Peering VPC

Amazon Virtual Private Cloud

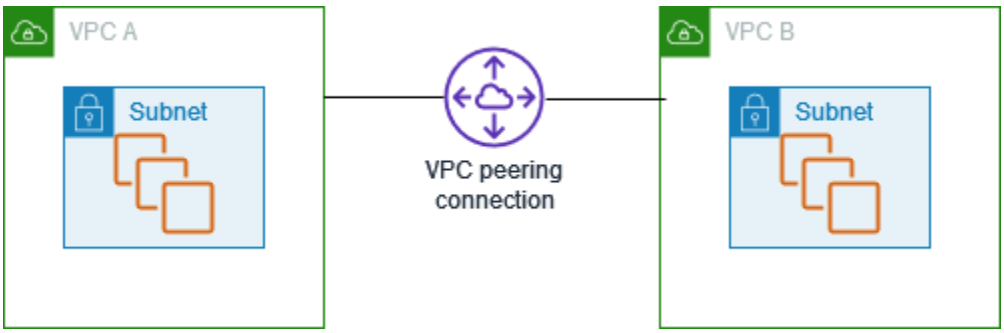
Amazon Virtual Private Cloud: Peering VPC

Table of Contents

Apa yang dimaksud dengan peering VPC?

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

Koneksi peering VPC adalah koneksi jaringan antara dua VPC yang memungkinkan Anda mengarahkan lalu lintas antara kedua VPC menggunakan alamat IPv4 atau alamat IPv6 pribadi. Instans pada VPC manapun dapat berkomunikasi satu sama lain seolah-olah mereka ada di jaringan yang sama. Anda dapat menciptakan koneksi peering VPC di antara dua VPC milik Anda sendiri, atau dengan VPC di akun AWS lain. VPC dapat berada 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 VPC di seluruh akun tersebut untuk membuat jaringan berbagi file. Anda juga dapat menggunakan koneksi peering VPC untuk mengizinkan VPC lainnya mengakses sumber daya yang Anda miliki di salah satu VPC Anda.

Saat Anda menjalin hubungan peering antara VPC di berbagai AWS Wilayah, sumber daya di VPC (misalnya, instans EC2 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 DDoS. 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 VPC Peering yang tetap berada dalam Availability Zone (meskipun berada di antara akun yang berbeda) gratis. Biaya berlaku untuk transfer data melalui koneksi VPC Peering yang melintasi Availability Zone dan Regions. Untuk informasi selengkapnya, lihat Harga Amazon EC2 Harga .

Dasar-dasar peering VPC

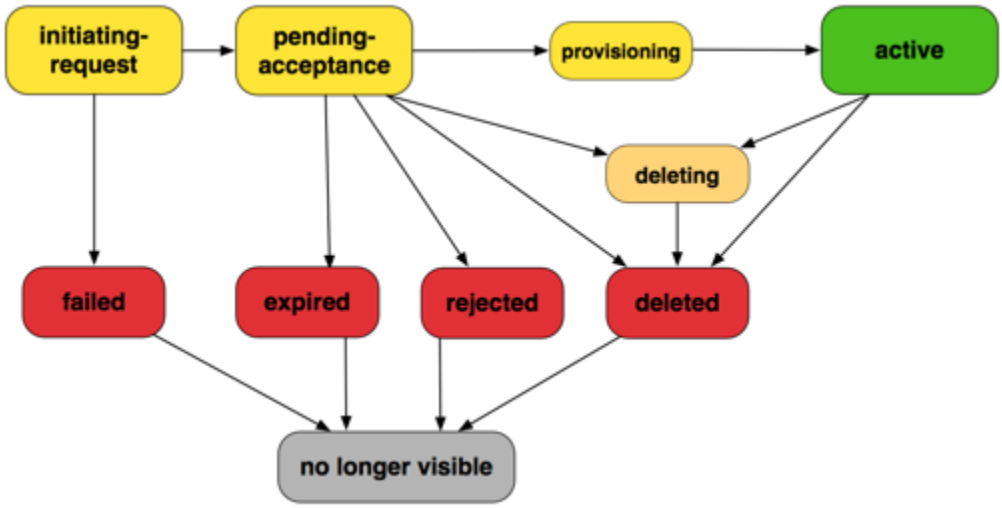
Untuk membuat koneksi peering VPC, lakukan hal berikut:

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 dari VPC penerima menerima permintaan koneksi peering VPC untuk mengaktivasi koneksi peering VPC.
3. Untuk mengaktifkan aliran lalu lintas antar VPC menggunakan alamat IP pribadi, pemilik dari setiap VPC di koneksi peering VPC harus secara manual menambahkan sebuah rute ke satu atau lebih tabel rute VPC mereka yang mengacu ke kisaran alamat IP dari VPC lain (VPC rekan).
4. Jika diperlukan, perbarui aturan grup keamanan yang terkait dengan instans EC2 Anda untuk memastikan bahwa lalu lintas ke dan dari VPC rekan tidak dibatasi. Jika kedua VPC 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 instans EC2 di kedua sisi alamat koneksi peering VPC satu sama lain menggunakan nama host DNS publik, nama host diselesaikan ke alamat IP publik dari instans EC2. Untuk mengubah perilaku ini, Aktifkan resolusi nama host DNS untuk koneksi VPC Anda. Setelah mengaktifkan resolusi nama host DNS, jika instans EC2 di kedua sisi alamat koneksi peering VPC satu sama lain menggunakan nama host DNS publik, nama host menyelesaikan ke alamat IP pribadi instans EC2.

Untuk informasi selengkapnya, lihat Bekerja dengan 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 sedang aktif, dan lalu lintas dapat mengalir antar VPC (asalkan grup keamanan dan tabel rute Anda mengizinkan aliran lalu lintas). Selagi berada dalam status ini,

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

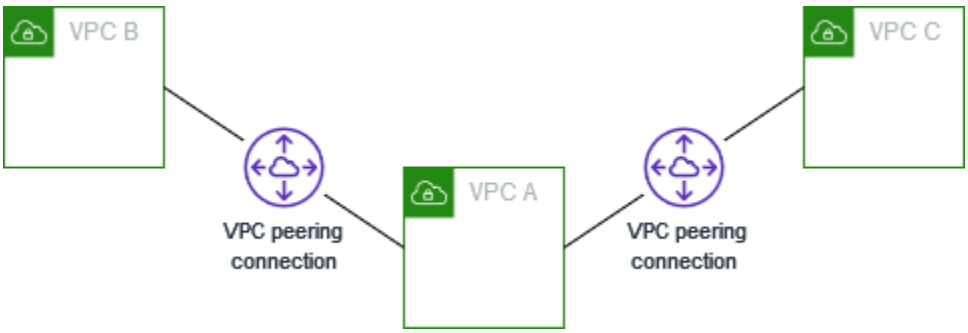
> **Note**
>
> Jika suatu peristiwa di Wilayah di mana VPC berada mencegah arus lalu lintas, status koneksi peering VPC tetap ada. `Active`

- 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 dalam AWS akun yang sama, permintaan yang dihapus tetap terlihat selama 2 jam.

Berbagai koneksi peering VPC

Koneksi peering VPC adalah hubungan satu-satu antara dua VPC. Anda dapat membuat beberapa koneksi peering VPC untuk setiap VPC yang Anda miliki, tetapi hubungan peering transitif tidak di-support. Anda tidak memiliki hubungan sambungan apapun dengan VPC-VPC karena VPC Anda tidak langsungdisambungkan dengannya.

Diagram berikut adalah contoh dari satu VPC yang tersambung ke dua VPC yang berbeda. 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 di Gateway Transit Amazon VPC.

Koneksi

- Ada kuota jumlah koneksi peering VPC yang aktif dan tertunda per VPC. Untuk informasi selengkapnya, lihat Quotas.
- Anda tidak dapat memiliki lebih dari satu koneksi peering VPC antara dua VPC secara 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 CIDR IPv4 dari sebuah VPC di koneksi peering VPC berada di luar kisaran alamat IPv4 pribadi yang ditentukan oleh RFC 1918, nama host DNS pribadi untuk VPC itu tidak dapat diatasi menjadi 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 melalui IPv6. Anda harus mengaitkan blok IPv6 CIDR dengan setiap VPC, mengaktifkan instance di VPC untuk komunikasi IPv6, dan merutekan lalu lintas IPv6 yang ditujukan untuk VPC rekan 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 antar VPC yang blok CIDR IPv4 atau IPv6 nya memiliki kecocokan atau saling tumpang tindih.
- Jika Anda memiliki beberapa blok CIDR IPv4, 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 VPC disambungkan 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

- Unit Transmisi Maksimum (MTU) di seluruh koneksi peering VPC melalui Wilayah adalah 1500 byte. Frame jumbo (MTU hingga 9001 byte) tidak didukung untuk koneksi peering VPC antar wilayah. Namun, mereka didukung untuk koneksi peering VPC di Wilayah yang sama. Untuk

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

- Anda harus mengaktifkan support resolusi DNS untuk koneksi peering VPC untuk menyelesaikan nama host DNS pribadi pada VPC yang tersambung ke alamat IP pribadi, bahkan jika CIDR IPv4 berada di kisaran alamat IPv4 pribadi yang ditentukan oleh RFC 1918.

VPC dan subnet bersama

- 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.

