Peering VPC

Amazon Virtual Private Cloud

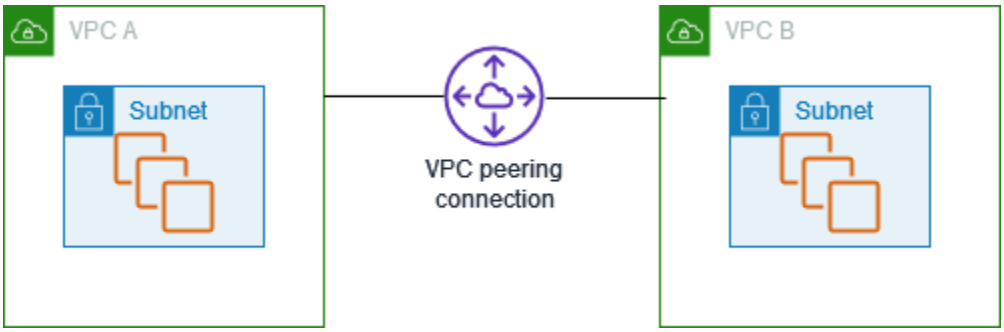
Amazon Virtual Private Cloud: Peering VPC

Table of Contents

Apa yang dimaksud dengan peering VPC?

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

Koneksi peering VPC adalah koneksi jaringan antara dua VPCs yang memungkinkan Anda untuk merutekan lalu lintas di antara mereka menggunakan alamat atau IPv4 alamat pribadi. IPv6 Instans di kedua VPC tersebut dapat berkomunikasi satu sama lain seolah berada di jaringan yang sama. Anda dapat membuat koneksi peering VPC antara Anda sendiri VPCs, atau dengan VPC di akun lain. AWS VPCs Bisa di Wilayah yang berbeda (juga dikenal sebagai koneksi peering VPC antar wilayah).



AWS menggunakan infrastruktur VPC yang ada untuk membuat koneksi peering VPC; itu bukan gateway atau koneksi VPN, dan tidak bergantung pada perangkat keras fisik yang terpisah. Tidak ada satupun titik kegagalan untuk berkomunikasi atau kemacetan bandwidth.

Koneksi peering VPC membantu Anda mempermudah transfer data. Misalnya, jika Anda memiliki lebih dari satu AWS akun, Anda dapat mengintip VPCs seluruh akun tersebut untuk membuat jaringan berbagi file. Anda juga dapat menggunakan koneksi peering VPC untuk memungkinkan orang lain VPCs mengakses sumber daya yang Anda miliki di salah satu sumber daya Anda. VPCs

Ketika Anda membangun hubungan peering antara VPCs seluruh AWS Wilayah yang berbeda, sumber daya dalam VPCs (misalnya, EC2 instance dan fungsi Lambda) di AWS Wilayah yang berbeda dapat berkomunikasi satu sama lain menggunakan alamat IP pribadi, tanpa menggunakan gateway, koneksi VPN, atau alat jaringan. Lalu lintas tetap berada di ruang alamat IP pribadi. Semua lalu lintas antar wilayah dienkripsi tanpa titik kegagalan tunggal, atau hambatan bandwidth. Lalu lintas selalu berada di AWS tulang punggung global, dan tidak pernah melintasi internet publik, yang mengurangi ancaman, seperti eksploitasi umum, dan serangan S. DDo Peering VPC Antar Wilayah menyediakan cara sederhana dan hemat biaya untuk berbagi sumber daya antar Wilayah atau mereplikasi data untuk redundansi geografis.

Penetapan harga untuk koneksi peering VPC

Tidak ada biaya untuk membuat koneksi peering VPC. Semua transfer data melalui koneksi peering VPC yang tetap berada dalam Availability Zone gratis, bahkan jika itu antara akun yang berbeda. Biaya berlaku untuk transfer data melalui koneksi peering VPC yang melintasi Availability Zone dan Regions. Untuk informasi selengkapnya, lihat EC2 Harga Amazon EC2 .

Cara kerja koneksi peering VPC

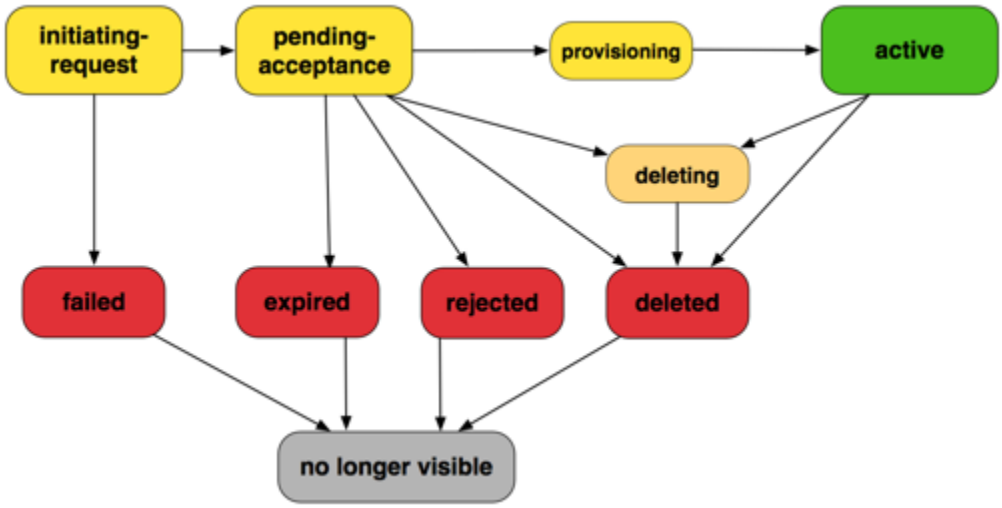
Langkah-langkah berikut menjelaskan proses peering VPC:

1. Pemilik dari VPC peminta mengirimkan permintaan ke pemilik VPC penerima untuk membuat koneksi peering VPC. VPC penerima dapat dimiliki oleh Anda, atau akun AWS lain, dan tidak dapat memiliki blok CIDR yang tumpang tindih dengan blok CIDR dari VPC pemohon.
2. Pemilik VPC penerima menerima permintaan koneksi peering VPC untuk mengaktifkan koneksi peering VPC.
3. Untuk mengaktifkan arus lalu lintas antara VPCs menggunakan alamat IP pribadi, pemilik setiap VPC dalam koneksi peering VPC harus secara manual menambahkan rute ke satu atau lebih tabel rute VPC mereka yang menunjuk ke kisaran alamat IP dari VPC lainnya (VPC rekan).
4. Jika diperlukan, perbarui aturan grup keamanan yang terkait dengan EC2 instans Anda untuk memastikan bahwa lalu lintas ke dan dari VPC rekan tidak dibatasi. Jika keduanya VPCs berada di Wilayah yang sama, Anda dapat mereferensikan grup keamanan dari VPC rekan sebagai sumber atau tujuan untuk aturan masuk atau keluar di grup keamanan Anda.
5. Dengan opsi koneksi peering VPC default, jika EC2 instance di kedua sisi koneksi peering VPC saling beralamat menggunakan nama host DNS publik, nama host akan diselesaikan ke alamat IP publik instance. EC2 Untuk mengubah perilaku ini, Aktifkan resolusi nama host DNS untuk koneksi VPC Anda. Setelah mengaktifkan resolusi nama host DNS, jika EC2 instance di kedua sisi koneksi peering VPC saling beralamat menggunakan nama host DNS publik, nama host menyelesaikan ke alamat IP pribadi instance. EC2

Untuk informasi selengkapnya, lihat Koneksi peering VPC.

Siklus hidup koneksi peering VPC

Koneksi peering VPC melewati berbagai tahap mulai dari ketika permintaan diinisiasi. Pada setiap tahap, mungkin saja ada tindakan yang bisa Anda lakukan, dan di akhir siklus hidupnya, koneksi peering VPC tetap terlihat di konsol Amazon VPC dan API atau hasil baris perintah selama jangka waktu tertentu.



- Initiating-request: Permintaan untuk koneksi peering VPC telah dimulai. Pada tahap ini, koneksi peering bisa gagal, atau bisa saja masuk ke `pending-acceptance`.
- Gagal: Permintaan untuk koneksi peering VPC telah gagal. Selagi berada dalam status ini, koneksi tidak dapat diterima, ditolak, atau dihapus. Koneksi peering VPC yang gagal tetap terlihat oleh peminta selama 2 jam.
- Pending-acceptance: permintaan koneksi peering VPC sedang menunggu penerimaan dari pemilik atas VPC penerima. Selama dalam status ini, pemilik atas VPC peminta dapat menghapus permintaan tersebut, dan pemilik dari VPC penerima dapat menerima atau menolak permintaan tersebut. Jika tidak ada tindakan yang diambil atas permintaan tersebut, status kedaluwarsa setelah 7 hari.
- Kedaluwarsa: Permintaan koneksi peering VPC telah kedaluwarsa, dan tidak ada tindakan yang dapat diambil oleh pemilik VPC manapun. Koneksi peering VPC yang kedaluwarsa tetap terlihat oleh kedua pemilik VPC selama 2 hari.
- Ditolak: Pemilik dari VPC penerima telah menolak `pending-acceptance` permintaan koneksi peering VPC. Sementara dalam status ini, permintaan tidak dapat diterima. Koneksi peering VPC yang ditolak tetap dapat dilihat oleh pemilik VPC peminta selama 2 hari, dan dapat dilihat oleh pemilik VPC penerima selama 2 jam. Jika permintaan dibuat dalam AWS akun yang sama, permintaan yang ditolak tetap terlihat selama 2 jam.
- Penyediaan: Permintaan koneksi peering VPC telah diterima, dan akan segera berada dalam status `active`.
- Aktif: Koneksi peering VPC aktif, dan lalu lintas dapat mengalir di antara VPCs (asalkan grup keamanan dan tabel rute Anda memungkinkan arus lalu lintas). Selagi berada dalam status ini,

salah satu dari pemilik VPC dapat menghapus koneksi peering VPC tersebut, tetapi tidak dapat menolaknya.

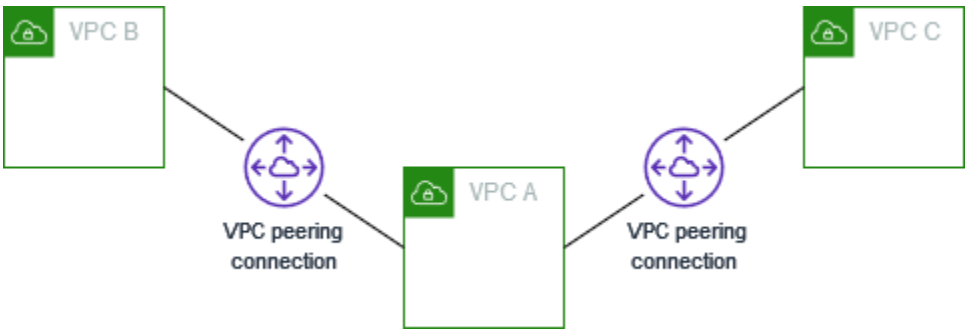
> **Note**
>
> Jika suatu peristiwa di Wilayah di mana VPC berada mencegah arus lalu lintas, status koneksi peering VPC tetap ada. `Active`

- Menghapus: Berlaku untuk koneksi peering VPC antar wilayah yang sedang dalam proses dihapus. Pemilik salah satu VPC telah mengajukan permintaan untuk menghapuskoneksi peering VPC `active`, atau pemilik dari VPC peminta telah mengajukan permintaan untuk menghapus permintaan koneksi peering VPC `pending-acceptance`.
- Dihapus: Sebuah koneksi peering VPC `active` telah dihapus oleh salah satu pemilik VPC, atau sebuah permintaan koneksi peering VPC `pending-acceptance` telah dihapus oleh pemilik VPC peminta. Sementara dalam status ini, koneksi peering VPC tidak dapat diterima atau ditolak. Koneksi peering VPC masih tetap terlihat oleh pihak yang menghapusnya selama 2 jam, dan terlihat oleh pihak lain selama 2 hari. Jika koneksi peering VPC dibuat akun AWS yang sama, permintaan yang dihapus tetap terlihat selama 2 jam.

Berbagai koneksi peering VPC

Koneksi peering VPC adalah hubungan satu lawan satu antara dua. VPCs Anda dapat membuat beberapa koneksi peering VPC untuk setiap VPC yang Anda miliki, tetapi hubungan peering transitif tidak di-support. Anda tidak memiliki hubungan peering dengan VPCs VPC Anda tidak langsung diintip.

Diagram berikut adalah contoh dari satu VPC yang diintip ke dua yang berbeda. VPCs Terdapat dua koneksi peering VPC: VPC A disambungkan dengan kedua VPC B dan VPC C. VPC B dan VPC C tidak tersambung, dan Anda tidak dapat menggunakan VPC A sebagai titik transit untuk menyambungkan VPC B dan VPC C. Jika Anda ingin mengaktifkan perutean lalu lintas antara VPC B dan VPC C, Anda harus membuat koneksi peering VPC tersendiri antara keduanya.



Keterbatasan peering VPC

Pertimbangkan batasan berikut untuk koneksi peering VPC. Dalam beberapa kasus, Anda dapat menggunakan lampiran gateway transit alih-alih koneksi peering VPC. Untuk informasi selengkapnya, lihat Contoh skenario gateway transit di Amazon VPC Transit Gateways.

Koneksi

- Ada kuota jumlah koneksi peering VPC yang aktif dan tertunda per VPC. Untuk informasi selengkapnya, lihat Kuota.
- Anda tidak dapat memiliki lebih dari satu koneksi peering VPC antara dua VPCs pada saat yang bersamaan.
- Tag apa pun yang Anda buat untuk koneksi peering VPC Anda hanya diterapkan di akun atau Wilayah tempat Anda membuatnya.
- Anda tidak dapat tersambung atau melakukan kueri server DNS Amazon di VPC rekan.
- Jika blok IPv4 CIDR dari VPC dalam koneksi peering VPC berada di luar rentang alamat IPv4 pribadi yang ditentukan oleh RFC 1918, nama host DNS pribadi untuk VPC tersebut tidak dapat diselesaikan ke alamat IP pribadi. Untuk menentukan nama host DNS pribadi menjadi alamat IP pribadi, Anda dapat mengaktifkan support resolusi DNS untuk koneksi peering VPC. Untuk informasi selengkapnya, lihat Aktifkan resolusi DNS untuk koneksi peering VPC.
- Anda dapat mengaktifkan sumber daya di kedua sisi koneksi peering VPC untuk berkomunikasi. IPv6 Anda harus mengaitkan blok IPv6 CIDR dengan setiap VPC, mengaktifkan instance di VPCs IPv6 for communication, dan IPv6 merutekan lalu lintas yang ditujukan untuk VPC peer ke koneksi peering VPC.
- Penerusan jalur terbalik Unicast pada koneksi peering VPC tidak di-support. Untuk informasi selengkapnya, lihat Perutean untuk lalu lintas respons.

