



Panduan Pengguna

AWS Site-to-Site VPN



AWS Site-to-Site VPN: Panduan Pengguna

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

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

Table of Contents

Apa itu Site-to-Site VPN	1
Konsep	1
Fitur VPN Site-to-Site	2
Batasan Site-to-Site VPN	2
Bekerja dengan Site-to-Site VPN	3
Harga	3
Bagaimana cara AWS Site-to-Site VPN kerja	4
Gateway privat virtual	4
Gateway transit	5
Perangkat gateway pelanggan	5
Gateway pelanggan	6
Opsi terowongan VPN	6
VPNopsi otentikasi terowongan	13
Kunci pra-berbagi	13
Sertifikat pribadi dari AWS Private Certificate Authority	14
Opsi inisiasi terowongan VPN	14
Opsi inisiasi IKE terowongan VPN	14
Aturan dan batasan	15
Bekerja dengan opsi inisiasi terowongan VPN	15
Penggantian titik akhir	16
Penggantian titik akhir yang diprakarsai pelanggan	16
AWS mengelola penggantian endpoint	17
Siklus hidup titik akhir terowongan	17
Opsi gateway pelanggan	23
Koneksi VPN yang dipercepat	26
Mengaktifkan akselerasi	26
Peraturan dan pembatasan	26
Opsi perutean VPN situs-ke-situs	27
Perutean statis dan dinamis	28
Tabel rute dan prioritas VPN rute	28
Perutean selama pembaruan titik akhir VPN terowongan	31
Lalu lintas IPv4 dan IPv6	31
Tutorial memulai	33
Prasyarat	33

Buat gateway pelanggan	35
Buat gateway target	36
Buat gateway privat virtual	36
Buat transit gateway	37
Konfigurasi perutean	37
(Gateway privat virtual) Aktifkan propagasi rute di tabel rute Anda	37
(Transit gateway) Tambahkan rute ke tabel rute Anda	39
Perbarui grup keamanan Anda	39
Buat koneksi VPN	40
Unduh file konfigurasi	41
Konfigurasi perangkat gateway pelanggan	42
Arsitektur	43
Beberapa skenario VPN koneksi	43
Koneksi VPN tunggal dan ganda	43
AWS VPN CloudHub	48
Koneksi VPN redundan	50
Perangkat gateway pelanggan Anda	53
Persyaratan	54
Praktik terbaik	57
Aturan firewall	59
Contoh file konfigurasi	62
Contoh konfigurasi untuk perutean statis	64
Contoh konfigurasi untuk perutean dinamis	77
Windows Server sebagai perangkat gateway pelanggan	89
Mengonfigurasi instans Windows Anda	89
Langkah 1: Buat koneksi VPN dan konfigurasi VPC Anda	90
Langkah 2: Unduh file konfigurasi untuk koneksi VPN	91
Langkah 3: Mengonfigurasi Windows Server	94
Langkah 4: Mengatur terowongan VPN	95
Langkah 5: Aktifkan deteksi gateway mati	102
Langkah 6: Uji koneksi VPN	102
Pemecahan Masalah	103
Perangkat dengan BGP	104
Perangkat tanpa BGP	107
Cisco ASA	110
Cisco IOS	114

Cisco tanpa IOS BGP	120
Juniper JunOS	126
Juniper ScreenOS	131
Yamaha	134
Bekerja dengan Site-to-Site VPN	140
Buat lampiran VPN untuk AWS Cloud WAN	140
Buat lampiran VPN gateway transit	142
Uji koneksi VPN	144
Hapus koneksi VPN	145
Hapus koneksi VPN	146
Hapus gateway pelanggan	147
Lepaskan dan hapus gateway pribadi virtual	147
Ubah gateway target koneksi VPN	148
Langkah 1: Buat gateway target baru	149
Langkah 2: Hapus rute statis Anda (bersyarat)	149
Langkah 3: Migrasi ke gateway baru	150
Langkah 4: Perbarui tabel rute VPC	150
Langkah 5: Perbarui perutean gateway target (bersyarat)	151
Langkah 6: Perbarui gateway pelanggan ASN (bersyarat)	152
Mengubah opsi koneksi VPN	152
Ubah opsi terowongan VPN	153
Edit rute statis untuk koneksi VPN	153
Ubah gateway pelanggan untuk koneksi VPN	154
Ganti kredensial yang dikompromikan	155
Putar sertifikat titik akhir terowongan VPN	156
VPN IP pribadi dengan AWS Direct Connect	156
Manfaat VPN IP Pribadi	157
Cara kerja VPN IP pribadi	158
Prasyarat	158
Buat gateway pelanggan	158
Siapkan gerbang transit	159
Buat AWS Direct Connect gateway	160
Buat asosiasi gateway transit	160
Buat koneksi VPN	160
Keamanan	162
Perlindungan data	162

Privasi lalu lintas antar jaringan	164
Pengelolaan identitas dan akses	164
Audiens	165
Mengautentikasi dengan identitas	166
Mengelola akses menggunakan kebijakan	169
Bagaimana AWS VPN Site-to-Site bekerja dengan IAM	172
Contoh kebijakan berbasis identitas	179
Pemecahan Masalah	182
Menggunakan peran terkait layanan	184
Ketangguhan	187
Dua terowongan per koneksi VPN	187
Redundansi	187
Keamanan infrastruktur	188
Memantau koneksi Site-to-Site VPN Anda	189
Alat pemantauan	190
Alat pemantauan otomatis	190
Alat pemantauan manual	190
AWS Site-to-Site VPN log	191
Manfaat log VPN Site-to-Site	192
Pembatasan ukuran kebijakan sumber daya Amazon CloudWatch Logs	192
Isi log VPN Site-to-Site	193
Persyaratan IAM untuk mempublikasikan ke CloudWatch Log	196
Lihat konfigurasi log VPN Site-to-Site	197
Aktifkan log VPN Site-to-Site	198
Nonaktifkan log VPN Site-to-Site	199
Memantau terowongan VPN menggunakan Amazon CloudWatch	200
Metrik dan dimensi VPN	200
Melihat CloudWatch metrik VPN	202
Membuat CloudWatch alarm untuk memantau terowongan VPN	202
Memantau koneksi VPN menggunakan AWS Health acara	205
Notifikasi penggantian titik akhir terowongan	205
Notifikasi VPN terowongan tunggal	206
Kuota	207
Sumber daya Site-to-Site VPN	207
Rute	208
Bandwidth dan throughput	209

Unit transmisi maksimum (MTU)	209
Sumber daya kuota tambahan	210
Riwayat dokumen	211
.....	ccxvi

Apa itu AWS Site-to-Site VPN?

Secara default, instans yang Anda luncurkan ke Amazon VPC tidak dapat berkomunikasi dengan jaringan (jarak jauh) Anda sendiri. Anda dapat mengaktifkan akses ke jaringan jarak jauh dari VPC Anda dengan membuat koneksi AWS Site-to-Site VPN (Site-to-Site VPN), dan mengonfigurasi perutean untuk melewati lalu lintas melalui koneksi.

Meskipun syarat Koneksi VPN adalah syarat umum, dalam dokumentasi ini, koneksi VPN mengacu pada koneksi antara VPC dan jaringan On-Premise Anda sendiri. Site-to-Site VPN mendukung koneksi VPN keamanan Internet Protocol (IPSec).

Daftar Isi

- [Konsep](#)
- [Fitur VPN Site-to-Site](#)
- [Batasan Site-to-Site VPN](#)
- [Bekerja dengan Site-to-Site VPN](#)
- [Harga](#)

Konsep

Berikut ini adalah konsep kunci untuk Site-to-Site VPN:

- Koneksi VPN: Koneksi aman antara peralatan On-Premise dan VPC Anda.
- Terowongan VPN: Tautan terenkripsi tempat data dapat lewat dari jaringan pelanggan ke atau dari AWS.

Setiap koneksi VPN mencakup dua terowongan VPN yang dapat Anda gunakan secara bersamaan untuk ketersediaan tinggi.

- Customer Gateway: AWS Sumber daya yang menyediakan informasi AWS tentang perangkat gateway pelanggan Anda.
- Perangkat gateway pelanggan: Perangkat fisik atau aplikasi perangkat lunak di sisi koneksi Site-to-Site VPN Anda.
- Gateway target: Istilah umum untuk titik akhir VPN di sisi Amazon dari koneksi VPN Site-to-Site.
- Gateway pribadi virtual: Gateway pribadi virtual adalah titik akhir VPN di sisi Amazon dari koneksi VPN Site-to-Site Anda yang dapat dilampirkan ke satu VPC.

- Transit gateway: Hub transit yang dapat digunakan untuk menghubungkan beberapa VPC dan jaringan lokal, dan sebagai titik akhir VPN untuk sisi Amazon dari koneksi VPN Site-to-Site.

Fitur VPN Site-to-Site

Fitur-fitur berikut didukung pada AWS Site-to-Site VPN koneksi:

- Pertukaran Kunci Internet versi 2 (IKEv2)
- NAT traversal
- ASN 4-byte dalam kisaran 1 — 2147483647 untuk konfigurasi Virtual Private Gateway (VGW). Untuk informasi selengkapnya, lihat [Opsi gateway pelanggan untuk koneksi Site-to-Site VPN](#).
- ASN 2-byte untuk Customer Gateway (CGW) dalam kisaran 1 - 65535. Untuk informasi selengkapnya, lihat [Opsi gateway pelanggan untuk koneksi Site-to-Site VPN](#).
- CloudWatch metrik
- Alamat IP yang dapat digunakan kembali untuk gateway pelanggan Anda
- Pilihan enkripsi tambahan; termasuk enkripsi AES 256-bit, hashing SHA-2, dan grup Diffie-Hellman tambahan
- Opsi terowongan yang dapat dikonfigurasi
- ASN privat kustom untuk sisi Amazon dari sesi BGP
- Sertifikat Pribadi dari CA bawahan dari AWS Private Certificate Authority
- Mendukung lalu lintas IPv6 untuk koneksi VPN pada gateway transit

Batasan Site-to-Site VPN

Koneksi Site-to-Site VPN memiliki keterbatasan sebagai berikut.

- Lalu lintas IPv6 tidak didukung untuk koneksi VPN pada gateway privat virtual.
- AWS VPN Koneksi tidak mendukung Path MTU Discovery.

Selain itu, pertimbangkan hal berikut saat Anda menggunakan Site-to-Site VPN.

- Saat menghubungkan VPC ke jaringan On-Premise umum, kami merekomendasikan penggunaan blok CIDR yang tidak tumpang tindih untuk jaringan Anda.

Bekerja dengan Site-to-Site VPN

Anda dapat membuat, mengakses, dan mengelola sumber daya Site-to-Site VPN menggunakan salah satu antarmuka berikut:

- **AWS Management Console**— Menyediakan antarmuka web yang dapat Anda gunakan untuk mengakses sumber daya Site-to-Site VPN Anda.
- **AWS Command Line Interface (AWS CLI)** - Menyediakan perintah untuk serangkaian AWS layanan yang luas, termasuk Amazon VPC, dan didukung di Windows, macOS, dan Linux. Untuk informasi selengkapnya, lihat [AWS Command Line Interface](#).
- **AWS SDK** — Menyediakan API khusus bahasa dan menangani banyak detail koneksi, seperti menghitung tanda tangan, menangani percobaan ulang permintaan, dan penanganan kesalahan. Untuk informasi selengkapnya, lihat [SDK AWS](#).
- **API Kueri**— Menyediakan tindakan API tingkat rendah yang Anda hubungi menggunakan permintaan HTTPS. Menggunakan API Kueri merupakan cara paling langsung untuk mengakses Amazon VPC, tetapi mengharuskan aplikasi Anda menangani detail tingkat rendah seperti membuat hash untuk menandatangani permintaan, dan penanganan kesalahan. Untuk informasi selengkapnya, lihat [Referensi API Amazon EC2](#).

Harga

Anda dikenakan biaya untuk setiap jam koneksi VPN sehingga koneksi VPN Anda disediakan dan tersedia. Untuk informasi selengkapnya, lihat [AWS Site-to-Site VPN dan harga Koneksi VPN Site-to-Site yang Dipercepat](#).

Anda dikenakan biaya untuk transfer data dari Amazon EC2 ke internet. Untuk informasi selengkapnya, lihat [Transfer Data](#) di halaman Harga Sesuai Permintaan Amazon EC2.

Ketika Anda membuat koneksi VPN yang terakselerasi, kami membuat dan mengelola dua akselerator atas nama Anda. Anda akan dikenakan biaya per jam dan biaya transfer data untuk setiap akselerator. Untuk informasi selengkapnya, lihat [Harga AWS Global Accelerator](#).

Bagaimana cara AWS Site-to-Site VPN kerja

Koneksi VPN Site-to-Site terdiri dari komponen-komponen berikut:

- [Gateway pribadi virtual](#) atau [gateway transit](#)
- [Perangkat gateway pelanggan](#)
- [Gateway pelanggan](#)

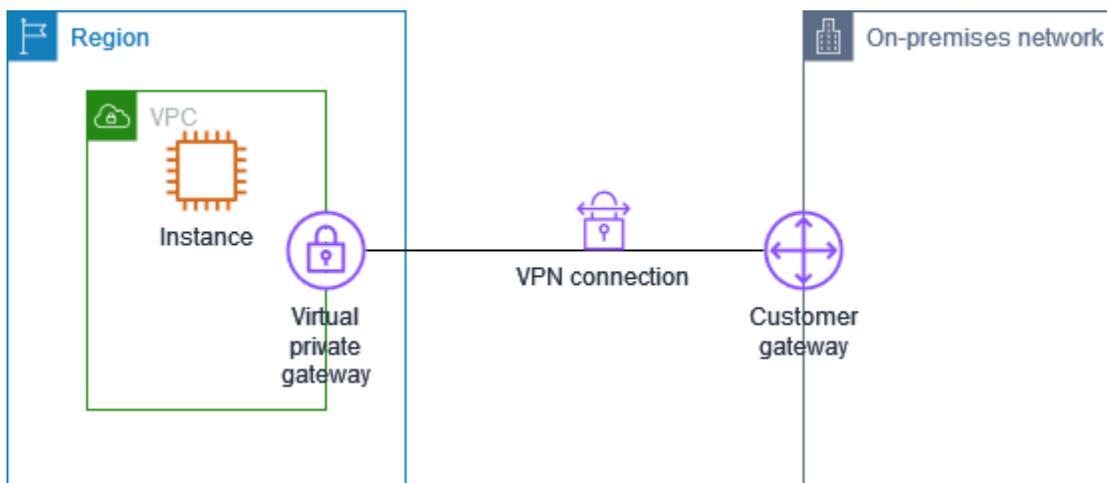
Koneksi VPN menawarkan dua terowongan VPN antara gateway pribadi virtual atau gateway transit di AWS samping, dan gateway pelanggan di sisi lokal.

Untuk informasi selengkapnya tentang kuota Site-to-Site VPN, lihat [Kuota Site-to-Site VPN](#).

Gateway privat virtual

Gateway privat virtual adalah konsentrator VPN di sisi Amazon dari koneksi Site-to-Site VPN. Anda membuat gateway pribadi virtual dan melampirkannya ke cloud pribadi virtual (VPC) dengan sumber daya yang harus mengakses koneksi VPN Site-to-Site.

Diagram berikut menunjukkan koneksi VPN antara VPC dan jaringan lokal Anda menggunakan gateway pribadi virtual.



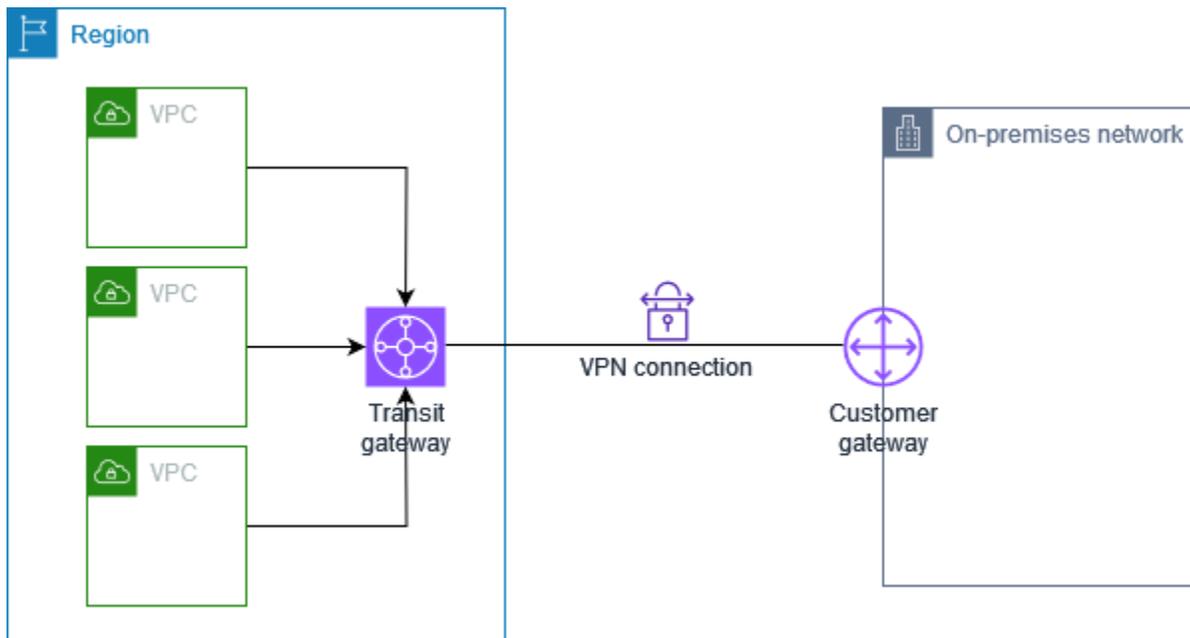
Ketika Anda membuat gateway privat virtual, Anda dapat menentukan Nomor Sistem Otonom (ASN) privat untuk sisi Amazon gateway. Jika Anda tidak menentukan ASN, gateway privat virtual dibuat menggunakan ASN default (64512). Anda tidak dapat mengubah ASN setelah Anda membuat gateway privat virtual. Untuk memeriksa ASN untuk gateway pribadi virtual Anda, lihat detailnya

di halaman gateway pribadi virtual di konsol VPC Amazon, atau gunakan perintah. [describe-vpn-gateways](#) AWS CLI

Gateway transit

Gateway transit adalah hub transit yang dapat Anda gunakan untuk menghubungkan VPC dan jaringan lokal Anda. Untuk informasi selengkapnya, lihat [Amazon VPC Transit Gateways](#). Anda dapat membuat koneksi Site-to-Site VPN sebagai lampiran pada gateway transit.

Diagram berikut menunjukkan koneksi VPN antara beberapa VPC dan jaringan lokal Anda menggunakan gateway transit. Gateway transit memiliki tiga lampiran VPC dan lampiran VPN.



Koneksi Site-to-Site VPN Anda pada gateway transit dapat mendukung lalu lintas IPv4 atau lalu lintas IPv6 di dalam terowongan VPN. Untuk informasi selengkapnya, lihat [Lalu lintas IPv4 dan IPv6](#).

Anda dapat mengubah gateway target koneksi Site-to-Site VPN dari gateway privat virtual untuk gateway transit. Untuk informasi selengkapnya, lihat [the section called “Ubah gateway target koneksi VPN”](#).

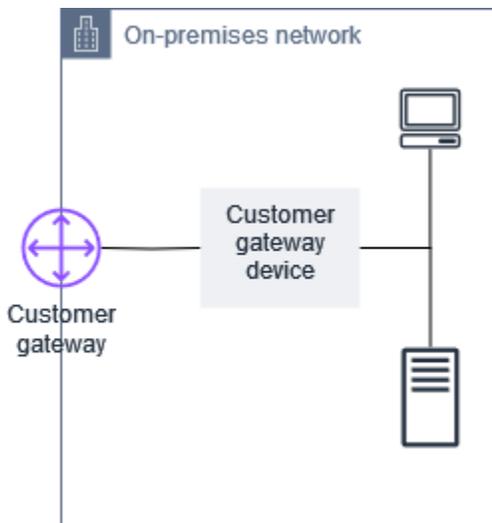
Perangkat gateway pelanggan

Perangkat gateway pelanggan adalah perangkat fisik atau aplikasi perangkat lunak di sisi koneksi Site-to-Site VPN Anda. Anda mengonfigurasi perangkat untuk bekerja dengan koneksi Site-to-Site VPN. Untuk informasi selengkapnya, lihat [Perangkat gateway pelanggan Anda](#).

Secara default, perangkat gateway pelanggan Anda harus memunculkan terowongan untuk koneksi Site-to-Site VPN Anda dengan menghasilkan lalu lintas dan memulai proses negosiasi Pertukaran Kunci Internet (IKE). Anda dapat mengkonfigurasi koneksi Site-to-Site VPN untuk menentukan bahwa AWS harus memulai proses negosiasi IKE. Untuk informasi selengkapnya, lihat [Opsi inisiasi terowongan Site-to-Site VPN](#).

Gateway pelanggan

Gateway pelanggan adalah sumber daya yang Anda buat di AWS yang mewakili perangkat gateway pelanggan di jaringan on premise. Saat membuat gateway pelanggan, Anda memberikan informasi tentang perangkat Anda AWS. Untuk informasi selengkapnya, lihat [the section called “Opsi gateway pelanggan”](#).



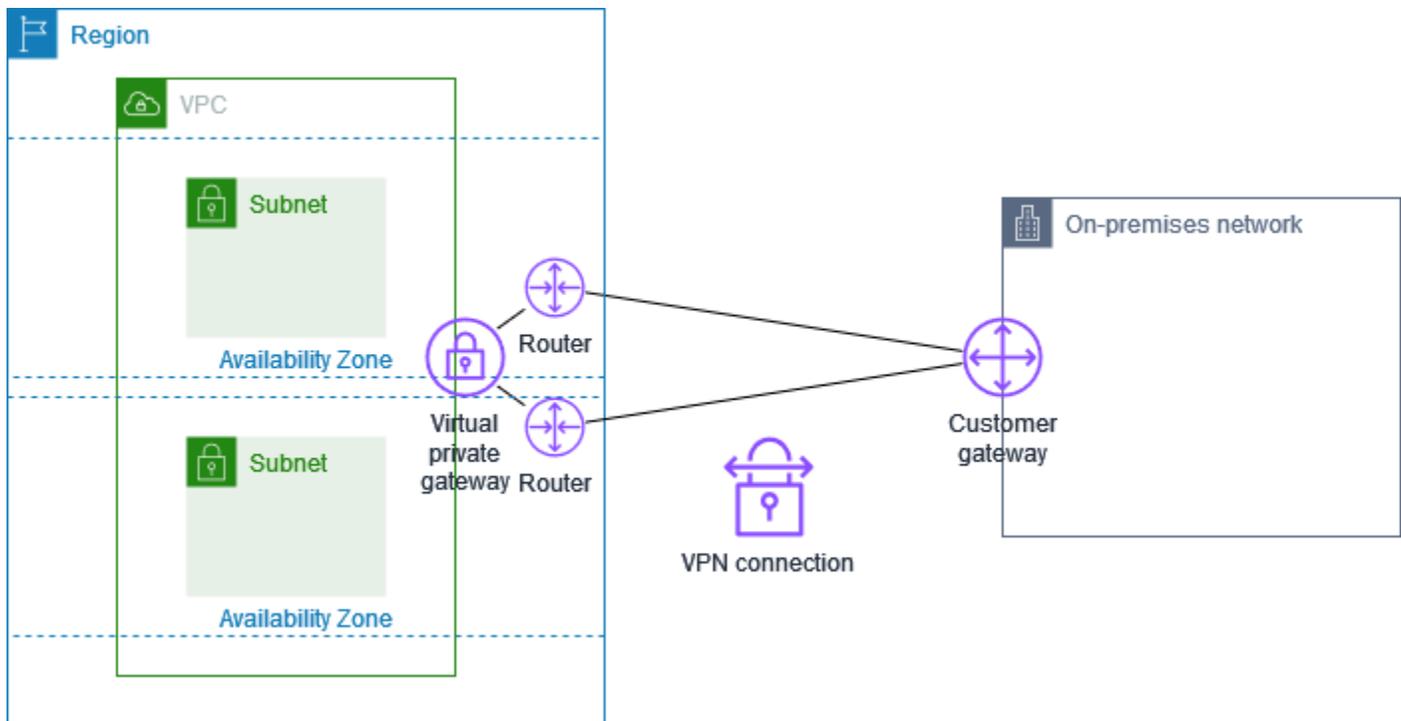
Untuk menggunakan Amazon VPC dengan koneksi Site-to-Site VPN, Anda atau administrator jaringan Anda juga harus mengkonfigurasi perangkat gateway pelanggan atau aplikasi di jaringan jarak jauh Anda. Ketika Anda membuat koneksi Site-to-Site VPN, kami menyediakan informasi konfigurasi yang diperlukan dan administrator jaringan Anda biasanya melakukan konfigurasi ini. Untuk informasi tentang persyaratan dan konfigurasi gateway pelanggan, lihat [Perangkat gateway pelanggan Anda](#).

Opsi terowongan untuk koneksi Site-to-Site VPN Anda

Anda menggunakan koneksi Site-to-Site VPN untuk menghubungkan jaringan jarak jauh Anda ke VPC. Setiap koneksi VPN Site-to-Site memiliki dua terowongan, dengan masing-masing terowongan menggunakan alamat IP publik yang unik. Penting untuk mengonfigurasi kedua terowongan

untuk redundansi. Ketika satu terowongan menjadi tidak tersedia (misalnya, terganggu karena pemeliharaan), lalu lintas jaringan secara otomatis dirutekan ke terowongan yang tersedia untuk koneksi Site-to-Site VPN tertentu.

Diagram berikut menunjukkan dua terowongan koneksi VPN. Setiap terowongan berakhir di Availability Zone yang berbeda untuk memberikan peningkatan ketersediaan. Lalu lintas dari jaringan lokal untuk AWS menggunakan kedua terowongan. Lalu lintas dari AWS ke jaringan lokal lebih memilih salah satu terowongan, tetapi secara otomatis dapat gagal ke terowongan lain jika ada kegagalan di AWS samping.



Ketika Anda membuat koneksi Site-to-Site VPN, Anda mengunduh file konfigurasi khusus untuk perangkat gateway pelanggan Anda yang berisi informasi untuk mengonfigurasi perangkat, termasuk informasi untuk mengonfigurasi setiap terowongan. Anda dapat secara opsional menentukan beberapa opsi terowongan sendiri ketika Anda membuat koneksi Site-to-Site VPN. Jika tidak, AWS memberikan nilai default.

Note

Titik akhir terowongan Site-to-Site VPN mengevaluasi proposal dari gateway pelanggan Anda dimulai dengan nilai terkonfigurasi terendah dari daftar di bawah ini, terlepas dari urutan proposal dari gateway pelanggan. Anda dapat menggunakan `modify-vpn-connection-options` perintah untuk membatasi daftar opsi AWS endpoint akan menerima. Untuk

informasi selengkapnya, lihat [modify-vpn-connection-options](#) di Referensi Baris Perintah Amazon EC2.

Berikut ini adalah opsi terowongan yang dapat Anda konfigurasi.

Waktu habis deteksi peer mati (DPD)

Jumlah detik setelah batas waktu DPD terjadi. Batas waktu DPD 40 detik berarti bahwa titik akhir VPN akan menganggap peer mati 30 detik setelah kegagalan pertama tetap hidup. Anda dapat menentukan 30 atau lebih tinggi.

Default: 40

Tindakan waktu habis DPD

Tindakan yang diambil setelah waktu habis deteksi peer mati (DPD) terjadi. Anda dapat menentukan sebagai berikut:

- `Clear`: Mengakhiri sesi IKE ketika waktu habis DPD terjadi (menghentikan terowongan dan menghapus rute)
- `None`: Tidak mengambil tindakan ketika waktu habis DPD terjadi
- `Restart`: Memulai ulang sesi IKE ketika waktu habis DPD terjadi

Untuk informasi selengkapnya, lihat [Opsi inisiasi terowongan Site-to-Site VPN](#).

Default: `Clear`

Opsi pencatatan VPN

Dengan log VPN Site-to-Site, Anda dapat memperoleh akses ke detail tentang pembentukan terowongan IP Security (IPsec), negosiasi Internet Key Exchange (IKE), dan pesan protokol deteksi rekan mati (DPD).

Untuk informasi selengkapnya, lihat [AWS Site-to-Site VPN log](#).

Format log yang tersedia: `json`, `text`

Versi IKE

Versi (IKE) yang diizinkan untuk terowongan VPN. Anda dapat menentukan satu atau beberapa nilai default.

Default: `ikev1`, `ikev2`

Di dalam terowongan IPv4 CIDR

Rentang alamat IPv4 di dalam (internal) untuk terowongan VPN. Anda dapat menentukan blok CIDR ukuran /30 dari rentang 169.254.0.0/16. Blok CIDR harus unik di semua koneksi Site-to-Site VPN yang menggunakan gateway privat virtual yang sama.

Note

Blok CIDR tidak perlu unik di semua koneksi pada gateway transit. Namun, jika mereka tidak unik, itu dapat menciptakan konflik di gateway pelanggan Anda. Lanjutkan dengan hati-hati saat menggunakan kembali blok CIDR yang sama pada beberapa koneksi VPN Site-to-Site pada gateway transit.

Blok CIDR berikut dicadangkan dan tidak dapat digunakan:

- 169.254.0.0/30
- 169.254.1.0/30
- 169.254.2.0/30
- 169.254.3.0/30
- 169.254.4.0/30
- 169.254.5.0/30
- 169.254.169.252/30

Default: Blok CIDR IPv4 ukuran /30 dari rentang 169.254.0.0/16.

Di dalam terowongan IPv6 CIDR

(Hanya koneksi VPN IPv6) Rentang alamat IPv6 di dalam (internal) untuk terowongan VPN. Anda dapat menentukan blok CIDR ukuran /126 dari rentang fd00:::/8 lokal. Blok CIDR harus unik di semua koneksi Site-to-Site VPN yang menggunakan gateway transit yang sama.

Default: Blok CIDR IPv6 CIDR /126 dari rentang fd00:::/8.

CIDR Jaringan IPv4 Lokal

(Hanya koneksi VPN IPv4) Rentang CIDR IPv4 di sisi gateway pelanggan (on-premise) yang diizinkan untuk berkomunikasi melalui terowongan VPN.

Default 0.0.0.0/0

CIDR Jaringan IPv4 Jarak Jauh

(Hanya koneksi IPv4 VPN) Rentang IPv4 CIDR di AWS samping yang diizinkan untuk berkomunikasi melalui terowongan VPN.

Default 0.0.0.0/0

CIDR Jaringan IPv6 Lokal

(Hanya koneksi VPN IPv6) Rentang CIDR IPv6 di sisi gateway pelanggan (on-premise) yang diizinkan untuk berkomunikasi melalui terowongan VPN.

Default: ::/0

CIDR Jaringan IPv6 Jarak Jauh

(Hanya koneksi IPv6 VPN) Rentang IPv6 CIDR di AWS samping yang diizinkan untuk berkomunikasi melalui terowongan VPN.

Default: ::/0

Nomor grup Diffie-Hellman (DH) fase 1

Nomor grup DH yang diizinkan untuk terowongan VPN fase 1 dari negosiasi IKE. Anda dapat menentukan satu atau beberapa nilai default.

Default: 2, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24

Nomor grup Diffie-Hellman (DH) fase 2

Nomor grup DH yang diizinkan untuk terowongan VPN fase 2 dari negosiasi IKE. Anda dapat menentukan satu atau beberapa nilai default.

Default: 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24

Algoritme enkripsi fase 1

Algoritme enkripsi yang diizinkan untuk terowongan VPN fase 1 dari negosiasi IKE. Anda dapat menentukan satu atau beberapa nilai default.

Default: AES128, AES256, AES128-GCM-16, AES256-GCM-16

Algoritme enkripsi fase 2

Algoritme enkripsi yang diizinkan untuk terowongan VPN fase 2 dari negosiasi IKE. Anda dapat menentukan satu atau beberapa nilai default.

Default: AES128, AES256, AES128-GCM-16, AES256-GCM-16

Algoritme integritas fase 1

Algoritme integritas yang diizinkan untuk terowongan VPN fase 1 dari negosiasi IKE. Anda dapat menentukan satu atau beberapa nilai default.

Standar: SHA1, SHA2-256, SHA2-384, SHA2-512

Algoritme integritas fase 2

Algoritme integritas yang diizinkan untuk terowongan VPN fase 2 dari negosiasi IKE. Anda dapat menentukan satu atau beberapa nilai default.

Standar: SHA1, SHA2-256, SHA2-384, SHA2-512

Masa hidup fase 1

Note

AWS memulai tombol ulang dengan nilai waktu yang ditetapkan dalam bidang seumur hidup Fase 1 dan Fase 2 seumur hidup. Jika masa hidup berbeda dari nilai handshake yang dinegosiasikan, hal ini dapat mengganggu konektivitas terowongan.

Masa hidup dalam hitungan detik untuk fase 1 dari negosiasi IKE. Anda dapat menentukan angka antara 900 hingga 28.800.

Default: 28.800 (8 jam)

Masa hidup fase 2

Note

AWS memulai tombol ulang dengan nilai waktu yang ditetapkan dalam bidang seumur hidup Fase 1 dan Fase 2 seumur hidup. Jika masa hidup berbeda dari nilai handshake yang dinegosiasikan, hal ini dapat mengganggu konektivitas terowongan.