Bekerja dengan koneksi peering VPC

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

Tugas

- Buat koneksi peering VPC
- Terima koneksi peering VPC
- Tolak koneksi peering VPC
- Melihat koneksi peering VPC Anda
- Perbarui tabel rute Anda untuk koneksi peering VPC
- Memperbarui grup keamanan Anda untuk mereferensikan grup keamanan rekan
- Memodifikasi opsi koneksi peering VPC
- Menghapus 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. Anda dapat meminta koneksi peering VPC dengan VPC lain di akun Anda, atau dengan VPC di akun AWS yang berbeda. Untuk koneksi peering VPC antar-Wilayah di mana VPC-VPC berada di Wilayah-Wilayah yang berbeda, permintaan harus dilakukan dari Wilayah VPC peminta.

Untuk mengaktivasi permintaan, pemilik VPC penerima harus menerima permintaan tersebut. Untuk koneksi peering VPC antar-WIlayah, permintaan harus diterima di Wilayah VPC penerima. Untuk informasi selengkapnya, lihat the section called “Menerima”. Untuk informasi selengkapnya tentang status koneksi `Pending acceptance` peering, lihatSiklus hidup koneksi peering VPC.

Tugas

- Prasyarat
- Buat dengan VPC di akun dan Wilayah yang sama
- Buat dengan VPC di akun yang sama dan Wilayah yang berbeda
- Buat dengan VPC di akun yang berbeda dan Wilayah yang sama
- Buat dengan VPC di berbagai akun dan Wilayah
- Buat koneksi peering VPC menggunakan baris perintah

Prasyarat

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

Buat dengan VPC di akun dan Wilayah yang sama

Untuk membuat koneksi peering VPC dengan VPC di akun dan Wilayah yang sama

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Mengintip koneksi.
3. Memilih Buat koneksi peering.
4. Konfigurasikan informasi berikut, dan pilih Buat koneksi peering saat Anda selesai:
   - Nama: Anda dapat secara opsional memberi nama koneksi peering VPC Anda.
   - VPC ID (Peminta): Pilih VPC di akun Anda yang ingin Anda buat koneksi peering VPC.
   - Untuk Pilih VPC lain untuk diintip, pilih Akun saya dan pilih VPC Anda yang lain.
   - (Opsional) Untuk menambahkan tag, pilih Tambahkan tag baru dan masukkan kunci dan nilai tag.
5. Pilih Tindakan, Terima permintaan.
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.

Buat dengan VPC di akun yang sama dan Wilayah yang berbeda

Untuk membuat koneksi peering VPC dengan VPC di akun yang sama dan Wilayah yang berbeda

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

4. Konfigurasikan informasi berikut, dan pilih Buat koneksi peering saat Anda selesai:
   - Nama: Anda dapat secara opsional memberi nama koneksi peering VPC Anda. Melakukan hal itu akan menciptakan tag dengan kunci `Name` dan nilai yang Anda tentukan.
   - VPC ID (Peminta): Pilih VPC pemohon di akun Anda untuk meminta koneksi peering VPC.
   - Akun: Pilih Akun saya.
   - Wilayah: Pilih Wilayah lain dan pilih Wilayah iuntuk akseptor VPC.
   - VPC ID (Accepter): Pilih akseptor VPC.
5. Di pemilih Wilayah, pilih Wilayah VPC penerima.
6. Di panel navigasi, pilih Mengintip koneksi. Pilih koneksi peering VPC yang Anda buat, dan pilih Tindakan, Terima permintaan.
7. Saat diminta konfirmasi, pilih Terima permintaan.
8. 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.

Buat dengan VPC di akun yang berbeda dan Wilayah yang sama

Untuk meminta koneksi peering VPC dengan VPC di akun yang berbeda dan Wilayah yang sama

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Mengintip koneksi.
3. Memilih Buat koneksi peering.
4. Konfigurasikan informasi sebagai berikut, dan pilih Buat koneksi peering setelah Anda selesai:
   - Nama: Anda dapat secara opsional memberi nama koneksi peering VPC Anda. Dengan melakukannya akan menciptakan tag dengan kunci `Name` dan sebuah nilai yang Anda tentukan. Tag ini hanya terlihat oleh Anda; pemilik VPC rekan dapat membuat tag mereka sendiri untuk koneksi peering VPC tersebut.
   - VPC ID (Peminta): Pilih VPC di akun Anda untuk membuat koneksi peering VPC.
   - Akun: Pilih Akun lain.
   - Account ID: Masukkan ID Akun AWS yang memiliki akseptor VPC.
   - VPC ID (Accepter): Masukkan ID VPC yang dapat digunakan untuk membuat koneksi peering VPC.

Buat dengan VPC di berbagai akun dan Wilayah

Untuk meminta koneksi peering VPC dengan VPC di berbagai akun dan Wilayah

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Mengintip koneksi.
3. Memilih Buat koneksi peering.
4. Konfigurasikan informasi sebagai berikut, dan pilih Buat koneksi peering setelah Anda selesai:

   - Nama: Anda dapat secara opsional memberi nama koneksi peering VPC Anda. Dengan melakukannya akan menciptakan tag dengan kunci `Name` dan sebuah nilai yang Anda tentukan. Tag ini hanya terlihat oleh Anda; pemilik VPC rekan dapat membuat tag mereka sendiri untuk koneksi peering VPC tersebut.
   - VPC ID (Peminta): Pilih VPC di akun Anda untuk membuat koneksi peering VPC.
   - Akun: Pilih Akun lain.
   - Account ID: Masukkan ID Akun AWS yang memiliki akseptor VPC.
   - Wilayah: Pilih wilayah lain dan pilih Wilayah di mana akseptor VPC berada.
   - VPC ID (Accepter): Masukkan ID VPC yang dapat digunakan untuk membuat koneksi peering VPC.

Buat koneksi peering VPC menggunakan baris perintah

Anda dapat membuat koneksi peering VPC menggunakan perintah berikut:

- create-vpc-peering-connection (AWS CLI)
- Baru-EC2 (VpcPeeringConnection) AWS Tools for Windows PowerShell

Terima 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 telah Anda kirim ke akun AWS. Jika Anda membuat koneksi peering VPC di akun AWS yang sama, Anda berdua harus membuat dan menerima permintaan itu sendiri.

Jika VPC berada di Wilayah yang berbeda, permintaan harus diterima di Wilayah VPC penerima.

> **Important**
>
> Jangan terima koneksi peering VPC dari yang akun AWS yang tidak dikenal. 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 sang peminta mendapatkan akses ke informasi apa pun tentang akun AWS Anda atau VPC Anda. Untuk informasi selengkapnya, lihat Tolak koneksi peering VPC. Anda juga dapat mengabaikan permintaan dan membiarkannya kedaluwarsa; secara default, permintaan kedaluwarsa setelah 7 hari.

Setelah Anda menerima koneksi peering VPC, Anda harus menambahkan entri ke tabel rute Anda untuk mengaktifkan lalu lintas antara VPC yang diintip. Untuk informasi selengkapnya, lihat Perbarui tabel rute Anda untuk koneksi peering VPC.

Untuk menerima koneksi peering VPC

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 Mengintip koneksi.
4. Pilih koneksi peering VPC yang tertunda (statusnya`pending-acceptance`), dan pilih Tindakan, Terima permintaan. Untuk informasi selengkapnya tentang peering status siklus hidup koneksi, lihat. Siklus hidup koneksi peering VPC

   > **Tip**
   >
   > Jika Anda tidak melihat status koneksi peering VPC yang tertunda, periksa Wilayah. Permintaan peering antar-wilayah harus diterima di Wilayah VPC penerima.

5. Saat diminta konfirmasi, pilih Terima permintaan.
6. 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 VPC menggunakan baris perintah atau API

- accept-vpc-peering-connection (AWS CLI)
- Setujui-EC2 VpcPeeringConnection () AWS Tools for Windows PowerShell
- AcceptVpcPeeringConnection (Amazon EC2 Query API)

Tolak koneksi peering VPC

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 ketahui dan percayai; Anda dapat menolak permintaan yang tidak diinginkan. Untuk informasi selengkapnya tentang status koneksi `Rejected` peering, lihatSiklus hidup koneksi peering VPC.

Untuk menolak koneksi peering VPC

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Mengintip koneksi.
3. Pilih koneksi peering VPC, dan pilih Tindakan, Tolak permintaan.
4. Saat diminta konfirmasi, pilih Tolak permintaan.

Untuk menolak koneksi peering VPC menggunakan baris perintah atau API

- reject-vpc-peering-connection (AWS CLI)
- Deny-EC2 (VpcPeeringConnection) AWS Tools for Windows PowerShell
- RejectVpcPeeringConnection (Amazon EC2 Query API)

Melihat koneksi peering VPC Anda

Anda dapat melihat semua koneksi peering VPC Anda di konsol Amazon VPC. Secara default, konsol menampilkan semua koneksi peering VPC dalam status-status yang berbeda, termasuk yang mungkin baru saja dihapus atau ditolak. Untuk informasi lebih lanjut tentang siklus hidup koneksi peering VPC, lihat Siklus hidup koneksi peering VPC.

Untuk melihat koneksi peering VPC

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Mengintip koneksi.
3. Semua koneksi peering VPC Anda ada dalam daftar. Gunakan bilah pem-filter-an hasil cari untuk mempersempit hasil pencarian.

Untuk mendeskripsikan koneksi peering VPC menggunakan baris perintah atau API

- describe-vpc-peering-connections (AWS CLI)
- Dapatkan-EC2 (VpcPeeringConnections) AWS Tools for Windows PowerShell
- DescribeVpcPeeringConnections (Amazon EC2 Query API)

Perbarui tabel rute Anda untuk koneksi peering VPC

Untuk mengaktifkan lalu lintas IPv4 pribadi antar instance di VPC peered, 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 peer dan targetnya adalah ID koneksi peering VPC. Untuk informasi selengkapnya, lihat Mengonfigurasi tabel rute di Panduan Pengguna Amazon VPC.