Blok CIDR tumpang tindih

- Anda tidak dapat membuat koneksi peering VPC antara yang memiliki blok VPCs yang cocok atau tumpang tindih atau CIDR IPv4 . IPv6
- Jika Anda memiliki beberapa blok IPv4 CIDR, Anda tidak dapat membuat koneksi peering VPC jika ada blok CIDR yang tumpang tindih, bahkan jika Anda hanya bermaksud menggunakan blok CIDR yang tidak tumpang tindih atau hanya blok CIDR. IPv6

Peering Transitif

- Peering VPC tidak men-support hubungan sambungan transitif. Misalnya, jika ada koneksi peering VPC antara VPC A dan VPC B, dan antara VPC A dan VPC C, Anda tidak dapat merutekan lalu lintas dari VPC B ke VPC C melalui VPC A. Untuk merutekan lalu lintas antara VPC B dan VPC C, Anda harus membuat koneksi peering VPC di antara mereka. Untuk informasi selengkapnya, lihat Tiga VPCs mengintip bersama.

Perutean edge ke edge melalui gateway atau koneksi pribadi

- Jika VPC A memiliki gateway internet, sumber daya di VPC B tidak dapat menggunakan gateway internet di VPC A untuk mengakses internet.
- Jika VPC A memiliki perangkat NAT yang menyediakan akses internet ke subnet di VPC A, sumber daya di VPC B tidak dapat menggunakan perangkat NAT di VPC A untuk mengakses internet.
- Jika VPC A memiliki koneksi VPN ke jaringan perusahaan, sumber daya di VPC B tidak dapat menggunakan koneksi VPN untuk berkomunikasi dengan jaringan perusahaan.
- Jika VPC A memiliki AWS Direct Connect koneksi ke jaringan perusahaan, sumber daya di VPC B tidak dapat menggunakan AWS Direct Connect koneksi untuk berkomunikasi dengan jaringan perusahaan.
- Jika VPC A memiliki titik akhir gateway yang menyediakan konektivitas ke Amazon S3 ke subnet pribadi di VPC A, sumber daya di VPC B tidak dapat menggunakan titik akhir gateway untuk mengakses Amazon S3.

Koneksi peering VPC Antar Wilayah

- Untuk frame jumbo, Unit Transmisi Maksimum (MTU) antara koneksi peering VPC dalam Wilayah yang sama adalah 9001 byte. MTU untuk koneksi peering VPC antar wilayah adalah 8500 byte.

Untuk informasi selengkapnya tentang bingkai jumbo, lihat Jumbo frame (9001 MTU) di Panduan Pengguna Amazon EC2 .

- Anda harus mengaktifkan dukungan resolusi DNS untuk koneksi peering VPC untuk menyelesaikan nama host DNS pribadi dari VPC peered ke alamat IP pribadi, bahkan jika CIDR untuk VPC termasuk IPv4 dalam rentang alamat pribadi yang ditentukan oleh RFC 1918. IPv4

Bersama VPCs dan subnet

- Hanya pemilik VPC yang dapat bekerja dengan (mendeskripsikan, membuat, menerima, menolak, memodifikasi, atau menghapus) koneksi peering. Peserta tidak dapat bekerja dengan koneksi peering. Untuk informasi selengkapnya, lihat, Bagikan VPC Anda dengan akun lain di Panduan Pengguna Amazon VPC.

Koneksi peering VPC

Pengintipan VPC memungkinkan Anda menghubungkan dua VPCs di Wilayah yang sama atau berbeda. AWS Hal ini memungkinkan instance dalam satu VPC untuk berkomunikasi dengan instance di VPC lain seolah-olah mereka semua adalah bagian dari jaringan yang sama.

VPC peering membuat rute jaringan langsung antara keduanya VPCs menggunakan alamat atau IPv4 alamat pribadi. IPv6 Lalu lintas yang dikirim antara yang terhubung VPCs tidak melintasi internet, koneksi VPN, atau koneksi Direct AWS Connect. Hal ini membuat VPC mengintip cara yang aman untuk berbagi sumber daya, seperti database atau server web, melintasi batas-batas VPC.

Untuk membuat koneksi peering VPC, Anda membuat permintaan koneksi peering dari satu VPC dan pemilik VPC lainnya menerima permintaan tersebut. Setelah koneksi dibuat, Anda dapat memperbarui tabel rute Anda untuk merutekan lalu lintas antara VPCs. Hal ini memungkinkan instance dalam satu VPC untuk mengakses sumber daya di VPC lainnya.

Pengintipan VPC adalah alat penting untuk membangun arsitektur multi-VPC dan berbagi sumber daya melintasi batas-batas organisasi di. AWS Ini menyediakan cara sederhana, latensi rendah untuk terhubung VPCs tanpa kerumitan mengkonfigurasi VPN atau layanan jaringan lainnya.

Gunakan prosedur berikut untuk membuat dan bekerja dengan koneksi peering VPC.

Tugas

- Buat koneksi peering VPC
- Menerima atau menolak koneksi peering VPC
- Perbarui tabel rute Anda untuk koneksi peering VPC
- Perbarui grup keamanan Anda untuk mereferensikan grup keamanan sejawat
- Aktifkan resolusi DNS untuk koneksi peering VPC
- Hapus koneksi peering VPC
- Memecahkan masalah koneksi peering VPC

Buat koneksi peering VPC

Untuk membuat koneksi peering VPC, pertama buat permintaan untuk tersambung dengan VPC lain. Untuk mengaktivasi permintaan, pemilik VPC penerima harus menerima permintaan tersebut. Koneksi peering berikut didukung:

- Antara VPCs di akun dan Wilayah yang sama
- Antara VPCs di akun yang sama dan Wilayah yang berbeda
- Antara VPCs di akun yang berbeda dan Wilayah yang sama
- Antara VPCs di berbagai akun dan Wilayah

Untuk koneksi peering VPC antar wilayah, permintaan harus dibuat dari Wilayah VPC pemohon, dan permintaan harus diterima dari Wilayah VPC penerima. Untuk informasi selengkapnya, lihat the section called “Menerima atau menolak”.

Tugas

- Prasyarat
- Buat koneksi peering menggunakan konsol
- Buat koneksi peering menggunakan baris perintah

Prasyarat

- Tinjau batasan untuk koneksi peering VPC.
- Pastikan VPCs tidak memiliki blok IPv4 CIDR yang tumpang tindih. Jika tumpang tindih, status koneksi peering VPC segera masuk ke. `failed` Batasan ini berlaku bahkan jika VPCs memiliki blok IPv6 CIDR yang unik.

Buat koneksi peering menggunakan konsol

Gunakan prosedur berikut untuk membuat koneksi peering VPC.

Untuk membuat koneksi peering menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Koneksi peering.
3. Pilih Buat koneksi peering.
4. (Opsional) Untuk Nama, tentukan nama koneksi peering VPC. Ini menciptakan tag dengan kunci dari Name dan nilai yang Anda tentukan.
5. Untuk ID VPC (Pemohon), pilih VPC dari akun saat ini.
6. Di bawah Pilih VPC lain untuk diajak, lakukan hal berikut:

a. Untuk Akun, untuk mengintip dengan VPC di akun lain, pilih Akun lain dan masukkan ID akun. Jika tidak, simpan akun Saya.

b. Untuk Wilayah, untuk mengintip VPC di Wilayah lain, pilih Wilayah Lain dan pilih Wilayah. Jika tidak, pertahankan Wilayah Ini.

c. Untuk ID VPC (Penerima), pilih VPC dari akun dan Wilayah yang ditentukan.

7. (Opsional) Untuk menambahkan tag, pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.
8. Pilih Buat koneksi peering.
9. Pemilik akun aksepter harus menerima koneksi peering. Untuk informasi selengkapnya, lihat the section called “Menerima atau menolak”.
10. Perbarui tabel rute untuk keduanya VPCs untuk mengaktifkan komunikasi di antara keduanya. Untuk informasi selengkapnya, lihat the section called “Perbarui tabel rute”.

Buat koneksi peering menggunakan baris perintah

Anda dapat membuat koneksi peering VPC menggunakan perintah berikut:

- create-vpc-peering-connection (AWS CLI)
- New-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

Menerima atau menolak koneksi peering VPC

Koneksi peering VPC yang sedang berstatus `pending-acceptance` harus diterima oleh pemilik VPC penerima untuk bisa diaktivasi. Untuk informasi selengkapnya tentang status koneksi `Deleted` peering, lihatSiklus hidup koneksi peering VPC. Anda tidak dapat menerima permintaan koneksi peering VPC yang Anda kirim ke akun lain. AWS Untuk membuat koneksi peering VPC antara VPCs di AWS akun yang sama, Anda dapat membuat dan menerima permintaan sendiri.

Anda dapat menolak permintaan koneksi peering VPC apa pun yang telah Anda terima yang sedang berstatus `pending-acceptance`. Anda hanya boleh menerima koneksi peering VPC dari Akun AWS yang Anda kenal dan percayai; Anda dapat menolak permintaan yang tidak diinginkan. Untuk informasi selengkapnya tentang status koneksi `Rejected` peering, lihatSiklus hidup koneksi peering VPC.

> **Important**
>
> Jangan terima koneksi peering VPC dari akun yang tidak dikenal. AWS Pengguna berbahaya mungkin telah mengirimi Anda permintaan koneksi peering VPCuntuk mendapatkan akses jaringan yang tidak sah ke VPC Anda. Hal ini dikenal sebagai peer phishing. Anda dapat dengan aman menolak permintaan koneksi peering VPC yang tidak diinginkan tanpa risiko pemohon mendapatkan akses ke informasi apa pun tentang AWS akun Anda atau VPC Anda. Untuk informasi selengkapnya, lihat Menerima atau menolak koneksi peering VPC. Anda juga dapat mengabaikan permintaan dan membiarkannya kedaluwarsa; secara default, permintaan kedaluwarsa setelah 7 hari.

Untuk menerima atau menolak koneksi peering menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Gunakan pemilih Wilayah untuk memilih Wilayah penerima VPC.
3. Di panel navigasi, pilih Koneksi peering.
4. Untuk menolak koneksi peering, pilih koneksi peering VPC, dan pilih Actions, Reject request. Saat diminta konfirmasi, pilih Tolak permintaan.
5. Untuk menerima koneksi peering, pilih koneksi peering VPC yang tertunda (statusnya**`pending-acceptance`**), dan pilih Actions, Accept request. Untuk informasi selengkapnya tentang status siklus hidup koneksi peering, lihat. Siklus hidup koneksi peering VPC

   Jika tidak ada koneksi peering VPC yang tertunda, verifikasi bahwa Anda memilih Wilayah VPC penerima.
6. Saat diminta konfirmasi, pilih Terima permintaan.
7. Pilih Ubah tabel rute saya sekarang untuk menambahkan rute ke tabel rute VPC sehingga Anda dapat mengirim dan menerima lalu lintas melintasi koneksi peering. Untuk informasi selengkapnya, lihat Perbarui tabel rute Anda untuk koneksi peering VPC.

Untuk menerima koneksi peering menggunakan baris perintah

- accept-vpc-peering-connection (AWS CLI)
- Approve-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

Untuk menolak koneksi peering menggunakan baris perintah

- reject-vpc-peering-connection (AWS CLI)
- Deny-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

Perbarui tabel rute Anda untuk koneksi peering VPC

Untuk mengaktifkan IPv4 lalu lintas pribadi antar instance di peered VPCs, Anda harus menambahkan rute ke tabel rute yang terkait dengan subnet untuk kedua instance. Tujuan rute adalah blok CIDR (atau bagian dari blok CIDR) dari VPC rekan dan targetnya adalah ID koneksi peering VPC. Untuk informasi selengkapnya, lihat Mengonfigurasi tabel rute dalam Panduan Pengguna Amazon VPC.

Berikut ini adalah contoh tabel rute yang memungkinkan komunikasi antara instance dalam dua peered, VPC A dan VPCs VPC B. Setiap tabel memiliki rute lokal dan rute yang mengirimkan lalu lintas untuk VPC rekan ke koneksi peering VPC VPC.

Tabel rute	Tujuan	Target
VPC A	*VPC A CIDR*	Lokal:
	VPC B CIDR	pcx- *11112222*
VPC B	*VPC B CIDR*	Lokal:
	VPC A CIDR	pcx- *11112222*

Demikian pula, jika koneksi peering VPCs di VPC memiliki blok IPv6 CIDR terkait, Anda dapat menambahkan rute yang memungkinkan komunikasi dengan VPC rekan. IPv6

Untuk informasi lebih lanjut tentang konfigurasi tabel rute yang di-support untuk koneksi peering VPC, lihat Konfigurasi koneksi peering VPC umum.

Pertimbangan

- Jika Anda memiliki VPC yang diintip dengan beberapa blok IPv4 CIDR VPCs yang tumpang tindih atau cocok, pastikan tabel rute Anda dikonfigurasi untuk menghindari pengiriman lalu lintas respons dari VPC Anda ke VPC yang salah. AWS saat ini tidak mendukung penerusan jalur balik

unicast dalam koneksi peering VPC yang memeriksa IP sumber paket dan merutekan paket balasan kembali ke sumbernya. Untuk informasi selengkapnya, lihat Perutean untuk lalu lintas respons.

- Akun Anda memiliki kuota pada jumlah entri yang dapat Anda tambahkan per tabel rute. Jika jumlah koneksi peering VPC di VPC Anda melebihi kuota entri tabel rute untuk tabel rute tunggal, pertimbangkan untuk menggunakan berbagai subnet yang masing-masingnya terkait dengan sebuah tabel rute kustom.
- Anda dapat menambahkan rute untuk koneksi peering VPC yang berada dalam status `pending-acceptance`. Namun, rute tersebut memiliki status`blackhole`, dan tidak berpengaruh sampai koneksi peering VPC berada di negara bagian. `active`

Untuk menambahkan IPv4 rute untuk koneksi peering VPC

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Tabel rute.
3. Centang kotak di samping tabel rute yang terkait dengan subnet tempat instans Anda berada.

   Jika Anda tidak memiliki tabel rute yang secara eksplisit terkait dengan subnet tersebut, tabel rute utama untuk VPC secara implisit terkait dengan subnet.
4. Pilih Tindakan, Sunting rute.
5. Pilih Tambahkan rute.
6. Untuk Tujuan, masukkan rentang IPv4 alamat tempat lalu lintas jaringan dalam koneksi peering VPC harus diarahkan. Anda dapat menentukan seluruh blok IPv4 CIDR dari VPC rekan, rentang tertentu, atau IPv4 alamat individual, seperti alamat IP dari instance yang dapat digunakan untuk berkomunikasi. Misalnya, jika blok CIDR dari VPC rekan `10.0.0.0/16`, Anda dapat menentukan porsi `10.0.0.0/24`, atau alamat IP tertentu `10.0.0.7/32`.
7. Untuk Target, pilih koneksi peering VPC.
8. Pilih Simpan perubahan.

Pemilik VPC rekan juga harus menyelesaikan langkah-langkah ini untuk menambahkan rute untuk mengarahkan lalu lintas kembali ke VPC Anda melalui koneksi peering VPC.