Masa hidup dalam hitungan detik untuk fase 2 dari negosiasi IKE. Anda dapat menentukan angka antara 900 hingga 3.600. Angka yang Anda tentukan harus kurang dari jumlah detik untuk masa hidup fase 1.

Default: 3.600 (1 jam)

Kunci pra-berbagi (PSK)

Kunci pra-bersama (PSK) untuk membangun asosiasi keamanan pertukaran kunci internet awal (IKE) antara gateway target dan gateway pelanggan.

Panjang karakter PSK harus antara 8 hingga 64 dan tidak boleh diawali dengan nol (0). Karakter yang diizinkan adalah karakter alfanumerik, titik (.), dan garis bawah (_).

Default: String alfanumerik 32-karakter.

Masukkan ulang data fuzz

Persentase jendela memasukkan ulang data (ditentukan oleh waktu margin memasukkan ulang data) pada saat waktu memasukkan ulang data dipilih secara acak.

Anda dapat menentukan nilai persentase antara 0 hingga 100.

Default: 100

Waktu margin memasukkan ulang data

Waktu margin dalam hitungan detik sebelum masa pakai fase 1 dan fase 2 berakhir, di mana AWS sisi koneksi VPN melakukan rekey IKE.

Anda dapat menentukan angka antara 60 dan setengah dari nilai masa pakai fase 2.

Waktu yang tepat saat memasukkan ulang data dipilih secara acak berdasarkan nilai untuk memasukkan ulang data fuzz.

Default: 270 (4,5 menit)

Paket ukuran jendela replay

Jumlah paket di jendela replay IKE.

Anda dapat menentukan nilai antara 64 hingga 2048.

Default: 1024

Tindakan awal

Tindakan yang dilakukan saat membuat terowongan untuk koneksi VPN. Anda dapat menentukan sebagai berikut:

- **Start:** AWS memulai negosiasi IKE untuk membawa terowongan ke atas. Hanya didukung jika gateway pelanggan Anda dikonfigurasi menggunakan alamat IP.
- **Add:** Perangkat gateway pelanggan Anda harus memulai negosiasi IKE untuk memunculkan terowongan.

Untuk informasi selengkapnya, lihat [Opsi inisiasi terowongan Site-to-Site VPN](#).

Default: Add

Kontrol siklus hidup titik akhir terowongan

Kontrol siklus hidup titik akhir terowongan memberikan kontrol atas jadwal penggantian titik akhir.

Untuk informasi selengkapnya, lihat [Kontrol siklus hidup titik akhir terowongan](#).

Default: Off

Anda dapat menentukan opsi terowongan ketika Anda membuat koneksi Site-to-Site VPN, atau Anda dapat mengubah opsi terowongan untuk koneksi VPN yang ada. Untuk informasi selengkapnya, lihat topik berikut.

- [Langkah 5: Buat koneksi VPN](#)
- [Mengubah opsi terowongan Site-to-Site VPN](#)

Opsi otentikasi terowongan situs-ke-situs VPN

Anda dapat menggunakan kunci yang telah dibagikan sebelumnya, atau sertifikat untuk mengotentikasi titik akhir terowongan Site-to-Site VPN Anda.

Kunci pra-berbagi

Kunci pra-berbagi adalah opsi autentikasi default.

Kunci yang telah dibagikan sebelumnya adalah opsi VPN terowongan Site-to-Site yang dapat Anda tentukan saat membuat terowongan Site-to-Site. VPN

Kunci pra-berbagi adalah string yang Anda masukkan ketika mengonfigurasi perangkat gateway pelanggan. Jika Anda tidak menentukan string, kami secara otomatis membuatnya untuk Anda. Untuk informasi selengkapnya, lihat [Perangkat gateway pelanggan Anda](#).

Sertifikat pribadi dari AWS Private Certificate Authority

Jika Anda tidak ingin menggunakan kunci yang telah dibagikan sebelumnya, Anda dapat menggunakan sertifikat pribadi dari AWS Private Certificate Authority untuk mengautentikasi Anda. VPN

Anda harus membuat sertifikat pribadi dari CA bawahan menggunakan AWS Private Certificate Authority (AWS Private CA). Untuk menandatangani CA ACM bawahan, Anda dapat menggunakan ACM Root CA atau CA eksternal. Untuk informasi selengkapnya tentang cara membuat sertifikat privat, lihat [Membuat dan Mengelola CA Privat](#) di Panduan Pengguna AWS Private Certificate Authority .

Anda harus membuat peran terkait layanan untuk menghasilkan dan menggunakan sertifikat untuk AWS sisi titik akhir terowongan Site-to-SiteVPN. Untuk informasi selengkapnya, lihat [the section called “Peran terkait layanan”](#).

Setelah membuat sertifikat privat, Anda akan menentukan sertifikat ketika membuat gateway pelanggan, dan kemudian menerapkannya ke perangkat gateway pelanggan Anda.

Jika Anda tidak menentukan alamat IP perangkat gateway pelanggan Anda, kami tidak akan memeriksa alamat IP. Operasi ini memungkinkan Anda untuk memindahkan perangkat gateway pelanggan ke alamat IP yang berbeda tanpa harus mengkonfigurasi ulang VPN koneksi.

Site-to-site VPN melakukan verifikasi rantai sertifikat pada sertifikat gateway pelanggan saat Anda membuat sertifikat. VPN Selain CA dasar dan pemeriksaan validitas, Site-to-Site VPN memeriksa apakah ekstensi X.509 ada, termasuk Authority Key Identifier, Subject Key Identifier, dan Basic Constraints.

Opsi inisiasi terowongan Site-to-Site VPN

Secara default, perangkat gateway pelanggan Anda harus memunculkan terowongan untuk koneksi Site-to-Site VPN Anda dengan menghasilkan lalu lintas dan memulai proses negosiasi Pertukaran Kunci Internet (IKE). Anda dapat mengonfigurasi terowongan VPN Anda untuk menentukan yang AWS harus memulai atau memulai kembali proses negosiasi IKE sebagai gantinya.

Opsi inisiasi IKE terowongan VPN

Opsi inisiasi IKE berikut tersedia. Anda dapat menerapkan salah satu atau kedua opsi, untuk salah satu atau kedua terowongan dalam koneksi VPN Site-to-Site Anda. Lihat [Opsi terowongan VPN](#) untuk detail selengkapnya tentang pengaturan opsi terowongan ini dan lainnya.

- Tindakan awal: Tindakan yang harus diambil saat membuat terowongan VPN untuk koneksi VPN baru atau yang diubah. Secara default, perangkat gateway pelanggan Anda memulai proses negosiasi IKE untuk membuka terowongan. Anda dapat menentukan yang AWS harus memulai proses negosiasi IKE sebagai gantinya.
- Tindakan batas waktu DPD: Tindakan yang harus diambil setelah batas waktu dead peer detection (DPD) terjadi. Secara default, sesi IKE dihentikan, terowongan turun, dan rute dihapus. Anda dapat menentukan yang AWS harus memulai ulang sesi IKE ketika batas waktu DPD terjadi, atau Anda dapat menentukan yang tidak AWS boleh mengambil tindakan ketika batas waktu DPD terjadi.

Aturan dan batasan

Aturan dan batasan berikut berlaku:

- Untuk memulai negosiasi IKE, AWS memerlukan alamat IP publik perangkat gateway pelanggan Anda. Jika Anda mengonfigurasi otentikasi berbasis sertifikat untuk koneksi VPN Anda dan Anda tidak menentukan alamat IP saat membuat sumber daya gateway pelanggan AWS, Anda harus membuat gateway pelanggan baru dan menentukan alamat IP. Kemudian, ubah koneksi VPN dan tentukan gateway pelanggan baru. Untuk informasi selengkapnya, lihat [Ubah gateway pelanggan untuk koneksi VPN Site-to-Site](#).
- Inisiasi IKE (aksi startup) dari AWS sisi koneksi VPN hanya didukung untuk IKEv2.
- Jika menggunakan inisiasi IKE dari AWS sisi koneksi VPN, itu tidak termasuk pengaturan batas waktu. Ini akan terus mencoba untuk membangun koneksi sampai satu dibuat. Selain itu, AWS sisi koneksi VPN akan memulai kembali negosiasi IKE ketika menerima pesan hapus SA dari gateway pelanggan Anda.
- Jika perangkat gateway pelanggan Anda berada di belakang firewall atau perangkat lain yang menggunakan Network Address Translation (NAT), perangkat tersebut harus memiliki identitas (IDr) yang dikonfigurasi. Untuk informasi lebih lanjut tentang IDr, lihat [RFC 7296](#).

Jika Anda tidak mengonfigurasi inisiasi IKE dari AWS samping untuk terowongan VPN Anda dan koneksi VPN mengalami periode waktu idle (biasanya 10 detik, tergantung pada konfigurasi Anda), terowongan mungkin akan turun. Untuk mencegah hal ini, Anda dapat menggunakan alat pemantauan jaringan untuk menghasilkan keepalive pings.

Bekerja dengan opsi inisiasi terowongan VPN

Untuk informasi lebih lanjut tentang penggunaan opsi inisiasi terowongan VPN, lihat topik berikut:

- Untuk membuat koneksi VPN baru dan menentukan opsi inisiasi terowongan VPN: [Langkah 5: Buat koneksi VPN](#)
- Untuk mengubah opsi inisiasi terowongan VPN untuk koneksi VPN yang ada: [Mengubah opsi terowongan Site-to-Site VPN](#)

Penggantian titik akhir terowongan Site-to-Site VPN

Koneksi Site-to-Site VPN Anda terdiri dari dua terowongan VPN untuk redundansi. Terkadang, salah satu atau kedua titik akhir terowongan VPN diganti saat AWS melakukan pembaruan terowongan, atau saat Anda memodifikasi koneksi VPN Anda. Selama penggantian titik akhir terowongan, konektivitas melalui terowongan mungkin terganggu saat titik akhir terowongan baru disediakan.

Topik

- [Penggantian titik akhir yang diprakarsai pelanggan](#)
- [AWS mengelola penggantian endpoint](#)
- [Kontrol siklus hidup titik akhir terowongan](#)

Penggantian titik akhir yang diprakarsai pelanggan

Ketika Anda mengubah komponen-komponen koneksi VPN Anda berikut ini, salah satu atau kedua titik akhir terowongan Anda diganti.

Modifikasi	Tindakan API	Dampak terowongan
Ubah gateway target untuk koneksi VPN	ModifyVpnConnection	Kedua terowongan tidak tersedia selagi titik akhir terowongan baru disediakan.
Ubah gateway pelanggan untuk koneksi VPN	ModifyVpnConnection	Kedua terowongan tidak tersedia selagi titik akhir terowongan baru disediakan.
Ubah opsi koneksi VPN	ModifyVpnConnectionOptions	Kedua terowongan tidak tersedia selagi titik akhir terowongan baru disediakan.

Modifikasi	Tindakan API	Dampak terowongan
Ubah opsi terowongan VPN	ModifyVpnTunnelOptions	Terowongan yang dimodifikasi tidak tersedia selama pembaruan.

AWS mengelola penggantian endpoint

AWS Site-to-Site VPN adalah layanan terkelola, dan secara berkala menerapkan pembaruan ke titik akhir terowongan VPN Anda. Pembaruan ini dilakukan karena beberapa alasan, seperti:

- Untuk menerapkan peningkatan umum, seperti tambalan, peningkatan ketahanan, dan peningkatan lainnya
- Untuk pensiunkan (retire) perangkat keras yang utama
- Saat pemantauan otomatis menentukan bahwa titik akhir terowongan VPN tidak sehat

AWS menerapkan pembaruan titik akhir terowongan ke satu terowongan koneksi VPN Anda sekaligus. Selama pembaruan titik akhir terowongan, koneksi VPN Anda mungkin mengalami kehilangan redundansi singkat. Oleh karena itu, penting untuk mengonfigurasi kedua terowongan di koneksi VPN Anda agar tingkat ketersediaannya tinggi.

Kontrol siklus hidup titik akhir terowongan

Kontrol siklus hidup titik akhir terowongan memberikan kontrol atas jadwal penggantian titik akhir, dan dapat membantu meminimalkan gangguan konektivitas selama penggantian titik akhir terowongan yang dikelola. AWS Dengan fitur ini, Anda dapat memilih untuk menerima pembaruan AWS terkelola ke titik akhir terowongan pada waktu yang paling sesuai untuk bisnis Anda. Gunakan fitur ini jika Anda memiliki kebutuhan bisnis jangka pendek atau hanya dapat mendukung satu terowongan per koneksi VPN.

Note

Dalam keadaan yang jarang terjadi, AWS mungkin segera menerapkan pembaruan penting ke titik akhir terowongan, bahkan jika fitur kontrol siklus hidup titik akhir terowongan diaktifkan.

Topik

- [Cara kerja kontrol siklus hidup titik akhir terowongan](#)
- [Aktifkan kontrol siklus hidup titik akhir terowongan](#)
- [Verifikasi apakah kontrol siklus hidup titik akhir terowongan diaktifkan](#)
- [Periksa pembaruan yang tersedia](#)
- [Terima pembaruan pemeliharaan](#)
- [Matikan kontrol siklus hidup titik akhir terowongan](#)

Cara kerja kontrol siklus hidup titik akhir terowongan

Aktifkan fitur kontrol siklus hidup titik akhir terowongan untuk setiap terowongan dalam koneksi VPN. Ini dapat diaktifkan pada saat pembuatan VPN atau dengan memodifikasi opsi terowongan untuk koneksi VPN yang ada.

Setelah kontrol siklus hidup titik akhir terowongan diaktifkan, Anda akan mendapatkan visibilitas tambahan ke acara pemeliharaan terowongan mendatang dengan dua cara:

- Anda akan menerima AWS Health pemberitahuan untuk penggantian titik akhir terowongan yang akan datang.
- Status pemeliharaan tertunda, bersama dengan pemeliharaan auto diterapkan setelah dan pemeliharaan terakhir diterapkan stempel waktu, dapat dilihat di AWS Management Console atau dengan menggunakan perintah [get-vpn-tunnel-replacement AWS CLI -status](#).

Ketika pemeliharaan titik akhir terowongan tersedia, Anda akan memiliki kesempatan untuk menerima pembaruan pada waktu yang nyaman bagi Anda, sebelum Pemeliharaan yang diberikan otomatis diterapkan setelah stempel waktu.

Jika Anda tidak menerapkan pembaruan sebelum Pemeliharaan otomatis diterapkan setelah tanggal, AWS akan secara otomatis melakukan penggantian titik akhir terowongan segera setelahnya, sebagai bagian dari siklus pembaruan pemeliharaan rutin.

Aktifkan kontrol siklus hidup titik akhir terowongan

Anda dapat mengaktifkan fitur ini menggunakan AWS Management Console atau AWS CLI.

Note

Secara default saat Anda mengaktifkan fitur untuk koneksi VPN yang ada, penggantian titik akhir terowongan akan dimulai pada saat yang bersamaan. Jika Anda ingin mengaktifkan fitur, tetapi tidak segera memulai penggantian titik akhir terowongan, Anda dapat menggunakan opsi penggantian terowongan lewati.

Existing VPN connection

Langkah-langkah berikut menunjukkan cara mengaktifkan kontrol siklus hidup titik akhir terowongan pada koneksi VPN yang ada.

Untuk mengaktifkan kontrol siklus hidup titik akhir terowongan menggunakan AWS Management Console

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi sisi kiri, pilih Koneksi VPN Site-to-Site.
3. Pilih koneksi yang sesuai di bawah koneksi VPN.
4. Pilih Tindakan, lalu Ubah opsi terowongan VPN.
5. Pilih terowongan tertentu yang ingin Anda modifikasi dengan memilih terowongan VPN yang sesuai di luar alamat IP.
6. Di bawah Kontrol Siklus Hidup Titik Akhir Tunnel, pilih kotak centang Aktifkan.
7. (Opsional) Pilih Lewati penggantian terowongan.
8. Pilih Simpan perubahan.

Untuk mengaktifkan kontrol siklus hidup titik akhir terowongan menggunakan AWS CLI

Gunakan [modify-vpn-tunnel-options](#) perintah untuk mengaktifkan kontrol siklus hidup titik akhir terowongan.

New VPN connection

Langkah-langkah berikut menunjukkan cara mengaktifkan kontrol siklus hidup titik akhir terowongan selama pembuatan koneksi VPN baru.

Untuk mengaktifkan kontrol siklus hidup titik akhir terowongan selama pembuatan koneksi VPN baru menggunakan AWS Management Console

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Koneksi Site-to-Site VPN.
3. Pilih Buat koneksi VPN.
4. Di bagian untuk opsi Tunnel 1 dan opsi Tunnel 2, di bawah Kontrol Siklus Hidup Titik Akhir Tunnel, pilih Aktifkan.
5. Pilih Buat Koneksi VPN.

Untuk mengaktifkan kontrol siklus hidup titik akhir terowongan selama pembuatan koneksi VPN baru menggunakan AWS CLI

Gunakan [create-vpn-connection](#) perintah untuk mengaktifkan kontrol siklus hidup titik akhir terowongan.

Verifikasi apakah kontrol siklus hidup titik akhir terowongan diaktifkan

Anda dapat memverifikasi apakah kontrol siklus hidup titik akhir terowongan diaktifkan pada terowongan VPN yang ada dengan menggunakan atau AWS Management Console CLI.

Untuk memverifikasi apakah kontrol siklus hidup titik akhir terowongan diaktifkan menggunakan AWS Management Console

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi sisi kiri, pilih Koneksi VPN Site-to-Site.
3. Pilih koneksi yang sesuai di bawah koneksi VPN.
4. Pilih tab Detail terowongan.
5. Dalam detail terowongan, cari Kontrol Siklus Hidup Titik Akhir Tunnel, yang akan melaporkan apakah fitur tersebut Diaktifkan atau Dinonaktifkan.

Untuk memverifikasi apakah kontrol siklus hidup titik akhir terowongan diaktifkan menggunakan AWS CLI

Gunakan [describe-vpn-connections](#) perintah untuk memverifikasi apakah kontrol siklus hidup titik akhir terowongan diaktifkan.

Periksa pembaruan yang tersedia

Setelah mengaktifkan fitur kontrol siklus hidup titik akhir terowongan, Anda dapat melihat apakah pembaruan pemeliharaan tersedia untuk koneksi VPN Anda dengan menggunakan atau AWS Management Console CLI.

Untuk memeriksa pembaruan yang tersedia menggunakan AWS Management Console

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi sisi kiri, pilih Koneksi VPN Site-to-Site.
3. Pilih koneksi yang sesuai di bawah koneksi VPN.
4. Pilih tab Detail terowongan.
5. Periksa kolom Pemeliharaan tertunda. Status akan tersedia atau tidak ada.

Untuk memeriksa pembaruan yang tersedia menggunakan AWS CLI

Gunakan perintah [get-vpn-tunnel-replacement-status](#) untuk memeriksa pembaruan yang tersedia.

Terima pembaruan pemeliharaan

Ketika pembaruan pemeliharaan tersedia, Anda dapat menerimanya menggunakan AWS Management Console atau CLI.

Untuk menerima pembaruan pemeliharaan yang tersedia menggunakan AWS Management Console

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi sisi kiri, pilih Koneksi VPN Site-to-Site.
3. Pilih koneksi yang sesuai di bawah koneksi VPN.
4. Pilih Tindakan, lalu Ganti Terowongan VPN.
5. Pilih terowongan tertentu yang ingin Anda ganti dengan memilih terowongan VPN yang sesuai di luar alamat IP.
6. Pilih Ganti.

Untuk menerima pembaruan pemeliharaan yang tersedia menggunakan AWS CLI

Gunakan [replace-vpn-tunnel](#) perintah untuk menerima pembaruan pemeliharaan yang tersedia.

Matikan kontrol siklus hidup titik akhir terowongan

Jika Anda tidak lagi ingin menggunakan fitur kontrol siklus hidup titik akhir terowongan, Anda dapat mematikannya menggunakan atau. AWS Management Console AWS CLI Ketika Anda mematikan fitur ini, secara otomatis AWS akan menyebarkan pembaruan pemeliharaan secara berkala, dan pembaruan ini mungkin terjadi selama jam kerja Anda. Untuk menghindari dampak bisnis apa pun, kami sangat menyarankan Anda mengonfigurasi kedua terowongan di koneksi VPN Anda untuk ketersediaan tinggi.

Note

Meskipun ada pemeliharaan tertunda yang tersedia, Anda tidak dapat menentukan opsi penggantian terowongan lewati saat mematikan fitur. Anda selalu dapat mematikan fitur tanpa menggunakan opsi penggantian terowongan lewati, tetapi AWS akan secara otomatis menerapkan pembaruan pemeliharaan tertunda yang tersedia dengan segera memulai penggantian titik akhir terowongan.

Untuk mematikan kontrol siklus hidup titik akhir terowongan menggunakan AWS Management Console

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi sisi kiri, pilih Koneksi VPN Site-to-Site.
3. Pilih koneksi yang sesuai di bawah koneksi VPN.
4. Pilih Tindakan, lalu Ubah opsi terowongan VPN.
5. Pilih terowongan tertentu yang ingin Anda modifikasi dengan memilih terowongan VPN yang sesuai di luar alamat IP.
6. Untuk mematikan kontrol siklus hidup titik akhir terowongan, di bawah Kontrol Siklus Hidup Titik Akhir Tunnel, kosongkan kotak centang Aktifkan.
7. (Opsional) Pilih Lewati penggantian terowongan.
8. Pilih Simpan perubahan.

Untuk mematikan kontrol siklus hidup titik akhir terowongan menggunakan AWS CLI

Gunakan [modify-vpn-tunnel-options](#) perintah untuk mematikan kontrol siklus hidup titik akhir terowongan.

Opsi gateway pelanggan untuk koneksi Site-to-Site VPN

Tabel berikut menjelaskan informasi yang Anda perlukan untuk membuat sumber daya gateway pelanggan di AWS.

Item	Deskripsi
(Opsional) Tag nama.	Membuat tag dengan kunci 'Nama' dan nilai yang Anda tentukan.
Border Gateway Protocol (BGP) Autonomous System Number (ASN) (Perutean dinamis saja) dari gateway pelanggan.	<p>ASN di kisaran 1 - 4.294.967,295 didukung. Anda dapat menggunakan ASN publik yang sudah ada yang ditetapkan ke jaringan Anda, dengan pengecualian berikut ini:</p> <ul style="list-style-type: none"> • 7224 - Dicalangkan di semua Wilayah • 9059 - Dicalangkan di Wilayah eu-west-1 • 10124 - Dicalangkan di Wilayah ap-northeast-1 • 17943 - Dicalangkan di Wilayah ap-southeast-1 <p>Jika Anda tidak memiliki ASN publik, Anda dapat menggunakan ASN pribadi di kisaran 64.512 - 65.534 atau 4.200.000.000 - 4.294.967.294. ASN default adalah 65000. Lihat Opsi perutean VPN situs-ke-situs untuk detail lebih lanjut tentang perutean.</p>
(Opsional) Alamat IP antarmuka eksternal perangkat gateway pelanggan.	<p>Alamat IP harus statis.</p> <p>Jika perangkat gateway pelanggan Anda berada di belakang perangkat terjemahan alamat jaringan (NAT), gunakan alamat IP perangkat NAT Anda. Juga, pastikan bahwa paket UDP pada port 500 (dan port 4500, jika NAT-traversal sedang digunakan) diizinkan</p>

Item	Deskripsi
	<p>untuk melewati antara jaringan Anda dan titik akhir. AWS Site-to-Site VPN Lihat Aturan firewall untuk info lebih lanjut.</p> <p>Alamat IP tidak diperlukan saat Anda menggunakan sertifikat pribadi dari AWS Private Certificate Authority dan VPN publik.</p>

Item	Deskripsi
(Opsional) Sertifikat pribadi dari bawahan CA using AWS Certificate Manager (ACM).	<p>Jika Anda ingin menggunakan autentikasi berbasis sertifikat, maka sediakan sertifikat ARN dari sertifikat privat ACM yang akan digunakan pada perangkat gateway pelanggan Anda.</p> <p>Ketika Anda membuat gateway pelanggan, Anda dapat mengonfigurasi gateway pelanggan untuk menggunakan sertifikat privat AWS Private Certificate Authority untuk mengautentikasi Site-to-Site VPN.</p> <p>Ketika Anda memilih untuk menggunakan opsi ini, Anda membuat otoritas sertifikat pribadi (CA) yang sepenuhnya AWS dihosting untuk penggunaan internal oleh organisasi Anda. Baik sertifikat CA root dan sertifikat CA bawahan disimpan dan dikelola oleh AWS Private CA.</p> <p>Sebelum Anda membuat gateway pelanggan, Anda membuat sertifikat pribadi dari CA bawahan menggunakan AWS Private Certificate Authority, dan kemudian menentukan sertifikat ketika Anda mengkonfigurasi gateway pelanggan. Untuk informasi tentang pembuatan sertifikat privat, lihat Membuat dan mengelola CA privat dalam Panduan Pengguna AWS Private Certificate Authority.</p>
(Opsional) Perangkat.	Nama untuk perangkat gateway pelanggan yang terkait dengan gateway pelanggan ini.

Koneksi Site-to-Site VPN terakselerasi

Anda dapat mengaktifkan akselerasi secara opsional untuk koneksi Site-to-Site VPN Anda. Koneksi VPN Site-to-Site yang dipercepat (koneksi VPN yang dipercepat) AWS Global Accelerator digunakan untuk merutekan lalu lintas dari jaringan lokal Anda ke lokasi tepi AWS yang paling dekat dengan perangkat gateway pelanggan Anda. AWS Global Accelerator mengoptimalkan jalur jaringan, menggunakan jaringan AWS global bebas kemacetan untuk mengarahkan lalu lintas ke titik akhir yang memberikan kinerja aplikasi terbaik (untuk informasi lebih lanjut, lihat) [AWS Global Accelerator](#) Anda dapat menggunakan koneksi VPN terakselerasi untuk menghindari gangguan jaringan yang mungkin terjadi ketika lalu lintas dirutekan melalui internet publik.

Ketika Anda membuat koneksi VPN terakselerasi, kami membuat dan mengelola dua akselerator atas nama Anda, masing-masing satu untuk setiap terowongan VPN. Anda tidak dapat melihat atau mengelola akselerator ini sendiri dengan menggunakan AWS Global Accelerator konsol atau API.

Untuk informasi tentang AWS Wilayah yang mendukung koneksi VPN yang Dipercepat, lihat FAQ VPN [Site-to-Site yang AWS Dipercepat](#).

Mengaktifkan akselerasi

Secara default, ketika Anda membuat koneksi Site-to-Site VPN, akselerasi dinonaktifkan. Anda dapat mengaktifkan akselerasi secara opsional ketika Anda membuat lampiran Site-to-Site VPN baru di transit gateway. Untuk informasi dan langkah-langkah selengkapnya, lihat [Buat lampiran VPN gateway transit](#).

Koneksi VPN terakselerasi menggunakan kolam terpisah dari alamat IP untuk alamat IP titik akhir terowongan. Alamat IP untuk dua terowongan VPN dipilih dari dua [zona jaringan](#) terpisah.

Peraturan dan pembatasan

Untuk menggunakan koneksi VPN terakselerasi, aturan berikut berlaku:

- Akselerasi hanya didukung untuk koneksi Site-to-Site VPN yang dilampirkan ke transit gateway. Virtual private gateway tidak mendukung koneksi VPN terakselerasi.
- Koneksi VPN Site-to-Site yang Dipercepat tidak dapat digunakan dengan antarmuka virtual publik. AWS Direct Connect
- Anda tidak dapat mengaktifkan atau menonaktifkan akselerasi koneksi Site-to-Site VPN yang sudah ada. Sebaliknya, Anda dapat membuat koneksi Site-to-Site VPN baru dengan akselerasi

aktif atau nonaktif sesuai kebutuhan. Kemudian, konfigurasi perangkat gateway pelanggan Anda untuk menggunakan koneksi Site-to-Site VPN baru dan hapus koneksi Site-to-Site VPN yang lama.

- NAT-traversal (NAT-T) diperlukan untuk koneksi VPN yang terakselerasi dan diaktifkan secara default. Jika Anda mengunduh [file konfigurasi](#) dari konsol Amazon VPC, periksa pengaturan NAT-T dan sesuaikan jika perlu.
- Negosiasi IKE untuk terowongan VPN yang dipercepat harus dimulai dari perangkat gateway pelanggan. Dua opsi terowongan yang mempengaruhi perilaku ini adalah `Startup Action` dan `DPD Timeout Action`. Lihat [Opsi terowongan VPN](#) dan [Opsi inisiasi terowongan VPN](#) untuk informasi lebih lanjut.
- Koneksi VPN Site-to-Site yang menggunakan otentikasi berbasis sertifikat mungkin tidak kompatibel, karena dukungan terbatas untuk fragmentasi paket di Global AWS Global Accelerator Accelerator. Untuk informasi selengkapnya, lihat [Cara kerja AWS Global Accelerator](#). Jika Anda memerlukan koneksi VPN terakselerasi yang menggunakan autentikasi berbasis sertifikat, maka perangkat gateway pelanggan Anda harus mendukung fragmentasi IKE. Sebaliknya, jangan aktifkan VPN Anda untuk akselerasi.

Opsi perutean VPN situs-ke-situs

AWS merekomendasikan mengiklankan BGP rute khusus untuk memengaruhi keputusan perutean di gateway pribadi virtual. Periksa dokumentasi vendor Anda untuk perintah khusus untuk perangkat Anda.

Saat Anda membuat beberapa VPN koneksi, gateway pribadi virtual mengirimkan lalu lintas jaringan ke VPN koneksi yang sesuai menggunakan rute yang ditetapkan secara statis atau iklan BGP rute. Rute mana yang tergantung pada bagaimana VPN koneksi dikonfigurasi. Rute yang ditetapkan secara statis lebih disukai daripada rute BGP yang diiklankan dalam kasus di mana rute identik ada di gateway pribadi virtual. Jika Anda memilih opsi untuk menggunakan BGP iklan, maka Anda tidak dapat menentukan rute statis.

Untuk informasi selengkapnya tentang prioritas rute, lihat [Tabel rute dan prioritas VPN rute](#).

Saat Anda membuat VPN koneksi Site-to-Site, Anda harus melakukan hal berikut:

- Tentukan jenis perutean yang ingin Anda gunakan (statis atau dinamis)
- Memperbarui [tabel rute](#) untuk subnet Anda

Terdapat kuota pada jumlah rute yang bisa Anda tambahkan ke tabel rute. Untuk informasi selengkapnya, lihat bagian Tabel Rute di [VPCkuota Amazon](#) di Panduan VPC Pengguna Amazon.

Topik

- [Perutean statis dan dinamis](#)
- [Tabel rute dan prioritas VPN rute](#)
- [Perutean selama pembaruan titik akhir VPN terowongan](#)
- [Lalu lintas IPv4 dan IPv6](#)

Perutean statis dan dinamis

Jenis perutean yang Anda pilih dapat bergantung pada pembuatan dan model perangkat gateway pelanggan Anda. Jika perangkat gateway pelanggan Anda mendukung Border Gateway Protocol (BGP), tentukan perutean dinamis saat Anda mengonfigurasi koneksi Site-to-Site VPN Anda. Jika perangkat gateway pelanggan Anda tidak mendukung BGP, tentukan perutean statis.

Jika Anda menggunakan perangkat yang mendukung BGP iklan, Anda tidak menentukan rute statis ke VPN koneksi Site-to-Site karena perangkat menggunakan BGP untuk mengiklankan rute ke gateway pribadi virtual. Jika Anda menggunakan perangkat yang tidak mendukung BGP iklan, Anda harus memilih perutean statis dan memasukkan rute (awalan IP) untuk jaringan Anda yang harus dikomunikasikan ke gateway pribadi virtual.

Kami menyarankan Anda menggunakan perangkat BGP berkemampuan, jika tersedia, karena BGP protokol menawarkan pemeriksaan deteksi keaktifan yang kuat yang dapat membantu failover ke VPN terowongan kedua jika terowongan pertama turun. Perangkat yang tidak mendukung juga BGP dapat melakukan pemeriksaan kesehatan untuk membantu failover ke terowongan kedua bila diperlukan.

Anda harus mengonfigurasi perangkat gateway pelanggan untuk merutekan lalu lintas dari jaringan lokal ke koneksi VPN Site-to-Site. Konfigurasi bergantung pada pembuatan dan model perangkat Anda. Untuk informasi selengkapnya, lihat [Perangkat gateway pelanggan Anda](#).

Tabel rute dan prioritas VPN rute

[Tabel rute](#) menentukan ke mana lalu lintas jaringan dari Anda VPC diarahkan. Dalam tabel VPC rute Anda, Anda harus menambahkan rute untuk jaringan jarak jauh Anda dan menentukan gateway pribadi virtual sebagai target. Ini memungkinkan lalu lintas dari Anda VPC yang ditujukan untuk jaringan jarak jauh Anda untuk rute melalui gateway pribadi virtual dan melalui salah satu VPN

terowongan. Anda dapat mengaktifkan propagasi rute untuk tabel rute Anda untuk secara otomatis menyebarkan rute jaringan Anda ke meja untuk Anda.