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

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

Demikian pula, jika VPC dalam koneksi peering VPC telah mengaitkan blok CIDR IPv6, Anda dapat menambahkan rute yang memungkinkan komunikasi dengan rekan VPC melalui IPv6.

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

Pertimbangan-pertimbangan

- Jika Anda memiliki VPC yang tersambung dengan berbagai VPC yang memiliki blok-blok CIDR IPv4 yang tumpang tindih atau saling bersesuaian, pastikan bahwa tabel rute Anda terkonfigurasi untuk menghindari pengiriman lalu lintas respons dari VPC Anda ke VPC yang salah. AWS saat ini tidak men-support penerusan jalur terbalik unicast pada koneksi peering VPC yang dapat memeriksa IP sumber paket dan mengarahkan paket balasan kembali ke sumber. 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 memiliki keadaan`blackhole`, dan tidak berpengaruh sampai koneksi peering VPC berada di negara bagian`active`.

Untuk menambahkan rute IPv4 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 itu, tabel rute utama untuk VPC secara implisit terkait dengan subnet.
4. Pilih Tindakan, Sunting rute.
5. Pilih Tambahkan rute.
6. Untuk Tujuan, masukkan kisaran alamat IPv4 yang lalu lintas jaringan pada koneksi peering VPC harus tuju. Anda dapat menentukan seluruh blok CIDR IPv4 dari rekan VPC, kisaran tertentu, atau alamat IPv4 individu, seperti alamat IP pada instans yang diajak 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 Save changes (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 WIlayah AWS yang berbeda yang menggunakan alamat IPv6, Anda dapat membuat koneksi peering antar-Wilayah. Anda kemudian dapat menambahkan rute IPv6 untuk komunikasi antar sumber daya.

Untuk menambahkan rute IPv6 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 kisaran alamat IPv6 untuk VPC rekan. Anda dapat menentukan seluruh blok CIDR IPv6 dari VPC rekan, kisaran tertentu, atau alamat IPv6 individu. Misalnya, jika blok CIDR dari VPC rekan adalah `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 Save changes (Simpan perubahan).

Untuk informasi selengkapnya, lihat Tabel Rute di Panduan Pengguna Amazon VPC.

Untuk menambah atau mengganti rute menggunakan baris perintah atau API

- create-route (AWS CLI)
- New-EC2Route (AWS Tools for Windows PowerShell)
- CreateRoute (Amazon EC2 Query API)
- replace-route (AWS CLI)
- Set-EC2Route (AWS Tools for Windows PowerShell)

- ReplaceRoute (Amazon EC2 Query API)

Memperbarui grup keamanan Anda untuk mereferensikan grup keamanan rekan

Anda dapat memperbarui aturan inbound atau outbound untuk grup keamanan VPC Anda untuk mereferensikan grup keamanan di VPC yang tersambung. Dengan melakukan hal itu, lalu lintas dapat mengalir ke dan dari instans yang dikaitkan dengan grup keamanan yang dirujuk di VPC yang tersambung.

Persyaratan

- VPC rekan bisa menjadi VPC di akun Anda, atau menjadi VPC di akun AWS yang lain. Untuk mereferensikan grup keamanan di akun AWS lain, sertakan nomor akun di isian Sumber atau Tujuan; misalnya saja, `123456789012/sg-1a2b3c4d`.
- Anda tidak dapat mereferensikan grup keamanan dari VPC rekan yang ada di Wilayah yang berbeda. Sebagai gantinya, gunakan blok CIDR dari VPC rekan.
- Untuk mereferensikan grup keamanan di VPC rekan, koneksi peering VPC harus berstatus `active`.
- 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. Di panel navigasi, pilih Grup keamanan.
3. Pilih grup keamanan, lalu pilih Tindakan, Edit aturan masuk untuk mengubah aturan masuk atau memilih Tindakan, Edit aturan keluar untuk mengubah aturan keluar.
4. Untuk menambahkan aturan, pilih Tambahkan aturan dan tentukan jenis, protokol, dan rentang port. Untuk Sumber (aturan masuk) atau Tujuan (aturan keluar), masukkan ID grup keamanan

di VPC peer jika berada di Wilayah yang sama atau blok CIDR dari VPC rekan jika berada di Wilayah yang berbeda.

> **Note**
>
> Grup keamanan di VPC rekan tidak ditampilkan secara otomatis.

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

Untuk memperbarui aturan inbound menggunakan baris perintah

- authorize-security-group-ingress (AWS CLI)
- Hibah-EC2 (SecurityGroupIngress) AWS Tools for Windows PowerShell
- Mencabut EC2 () SecurityGroupIngress AWS Tools for Windows PowerShell
- revoke-security-group-ingress (AWS CLI)

Untuk memperbarui aturan outbound menggunakan baris perintah

- authorize-security-group-egress (AWS CLI)
- Hibah-EC2 (SecurityGroupEgress) AWS Tools for Windows PowerShell
- Mencabut EC2 () SecurityGroupEgress AWS Tools for Windows PowerShell
- revoke-security-group-egress (AWS CLI)

Misalnya, untuk memperbarui grup keamanan `sg-aaaa1111` untuk mengizinkan akses inbound melalui HTTP dari `sg-bbbb2222` grup keamanan di VPC rekan, Anda dapat menggunakan perintah AWS CLI berikut ini:

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

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)
- Dapatkan-EC2 (SecurityGroupReference) AWS Tools for Windows PowerShell
- DescribeSecurityGroupReferences (Amazon EC2 Query API)

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.

Bekerja dengan aturan grup keamanan basi

Aturan grup keamanan basi adalah aturan yang mereferensikan grup keamanan yang dihapus di VPC yang sama atau di VPC peer, atau yang mereferensikan grup keamanan di VPC peer 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 menjadii kedaluwarsa karena koneksi peering VPC dihapus, aturan tersebut tidak lagi akan ditandai sebagai kedaluwarsa jika Anda membuat koneksi peering VPC baru dengan VPC-VPC yang sama.

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. Di 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 Anda yang kedaluwarsa menggunakan baris perintah atau API

- describe-stale-security-groups (AWS CLI)
- Dapatkan-EC2 (StaleSecurityGroup) AWS Tools for Windows PowerShell
- DescribeStaleSecurityGroups (Amazon EC2 Query API)

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-egress](#)perintah [revoke-security-group-ingress](#)atau.

Memodifikasi opsi koneksi peering VPC

Anda dapat memodifikasi koneksi peering VPC untuk melakukan hal berikut:

- Aktifkan VPC untuk mengubah nama host DNS IPv4 publik menjadi alamat IPv4 pribadi ketika diminta dari instans di VPC rekan. Untuk informasi selengkapnya, lihat [Aktifkan resolusi DNS untuk koneksi peering VPC](#).

Aktifkan resolusi DNS untuk koneksi peering VPC

Untuk mengaktifkan VPC untuk mengubah nama host DNS IPv4 publik menjadi alamat IPv4 pribadi ketika diminta dari instans di VPC rekan, Anda harus memodifikasi koneksi peering Anda yang ada.

Kedua VPC harus diaktifkan untuk nama host DNS dan resolusi DNS.

Anda tidak dapat mengaktifkan support resolusi DNS ketika Anda membuat sambungan peering baru. Anda dapat mengaktifkan support resolusi DNS untuk koneksi peering yang ada yang berstatus `active`.

Untuk mengaktifkan resolusi DNS untuk koneksi peering

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Mengintip koneksi.
3. Pilih koneksi peering VPC, dan pilih Tindakan, Edit pengaturan DNS.
4. Untuk memastikan kueri dari VPC rekan berubah menjadi alamat IP pribadi di VPC lokal Anda, pilih opsi untuk mengaktifkan resolusi DNS untuk kueri dari VPC rekan. Opsi ini adalah Resolusi DNS Peminta atau Resolusi DNS penerima, tergantung apakah VPC tersebut adalah peminta atau VPC penerima.
5. Jika VPC peer samaAkun AWS, Anda dapat mengaktifkan resolusi DNS untuk kedua VPC dalam koneksi peering.
6. Pilih Save changes (Simpan perubahan).
7. Jika rekan VPC berada di AWS akun yang berbeda atau Wilayah yang berbeda, pemilik VPC rekan harus masuk ke konsol VPC, melakukan langkah 2 hingga 4, dan memilih Simpan perubahan.

Untuk mengaktifkan resolusi DNS menggunakan baris perintah atau API

- modify-vpc-peering-connection-Pilihan () AWS CLI
- Mengedit-EC2 (VpcPeeringConnectionOption) AWS Tools for Windows PowerShell
- ModifyVpcPeeringConnectionOptions (Amazon EC2 Query API)

Anda harus memodifikasi opsi peering VPC peminta jika Anda adalah peminta koneksi peering VPC, dan Anda harus memodifikasi opsi peering VPC penerima jika Anda adalah penerima koneksi peering VPC. Anda dapat menggunakan VpcPeeringConnections perintah describe-vpc-peering-connectionsatau Get-EC2 untuk memverifikasi VPC mana yang akseptor dan pemohon untuk koneksi peering VPC. Untuk koneksi peering antar-WIlayah, Anda harus menggunakan Wilayah untuk VPC peminta untuk memodifikasi opsi peering VPC peminta dan Wilayah untuk VPC penerima untuk memodifikasi opsi peering VPC penerima.