Jika Anda memiliki sumber daya di AWS Wilayah berbeda yang menggunakan IPv6 alamat, Anda dapat membuat koneksi peering antar wilayah. Anda kemudian dapat menambahkan IPv6 rute untuk komunikasi antar sumber daya.

Untuk menambahkan IPv6 rute untuk koneksi peering VPC

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Tabel rute.
3. Centang kotak di samping tabel rute yang terkait dengan subnet tempat instans Anda berada.

> **Note**
>
> Jika Anda tidak memiliki tabel rute yang terkait dengan subnet tersebut, pilih tabel rute utama untuk VPC, karena subnet tersebut kemudian menggunakan tabel rute ini secara default.

4. Pilih Tindakan, Sunting rute.
5. Pilih Tambahkan rute.
6. Untuk Tujuan, masukkan rentang IPv6 alamat untuk VPC rekan. Anda dapat menentukan seluruh blok IPv6 CIDR dari VPC rekan, rentang tertentu, atau alamat individual. IPv6 Misalnya, jika blok CIDR dari VPC rekan `2001:db8:1234:1a00::/56`, Anda dapat menentukan porsi `2001:db8:1234:1a00::/64`, atau alamat IP tertentu `2001:db8:1234:1a00::123/128`.
7. Untuk Target, pilih koneksi peering VPC.
8. Pilih Simpan perubahan.

Untuk informasi selengkapnya, lihat Rutekan tabel di Panduan Pengguna Amazon VPC.

Untuk menambah atau mengganti rute menggunakan baris perintah

- create-route dan replace-route ()AWS CLI
- New-EC2Routedan Set-EC2RouteAWS Tools for Windows PowerShell

Perbarui grup keamanan Anda untuk mereferensikan grup keamanan sejawat

Anda dapat memperbarui aturan masuk atau keluar untuk grup keamanan VPC Anda untuk mereferensikan grup keamanan untuk peered. VPCs Melakukan hal itu memungkinkan lalu lintas mengalir ke dan dari instans yang terkait dengan grup keamanan yang dirujuk di VPC yang menjadi rekan/peer.

> **Note**
>
> Grup keamanan di VPC rekan tidak ditampilkan di konsol untuk Anda pilih.

Persyaratan

- Untuk mereferensikan grup keamanan di VPC rekan, koneksi peering VPC harus berstatus `active`.
- VPC rekan dapat berupa VPC di akun Anda, atau VPC di akun lain. AWS Untuk mereferensikan grup keamanan yang ada di AWS akun lain tetapi Wilayah yang sama, sertakan nomor akun dengan ID grup keamanan. Misalnya, `123456789012/sg-1a2b3c4d`.
- Anda tidak dapat mereferensikan grup keamanan VPC rekan yang berada di Wilayah berbeda. Sebagai gantinya, gunakan blok CIDR dari VPC rekan.
- Jika Anda mengonfigurasi rute untuk meneruskan lalu lintas antara dua instans di subnet yang berbeda melalui perangkat middlebox, Anda harus memastikan bahwa grup keamanan untuk kedua instans tersebut mengizinkan lalu lintas mengalir di antara instans. Grup keamanan untuk setiap instans harus mereferensikan alamat IP privat instans lain, atau rentang CIDR dari subnet yang berisi instans yang lain, sebagai sumbernya. Jika Anda mereferensikan grup keamanan instans lain sebagai sumbernya, hal ini tidak akan mengizinkan lalu lintas mengalir di antara instans.

Untuk memperbarui aturan keamanan menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Grup keamanan.
3. Pilih grup keamanan, dan lakukan salah satu hal berikut:
   - Untuk mengubah aturan masuk, pilih Tindakan, Edit aturan masuk.
   - Untuk mengubah aturan keluar, pilih Tindakan, Edit aturan keluar.
4. Untuk menambahkan aturan, pilih Tambahkan aturan dan tentukan jenis, protokol, dan rentang port. Untuk Sumber (aturan masuk) atau Tujuan (aturan keluar), lakukan salah satu hal berikut:
   - Untuk VPC rekan di akun dan Wilayah yang sama, masukkan ID grup keamanan.
   - Untuk VPC rekan di akun yang berbeda tetapi Wilayah yang sama, masukkan ID akun dan ID grup keamanan, dipisahkan oleh garis miring (misalnya,). `123456789012/sg-1a2b3c4d`

- Untuk VPC rekan di Wilayah yang berbeda, masukkan blok CIDR dari VPC rekan.

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

Untuk memperbarui aturan inbound menggunakan baris perintah

- authorize-security-group-ingressdan revoke-security-group-ingressAWS CLI
- Grant-EC2SecurityGroupIngressdan Revoke-EC2SecurityGroupIngressAWS Tools for Windows PowerShell

Misalnya, untuk memperbarui grup keamanan Anda `sg-aaaa1111` agar memungkinkan akses masuk melalui HTTP dari `sg-bbbb2222` VPC rekan, gunakan perintah berikut. Jika VPC rekan berada di Wilayah yang sama tetapi akun yang berbeda, tambahkan. `--group-owner` *aws-account-id*

```
aws ec2 authorize-security-group-ingress --group-id sg-aaaa1111 --protocol tcp --
port 80 --source-group sg-bbbb2222
```

Untuk memperbarui aturan outbound menggunakan baris perintah

- authorize-security-group-egressdan revoke-security-group-egressAWS CLI
- Grant-EC2SecurityGroupEgressdan Revoke-EC2SecurityGroupEgressAWS Tools for Windows PowerShell

Setelah memperbarui aturan grup keamanan, gunakan describe-security-groupsperintah untuk melihat grup keamanan yang direferensikan dalam aturan grup keamanan Anda.

Identifikasi grup keamanan yang direferensikan

Untuk menentukan apakah grup keamanan Anda sedang direferensikan dalam aturan grup keamanan di VPC rekan, gunakan salah satu dari perintah berikut untuk satu atau lebih grup keamanan di akun Anda.

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

Pada contoh berikut, respons menunjukkan bahwa grup keamanan `sg-bbbb2222` sedang direferensikan oleh grup keamanan di VPC `vpc-aaaaaaaa`:

```
aws ec2 describe-security-group-references --group-id sg-bbbb2222
```

```
{
  "SecurityGroupsReferenceSet": [
    {
      "ReferencingVpcId": "vpc-aaaaaaaa",
      "GroupId": "sg-bbbb2222",
      "VpcPeeringConnectionId": "pcx-b04deed9"
    }
  ]
}
```

Jika koneksi peering VPC dihapus, atau jika pemilik dari VPC rekan menghapus grup keamanan yang direferensikan, aturan grup keamanan menjadi kedaluwarsa.

Lihat dan hapus dengan aturan grup keamanan basi

Aturan grup keamanan basi adalah aturan yang mereferensikan grup keamanan yang dihapus dalam VPC yang sama atau dalam VPC rekan, atau yang mereferensikan grup keamanan dalam VPC rekan yang koneksi peering VPC telah dihapus. Bila aturan grup keamanan menjadi kedaluwarsa, aturan grup tidak secara otomatis terhapus dari grup keamanan Anda—Anda harus menghapusnya secara manual. Jika aturan grup keamanan basi karena koneksi peering VPC telah dihapus, aturan tidak akan lagi ditandai sebagai basi jika Anda membuat koneksi peering VPC baru dengan yang sama. VPCs

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

Untuk melihat dan menghapus aturan grup keamanan yang kedaluwarsa

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi, pilih Grup keamanan.
3. Pilih Tindakan, Kelola aturan kedaluwarsa.
4. Untuk VPC, pilih VPC dengan aturan kedaluwarsa.
5. Pilih Sunting.

6. Pilih tombol Hapus di samping aturan yang ingin Anda hapus. Pilih Tinjau perubahan, Simpan aturan.

Untuk mendeskripsikan aturan grup keamanan basi Anda menggunakan baris perintah

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

Pada contoh berikut, VPC A (`vpc-aaaaaaaa`) dan VPC B disambungkan, dan koneksi peering VPC telah dihapus. Grup keamanan Anda `sg-aaaa1111` di VPC A mereferensikan `sg-bbbb2222` di VPC B. Ketika Anda menjalankan perintah `describe-stale-security-groups` untuk VPC Anda, respons menunjukkan bahwa grup keamanan `sg-aaaa1111` memiliki aturan SSH kedaluwarsa yang mereferensikan `sg-bbbb2222`.

```
aws ec2 describe-stale-security-groups --vpc-id vpc-aaaaaaaa
```

```
{
    "StaleSecurityGroupSet": [
        {
            "VpcId": "vpc-aaaaaaaa",
            "StaleIpPermissionsEgress": [],
            "GroupName": "Access1",
            "StaleIpPermissions": [
                {
                    "ToPort": 22,
                    "FromPort": 22,
                    "UserIdGroupPairs": [
                        {
                            "VpcId": "vpc-bbbbbbbb",
                            "PeeringStatus": "deleted",
                            "UserId": "123456789101",
                            "GroupName": "Prod1",
                            "VpcPeeringConnectionId": "pcx-b04deed9",
                            "GroupId": "sg-bbbb2222"
                        }
                    ],
                    "IpProtocol": "tcp"
                }
            ],
            "GroupId": "sg-aaaa1111",
```

```
            "Description": "Reference remote SG"
        }
    ]
}
```

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

Aktifkan resolusi DNS untuk koneksi peering VPC

Pengaturan DNS untuk koneksi peering VPC menentukan bagaimana nama host DNS publik diselesaikan untuk permintaan yang melintasi koneksi peering VPC. Jika EC2 instance di satu sisi koneksi peering VPC mengirimkan permintaan ke EC2 instance di sisi lain menggunakan nama host DNS publik dari instance tersebut, nama host IPv4 DNS diselesaikan sebagai berikut.

Resolusi DNS dinonaktifkan (default)

Nama host IPv4 DNS publik menyelesaikan ke IPv4 alamat publik instance.

Resolusi DNS diaktifkan

Nama host IPv4 DNS publik menyelesaikan ke IPv4 alamat pribadi instance.

Persyaratan

- Keduanya VPCs harus diaktifkan untuk nama host DNS dan resolusi DNS. Untuk informasi selengkapnya, lihat Atribut DNS untuk VPC Anda dalam Panduan Pengguna Amazon VPC.
- Koneksi mengintip harus di `active` negara bagian. Anda tidak dapat mengaktifkan resolusi DNS saat membuat koneksi peering.
- Pemilik VPC pemohon harus memodifikasi opsi peering VPC pemohon, dan pemilik VPC penerima harus memodifikasi opsi peering VPC penerima. Jika VPCs berada di akun dan Wilayah yang sama, Anda dapat mengaktifkan resolusi DNS untuk pemohon dan penerima VPCs pada saat yang sama.

Untuk mengaktifkan resolusi DNS untuk koneksi peering menggunakan konsol

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Koneksi peering.
3. Pilih koneksi peering VPC.

4. Pilih Tindakan, Edit pengaturan DNS.
5. Untuk mengaktifkan resolusi DNS untuk permintaan dari VPC pemohon, pilih Resolusi DNS Peminta, Izinkan VPC penerima untuk menyelesaikan DNS VPC pemohon.
6. Untuk memastikan resolusi DNS untuk permintaan dari VPC penerima, pilih Resolusi DNS Penerima, Izinkan VPC pemohon menyelesaikan DNS VPC penerima.
7. Pilih Simpan perubahan.

Untuk mengaktifkan resolusi DNS menggunakan baris perintah

- modify-vpc-peering-connection-pilihan ()AWS CLI
- Edit-EC2VpcPeeringConnectionOption (AWS Tools for Windows PowerShell)

Untuk menggambarkan opsi koneksi peering VPC menggunakan baris perintah

- describe-vpc-peering-connections (AWS CLI)
- Get-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

Hapus koneksi peering VPC

Pemilik VPC manapun dalam koneksi peering dapat menghapus koneksi peering VPC kapan saja. Anda juga dapat menghapus koneksi peering VPC yang Anda minta yang masih berstatus `pending-acceptance`.

Anda tidak dapat menghapus koneksi peering VPC ketika koneksi peering VPC berstatus `rejected`. Kami secara otomatis menghapus koneksi untuk anda.

Menghapus VPC di konsol Amazon VPC yang merupakan bagian dari koneksi peering VPC aktif juga akan menghapus koneksi peering VPC. Jika Anda telah meminta koneksi peering VPC dengan sebuah VPC di akun lain, dan Anda menghapus VPC Anda sebelum pihak lain menerima permintaan tersebut, koneksi peering VPC juga terhapus. Anda tidak dapat menghapus VPC yang telah menerima permintaan `pending-acceptance` dari sebuah VPC di akun lain. Anda harus terlebih dahulu menolak permintaan koneksi peering VPC.

Ketika Anda menghapus koneksi peering, status diatur ke `Deleting` dan kemudian`Deleted`. Setelah Anda menghapus koneksi, koneksi tidak dapat diterima, ditolak, atau diedit. Untuk informasi lebih lanjut tentang berapa lama koneksi peering tetap terlihat, lihatSiklus hidup koneksi peering VPC.

Untuk menghapus koneksi peering VPC

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Koneksi peering.
3. Pilih koneksi peering VPC.
4. Pilih Tindakan, Hapus koneksi peering.
5. Saat diminta konfirmasi, masukkan **`delete`**, lalu pilih Hapus.

Untuk menghapus koneksi peering VPC menggunakan baris perintah

- delete-vpc-peering-connection (AWS CLI)
- Remove-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

Memecahkan masalah koneksi peering VPC

Jika Anda mengalami masalah saat menghubungkan ke sumber daya di VPC dari sumber daya di VPC rekan, lakukan hal berikut:

- Untuk setiap sumber daya di setiap VPC, verifikasi bahwa tabel rute untuk subnetnya berisi rute yang mengirimkan lalu lintas yang ditujukan untuk VPC rekan ke koneksi peering VPC. Ini memastikan lalu lintas jaringan dapat mengalir dengan benar di antara keduanya VPCs. Untuk informasi selengkapnya, lihat Perbarui tabel rute.
- Untuk setiap EC2 kasus yang terlibat, verifikasi bahwa grup keamanan untuk instans tersebut mengizinkan lalu lintas masuk dan keluar dari VPC rekan. Aturan grup keamanan mengontrol lalu lintas mana yang diizinkan untuk mengakses EC2 instans Anda. Untuk informasi selengkapnya, lihat Referensi kelompok keamanan sejawat.
- Periksa apakah jaringan ACLs untuk subnet yang berisi sumber daya Anda memungkinkan lalu lintas yang diperlukan dari VPC rekan. Jaringan ACLs adalah lapisan keamanan tambahan yang menyaring lalu lintas di tingkat subnet.

Jika masih mengalami masalah, Anda dapat memanfaatkan Reachability Analyzer. Reachability Analyzer dapat membantu mengidentifikasi komponen tertentu - apakah tabel rute, grup keamanan, atau ACL jaringan - yang menyebabkan masalah konektivitas di antara keduanya. VPCs Untuk informasi selengkapnya, lihat Panduan Reachability Analyzer.