Kami menggunakan rute paling spesifik dalam tabel rute Anda yang cocok dengan lalu lintas untuk menentukan cara perutean lalu lintas (kecocokan dengan prefiks terpanjang). Jika tabel rute Anda memiliki tumpang tindih atau pencocokan rute, aturan berikut berlaku:

- Jika rute yang disebarkan dari koneksi VPN Site-to-Site atau AWS Direct Connect koneksi tumpang tindih dengan rute lokal untuk Anda VPC, rute lokal paling disukai bahkan jika rute yang disebarkan lebih spesifik.
- Jika rute yang disebarkan dari koneksi VPN Site-to-Site atau AWS Direct Connect koneksi memiliki CIDR blok tujuan yang sama dengan rute statis lainnya yang ada (kecocokan awalan terpanjang tidak dapat diterapkan), kami memprioritaskan rute statis yang targetnya adalah gateway internet, gateway pribadi virtual, antarmuka jaringan, ID instance, koneksi VPC peering, gateway, gateway transit, atau titik NAT akhir gateway. VPC

Sebagai contoh, tabel rute berikut memiliki rute statis ke gateway internet, dan rute disebarkan ke gateway privat virtual. Kedua rute memiliki tujuan `172.31.0.0/24`. Dalam hal ini, semua lalu lintas yang ditujukan untuk `172.31.0.0/24` diarahkan ke gateway internet - itu adalah rute statis dan oleh karenanya mengambil prioritas atas rute yang disebarkan.

Tujuan	Target
10.0.0.0/16	Lokal
172.31.0.0/24	vgw-11223344556677889 (disebarkan)
172.31.0.0/24	igw-12345678901234567 (statis)

Hanya awalan IP yang diketahui oleh gateway pribadi virtual, baik melalui BGP iklan atau entri rute statis, yang dapat menerima lalu lintas dari Anda. VPC Gateway pribadi virtual tidak merutekan lalu lintas lain yang ditujukan di luar BGP iklan yang diterima, entri rute statis, atau terlampir. VPC CIDR Gateway pribadi virtual tidak mendukung IPv6 lalu lintas.

Ketika gateway privat virtual menerima informasi perutean, itu menggunakan pilihan jalur untuk menentukan bagaimana merutekan lalu lintas. Pencocokan awalan terpanjang berlaku, jika semua titik akhir sehat. Kesehatan titik akhir terowongan lebih diutamakan daripada atribut routing lainnya.

Prioritas ini berlaku untuk VPNs gateway pribadi virtual dan Gateway Transit. Jika prefiks yang sama, maka gateway privat virtual memprioritaskan rute sebagai berikut, dari yang paling dipilih hingga yang tidak dipilih:

- BGPrute yang disebarkan dari koneksi AWS Direct Connect
- Menambahkan rute statis secara manual untuk koneksi Site-to-Site VPN
- BGPrute yang disebarkan dari koneksi VPN Site-to-Site
- Untuk awalan pencocokan di mana setiap VPN koneksi Site-to-Site menggunakan BGP, AS PATH dibandingkan dan awalan dengan AS terpendek lebih disukai. PATH

Note

AWS sangat merekomendasikan menggunakan perangkat gateway pelanggan yang mendukung perutean asimetris.

Untuk perangkat gateway pelanggan yang mendukung perutean asimetris, kami tidak menyarankan menggunakan AS PATH prepending, untuk memastikan bahwa kedua terowongan memiliki AS yang sama. PATH Ini membantu memastikan bahwa nilai multi-exit discriminator (MED) yang kami tetapkan pada terowongan selama [pembaruan titik akhir VPN terowongan](#) digunakan untuk menentukan prioritas terowongan.

Untuk perangkat gateway pelanggan yang tidak mendukung perutean asimetris, Anda dapat menggunakan AS PATH prepending dan Local Preference untuk memilih satu terowongan daripada yang lain. Namun, ketika jalur keluar berubah, ini dapat menyebabkan lalu lintas turun.

- Ketika AS PATHs memiliki panjang yang sama dan jika AS pertama di AS_SEQUENCE sama di beberapa jalur, multi-exit discriminators (MEDs) dibandingkan. Jalur dengan MED nilai terendah lebih disukai.

Prioritas rute terpengaruh selama [pembaruan titik akhir VPN terowongan](#).

Pada VPN koneksi Site-to-Site, AWS pilih salah satu dari dua terowongan redundan sebagai jalur keluar utama. Pilihan ini dapat berubah sewaktu-waktu, dan kami sangat menyarankan Anda mengonfigurasi kedua terowongan untuk ketersediaan tinggi, dan memungkinkan perutean asimetris. Kesehatan titik akhir terowongan lebih diutamakan daripada atribut routing lainnya. Prioritas ini berlaku untuk VPNs gateway pribadi virtual dan Gateway Transit.

Untuk gateway pribadi virtual, satu terowongan di semua VPN koneksi Site-to-Site pada gateway akan dipilih. Untuk menggunakan lebih dari satu terowongan, sebaiknya jelajahi Equal Cost Multipath (ECMP), yang didukung untuk VPN koneksi Site-to-Site pada gateway transit. Untuk informasi selengkapnya, lihat [Gateway transit di Amazon VPC Transit Gateways](#). ECMP tidak didukung untuk VPN koneksi Site-to-Site pada gateway pribadi virtual.

Untuk VPN koneksi Site-to-site yang digunakan BGP, terowongan utama dapat diidentifikasi dengan nilai multi-exit discriminator (MED). Kami merekomendasikan untuk mengiklankan BGP rute yang lebih spesifik untuk memengaruhi keputusan perutean.

Untuk VPN koneksi Site-to-Site yang menggunakan perutean statis, terowongan utama dapat diidentifikasi oleh statistik lalu lintas atau metrik.

Perutean selama pembaruan titik akhir VPN terowongan

VPN Koneksi Site-to-Site terdiri dari dua VPN terowongan antara perangkat gateway pelanggan dan gateway pribadi virtual atau gateway transit. Kami merekomendasikan bahwa Anda mengonfigurasi kedua terowongan untuk redundansi. Dari waktu ke waktu, AWS juga melakukan pemeliharaan rutin pada VPN koneksi Anda, yang mungkin secara singkat menonaktifkan salah satu dari dua terowongan VPN koneksi Anda. Untuk informasi selengkapnya, lihat [Notifikasi penggantian titik akhir terowongan](#).

Saat kami melakukan pembaruan pada satu VPN terowongan, kami menetapkan nilai outbound multi-exit discriminator (MED) yang lebih rendah di terowongan lainnya. Jika Anda telah mengonfigurasi perangkat gateway pelanggan untuk menggunakan kedua terowongan, VPN koneksi Anda menggunakan terowongan (atas) lainnya selama proses pembaruan titik akhir terowongan.

Note

Untuk memastikan bahwa terowongan atas dengan yang lebih rendah MED lebih disukai, pastikan perangkat gateway pelanggan Anda menggunakan nilai Berat dan Preferensi Lokal yang sama untuk kedua terowongan (Berat dan Preferensi Lokal memiliki prioritas lebih tinggi daripada MED).

Lalu lintas IPv4 dan IPv6

Koneksi Site-to-Site VPN Anda pada gateway transit dapat mendukung lalu lintas IPv4 atau lalu lintas IPv6 di dalam terowongan VPN. Secara default, koneksi Site-to-Site VPN mendukung lalu lintas

IPv4 di dalam terowongan VPN. Anda dapat mengonfigurasi koneksi Site-to-Site VPN baru untuk mendukung lalu lintas IPv6 di dalam terowongan VPN. Kemudian, jika VPC dan jaringan on-premise dikonfigurasi untuk membuat alamat IPv6, Anda dapat mengirim lalu lintas IPv6 melalui koneksi VPN.

Jika Anda mengaktifkan IPv6 untuk terowongan VPN untuk koneksi Site-to-Site VPN Anda, setiap tunnel memiliki dua blok CIDR. Salah satunya adalah blok CIDR IPv4 berukuran /30, dan yang lainnya adalah blok CIDR IPv6 berukuran /126.

Aturan berikut berlaku:

- Alamat IPv6 hanya didukung untuk alamat IP di dalam terowongan VPN. Alamat IP terowongan luar untuk AWS titik akhir adalah alamat IPv4, dan alamat IP publik gateway pelanggan Anda harus berupa alamat IPv4.
- Koneksi Site-to-Site VPN pada gateway privat virtual tidak mendukung IPv6.
- Anda tidak dapat mengaktifkan dukungan IPv6 untuk koneksi Site-to-Site VPN yang tersedia.
- Koneksi Site-to-Site VPN tidak dapat mendukung lalu lintas IPv4 dan IPv6.

Untuk informasi lebih lanjut tentang membuat koneksi VPN lihat [Langkah 5: Buat koneksi VPN](#).

Memulai dengan AWS Site-to-Site VPN

Gunakan prosedur berikut untuk mengatur AWS Site-to-Site VPN koneksi. Selama pembuatan, Anda akan menentukan gateway pribadi virtual, gateway transit, atau “Tidak terkait” sebagai jenis gateway target. Jika Anda menentukan “Tidak terkait”, Anda dapat memilih jenis gateway target di lain waktu, atau Anda dapat menggunakannya sebagai lampiran VPN untuk AWS Cloud WAN. Tutorial ini membantu Anda membuat koneksi VPN menggunakan gateway pribadi virtual. Ini mengasumsikan bahwa Anda memiliki VPC yang ada dengan satu atau lebih subnet.

Untuk mengatur koneksi VPN menggunakan gateway pribadi virtual, selesaikan langkah-langkah berikut:

Tugas

- [Prasyarat](#)
- [Langkah 1: Buat gateway pelanggan](#)
- [Langkah 2: Buat gateway target](#)
- [Langkah 3: Konfigurasi perutean](#)
- [Langkah 4: Perbarui grup keamanan Anda](#)
- [Langkah 5: Buat koneksi VPN](#)
- [Langkah 6: Unduh file konfigurasi](#)
- [Langkah 7: Konfigurasi perangkat gateway pelanggan](#)

Tugas terkait

- Untuk membuat koneksi VPN untuk AWS Cloud WAN, lihat [Buat lampiran VPN untuk AWS Cloud WAN](#).
- Untuk membuat koneksi VPN di gateway transit, lihat [Buat lampiran VPN gateway transit](#).

Prasyarat

Anda memerlukan informasi berikut untuk mengatur dan mengkonfigurasi komponen koneksi VPN.

Item	Informasi
Perangkat gateway pelanggan	Perangkat fisik atau perangkat lunak koneksi VPN di sisi Anda. Anda memerlukan vendor (misalnya, Cisco), platform (misalnya, Router Seri ISR), dan versi perangkat lunak (misalnya, IOS 12.4).
Gateway pelanggan	<p>Untuk membuat sumber daya gateway pelanggan di AWS, Anda memerlukan informasi berikut:</p> <ul style="list-style-type: none"> • Alamat IP yang dapat dirutekan internet untuk antarmuka eksternal perangkat • Jenis perutean: statis atau dinamis • Untuk perutean dinamis, Border Gateway Protocol (BGP) Autonomous System Number (ASN) • (Opsional) Sertifikat pribadi dari AWS Private Certificate Authority untuk mengautentikasi VPN Anda <p>Untuk informasi selengkapnya, lihat Opsional gateway pelanggan.</p>
(Opsional) ASN untuk AWS sisi sisi BGP	Anda menentukannya ketika membuat gateway privat virtual atau transit gateway. Jika Anda tidak menentukan nilai, ASN default diterapkan. Untuk informasi selengkapnya, lihat Gateway privat virtual .
Koneksi VPN	<p>Untuk membuat koneksi VPN, Anda memerlukan informasi berikut:</p> <ul style="list-style-type: none"> • Untuk perutean statis, prefiks IP untuk jaringan privat Anda.

Item	Informasi
	<ul style="list-style-type: none">• (Opsional) Opsi terowongan untuk setiap terowongan VPN. Untuk informasi selengkapnya, lihat Opsi terowongan untuk koneksi Site-to-Site VPN Anda.

Langkah 1: Buat gateway pelanggan

Gateway pelanggan memberikan informasi AWS tentang perangkat gateway pelanggan atau aplikasi perangkat lunak Anda. Untuk informasi selengkapnya, lihat [Gateway pelanggan](#).

Jika Anda berencana untuk menggunakan sertifikat pribadi untuk mengautentikasi VPN Anda, buat sertifikat pribadi dari CA bawahan menggunakan AWS Private Certificate Authority Untuk informasi tentang pembuatan sertifikat privat, lihat [Pembuatan dan Pengelolaan CA privat](#) dalam Panduan Pengguna AWS Private Certificate Authority .

Note

Anda harus menentukan alamat IP, atau Nama Sumber Daya Amazon dari sertifikat privat.

Untuk membuat gateway pelanggan menggunakan konsol tersebut

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih gateway Pelanggan.
3. Pilih Buat gateway pelanggan.
4. (Opsional) Untuk tag Nama, masukkan nama untuk gateway pelanggan Anda. Melakukan hal itu akan menciptakan tag dengan kunci Name dan nilai yang Anda tentukan.
5. Untuk BGP ASN, masukkan Border Gateway Protocol (BGP) Autonomous System Number (ASN) untuk gateway pelanggan Anda.
6. (Opsional) Untuk alamat IP, masukkan alamat IP statis yang dapat dirutekan internet untuk perangkat gateway pelanggan Anda. Jika perangkat gateway pelanggan Anda berada di belakang perangkat NAT yang diaktifkan untuk NAT-T, gunakan alamat IP publik perangkat NAT.
7. (Opsional) Jika Anda ingin menggunakan sertifikat privat, pada ARN Sertifikat, pilih nama sumber daya Amazon sertifikat privat.

8. (Opsional) Untuk Perangkat, masukkan nama untuk perangkat gateway pelanggan yang terkait dengan gateway pelanggan ini.
9. Pilih Buat gateway pelanggan.

Untuk membuat gateway pelanggan menggunakan baris perintah atau API

- [CreateCustomerGateway](#) (Amazon EC2 Query API)
- [create-customer-gateway](#) (AWS CLI)
- [New-EC2CustomerGateway](#) (AWS Tools for Windows PowerShell)

Langkah 2: Buat gateway target

Untuk membuat koneksi VPN antara VPC dan jaringan lokal, Anda harus membuat gateway target di AWS sisi koneksi. Target gateway dapat berupa gateway privat virtual atau transit gateway.

Buat gateway privat virtual

Saat membuat gateway pribadi virtual, Anda dapat menentukan Nomor Sistem Otonom (ASN) pribadi khusus untuk sisi Amazon dari gateway, atau menggunakan ASN default Amazon. ASN ini harus berbeda dari ASN yang Anda tentukan untuk gateway pelanggan.

Setelah Anda membuat gateway privat virtual, Anda harus melampirkannya ke VPC Anda.

Untuk membuat gateway privat virtual dan melampirkannya ke VPC Anda

1. Di panel navigasi, pilih Gateway pribadi virtual.
2. Pilih Buat gateway pribadi virtual.
3. (Opsional) Untuk tag Nama, masukkan nama untuk gateway pribadi virtual Anda. Melakukan hal itu akan menciptakan tag dengan kunci Name dan nilai yang Anda tentukan.
4. Untuk Autonomous System Number (ASN), pertahankan pilihan default, Amazon default ASN, untuk menggunakan Amazon ASN default. Jika tidak, mohon untuk memilih ASN kustom dan silahkan memasukkan sebuah nilai. Untuk ASN 16-bit, nilainya harus berada dalam rentang 64512 hingga 65534. Untuk ASN 32-bit, nilainya harus berada dalam rentang 4200000000 hingga 4294967294.
5. Pilih Buat gateway pribadi virtual.
6. Pilih gateway pribadi virtual yang Anda buat, lalu pilih Tindakan, Lampirkan ke VPC.

7. Untuk VPC yang Tersedia, pilih VPC Anda dan kemudian pilih Lampirkan ke VPC.

Untuk membuat gateway privat virtual menggunakan baris perintah atau API

- [CreateVpnGateway](#) (Amazon EC2 Query API)
- [create-vpn-gateway](#) (AWS CLI)
- [New-EC2VpnGateway](#) (AWS Tools for Windows PowerShell)

Untuk melampirkan gateway privat virtual ke VPC menggunakan baris perintah atau API

- [AttachVpnGateway](#) (Amazon EC2 Query API)
- [attach-vpn-gateway](#) (AWS CLI)
- [Add-EC2VpnGateway](#) (AWS Tools for Windows PowerShell)

Buat transit gateway

Untuk informasi selengkapnya tentang cara membuat transit gateway, lihat [Transit Gateway](#) dalam Transit Gateway Amazon VPC.

Langkah 3: Konfigurasi perutean

Untuk mengaktifkan instance di VPC Anda untuk mencapai gateway pelanggan Anda, Anda harus mengonfigurasi tabel rute Anda untuk menyertakan rute yang digunakan oleh koneksi VPN Anda dan mengarahkannya ke gateway pribadi virtual atau gateway transit Anda.

(Gateway privat virtual) Aktifkan propagasi rute di tabel rute Anda

Anda dapat mengaktifkan propagasi rute untuk tabel rute agar menyebarkan rute Site-to-Site VPN secara otomatis.

Untuk perutean statis, awalan IP statis yang Anda tentukan untuk konfigurasi VPN Anda disebarkan ke tabel rute saat status koneksi VPN. UP Demikian pula, untuk perutean dinamis, rute yang diiklankan BGP dari gateway pelanggan Anda disebarkan ke tabel rute saat status koneksi VPN. UP

Note

Jika koneksi Anda terganggu tetapi koneksi VPN tetap AKTIF, rute manapun yang disebarakan yang berada dalam tabel rute Anda secara otomatis tidak akan dihapus. Ingatlah hal ini, misalnya, jika Anda ingin lalu lintas dialihkan ke rute statis. Dalam hal ini, Anda mungkin harus menonaktifkan propagasi rute untuk menghapus rute yang disebarakan.

Untuk mengaktifkan propagasi rute menggunakan konsol tersebut

1. Di panel navigasi, pilih Tabel rute.
2. Pilih tabel rute yang terkait dengan subnet.
3. Pada tab Rute propagation, pilih Edit propagasi rute. Pilih gateway pribadi virtual yang Anda buat di prosedur sebelumnya, lalu pilih Simpan.

Note

Jika Anda tidak mengaktifkan propagasi rute, Anda harus secara manual memasukkan rute statis yang digunakan oleh koneksi VPN Anda. Untuk melakukannya, pilih tabel rute Anda, pilih Rute, Edit. Untuk Tujuan, tambahkan rute statis yang digunakan oleh koneksi Site-to-Site VPN Anda. Untuk Target, pilih ID gateway privat virtual, dan pilih Simpan.

Untuk menonaktifkan propagasi rute menggunakan konsol tersebut

1. Di panel navigasi, pilih Tabel rute.
2. Pilih tabel rute yang terkait dengan subnet.
3. Pada tab Rute propagation, pilih Edit propagasi rute. Kosongkan kotak centang Propagate untuk gateway pribadi virtual.
4. Pilih Simpan.

Untuk mengaktifkan propagasi rute menggunakan baris perintah atau API

- [EnableVgwRoutePropagation](#) (Amazon EC2 Query API)
- [enable-vgw-route-propagation](#) (AWS CLI)
- [Enable-EC2VgwRoutePropagation](#) (AWS Tools for Windows PowerShell)

Untuk menonaktifkan propagasi rute menggunakan baris perintah atau API

- [DisableVgwRoutePropagation](#) (Amazon EC2 Query API)
- [disable-vgw-route-propagation](#) (AWS CLI)
- [Disable-EC2VgwRoutePropagation](#) (AWS Tools for Windows PowerShell)

(Transit gateway) Tambahkan rute ke tabel rute Anda

Jika Anda mengaktifkan propagasi tabel rute untuk gateway transit Anda, rute untuk lampiran VPN disebarkan ke tabel rute gateway transit. Untuk informasi selengkapnya, lihat [Perutean](#) di Transit Gateway Amazon VPC.

Jika Anda melampirkan VPC ke transit gateway dan ingin mengaktifkan sumber daya di dalam VPC untuk menjangkau gateway pelanggan, Anda harus menambahkan rute ke tabel rute subnet untuk mengarah ke transit gateway.

Untuk menambahkan rute ke tabel rute VPC

1. Pada panel navigasi, pilih Tabel rute.
2. Pilih tabel rute yang terkait dengan VPC Anda.
3. Di tab Rute, pilih Edit rute.
4. Pilih Tambahkan rute.
5. Untuk Tujuan, masukkan rentang alamat IP tujuan. Untuk Target, pilih transit gateway.
6. Pilih Simpan perubahan.

Langkah 4: Perbarui grup keamanan Anda

Untuk mengizinkan akses ke instans di VPC serta dari jaringan Anda, maka Anda harus memperbarui aturan grup keamanan untuk mengaktifkan akses masuk SSH, RDP, dan ICMP.

Untuk menambahkan aturan ke grup keamanan Anda untuk mengaktifkan akses

1. Pada panel navigasi, pilih Grup keamanan.
2. Pilih grup keamanan untuk instance di VPC yang ingin Anda izinkan aksesnya.
3. Pada tab Inbound rules (Aturan ke dalam), pilih Edit inbound rules (Edit aturan ke dalam).

4. Tambahkan aturan yang memungkinkan akses SSH, RDP, dan ICMP masuk dari jaringan Anda, lalu pilih Simpan aturan. Untuk informasi selengkapnya, lihat [Bekerja dengan aturan grup keamanan](#) di Panduan Pengguna Amazon VPC.

Langkah 5: Buat koneksi VPN

Buat koneksi VPN menggunakan gateway pelanggan dalam kombinasi dengan gateway pribadi virtual atau gateway transit yang Anda buat sebelumnya.

Untuk membuat koneksi VPN

1. Di panel navigasi, pilih Koneksi VPN Site-to-Site.
2. Pilih Buat koneksi VPN.
3. (Opsional) Untuk tag Nama, masukkan nama untuk koneksi VPN Anda. Dengan melakukan hal tersebut akan menciptakan tanda dengan kunci Name dan nilai yang Anda tentukan.
4. Untuk jenis gateway Target, pilih salah satu Virtual Private Gateway atau Transit gateway. Kemudian, pilih gateway privat virtual atau transit gateway yang telah Anda buat sebelumnya.
5. Untuk gateway Pelanggan, pilih Existing, lalu pilih gateway pelanggan yang Anda buat sebelumnya dari ID gateway Pelanggan.
6. Pilih salah satu opsi perutean berdasarkan apakah perangkat gateway pelanggan Anda mendukung Border Gateway Protocol (BGP):
 - Jika perangkat gateway pelanggan Anda mendukung BGP, pilih Dinamis (membutuhkan BGP).
 - Jika perangkat gateway pelanggan Anda tidak mendukung BGP, pilih Statis. Untuk Awalan IP Statis, tentukan setiap awalan IP untuk jaringan pribadi koneksi VPN Anda.
7. Jika jenis gateway target Anda adalah gateway transit, untuk Tunnel di dalam versi IP, tentukan apakah terowongan VPN mendukung lalu lintas IPv4 atau IPv6. Lalu lintas IPv6 hanya didukung untuk koneksi VPN pada transit gateway.
8. Jika Anda menentukan IPv4 untuk Tunnel di dalam versi IP, Anda dapat secara opsional menentukan rentang IPv4 CIDR untuk gateway pelanggan dan AWS sisi yang diizinkan untuk berkomunikasi melalui terowongan VPN. Nilai default-nya `0.0.0.0/0`.

Jika Anda menentukan IPv6 untuk Tunnel di dalam versi IP, Anda dapat secara opsional menentukan rentang IPv6 CIDR untuk gateway pelanggan dan AWS sisi yang diizinkan untuk berkomunikasi melalui terowongan VPN. Default untuk kedua rentang tersebut adalah `::/0`.

9. Untuk jenis alamat IP Luar, pertahankan opsi default, PublicIpv4.
10. (Opsional) Untuk opsi Tunnel, Anda dapat menentukan informasi berikut untuk setiap terowongan:
 - Sebuah blok CIDR berukuran /30 IPv4 dari rentang 169.254.0.0/16 untuk alamat IPv4 terowongan dalam.
 - Jika Anda menentukan IPv6 untuk Tunnel di dalam versi IP, blok CIDR /126 IPv6 dari fd00::/8 rentang untuk alamat IPv6 terowongan di dalam.
 - Kunci pra-berbagi IKE (PSK). Versi berikut telah didukung: IKEv1 atau IKEv2.
 - Untuk mengedit opsi lanjutan untuk terowongan Anda, pilih opsi Edit terowongan. Untuk informasi selengkapnya, lihat [Opsional terowongan VPN](#).
11. Pilih Buat koneksi VPN. Mungkin perlu beberapa menit untuk membuat koneksi VPN.

Untuk membuat koneksi VPN menggunakan baris perintah atau API

- [CreateVpnConnection](#) (Amazon EC2 Query API)
- [create-vpn-connection](#) (AWS CLI)
- [New-EC2VpnConnection](#) (AWS Tools for Windows PowerShell)

Langkah 6: Unduh file konfigurasi

Setelah Anda membuat koneksi VPN, Anda dapat mengunduh file konfigurasi sampel yang akan digunakan untuk mengonfigurasi perangkat gateway pelanggan.

Important

File konfigurasi adalah contoh saja dan mungkin tidak cocok dengan pengaturan koneksi VPN yang Anda inginkan sepenuhnya. Ini menentukan persyaratan minimum untuk koneksi VPN AES128, SHA1, dan Diffie-Hellman grup 2 di sebagian besar AWS Wilayah, dan AES128, SHA2, dan Diffie-Hellman grup 14 di Wilayah. AWS GovCloud Ini juga menentukan kunci pra-berbagi untuk autentikasi. Anda harus memodifikasi contoh file konfigurasi untuk memanfaatkan algoritma keamanan tambahan, grup Diffie-Hellman, sertifikat pribadi, dan lalu lintas IPv6.

Kami telah memperkenalkan dukungan IKEv2 dalam file konfigurasi untuk banyak perangkat gateway pelanggan populer dan akan terus menambahkan file tambahan dari waktu ke

waktu. Untuk daftar file konfigurasi dengan dukungan IKEv2, lihat. [Perangkat gateway pelanggan Anda](#)

Izin

Untuk memuat layar konfigurasi unduhan dengan benar dari AWS Management Console, Anda harus memastikan bahwa peran IAM atau pengguna Anda memiliki izin untuk API `GetVpnConnectionDeviceTypes` Amazon EC2 berikut: dan. `GetVpnConnectionDeviceSampleConfiguration`

Untuk mengunduh file konfigurasi menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Koneksi VPN Site-to-Site.
3. Pilih koneksi VPN Anda dan pilih Unduh konfigurasi.
4. Pilih versi Vendor, Platform, Perangkat Lunak, dan IKE yang sesuai dengan perangkat gateway pelanggan Anda. Jika perangkat Anda tidak terdaftar, pilih Generik.
5. Pilih Unduh.

Untuk mengunduh file konfigurasi sampel menggunakan baris perintah atau API

- [GetVpnConnectionDeviceTypes](#) (Amazon EC2 API)
- [GetVpnConnectionDeviceSampleConfiguration](#) (Amazon EC2 Query API)
- [get-vpn-connection-device-jenis](#) ()AWS CLI
- [get-vpn-connection-device-sampel-konfigurasi](#) ()AWS CLI

Langkah 7: Konfigurasikan perangkat gateway pelanggan

Gunakan file konfigurasi sampel untuk mengonfigurasi perangkat gateway pelanggan Anda.

Perangkat gateway pelanggan adalah alat fisik atau perangkat lunak di sisi koneksi VPN Anda. Untuk informasi selengkapnya, lihat [Perangkat gateway pelanggan Anda](#).

Arsitektur situs-ke-situs VPN

Beberapa skenario VPN koneksi

Berikut ini adalah skenario di mana Anda dapat membuat beberapa VPN koneksi dengan satu atau beberapa perangkat gateway pelanggan.

Beberapa VPN koneksi menggunakan perangkat gateway pelanggan yang sama

Anda dapat membuat VPN sambungan tambahan dari lokasi lokal ke lokasi lain VPCs menggunakan perangkat gateway pelanggan yang sama. Anda dapat menggunakan kembali alamat IP gateway pelanggan yang sama untuk masing-masing VPN koneksi tersebut.

VPN Koneksi redundan menggunakan perangkat gateway pelanggan kedua

Untuk melindungi dari hilangnya konektivitas jika perangkat gateway pelanggan Anda tidak tersedia, Anda dapat mengatur VPN koneksi kedua menggunakan perangkat gateway pelanggan kedua. Untuk informasi selengkapnya, lihat [Menggunakan koneksi Site-to-Site VPN berlebih untuk memberikan failover](#). Ketika Anda membuat perangkat gateway pelanggan berlebihan di satu lokasi, kedua perangkat harus mengiklankan rentang IP yang sama.

Beberapa perangkat gateway pelanggan ke satu gateway pribadi virtual (AWS VPN CloudHub)

Anda dapat membuat beberapa VPN koneksi ke satu gateway pribadi virtual dari beberapa perangkat gateway pelanggan. Ini memungkinkan Anda untuk memiliki beberapa lokasi yang terhubung ke AWS VPN CloudHub. Untuk informasi selengkapnya, lihat [Menyediakan komunikasi yang aman antar situs menggunakan VPN CloudHub](#). Bila Anda memiliki perangkat gateway pelanggan di beberapa lokasi geografis, setiap perangkat harus mengiklankan rangkaian IP khusus yang spesifik ke lokasi.

Berikut ini adalah arsitektur VPN Site-to-Site yang umum:

- [the section called “Koneksi VPN tunggal dan ganda”](#)
- [the section called “Koneksi VPN redundan”](#)
- [the section called “AWS VPN CloudHub”](#)

Contoh koneksi VPN tunggal dan ganda Site-to-Site

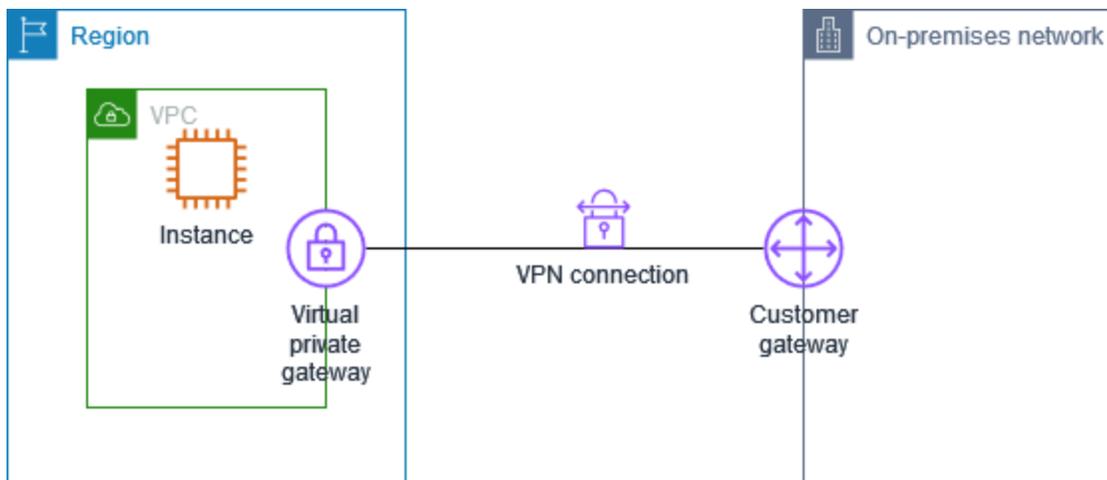
Diagram berikut menggambarkan koneksi tunggal dan ganda Site-to-Site VPN.

Contoh

- [Koneksi tunggal Site-to-Site VPN.](#)
- [Koneksi Site-to-Site VPN tunggal dengan transit gateway](#)
- [Koneksi ganda Site-to-Site VPN](#)
- [Beberapa koneksi Site-to-Site VPN dengan transit gateway](#)
- [Koneksi VPN Site-to-Site dengan AWS Direct Connect](#)
- [Koneksi VPN Site-to-Site IP pribadi dengan AWS Direct Connect](#)

Koneksi tunggal Site-to-Site VPN.

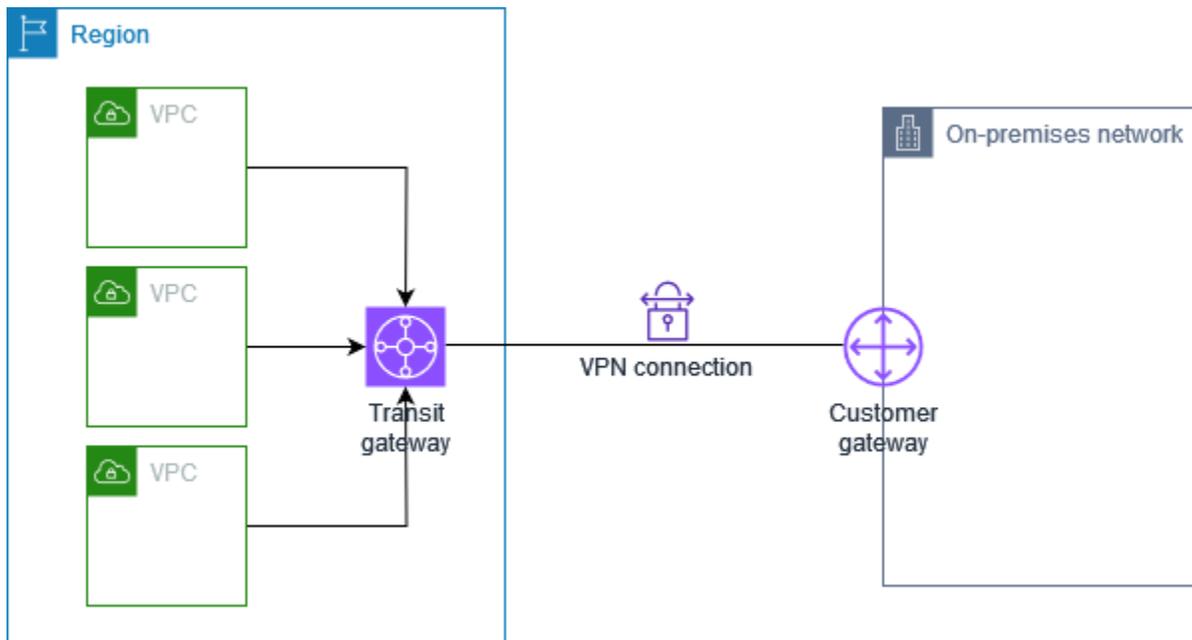
VPC memiliki gateway pribadi virtual terlampir, dan jaringan lokal (jarak jauh) Anda menyertakan perangkat gateway pelanggan, yang harus Anda konfigurasi untuk mengaktifkan koneksi VPN. Anda harus memperbarui tabel rute VPC sehingga lalu lintas apa pun dari VPC yang terikat untuk jaringan Anda masuk ke gateway pribadi virtual.