Dalam contoh ini, Anda adalah peminta koneksi peering VPC, oleh karenanya modifikasikan opsi koneksi peering dengan menggunakan AWS CLI sebagai berikut:

```
aws ec2 modify-vpc-peering-connection-options --vpc-peering-connection-id pcx-aaaabbbb
 --requester-peering-connection-options AllowDnsResolutionFromRemoteVpc=true
```

Menghapus 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 sambungan, sambungan 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 Mengintip koneksi.
3. Pilih koneksi peering VPC.
4. Pilih Tindakan, Hapus koneksi peering.
5. Ketika diminta konfirmasi, masukkan **`delete`** lalu pilih Hapus.

Untuk menghapus koneksi peering VPC menggunakan baris perintah atau API

- delete-vpc-peering-connection (AWS CLI)
- Hapus-EC2 VpcPeeringConnection () AWS Tools for Windows PowerShell
- DeleteVpcPeeringConnection (Amazon EC2 Query API)

Memecahkan masalah koneksi peering VPC

Jika Anda mengalami masalah saat menghubungkan ke sumber daya di VPC dari sumber daya di VPC peer, 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 peer ke koneksi peering VPC. Untuk informasi selengkapnya, lihat Perbarui tabel rute.
- Untuk instans EC2, verifikasi bahwa grup keamanan untuk instans EC2 mengizinkan lalu lintas dari VPC peer. Untuk informasi selengkapnya, lihat Referensi kelompok keamanan rekan.
- Untuk setiap sumber daya di setiap VPC, verifikasi bahwa ACL jaringan untuk subnetnya memungkinkan lalu lintas dari VPC peer.

Anda juga dapat menggunakan Reachability Analyzer untuk mengidentifikasi komponen dengan masalah konfigurasi, seperti tabel rute, grup keamanan, atau ACL jaringan. Untuk informasi selengkapnya, lihat Panduan Reachability Analyzer.

Konfigurasi peering VPC

Dokumentasi berikut menjelaskan berbagai jenis konfigurasi peering VPC.

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 peering VPC. Untuk informasi selengkapnya tentang membuat dan bekerja dengan koneksi peering VPC, lihat Bekerja dengan koneksi peering VPC.

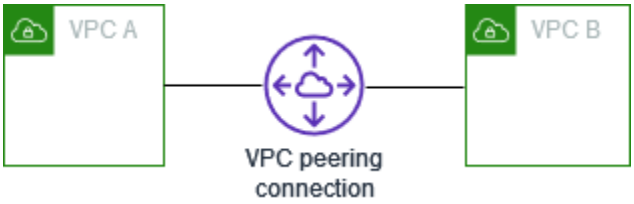
Untuk informasi selengkapnya tentang pembaruan tabel rute Anda, lihat Perbarui tabel rute Anda untuk koneksi peering VPC.

Konfigurasi

- Dua VPC disambungkan bersama
- Satu VPC disambungkan dengan dua VPC
- Tiga VPC disambungkan bersama
- Beberapa VPC disambungkan bersama

Dua VPC disambungkan bersama

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



Anda mungkin menggunakan konfigurasi ini ketika Anda memiliki dua VPC yang memerlukan akses ke sumber daya satu sama lain. Misalnya, Anda mengatur VPC A untuk catatan akun Anda dan VPC B untuk catatan keuangan Anda, dan setiap VPC ini harus dapat mengakses sumber daya dari VPC lain tanpa batasan.

CIDR VPC Tunggal

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

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

Beberapa IPv4 VPC CIDR

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

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

Tabel rute	Tujuan	Target
	VPC KE CIDR 2	pcx-11112222

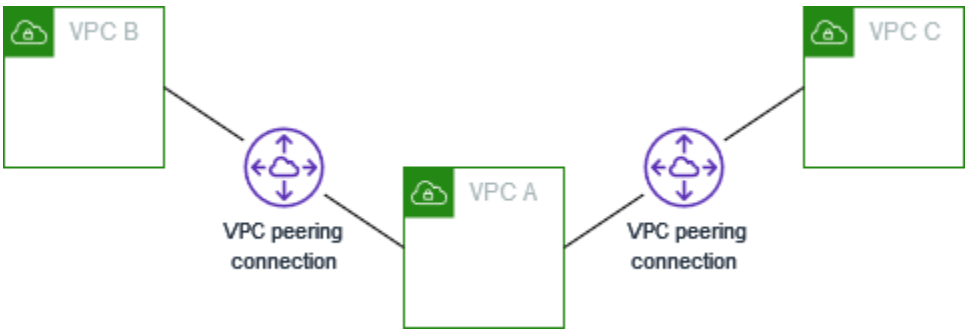
IPv4 dan IPv6 VPC CIDR

Jika VPC A dan VPC B telah mengaitkan blok CIDR IPv6, Anda dapat memperbarui tabel rute untuk setiap VPC dengan rute untuk blok IPv4 dan IPv6 CIDR dari VPC peer.

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

Satu VPC disambungkan dengan dua VPC

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



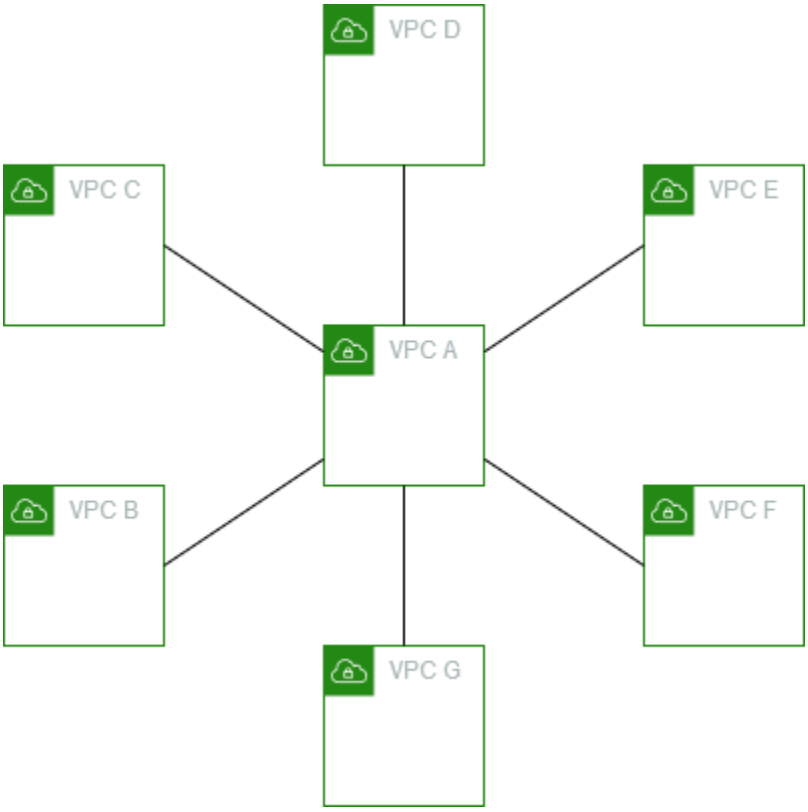
VPC B dan VPC C tidak dapat mengirim lalu lintas secara langsung satu sama lain satu sama lain satu sama lain melalui VPC A, karena VPC peering VPC tidak mendukung hubungan peering hubungan sambungan transitif. Anda dapat membuat koneksi peering VPC antara VPC B dan VPC C, seperti yang ditunjukkan padaTiga VPC disambungkan bersama. Untuk informasi selengkapnya tentang skenario peering yang tidak disupport, lihat the section called “Keterbatasan peering VPC”.

Anda mungkin menggunakan konfigurasi ini ketika Anda memiliki sumber daya pada VPC pusat, seperti repositori layanan, yang perlu diakses VPC-VPC lain. VPC-VPC lain tidak memerlukan akses ke sumber daya satu sama lain; VPC-VPC tersebut 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 KE CIDR*	Lokal:
	VPC B CIDR	pcx-12121212
	VPC C CIDR	pcx-23232323
VPC B	*VPC B CIDR*	Lokal:
	VPC KE CIDR	pcx-12121212
VPC C	*VPC C CIDR*	Lokal:
	VPC KE CIDR	pcx-23232323

Anda dapat memperluas konfigurasi ini ke VPC tambahan. Misalnya, VPC A disambungkan dengan VPC B melalui VPC G menggunakan CIDR IPv4 dan IPv6, tetapi VPC-VPC-VPC lain tidak tersambung satu sama lain. Dalam diagram ini, garis mewakili koneksi peering VPC.



Perbarui tabel rute sebagai berikut.