Memverifikasi konfigurasi jaringan VPC Anda secara menyeluruh adalah kunci untuk memecahkan masalah dan menyelesaikan masalah koneksi peering VPC yang mungkin Anda temui.

Konfigurasi koneksi peering VPC umum

Bagian ini menjelaskan dua jenis umum konfigurasi peering VPC yang dapat Anda terapkan:

- Konfigurasi peering VPC dengan rute ke seluruh VPC: Dalam konfigurasi ini, Anda membuat rute di setiap tabel rute VPC yang mengirimkan semua lalu lintas yang ditujukan untuk VPC rekan ke koneksi peering VPC. Ini memungkinkan sumber daya apa pun dalam satu VPC untuk berkomunikasi dengan sumber daya apa pun di VPC rekan, menyederhanakan manajemen. Namun, itu juga berarti bahwa semua lalu lintas antara VPCs akan mengalir melalui koneksi peering, yang bisa menjadi hambatan jika volume lalu lintas tinggi.
- Konfigurasi peering VPC dengan rute tertentu: Atau, Anda dapat membuat rute yang lebih terperinci di setiap tabel rute VPC yang hanya mengirim lalu lintas ke subnet atau sumber daya tertentu di VPC rekan. Ini memungkinkan Anda untuk membatasi lalu lintas yang mengalir melalui koneksi peering hanya untuk apa yang diperlukan, yang bisa lebih efisien. Namun, ini juga membutuhkan lebih banyak perawatan, karena Anda harus memperbarui tabel rute setiap kali Anda menambahkan sumber daya baru di VPC rekan yang perlu berkomunikasi.

Pendekatan terbaik tergantung pada faktor-faktor seperti ukuran dan kompleksitas arsitektur VPC Anda, volume lalu lintas yang diharapkan antara VPCs, dan kebutuhan organisasi Anda seputar keamanan dan akses sumber daya. Banyak perusahaan menggunakan pendekatan hibrida, dengan rute yang luas untuk pola lalu lintas umum dan rute khusus untuk kasus penggunaan yang lebih sensitif atau bandwidth intensif.

Konfigurasi

- Konfigurasi peering VPC dengan rute ke seluruh VPC
- Konfigurasi peering VPC dengan rute tertentu

Konfigurasi peering VPC dengan rute ke seluruh VPC

Anda dapat mengonfigurasi koneksi peering VPC sehingga tabel rute Anda memiliki akses ke seluruh blok CIDR pada rekan VPC. Untuk informasi selengkapnya tentang skenario di mana Anda mungkin memerlukan konfigurasi koneksi peering VPC tertentu, lihat Skenario jaringan koneksi peering VPC. Untuk informasi selengkapnya tentang membuat dan bekerja dengan koneksi peering VPC, lihat Koneksi peering VPC.

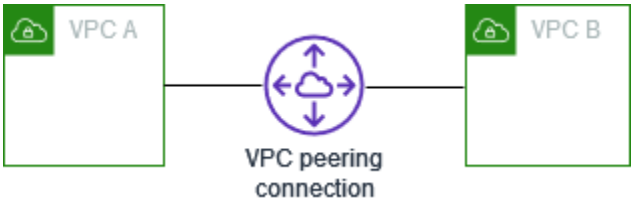
Untuk informasi selengkapnya tentang pembaruan tabel rute Anda, lihat Perbarui tabel rute Anda untuk koneksi peering VPC.

Konfigurasi

- Dua VPCs mengintip bersama
- Satu VPC mengintip dengan dua VPCs
- Tiga VPCs mengintip bersama
- Beberapa VPCs mengintip bersama

Dua VPCs mengintip bersama

Dalam konfigurasi ini, ada koneksi peering antara VPC A dan VPC B (). `pcx-11112222` Itu VPCs sama Akun AWS dan blok CIDR mereka tidak tumpang tindih.



Anda dapat menggunakan konfigurasi ini ketika Anda memiliki dua VPCs yang memerlukan akses ke sumber daya satu sama lain. Misalnya, Anda menyiapkan VPC A untuk catatan akuntansi dan VPC B untuk catatan keuangan Anda, dan masing-masing VPC ini harus dapat mengakses sumber daya dari VPC lain tanpa batasan.

CIDR VPC Tunggal

Perbarui tabel rute untuk setiap VPC dengan rute yang mengirimkan lalu lintas untuk blok CIDR dari VPC rekan ke koneksi peering VPC.

Tabel rute	Tujuan	Target
VPC A	*VPC A CIDR*	Lokal:
	VPC B CIDR	pcx-11112222
VPC B	*VPC B CIDR*	Lokal:
	VPC A CIDR	pcx-11112222

Beberapa IPv4 VPC CIDRs

Jika VPC A dan VPC B memiliki beberapa blok IPv4 CIDR terkait, Anda dapat memperbarui tabel rute untuk setiap VPC dengan rute untuk beberapa atau semua blok IPv4 CIDR dari VPC rekan.

Tabel rute	Tujuan	Target
VPC A	*VPC A CIDR 1*	Lokal:
	VPC A CIDR 2	Lokal:
	VPC B CIDR 1	pcx-11112222
	VPC B CIDR 2	pcx-11112222
VPC B	*VPC B CIDR 1*	Lokal:
	VPC B CIDR 2	Lokal:
	VPC A CIDR 1	pcx-11112222
	VPC A CIDR 2	pcx-11112222

IPv4 dan IPv6 VPC CIDRs

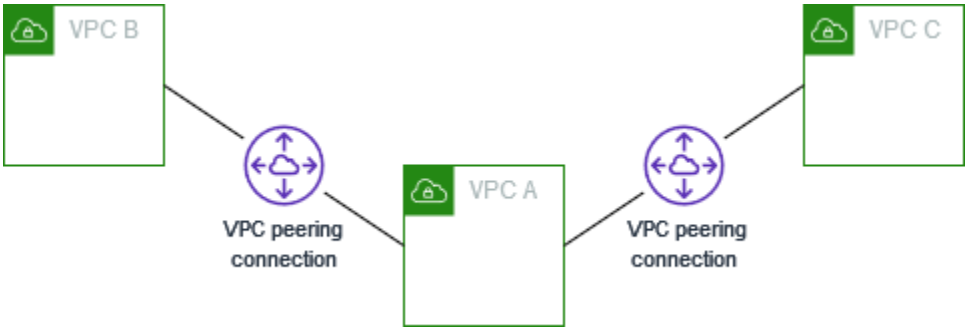
Jika VPC A dan VPC B memiliki blok IPv6 CIDR terkait, Anda dapat memperbarui tabel rute untuk setiap VPC dengan rute untuk blok IPv4 IPv6 CIDR dan VPC rekan.

Tabel rute	Tujuan	Target
VPC A	*VPC A IPv4 CIDR*	Lokal:
	VPC A IPv6 CIDR	Lokal:
	VPC B IPv4 CIDR	pcx-11112222
	VPC B IPv6 CIDR	pcx-11112222
VPC B	*VPC B IPv4 CIDR*	Lokal:

Tabel rute	Tujuan	Target
	VPC B IPv6 CIDR	Lokal:
	VPC A IPv4 CIDR	pcx-11112222
	VPC A IPv6 CIDR	pcx-11112222

Satu VPC mengintip dengan dua VPCs

Dalam konfigurasi ini, terdapat VPC pusat (VPC A), koneksi peering antara VPC A dan VPC `pcx-12121212` B (), dan koneksi peering antara VPC A dan VPC C (). `pcx-23232323` VPCs Ketiganya sama Akun AWS dan blok CIDR mereka tidak tumpang tindih.



VPC B dan VPC C tidak dapat mengirim lalu lintas langsung satu sama lain melalui VPC A, karena VPC peering tidak mendukung hubungan peering transitif. Anda dapat membuat koneksi peering VPC antara VPC B dan VPC C, seperti yang ditunjukkan pada. Tiga VPCs mengintip bersama Untuk informasi selengkapnya tentang skenario peering yang tidak di-support, lihat the section called "Keterbatasan peering VPC".

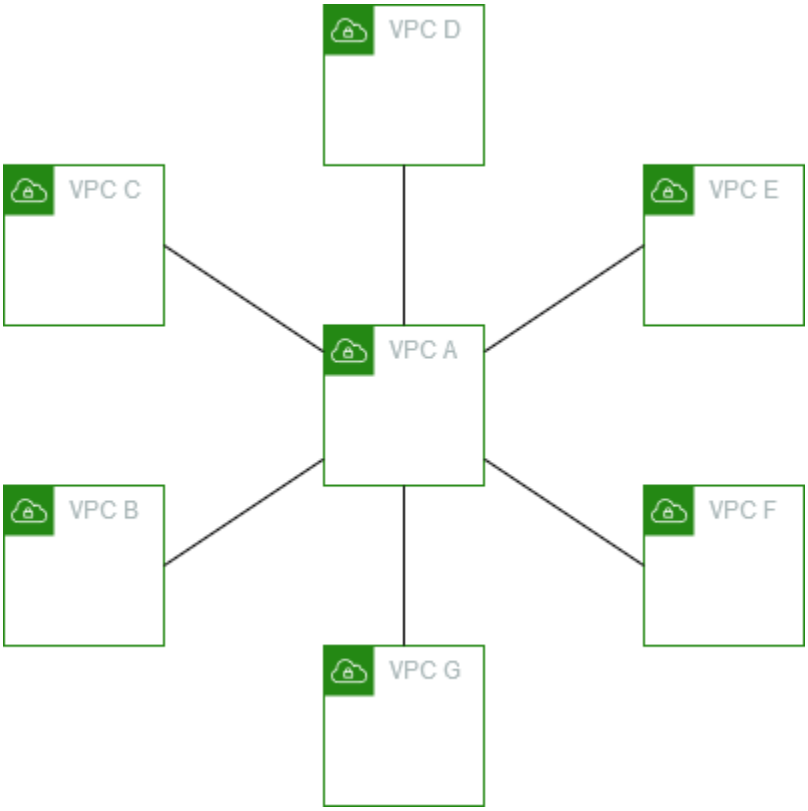
Anda dapat menggunakan konfigurasi ini ketika Anda memiliki sumber daya pada VPC pusat, seperti repositori layanan, yang lain VPCs perlu diakses. Yang lain VPCs tidak memerlukan akses ke sumber daya satu sama lain; mereka hanya perlu mengakses sumber daya di VPC pusat.

Perbarui tabel rute untuk setiap VPC sebagai berikut untuk mengimplementasikan konfigurasi ini menggunakan satu blok CIDR per VPC.

Tabel rute	Tujuan	Target
VPC A	*VPC A CIDR*	Lokal:

Tabel rute	Tujuan	Target
	VPC B CIDR	pcx-12121212
	VPC C CIDR	pcx-23232323
VPC B	*VPC B CIDR*	Lokal:
	VPC A CIDR	pcx-12121212
VPC C	*VPC C CIDR*	Lokal:
	VPC A CIDR	pcx-23232323

Anda dapat memperluas konfigurasi ini ke tambahan VPCs. Misalnya, VPC A diintip dengan VPC B melalui VPC G menggunakan IPv4 keduanya IPv6 CIDRs dan, tetapi yang lain tidak VPCs saling mengintip. Dalam diagram ini, garis mewakili koneksi peering VPC.



Perbarui tabel rute sebagai berikut.

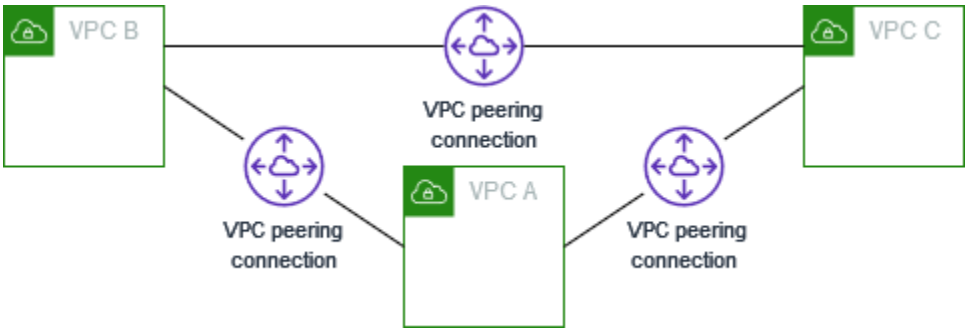
Tabel rute	Tujuan	Target
VPC A	*VPC A IPv4 CIDR*	Lokal:
	VPC A IPv6 CIDR	Lokal:
	VPC B IPv4 CIDR	pcx-aaaabbbb
	VPC B IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-aaaacccc
	VPC C IPv6 CIDR	pcx-aaaacccc
	VPC D IPv4 CIDR	pcx-aaaadddd
	VPC D IPv6 CIDR	pcx-aaaadddd
	VPC E IPv4 CIDR	pcx-aaaaeeee
	VPC E IPv6 CIDR	pcx-aaaaeeee
	VPC F IPv4 CIDR	pcx-aaaaffff
	VPC F IPv6 CIDR	pcx-aaaaffff
	VPC G IPv4 CIDR	pcx-aaaagggg
	VPC G IPv6 CIDR	pcx-aaaagggg
VPC B	*VPC B IPv4 CIDR*	Lokal:
	VPC B IPv6 CIDR	Lokal:
	VPC A IPv4 CIDR	pcx-aaaabbbb
	VPC A IPv6 CIDR	pcx-aaaabbbb
VPC C	*VPC C IPv4 CIDR*	Lokal:
	VPC C IPv6 CIDR	Lokal:

Tabel rute	Tujuan	Target
	VPC A IPv4 CIDR	pcx-aaaacccc
	VPC A IPv6 CIDR	pcx-aaaacccc
VPC D	*VPC D IPv4 CIDR*	Lokal:
	VPC D IPv6 CIDR	Lokal:
	VPC A IPv4 CIDR	pcx-aaaadddd
	VPC A IPv6 CIDR	pcx-aaaadddd
VPC E	*VPC E IPv4 CIDR*	Lokal:
	VPC E IPv6 CIDR	Lokal:
	VPC A IPv4 CIDR	pcx-aaaaeeee
	VPC A IPv6 CIDR	pcx-aaaaeeee
VPC F	*VPC F IPv4 CIDR*	Lokal:
	VPC F IPv6 CIDR	Lokal:
	VPC A IPv4 CIDR	pcx-aaaaffff
	VPC A IPv6 CIDR	pcx-aaaaffff
VPC G	*VPC G IPv4 CIDR*	Lokal:
	VPC G IPv6 CIDR	Lokal:
	VPC A IPv4 CIDR	pcx-aaaagggg
	VPC A IPv6 CIDR	pcx-aaaagggg

Tiga VPCs mengintip bersama

Dalam konfigurasi ini, ada tiga VPCs yang sama Akun AWS dengan blok CIDR yang tidak tumpang tindih. Yang VPCs diintip dalam jaring penuh sebagai berikut:

- VPC A disambungkan ke VPC B melalui koneksi peering VPC `pcx-aaaabbbb`
- VPC A disambungkan ke VPC C melalui koneksi peering VPC `pcx-aaaacccc`
- VPC B disambungkan ke VPC C melalui koneksi peering VPC `pcx-bbbbcccc`



Anda dapat menggunakan konfigurasi ini ketika Anda memiliki VPCs kebutuhan untuk berbagi sumber daya satu sama lain tanpa batasan. Misalnya, sebagai sistem berbagi file.