Untuk langkah-langkah untuk mengatur skenario ini, lihat [Memulai dengan AWS Site-to-Site VPN.](#)

Koneksi Site-to-Site VPN tunggal dengan transit gateway

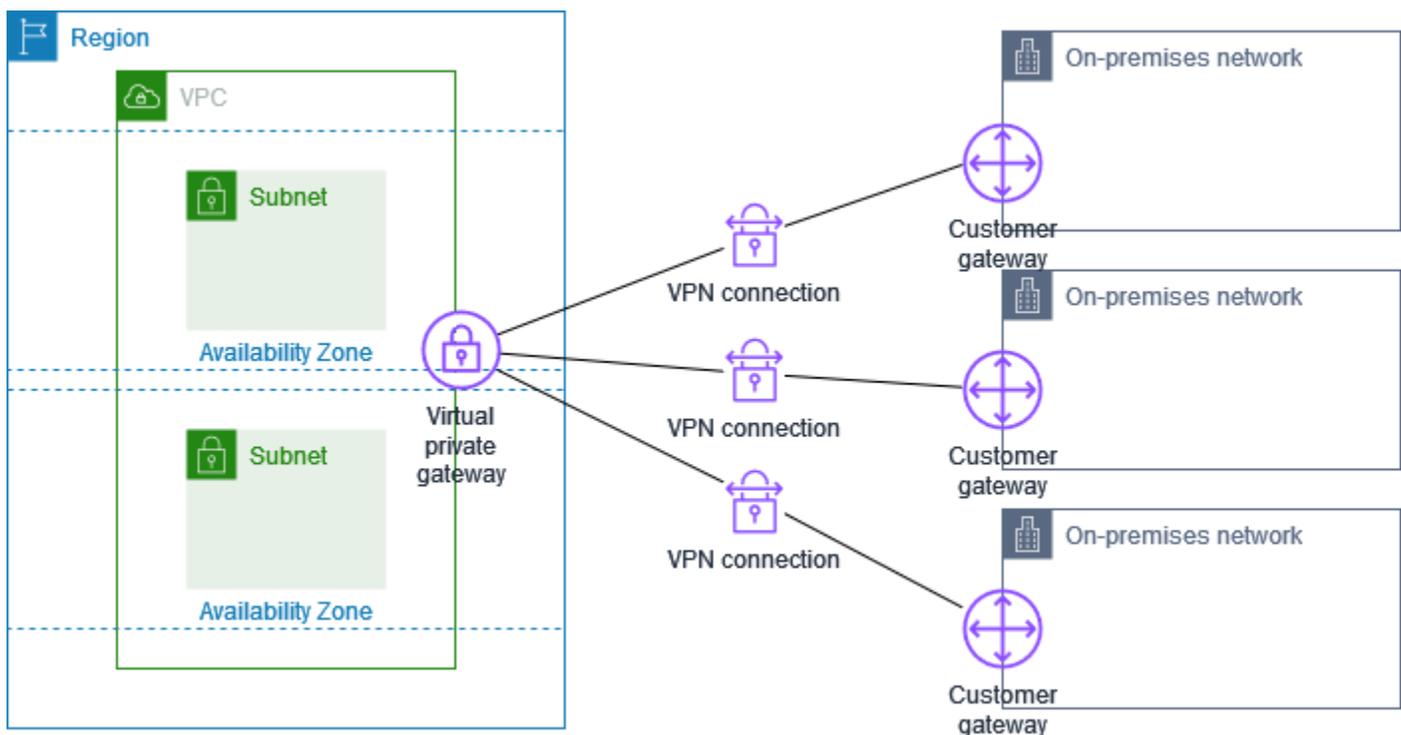
VPC memiliki gateway transit terlampir, dan jaringan lokal (jarak jauh) Anda menyertakan perangkat gateway pelanggan, yang harus Anda konfigurasi untuk mengaktifkan koneksi VPN. Anda harus memperbarui tabel rute VPC sehingga lalu lintas apa pun dari VPC yang terikat untuk jaringan Anda masuk ke gateway transit.



Langkah-langkah untuk mengatur skenario ini, lihat [Memulai dengan AWS Site-to-Site VPN](#).

Koneksi ganda Site-to-Site VPN

VPC memiliki virtual private gateway yang terpasang, dan Anda memiliki koneksi ganda Site-to-Site VPN ke beberapa lokasi on-premise. Anda mengatur perutean sehingga setiap lalu lintas apa pun dari VPC yang terikat untuk jaringan Anda dirutekan ke virtual private gateway.

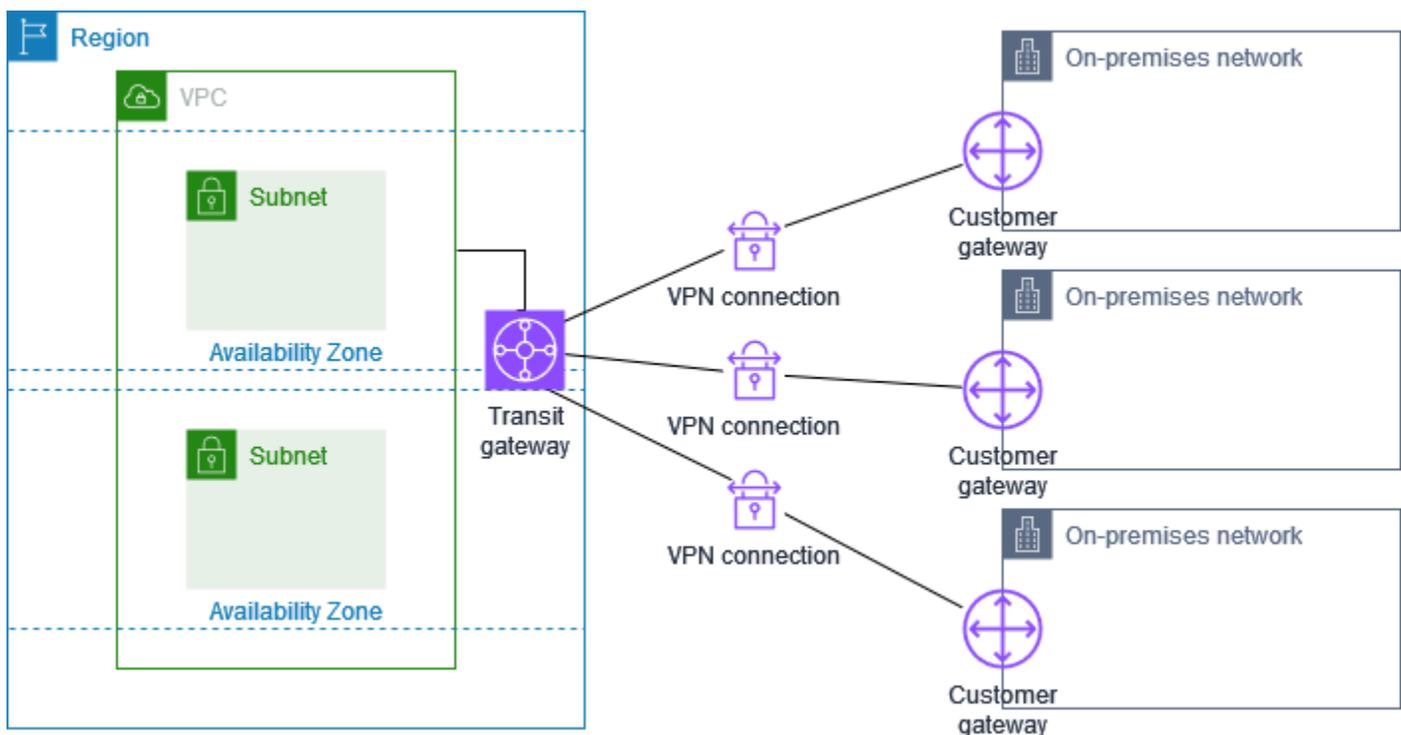


Ketika Anda membuat koneksi ganda Site-to-Site VPN ke VPC tunggal, Anda dapat mengonfigurasi gateway pelanggan kedua untuk membuat koneksi lebih ke lokasi eksternal yang sama. Untuk informasi selengkapnya, lihat [Menggunakan koneksi Site-to-Site VPN berlebih untuk memberikan failover](#).

Anda juga dapat menggunakan skenario ini untuk membuat koneksi Site-to-Site VPN ke beberapa lokasi geografis dan menyediakan komunikasi yang aman antar situs. Untuk informasi selengkapnya, lihat [Menyediakan komunikasi yang aman antar situs menggunakan VPN CloudHub](#).

Beberapa koneksi Site-to-Site VPN dengan transit gateway

VPC memiliki transit gateway yang terlampir, dan Anda memiliki beberapa koneksi Site-to-Site VPN ke beberapa lokasi on-premise. Anda mengatur perutean sehingga lalu lintas apa pun dari VPC yang menuju jaringan Anda dirutekan ke transit gateway.

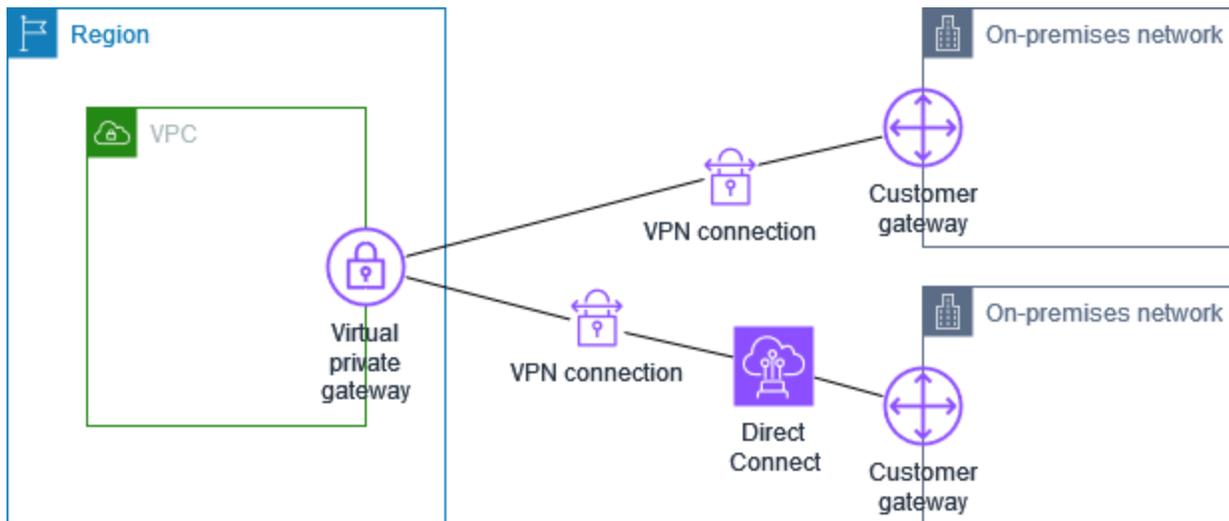


Ketika Anda membuat koneksi ganda Site-to-Site VPN ke transit gateway tunggal, Anda dapat mengonfigurasi gateway pelanggan kedua untuk membuat koneksi lebih ke lokasi eksternal yang sama.

Anda juga dapat menggunakan skenario ini untuk membuat koneksi Site-to-Site VPN ke beberapa lokasi geografis dan menyediakan komunikasi yang aman antar situs.

Koneksi VPN Site-to-Site dengan AWS Direct Connect

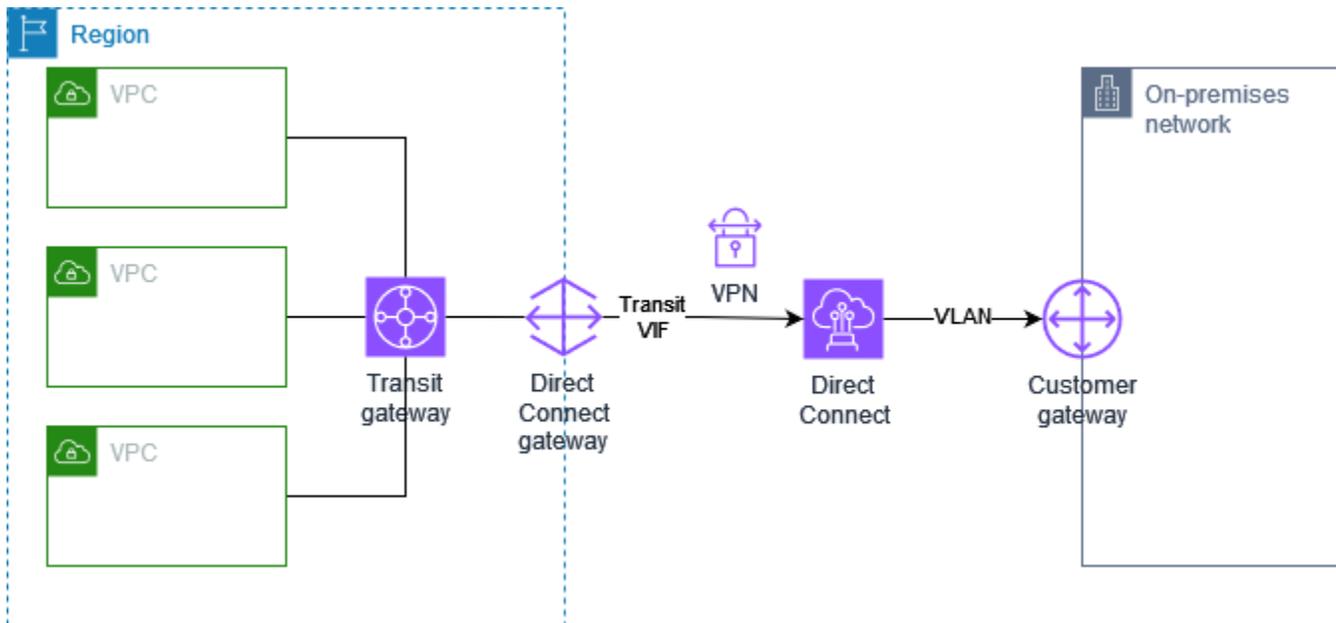
VPC memiliki gateway pribadi virtual terlampir, dan terhubung ke jaringan lokal (jarak jauh) Anda melalui. AWS Direct Connect Anda dapat mengonfigurasi antarmuka virtual AWS Direct Connect publik untuk membuat koneksi jaringan khusus antara jaringan Anda ke AWS sumber daya publik melalui gateway pribadi virtual. Anda mengatur perutean sehingga setiap lalu lintas dari VPC terikat untuk rute jaringan Anda ke gateway pribadi virtual dan AWS Direct Connect koneksi.



Ketika keduanya AWS Direct Connect dan koneksi VPN diatur pada gateway pribadi virtual yang sama, menambahkan atau menghapus objek dapat menyebabkan gateway pribadi virtual memasuki status 'melampirkan'. Hal ini menunjukkan perubahan sedang dibuat untuk perutean internal yang akan beralih antara koneksi AWS Direct Connect dan koneksi VPN untuk meminimumkan gangguan dan kehilangan paket. Setelah hal ini selesai, virtual private gateway kembali ke status 'terlampir'.

Koneksi VPN Site-to-Site IP pribadi dengan AWS Direct Connect

Dengan IP pribadi Site-to-Site VPN Anda dapat AWS Direct Connect mengenkripsi lalu lintas antara jaringan lokal Anda AWS dan tanpa menggunakan alamat IP publik. Private IP VPN over AWS Direct Connect memastikan bahwa lalu lintas antara AWS dan jaringan lokal aman dan pribadi, memungkinkan pelanggan untuk mematuhi mandat peraturan dan keamanan.



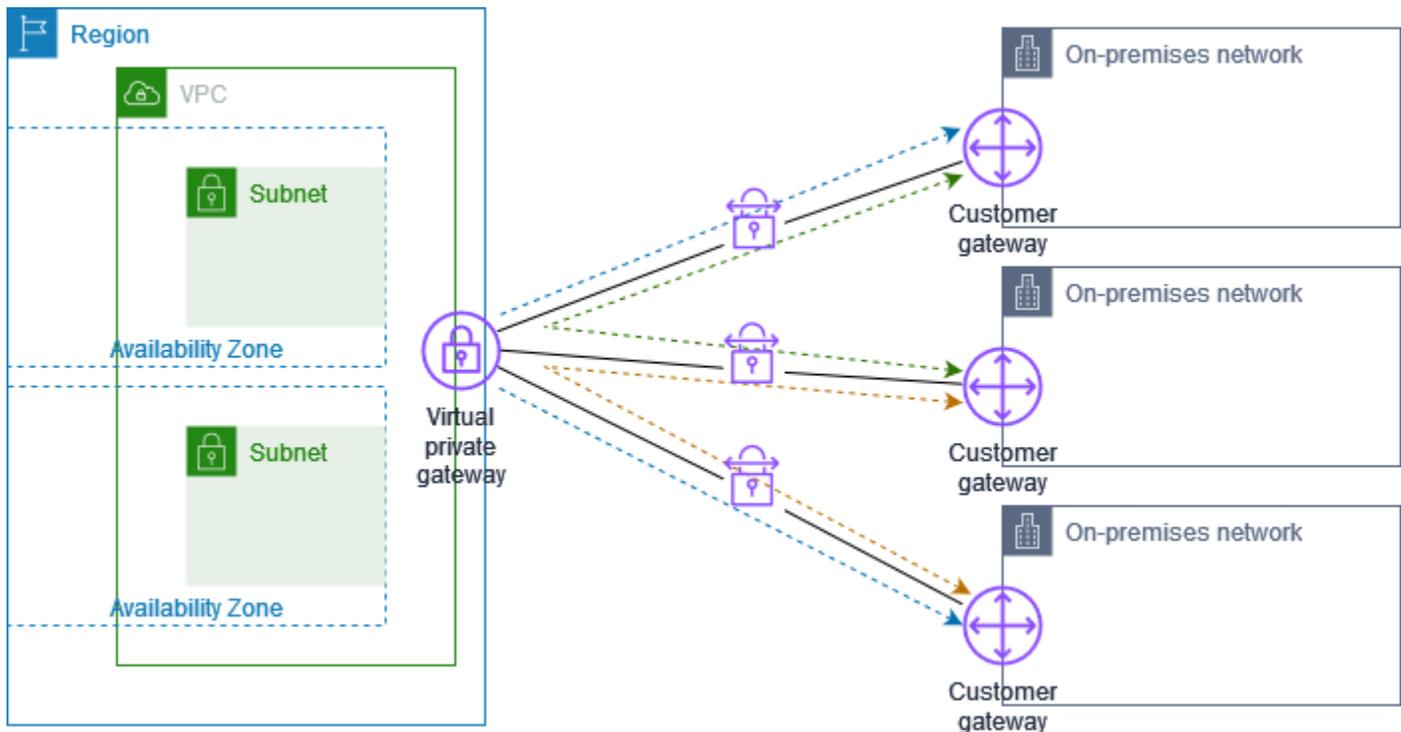
Untuk informasi selengkapnya, lihat posting blog berikut: [Memperkenalkan AWS Site-to-Site VPN VPN IP Pribadi.](#)

Menyediakan komunikasi yang aman antar situs menggunakan VPN CloudHub

Jika Anda memiliki banyak AWS Site-to-Site VPN koneksi, Anda dapat menyediakan komunikasi yang aman antar situs menggunakan AWS VPN CloudHub. Ini memungkinkan situs Anda untuk berkomunikasi satu sama lain, dan tidak hanya dengan sumber daya di VPC Anda. VPN CloudHub beroperasi pada hub-and-spoke model sederhana yang dapat Anda gunakan dengan atau tanpa VPC. Desain ini cocok jika Anda memiliki beberapa kantor cabang dan koneksi internet yang ada dan ingin menerapkan hub-and-spoke model yang nyaman dan berpotensi murah untuk konektivitas primer atau cadangan antara situs-situs ini.

Gambaran Umum

Diagram berikut menunjukkan CloudHub arsitektur VPN. Garis putus-putus menunjukkan lalu lintas jaringan antara situs jarak jauh yang dirutekan melalui koneksi VPN. Situs tidak boleh memiliki rentang IP yang tumpang tindih.



Untuk skenario ini, lakukan hal-hal berikut:

1. Buat satu virtual private gateway.
2. Buat beberapa gateway pelanggan, masing-masing dengan alamat IP publik gateway. Anda harus menggunakan Border Gateway Protocol (BGP) Autonomous System Number (ASN) yang unik untuk setiap gateway pelanggan.
3. Buat koneksi Site-to-Site VPN yang dirutekan secara dinamis dari setiap gateway pelanggan ke virtual private gateway umum.
4. Konfigurasi perangkat gateway pelanggan untuk mengiklankan prefix situs yang spesifik (seperti 10.0.0.0/24, 10.0.1.0/24) ke virtual private gateway. Iklan perutean ini diterima dan diiklankan kembali ke setiap peer BGP, memungkinkan setiap situs untuk mengirimkan data ke situs lain serta menerima data dari situs lain. Hal ini dilakukan menggunakan pernyataan jaringan dalam file konfigurasi VPN untuk koneksi Site-to-Site VPN. Pernyataan jaringan sedikit berbeda tergantung pada jenis router yang Anda gunakan.
5. Konfigurasi rute di tabel rute subnet Anda untuk mengaktifkan instans di VPC Anda untuk berkomunikasi dengan situs Anda. Untuk informasi selengkapnya, lihat [\(Gateway privat virtual\) Aktifkan propagasi rute di tabel rute Anda](#). Anda dapat mengonfigurasi rute agregat di tabel rute Anda (misalnya, 10.0.0.0/16). Gunakan prefix yang lebih spesifik diantara perangkat gateway pelanggan dan virtual private gateway.

Situs yang menggunakan AWS Direct Connect koneksi ke gateway pribadi virtual juga dapat menjadi bagian dari AWS VPN CloudHub. Misalnya, kantor pusat perusahaan Anda di New York dapat memiliki koneksi AWS Direct Connect ke VPC, dan kantor cabang Anda dapat menggunakan koneksi Site-to-Site VPN ke VPC. Kantor cabang di Los Angeles dan Miami dapat mengirim dan menerima data satu sama lain dan dengan kantor pusat perusahaan Anda, semuanya menggunakan AWS VPN CloudHub.

Harga

Untuk menggunakan AWS VPN CloudHub, Anda membayar tarif koneksi VPN Site-to-Site Amazon VPC yang khas. Anda akan ditagih tarif koneksi per jam setiap VPN terkoneksi ke virtual private gateway. Ketika Anda mengirim data dari satu situs ke situs lain menggunakan AWS VPN CloudHub, tidak ada biaya untuk mengirim data dari situs Anda ke gateway pribadi virtual. Anda hanya membayar tarif transfer data AWS standar untuk data yang diteruskan dari virtual private gateway ke titik akhir Anda.

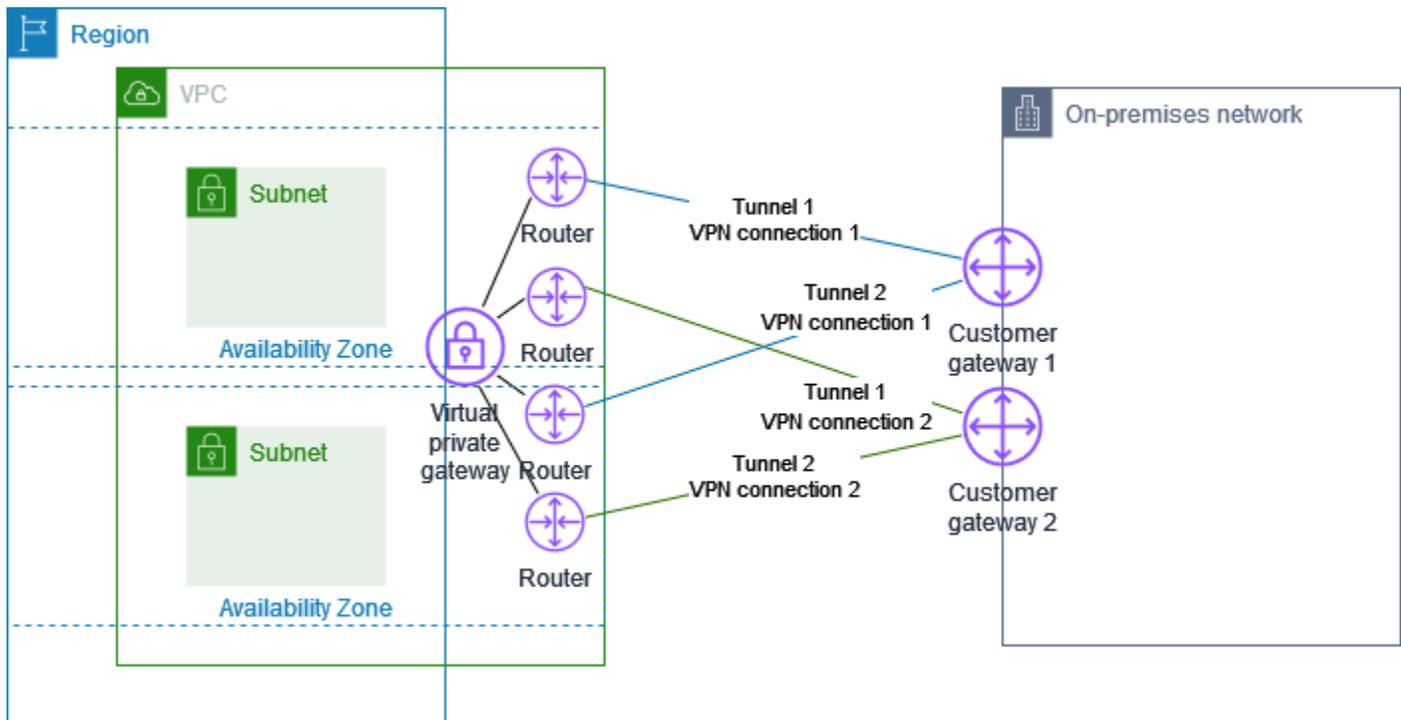
Misalnya, jika Anda memiliki situs di Los Angeles dan situs kedua di New York, serta kedua situs memiliki koneksi Site-to-Site VPN ke virtual private gateway, maka Anda perlu membayar tarif per jam untuk setiap koneksi Site-to-Site VPN (sehingga jika tarifnya \$0,05 per jam, totalnya akan menjadi \$0,10 per jam). Anda juga membayar tarif transfer AWS data standar untuk semua data yang Anda kirim dari Los Angeles ke New York (dan sebaliknya) yang melintasi setiap koneksi VPN Site-to-Site. Lalu lintas jaringan yang dikirim melalui koneksi VPN Site-to-Site ke gateway pribadi virtual gratis tetapi lalu lintas jaringan yang dikirim melalui koneksi VPN Site-to-Site dari gateway pribadi virtual ke titik akhir ditagih pada kecepatan transfer data standar. AWS

Untuk informasi selengkapnya, lihat [Harga Site-to-Site VPN](#).

Menggunakan koneksi Site-to-Site VPN berlebih untuk memberikan failover

Untuk melindungi dari hilangnya konektivitas jika perangkat gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi VPN Site-to-Site kedua ke VPC dan gateway pribadi virtual Anda dengan menambahkan perangkat gateway pelanggan kedua. Dengan menggunakan koneksi VPN yang berlebihan dan perangkat gateway pelanggan, Anda dapat melakukan pemeliharaan di salah satu perangkat Anda sementara lalu lintas terus mengalir melalui koneksi VPN kedua.

Diagram berikut menunjukkan dua koneksi VPN. Setiap koneksi VPN memiliki terowongan sendiri dan gateway pelanggannya sendiri.



Untuk skenario ini, lakukan hal berikut ini:

- Atur koneksi Site-to-Site VPN kedua menggunakan gateway privat virtual yang sama dan membuat gateway pelanggan baru. Alamat IP gateway pelanggan untuk koneksi Site-to-Site VPN kedua harus dapat diakses secara publik.
- Konfigurasi perangkat gateway pelanggan kedua. Kedua perangkat harus mengiklankan rentang IP yang sama ke gateway privat virtual. Kami menggunakan perutean BGP untuk menentukan jalur lalu lintas. Jika salah satu perangkat gateway pelanggan tidak berfungsi, gateway privat virtual mengarahkan semua lalu lintas ke perangkat gateway pelanggan yang masih berfungsi.

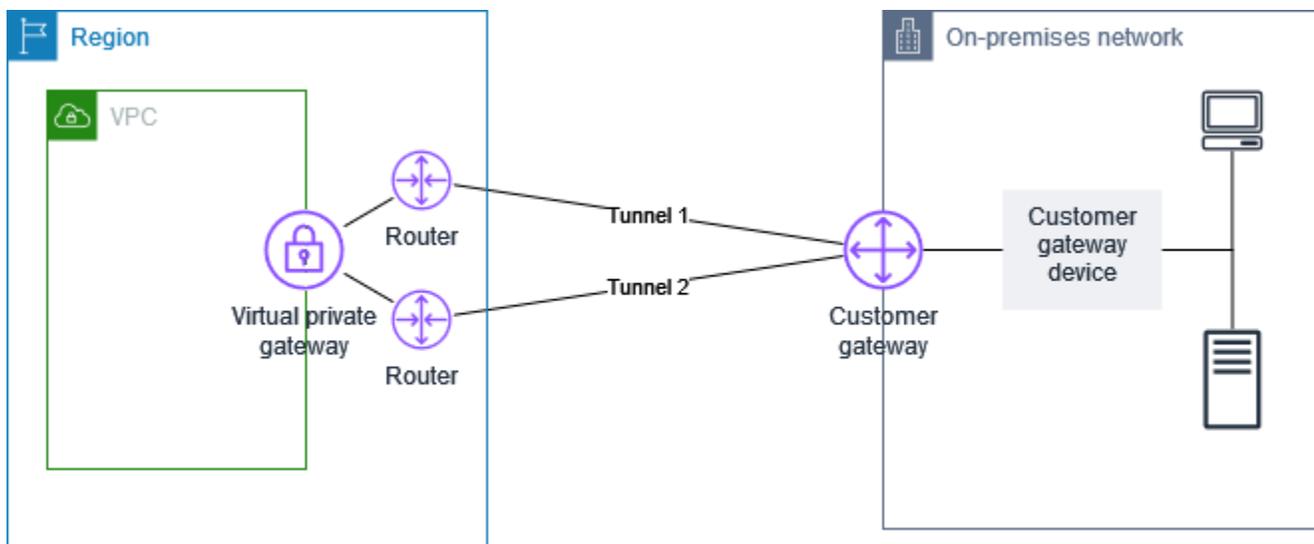
Koneksi Site-to-Site VPN yang dirutekan secara dinamis menggunakan Border Gateway Protocol (BGP) untuk bertukar informasi perutean antara gateway pelanggan dan gateway privat virtual Anda. Koneksi Site-to-Site VPN yang dirutekan secara statis mengharuskan Anda untuk memasukkan rute statis untuk jaringan jarak jauh di sisi gateway pelanggan Anda. Informasi rute yang diiklankan BGP dan dimasukkan secara statis mengizinkan gateway di kedua sisi untuk menentukan terowongan yang tersedia dan mengalihkan rute lalu lintas jika terjadi kegagalan. Kami merekomendasikan agar Anda mengonfigurasi jaringan Anda untuk menggunakan informasi perutean yang disediakan oleh BGP (jika tersedia) untuk memilih jalur yang tersedia. Konfigurasi yang tepat tergantung pada arsitektur jaringan Anda.

Untuk informasi lebih lanjut tentang cara membuat dan mengonfigurasi gateway pelanggan dan koneksi Site-to-Site VPN, lihat [Memulai dengan AWS Site-to-Site VPN](#).

Perangkat gateway pelanggan Anda

Perangkat gateway pelanggan adalah alat fisik atau perangkat lunak yang Anda miliki atau kelola di jaringan lokal (di sisi koneksi VPN Situs-ke-Situs). Anda atau administrator jaringan Anda harus mengonfigurasi perangkat agar berfungsi dengan koneksi VPN Site-to-Site.

Diagram berikut menunjukkan jaringan Anda, perangkat gateway pelanggan, dan VPN koneksi yang menuju ke gateway pribadi virtual yang dilampirkan ke AndaVPC. Dua jalur antara gateway pelanggan dan gateway pribadi virtual mewakili terowongan untuk VPN koneksi. Jika ada kegagalan perangkat di dalam AWS, VPN koneksi Anda secara otomatis gagal ke terowongan kedua sehingga akses Anda tidak terganggu. Dari waktu ke waktu, AWS juga melakukan pemeliharaan rutin pada VPN koneksi, yang mungkin secara singkat menonaktifkan salah satu dari dua terowongan VPN koneksi Anda. Untuk informasi selengkapnya, lihat [Penggantian titik akhir terowongan Site-to-Site VPN](#). Ketika Anda mengonfigurasi perangkat gateway pelanggan Anda, oleh karena itu penting bagi Anda untuk mengonfigurasinya untuk menggunakan kedua terowongan.