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

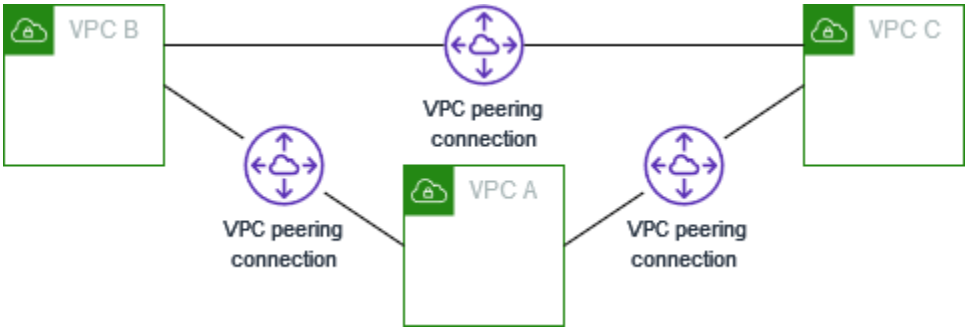
Tabel rute	Tujuan	Target
	VPC D IPv6	pcx-aaaadddd
	VPC & IPv4 CIDR	pcx-aaaaeeee
	VPC & IPv6 CIDR	pcx-aaaaeeee
	VPC F IPv4	pcx-aaaaffff
	VPC F IPv6	pcx-aaaaffff
	VPC G IPv4	pcx-aaaagggg
	VPC G IPv6	pcx-aaaagggg
VPC B	*VPC B IPv4*	Lokal:
	VPC B IPv6	Lokal:
	VPC KE IPv4 CIDR	pcx-aaaabbbb
	VPC KE IPv6 CIDR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

Tabel rute	Tujuan	Target
	VPC & IPv6 CIDR	Lokal:
	VPC KE IPv4 CIDR	pcx-aaaaeeee
	VPC KE IPv6 CIDR	pcx-aaaaeeee
VPC F	*VPC F IPv4*	Lokal:
	VPC F IPv6	Lokal:
	VPC KE IPv4 CIDR	pcx-aaaaffff
	VPC KE IPv6 CIDR	pcx-aaaaffff
VPC G	*VPC G IPv4*	Lokal:
	VPC G IPv6	Lokal:
	VPC KE IPv4 CIDR	pcx-aaaagggg
	VPC KE IPv6 CIDR	pcx-aaaagggg

Tiga VPC disambungkan bersama

Dalam konfigurasi ini, ada tiga VPC yang samaAkun AWS dengan blok CIDR yang tidak tumpang tindih. VPC diintip dalam mesh 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 mungkin menggunakan konfigurasi ini ketika Anda memiliki VPC yang perlu berbagi sumber daya dengan satu sama lain tanpa batasan. Misalnya, sebagai sistem berbagi file.

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

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

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

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

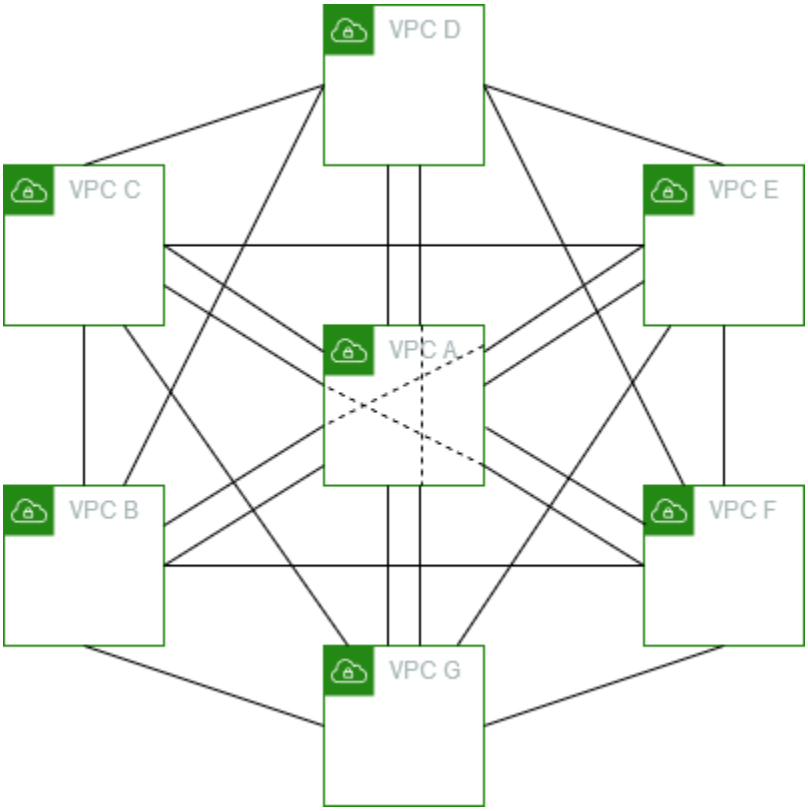
Beberapa VPC disambungkan bersama

Dalam konfigurasi ini, terdapat tujuh VPC yang tersambung dalam sebuah konfigurasi mesh penuh. VPC-VPC berada di 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

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

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



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

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

Tabel rute	Tujuan	Target
	VPC C CIDR	pcx-bbbbcccc
	VPC D CIDR	pcx-bbbbdddd
	VPC E CIDR	pcx-bbbbeeee
	VPC F CIDR	pcx-bbbbffff
	VPC G	pcx-bbbbgggg
VPC C	*VPC C CIDR*	Lokal:
	VPC KE CIDR	pcx-aaaacccc
	VPC B CIDR	pcx-bbbbcccc
	VPC D CIDR	pcx-ccccdddd
	VPC E CIDR	pcx-cccceeee
	VPC F CIDR	pcx-ccccffff
	VPC G	pcx-ccccgggg
VPC D	*VPC D CIDR*	Lokal:
	VPC KE 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	pcx-ddddgggg
VPC E	*VPC E CIDR*	Lokal:

Tabel rute	Tujuan	Target
	VPC KE 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	pcx-eeeegggg
VPC F	*VPC F CIDR*	Lokal:
	VPC KE 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	pcx-ffffgggg
VPC G	*VPC G*	Lokal:
	VPC KE 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 VPC memiliki blok CIDR IPv6 terkait, perbarui tabel rute sebagai berikut.

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

Tabel rute	Tujuan	Target
	VPC C IPv6	pcx-bbbbcccc
	VPC D IPv4	pcx-bbbbdddd
	VPC D IPv6	pcx-bbbbdddd
	VPC & IPv4 CIDR	pcx-bbbbeeee
	VPC & IPv6 CIDR	pcx-bbbbeeee
	VPC F IPv4	pcx-bbbbffff
	VPC F IPv6	pcx-bbbbffff
	VPC G IPv4	pcx-bbbbgggg
	VPC G IPv6	pcx-bbbbgggg
VPC C	*VPC C IPv4*	Lokal:
	VPC C IPv6	Lokal:
	VPC KE IPv4 CIDR	pcx-aaaacccc
	VPC KE IPv6 CIDR	pcx-aaaacccc
	VPC B IPv4	pcx-bbbbcccc
	VPC B IPv6	pcx-bbbbcccc
	VPC D IPv4	pcx-ccccdddd
	VPC D IPv6	pcx-ccccdddd
	VPC & IPv4 CIDR	pcx-cccceeee
	VPC & IPv6 CIDR	pcx-cccceeee
	VPC F IPv4	pcx-ccccffff

Tabel rute	Tujuan	Target
	VPC F IPv6	pcx-ccccffff
	VPC G IPv4	pcx-ccccgggg
	VPC G IPv6	pcx-ccccgggg
VPC D	*VPC D IPv4*	Lokal:
	VPC D IPv6	Lokal:
	VPC KE IPv4 CIDR	pcx-aaaadddd
	VPC KE IPv6 CIDR	pcx-aaaadddd
	VPC B IPv4	pcx-bbbbdddd
	VPC B IPv6	pcx-bbbbdddd
	VPC C IPv4	pcx-ccccdddd
	VPC C IPv6	pcx-ccccdddd
	VPC & IPv4 CIDR	pcx-ddddeeee
	VPC & IPv6 CIDR	pcx-ddddeeee
	VPC F IPv4	pcx-ddddffff
	VPC F IPv6	pcx-ddddffff
	VPC G IPv4	pcx-ddddgggg
	VPC G IPv6	pcx-ddddgggg
VPC E	*VPC & IPv4 CIDR*	Lokal:
	VPC & IPv6 CIDR	Lokal:
	VPC KE IPv4 CIDR	pcx-aaaaeeee

Tabel rute	Tujuan	Target
	VPC KE IPv6 CIDR	pcx-aaaaeeee
	VPC B IPv4	pcx-bbbbeeee
	VPC B IPv6	pcx-bbbbeeee
	VPC C IPv4	pcx-cccceeee
	VPC C IPv6	pcx-cccceeee
	VPC D IPv4 CIDR	pcx-ddddeeee
	VPC D IPv6	pcx-ddddeeee
	VPC F IPv4	pcx-eeeeffff
	VPC F IPv6	pcx-eeeeffff
	VPC G IPv4	pcx-eeeegggg
	VPC G IPv6	pcx-eeeegggg
VPC F	*VPC F IPv4*	Lokal:
	VPC F IPv6	Lokal:
	VPC KE IPv4 CIDR	pcx-aaaaffff
	VPC KE IPv6 CIDR	pcx-aaaaffff
	VPC B IPv4	pcx-bbbbffff
	VPC B IPv6	pcx-bbbbffff
	VPC C IPv4	pcx-ccccffff
	VPC C IPv6	pcx-ccccffff
	VPC D IPv4 CIDR	pcx-ddddffff

Tabel rute	Tujuan	Target
	VPC D IPv6	pcx-ddddffff
	VPC & IPv4 CIDR	pcx-eeeeffff
	VPC & IPv6 CIDR	pcx-eeeeffff
	VPC G IPv4	pcx-ffffgggg
	VPC G IPv6	pcx-ffffgggg
VPC G	*VPC G IPv4*	Lokal:
	VPC G IPv6	Lokal:
	VPC KE IPv4 CIDR	pcx-aaaagggg
	VPC KE IPv6 CIDR	pcx-aaaagggg
	VPC B IPv4	pcx-bbbbgggg
	VPC B IPv6	pcx-bbbbgggg
	VPC C IPv4	pcx-ccccgggg
	VPC C IPv6	pcx-ccccgggg
	VPC D IPv4 CIDR	pcx-ddddgggg
	VPC D IPv6	pcx-ddddgggg
	VPC & IPv4 CIDR	pcx-eeeegggg
	VPC & IPv6 CIDR	pcx-eeeegggg
	VPC F IPv4	pcx-ffffgggg
	VPC F IPv6	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 VPC yang memiliki blok CIDR yang tumpang tindih.