Perbarui tabel rute untuk setiap VPC sebagai berikut untuk mengimplementasikan konfigurasi ini.

Tabel rute	Tujuan	Target
VPC A	*VPC A CIDR*	Lokal:
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
VPC B	*VPC B CIDR*	Lokal:
	VPC A CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-bbbbcccc
VPC C	*VPC C CIDR*	Lokal:
	VPC A CIDR	pcx-aaaacccc

Tabel rute	Tujuan	Target
	VPC B CIDR	pcx-bbbbcccc

Jika VPC A dan VPC B memiliki keduanya IPv4 dan IPv6 blok CIDR, tetapi VPC C tidak memiliki blok IPv6 CIDR, perbarui tabel rute sebagai berikut. Sumber daya di VPC A dan VPC B dapat berkomunikasi menggunakan melalui IPv6 koneksi peering VPC. Namun, VPC C tidak dapat berkomunikasi dengan VPC A atau VPC B menggunakan. IPv6

Tabel rute	Tujuan	Target
VPC A	*VPC A IPv4 CIDR*	Lokal:
	VPC A IPv6 CIDR	Lokal:
	VPC B IPv4 CIDR	pcx-aaaabbbb
	VPC B IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-aaaacccc
VPC B	*VPC B IPv4 CIDR*	Lokal:
	VPC B IPv6 CIDR	Lokal:
	VPC A IPv4 CIDR	pcx-aaaabbbb
	VPC A IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-bbbbcccc
VPC C	*VPC C IPv4 CIDR*	Lokal:
	VPC A IPv4 CIDR	pcx-aaaacccc
	VPC B IPv4 CIDR	pcx-bbbbcccc

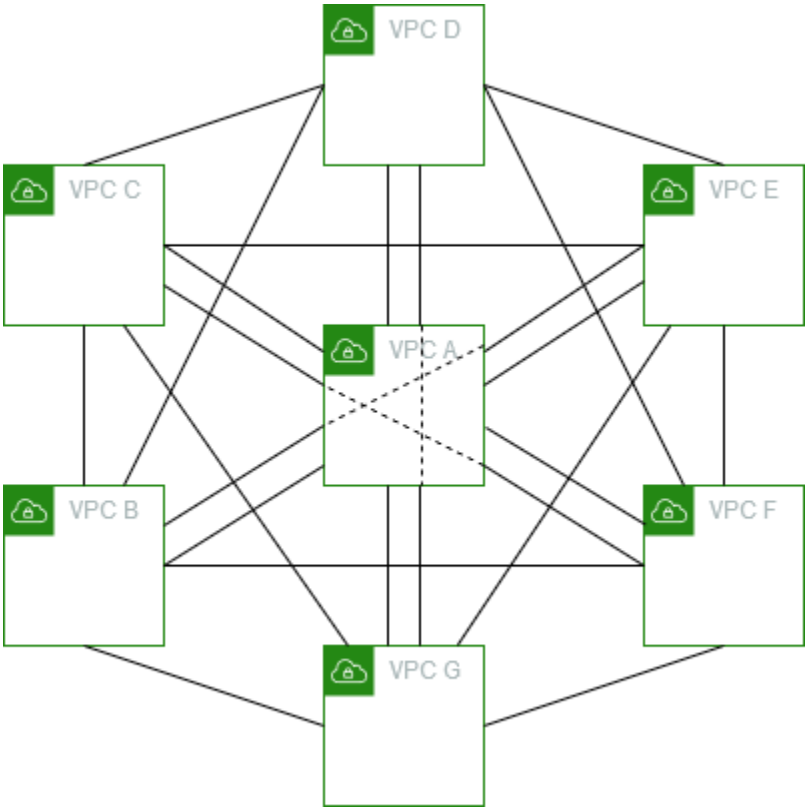
Beberapa VPCs mengintip bersama

Dalam konfigurasi ini, ada tujuh VPCs peered dalam konfigurasi full mesh. Itu VPCs sama Akun AWS dan blok CIDR mereka tidak tumpang tindih.

VPC	VPC	Koneksi peering VPC
A	B	pcx-aaaabbbb
A	C	pcx-aaaacccc
A	D	pcx-aaaadddd
A	E	pcx-aaaaeeee
A	F	pcx-aaaaffff
A	G	pcx-aaaagggg
B	C	pcx-bbbbcccc
B	D	pcx-bbbbdddd
B	E	pcx-bbbbeeee
B	F	pcx-bbbbffff
B	G	pcx-bbbbgggg
C	D	pcx-ccccdddd
C	E	pcx-cccceeee
C	F	pcx-ccccffff
C	G	pcx-ccccgggg
D	E	pcx-ddddeeee
D	F	pcx-ddddffff
D	G	pcx-ddddgggg

VPC	VPC	Koneksi peering VPC
E	F	pcx-eeeeffff
E	G	pcx-eeeegggg
F	G	pcx-ffffgggg

Anda dapat menggunakan konfigurasi ini ketika Anda memiliki beberapa VPCs yang harus dapat mengakses sumber daya satu sama lain tanpa batasan. Misalnya, sebagai jaringan berbagi file. Dalam diagram ini, garis mewakili koneksi peering VPC.



Perbarui tabel rute untuk setiap VPC sebagai berikut untuk mengimplementasikan konfigurasi ini.

Tabel rute	Tujuan	Target
VPC A	*VPC A CIDR*	Lokal:
	VPC B CIDR	pcx-aaaabbbb

Tabel rute	Tujuan	Target
	VPC C CIDR	pcx-aaaacccc
	VPC D CIDR	pcx-aaaadddd
	VPC E CIDR	pcx-aaaaeeee
	VPC F CIDR	pcx-aaaaffff
	VPC G CIDR	pcx-aaaagggg
VPC B	*VPC B CIDR*	Lokal:
	VPC A CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-bbbbcccc
	VPC D CIDR	pcx-bbbbdddd
	VPC E CIDR	pcx-bbbbeeee
	VPC F CIDR	pcx-bbbbffff
	VPC G CIDR	pcx-bbbbgggg
VPC C	*VPC C CIDR*	Lokal:
	VPC A CIDR	pcx-aaaacccc
	VPC B CIDR	pcx-bbbbcccc
	VPC D CIDR	pcx-ccccdddd
	VPC E CIDR	pcx-ccceeeee
	VPC F CIDR	pcx-ccccffff
	VPC G CIDR	pcx-ccccgggg
VPC D	*VPC D CIDR*	Lokal:

Tabel rute	Tujuan	Target
	VPC A CIDR	pcx-aaaadddd
	VPC B CIDR	pcx-bbbbdddd
	VPC C CIDR	pcx-ccccdddd
	VPC E CIDR	pcx-ddddeeee
	VPC F CIDR	pcx-ddddffff
	VPC G CIDR	pcx-ddddgggg
VPC E	*VPC E CIDR*	Lokal:
	VPC A CIDR	pcx-aaaaeeee
	VPC B CIDR	pcx-bbbbeeee
	VPC C CIDR	pcx-cccceeee
	VPC D CIDR	pcx-ddddeeee
	VPC F CIDR	pcx-eeeeffff
	VPC G CIDR	pcx-eeeegggg
VPC F	*VPC F CIDR*	Lokal:
	VPC A CIDR	pcx-aaaaffff
	VPC B CIDR	pcx-bbbbffff
	VPC C CIDR	pcx-ccccffff
	VPC D CIDR	pcx-ddddffff
	VPC E CIDR	pcx-eeeeffff
	VPC G CIDR	pcx-ffffgggg

Tabel rute	Tujuan	Target
VPC G	*VPC G CIDR*	Lokal:
	VPC A CIDR	pcx-aaaagggg
	VPC B CIDR	pcx-bbbbgggg
	VPC C CIDR	pcx-ccccgggg
	VPC D CIDR	pcx-ddddgggg
	VPC E CIDR	pcx-eeeegggg
	VPC F CIDR	pcx-ffffgggg

Jika semua VPCs memiliki blok IPv6 CIDR terkait, perbarui tabel rute sebagai berikut.

Tabel rute	Tujuan	Target
VPC A	*VPC A IPv4 CIDR*	Lokal:
	VPC A IPv6 CIDR	Lokal:
	VPC B IPv4 CIDR	pcx-aaaabbbb
	VPC B IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-aaaacccc
	VPC C IPv6 CIDR	pcx-aaaacccc
	VPC D IPv4 CIDR	pcx-aaaadddd
	VPC D IPv6 CIDR	pcx-aaaadddd
	VPC E IPv4 CIDR	pcx-aaaaeeee
	VPC E IPv6 CIDR	pcx-aaaaeeee

Tabel rute	Tujuan	Target
	VPC F IPv4 CIDR	pcx-aaaaffff
	VPC F IPv6 CIDR	pcx-aaaaffff
	VPC G IPv4 CIDR	pcx-aaaagggg
	VPC G IPv6 CIDR	pcx-aaaagggg
VPC B	*VPC B IPv4 CIDR*	Lokal:
	VPC B IPv6 CIDR	Lokal:
	VPC A IPv4 CIDR	pcx-aaaabbbb
	VPC A IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-bbbbcccc
	VPC C IPv6 CIDR	pcx-bbbbcccc
	VPC D IPv4 CIDR	pcx-bbbbdddd
	VPC D IPv6 CIDR	pcx-bbbbdddd
	VPC E IPv4 CIDR	pcx-bbbbeeee
	VPC E IPv6 CIDR	pcx-bbbbeeee
	VPC F IPv4 CIDR	pcx-bbbbffff
	VPC F IPv6 CIDR	pcx-bbbbffff
	VPC G IPv4 CIDR	pcx-bbbbgggg
	VPC G IPv6 CIDR	pcx-bbbbgggg
VPC C	*VPC C IPv4 CIDR*	Lokal:
	VPC C IPv6 CIDR	Lokal:

Tabel rute	Tujuan	Target
	VPC A IPv4 CIDR	pcx-aaaacccc
	VPC A IPv6 CIDR	pcx-aaaacccc
	VPC B IPv4 CIDR	pcx-bbbbcccc
	VPC B IPv6 CIDR	pcx-bbbbcccc
	VPC D IPv4 CIDR	pcx-ccccdddd
	VPC D IPv6 CIDR	pcx-ccccdddd
	VPC E IPv4 CIDR	pcx-cccceeee
	VPC E IPv6 CIDR	pcx-cccceeee
	VPC F IPv4 CIDR	pcx-ccccffff
	VPC F IPv6 CIDR	pcx-ccccffff
	VPC G IPv4 CIDR	pcx-ccccgggg
	VPC G IPv6 CIDR	pcx-ccccgggg
VPC D	*VPC D IPv4 CIDR*	Lokal:
	VPC D IPv6 CIDR	Lokal:
	VPC A IPv4 CIDR	pcx-aaaadddd
	VPC A IPv6 CIDR	pcx-aaaadddd
	VPC B IPv4 CIDR	pcx-bbbbdddd
	VPC B IPv6 CIDR	pcx-bbbbdddd
	VPC C IPv4 CIDR	pcx-ccccdddd
	VPC C IPv6 CIDR	pcx-ccccdddd

Tabel rute	Tujuan	Target
	VPC E IPv4 CIDR	pcx-ddddeeee
	VPC E IPv6 CIDR	pcx-ddddeeee
	VPC F IPv4 CIDR	pcx-ddddffff
	VPC F IPv6 CIDR	pcx-ddddffff
	VPC G IPv4 CIDR	pcx-ddddgggg
	VPC G IPv6 CIDR	pcx-ddddgggg
VPC E	*VPC E IPv4 CIDR*	Lokal:
	VPC E IPv6 CIDR	Lokal:
	VPC A IPv4 CIDR	pcx-aaaaeeee
	VPC A IPv6 CIDR	pcx-aaaaeeee
	VPC B IPv4 CIDR	pcx-bbbbeeee
	VPC B IPv6 CIDR	pcx-bbbbeeee
	VPC C IPv4 CIDR	pcx-cccceeee
	VPC C IPv6 CIDR	pcx-cccceeee
	VPC D IPv4 CIDR	pcx-ddddeeee
	VPC D IPv6 CIDR	pcx-ddddeeee
	VPC F IPv4 CIDR	pcx-eeeeffff
	VPC F IPv6 CIDR	pcx-eeeeffff
	VPC G IPv4 CIDR	pcx-eeeegggg
	VPC G IPv6 CIDR	pcx-eeeegggg

Tabel rute	Tujuan	Target
VPC F	*VPC F IPv4 CIDR*	Lokal:
	VPC F IPv6 CIDR	Lokal:
	VPC A IPv4 CIDR	pcx-aaaaffff
	VPC A IPv6 CIDR	pcx-aaaaffff
	VPC B IPv4 CIDR	pcx-bbbbffff
	VPC B IPv6 CIDR	pcx-bbbbffff
	VPC C IPv4 CIDR	pcx-ccccffff
	VPC C IPv6 CIDR	pcx-ccccffff
	VPC D IPv4 CIDR	pcx-ddddffff
	VPC D IPv6 CIDR	pcx-ddddffff
	VPC E IPv4 CIDR	pcx-eeeeffff
	VPC E IPv6 CIDR	pcx-eeeeffff
	VPC G IPv4 CIDR	pcx-ffffgggg
	VPC G IPv6 CIDR	pcx-ffffgggg
VPC G	*VPC G IPv4 CIDR*	Lokal:
	VPC G IPv6 CIDR	Lokal:
	VPC A IPv4 CIDR	pcx-aaaagggg
	VPC A IPv6 CIDR	pcx-aaaagggg
	VPC B IPv4 CIDR	pcx-bbbbgggg
	VPC B IPv6 CIDR	pcx-bbbbgggg

Tabel rute	Tujuan	Target
	VPC C IPv4 CIDR	pcx-ccccgggg
	VPC C IPv6 CIDR	pcx-ccccgggg
	VPC D IPv4 CIDR	pcx-ddddgggg
	VPC D IPv6 CIDR	pcx-ddddgggg
	VPC E IPv4 CIDR	pcx-eeeegggg
	VPC E IPv6 CIDR	pcx-eeeegggg
	VPC F IPv4 CIDR	pcx-ffffgggg
	VPC F IPv6 CIDR	pcx-ffffgggg

Konfigurasi peering VPC dengan rute tertentu

Anda dapat mengonfigurasi tabel rute untuk koneksi peering VPC untuk membatasi akses ke blok CIDR subnet, blok CIDR tertentu (jika VPC memiliki beberapa blok CIDR), atau sumber daya tertentu di VPC rekan. Dalam contoh ini, VPC pusat diintip ke setidaknya dua yang memiliki blok CIDR VPCs yang tumpang tindih.

