateway	Transit Gateways sekarang mendukung Transit Gateway Flow Logs, memungkinkan Anda untuk memantau dan mencatat lalu lintas jaringan antara gateway transit.	Juli 14, 2022
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 dariAWSPanduan Pengguna Transit Gateway.	Desember 2, 2021
Lampiran Peering	Anda dapat membuat koneksi peering dengan gateway transit di Wilayah yang sama.	Desember 1, 2021
Transit Gateway Terhubung	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 lampiran gateway transit individu.	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

AWSManajer Jaringan	Anda dapat memvisual isasikan dan memantau jaringan global Anda yang dibangun di sekitar gateway transit.	3 Desember 2019
AWS Direct Connectdukungan	Anda dapat menggunak anAWS Direct Connectge rbang untuk menghubun gkanAWS Direct Connectko neksi 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.