Untuk langkah-langkah untuk mengatur VPN koneksi, lihat [Memulai dengan AWS Site-to-Site VPN](#). Selama proses ini, Anda membuat sumber daya gateway pelanggan di AWS, yang memberikan informasi AWS tentang perangkat Anda, misalnya, alamat IP yang menghadap publik. Untuk informasi selengkapnya, lihat [Opsis gateway pelanggan untuk koneksi Site-to-Site VPN](#). Sumber daya gateway pelanggan di AWS tidak mengonfigurasi atau membuat perangkat gateway pelanggan. Anda harus mengonfigurasi perangkat itu sendiri.

Anda juga dapat menemukan perangkat VPN lunak di [AWS Marketplace](#).

Persyaratan untuk perangkat gateway pelanggan Anda

Jika Anda memiliki perangkat yang tidak ada dalam daftar contoh sebelumnya, bagian ini menjelaskan persyaratan yang harus dipenuhi perangkat agar Anda dapat menggunakannya untuk membuat koneksi VPN Situs-ke-Situs.

Ada empat bagian utama untuk konfigurasi perangkat gateway pelanggan Anda. Simbol-simbol berikut mewakili setiap bagian dari konfigurasi.

IKE	Asosiasi keamanan pertukaran kunci internet (IKE). Ini diperlukan untuk bertukar kunci yang digunakan untuk mendirikan asosiasi IPsec keamanan.
IPsec	IPsec asosiasi keamanan. Hal ini menangani enkripsi terowongan, autentikasi, dan sebagainya.
Tunnel	Antarmuka terowongan. Antarmuka terowongan menerima lalu lintas pergi ke dan dari terowongan.
BGP	(Opsional) Border Gateway Protocol (BGP) mengintip. Untuk perangkat yang menggunakan BGP, ini bertukar rute antara perangkat gateway pelanggan dan gateway pribadi virtual.

Tabel berikut mencantumkan persyaratan untuk perangkat gateway pelanggan, yang terkait RFC (untuk referensi), dan komentar tentang persyaratan.

Setiap VPN koneksi terdiri dari dua terowongan terpisah. Setiap terowongan berisi asosiasi IKE keamanan, asosiasi IPsec keamanan, dan BGP pengintip. Anda terbatas pada satu pasangan asosiasi keamanan unik (SA) per terowongan (satu inbound dan satu outbound), dan oleh karena itu dua pasangan SA unik secara total untuk dua terowongan (empat). SAs Beberapa perangkat menggunakan berbasis kebijakan VPN dan membuat SAs sebanyak ACL entri. Oleh karena itu, Anda mungkin perlu untuk mengkonsolidasikan aturan Anda dan kemudian mem-filter sehingga Anda tidak mengizinkan lalu lintas yang tidak diinginkan.

Secara default, VPN terowongan muncul ketika lalu lintas dihasilkan dan IKE negosiasi dimulai dari sisi koneksi Anda. VPN Anda dapat mengonfigurasi VPN koneksi untuk memulai IKE negosiasi dari AWS sisi koneksi sebagai gantinya. Untuk informasi selengkapnya, lihat [Opsis inisiasi terowongan Site-to-Site VPN](#).

VPN endpoint mendukung rekey dan dapat memulai negosiasi ulang ketika fase 1 akan kedaluwarsa jika perangkat gateway pelanggan belum mengirim lalu lintas negosiasi ulang apa pun.

Persyaratan	RFC	Komentar
<p>Mendirikan asosiasi IKE keamanan</p> <p>IKE</p>	<p>RFC2409</p> <p>RFC7296</p>	<p>Asosiasi IKE keamanan didirikan pertama antara gateway pribadi virtual dan perangkat gateway pelanggan menggunakan kunci pra-bersama atau sertifikat pribadi yang digunakan AWS Private Certificate Authority sebagai autentikator. Ketika didirikan, IKE menegosiasikan kunci singkat untuk mengamankan pesan future. IKE Harus ada kesepakatan lengkap di antara parameter, termasuk enkripsi dan autentikasi parameter.</p> <p>Saat Anda membuat VPN koneksi AWS, Anda dapat menentukan kunci pra-bersama Anda sendiri untuk setiap terowongan, atau Anda dapat membiarkan AWS menghasilkan satu untuk Anda. Atau, Anda dapat menentukan sertifikat pribadi yang digunakan AWS Private Certificate Authority untuk digunakan untuk perangkat gateway pelanggan Anda. Untuk informasi selengkapnya, tentang mengonfigurasi VPN terowongan, lihat. Opsional terowongan untuk koneksi Site-to-Site VPN Anda</p> <p>Versi berikut didukung: IKEv1 dan IKEv2.</p> <p>Kami mendukung mode Utama hanya dengan IKEv1.</p> <p>VPN Layanan Site-to-Site adalah solusi berbasis rute. Jika Anda menggunakan konfigurasi berbasis kebijakan, Anda harus membatasi konfigurasi Anda untuk satu keamanan Asosiasi (SA).</p>
<p>Membangun asosiasi IPsec keamanan dalam mode Tunnel</p>	<p>RFC4301</p>	<p>Menggunakan kunci IKE singkat, kunci dibuat antara gateway pribadi virtual dan perangkat gateway pelanggan untuk membentuk asosiasi IPsec</p>

Persyaratan	RFC	Komentar
IPsec		keamanan (SA). Lalu lintas antara gateway dienkripsi dan didekripsi menggunakan SA ini. Kunci singkat yang digunakan untuk mengenkripsi lalu lintas dalam IPsec SA secara otomatis diputar oleh IKE secara teratur untuk memastikan kerahasiaan komunikasi.
Gunakan enkripsi AES 128-bit atau fungsi enkripsi AES 256-bit	RFC3602	Fungsi enkripsi digunakan untuk memastikan privasi untuk keduanya IKE dan asosiasi IPsec keamanan.
Gunakan fungsi hashing SHA -1 atau SHA -2 (256)	RFC2404	Fungsi hashing ini digunakan untuk mengautentikasi keduanya IKE dan asosiasi IPsec keamanan.
Gunakan Diffie-Hellman Perfect Forward Secrecy.	RFC2409	<p>IKE menggunakan Diffie-Hellman untuk membuat kunci fana untuk mengamankan semua komunikasi antara perangkat gateway pelanggan dan gateway pribadi virtual.</p> <p>Grup berikut didukung:</p> <ul style="list-style-type: none"> • Grup tahap 1: 2, 14-24 • Grup tahap 2: 2, 5, 14-24
(VPN Koneksi yang dirutekan secara dinamis) Gunakan Dead Peer Detection IPsec	RFC3706	Dead Peer Detection memungkinkan VPN perangkat untuk mengidentifikasi dengan cepat ketika kondisi jaringan mencegah pengiriman paket di internet. Ketika ini terjadi, gateway menghapus Asosiasi keamanan dan mencoba untuk membuat Asosiasi baru. Selama proses ini, IPsec terowongan alternatif digunakan jika memungkinkan.

Persyaratan	RFC	Komentar
(VPN Koneksi yang dirutekan secara dinamis) Ikat terowongan ke antarmuka logis (berbasis rute) VPN Tunnel	Tidak ada	Perangkat Anda harus dapat mengikat IPsec terowongan ke antarmuka logis. Antarmuka logis berisi alamat IP yang digunakan untuk membuat BGP peering ke gateway pribadi virtual. Antarmuka logis ini seharusnya tidak melakukan enkapsulasi tambahan (misalnya, GRE atau IP dalam IP). Antarmuka Anda harus diatur ke 1399 byte Maximum Transmission Unit (MTU).
(Koneksi yang dirutekan secara dinamis) Membangun peerings VPN BGP BGP	RFC4271	BGP digunakan untuk bertukar rute antara perangkat gateway pelanggan dan gateway pribadi virtual untuk perangkat yang digunakan BGP. Semua BGP lalu lintas dienkripsi dan ditransmisikan melalui Asosiasi IPsec Keamanan. BGP diperlukan untuk kedua gateway untuk menukar awalan IP yang dapat dijangkau melalui SA. IPsec

AWS VPN Koneksi tidak mendukung Path MTU Discovery ([RFC1191](#)).

Jika Anda memiliki firewall antara perangkat gateway pelanggan dan internet, lihat [Aturan firewall untuk perangkat gateway pelanggan Anda](#).

Praktik terbaik untuk perangkat gateway pelanggan Anda

Gunakan IKEv2

Kami sangat menyarankan IKEv2 untuk menggunakan koneksi Site-to-Site VPN Anda. IKEv2 adalah protokol yang lebih sederhana, lebih kuat, dan lebih aman daripada IKEv1. Anda hanya boleh menggunakan IKEv1 jika perangkat gateway pelanggan Anda tidak mendukung IKEv2. Untuk detail lebih lanjut tentang perbedaan antara IKEv1 dan IKEv2, lihat [Lampiran A dari RFC7296](#)

Setel ulang flag “Don't Fragment (DF)” pada paket

Beberapa paket membawa bendera, yang dikenal sebagai bendera Jangan Fragment (DF), yang menunjukkan bahwa paket tidak boleh terfragmentasi. Jika paket membawa bendera, gateway menghasilkan pesan ICMP Path MTU Exceeded. Dalam beberapa kasus, aplikasi tidak mengandung

mekanisme yang memadai untuk memproses ICMP pesan-pesan ini dan untuk mengurangi jumlah data yang dikirimkan dalam setiap paket. Beberapa VPN perangkat dapat mengganti flag DF dan paket fragmen tanpa syarat sesuai kebutuhan. Jika perangkat gateway pelanggan Anda memiliki kemampuan ini, kami sarankan Anda menggunakannya sesuai kebutuhan. Lihat [RFC791](#) untuk lebih jelasnya.

Paket fragmen IP sebelum enkripsi

Jika paket yang dikirim melalui VPN koneksi Site-to-Site Anda melebihi MTU ukuran, mereka harus terfragmentasi. Untuk menghindari penurunan kinerja, kami sarankan Anda mengonfigurasi perangkat gateway pelanggan Anda untuk memecah paket sebelum dienkripsi. Site-to-site kemudian VPN akan memasang kembali paket yang terfragmentasi sebelum meneruskannya ke tujuan berikutnya, untuk mencapai arus yang lebih tinggi melalui jaringan. packet-per-second AWS Lihat [RFC4459](#) untuk lebih jelasnya.

Pastikan ukuran paket tidak melebihi MTU untuk jaringan tujuan

Karena Site-to-Site VPN akan memasang kembali paket terfragmentasi yang diterima dari perangkat gateway pelanggan Anda sebelum meneruskan ke tujuan berikutnya, perlu diingat, mungkin ada MTU ukuran/pertimbangan paket untuk jaringan tujuan di mana paket-paket ini diteruskan berikutnya, seperti over. AWS Direct Connect

Sesuaikan MTU dan MSS ukuran sesuai dengan algoritma yang digunakan

TCP Paket sering merupakan jenis paket yang paling umum di IPsec terowongan. Site-to-site VPN mendukung unit transmisi maksimum (MTU) 1446 byte dan ukuran segmen maksimum yang sesuai (MSS) 1406 byte. Namun, algoritma enkripsi memiliki ukuran header yang bervariasi dan dapat mencegah kemampuan untuk mencapai nilai maksimum ini. Untuk mendapatkan kinerja optimal dengan menghindari fragmentasi, kami sarankan Anda mengatur MTU dan MSS berdasarkan secara khusus pada algoritma yang digunakan.

Gunakan tabel berikut untuk mengatur MTU/MSS untuk menghindari fragmentasi dan mencapai kinerja optimal:

Algoritma Enkripsi	Algoritma Hashing	NAT-Traversal	MTU	MSS (IPv4)	MSS (IPv6-dalam-IPv4)
AES-GCM-16	N/A	dinonaktifkan	1446	1406	1386

Algoritma Enkripsi	Algoritma Hashing	NAT-Traversal	MTU	MSS (IPv4)	MSS(IPv6-dalam-IPv4)
AES- GCM -16	N/A	diaktifkan	1438	1398	1378
AES-CBC	SHA1/SHA2-256	dinonaktifkan	1438	1398	1378
AES-CBC	SHA1/SHA2-256	diaktifkan	1422	1382	1362
AES-CBC	SHA2-384	dinonaktifkan	1422	1382	1362
AES-CBC	SHA2-384	diaktifkan	1422	1382	1362
AES-CBC	SHA2-512	dinonaktifkan	1422	1382	1362
AES-CBC	SHA2-512	diaktifkan	1406	1366	1346

Note

GCMAlgoritma AES - mencakup enkripsi dan otentikasi, sehingga tidak ada pilihan algoritma otentikasi yang berbeda yang akan mempengaruhi. MTU

Nonaktifkan IKE unik IDs

Beberapa perangkat gateway pelanggan mendukung pengaturan yang memastikan bahwa paling banyak, satu asosiasi keamanan Fase 1 ada per konfigurasi terowongan. Pengaturan ini dapat mengakibatkan keadaan Fase 2 yang tidak konsisten antara VPN rekan-rekan. Jika perangkat gateway pelanggan Anda mendukung pengaturan ini, kami sarankan untuk menonaktifkannya.

Aturan firewall untuk perangkat gateway pelanggan Anda

Anda harus memiliki alamat IP statis untuk digunakan sebagai titik akhir untuk IPsec terowongan yang menghubungkan perangkat gateway pelanggan Anda ke AWS Site-to-Site VPN titik akhir. Jika firewall berada di antara AWS dan perangkat gateway pelanggan Anda, aturan dalam tabel

berikut harus ada untuk membuat IPsec terowongan. Alamat IP untuk AWS-side akan berada di file konfigurasi.

Inbound (dari internet)

Aturan masukan I1

IP sumber	Tunnel1 Luar IP
IP dest	Gateway pelanggan
Protokol	UDP
Port sumber	500
Tujuan	500

Aturan input I2

IP sumber	Tunnel2 Luar IP
IP dest	Gateway pelanggan
Protokol	UDP
Port sumber	500
Port tujuan	500

Aturan input I3

IP sumber	Tunnel1 Luar IP
IP dest	Gateway pelanggan
Protokol	IP 50 (ESP)

Aturan masukan I4

IP sumber	Tunnel2 Luar IP
IP dest	Gateway pelanggan

Protokol IP 50 (ESP)

Outbound (ke internet)

Aturan keluaran O1

IP sumber Gateway pelanggan

IP Tujuan Tunnel1 Luar IP

Protokol UDP

Port sumber 500

Port tujuan 500

Aturan keluaran O2

IP sumber Gateway pelanggan

IP Tujuan Tunnel2 Luar IP

Protokol UDP

Port sumber 500

Port tujuan 500

Aturan output O3

IP sumber Gateway pelanggan

IP Tujuan Tunnel1 Luar IP

Protokol IP 50 (ESP)

Aturan output O4

IP sumber Gateway pelanggan

IP Tujuan Tunnel2 Luar IP

Protokol

IP 50 (ESP)

Aturan I1, I2, O1, dan O2 memungkinkan transmisi paket. IKE Aturan I3, I4, O3, dan O4 memungkinkan transmisi IPsec paket yang berisi lalu lintas jaringan terenkripsi.

Note

Jika Anda menggunakan NAT traversal (NAT-T) pada perangkat Anda, pastikan bahwa UDP lalu lintas pada port 4500 juga diizinkan untuk melewati antara jaringan Anda dan titik akhir. AWS Site-to-Site VPN Periksa apakah perangkat Anda beriklan NAT -T.

Contoh file konfigurasi untuk perangkat gateway pelanggan Anda

Setelah membuat VPN koneksi, Anda juga memiliki opsi untuk mengunduh file konfigurasi sampel AWS yang disediakan dari VPC konsol Amazon, atau dengan menggunakan file. EC2 API Untuk informasi selengkapnya, lihat [Langkah 6: Unduh file konfigurasi](#). Anda juga dapat mengunduh file.zip dari konfigurasi sampel khusus untuk perutean statis vs. dinamis dari halaman masing-masing.

File konfigurasi sampel AWS yang disediakan berisi informasi khusus untuk VPN koneksi Anda yang dapat Anda gunakan untuk mengonfigurasi perangkat gateway pelanggan Anda. File konfigurasi khusus perangkat ini hanya tersedia untuk perangkat yang AWS telah diuji. Jika perangkat gateway pelanggan spesifik Anda tidak terdaftar, Anda dapat mengunduh file konfigurasi umum untuk memulai.

Important

File konfigurasi adalah contoh saja dan mungkin tidak cocok dengan pengaturan VPN koneksi Site-to-Site yang Anda inginkan sepenuhnya. Ini menentukan persyaratan minimum untuk VPN koneksi Site-to-Site dari,, dan Diffie-Hellman grup 2 di sebagian besar AWS Wilayah AES128SHA1, dan,, dan Diffie-Hellman grup 14 di Wilayah. AES128 SHA2 AWS GovCloud Ini juga menentukan kunci pra-berbagi untuk autentikasi. Anda harus memodifikasi contoh file konfigurasi untuk memanfaatkan algoritma keamanan tambahan, grup Diffie-Hellman, sertifikat pribadi, dan lalu lintas. IPv6

Note

File konfigurasi khusus perangkat ini disediakan oleh dengan upaya AWS terbaik. Meskipun mereka telah diuji oleh AWS, pengujian ini terbatas. Jika Anda mengalami masalah dengan file konfigurasi, Anda mungkin perlu menghubungi vendor tertentu untuk mendapatkan dukungan tambahan.

Tabel berikut berisi daftar perangkat yang memiliki contoh file konfigurasi yang tersedia untuk diunduh yang telah diperbarui untuk mendukung IKEv2. Kami telah memperkenalkan IKEv2 dukungan dalam file konfigurasi untuk banyak perangkat gateway pelanggan populer dan akan terus menambahkan file tambahan dari waktu ke waktu. Daftar ini akan diperbarui karena lebih banyak contoh file konfigurasi ditambahkan.

Penjual	Platform	Perangkat lunak
Titik pemeriksaan	Gaia	R80.10+
Cisco Meraki	Seri MX	15.12+ (WebUI)
Sistem Cisco, Inc.	ASA Seri 5500	ASA9.7+ VTI
Sistem Cisco, Inc.	CSRv AMI	IOS12.4+
Fortinet	Fortigate 40+ Seri	FortiOS 6.4.4+ () GUI
Jaringan Juniper, Inc.	J-Series Router	JunOS 9.5+
Jaringan Juniper, Inc.	SRX Router	JunOS 11.0+
Mikrotik	RouterOS	6.44.3
Jaringan Palo Alto	Seri PA	PANOS7.0+
SonicWall	NSA, TZ	OS 6.5
Sophos	Firewall Sophos	v19+
Angsa Kuat	Ubuntu 16.04	Strongswan 5.5.1+

Penjual	Platform	Perangkat lunak
Yamaha	RTXRouter	Rev.10.01.16+

Contoh konfigurasi perangkat gateway pelanggan untuk perutean statis

Untuk mengunduh file konfigurasi sampel dengan nilai khusus untuk konfigurasi VPN koneksi Site-to-Site Anda, gunakan VPC konsol Amazon, baris AWS perintah, atau Amazon. EC2 API Untuk informasi selengkapnya, lihat [Langkah 6: Unduh file konfigurasi](#).

[Anda juga dapat mengunduh file konfigurasi contoh umum untuk perutean statis yang tidak menyertakan nilai khusus untuk konfigurasi koneksi Site-to-Site VPN Anda: .zip static-routing-examples](#)

File menggunakan nilai placeholder untuk beberapa komponen. Misalnya, menggunakan:

- Contoh nilai untuk ID VPN koneksi, ID gateway pelanggan, dan ID gateway pribadi virtual
- Placeholder untuk titik akhir alamat AWS IP jarak jauh (luar) (*AWS_ENDPOINT_1* and *AWS_ENDPOINT_2*)
- Placeholder untuk alamat IP untuk antarmuka eksternal yang dapat dirutekan internet pada perangkat gateway pelanggan (*your-cgw-ip-address*)
- Placeholder untuk nilai kunci yang telah dibagikan sebelumnya () pre-shared-key
- Contoh nilai terowongan di dalam alamat IP.
- Contoh nilai untuk MTU pengaturan.

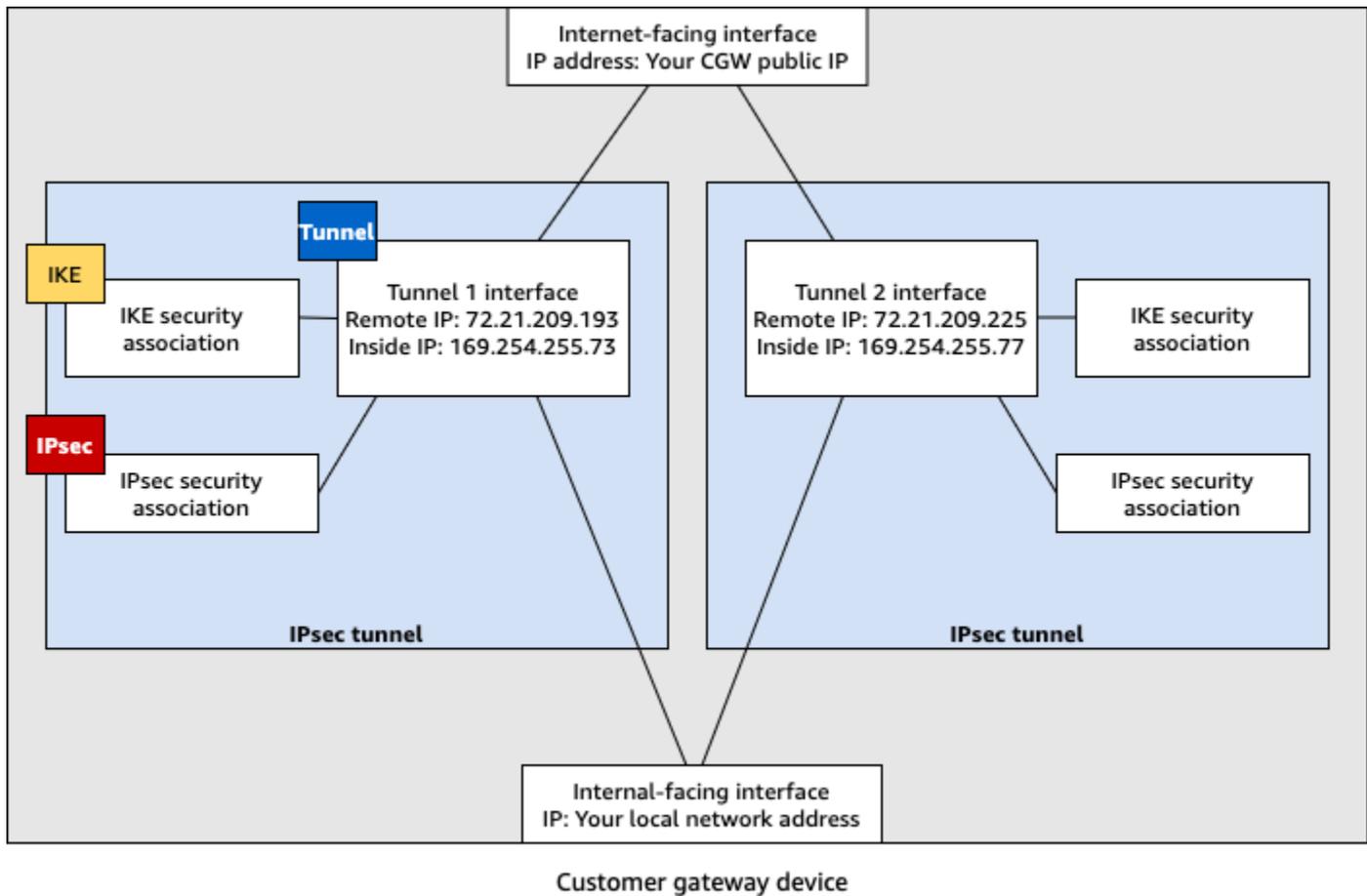
Note

MTU pengaturan yang disediakan dalam file konfigurasi sampel hanya contoh. Silakan merujuk ke [Praktik terbaik untuk perangkat gateway pelanggan Anda](#) untuk informasi tentang pengaturan MTU nilai optimal untuk situasi Anda.

Selain memberikan nilai placeholder, file menentukan persyaratan minimum untuk VPN koneksi Site-to-Site dari, dan Diffie-Hellman grup 2 di sebagian besar AWS Wilayah AES128SHA1, dan, dan Diffie-Hellman grup 14 di Wilayah. AES128 SHA2 AWS GovCloud File juga menentukan kunci pra-

berbagi untuk [otentikasi](#). Anda harus memodifikasi contoh file konfigurasi untuk memanfaatkan algoritma keamanan tambahan, grup Diffie-Hellman, sertifikat pribadi, dan lalu lintas IPv6

Diagram berikut memberikan gambaran umum mengenai komponen berbeda yang dikonfigurasi di perangkat gateway pelanggan. Komponen tersebut termasuk contoh nilai untuk alamat IP antarmuka terowongan.



Prosedur antarmuka pengguna untuk perutean statis

Berikut ini adalah beberapa contoh prosedur untuk mengonfigurasi perangkat gateway pelanggan menggunakan antarmuka pengguna (jika ada).

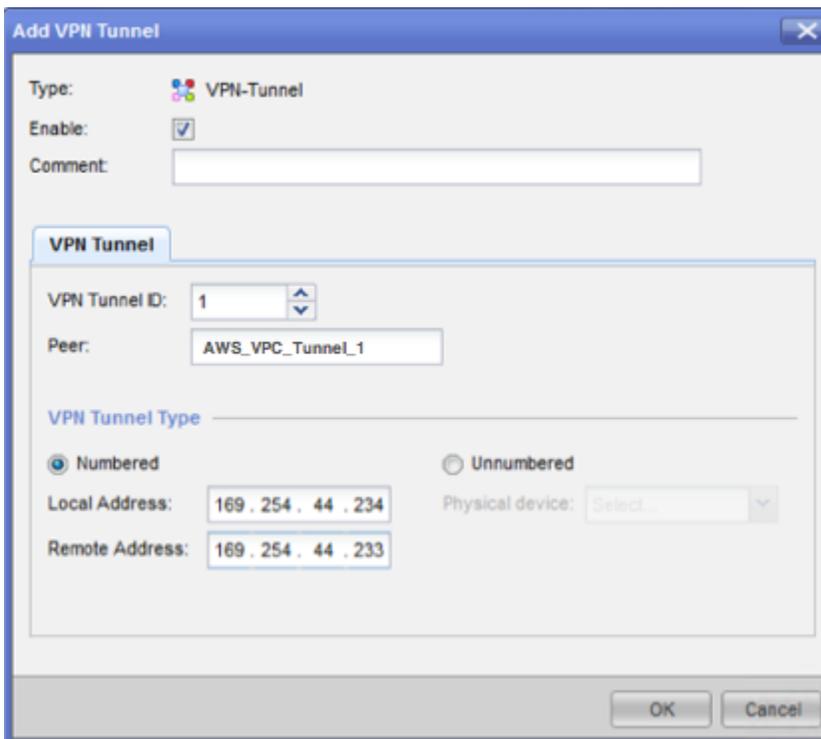
Check Point

Berikut ini adalah langkah-langkah untuk mengonfigurasi perangkat gateway pelanggan Anda jika perangkat Anda adalah perangkat Check Point Security Gateway yang menjalankan R77.10 atau lebih tinggi, menggunakan sistem operasi Gaia dan Check Point. SmartDashboard Anda juga dapat merujuk ke VPC artikel [Check Point Security Gateway IPsec VPN to Amazon Web Services](#) di Pusat Dukungan Check Point.

Untuk mengonfigurasi antarmuka terowongan

Langkah pertama adalah membuat VPN terowongan dan menyediakan alamat IP pribadi (dalam) dari gateway pelanggan dan gateway pribadi virtual untuk setiap terowongan. Untuk membuat terowongan pertama, gunakan informasi yang disediakan di bagian IPSec Tunnel #1 dari file konfigurasi. Untuk membuat terowongan kedua, gunakan nilai yang disediakan di bagian IPSec Tunnel #2 dari file konfigurasi.

1. Buka portal Gaia di perangkat Check Point Security Gateway Anda.
2. Pilih Antarmuka Jaringan, Tambah, VPNterowongan.
3. Pada kotak dialog, konfigurasi pengaturan seperti berikut, dan pilih OKE ketika Anda selesai:
 - Untuk ID VPN Tunnel, masukkan nilai unik apa pun, seperti 1.
 - Untuk Peer, masukkan nama unik untuk terowongan Anda, contohnya `AWS_VPC_Tunnel_1` atau `AWS_VPC_Tunnel_2`.
 - Pastikan bahwa Bernomor dipilih, dan untuk Alamat Lokal, masukkan alamat IP yang ditentukan untuk CGW Tunnel IP dalam file konfigurasi, misalnya, `169.254.44.234`.
 - Untuk Alamat Jarak Jauh, masukkan alamat IP yang ditentukan untuk VGW Tunnel IP dalam file konfigurasi, misalnya, `169.254.44.233`.



4. Connect ke gateway keamanan AndaSSH. Jika Anda menggunakan shell non-default, ubah ke clish dengan menjalankan perintah berikut: `clish`
5. Untuk terowongan 1, jalankan perintah berikut.

```
set interface vpnt1 mtu 1436
```

Untuk terowongan 2, jalankan perintah berikut.

```
set interface vpnt2 mtu 1436
```

6. Ulangi langkah tersebut untuk membuat terowongan kedua, menggunakan informasi di bagian IPsec Tunnel #2 dari file konfigurasi.

Untuk mengonfigurasi rute statis

Pada langkah ini, tentukan rute statis ke subnet di VPC untuk setiap terowongan untuk memungkinkan Anda mengirim lalu lintas melalui antarmuka terowongan. Terowongan kedua memungkinkan failover jika terjadi masalah dengan terowongan pertama. Jika masalah terdeteksi, rute statis berbasis kebijakan akan dihapus dari tabel perutean, dan rute kedua diaktifkan. Anda

juga harus memungkinkan gateway Check Point untuk mengirim ping ke ujung lain terowongan untuk memeriksa apakah terowongan sudah siap.

1. Di portal Gaia, pilih Rute IPv4 Statis, Tambah.
2. Tentukan CIDR subnet Anda, misalnya, `10.28.13.0/24`.
3. Pilih Tambahkan Gateway, Alamat IP.
4. Masukkan alamat IP yang ditentukan untuk VGW Tunnel IP dalam file konfigurasi (misalnya, `169.254.44.233`), dan tentukan prioritas 1.
5. Pilih Ping.
6. Ulangi langkah 3 dan 4 untuk terowongan kedua, menggunakan nilai VGW Tunnel IP di bagian IPsec Tunnel #2 dari file konfigurasi. Tentukan prioritas 2.

Destination: 10.28.13.0/24

Next Hop Type: Normal

Normal: Accept and forward packets.
Reject: Drop packets, and send unreachable messages.
Black Hole: Drop packets, but don't send unreachable messages.

Rank: Default: 60

Local Scope:

Comment:

Add Gateway

Ping:

Gateway	Priority
169.254.44.233	1
169.254.44.5	2

Save Cancel

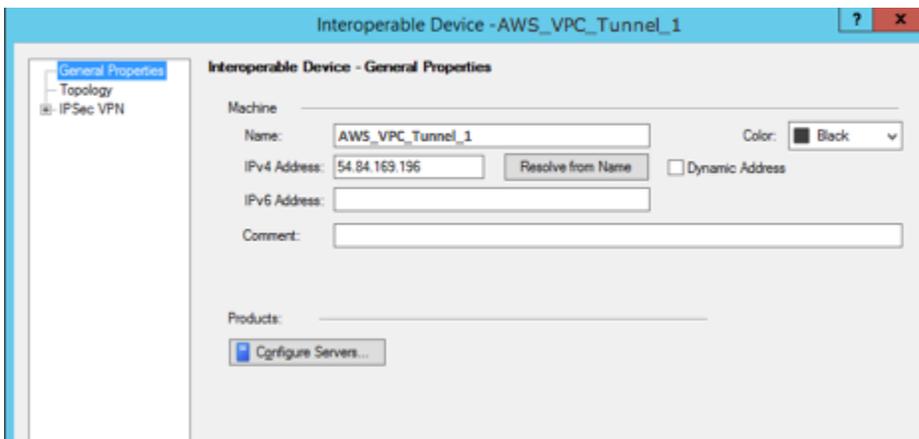
7. Pilih Simpan.

Jika Anda menggunakan klaster, ulangi langkah-langkah sebelumnya untuk anggota klaster lainnya.

Untuk menentukan objek jaringan baru

Pada langkah ini, Anda membuat objek jaringan untuk setiap VPN terowongan, menentukan alamat IP publik (luar) untuk gateway pribadi virtual. Anda kemudian menambahkan objek jaringan ini sebagai gateway satelit untuk komunitas AndaVPN. Anda juga perlu membuat grup kosong untuk bertindak sebagai placeholder untuk domain. VPN

1. Buka Check Point SmartDashboard.
2. Untuk Grup, buka menu konteks dan pilih Grup, Grup Sederhana. Anda dapat menggunakan grup yang sama untuk setiap objek jaringan.
3. Untuk Objek Jaringan, buka menu konteks (klik kanan) lalu pilih Baru, Perangkat Interoperasi.
4. Untuk Nama, masukkan nama yang Anda berikan untuk terowongan Anda, misalnya, AWS_VPC_Tunnel_1 atau AWS_VPC_Tunnel_2.
5. Untuk IPv4Alamat, masukkan alamat IP luar dari gateway pribadi virtual yang disediakan dalam file konfigurasi, misalnya, 54.84.169.196. Simpan pengaturan Anda dan tutup kotak dialog.