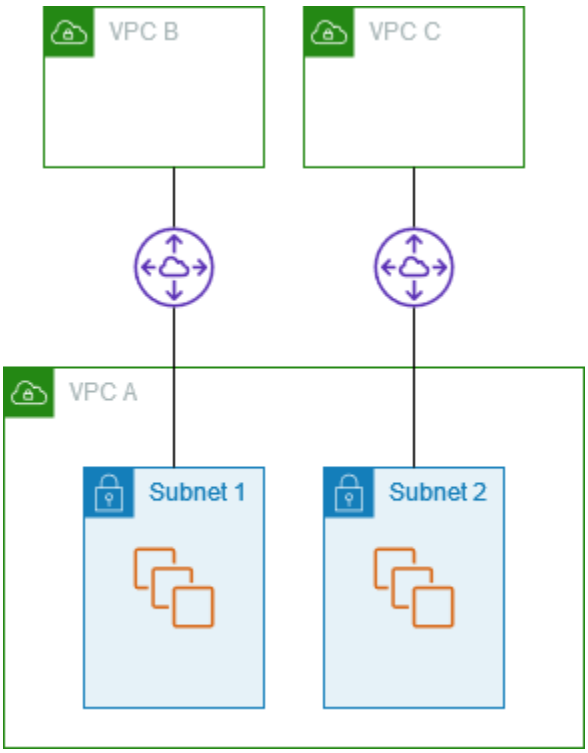
Untuk contoh skenario di mana Anda mungkin memerlukan konfigurasi koneksi peering VPC tertentu, lihat Skenario jaringan koneksi peering VPC. Untuk informasi selengkapnya tentang bekerja dengan koneksi peering VPC, lihat. Koneksi peering VPC Untuk informasi selengkapnya tentang pembaruan tabel rute Anda, lihat Perbarui tabel rute Anda untuk koneksi peering VPC.

Konfigurasi

- Dua VPCs yang mengakses subnet tertentu dalam satu VPC
- Dua VPCs yang mengakses blok CIDR tertentu dalam satu VPC
- Satu VPC yang mengakses subnet tertentu dalam dua VPCs
- Instans dalam satu VPC yang mengakses instance tertentu dalam dua VPCs
- Satu VPC yang mengakses dua VPCs menggunakan kecocokan awalan terpanjang
- Beberapa konfigurasi VPC

Dua VPCs yang mengakses subnet tertentu dalam satu VPC

Dalam konfigurasi ini, terdapat VPC pusat dengan dua subnet (VPC A), koneksi peering antara VPC A dan VPC B ()pcx-aaaabbbb, dan koneksi peering antara VPC A dan VPC C (). pcx-aaaacccc Setiap VPC memerlukan akses ke sumber daya hanya di salah satu subnet di VPC A.



Tabel rute untuk subnet 1 menggunakan pcx-aaaabbbb koneksi peering VPC untuk mengakses seluruh blok CIDR VPC B. Tabel rute untuk VPC B digunakan untuk mengakses blok CIDR subnet 1 di VPC pcx-aaaabbbb A. Tabel rute untuk subnet 2 menggunakan pcx-aaaacccc koneksi peering VPC untuk mengakses seluruh blok CIDR VPC C. Tabel rute untuk tabel VPC C digunakan untuk mengakses blok CIDR subnet 2 di VPC A. pcx-aaaacccc

Tabel rute	Tujuan	Target
Subnet 1 (VPC A)	*VPC A CIDR*	Lokal:
	VPC B CIDR	pcx-aaaabbbb
Subnet 2 (VPC A)	*VPC A CIDR*	Lokal:
	VPC C CIDR	pcx-aaaacccc

Tabel rute	Tujuan	Target
VPC B	*VPC B CIDR*	Lokal:
	Subnet 1 CIDR	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Lokal:
	Subnet 2 CIDR	pcx-aaaacccc

Anda dapat memperluas konfigurasi ini ke beberapa blok CIDR. Misalkan VPC A dan VPC B memiliki keduanya IPv4 dan blok IPv6 CIDR, dan subnet 1 memiliki blok CIDR terkait. IPv6 Anda dapat mengaktifkan VPC B untuk berkomunikasi dengan subnet 1 di VPC A melalui menggunakan IPv6 koneksi peering VPC. Untuk melakukan ini, tambahkan rute ke tabel rute untuk VPC A dengan tujuan blok IPv6 CIDR untuk VPC B, dan rute ke tabel rute untuk VPC B dengan tujuan IPv6 CIDR subnet 1 di VPC A.

Tabel rute	Tujuan	Target	Catatan
Subnet 1 di VPC A	*VPC A IPv4 CIDR*	Lokal:	
	VPC A IPv6 CIDR	Lokal:	Rute lokal yang ditambahkan secara otomatis untuk IPv6 komunikasi dalam VPC.
	VPC B IPv4 CIDR	pcx-aaaabbbb	
	VPC B IPv6 CIDR	pcx-aaaabbbb	Rute ke blok IPv6 CIDR VPC B.
Subnet 2 di VPC A	*VPC A IPv4 CIDR*	Lokal:	
	VPC A IPv6 CIDR	Lokal:	Rute lokal yang ditambahkan secara otomatis untuk IPv6

Tabel rute	Tujuan	Target	Catatan
			komunikasi dalam VPC.
	VPC C IPv4 CIDR	pcx-aaaacccc	
VPC B	*VPC B IPv4 CIDR*	Lokal:	
	VPC B IPv6 CIDR	Lokal:	Rute lokal yang ditambahkan secara otomatis untuk IPv6 komunikasi dalam VPC.
	Subnet 1 IPv4 CIDR	pcx-aaaabbbb	
	Subnet 1 IPv6 CIDR	pcx-aaaabbbb	Rute ke blok IPv6 CIDR VPC A.
VPC C	*VPC C IPv4 CIDR*	Lokal:	
	Subnet 2 IPv4 CIDR	pcx-aaaacccc	

Dua VPCs yang mengakses blok CIDR tertentu dalam satu VPC

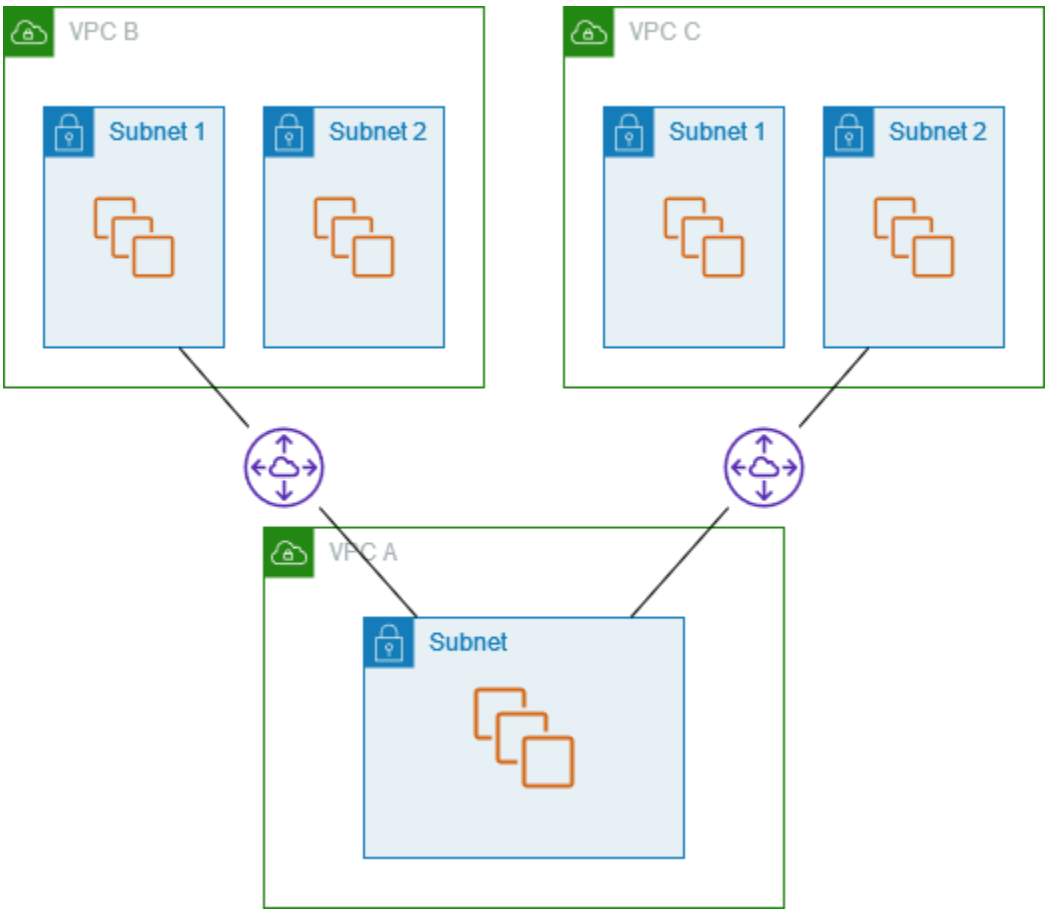
Dalam konfigurasi ini, terdapat VPC pusat (VPC A), koneksi peering antara VPC A dan VPC `pcx-aaaabbbb` B (), dan koneksi peering antara VPC A dan VPC C (). `pcx-aaaacccc` VPC A memiliki satu blok CIDR untuk setiap koneksi peering.

Tabel rute	Tujuan	Target
VPC A	*VPC A CIDR 1*	Lokal:
	VPC A CIDR 2	Lokal:
	VPC B CIDR	pcx-aaaabbbb

Tabel rute	Tujuan	Target
	VPC C CIDR	pcx-aaaacccc
VPC B	*VPC B CIDR*	Lokal:
	VPC A CIDR 1	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Lokal:
	VPC A CIDR 2	pcx-aaaacccc

Satu VPC yang mengakses subnet tertentu dalam dua VPCs

Dalam konfigurasi ini, terdapat VPC pusat (VPC A) dengan satu subnet, koneksi peering antara VPC A dan VPC B ()pcx-aaaabbbb, dan koneksi peering antara VPC A dan VPC C (). pcx-aaaacccc VPC B dan VPC C masing-masing memiliki dua subnet. Koneksi peering antara VPC A dan VPC B hanya menggunakan salah satu subnet di VPC B. Koneksi peering antara VPC A dan VPC C hanya menggunakan salah satu subnet di VPC C.



Gunakan konfigurasi ini ketika Anda memiliki VPC pusat yang memiliki satu set sumber daya, seperti layanan Active Directory, yang lain VPCs perlu diakses. VPC pusat tidak memerlukan akses penuh ke VPCs yang diintip.

Tabel rute untuk VPC A menggunakan koneksi peering untuk mengakses hanya subnet tertentu di peered. VPCs Tabel rute untuk subnet 1 menggunakan koneksi peering dengan VPC A untuk mengakses subnet di VPC A. Tabel rute untuk subnet 2 menggunakan koneksi peering dengan VPC A untuk mengakses subnet di VPC A.

Tabel rute	Tujuan	Target
VPC A	*VPC A CIDR*	Lokal:
	Subnet 1 CIDR	pcx-aaaabbbb
	Subnet 2 CIDR	pcx-aaaacccc
Subnet 1 (VPC B)	*VPC B CIDR*	Lokal:

Tabel rute	Tujuan	Target
	Subnet in VPC A CIDR	pcx-aaaabbbb
Subnet 2 (VPC C)	*VPC C CIDR*	Lokal:
	Subnet in VPC A CIDR	pcx-aaaacccc

Perutean untuk lalu lintas respons

Jika Anda memiliki VPC yang diintip dengan beberapa blok CIDR VPCs yang tumpang tindih atau cocok, pastikan tabel rute Anda dikonfigurasi untuk menghindari pengiriman lalu lintas respons dari VPC Anda ke VPC yang salah. AWS tidak mendukung penerusan jalur balik unicast dalam koneksi peering VPC yang memeriksa IP sumber paket dan merutekan paket balasan kembali ke sumbernya.

Misalnya, VPC A disambungkan dengan VPC B dan VPC C. VPC B dan VPC C memiliki blok CIDR yang cocok, dan subnet-subnet mereka memiliki blok CIDR yang cocok. Tabel rute untuk subnet 2 di VPC B menunjuk ke koneksi peering VPC `pcx-aaaabbbb` untuk mengakses subnet VPC A. Tabel rute VPC A dikonfigurasi untuk mengirim lalu lintas yang ditujukan untuk VPC CIDR ke koneksi peering. `pcx-aaaaccccc`

Tabel rute	Tujuan	Target
Subnet 2 (VPC B)	*VPC B CIDR*	Lokal:
	Subnet in VPC A CIDR	pcx-aaaabbbb
VPC A	*VPC A CIDR*	Lokal:
	VPC C CIDR	pcx-aaaacccc

Misalkan sebuah instance di subnet 2 di VPC B mengirimkan lalu lintas ke server Active Directory di VPC A menggunakan koneksi peering VPC. `pcx-aaaabbbb` VPC A mengirimkan lalu lintas respons ke server Active Directory. Namun, tabel rute VPC A dikonfigurasi untuk mengirim semua lalu lintas dalam rentang VPC CIDR ke koneksi peering VPC. `pcx-aaaacccc` Jika subnet 2 di VPC C memiliki instance dengan alamat IP yang sama dengan instance di subnet dua dari VPC B, ia

menerima lalu lintas respons dari VPC A. Instans di subnet 2 di VPC B tidak menerima tanggapan atas permintaannya ke VPC A.

Untuk mencegah hal ini, Anda dapat menambahkan rute tertentu ke tabel rute VPC A dengan CIDR subnet 2 di VPC B sebagai tujuan dan target. `pcx-aaaabbbb` Rute baru lebih spesifik, oleh karena itu lalu lintas yang ditujukan untuk subnet 2 CIDR dialihkan ke koneksi peering VPC `pcx-aaaabbbb`

Atau, dalam contoh berikut, tabel rute VPC A memiliki rute untuk setiap subnet untuk setiap koneksi peering VPC. VPC A dapat berkomunikasi dengan subnet 2 di VPC B dan dengan subnet 1 di VPC C. Skenario ini berguna jika Anda perlu menambahkan koneksi peering VPC lain dengan subnet lain yang berada dalam kisaran alamat yang sama seperti VPC B dan VPC C -Anda cukup menambahkan rute lain untuk subnet tertentu.