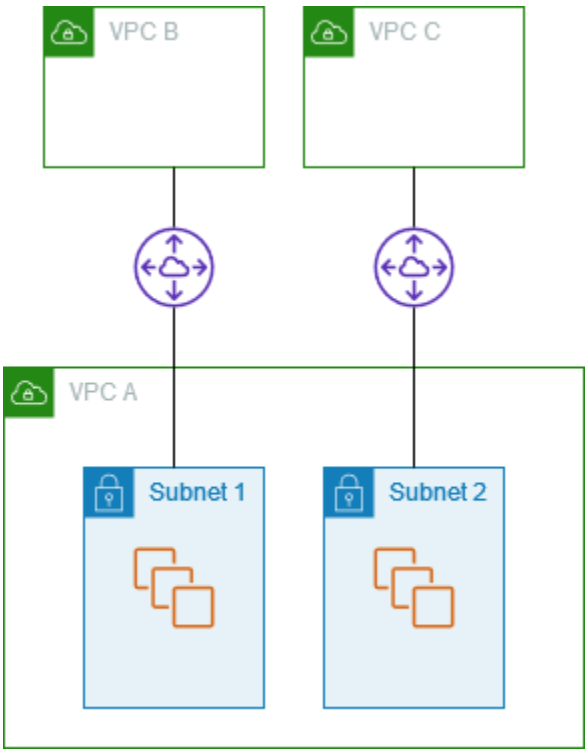
Untuk contoh skenario di mana Anda mungkin memerlukan konfigurasi koneksi peering VPC tertentu, lihat Skenario peering VPC. Untuk informasi selengkapnya tentang bekerja dengan koneksi peering VPC, lihat. Bekerja dengan koneksi peering VPC Untuk informasi selengkapnya tentang pembaruan tabel rute Anda,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

Konfigurasi

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

Dua VPC 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 KE CIDR*	Lokal:
	VPC B CIDR	pcx-aaaabbbb
Subnet 2 (VPC A)	*VPC KE CIDR*	Lokal:
	VPC C CIDR	pcx-aaaacccc
VPC B	*VPC B CIDR*	Lokal:
	Subnet 1 CIDR	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Lokal:

Tabel rute	Tujuan	Target
	Subnet 2 CIDR	pcx-aaaacccc

Anda dapat memperluas konfigurasi ini ke beberapa blok CIDR. Misalkan VPC A dan VPC B memiliki blok CIDR IPv4 dan IPv6, dan subnet 1 memiliki blok CIDR IPv6 terkait. Anda dapat mengaktifkan VPC B untuk berkomunikasi dengan subnet 1 di VPC A melalui IPv6 menggunakan 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 ke IPv4 CIDR*	Lokal:	
	VPC ke IPv6 CIDR	Lokal:	Rute lokal yang secara otomatis ditambahkan untuk komunikasi IPv6 dalam VPC.
	VPC B IPv4 CIDR	pcx-aaaabbbb	
	VPC B IPv6 CIDR	pcx-aaaabbbb	Rute ke blok CIDR IPv6 dari VPC B.
Subnet 2 di VPC A	*VPC ke IPv4 CIDR*	Lokal:	
	VPC ke IPv6 CIDR	Lokal:	Rute lokal yang secara otomatis ditambahkan untuk komunikasi IPv6 dalam VPC.
	VPC C IPv4 CIDR	pcx-aaaacccc	
VPC B	*VPC B IPv4 CIDR*	Lokal:	

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

Dua VPC yang mengakses blok CIDR tertentu dalam satu VPC

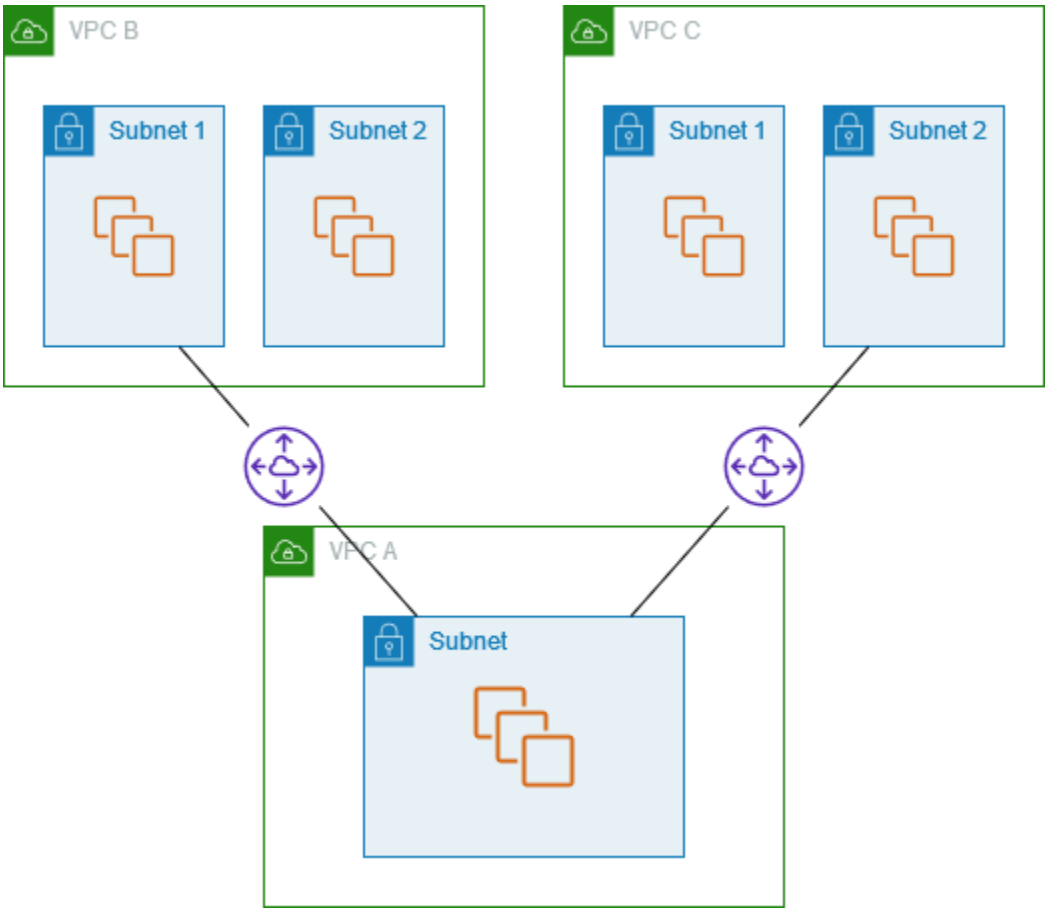
Dalam konfigurasi ini, terdapat VPC pusat (VPC A), koneksi peering antara VPC A dan VPC `pcx-aaaabbbb` B (), dan koneksi peering antara VPC A dan VPC C (). `pcx-aaaacccc` VPC A memiliki satu blok CIDR untuk setiap koneksi peering.

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

Tabel rute	Tujuan	Target
VPC C	*VPC C CIDR*	Lokal:
	VPC KE CIDR 2	pcx-aaaacccc

Satu VPC yang mengakses subnet tertentu dalam dua VPC

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 perlu diakses oleh VPC lain. VPC pusat tidak memerlukan akses penuh ke VPC yang tersambung kepadanya.

Tabel rute untuk VPC A menggunakan koneksi peering untuk mengakses hanya subnet tertentu di VPC peered. 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 KE CIDR*	Lokal:
	Subnet 1 CIDR	pcx-aaaabbbb
	Subnet 2 CIDR	pcx-aaaacccc
Subnet 1 (VPC B)	*VPC B CIDR*	Lokal:
	Subnet di VPC A CIDR	pcx-aaaabbbb
Subnet 2 (VPC C)	*VPC C CIDR*	Lokal:
	Subnet di VPC A CIDR	pcx-aaaacccc

Perutean untuk lalu lintas respons

Jika Anda memiliki VPC yang diintip dengan beberapa VPC yang memiliki blok CIDR yang tumpang tindih atau cocok, pastikan tabel rute Anda dikonfigurasi untuk menghindari pengiriman lalu lintas respons dari VPC Anda ke VPC yang salah. AWStidak 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:

Tabel rute	Tujuan	Target
	Subnet di VPC A CIDR	pcx-aaaabbbb
VPC A	*VPC KE 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 B di VPC B dan dengan subnet A 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.