6. Di SmartDashboard, buka properti gateway Anda dan di panel kategori, pilih Topologi.
7. Untuk mengambil konfigurasi antarmuka, pilih Dapatkan Topologi.
8. Di bagian VPNDomain, pilih Ditentukan secara manual, lalu telusuri ke dan pilih grup sederhana kosong yang Anda buat di langkah 2. Pilih OKE.

Note

Anda dapat menyimpan VPN domain yang sudah ada yang telah Anda konfigurasi. Namun, pastikan bahwa host dan jaringan yang digunakan atau

dilayani oleh VPN koneksi baru tidak dinyatakan dalam VPN domain itu, terutama jika VPN domain tersebut diturunkan secara otomatis.

9. Ulangi langkah-langkah ini untuk membuat objek jaringan kedua, menggunakan informasi di bagian IPsec Tunnel #2 dari file konfigurasi.

 Note

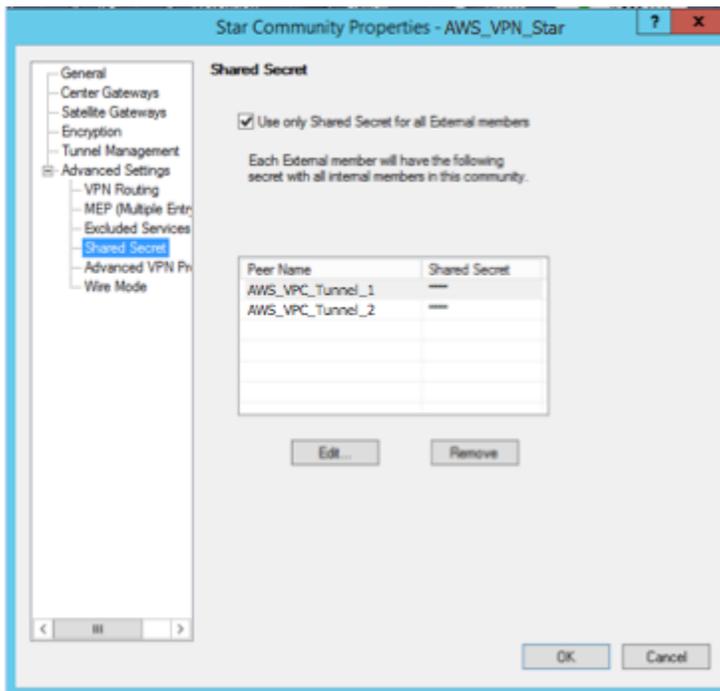
Jika Anda menggunakan kluster, edit topologi dan tentukan antarmuka sebagai antarmuka kluster. Gunakan alamat IP yang ditentukan dalam file konfigurasi.

Untuk membuat dan mengkonfigurasi VPN komunitas, IKE, dan IPsec pengaturan

Pada langkah ini, Anda membuat VPN komunitas di gateway Check Point Anda, tempat Anda menambahkan objek jaringan (perangkat yang dapat dioperasikan) untuk setiap terowongan. Anda juga mengonfigurasi Internet Key Exchange (IKE) dan IPsec pengaturan.

1. Dari properti gateway Anda, pilih IPsecVPN di panel kategori.
2. Pilih Komunitas, Baru, Komunitas Bintang.
3. Berikan nama untuk komunitas Anda (misalnya, `AWS_VPN_Star`), lalu pilih Gateway Pusat di panel kategori.
4. Pilih Tambahkan, dan tambahkan gateway atau kluster Anda ke daftar gateway peserta.
5. Di panel kategori, pilih Gateway Satelit, Tambahkan, lalu tambahkan perangkat interoperasi yang Anda buat sebelumnya (`AWS_VPC_Tunnel_1` dan `AWS_VPC_Tunnel_2`) ke daftar gateway peserta.
6. Di panel kategori, pilih Enkripsi. Di bagian Metode Enkripsi, pilih IKEv1 saja. Di bagian Suite Enkripsi, pilih Kustom, Enkripsi Kustom.
7. Pada kotak dialog, konfigurasi atribut enkripsi berikut, dan pilih OKE ketika Anda selesai:
 - IKE Properti Asosiasi Keamanan (Fase 1):
 - Lakukan enkripsi pertukaran kunci dengan: AES -128
 - Lakukan integritas data dengan: SHA -1
 - IPsec Properti Asosiasi Keamanan (Tahap 2):
 - Lakukan enkripsi IPsec data dengan: AES -128

- Lakukan integritas data dengan: SHA -1
8. Di panel kategori, pilih Manajemen Terowongan. Pilih Atur Terowongan Permanen, Di semua terowongan komunitas. Di bagian Berbagi VPN Tunnel, pilih Satu VPN terowongan per pasangan Gateway.
 9. Dalam panel kategori, perluas Pengaturan lanjutan, dan pilih Rahasia Bersama.
 10. Pilih nama peer untuk terowongan pertama, pilih Edit, dan kemudian masukkan kunci pra-berbagi seperti yang ditentukan dalam file konfigurasi di bagian IPsec Tunnel #1.
 11. Pilih nama peer untuk terowongan kedua, pilih Edit, dan kemudian masukkan kunci pra-berbagi seperti yang ditentukan dalam file konfigurasi di bagian IPsec Tunnel #2.



12. Masih dalam kategori Advanced Settings, pilih Advanced VPN Properties, konfigurasi properti sebagai berikut, lalu pilih OK setelah selesai:

- IKE(Fase 1):
 - Gunakan grup Diffie-Hellman: Group 2
 - Negosiasi ulang asosiasi IKE keamanan setiap menit **480**
- IPsec(Tahap 2):
 - Pilih Gunakan Perfect Forward Secrecy
 - Gunakan grup Diffie-Hellman: Group 2
 - Negosiasi ulang asosiasi IPsec keamanan setiap detik **3600**

Untuk membuat aturan firewall

Pada langkah ini, Anda mengonfigurasi kebijakan dengan aturan firewall dan aturan pencocokan arah yang memungkinkan komunikasi antara jaringan lokal VPC dan jaringan lokal. Kemudian Anda menginstal kebijakan di gateway Anda.

1. Di bagian SmartDashboard, pilih Properti Global untuk gateway Anda. Di panel kategori, perluas VPN, dan pilih Advanced.
2. Pilih Aktifkan VPN Pencocokan Arah di VPN Kolom, dan simpan perubahan Anda.
3. Di dalam SmartDashboard, pilih Firewall, dan buat kebijakan dengan aturan berikut:
 - Memungkinkan VPC subnet untuk berkomunikasi dengan jaringan lokal melalui protokol yang diperlukan.
 - Memungkinkan jaringan lokal untuk berkomunikasi dengan VPC subnet melalui protokol yang diperlukan.
4. Buka menu konteks untuk sel di VPN kolom, dan pilih Edit Sel.
5. Di kotak dialog Ketentuan VPN Pencocokan, pilih Cocokkan lalu lintas ke arah ini saja. Buat aturan kesesuaian arah berikut dengan memilih Tambahkan untuk masing-masing, dan pilih OKE ketika Anda selesai:
 - `internal_clear > VPN komunitas (Komunitas VPN bintang yang Anda buat sebelumnya, misalnya, AWS_VPN_Star)`
 - `VPNkomunitas > VPN komunitas`
 - `VPNkomunitas > internal_clear`
6. Dalam SmartDashboard, pilih Kebijakan, Instal.
7. Di kotak dialog, pilih gateway Anda dan pilih OKE untuk menginstal kebijakan.

Untuk mengubah properti `tunnel_keepalive_method`

Gateway Check Point Anda dapat menggunakan Dead Peer Detection (DPD) untuk mengidentifikasi kapan IKE asosiasi sedang down. Untuk mengkonfigurasi terowongan permanen, terowongan permanen harus dikonfigurasi di AWS VPN komunitas (lihat Langkah 8).

Secara default, `tunnel_keepalive_method` properti untuk VPN gateway diatur ke `tunnel_test`. Anda harus mengubah nilai ke `dpd`. Setiap VPN gateway di VPN komunitas yang memerlukan DPD pemantauan harus dikonfigurasi dengan `tunnel_keepalive_method`

properti, termasuk VPN gateway pihak ketiga mana pun. Anda tidak dapat mengonfigurasi mekanisme pemantauan yang berbeda untuk gateway yang sama.

Anda dapat memperbarui `tunnel_keepalive_method` properti menggunakan `uiDBedit` alat G.

1. Buka Check Point SmartDashboard, dan pilih Security Management Server, Domain Management Server.
2. Pilih File, Kontrol Revisi Basis Data... dan buat snapshot revisi.
3. Tutup semua SmartConsole jendela, seperti, SmartView Tracker SmartDashboard, dan SmartView Monitor.
4. Mulai `uiDBedit` alat G. Untuk informasi selengkapnya, lihat artikel [Alat Basis Data Check Point](#) di Pusat Dukungan Check Point.
5. Pilih Server Manajemen Keamanan, Server Manajemen Domain.
6. Di panel kiri atas, pilih Tabel, Objek Jaringan, `network_objects`.
7. Pada panel kanan atas, pilih Gateway Keamanan yang relevan, objek Klaster.
8. Tekan CTRL +F, atau gunakan menu Pencarian untuk mencari yang berikut:`tunnel_keepalive_method`.
9. Pada panel bawah, buka menu konteks untuk `tunnel_keepalive_method`, dan pilih Edit.... Pilih `dpd` lalu pilih OKE.
10. Ulangi langkah 7 hingga 9 untuk setiap gateway yang merupakan bagian dari AWS VPN Komunitas.
11. Pilih File, Simpan Semua.
12. Tutup `uiDBedit` alat G.
13. Buka Check Point SmartDashboard, dan pilih Security Management Server, Domain Management Server.
14. Instal kebijakan pada Gateway Keamanan yang relevan, objek Klaster.

Untuk informasi selengkapnya, lihat artikel [VPNFitur baru di R77.10](#) di Pusat Dukungan Check Point.

Untuk mengaktifkan TCP MSS penjepitan

TCPMSSpenjepitan mengurangi ukuran segmen maksimum TCP paket untuk mencegah fragmentasi paket.

1. Navigasikan ke direktori berikut: C:\Program Files (x86)\CheckPoint\SmartConsole\R77.10\PROGRAM\.
2. Buka Alat Basis Data Check Point dengan menjalankan file GuidBEdit.exe.
3. Pilih Tabel, Properti Global, properti.
4. Untuk fw_clamp_tcp_mss, pilih Edit. Ubah nilai ke true dan pilih OKE.

Untuk memverifikasi status terowongan

Anda dapat memverifikasi status terowongan dengan menjalankan perintah berikut dari alat baris perintah dalam mode ahli.

```
vpn tunnelutil
```

Dalam opsi yang ditampilkan, pilih 1 untuk memverifikasi IKE asosiasi dan 2 untuk memverifikasi IPsec asosiasi.

Anda juga dapat menggunakan Check Point Smart Tracker Log untuk memverifikasi bahwa paket yang melalui koneksi sedang dienkripsi. Misalnya, log berikut menunjukkan bahwa paket ke dikirim melalui terowongan 1 dan dienkripsi. VPC

Log Info		Rule	
Product	Security Gateway/Management	Action	Encrypt
Date	4Nov2015	Rule	4
Time	9:42:01	Current Rule Number	4-Standard
Number	21254	Rule Name	---
Type	Log	User	---
Origin	cpgw-997695	More	
Traffic		Rule UID	{0AA18015-FF7B-4650-B0CE-3989E658CF04}
Source	Management_PC (192.168.1.116)	Community	AWS_VPN_Star
Destination	10.28.13.28	Encryption Scheme	IKE
Service	---	Data Encryption Methods	ESP: AES-128 + SHA1 + PFS (group 2)
Protocol	icmp	VPN Peer Gateway	AWS_VPC_Tunnel_1 (54.84.169.196)
Interface	eth0	Subproduct	VPN
Source Port	---	VPN Feature	VPN
Policy		Product Family	Network
Policy Name	Standard	Information	service_id: icmp-proto ICMP: Echo Request ICMP Type: 8 ICMP Code: 0
Policy Date	Tue Nov 03 11:33:45 2015		
Policy Management	cpgw-997695		

SonicWALL

Prosedur berikut menunjukkan cara mengkonfigurasi VPN terowongan pada WALL perangkat Sonic menggunakan antarmuka manajemen SonicOS.

Untuk mengonfigurasi terowongan

1. Buka antarmuka manajemen Sonic WALL SonicOS.
2. Di panel kiri, pilih VPN, Pengaturan. Di bawah VPNKebijakan, pilih Tambah... .
3. Di jendela VPN kebijakan pada tab Umum, lengkapi informasi berikut:
 - Jenis Kebijakan: Pilih Antarmuka Terowongan.
 - Metode Otentikasi: Pilih IKEmenggunakan Rahasia Preshared.
 - Nama: Masukkan nama untuk VPN kebijakan. Kami menyarankan Anda menggunakan nama VPN ID, seperti yang disediakan dalam file konfigurasi.
 - IPsecNama atau Alamat Gateway Utama: Masukkan alamat IP gateway pribadi virtual seperti yang disediakan dalam file konfigurasi (misalnya,72 . 21 . 209 . 193).
 - IPsecNama atau Alamat Gerbang Sekunder: Tinggalkan nilai default.
 - Rahasia Bersama: Masukkan kunci pra-berbagi seperti yang disediakan dalam file konfigurasi, dan masukkan kembali di Konfirmasi Rahasia Bersama.
 - IKEID Lokal: Masukkan IPv4 alamat gateway pelanggan (WALLperangkat Sonic).
 - Peer IKE ID: Masukkan IPv4 alamat gateway pribadi virtual.
4. Pada tab Jaringan, lengkapi informasi berikut:
 - Di bawah Jaringan Lokal, pilih Alamat apa pun. Kami merekomendasikan opsi ini untuk mencegah masalah konektivitas dari jaringan lokal Anda.
 - Di bawah Jaringan Jarak Jauh, pilih Pilih jaringan tujuan dari daftar. Buat objek alamat dengan CIDR VPC in Anda AWS.
5. Pada tab Proposal, lengkapi informasi berikut:
 - Di bawah Proposal IKE (Fase 1), lakukan hal berikut:
 - Pertukaran: Pilih Mode Utama.
 - Grup DH: Masukkan nilai untuk grup Diffie-Hellman (misalnya, 2).
 - Enkripsi: Pilih AES-128 atau AES-256.
 - Otentikasi: Pilih SHA1atau SHA256.

- Waktu Hidup: Masukkan 28800.
- Di bawah Proposal IKE (Tahap 2), lakukan hal berikut:
 - Protokol: Pilih ESP.
 - Enkripsi: Pilih AES-128 atau AES-256.
 - Otentikasi: Pilih SHA1 atau SHA256.
 - Pilih kotak centang Aktifkan Perfect Forward Secrecy, lalu pilih grup Diffie-Hellman.
 - Waktu Hidup: Masukkan 3600.

 Important

Jika Anda membuat gateway pribadi virtual sebelum Oktober 2015, Anda harus menentukan Diffie-Hellman grup 2, AES -128, dan untuk kedua fase. SHA1

6. Pada tab Lanjutan, lengkapi informasi berikut:
 - Pilih Aktifkan Tetap Aktif.
 - Pilih Aktifkan Tahap2 Deteksi Peer Mati dan masukkan hal berikut:
 - Untuk Interval Deteksi Rekan Mati, masukkan 60 (ini adalah minimum yang diterima WALL perangkat Sonic).
 - Untuk Tingkat Pemicu Kegagalan, masukkan 3.
 - Untuk VPNKebijakan terikat, pilih Antarmuka X1. Ini adalah antarmuka yang biasanya ditujukan untuk alamat IP publik.
7. Pilih OKE. Pada halaman Pengaturan, Aktifkan kotak centang untuk terowongan yang harus dipilih secara default. Tanda titik hijau menunjukkan bahwa terowongan sudah siap.

Informasi tambahan untuk perangkat Cisco

Beberapa Cisco ASAs hanya mendukung mode Aktif/Siaga. Ketika Anda menggunakan Cisco iniASAs, Anda hanya dapat memiliki satu terowongan aktif pada satu waktu. Terowongan siaga lainnya menjadi aktif jika terowongan pertama menjadi tidak tersedia. Dengan redundansi ini, Anda harus selalu memiliki konektivitas ke Anda VPC melalui salah satu terowongan.

Cisco ASAs dari versi 9.7.1 dan yang lebih baru mendukung mode Aktif/Aktif. Saat Anda menggunakan Cisco iniASAs, Anda dapat mengaktifkan kedua terowongan secara bersamaan.

Dengan redundansi ini, Anda harus selalu memiliki konektivitas ke Anda VPC melalui salah satu terowongan.

Untuk perangkat Cisco, Anda harus melakukan hal berikut:

- Konfigurasi antarmuka luar.
- Pastikan nomor Urutan ISAKMP Kebijakan Crypto unik.
- Pastikan bahwa nomor Urutan Kebijakan Daftar Crypto unik.
- Pastikan bahwa Crypto IPsec Transform Set dan Crypto ISAKMP Policy Sequence selaras dengan IPsec terowongan lain yang dikonfigurasi pada perangkat.
- Pastikan nomor SLA pemantauan unik.
- Konfigurasi semua perutean internal yang memindahkan lalu lintas antara perangkat gateway pelanggan dan jaringan lokal Anda.

Contoh konfigurasi perangkat gateway pelanggan untuk perutean dinamis

Untuk mengunduh file konfigurasi sampel dengan nilai khusus untuk konfigurasi VPN koneksi Site-to-Site Anda, gunakan VPC konsol Amazon, baris AWS perintah, atau Amazon. EC2 API Untuk informasi selengkapnya, lihat [Langkah 6: Unduh file konfigurasi](#).

[Anda juga dapat mengunduh file konfigurasi contoh umum untuk perutean dinamis yang tidak menyertakan nilai khusus untuk konfigurasi koneksi Site-to-Site VPN Anda: `.zip dynamic-routing-examples`](#)

File menggunakan nilai placeholder untuk beberapa komponen. Misalnya, menggunakan:

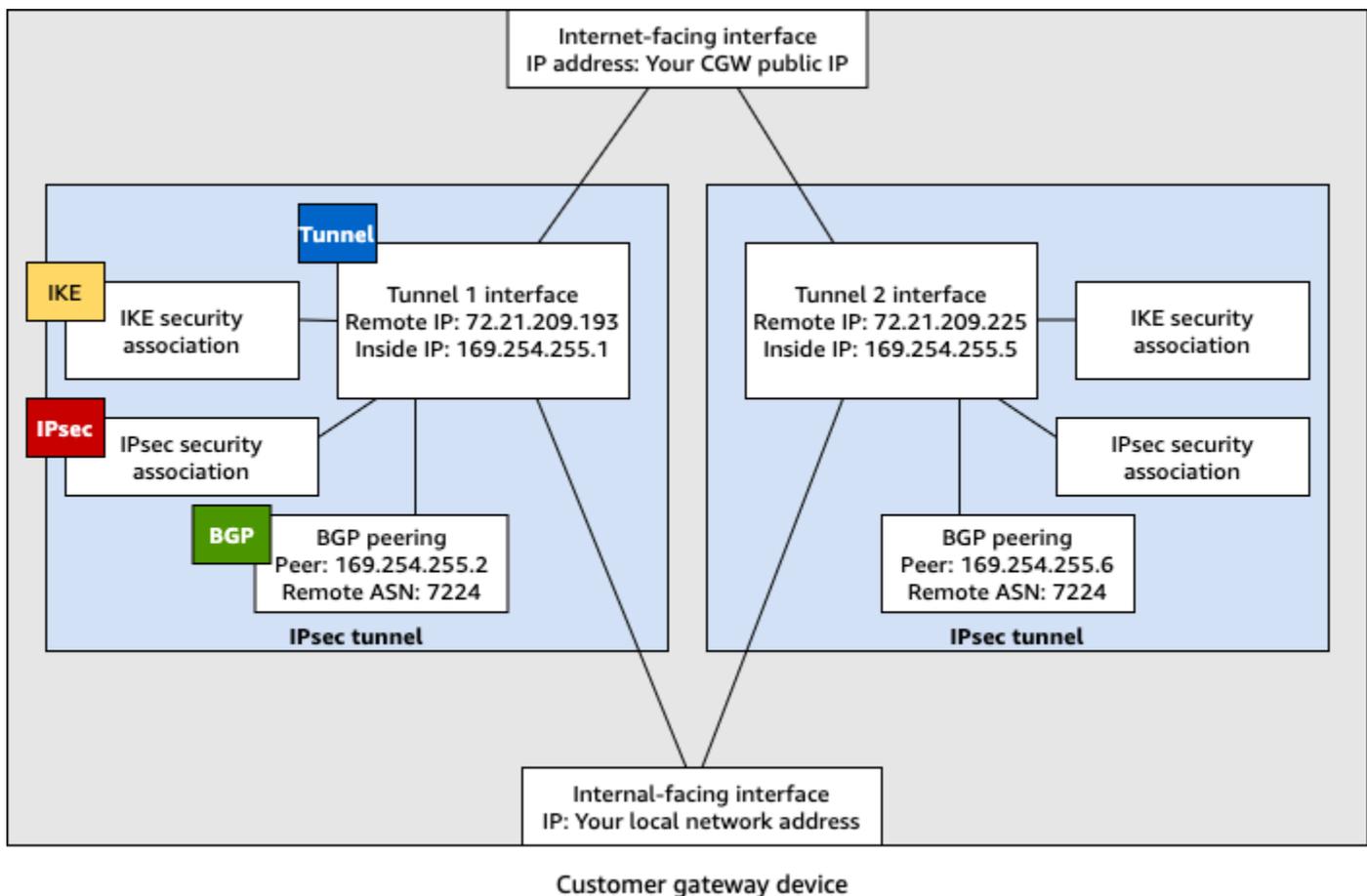
- Contoh nilai untuk ID VPN koneksi, ID gateway pelanggan, dan ID gateway pribadi virtual
- Placeholder untuk titik akhir alamat AWS IP jarak jauh (luar) (*AWS_ENDPOINT_1* and *AWS_ENDPOINT_2*)
- Placeholder untuk alamat IP untuk antarmuka eksternal yang dapat dirutekan internet pada perangkat gateway pelanggan (*your-cgw-ip-address*)
- Placeholder untuk nilai kunci yang telah dibagikan sebelumnya () pre-shared-key
- Contoh nilai terowongan di dalam alamat IP.
- Contoh nilai untuk MTU pengaturan.

Note

MTU pengaturan yang disediakan dalam file konfigurasi sampel adalah contoh saja. Silakan merujuk ke [Praktik terbaik untuk perangkat gateway pelanggan Anda](#) untuk informasi tentang pengaturan MTU nilai optimal untuk situasi Anda.

Selain memberikan nilai placeholder, file menentukan persyaratan minimum untuk VPN koneksi Site-to-Site dari, dan Diffie-Hellman grup 2 di sebagian besar AWS Wilayah AES128SHA1, dan, dan Diffie-Hellman grup 14 di Wilayah. AES128 SHA2 AWS GovCloud File juga menentukan kunci pra-berbagi untuk [autentikasi](#). Anda harus memodifikasi contoh file konfigurasi untuk memanfaatkan algoritma keamanan tambahan, grup Diffie-Hellman, sertifikat pribadi, dan lalu lintas. IPv6

Diagram berikut memberikan gambaran umum mengenai komponen berbeda yang dikonfigurasi di perangkat gateway pelanggan. Ini termasuk contoh nilai untuk antarmuka terowongan alamat IP.



Prosedur antarmuka pengguna untuk perutean dinamis

Berikut ini adalah beberapa contoh prosedur untuk mengonfigurasi perangkat gateway pelanggan menggunakan antarmuka pengguna (jika ada).

Check Point

Berikut ini adalah langkah-langkah untuk mengonfigurasi perangkat Check Point Security Gateway yang menjalankan R77.10 atau lebih tinggi, menggunakan portal web Gaia dan Check Point. SmartDashboard Anda juga dapat merujuk ke VPN BGP artikel [Amazon Web Services \(AWS\)](#) di Pusat Dukungan Check Point.

Untuk mengonfigurasi antarmuka terowongan

Langkah pertama adalah membuat VPN terowongan dan menyediakan alamat IP pribadi (dalam) dari gateway pelanggan dan gateway pribadi virtual untuk setiap terowongan. Untuk membuat terowongan pertama, gunakan informasi yang disediakan di bagian IPsec Tunnel #1 dari file konfigurasi. Untuk membuat terowongan kedua, gunakan nilai yang disediakan di bagian IPsec Tunnel #2 dari file konfigurasi.

1. Connect ke gateway keamanan AndaSSH. Jika Anda menggunakan shell non-default, ubah ke clish dengan menjalankan perintah berikut: `clish`
2. Tetapkan gateway pelanggan ASN (ASNyang disediakan saat gateway pelanggan dibuat AWS) dengan menjalankan perintah berikut.

```
set as 65000
```

3. Buat antarmuka terowongan untuk terowongan pertama, menggunakan informasi yang disediakan di bagian IPsec Tunnel #1 dari file konfigurasi. Berikan nama yang unik untuk terowongan Anda, seperti `AWS_VPC_Tunnel_1`.

```
add vpn tunnel 1 type numbered local 169.254.44.234 remote 169.254.44.233
peer AWS_VPC_Tunnel_1
set interface vpnt1 state on
set interface vpnt1 mtu 1436
```

4. Ulangi perintah ini untuk membuat terowongan kedua, menggunakan informasi yang disediakan di bagian IPsec Tunnel #2 dari file konfigurasi. Berikan nama unik untuk terowongan Anda, seperti `AWS_VPC_Tunnel_2`.

```
add vpn tunnel 1 type numbered local 169.254.44.38 remote 169.254.44.37
peer AWS_VPC_Tunnel_2
set interface vpnt2 state on
set interface vpnt2 mtu 1436
```

5. Atur gateway pribadi virtualASN.

```
set bgp external remote-as 7224 on
```

6. Konfigurasi BGP untuk terowongan pertama, menggunakan IPsec Tunnel #1 bagian informasi yang disediakan dari file konfigurasi.

```
set bgp external remote-as 7224 peer 169.254.44.233 on
set bgp external remote-as 7224 peer 169.254.44.233 holdtime 30
set bgp external remote-as 7224 peer 169.254.44.233 keepalive 10
```

7. Konfigurasi BGP untuk terowongan kedua, menggunakan IPsec Tunnel #2 bagian informasi yang disediakan dari file konfigurasi.

```
set bgp external remote-as 7224 peer 169.254.44.37 on
set bgp external remote-as 7224 peer 169.254.44.37 holdtime 30
set bgp external remote-as 7224 peer 169.254.44.37 keepalive 10
```

8. Simpan konfigurasi.

```
save config
```

Untuk membuat BGP kebijakan

Selanjutnya, buat BGP kebijakan yang memungkinkan impor rute yang diiklankan oleh AWS. Kemudian, konfigurasi gateway pelanggan Anda untuk me-notice rute lokal ke AWS.

1. Dalam Gaia WebUI, pilih Perutean Lanjutan, Filter Rute Inbound. Pilih Tambah, dan pilih Tambah BGP Kebijakan (Berdasarkan AS).
2. Untuk Tambahkan BGP Kebijakan, pilih nilai antara 512 dan 1024 di bidang pertama, dan masukkan gateway pribadi virtual ASN di bidang kedua (misalnya,7224).
3. Pilih Simpan.

Untuk me-notice rute lokal

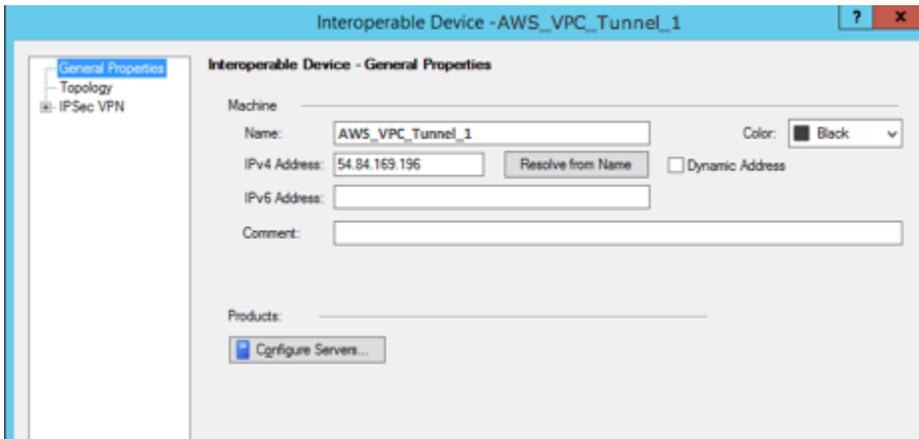
Langkah-langkah berikut adalah cara untuk mendistribusikan rute antarmuka lokal. Anda juga dapat mendistribusikan rute dari sumber yang berbeda (misalnya, rute statis, atau rute yang diperoleh melalui protokol perutean dinamis). Untuk informasi lebih lanjut, lihat [Perutean Lanjutan Gaia R77 Versi Panduan Administrasi](#).

1. Dalam Gaia WebUI, pilih Perutean Lanjutan, Redistribusi Perutean. Pilih Menambahkan Redistribusi Dari dan kemudian pilih Antarmuka.
2. Untuk To Protocol, pilih gateway pribadi virtual ASN (misalnya,7224).
3. Untuk Antarmuka, pilih antarmuka internal. Pilih Simpan.

Untuk menentukan objek jaringan baru

Selanjutnya, buat objek jaringan untuk setiap VPN terowongan, tentukan alamat IP publik (luar) untuk gateway pribadi virtual. Anda kemudian menambahkan objek jaringan ini sebagai gateway satelit untuk komunitas AndaVPN. Anda juga perlu membuat grup kosong untuk bertindak sebagai placeholder untuk domain. VPN

1. Buka Check Point SmartDashboard.
2. Untuk Grup, buka menu konteks dan pilih Grup, Grup Sederhana. Anda dapat menggunakan grup yang sama untuk setiap objek jaringan.
3. Untuk Objek Jaringan, buka menu konteks (klik kanan) dan pilih Baru, Perangkat yang dapat dioperasikan.
4. Untuk Nama, masukkan nama yang Anda berikan untuk terowongan pada langkah 1, misalnya, AWS_VPC_Tunnel_1 atau AWS_VPC_Tunnel_2.
5. Untuk IPv4Alamat, masukkan alamat IP luar dari gateway pribadi virtual yang disediakan dalam file konfigurasi, misalnya,54.84.169.196. Simpan pengaturan Anda dan tutup kotak dialog.



6. Di panel kategori sebelah kiri, pilih Topologi.
7. Di bagian VPNDomain, pilih Ditentukan secara manual, lalu telusuri ke dan pilih grup sederhana kosong yang Anda buat di langkah 2. Pilih OKE.
8. Ulangi langkah-langkah ini untuk membuat objek jaringan kedua, menggunakan informasi di bagian IPsec Tunnel #2 dari file konfigurasi.
9. Pergi ke objek jaringan gateway Anda, buka gateway atau objek klaster, dan pilih Topologi.
10. Di bagian VPNDomain, pilih Ditentukan secara manual, lalu telusuri ke dan pilih grup sederhana kosong yang Anda buat di langkah 2. Pilih OKE.

Note

Anda dapat menyimpan VPN domain yang sudah ada yang telah Anda konfigurasi. Namun, pastikan bahwa host dan jaringan yang digunakan atau dilayani oleh VPN koneksi baru tidak dinyatakan dalam VPN domain itu, terutama jika VPN domain tersebut diturunkan secara otomatis.

Note

Jika Anda menggunakan klaster, edit topologi dan tentukan antarmuka sebagai antarmuka klaster. Gunakan alamat IP yang ditentukan dalam file konfigurasi.

Untuk membuat dan mengkonfigurasi VPN komunitas, IKE, dan IPsec pengaturan

Selanjutnya, buat VPN komunitas di gateway Check Point Anda, tempat Anda menambahkan objek jaringan (perangkat yang dapat dioperasikan) untuk setiap terowongan. Anda juga mengonfigurasi Internet Key Exchange (IKE) dan IPsec pengaturan.

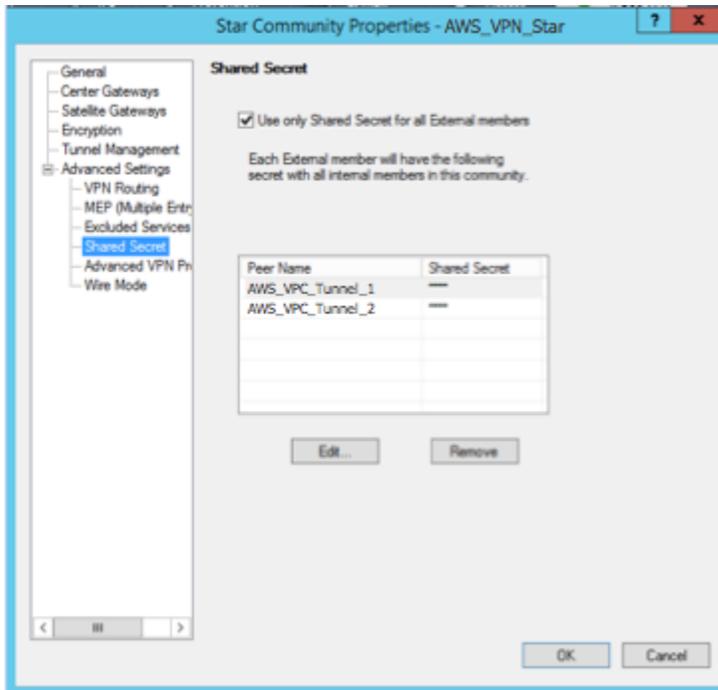
1. Dari properti gateway Anda, pilih IPsecVPN di panel kategori.
2. Pilih Komunitas, Baru, Komunitas Bintang.
3. Berikan nama untuk komunitas Anda (misalnya, `AWS_VPN_Star`), lalu pilih Gateway Pusat di panel kategori.
4. Pilih Tambahkan, dan tambahkan gateway atau kluster Anda ke daftar gateway peserta.
5. Di panel kategori, pilih Gateway satelit, Tambahkan, dan tambahkan perangkat interoperable yang Anda buat sebelumnya (`AWS_VPC_Tunnel_1` dan `AWS_VPC_Tunnel_2`) ke daftar gateway peserta.
6. Di panel kategori, pilih Enkripsi. Di bagian Metode Enkripsi, pilih IKEv1 untuk IPv4 dan IKEv2 untuk IPv6. Di bagian Suite Enkripsi, pilih Kustom, Enkripsi Kustom.