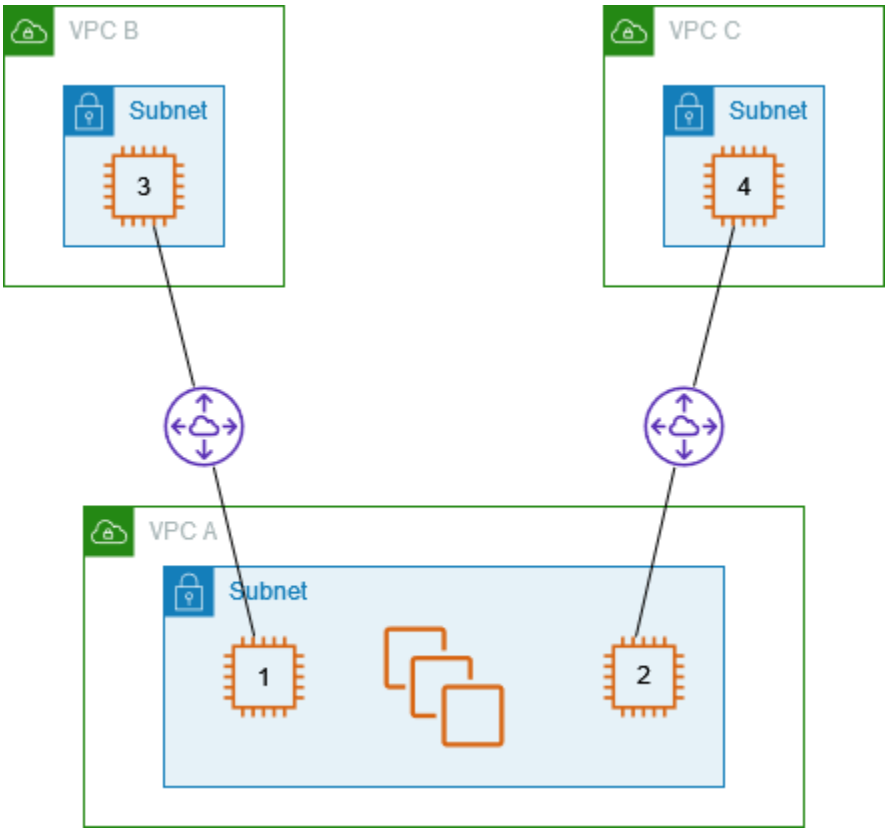
Tujuan	Target
VPC A CIDR	Lokal:
Subnet 2 CIDR	pcx-aaaabbbb
Subnet 1 CIDR	pcx-aaaacccc

Sebagai alternatif, tergantung pada kasus penggunaan Anda, Anda dapat membuat rute ke alamat IP tertentu di VPC B untuk memastikan bahwa lalu lintas diarahkan kembali ke server yang benar (tabel rute menggunakan pencocokan prefiks terpanjang untuk memprioritaskan rute):

Tujuan	Target
VPC A CIDR	Lokal:
Specific IP address in subnet 2	pcx-aaaabbbb
VPC B CIDR	pcx-aaaacccc

Instans dalam satu VPC yang mengakses instance tertentu dalam dua VPCs

Dalam konfigurasi ini, terdapat VPC pusat (VPC A) dengan satu subnet, koneksi peering antara VPC A dan VPC B ()`pcx-aaaabbbb`, dan koneksi peering antara VPC A dan VPC C (). `pcx-aaaacccc` VPC A memiliki subnet dengan satu instance untuk setiap koneksi peering. Anda dapat menggunakan konfigurasi ini untuk membatasi lalu lintas peering ke instance tertentu.



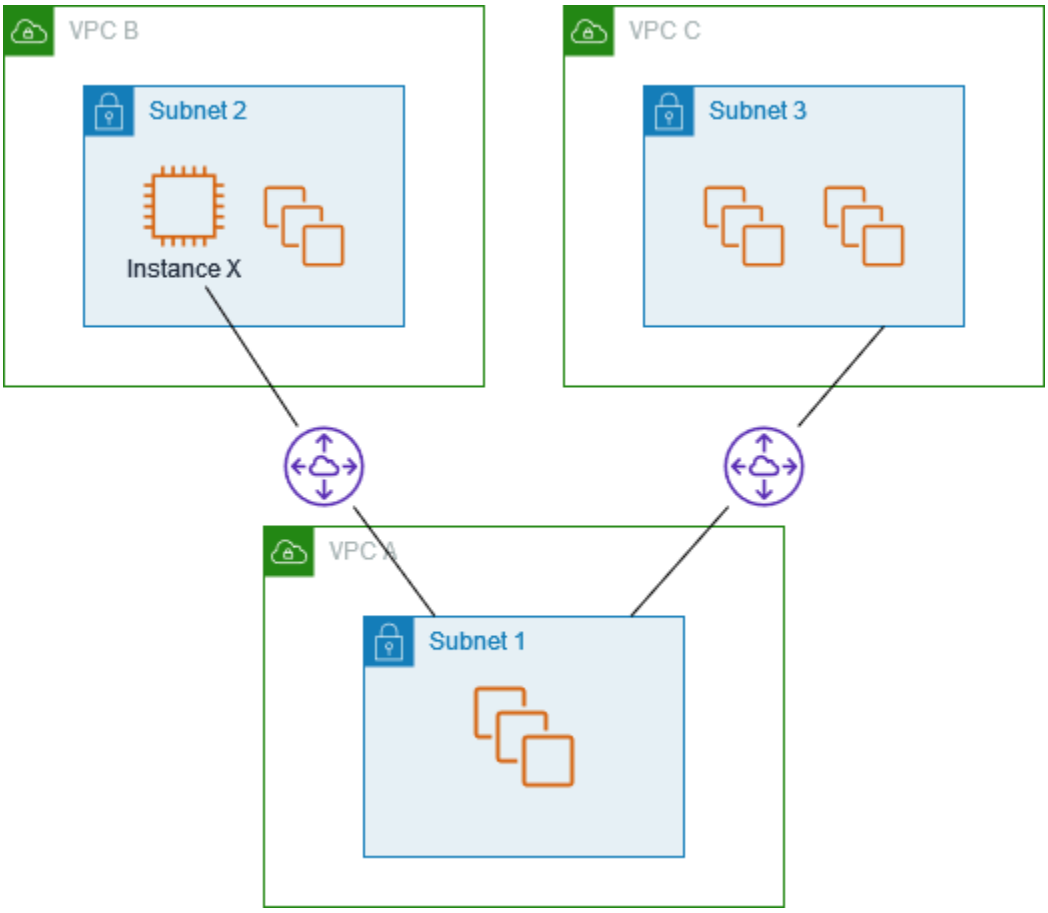
Setiap tabel rute VPC mengacu ke koneksi peering VPC yang relevan untuk mengakses sebuah alamat IP (dan karena itulah terdapat instans khusus) di VPC rekan.

Tabel rute	Tujuan	Target
VPC A	*VPC A CIDR*	Lokal:
	Instance 3 IP address	pcx-aaaabbbb
	Instance 4 IP address	pcx-aaaacccc
VPC B	*VPC B CIDR*	Lokal:

Tabel rute	Tujuan	Target
	Instance 1 IP address	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Lokal:
	Instance 2 IP address	pcx-aaaacccc

Satu VPC yang mengakses dua VPCs menggunakan kecocokan awalan terpanjang

Dalam konfigurasi ini, terdapat VPC pusat (VPC A) dengan satu subnet, koneksi peering antara VPC A dan VPC B ()`pcx-aaaabbbb`, dan koneksi peering antara VPC A dan VPC C (). `pcx-aaaacccc` VPC B dan VPC C memiliki blok CIDR yang cocok. Anda menggunakan koneksi peering VPC `pcx-aaaabbbb` untuk merutekan lalu lintas antara VPC A dan instance tertentu di VPC B. Semua lalu lintas lain yang ditujukan untuk rentang alamat CIDR yang dibagikan oleh VPC B dan VPC C dialihkan ke VPC C melalui. `pcx-aaaacccc`



Tabel rute VPC menggunakan pencocokan prefiks terpanjang untuk memilih rute yang paling spesifik di seluruh koneksi peering VPC yang dimaksud. Semua lalu lintas lain diarahkan melalui rute pencocokan berikutnya, dalam hal ini, di seluruh koneksi peering VPC `pcx-aaaacccc`.

Tabel rute	Tujuan	Target
VPC A	*VPC A CIDR block*	Lokal:
	Instance X IP address	pcx-aaaabbbb
	VPC C CIDR block	pcx-aaaacccc
VPC B	*VPC B CIDR block*	Lokal:
	VPC A CIDR block	pcx-aaaabbbb
VPC C	*VPC C CIDR block*	Lokal:
	VPC A CIDR block	pcx-aaaacccc

Important

Jika instance selain instance X di VPC B mengirimkan lalu lintas ke VPC A, lalu lintas respons mungkin diarahkan ke VPC C, bukan VPC B. Untuk informasi lebih lanjut, lihat. Perutean untuk lalu lintas respons

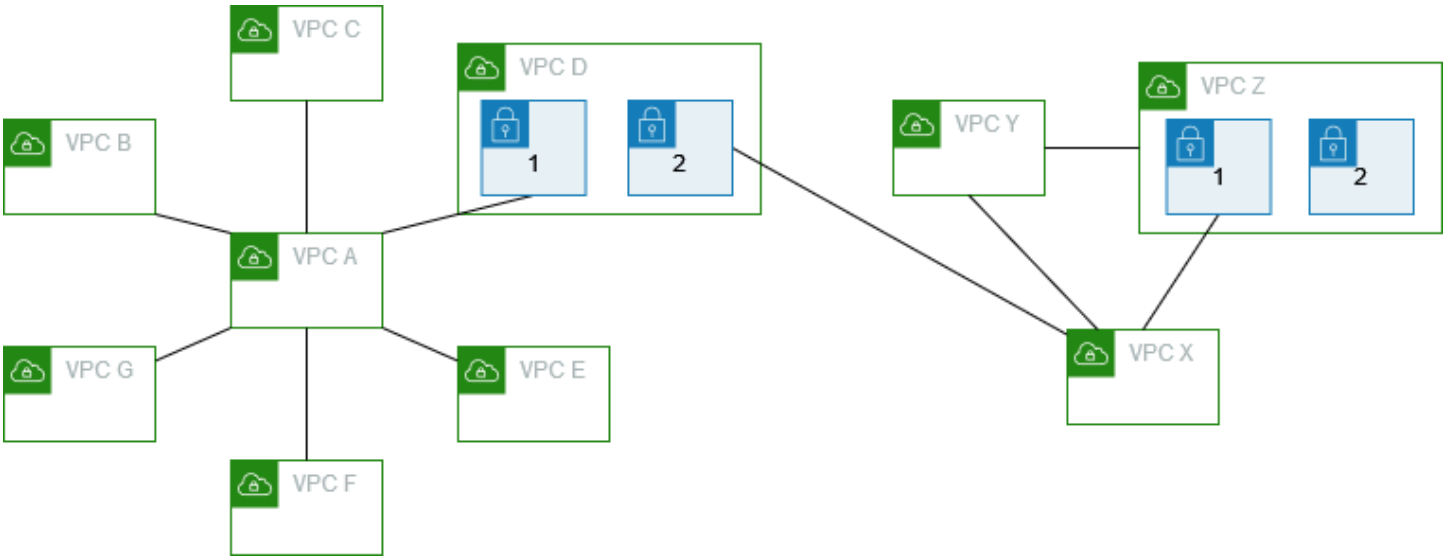
Beberapa konfigurasi VPC

Dalam konfigurasi ini, ada VPC pusat (VPC A) yang diintip dengan beberapa VPCs dalam konfigurasi spoke. Anda juga memiliki tiga VPCs (VPCs X, Y, dan Z) yang diintip dalam konfigurasi mesh penuh.

VPC D juga memiliki koneksi peering VPC dengan VPC X (). `pcx-ddddxxxx` VPC A dan VPC X memiliki blok CIDR yang tumpang tindih. Ini berarti bahwa peering lalu lintas antara VPC A dan VPC D terbatas pada subnet tertentu (subnet 1) di VPC D. Ini untuk memastikan bahwa jika VPC D menerima permintaan dari VPC A atau VPC X, ia mengirimkan lalu lintas respons ke VPC yang benar. AWS tidak mendukung penerusan jalur balik unicast dalam koneksi peering VPC yang

memeriksa IP sumber paket dan merutekan paket balasan kembali ke sumbernya. Untuk informasi selengkapnya, lihat Perutean untuk lalu lintas respons.

Demikian pula, VPC D dan VPC Z memiliki blok CIDR yang tumpang tindih. Lalu lintas peering antara VPC D dan VPC X terbatas pada subnet 2 di VPC D, dan lalu lintas peering antara VPC X dan VPC Z terbatas pada subnet 1 di VPC Z. Ini untuk memastikan bahwa jika VPC X menerima lalu lintas peering dari VPC D atau VPC Z, ia mengirimkan lalu lintas respons kembali ke yang benar VPC.



Tabel rute untuk VPCs B, C, E, F, dan G menunjuk ke koneksi peering yang relevan untuk mengakses blok CIDR penuh untuk VPC A, dan tabel rute VPC A menunjuk ke koneksi peering yang relevan untuk VPCs B, C, E, F, dan G untuk mengakses blok CIDR lengkapnya. Untuk koneksi peering`pcx-aaaadddd`, tabel rute VPC A merutekan lalu lintas hanya ke subnet 1 di VPC D dan tabel rute subnet 1 di VPC D menunjuk ke blok CIDR penuh VPC A.

Tabel rute VPC Y menunjuk ke koneksi peering yang relevan untuk mengakses blok CIDR penuh VPC X dan VPC Z, dan tabel rute VPC Z menunjuk ke koneksi peering yang relevan untuk mengakses blok CIDR penuh VPC Y. Tabel rute subnet 1 di VPC Z menunjuk ke koneksi peering yang relevan untuk mengakses blok CIDR penuh VPC Tabel rute VPC X menunjuk ke koneksi peering yang relevan untuk mengakses subnet 2 di VPC D dan subnet 1 di VPC Z.

Tabel rute	Tujuan	Target
VPC A	*VPC A CIDR*	Lokal:
	VPC B CIDR	pcx-aaaabbbb

Tabel rute	Tujuan	Target
	VPC C CIDR	pcx-aaaacccc
	Subnet 1 CIDR in VPC D	pcx-aaaadddd
	VPC E CIDR	pcx-aaaaeeee
	VPC F CIDR	pcx-aaaaffff
	VPC G CIDR	pcx-aaaagggg
VPC B	*VPC B CIDR*	Lokal:
	VPC A CIDR	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Lokal:
	VPC A CIDR	pcx-aaaacccc
Subnet 1 di VPC D	*VPC D CIDR*	Lokal:
	VPC A CIDR	pcx-aaaadddd
Subnet 2 di VPC D	*VPC D CIDR*	Lokal:
	VPC X CIDR	pcx-ddddxxxx
VPC E	*VPC E CIDR*	Lokal:
	VPC A CIDR	pcx-aaaaeeee
VPC F	*VPC F CIDR*	Lokal:
	VPC A CIDR	pcx-aaaaffff
VPC G	*VPC G CIDR*	Lokal:
	VPC A CIDR	pcx-aaaagggg
VPC X	*VPC X CIDR*	Lokal:

Tabel rute	Tujuan	Target
	Subnet 2 CIDR in VPC D	pcx-ddddxxxx
	VPC Y CIDR	pcx-xxxxyyyy
	Subnet 1 CIDR in VPC Z	pcx-xxxxzzzz
VPC Y	*VPC Y CIDR*	Lokal:
	VPC X CIDR	pcx-xxxxyyyy
	VPC Z CIDR	pcx-yyyzzzz
VPC Z	*VPC Z CIDR*	Lokal:
	VPC Y CIDR	pcx-yyyzzzz
	VPC X CIDR	pcx-xxxxzzzz

Skenario jaringan koneksi peering VPC

Ada sejumlah alasan mengapa Anda mungkin perlu mengatur koneksi peering VPC antara Anda VPCs, atau antara VPC yang Anda miliki dan VPC di akun yang berbeda. AWS Skenario berikut ini dapat membantu Anda menentukan konfigurasi yang paling sesuai dengan kebutuhan jaringan Anda.