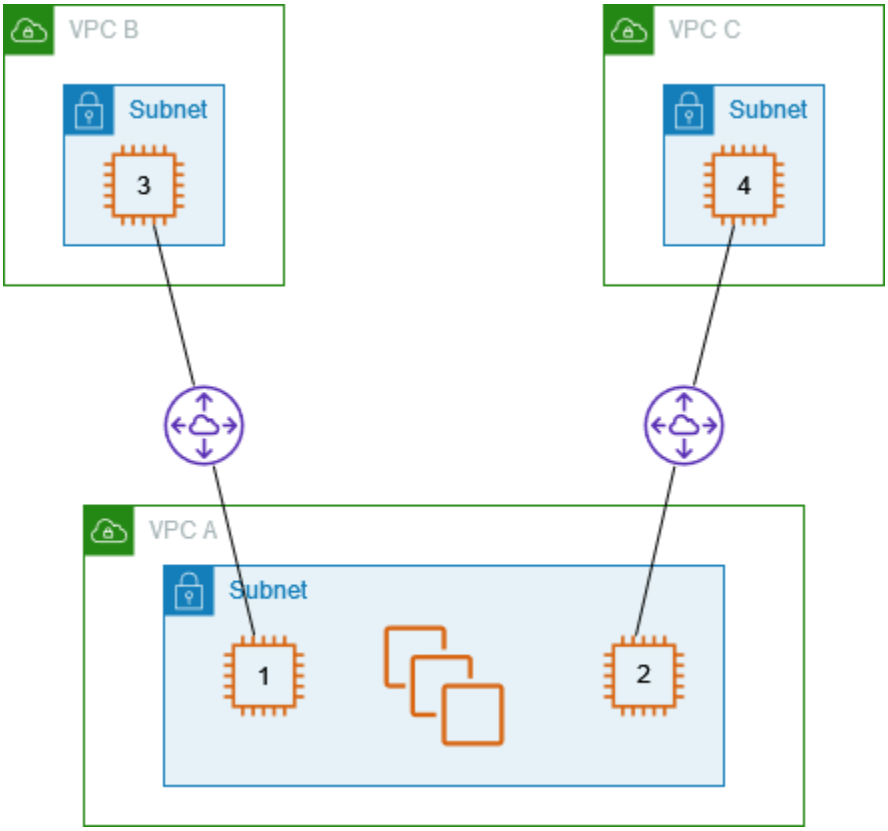
Tujuan	Target
VPC KE CIDR	Lokal:
Subnet 2 CIDR	pcx-aaaabbbb
Subnet 1 CIDR	pcx-aaaacccc

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 KE CIDR	Lokal:
Alamat IP spesifik di subnet 2	pcx-aaaabbbb
VPC B CIDR	pcx-aaaacccc

Instans dalam satu VPC yang mengakses instance tertentu dalam dua VPC

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.

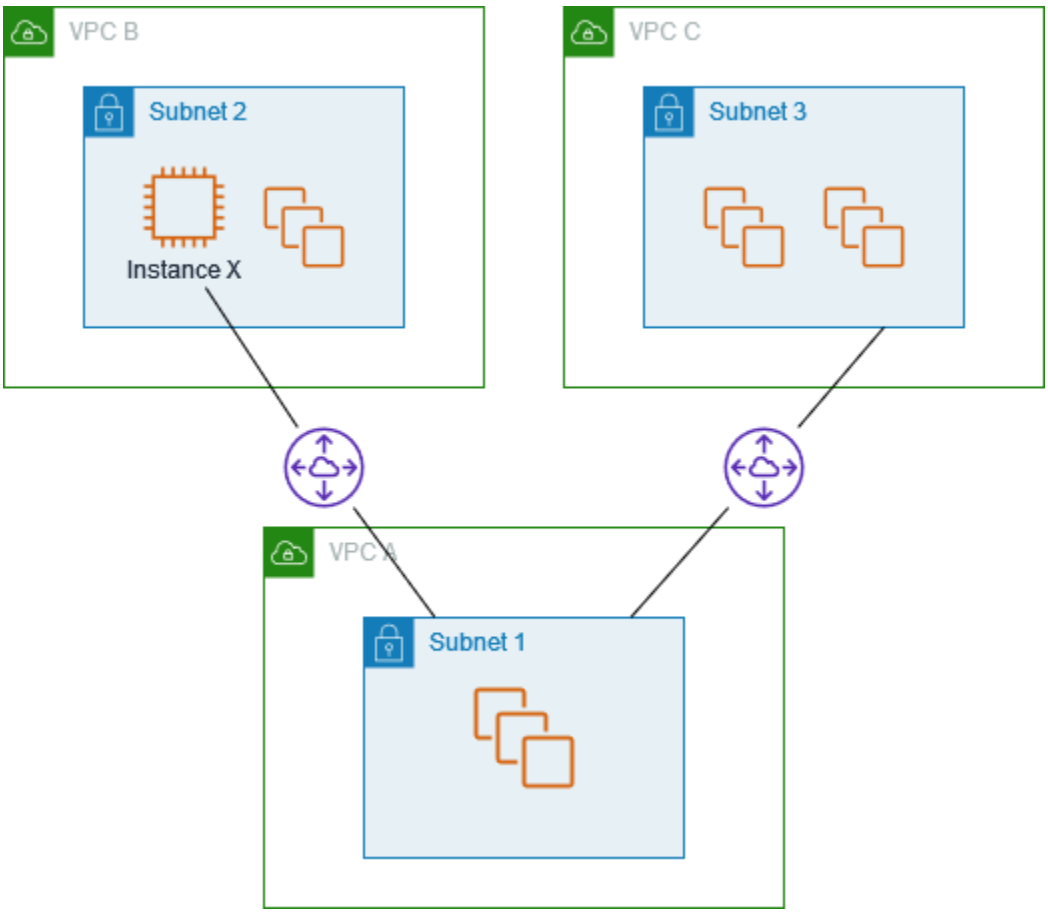


Setiap tabel rute VPC mengacu ke koneksi peering VPC yang relevan untuk mengakses sebuah alamat IP (dan karena itulah terdapat instans khusus) di VPC rekan.

Tabel rute	Tujuan	Target
VPC A	*VPC KE CIDR*	Lokal:
	Alamat IP instans 3	pcx-aaaabbbb
	Alamat IP Instance 4	pcx-aaaacccc
VPC B	*VPC B CIDR*	Lokal:
	Alamat IP instans 1	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Lokal:
	Alamat IP Instance 2	pcx-aaaacccc

Satu VPC yang mengakses dua VPC 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 blok CIDR*	Lokal:
	Alamat IP Instance X	pcx-aaaabbbb
	Blok VPC C CIDR	pcx-aaaacccc
VPC B	*Blok VPC B CIDR*	Lokal:
	VPC A blok CIDR	pcx-aaaabbbb
VPC C	*Blok VPC C CIDR*	Lokal:

Tabel rute	Tujuan	Target
	VPC A blok CIDR	pcx-aaaacccc

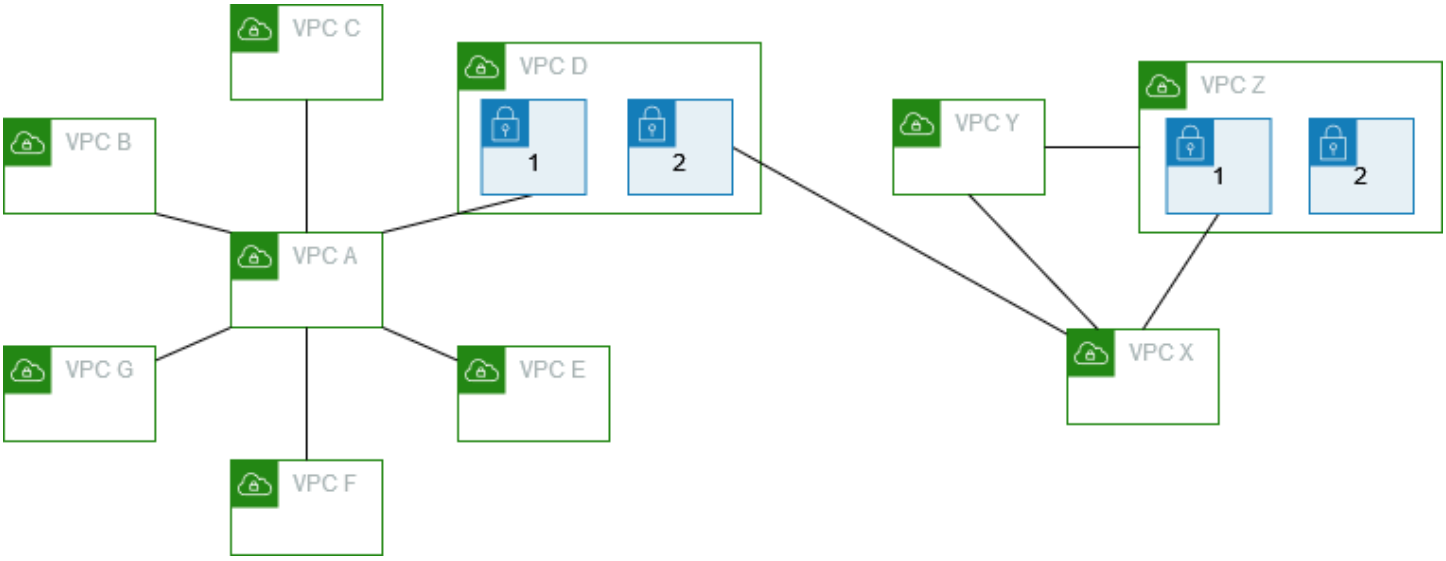
> **Important**
>
> Jika instance selain instance X di VPC B mengirimkan lalu lintas ke VPC A, lalu lintas respons mungkin diarahkan ke VPC C, bukan VPC B. Untuk informasi lebih lanjut, lihat. Perutean untuk lalu lintas respons

Beberapa konfigurasi VPC

Dalam konfigurasi ini, ada VPC pusat (VPC A) yang diintip dengan beberapa VPC dalam konfigurasi spoke. Anda juga memiliki tiga VPC (VPC 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. AWStidak 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 VPC 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 VPC 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 KE CIDR*	Lokal:
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
	Subnet 1 CIDR dalam VPC D	pcx-aaaadddd
	VPC DAN CIDR	pcx-aaaaeeee
	VPC F CIDR	pcx-aaaaffff