 Note

Anda harus memilih IPv6 opsi IKEv1 untuk IPv4 dan IKEv2 untuk IKEv1 fungsionalitas.

7. Di kotak dialog, konfigurasi properti enkripsi sebagai berikut, kemudian pilih OKE ketika Anda selesai:
 - IKE Properti Asosiasi Keamanan (Fase 1):
 - Lakukan enkripsi pertukaran kunci dengan: AES -128
 - Lakukan integritas data dengan: SHA -1
 - IPsec Properti Asosiasi Keamanan (Fase 2):
 - Lakukan enkripsi IPsec data dengan: AES -128
 - Lakukan integritas data dengan: SHA -1
8. Di panel kategori, pilih Manajemen Terowongan. Pilih Atur Terowongan Permanen, Di semua terowongan komunitas. Di bagian Berbagi VPN Tunnel, pilih Satu VPN terowongan per pasangan Gateway.
9. Dalam panel kategori, perluas Pengaturan lanjutan, dan pilih Rahasia Bersama.

10. Pilih nama peer untuk terowongan pertama, pilih Edit, dan kemudian masukkan kunci pra-berbagi seperti yang ditentukan dalam file konfigurasi di bagian IPsec Tunnel #1.
11. Pilih nama peer untuk terowongan kedua, pilih Edit, dan kemudian masukkan kunci pra-berbagi seperti yang ditentukan dalam file konfigurasi di bagian IPsec Tunnel #2.



12. Masih dalam kategori Advanced Settings, pilih Advanced VPN Properties, konfigurasi properti sebagai berikut, lalu pilih OK setelah selesai:

- IKE(Fase 1):
 - Gunakan grup Diffie-Hellman: Group 2 (1024 bit)
 - Negosiasi ulang asosiasi IKE keamanan setiap menit **480**
- IPsec(Fase 2):
 - Pilih Gunakan Perfect Forward Secrecy
 - Gunakan grup Diffie-Hellman: Group 2 (1024 bit)
 - Negosiasi ulang asosiasi IPsec keamanan setiap detik **3600**

Untuk membuat aturan firewall

Selanjutnya, konfigurasi kebijakan dengan aturan firewall dan aturan pencocokan arah yang memungkinkan komunikasi antara jaringan lokal VPC dan jaringan lokal. Kemudian Anda menginstal kebijakan di gateway Anda.

1. Dalam SmartDashboard, pilih Global Properties untuk gateway Anda. Di panel kategori, perluas VPN, dan pilih Advanced.
2. Pilih Aktifkan VPN Pencocokan Arah di VPN Kolom, dan pilih OK.
3. Di dalam SmartDashboard, pilih Firewall, dan buat kebijakan dengan aturan berikut:
 - Izinkan VPC subnet untuk berkomunikasi dengan jaringan lokal melalui protokol yang diperlukan.
 - Izinkan jaringan lokal untuk berkomunikasi dengan VPC subnet melalui protokol yang diperlukan.
4. Buka menu konteks untuk sel di VPN kolom, dan pilih Edit Sel.
5. Di kotak dialog Ketentuan VPN Pencocokan, pilih Cocokkan lalu lintas ke arah ini saja. Buat aturan kecocokan terarah berikut dengan memilih Tambahkan untuk masing-masing, dan kemudian pilih OKE ketika Anda selesai:
 - `internal_clear` > VPN komunitas (Komunitas VPN bintang yang Anda buat sebelumnya, misalnya, `AWS_VPN_Star`)
 - VPNkomunitas > VPN komunitas
 - VPNkomunitas > `internal_clear`
6. Dalam SmartDashboard, pilih Kebijakan, Instal.
7. Di kotak dialog, pilih gateway Anda dan pilih OKE untuk menginstal kebijakan.

Untuk mengubah properti `tunnel_keepalive_method`

Gateway Check Point Anda dapat menggunakan Dead Peer Detection (DPD) untuk mengidentifikasi kapan IKE asosiasi sedang down. DPD untuk mengkonfigurasi terowongan permanen, terowongan permanen harus dikonfigurasi di AWS VPN komunitas.

Secara default, `tunnel_keepalive_method` properti untuk VPN gateway diatur ke `tunnel_test`. Anda harus mengubah nilai ke `dpd`. Setiap VPN gateway di VPN komunitas yang memerlukan DPD pemantauan harus dikonfigurasi dengan `tunnel_keepalive_method` properti, termasuk VPN gateway pihak ketiga mana pun. Anda tidak dapat mengonfigurasi mekanisme pemantauan yang berbeda untuk gateway yang sama.

Anda dapat memperbarui `tunnel_keepalive_method` properti menggunakan `uiDBedit` alat G.

1. Buka Check Point SmartDashboard, dan pilih Security Management Server, Domain Management Server.

2. Pilih File, Kontrol Revisi Basis Data... dan buat snapshot revisi.
3. Tutup semua SmartConsole jendela, seperti, SmartView Tracker SmartDashboard, dan SmartView Monitor.
4. Mulai uiBDedit alat G. Untuk informasi selengkapnya, lihat artikel [Alat Basis Data Check Point](#) di Pusat Dukungan Check Point.
5. Pilih Server Manajemen Keamanan, Server Manajemen Domain.
6. Di panel kiri atas, pilih Tabel, Objek Jaringan, network_objects.
7. Pada panel kanan atas, pilih Gateway Keamanan yang relevan, objek Klaster.
8. Tekan CTRL +F, atau gunakan menu Pencarian untuk mencari yang berikut:
tunnel_keepalive_method
9. Pada panel bawah, buka menu konteks untuk tunnel_keepalive_method, dan pilih Sunting.... Pilih dpd, OKE.
10. Ulangi langkah 7 hingga 9 untuk setiap gateway yang merupakan bagian dari AWS VPN Komunitas.
11. Pilih File, Simpan Semua.
12. Tutup uiBDedit alat G.
13. Buka Check Point SmartDashboard, dan pilih Security Management Server, Domain Management Server.
14. Instal kebijakan pada Gateway Keamanan yang relevan, objek Klaster.

Untuk informasi selengkapnya, lihat artikel [VPNFitur baru di R77.10](#) di Pusat Dukungan Check Point.

Untuk mengaktifkan TCP MSS penjepitan

TCPMSSpenjepitan mengurangi ukuran segmen maksimum TCP paket untuk mencegah fragmentasi paket.

1. Navigasikan ke direktori berikut: C:\Program Files (x86)\CheckPoint\SmartConsole\R77.10\PROGRAM\.
2. Buka Alat Basis Data Check Point dengan menjalankan file GuiDBedit.exe.
3. Pilih Tabel, Properti Global, properti.
4. Untuk fw_clamp_tcp_mss, pilih Sunting. Ubah nilai ke true lalu pilih OKE.

Untuk memverifikasi status terowongan

Anda dapat memverifikasi status terowongan dengan menjalankan perintah berikut dari alat baris perintah dalam mode ahli.

```
vpn tunnelutil
```

Dalam opsi yang ditampilkan, pilih 1 untuk memverifikasi IKE asosiasi dan 2 untuk memverifikasi IPsec asosiasi.

Anda juga dapat menggunakan Check Point Smart Tracker Log untuk memverifikasi bahwa paket yang melalui koneksi sedang dienkripsi. Misalnya, log berikut menunjukkan bahwa paket ke dikirim melalui terowongan 1 dan dienkripsi. VPC

Log Info		Rule	
Product	Security Gateway/Management	Action	Encrypt
Date	4Nov2015	Rule	4
Time	9:42:01	Current Rule Number	4-Standard
Number	21254	Rule Name	---
Type	Log	User	---
Origin	cpgw-997695	More	
Traffic		Rule UID	{0AA18015-FF7B-4650-B0CE-3989E658CF04}
Source	Management_PC (192.168.1.116)	Community	AWS_VPN_Star
Destination	10.28.13.28	Encryption Scheme	IKE
Service	---	Data Encryption Methods	ESP: AES-128 + SHA1 + PFS (group 2)
Protocol	icmp	VPN Peer Gateway	AWS_VPC_Tunnel_1 (54.84.169.196)
Interface	eth0	Subproduct	VPN
Source Port	---	VPN Feature	VPN
Policy		Product Family	Network
Policy Name	Standard	Information	service_id: icmp-proto ICMP: Echo Request ICMP Type: 8 ICMP Code: 0
Policy Date	Tue Nov 03 11:33:45 2015		
Policy Management	cpgw-997695		

SonicWALL

Anda dapat mengonfigurasi WALL perangkat Sonic menggunakan antarmuka manajemen SonicOS. Untuk informasi selengkapnya tentang mengonfigurasi terowongan, lihat [Prosedur antarmuka pengguna untuk perutean statis](#).

Anda tidak dapat mengonfigurasi BGP untuk perangkat menggunakan antarmuka manajemen. Sebagai gantinya, gunakan instruksi baris perintah yang disediakan dalam file konfigurasi contoh, di bawah bagian bernama BGP.

Informasi tambahan untuk perangkat Cisco

Beberapa Cisco ASAs hanya mendukung mode Aktif/Siaga. Ketika Anda menggunakan Cisco iniASAs, Anda hanya dapat memiliki satu terowongan aktif pada satu waktu. Terowongan siaga lainnya menjadi aktif jika terowongan pertama menjadi tidak tersedia. Dengan redundansi ini, Anda harus selalu memiliki konektivitas ke Anda VPC melalui salah satu terowongan.

Cisco ASAs dari versi 9.7.1 dan yang lebih baru mendukung mode Aktif/Aktif. Saat Anda menggunakan Cisco iniASAs, Anda dapat mengaktifkan kedua terowongan secara bersamaan. Dengan redundansi ini, Anda harus selalu memiliki konektivitas ke Anda VPC melalui salah satu terowongan.

Untuk perangkat Cisco, Anda harus melakukan hal berikut:

- Konfigurasi antarmuka luar.
- Pastikan nomor Urutan ISAKMP Kebijakan Crypto unik.
- Pastikan bahwa nomor Urutan Kebijakan Daftar Crypto unik.
- Pastikan bahwa Crypto IPsec Transform Set dan Crypto ISAKMP Policy Sequence selaras dengan IPsec terowongan lain yang dikonfigurasi pada perangkat.
- Pastikan nomor SLA pemantauannya unik.
- Mengonfigurasi semua perutean internal yang memindahkan lalu lintas antara perangkat gateway pelanggan dan jaringan lokal Anda.

Informasi tambahan untuk perangkat Juniper

Informasi berikut berlaku untuk contoh file konfigurasi untuk Juniper J-Series dan perangkat gateway SRX pelanggan.

- Antarmuka luar disebut sebagai *ge-0/0/0.0*.
- Antarmuka IDs terowongan disebut sebagai *st0.1* and *st0.2*.
- Pastikan bahwa Anda mengidentifikasi zona keamanan untuk antarmuka uplink (informasi konfigurasi menggunakan default zona 'tidak andal').

- Pastikan bahwa Anda mengidentifikasi zona keamanan untuk antarmuka bagian dalam (informasi konfigurasi menggunakan default zona 'andal').

Mengonfigurasi Windows Server sebagai perangkat gateway pelanggan

Anda dapat mengonfigurasi server yang menjalankan Windows Server sebagai perangkat gateway pelanggan untuk VPC Anda. Gunakan proses berikut agar Anda dapat menjalankan Windows Server pada instans EC2 di VPC, atau di server Anda sendiri. Prosedur berikut berlaku untuk Windows Server 2012 R2 dan versi yang lebih baru.

Daftar Isi

- [Mengonfigurasi instans Windows Anda](#)
- [Langkah 1: Buat koneksi VPN dan konfigurasi VPC Anda](#)
- [Langkah 2: Unduh file konfigurasi untuk koneksi VPN](#)
- [Langkah 3: Mengonfigurasi Windows Server](#)
- [Langkah 4: Mengatur terowongan VPN](#)
- [Langkah 5: Aktifkan deteksi gateway mati](#)
- [Langkah 6: Uji koneksi VPN](#)

Mengonfigurasi instans Windows Anda

Jika Anda mengonfigurasi Windows Server pada instans EC2 yang diluncurkan dari Windows AMI, lakukan hal berikut:

- Nonaktifkan pemeriksaan sumber/tujuan untuk instans tersebut:
 1. Buka konsol Amazon EC2 di <https://console.aws.amazon.com/ec2/>.
 2. Pilih instans Windows Anda, dan pilih Tindakan, Jaringan, Ubah pemeriksaan sumber/tujuan. Pilih Berhenti, lalu pilih Simpan.
- Perbarui pengaturan adaptor Anda sehingga Anda dapat merutekan lalu lintas dari instans lain:
 1. Hubungkan ke instans Windows Anda. Untuk informasi selengkapnya, lihat [Menghubungkan ke instans Windows Anda](#).
 2. Buka Panel Kontrol, dan mulai Device Manager.

3. Perluas simpul Adaptor jaringan.
 4. Pilih adaptor jaringan (tergantung pada tipe instans, mungkin Amazon Elastic Network Adapter atau Intel 82599 Virtual Function), dan pilih Tindakan, Properti.
 5. Pada tab Lanjutan, nonaktifkan properti IPv4 Checksum Offload, TCP Checksum Offload (IPv4), dan UDP Checksum Offload (IPv4), lalu pilih OKE.
- Alokasikan alamat IP Elastis ke akun Anda dan asosiasikan dengan instans Anda. Untuk informasi selengkapnya, lihat [Bekerja dengan alamat IP Elastis](#). Catat alamat ini — Anda memerlukannya saat membuat gateway pelanggan di VPC Anda.
 - Pastikan bahwa aturan instans grup keamanan mengizinkan lalu lintas IPsec keluar. Secara default, grup keamanan mengizinkan semua lalu lintas ke luar. Namun, jika aturan keluar grup keamanan telah diubah dari status aslinya, Anda harus membuat aturan protokol kustom keluar berikut untuk lalu lintas IPsec: protokol IP 50, protokol IP 51, dan UDP 500.

Perhatikan rentang CIDR dari jaringan tempat instans Windows Anda berada, misalnya, 172.31.0.0/16.

Langkah 1: Buat koneksi VPN dan konfigurasi VPC Anda

Untuk membuat koneksi VPN dari VPC Anda, lakukan hal berikut:

1. Buat virtual private gateway dan lampirkan ke VPC Anda. Untuk informasi selengkapnya, lihat [Buat gateway privat virtual](#).
2. Buat koneksi VPN dan gateway pelanggan baru. Untuk gateway pelanggan, tentukan alamat IP publik Windows Server Anda. Untuk koneksi VPN, pilih perutean statis, lalu masukkan rentang CIDR untuk jaringan Anda pada tempat Windows Server berada, misalnya, 172.31.0.0/16. Untuk informasi selengkapnya, lihat [Langkah 5: Buat koneksi VPN](#).

Setelah Anda membuat koneksi VPN, konfigurasi VPC untuk mengaktifkan komunikasi melalui koneksi VPN.

Untuk mengonfigurasi VPC Anda

- Buat subnet privat di VPC Anda (jika Anda belum punya) untuk meluncurkan instans untuk berkomunikasi dengan Windows Server. Untuk informasi selengkapnya, lihat [Membuat subnet di VPC Anda](#).

Note

Subnet privat adalah subnet yang tidak memiliki rute ke gateway internet. Perutean untuk subnet ini dijelaskan pada item berikutnya.

- Perbarui tabel rute Anda untuk koneksi VPN:
 - Tambahkan rute ke tabel rute subnet privat Anda dengan virtual private gateway sebagai target, dan jaringan Windows Server (rentang CIDR) sebagai tujuan. Untuk informasi selengkapnya, lihat [Menambahkan dan menghapus rute dari tabel rute](#) di Panduan Pengguna Amazon VPC.
 - Aktifkan propagasi rute untuk virtual private gateway. Untuk informasi selengkapnya, lihat [\(Gateway privat virtual\) Aktifkan propagasi rute di tabel rute Anda](#).
- Buat grup keamanan untuk instans Anda yang memungkinkan komunikasi antara VPC dan jaringan Anda:
 - Tambahkan aturan yang mengizinkan akses masuk RDP atau SSH dari jaringan Anda. Ini memungkinkan Anda dapat terhubung ke instans dalam VPC Anda dari jaringan Anda. Misalnya, untuk mengizinkan komputer di jaringan Anda mengakses instans Linux di VPC Anda, buat aturan masuk dengan tipe SSH, dan sumber yang diatur ke rentang CIDR jaringan Anda (misalnya, 172.31.0.0/16). Untuk informasi selengkapnya, lihat [Grup keamanan untuk VPC Anda](#) di Panduan pengguna Amazon VPC.
 - Tambahkan aturan yang mengizinkan akses ICMP masuk dari jaringan Anda. Hal ini memungkinkan Anda untuk menguji koneksi VPN Anda dengan mengirim ping ke instans di VPC Anda dari Windows Server Anda.

Langkah 2: Unduh file konfigurasi untuk koneksi VPN

Anda dapat menggunakan konsol Amazon VPC untuk mengunduh file konfigurasi Windows Server untuk koneksi VPN Anda.

Untuk mengunduh file konfigurasi

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Koneksi Site-to-Site VPN.
3. Pilih koneksi VPN Anda dan pilih Unduh Konfigurasi.
4. Pilih Microsoft sebagai vendor, Windows Server sebagai platform, dan 2012 R2 sebagai perangkat lunak. Pilih Unduh. Anda bisa membuka file atau menyimpannya.

File konfigurasi berisi bagian informasi yang sama dengan contoh berikut. Anda melihat informasi ini disajikan dua kali, satu kali untuk masing-masing terowongan.

```
vgw-1a2b3c4d Tunnel1
-----
Local Tunnel Endpoint:      203.0.113.1
Remote Tunnel Endpoint:    203.83.222.237
Endpoint 1:                 [Your_Static_Route_IP_Prefix]
Endpoint 2:                 [Your_VPC_CIDR_Block]
Preshared key:             xCjNLsLoCmKsawkdoR9yX6GsEXAMPLE
```

Local Tunnel Endpoint

Alamat IP yang Anda tentukan untuk gateway pelanggan saat Anda membuat koneksi VPN.

Remote Tunnel Endpoint

Salah satu dari dua alamat IP untuk gateway pribadi virtual yang mengakhiri koneksi VPN di AWS sisi koneksi.

Endpoint 1

Prefiks IP yang Anda tentukan sebagai rute statis saat Anda membuat koneksi VPN. Ini adalah alamat IP di jaringan Anda yang diizinkan untuk menggunakan koneksi VPN untuk mengakses VPC Anda.

Endpoint 2

Rentang alamat IP (blok CIDR) dari VPC yang terlampir ke virtual private gateway (misalnya 10.0.0.0/16).

Preshared key

Kunci pra-berbagi yang digunakan untuk membuat koneksi VPN IPsec antara Local Tunnel Endpoint dan Remote Tunnel Endpoint.

Kami menyarankan agar Anda mengonfigurasi kedua terowongan sebagai bagian dari koneksi VPN. Setiap terowongan terhubung ke konsentrator VPN terpisah di sisi Amazon dari koneksi VPN. Meskipun hanya satu terowongan yang muncul pada satu waktu, terowongan kedua secara otomatis dibuat sendiri jika terowongan pertama gagal. Memiliki terowongan berlebih memastikan ketersediaan berkelanjutan dalam kasus kegagalan perangkat. Karena hanya satu terowongan yang tersedia pada satu waktu, konsol Amazon VPC menunjukkan bahwa satu terowongan gagal. Ini adalah perilaku yang diharapkan, jadi Anda tidak perlu bertindak.

Dengan dua terowongan yang dikonfigurasi, jika terjadi kegagalan perangkat AWS, koneksi VPN Anda secara otomatis gagal ke terowongan kedua dari gateway pribadi virtual dalam hitungan menit. Saat mengonfigurasi perangkat gateway pelanggan Anda, penting untuk mengonfigurasi kedua terowongan.

Note

Dari waktu ke waktu, AWS melakukan pemeliharaan rutin pada gateway pribadi virtual. Pemeliharaan ini mungkin menonaktifkan salah satu dari dua terowongan koneksi VPN Anda untuk jangka waktu singkat. Koneksi VPN Anda secara otomatis gagal ke terowongan kedua saat kami melakukan pemeliharaan ini.

Informasi tambahan mengenai Pertukaran Kunci Internet (IKE) dan Security Associations (SA) IPsec disajikan dalam file konfigurasi yang diunduh.

```
MainModeSecMethods:    DHGroup2-AES128-SHA1
MainModeKeyLifetime:   480min,0sess
QuickModeSecMethods:   ESP:SHA1-AES128+60min+100000kb
QuickModePFS:          DHGroup2
```

MainModeSecMethods

Enkripsi dan autentikasi algoritme untuk SA IKE. Ini adalah pengaturan yang disarankan untuk koneksi VPN, dan pengaturan default untuk koneksi VPN Windows Server IPsec.

MainModeKeyLifetime

Waktu hidup kunci SA IKE. Ini adalah pengaturan yang disarankan untuk koneksi VPN, dan pengaturan default untuk koneksi VPN Windows Server IPsec.

QuickModeSecMethods

Enkripsi dan autentikasi algoritme untuk IPsec SA. Ini adalah pengaturan yang disarankan untuk koneksi VPN, dan pengaturan default untuk koneksi VPN Windows Server IPsec.

QuickModePFS

Kami menyarankan Anda untuk menggunakan kunci utama perfect forward secrecy (PFS) untuk sesi IPsec Anda.

Langkah 3: Mengonfigurasi Windows Server

Sebelum Anda mengatur terowongan VPN, Anda harus menginstal dan mengonfigurasi Perutean dan Layanan Akses Jarak Jauh pada Windows Server. Hal tersebut memungkinkan pengguna jarak jauh untuk mengakses sumber daya pada jaringan Anda.

Untuk menginstal Perutean dan Layanan Akses Jarak Jauh

1. Masuk ke Windows Server Anda.
2. Buka menu Mulai, dan pilih Server Manager.
3. Instal Perutean dan Layanan Akses Jarak Jauh:
 - a. Dari menu Mengelola, pilih Tambah Peran dan Fitur.
 - b. Pada halaman Sebelum Anda Memulai, verifikasi bahwa server Anda memenuhi prasyarat, lalu pilih Selanjutnya.
 - c. Pilih Instalasi berbasis peran atau berbasis fitur, lalu pilih Selanjutnya.
 - d. Pilih server dari kolam server, pilih Windows Server, lalu pilih Selanjutnya.
 - e. Pilih Kebijakan Jaringan dan Layanan Akses dalam daftar. Dalam kotak dialog yang ditampilkan, pilih Tambahkan Fitur untuk mengonfirmasi fitur yang diperlukan untuk peran ini.
 - f. Dalam daftar yang sama, pilih Akses Jarak Jauh, Selanjutnya.
 - g. Pada halaman Pilih fitur, pilih Selanjutnya.
 - h. Pada halaman Kebijakan Jaringan dan Layanan Akses, pilih Selanjutnya.
 - i. Pada halaman Akses Jarak Jauh, pilih Selanjutnya. Di halaman berikutnya, pilih DirectAccess dan VPN (RAS). Dalam kotak dialog yang ditampilkan, pilih Tambahkan Fitur untuk mengonfirmasi fitur yang diperlukan untuk layanan peran ini. Dalam daftar yang sama, pilih Perutean, lalu pilih Selanjutnya.
 - j. Pada halaman Web Server Role (IIS), pilih Selanjutnya. Abaikan pilihan default, dan pilih Selanjutnya.
 - k. Pilih Instal. Saat instalasi selesai, pilih Tutup.

Untuk mengonfigurasi serta mengaktifkan Perutean dan Server Akses Jarak Jauh

1. Di dasbor, pilih Notifikasi (ikon bendera). Harus ada tugas untuk menyelesaikan konfigurasi pasca-deployment. Pilih tautan Buka Memulai Wizard.

2. Pilih Deploy VPN saja.
3. Di kotak dialog Perutean dan Akses Jarak Jauh, pilih nama server, pilih Tindakan, dan kemudian pilih Mengonfigurasi dan Mengaktifkan Perutean dan Akses Jarak Jauh.
4. Di Wizard Pengaturan Perutean dan Server Akses Jarak Jauh, pada halaman pertama, pilih Selanjutnya.
5. Pada halaman Konfigurasi, pilih Konfigurasi Kustom, Selanjutnya.
6. Pilih Perutean LAN, Selanjutnya, Selesai.
7. Saat diminta oleh kotak dialog Perutean dan Akses Jarak Jauh, pilih Mulai layanan.

Langkah 4: Mengatur terowongan VPN

Anda dapat mengonfigurasi terowongan VPN dengan menjalankan skrip netsh yang disertakan dalam file konfigurasi yang diunduh, atau dengan menggunakan antarmuka pengguna Windows Server.

Important

Kami menyarankan Anda untuk menggunakan kunci utama perfect forward secrecy (PFS) untuk sesi IPsec Anda. Jika Anda memilih untuk menjalankan skrip netsh, hal itu termasuk parameter untuk mengaktifkan PFS (`qmpfs=dhgroup2`). Anda tidak dapat mengaktifkan PFS menggunakan antarmuka pengguna Windows — Anda harus mengaktifkannya menggunakan baris perintah.

Opsi

- [Opsi 1: Jalankan skrip netsh](#)
- [Opsi 2: Gunakan antarmuka pengguna Windows Server](#)

Opsi 1: Jalankan skrip netsh

Salin skrip netsh dari file konfigurasi yang diunduh dan ganti variabelnya. Berikut adalah contoh skrip.

```
netsh advfirewall consec add rule Name="vgw-1a2b3c4d Tunnel 1" ^
Enable=Yes Profile=any Type=Static Mode=Tunnel ^
LocalTunnelEndpoint=Windows_Server_Private_IP_address ^
RemoteTunnelEndpoint=203.83.222.236 Endpoint1=Your_Static_Route_IP_Prefix ^
```

```
Endpoint2=Your_VPC_CIDR_Block Protocol=Any Action=RequireInClearOut ^  
Auth1=ComputerPSK Auth1PSK=xCjNLsLoCmKsawkdoR9yX6GsEXAMPLE ^  
QMSecMethods=ESP:SHA1-AES128+60min+100000kb ^  
ExemptIPsecProtectedConnections=No ApplyAuthz=No QMPFS=dhgroup2
```

Nama: Anda dapat mengganti nama yang disarankan (vgw-1a2b3c4d Tunnel 1) dengan nama pilihan Anda.

LocalTunnelEndpoint: Masukkan alamat IP pribadi Windows Server di jaringan Anda.

Endpoint1: Blok CIDR jaringan Anda di tempat Windows Server berada, misalnya, 172.31.0.0/16. Apit nilai ini dengan tanda petik dua (").

Endpoint2: Blok CIDR VPC atau subnet di VPC Anda, misalnya, 10.0.0.0/16. Apit nilai ini dengan tanda petik dua (").

Jalankan skrip yang diperbarui di jendela prompt perintah pada Windows Server Anda. (^ memungkinkan Anda untuk memotong dan menempelkan teks yang dibungkus pada baris perintah.) Untuk mengatur terowongan VPN kedua untuk koneksi VPN ini, ulangi proses menggunakan skrip netsh kedua di file konfigurasi.

Setelah Anda selesai, buka [Konfigurasi Windows firewall](#).

Untuk informasi selengkapnya tentang parameter netsh, lihat [Perintah Netsh AdvFirewall Consec di Perpustakaan](#) Microsoft. TechNet

Opsi 2: Gunakan antarmuka pengguna Windows Server

Anda juga dapat menggunakan antarmuka pengguna Windows Server untuk mengatur terowongan VPN.

Important

Anda tidak dapat mengaktifkan kunci utama perfect forward secrecy (PFS) menggunakan antarmuka pengguna Windows Server. Anda harus mengaktifkan PFS menggunakan baris perintah, seperti yang dijelaskan di [Aktifkan kunci utama perfect forward secrecy](#).

Tugas

- [Konfigurasi aturan keamanan untuk terowongan VPN](#)

- [Konfirmasikan konfigurasi terowongan](#)
- [Aktifkan kunci utama perfect forward secrecy](#)
- [Konfigurasi Windows firewall](#)

Konfigurasi aturan keamanan untuk terowongan VPN

Dalam bagian ini, Anda mengonfigurasi aturan keamanan pada Windows Server untuk membuat terowongan VPN.

Untuk mengonfigurasi aturan keamanan untuk terowongan VPN

1. Buka Server Manager, pilih Alat, lalu pilih Windows Defender Firewall with Advanced Security.
2. Pilih Aturan Keamanan Koneksi, pilih Tindakan, lalu Aturan Baru.
3. Di wizard Aturan Keamanan Koneksi Baru, pada halaman Tipe Aturan, pilih Terowongan, lalu pilih Selanjutnya.
4. Pada halaman Tipe Terowongan, di dalam Tipe terowongan apa yang ingin dibuat, pilih Konfigurasi kustom. Di dalam Apakah Anda ingin membebaskan koneksi yang dilindungi IPsec dari terowongan ini, abaikan nilai default yang diperiksa (Tidak Kirim semua lalu lintas jaringan yang cocok dengan aturan keamanan koneksi ini melalui terowongan), lalu pilih Selanjutnya.
5. Pada halaman Persyaratan, pilih Memerlukan autentikasi untuk koneksi masuk. Jangan membuat terowongan untuk koneksi keluar, lalu pilih Selanjutnya.
6. Pada halaman Titik Akhir Terowongan, di dalam Komputer mana yang berada di Titik Akhir 1, pilih Tambahkan. Masukkan rentang CIDR jaringan Anda (di belakang perangkat gateway pelanggan Windows Server; misalnya, 172.31.0.0/16), lalu pilih OKE. Rentang ini dapat mencakup alamat IP perangkat gateway pelanggan Anda.
7. Di dalam Apa titik akhir terowongan lokal (paling dekat dengan komputer di Titik Akhir 1), pilih Edit. Di bidang Alamat IPv4, masukkan alamat IP privat Windows Server Anda, lalu pilih OKE.
8. Di dalam Apa titik akhir terowongan jarak jauh (paling dekat dengan komputer di Titik Akhir 2), pilih Edit. Di bidang Alamat IPv4, masukkan alamat IP dari virtual private gateway untuk Terowongan 1 dari file konfigurasi (lihat Remote Tunnel Endpoint), lalu pilih OKE.

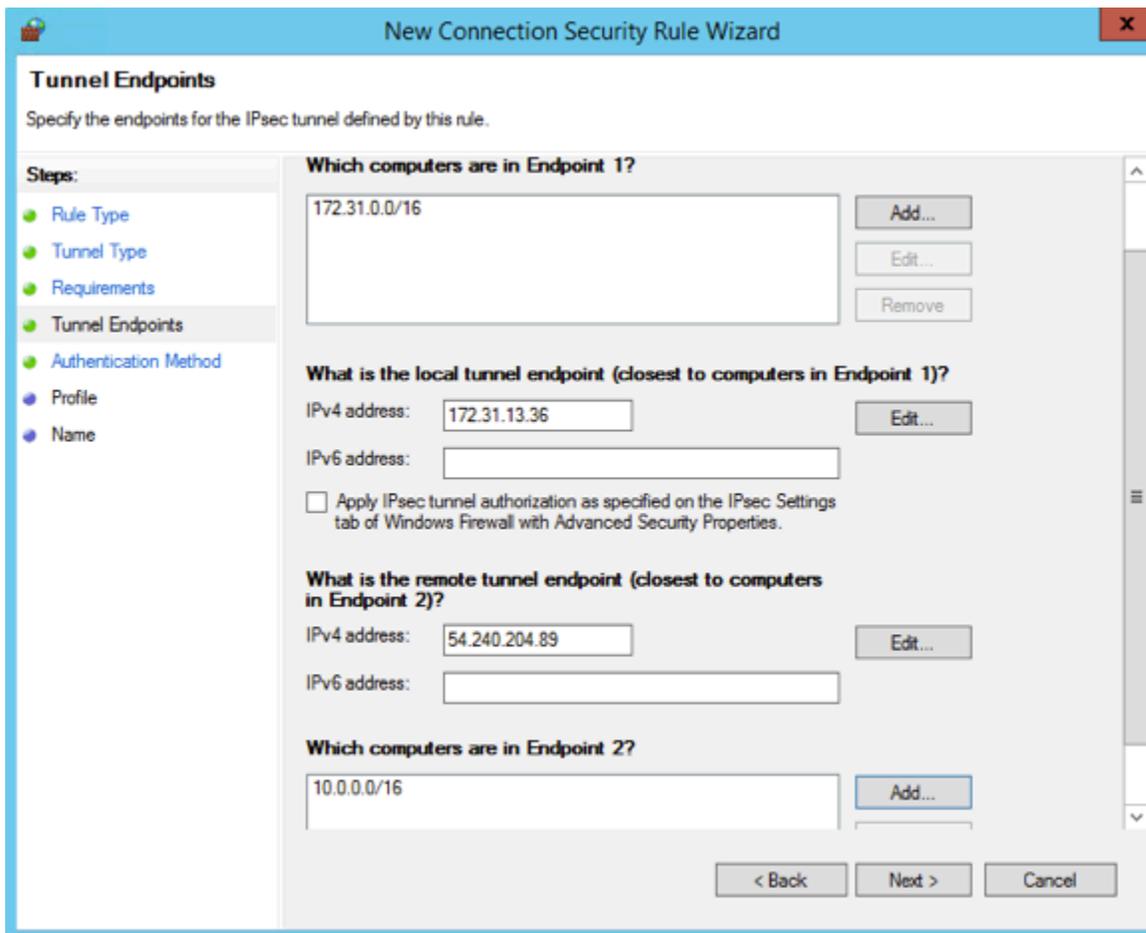
Important

Jika Anda mengulangi prosedur ini untuk Terowongan 2, pastikan untuk memilih titik akhir untuk Terowongan 2.