Skenario

- Mengintip dua atau lebih VPCs untuk menyediakan akses penuh ke sumber daya
- Menyambung ke satu VPC untuk mengakses sumber daya terpusat

Mengintip dua atau lebih VPCs untuk menyediakan akses penuh ke sumber daya

Dalam skenario ini, Anda memiliki dua atau lebih VPCs yang ingin Anda peer untuk memungkinkan berbagi sumber daya secara penuh di antara semuanya VPCs. Berikut ini beberapa contohnya:

- Perusahaan Anda memiliki sebuah VPC untuk departemen keuangan, dan VPC lain untuk departemen akuntansi. Departemen keuangan memerlukan akses ke semua sumber daya yang berada di departemen akuntansi, dan departemen akuntansi memerlukan akses ke semua sumber daya di departemen keuangan.
- Perusahaan Anda memiliki beberapa departemen IT, masing-masing dengan VPC mereka sendiri. Beberapa VPCs berada dalam AWS akun yang sama, dan yang lain di AWS akun yang berbeda. Anda ingin menyatukan semua VPCs untuk memungkinkan departemen TI memiliki akses penuh ke sumber daya satu sama lain.

Untuk informasi lebih lanjut tentang cara mengatur konfigurasi koneksi peering VPC dan tabel rute untuk skenario ini, lihat dokumentasi berikut:

- Dua VPCs mengintip bersama
- Tiga VPCs mengintip bersama
- Beberapa VPCs mengintip bersama

Untuk informasi lebih lanjut tentang membuat dan bekerja dengan koneksi peering VPC di konsol Amazon VPC, lihat Koneksi peering VPC.

Menyambung ke satu VPC untuk mengakses sumber daya terpusat

Dalam skenario ini, Anda memiliki VPC pusat yang berisi sumber daya yang ingin Anda bagikan dengan orang lain. VPCs VPC pusat Anda mungkin memerlukan akses penuh atau sebagian ke rekan VPCs, dan demikian pula, rekan VPCs mungkin memerlukan akses penuh atau sebagian ke VPC pusat. Berikut ini beberapa contohnya:

- Departemen IT perusahaan Anda memiliki sebuah VPC untuk berbagi file. Anda ingin mengintip orang lain VPCs ke VPC pusat itu, namun, Anda tidak ingin yang VPCs lain mengirim lalu lintas satu sama lain.
- Perusahaan Anda memiliki sebuah VPC yang ingin Anda bagikan dengan pelanggan Anda. Setiap pelanggan dapat membuat koneksi peering VPC dengan VPC Anda, namun, pelanggan Anda tidak dapat merutekan lalu lintas ke VPCs yang lain yang diintip ke Anda, juga tidak mengetahui rute pelanggan lain.
- Anda memiliki VPC pusat yang digunakan untuk layanan Direktori Aktif. Contoh spesifik dalam permintaan VPCs kirim rekan ke server Active Directory dan memerlukan akses penuh ke VPC pusat. VPC pusat tidak memerlukan akses penuh ke rekan VPCs; hanya perlu mengarahkan lalu lintas respons ke instance tertentu.

Untuk informasi lebih lanjut tentang membuat dan bekerja dengan koneksi peering VPC di konsol Amazon VPC, lihat Koneksi peering VPC.

Identity and access management untuk peering VPC

Secara default, pengguna tidak dapat membuat atau memodifikasi koneksi peering VPC. Untuk memberikan akses ke sumber daya peering VPC, lampirkan kebijakan IAM ke identitas IAM, seperti peran.

Contoh

- Contoh: Buat koneksi peering VPC
- Contoh: Terima koneksi peering VPC
- Contoh: Hapus koneksi peering VPC
- Contoh: Bekerja dalam akun tertentu
- Contoh: Kelola koneksi peering VPC menggunakan konsol

Untuk daftar tindakan VPC Amazon, serta kunci sumber daya dan kondisi yang didukung untuk setiap tindakan, lihat Tindakan, sumber daya, dan kunci kondisi untuk Amazon EC2 di Referensi Otorisasi Layanan.

Contoh: Buat koneksi peering VPC

Kebijakan berikut memberi pengguna izin untuk membuat permintaan koneksi peering VPC VPCs menggunakan yang diberi tag. `Purpose=Peering` Pernyataan pertama menerapkan kunci persyaratan (`ec2:ResourceTag`) ke sumber daya VPC. Perhatikan bahwa sumber daya VPC untuk tindakan `CreateVpcPeeringConnection` adalah selalu VPC peminta.

Pernyataan kedua memberikan izin kepada pengguna untuk membuat sumber daya koneksi peering VPC, dan karenanya menggunakan wildcard * sebagai pengganti ID sumber daya tertentu.

JSON

```
{
  "Version": "2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
```

```
      "Resource": "arn:aws:ec2:region:account-id:vpc/*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Purpose": "Peering"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id:vpc-peering-connection/*"
    }
  ]
}
```

Kebijakan berikut memberi pengguna izin AWS akun yang ditentukan untuk membuat koneksi peering VPC menggunakan VPC apa pun di Wilayah tertentu, tetapi hanya jika VPC yang menerima koneksi peering adalah VPC tertentu di akun tertentu.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect":"Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id-1:vpc/*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id-1:vpc-peering-connection/*",
      "Condition": {
        "ArnEquals": {
          "ec2:AccepterVpc": "arn:aws:ec2:region:account-id-2:vpc/vpc-id"
        }
      }
    }
  ]
}
```

Contoh: Terima koneksi peering VPC

Kebijakan berikut memberikan izin kepada pengguna untuk menerima permintaan koneksi peering VPC dari akun tertentu. AWS Hal ini membantu untuk mencegah pengguna menerima koneksi peering VPC dari akun tak dikenal. Pernyataan menggunakan kunci `ec2:RequesterVpc` kondisi untuk menegakkan ini.

JSON

```
{
  "Version": "2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action": "ec2:AcceptVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id-1:vpc-peering-connection/*",
      "Condition": {
        "ArnEquals": {
          "ec2:RequesterVpc": "arn:aws:ec2:region:account-id-2:vpc/*"
        }
      }
    }
  ]
}
```

Kebijakan berikut memberikan izin kepada pengguna untuk menerima permintaan peering VPC jika VPC memiliki tag. `Purpose=Peering`

JSON

```
{
  "Version": "2012-10-17",
  "Statement":[
    {
      "Effect": "Allow",
      "Action": "ec2:AcceptVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id:vpc/*",
      "Condition": {
        "StringEquals": {
```

```
          "ec2:ResourceTag/Purpose": "Peering"
        }
      }
    }
  ]
}
```

Contoh: Hapus koneksi peering VPC

Kebijakan berikut memberi pengguna izin akun yang ditentukan untuk menghapus koneksi peering VPC apa pun, kecuali yang menggunakan VPC yang ditentukan, yang berada di akun yang sama. Kebijakan menentukan kunci `ec2:AccepterVpc` dan `ec2:RequesterVpc` kondisi, karena VPC mungkin adalah VPC pemohon atau VPC rekan dalam permintaan koneksi peering VPC asli.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect":"Allow",
      "Action": "ec2:DeleteVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id:vpc-peering-connection/*",
      "Condition": {
        "ArnNotEquals": {
          "ec2:AccepterVpc": "arn:aws:ec2:region:account-id:vpc/vpc-id",
          "ec2:RequesterVpc": "arn:aws:ec2:region:account-id:vpc/vpc-id"
        }
      }
    }
  ]
}
```

Contoh: Bekerja dalam akun tertentu

Kebijakan berikut memberikan izin kepada pengguna untuk bekerja dengan koneksi peering VPC dalam akun tertentu. Pengguna dapat melihat, membuat, menerima, menolak, dan menghapus koneksi peering VPC, asalkan semuanya berada dalam akun yang sama. AWS

Pernyataan pertama memberi pengguna izin untuk melihat semua koneksi peering VPC. Elemen `Resource` membutuhkan sebuah wildcard * dalam hal ini, sebagai tindakan API ini (`DescribeVpcPeeringConnections`) saat ini tidak men-support izin di tingkat sumber daya.

Pernyataan kedua memberikan izin kepada pengguna untuk membuat koneksi peering VPC, dan akses ke VPCs semua akun yang ditentukan untuk melakukannya.

Pernyataan ketiga menggunakan wildcard * sebagai bagian dari `Action` elemen untuk memberikan izin untuk semua tindakan koneksi peering VPC. Kunci kondisi memastikan bahwa tindakan hanya dapat dilakukan pada koneksi peering VPC dengan VPCs yang merupakan bagian dari akun. Misalnya, pengguna tidak dapat menghapus koneksi peering VPC jika VPC penerima atau pemohon berada di akun yang berbeda. Pengguna tidak dapat membuat koneksi peering VPC dengan VPC di akun yang berbeda.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeVpcPeeringConnections",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action":
 ["ec2:CreateVpcPeeringConnection","ec2:AcceptVpcPeeringConnection"],
      "Resource": "arn:aws:ec2:*:account-id:vpc/*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:*VpcPeeringConnection",
      "Resource": "arn:aws:ec2:*:account-id:vpc-peering-connection/*",
      "Condition": {
        "ArnEquals": {
          "ec2:AccepterVpc": "arn:aws:ec2:*:account-id:vpc/*",
          "ec2:RequesterVpc": "arn:aws:ec2:*:account-id:vpc/*"
        }
      }
    }
```

```
  ]
}
```

Contoh: Kelola koneksi peering VPC menggunakan konsol

Untuk melihat koneksi peering VPC di konsol Amazon VPC, pengguna harus memiliki izin untuk menggunakan tindakan `ec2:DescribeVpcPeeringConnections`. Untuk menggunakan laman Buat Koneksi Peering, pengguna harus memiliki izin untuk menggunakan tindakan `ec2:DescribeVpcs`. Ini memberi mereka izin untuk melihat dan memilih VPC. Anda dapat menerapkan izin di tingkat sumber daya untuk semua tindakan `ec2:*PeeringConnection`, kecuali `ec2:DescribeVpcPeeringConnections`.

Kebijakan berikut memberikan izin kepada pengguna untuk melihat koneksi peering VPC, dan menggunakan kotak dialog Create VPC Peering Connection untuk membuat koneksi peering VPC hanya menggunakan VPC pemohon tertentu. Jika pengguna mencoba untuk membuat koneksi peering VPC dengan VPC pemohon yang berbeda, maka permintaan gagal.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect":"Allow",
      "Action": [
        "ec2:DescribeVpcPeeringConnections", "ec2:DescribeVpcs"
      ],
      "Resource": "*"
    },
    {
      "Effect":"Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": [
        "arn:aws:ec2:*:*:vpc/vpc-id",
        "arn:aws:ec2:*:*:vpc-peering-connection/*"
      ]
    }
  ]
}
```

Kuota koneksi peering VPC untuk akun

Peering VPC memungkinkan Anda menghubungkan dua. VPCs Hal ini memungkinkan sumber daya dalam satu VPC untuk berkomunikasi dengan sumber daya di VPC lain seolah-olah mereka berada di jaringan yang sama. VPC peering adalah fitur yang berguna untuk menghubungkan Anda VPCs, apakah mereka berada di Wilayah yang sama atau AWS Wilayah yang berbeda. Bagian ini menjelaskan kuota yang harus Anda ketahui saat bekerja dengan koneksi peering VPC.

Tabel berikut mencantumkan kuota, sebelumnya disebut sebagai batas, untuk koneksi peering VPC untuk akun Anda. AWS Kecuali disebutkan lain, Anda dapat meminta penambahan untuk kuota ini.

Jika Anda menemukan bahwa persyaratan koneksi peering VPC Anda saat ini melebihi kuota default, kami menyarankan Anda untuk mengirimkan permintaan peningkatan batas layanan. Kami akan meninjau kasus penggunaan Anda dan bekerja sama dengan Anda untuk menyesuaikan kuota yang sesuai, memastikan lingkungan VPC Anda dapat mendukung kebutuhan bisnis Anda yang terus berkembang.

Nama	Default	Dapat disesuaikan
Koneksi peering VPC aktif per VPC	50	Ya (hingga 125)
Permintaan koneksi peering VPC yang luar biasa	25	Ya
Waktu kedaluwarsa untuk permintaan koneksi peering VPC yang tidak diterima	1 minggu (168 jam)	Tidak

Untuk informasi selengkapnya tentang aturan penggunaan koneksi peering VPC, lihat. Keterbatasan peering VPC Untuk informasi tambahan tentang kuota untuk Amazon VPC, lihat kuota VPC Amazon di Panduan Pengguna Amazon VPC.

Riwayat dokumen untuk Panduan Peering VPC Amazon

Tabel berikut menjelaskan rilis dokumentasi untuk Panduan Peering VPC Amazon.

Perubahan	Deskripsi	Tanggal
Tag pada membuat	Anda dapat menambahkan tag ketika Anda membuat koneksi peering VPC tabel rute.	20 Juli 2020
Pengintip Antar Wilayah	Resolusi nama host DNS didukung untuk koneksi peering VPC antar wilayah di Wilayah Asia Pasifik (Hong Kong).	26 Agustus 2019
Pengintip Antar Wilayah	Anda dapat membuat koneksi peering VPC antara VPCs di Wilayah yang berbeda. AWS	29 November 2017
Dukungan resolusi DNS untuk pengintip VPC	Anda dapat mengaktifkan VPC lokal untuk mengubah nama host DNS publik menjadi alamat IP pribadi ketika di-kueri dari instans di VPC rekan.	28 Juli 2016
Aturan grup keamanan basi	Anda dapat mengidentifikasi apakah grup keamanan Anda direferensikan dalam aturan grup keamanan di VPC rekan dan Anda dapat mengident ifikasi aturan grup keamanan basi.	12 Mei 2016
Menggunakan ClassicLink melalui koneksi peering VPC	Anda dapat memodifikasi koneksi peering VPC Anda untuk mengaktifkan instance	26 April 2016

	EC2 -Classic tertaut lokal untuk berkomunikasi dengan instance di VPC rekan, atau sebaliknya.	
Pengintip VPC	Anda dapat membuat koneksi peering VPC antara dua VPCs, yang memungkin kan instance di VPC untuk berkomunikasi satu sama lain menggunakan alamat IP pribadi	24 Maret 2014

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.