Tabel rute	Tujuan	Target
	VPC G CIDR	pcx-aaaagggg
VPC B	*VPC B CIDR*	Lokal:
	VPC KE CIDR	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Lokal:
	VPC KE CIDR	pcx-aaaacccc
Subnet 1 di VPC D	*VPC D CIDR*	Lokal:
	VPC KE CIDR	pcx-aaaadddd
Subnet 2 di VPC D	*VPC D CIDR*	Lokal:
	VPC X CIDR	pcx-ddddxxxx
VPC E	*VPC DAN CIDR*	Lokal:
	VPC KE CIDR	pcx-aaaaeeee
VPC F	*VPC F CIDR*	Lokal:
	VPC KE CIDR	pcx-aaaaffff
VPC G	*VPC G CIDR*	Lokal:
	VPC KE CIDR	pcx-aaaagggg
VPC X	*VPC X CIDR*	Lokal:
	Subnet 2 CIDR di VPC D	pcx-ddddxxxx
	VPC DAN CIDR	pcx-xxxxyyyy
	Subnet 1 CIDR di VPC Z	pcx-xxxxzzzz
VPC Y	*VPC DAN CIDR*	Lokal:

Tabel rute	Tujuan	Target
	VPC X CIDR	pcx-xxxxyyyy
	VPC Z CIDR	pcx-yyyzzzz
VPC Z	*VPC Z CIDR*	Lokal:
	VPC DAN CIDR	pcx-yyyzzzz
	VPC X CIDR	pcx-xxxxzzzz

Skenario peering VPC

Ada beberapa alasan Anda mungkin perlu mengatur koneksi peering VPC antar VPC-VPC Anda, atau antara VPC yang Anda miliki dan VPC dalam akun AWS yang berbeda. Skenario berikut ini dapat membantu Anda menentukan konfigurasi yang paling sesuai dengan kebutuhan jaringan Anda.

Skenario

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

Menyambungkan dua VPC atau lebih untuk menyediakan akses penuh ke sumber daya

Dalam skenario ini, Anda memiliki dua atau lebih VPC yang ingin Anda sambungkan untuk mengaktifkan pembagian penuh sumber daya antara semua VPC. Berikut ini adalah beberapa contoh:

- 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 VPC terletak di akun AWS yang sama, dan VPC lainnya ada di akun AWS yang berbeda. Anda ingin menyambungankan semua VPC bersama-sama untuk memungkinkan departemen IT untuk 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 VPC disambungkan bersama
- Tiga VPC disambungkan bersama
- Beberapa VPC disambungkan bersama

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

Menyambung ke satu VPC untuk mengakses sumber daya terpusat

Dalam skenario ini, Anda memiliki sebuah VPC pusat yang berisikan sumber daya yang Anda ingin bagikan dengan VPC-VPC lain. VPC pusat Anda mungkin memerlukan akses penuh atau sebagian ke VPC rekan, dan demikian pula, VPC rekan mungkin memerlukan akses penuh atau sebagian ke VPC pusat. Berikut ini adalah beberapa contoh:

- Departemen IT perusahaan Anda memiliki sebuah VPC untuk berbagi file. Anda ingin menyambungkan VPC lain ke VPC pusat, akan tetapi, Anda tidak mau VPC-VPC lain saling 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, akan tetapi, pelanggan Anda tidak dapat mengarahkan lalu lintas ke VPC lain yang tersambung ke VPC Anda, juga tidak menyadari rute pelanggan lain.
- Anda memiliki VPC pusat yang digunakan untuk layanan Direktori Aktif. Instans tertentu di VPC-VPC rekan mengirim permintaan ke server Direktori Aktif dan memerlukan akses penuh ke VPC pusat. VPC pusat tidak memerlukan akses penuh ke VPC rekan; VPC pusat hanya perlu mengarahkan respons lalu lintas ke instans tertentu.

Untuk informasi lebih lanjut tentang membuat dan bekerja dengan koneksi peering VPC di konsol Amazon VPC, lihat Bekerja dengan 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 dalam identitas IAM, seperti peran.

Contoh

- Contoh: Membuat koneksi peering VPC
- Contoh: Menerima koneksi peering VPC
- Contoh: Menghapus koneksi peering VPC
- Contoh: Bekerja dalam akun tertentu
- Contoh: Mengelola koneksi peering VPC menggunakan konsol

Untuk daftar tindakan Amazon VPC, dan sumber daya yang di-support dan kunci persyaratan untuk setiap tindakan, lihat Tindakan, sumber daya, dan kunci persyaratan untuk Amazon EC2 di Amazon EC2 di Referensi Otorisasi Layanan.

Contoh: Membuat koneksi peering VPC

Kebijakan berikut memberikan izin pengguna untuk membuat permintaan koneksi peering VPC menggunakan VPC yang di-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 pengguna untuk membuat sumber daya koneksi peering VPC, dan oleh karenanya menggunakan wildcard * sebagai ID sumber daya tertentu.

```
{
  "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 memberikan izin pengguna diAWS akun tertentu untuk membuat koneksi peering VPC menggunakan VPC apapun di Wilayah yang ditentukan, tetapi hanya jika VPC yang menerima koneksi peering tersebut adalah VPC khusus di akun khusus.

```
{
  "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: Menerima koneksi peering VPC

Kebijakan berikut memberikan izin pengguna untuk menerima permintaan koneksi peering VPC dariAWS akun tertentu. Hal ini membantu untuk mencegah pengguna menerima koneksi

peering VPC dari akun tak dikenal. Pernyataan tersebut menggunakan kuncie`c2:RequesterVpc` persyaratan untuk memberlakukannya.

```
{
  "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 pengguna untuk menerima permintaan peering VPC jika VPC memiliki tag tersebut`Purpose=Peering`.

```
{
  "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: Menghapus koneksi peering VPC

Kebijakan berikut memberikan izin pengguna di akun tertentu untuk menghapus izin pengguna di akun tertentu untuk menghapus koneksi peering VPC apapun, kecuali yang menggunakan VPC yang sudah ditentukan, yang berada dalam akun yang sama. Kebijakan tersebut menentukan kedua kunci`ec2:AccepterVpc`e`c2:RequesterVpc` persyaratan, karena VPC mungkin adalah VPC peminta atau VPC rekan dalam permintaan koneksi peering VPC pada mulanya.

```
{
  "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 pengguna untuk bekerja dengan koneksi peering VPC dalam akun tertentu. Pengguna dapat melihat, membuat, menerima, dan menghapus koneksi peering VPC, asalkan semuanya berada dalamAWS akun yang sama.

Pernyataan pertama memberikan izin pengguna 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 pengguna untuk membuat koneksi peering VPC, dan akses ke semua VPC di akun yang ditentukan untuk melakukannya.

Pernyataan ketiga menggunakan wildcard * sebagai bagian dari`Action` elemen untuk memberikan izin untuk semua pelaksanaan koneksi peering VPC. Kunci persyaratan memastikan bahwa tindakan

hanya dapat dilakukan pada koneksi peering VPC pada VPC yang merupakan bagian dari akun. Sebagai contoh, pengguna tidak dapat menghapus koneksi peering VPC jika VPC penerima atau peminta tidak dalam akun yang berbeda. Pengguna tidak dapat membuat koneksi peering VPC dengan VPC di akun yang berbeda.

```
{
  "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: Mengelola 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`. Hal ini membuat mereka dapat melihat dan memilih VPC. Anda dapat menerapkan izin di tingkat sumber daya untuk semua tindakan `ec2:*PeeringConnection`, kecuali `ec2:DescribeVpcPeeringConnections`.

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

```
{
  "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/*"
      ]
    }
  ]
}
```

peering VPC Vpeering Vpeering Vpeering Vpeering

Tabel peering Vpeering Vpeering Vpeering Vpeering Vpeering Vpeering Vpeering Vpeering Vpeering Vpeering Vpeering VPC Vpeering Vpeering Vpeering VpeeringAWS Vpeering V Kecuali disebutkan lain, Anda dapat meminta penambahan untuk kuota ini.

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 lebih lanjut tentang aturan peering Vpeering Vpeering Vpeering Vpeering Vpeering Vpeering Vpeering Vpeering VpeeringKeterbatasan peering VPC Vpeering

Untuk kuota tambahan untuk Amazon VPC, lihat kuota Amazon VPC di Panduan Pengguna Amazon VPC.

Riwayat dokumen untuk Panduan Peering VPC Amazon

Tabel berikut menjelaskan dokumentasi rilis untuk Amazon VPC Peering Guide.

Perubahan	Deskripsi	Tanggal
Tag pada create	Anda dapat menambahkan tag ketika Anda membuat koneksi peering VPC tabel rute.	20 Juli 2020
peering	Resolusi nama host DNS di-support untuk koneksi peering VPC antar wilayah di Wilayah Asia Pacific (Hong Kong).	26 Agustus 2019
peering	Anda dapat membuat koneksi peering VPC antar VPC di berbagai Wilayah AWS.	29 November 2017
Support resolusi DNS untuk peering 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 yang kelaluwarsa	Anda dapat mengident ifikasi jika grup keamanan Anda sedang dirujuk di grup keamanan di VPC rekan dan Anda dapat mengidentifikasi aturan grup keamanan yang ketar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar tar	12 Mei 2016

Menggunakan ClassicLink koneksi peering VPC	Anda dapat memodifikasi koneksi peering VPC Anda untuk mengaktifkan instans EC2-Classic yang terkait lokal untuk berkomunikasi dengan instans-instans di VPC peer, atau sebaliknya.	26 April 2016
VPC mengintip	Anda dapat membuat koneksi peering VPC antara dua VPC, yang mengizinkan instans di salah satu VPC 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.