- Di dalam Komputer mana yang berada di Titik Akhir 2, pilih Tambahkan. Di Bidang alamat IP atau subnet ini, masukkan blok CIDR VPC Anda, lalu pilih OKE.

⚠ Important

Anda harus menggulir di kotak dialog hingga menemukan Komputer mana yang berada di Titik Akhir 2. Jangan memilih Selanjutnya hingga Anda menyelesaikan langkah ini, atau Anda tidak akan dapat terhubung ke server Anda.



- Pastikan bahwa semua pengaturan yang Anda tentukan sudah benar, lalu pilih Selanjutnya.
- Pada halaman Metode Autentikasi, pilih Lanjutan dan pilih Sesuaikan.
- Di dalam Metode autentikasi pertama, pilih Tambahkan.
- Pilih Kunci pra-berbagi, masukkan nilai kunci pra-berbagi dari file konfigurasi lalu pilih OKE.

⚠ Important

Jika Anda mengulangi prosedur ini untuk Terowongan 2, pastikan untuk memilih kunci pra-berbagi untuk Terowongan 2.

14. Pastikan bahwa Autentikasi pertama opsional tidak dipilih, dan pilih OKE.
15. Pilih Selanjutnya.
16. Pada halaman Profil, pilih ketiga kotak centang: Domain, Privat, dan Publik. Pilih Selanjutnya.
17. Pada halaman Nama, masukkan nama untuk aturan koneksi Anda; misalnya, VPN to Tunnel 1, lalu pilih Selesai.

Ulangi prosedur sebelumnya, menentukan data untuk Terowongan 2 dari file konfigurasi Anda.

Setelah Anda selesai, Anda akan memiliki dua terowongan yang dikonfigurasi untuk koneksi VPN Anda.

Konfirmasikan konfigurasi terowongan

Untuk mengonfirmasi konfigurasi terowongan

1. Buka Server Manager, pilih Alat, pilih Windows Firewall with Advanced Security, lalu pilih Aturan Koneksi Keamanan.
2. Verifikasi berikut untuk kedua terowongan:
 - Diaktifkan adalah Yes
 - Titik Akhir 1 adalah blok CIDR untuk jaringan Anda
 - Titik Akhir 2 adalah blok CIDR dari VPC Anda
 - Mode Autentikasi adalah Require inbound and clear outbound
 - Metode Autentikasi adalah Custom
 - Port Titik Akhir 1 adalah Any
 - Port Titik Akhir 2 adalah Any
 - Protokol adalah Any
3. Pilih aturan pertama dan pilih Properti.

4. Pada tab Autentikasi, di dalam Metode, pilih Sesuaikan. Verifikasi bahwa Metode autentikasi pertama berisi kunci pra-berbagi yang benar dari file konfigurasi Anda untuk terowongan, dan kemudian pilih OKE.
5. Pada tab Lanjutan, verifikasi bahwa Domain, Privat, dan Publik dipilih semua.
6. Di dalam IPsec tunneling, pilih Sesuaikan. Verifikasi pengaturan IPsec tunneling berikut, dan kemudian pilih OKE dan OKE lagi untuk menutup kotak dialog.
 - Gunakan IPsec tunneling yang dipilih.
 - Titik akhir terowongan lokal (terdekat ke Titik Akhir 1) berisi alamat IP Windows Server Anda. Jika perangkat gateway pelanggan Anda adalah instans EC2, ini adalah alamat IP privat instans.
 - Titik akhir terowongan jarak jauh (terdekat ke Titik Akhir 2) berisi alamat IP virtual private gateway untuk terowongan ini.
7. Buka properti untuk terowongan kedua Anda. Ulangi langkah 4 hingga 7 untuk terowongan ini.

Aktifkan kunci utama perfect forward secrecy

Anda dapat mengaktifkan kunci utama perfect forward secrecy dengan menggunakan baris perintah. Anda tidak dapat mengaktifkan fitur ini menggunakan antarmuka pengguna.

Untuk mengaktifkan kunci utama perfect forward secrecy

1. Di Windows Server, buka jendela prompt perintah baru.
2. Masukkan perintah berikut, ganti `rule_name` dengan nama yang Anda berikan pada aturan koneksi pertama.

```
netsh advfirewall consec set rule name="rule_name" new QMPFS=dhgroup2
QMPSecMethods=ESP:SHA1-AES128+60min+100000kb
```

3. Ulangi langkah 2 untuk terowongan kedua, kali ini ganti `rule_name` dengan nama yang Anda berikan pada aturan koneksi kedua.

Konfigurasi Windows firewall

Setelah menyiapkan aturan keamanan Anda pada server Anda, konfigurasi beberapa pengaturan IPsec dasar untuk bekerja dengan virtual private gateway.

Untuk mengonfigurasi Windows firewall

1. Buka Server Manager, pilih Alat, pilih Windows Defender Firewall with Advanced Security, lalu pilih Properti.
2. Pada tab Pengaturan IPsec, di dalam Pengecualian IPsec, verifikasi bahwa Bebaskan ICMP dari IPsec adalah Tidak ada (default). Verifikasi bahwa Otorisasi terowongan IPsec adalah Tidak ada.
3. Di dalam Default IPsec, pilih Sesuaikan.
4. Di dalam Pertukaran kunci (Mode Utama), pilih Lanjutan lalu pilih Sesuaikan.
5. Pada Sesuaikan Pengaturan Pertukaran Kunci Lanjutan, di dalam Metode keamanan, verifikasi bahwa nilai default berikut digunakan untuk entri pertama:
 - Integritas: SHA-1
 - Enkripsi: AES-CBC 128
 - Algoritme pertukaran kunci: Diffie-Hellman Grup 2
 - Di dalam Waktu hidup kunci, verifikasi bahwa Menit adalah 480 dan Sesi adalah 0.

Pengaturan ini sesuai dengan entri ini dalam file konfigurasi.

```
MainModeSecMethods: DHGroup2-AES128-SHA1,DHGroup2-3DES-SHA1
MainModeKeyLifetime: 480min,0sec
```

6. Di dalam Opsi pertukaran kunci, pilih Gunakan Diffie-Hellman untuk meningkatkan keamanan, lalu pilih OKE.
7. Di dalam Perlindungan data (Mode Cepat), pilih Lanjutan, lalu pilih Sesuaikan.
8. Pilih Memerlukan enkripsi untuk semua aturan keamanan koneksi yang menggunakan pengaturan ini.
9. Di dalam Integritas dan enkripsi data, abaikan nilai default:
 - Protokol: ESP
 - Integritas: SHA-1
 - Enkripsi: AES-CBC 128
 - Waktu hidup: 60 menit

Nilai-nilai ini sesuai dengan entri berikut dari file konfigurasi.

```
QuickModeSecMethods:  
ESP:SHA1-AES128+60min+100000kb
```

10. Pilih kotak dialog OKE untuk kembali ke Sesuaikan Pengaturan IPsec dan pilih OKE lagi untuk menyimpan konfigurasi.

Langkah 5: Aktifkan deteksi gateway mati

Selanjutnya, konfigurasi TCP untuk mendeteksi ketika gateway menjadi tidak tersedia. Anda dapat melakukannya dengan mengubah kunci registri ini: `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`. Jangan lakukan langkah ini hingga Anda menyelesaikan bagian sebelumnya. Setelah Anda mengubah kunci registri, Anda harus me-reboot server.

Untuk mengaktifkan deteksi gateway mati

1. Dari Windows Server Anda, luncurkan command prompt atau PowerShell sesi, dan masukkan `regedit` untuk memulai Registry Editor.
2. Perluas `HKEY_LOCAL_MACHINE`, perluas `SISTEM`, perluas, perluas Layanan `CurrentControlSet`, perluas `Tcpip`, lalu perluas `Parameter`.
3. Dari menu Edit, pilih Baru dan pilih Nilai `DWORD (32-bit)`.
4. Masukkan nama `EnableDeadGWDetect`.
5. Pilih `EnableDeadGWDetect` dan pilih Edit, Modify.
6. Di Data nilai, masukkan 1, lalu pilih OKE.
7. Tutup Editor Registri dan reboot server.

Untuk informasi selengkapnya, lihat [EnableDeadGWDetect](#) di Perpustakaan Microsoft TechNet.

Langkah 6: Uji koneksi VPN

Untuk menguji bahwa koneksi VPN berfungsi dengan benar, luncurkan sebuah instans ke VPC Anda, dan pastikan instans tersebut tidak memiliki koneksi internet. Setelah Anda meluncurkan instans, kirim ping alamat IP privatnya dari Windows Server Anda. Terowongan VPN muncul saat lalu lintas dihasilkan dari perangkat gateway pelanggan. Oleh karena itu, perintah ping juga memulai koneksi VPN.

Untuk langkah-langkah dalam menguji koneksi VPN, lihat [Uji koneksi VPN Site-to-Site](#).

Jika perintah ping gagal, periksa informasi berikut:

- Pastikan bahwa Anda telah mengonfigurasi aturan grup keamanan Anda untuk mengizinkan ICMP untuk instans di VPC Anda. Jika Windows Server adalah instans EC2, pastikan bahwa aturan keluar grup keamanan mengizinkan lalu lintas IPsec. Untuk informasi selengkapnya, lihat [Mengonfigurasi instans Windows Anda](#).
- Pastikan bahwa sistem operasi pada instans yang Anda ping dikonfigurasi untuk respons ICMP. Kami merekomendasikan agar Anda menggunakan salah satu Amazon Linux AMIs.
- Jika instans yang Anda ping adalah instans Windows, hubungkan ke instans dan aktifkan ICMPv4 masuk pada Windows firewall.
- Pastikan bahwa Anda telah mengonfigurasi tabel rute dengan benar untuk VPC atau subnet Anda. Untuk informasi selengkapnya, lihat [Langkah 1: Buat koneksi VPN dan konfigurasi VPC Anda](#).
- Jika perangkat gateway pelanggan Anda adalah instans EC2, pastikan bahwa Anda telah menonaktifkan pemeriksaan sumber/tujuan untuk instans. Untuk informasi selengkapnya, lihat [Mengonfigurasi instans Windows Anda](#).

Dalam konsol Amazon VPC, pada halaman Koneksi VPN, pilih koneksi VPN Anda. Terowongan pertama berada pada status UP. Terowongan kedua harus dikonfigurasi, tetapi tidak digunakan kecuali terowongan pertama gagal. Mungkin butuh waktu beberapa saat untuk membangun terowongan terenkripsi.

Memecahkan masalah perangkat gateway pelanggan Anda

Saat memecahkan masalah dengan perangkat gateway pelanggan Anda, penting untuk memiliki pendekatan terstruktur. Dua topik pertama di bagian ini menyediakan diagram alur umum untuk memecahkan masalah saat menggunakan perangkat yang dikonfigurasi untuk perutean dinamis (BGP diaktifkan), dan perangkat yang dikonfigurasi untuk perutean statis (tanpa diaktifkan), masing-masing. BGP Berikut topik tersebut adalah panduan pemecahan masalah khusus perangkat untuk perangkat gateway pelanggan Cisco, Juniper, dan Yamaha.

Selain topik di bagian ini, mengaktifkan [AWS Site-to-Site VPN log](#) dapat sangat membantu untuk memecahkan masalah dan menyelesaikan VPN masalah konektivitas. Untuk instruksi pengujian umum, lihat juga [Uji koneksi VPN Site-to-Site](#).

Topik

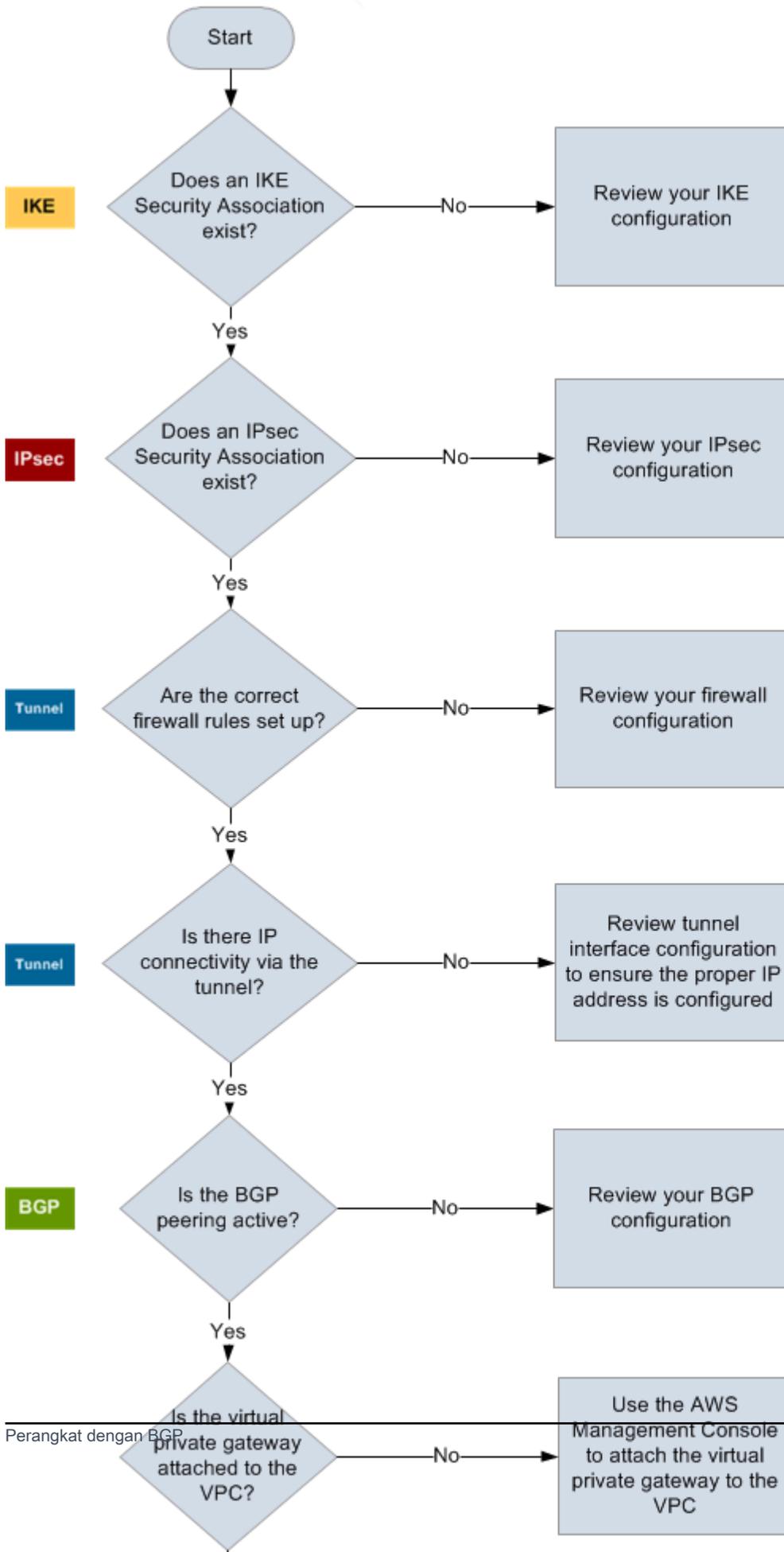
- [Pemecahan masalah konektivitas saat menggunakan Border Gateway Protocol](#)
- [Pemecahan masalah konektivitas tanpa Border Gateway Protocol](#)
- [Memecahkan masalah konektivitas perangkat gateway ASA pelanggan Cisco](#)
- [Memecahkan masalah konektivitas perangkat gateway IOS pelanggan Cisco](#)
- [Memecahkan masalah perangkat gateway IOS pelanggan Cisco tanpa konektivitas Border Gateway Protocol](#)
- [Pemecahan masalah konektivitas perangkat gateway pelanggan Juniper JunOS](#)
- [Pemecahan masalah konektivitas perangkat gateway pelanggan Juniper ScreenOS](#)
- [Pemecahan masalah konektivitas perangkat gateway pelanggan Yamaha](#)

Sumber daya tambahan

- [VPCForum Amazon](#)
- [Bagaimana cara memecahkan masalah konektivitas VPN terowongan ke Amazon saya? VPC](#)

Pemecahan masalah konektivitas saat menggunakan Border Gateway Protocol

Diagram dan tabel berikut memberikan petunjuk umum untuk pemecahan masalah perangkat gateway pelanggan yang menggunakan Border Gateway Protocol (BGP). Kami juga merekomendasikan agar Anda mengaktifkan fitur debug pada perangkat Anda. Konsultasikan dengan vendor perangkat gateway Anda untuk detailnya.



IKE	<p>Tentukan apakah ada asosiasi IKE keamanan.</p> <p>Asosiasi IKE keamanan diperlukan untuk bertukar kunci yang digunakan untuk membentuk asosiasi IPsec keamanan.</p> <p>Jika tidak ada asosiasi IKE keamanan, tinjau pengaturan IKE konfigurasi Anda. Anda harus mengonfigurasi enkripsi, autentikasi, perfect forward secrecy, dan parameter mode sesuai dengan yang tercantum dalam file konfigurasi.</p> <p>Jika ada asosiasi IKE keamanan, lanjutkan ke IPsec ".</p>
IPsec	<p>Tentukan apakah ada asosiasi IPsec keamanan (SA).</p> <p>IPsecSA adalah terowongan itu sendiri. Kueri perangkat gateway pelanggan Anda untuk menentukan apakah IPsec SA aktif. Anda harus mengonfigurasi enkripsi, autentikasi, perfect forward secrecy, dan parameter mode sesuai dengan yang tercantum dalam file konfigurasi.</p> <p>Jika tidak ada IPsec SA, tinjau IPsec konfigurasi Anda.</p> <p>Jika IPsec SA ada, lanjutkan ke 'Terowongan'.</p>
Terowongan	<p>Pastikan bahwa aturan firewall yang diperlukan telah disiapkan (untuk daftar aturan, lihat Aturan firewall untuk perangkat gateway pelanggan Anda). Jika sudah, silakan lanjutkan.</p> <p>Tentukan apakah terdapat konektivitas IP melalui terowongan.</p> <p>Setiap sisi pada terowongan memiliki alamat IP sebagaimana yang telah ditentukan dalam file konfigurasi. Alamat gateway pribadi virtual adalah alamat yang digunakan sebagai alamat BGP tetangga. Dari perangkat gateway pelanggan Anda, ping alamat ini untuk menentukan apakah lalu lintas IP telah dienkripsi dan didekripsi dengan benar.</p> <p>Jika ping tidak berhasil, tinjau konfigurasi antarmuka terowongan Anda untuk memastikan bahwa alamat IP yang tepat telah dikonfigurasi.</p> <p>Jika ping berhasil, lanjutkan ke 'BGP'.</p>
BGP	<p>Tentukan apakah sesi BGP peering aktif.</p>

Untuk setiap terowongan, lakukan hal berikut:

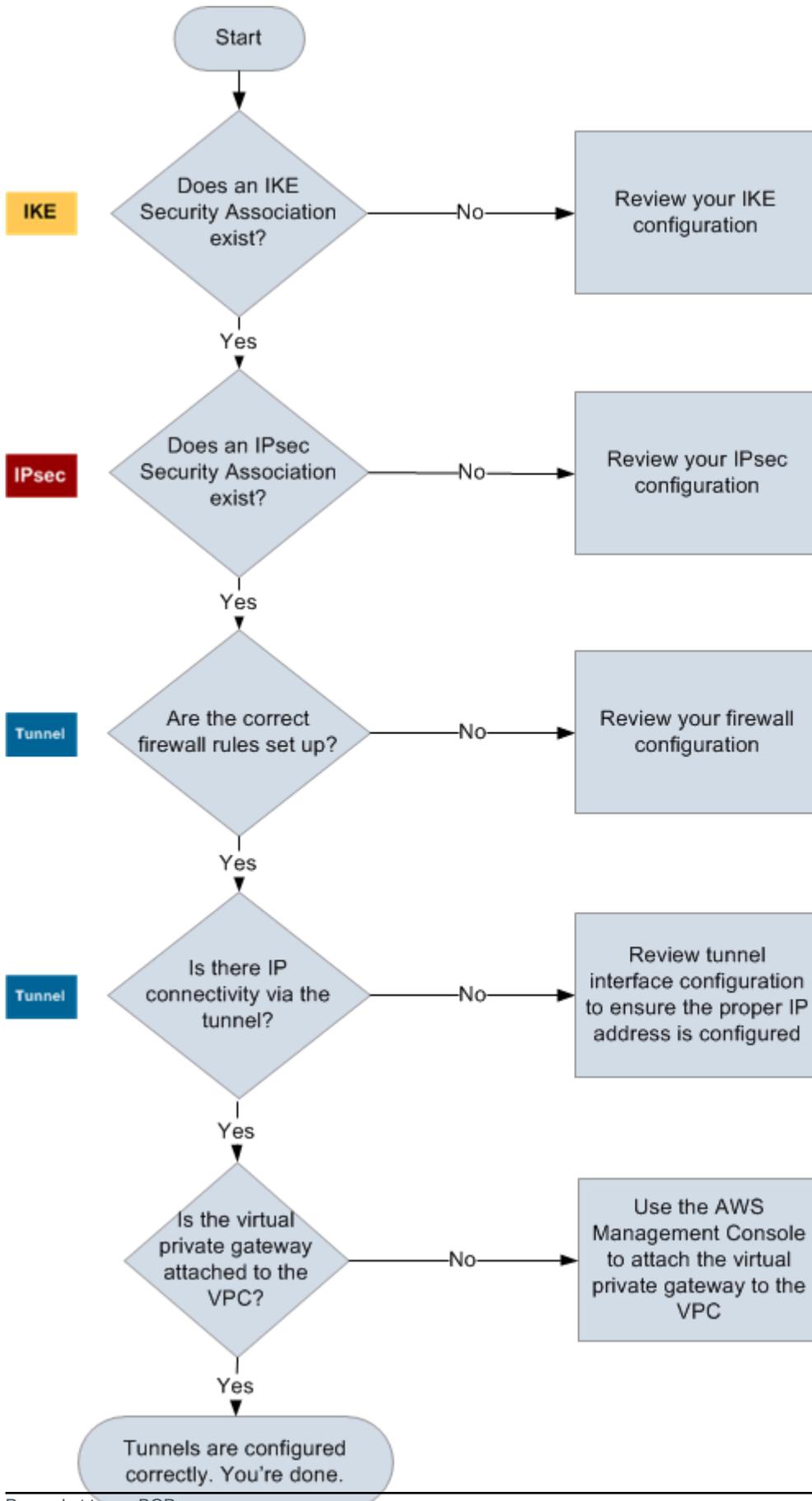
- Pada perangkat gateway pelanggan Anda, tentukan apakah BGP statusnya adalah `Active` atau `Established` . Mungkin diperlukan waktu sekitar 30 detik untuk BGP mengintip untuk menjadi aktif.
- Pastikan bahwa perangkat gateway pelanggan mengiklankan rute default (`0.0.0.0/0`) menuju virtual private gateway.

Jika terowongan tidak dalam status ini, tinjau BGP konfigurasi Anda.

Jika BGP peering dibuat, Anda menerima awalan, dan Anda mengiklankan awalan, terowongan Anda dikonfigurasi dengan benar. Pastikan kedua terowongan berada dalam status ini.

Pemecahan masalah konektivitas tanpa Border Gateway Protocol

Diagram dan tabel berikut memberikan petunjuk umum untuk pemecahan masalah perangkat gateway pelanggan yang tidak menggunakan Border Gateway Protocol (BGP). Kami juga merekomendasikan agar Anda mengaktifkan fitur debug pada perangkat Anda. Konsultasikan dengan vendor perangkat gateway Anda untuk detailnya.



IKE	<p>Tentukan apakah ada asosiasi IKE keamanan.</p> <p>Asosiasi IKE keamanan diperlukan untuk bertukar kunci yang digunakan untuk membentuk asosiasi IPsec keamanan.</p> <p>Jika tidak ada asosiasi IKE keamanan, tinjau pengaturan IKE konfigurasi Anda. Anda harus mengonfigurasi enkripsi, autentikasi, perfect forward secrecy, dan parameter mode sesuai dengan yang tercantum dalam file konfigurasi.</p> <p>Jika ada asosiasi IKE keamanan, lanjutkan ke IPsec ".</p>
IPsec	<p>Tentukan apakah ada asosiasi IPsec keamanan (SA).</p> <p>IPsecSA adalah terowongan itu sendiri. Kueri perangkat gateway pelanggan Anda untuk menentukan apakah IPsec SA aktif. Anda harus mengonfigurasi enkripsi, autentikasi, perfect forward secrecy, dan parameter mode sesuai dengan yang tercantum dalam file konfigurasi.</p> <p>Jika tidak ada IPsec SA, tinjau IPsec konfigurasi Anda.</p> <p>Jika IPsec SA ada, lanjutkan ke 'Terowongan'.</p>
Terowongan	<p>Pastikan bahwa aturan firewall yang diperlukan telah disiapkan (untuk daftar aturan, lihat Aturan firewall untuk perangkat gateway pelanggan Anda). Jika sudah, silakan lanjutkan.</p> <p>Tentukan apakah terdapat konektivitas IP melalui terowongan.</p> <p>Setiap sisi pada terowongan memiliki alamat IP sebagaimana yang telah ditentukan dalam file konfigurasi. Alamat gateway pribadi virtual adalah alamat yang digunakan sebagai alamat BGP tetangga. Dari perangkat gateway pelanggan Anda, ping alamat ini untuk menentukan apakah lalu lintas IP telah dienkripsi dan didekripsi dengan benar.</p> <p>Jika ping tidak berhasil, tinjau konfigurasi antarmuka terowongan Anda untuk memastikan bahwa alamat IP yang tepat telah dikonfigurasi.</p> <p>Jika ping berhasil, lanjutkan ke 'Rute Statis'.</p>

Rute statis

Untuk setiap terowongan, lakukan hal berikut:

- Verifikasi bahwa Anda telah menambahkan rute statis ke terowongan Anda VPC CIDR sebagai lompatan berikutnya.
- Verifikasi bahwa Anda telah menambahkan rute statis di VPC konsol Amazon, untuk memberi tahu gateway pribadi virtual untuk merutekan lalu lintas kembali ke jaringan internal Anda.

Jika terowongan tidak berada dalam status ini, tinjau konfigurasi perangkat Anda.

Pastikan bahwa kedua terowongan berada dalam status ini, dan setelah itu selesai.

Memecahkan masalah konektivitas perangkat gateway ASA pelanggan Cisco

Saat Anda memecahkan masalah konektivitas perangkat gateway pelanggan Cisco, pertimbangkan IKEIPsec, dan perutean. Anda dapat memecahkan masalah area ini dalam urutan apa pun, tetapi kami sarankan Anda memulai dengan IKE (di bagian bawah tumpukan jaringan) dan naik.

Important

Beberapa Cisco ASAs hanya mendukung mode Aktif/Siaga. Ketika Anda menggunakan Cisco iniASAs, Anda hanya dapat memiliki satu terowongan aktif pada satu waktu.

Terowongan siaga lainnya menjadi aktif hanya jika terowongan pertama tidak tersedia.

Terowongan siaga mungkin menghasilkan galat berikut dalam berkas log Anda, yang mana dapat diabaikan: `Rejecting IPSec tunnel: no matching crypto map entry for remote proxy 0.0.0.0/0.0.0.0/0/0 local proxy 0.0.0.0/0.0.0.0/0/0 on interface outside.`

IKE

Gunakan perintah berikut ini. Respons menunjukkan perangkat gateway pelanggan dengan IKE dikonfigurasi dengan benar.

```
ciscoasa# show crypto isakmp sa
```

```
Active SA: 2
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 2

1  IKE Peer: AWS_ENDPOINT_1
   Type    : L2L           Role    : initiator
   Rekey   : no           State   : MM_ACTIVE
```

Anda harus melihat satu atau lebih baris yang berisi nilai `src` untuk gateway jarak jauh yang ditentukan dalam terowongan. Nilai `state` seharusnya `MM_ACTIVE` dan status seharusnya `ACTIVE`. Tidak adanya entri, atau entri apa pun di negara bagian lain, menunjukkan bahwa tidak IKE dikonfigurasi dengan benar.

Untuk pemecahan masalah lebih lanjut, jalankan perintah berikut untuk mengaktifkan pesan log yang menyediakan informasi diagnostik.

```
router# term mon
router# debug crypto isakmp
```

Untuk menonaktifkan mode debug, gunakan perintah berikut.

```
router# no debug crypto isakmp
```

IPsec

Gunakan perintah berikut ini. Respons menunjukkan perangkat gateway pelanggan dengan IPsec dikonfigurasi dengan benar.

```
ciscoasa# show crypto ipsec sa
```

```
interface: outside
  Crypto map tag: VPN_crypto_map_name, seq num: 2, local addr: 172.25.50.101

  access-list integ-ppe-loopback extended permit ip any vpc_subnet subnet_mask
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (vpc_subnet/subnet_mask/0/0)
  current_peer: integ-ppel
```

```

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.25.50.101, remote crypto endpt.: AWS_ENDPOINT_1

path mtu 1500, ipsec overhead 74, media mtu 1500
current outbound spi: 6D9F8D3B
current inbound spi : 48B456A6

inbound esp sas:
spi: 0x48B456A6 (1219778214)
  transform: esp-aes esp-sha-hmac no compression
  in use settings = {L2L, Tunnel, PFS Group 2, }
  slot: 0, conn_id: 4710400, crypto-map: VPN_cry_map_1
  sa timing: remaining key lifetime (kB/sec): (4374000/3593)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001
outbound esp sas:
spi: 0x6D9F8D3B (1839172923)
  transform: esp-aes esp-sha-hmac no compression
  in use settings = {L2L, Tunnel, PFS Group 2, }
  slot: 0, conn_id: 4710400, crypto-map: VPN_cry_map_1
  sa timing: remaining key lifetime (kB/sec): (4374000/3593)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001

```

Untuk setiap antarmuka terowongan, Anda akan melihat, baik inbound esp sas maupun outbound esp sas. Ini mengasumsikan bahwa SA terdaftar (misalnya, spi: 0x48B456A6), dan itu IPsec dikonfigurasi dengan benar.

Di CiscoASA, IPsec satu-satunya muncul setelah lalu lintas yang menarik (lalu lintas yang harus dienkripsi) dikirim. Untuk selalu tetap IPsec aktif, kami sarankan untuk mengonfigurasi SLA monitor. SLAMonitor terus mengirim lalu lintas yang menarik, menjaga agar tetap IPsec aktif.

Anda juga dapat menggunakan perintah ping berikut untuk memaksa Anda IPsec memulai negosiasi dan naik.

```
ping ec2_instance_ip_address
```

```
Pinging ec2_instance_ip_address with 32 bytes of data:
```

```
Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128
```

```
Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128
```

```
Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 10.0.0.4:
```

```
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
```

```
Approximate round trip times in milliseconds:
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Untuk pemecahan masalah lebih lanjut, silahkan gunakan perintah berikut untuk mengaktifkan mode debug.

```
router# debug crypto ipsec
```

Untuk menonaktifkan mode debug, gunakan perintah berikut ini.

```
router# no debug crypto ipsec
```

Perutean

Ping ujung terowongan lainnya. Jika ini berhasil, maka Anda IPsec harus ditetapkan. Jika ini tidak berfungsi, periksa daftar akses Anda, dan lihat IPsec bagian sebelumnya.

Jika Anda tidak dapat menjangkau instans Anda, periksa informasi berikut.

1. Verifikasi bahwa daftar akses dikonfigurasi untuk mengizinkan lalu lintas yang terkait dengan peta krypto.

Anda dapat melakukannya dengan menggunakan perintah berikut.

```
ciscoasa# show run crypto
```

```
crypto ipsec transform-set transform-amzn esp-aes esp-sha-hmac
crypto map VPN_crypto_map_name 1 match address access-list-name
crypto map VPN_crypto_map_name 1 set pfs
crypto map VPN_crypto_map_name 1 set peer AWS_ENDPOINT_1 AWS_ENDPOINT_2
crypto map VPN_crypto_map_name 1 set transform-set transform-amzn
crypto map VPN_crypto_map_name 1 set security-association lifetime seconds 3600
```

2. Periksa daftar akses dengan menggunakan perintah berikut.

```
ciscoasa# show run access-list access-list-name
```

```
access-list access-list-name extended permit ip any vpc_subnet subnet_mask
```

3. Verifikasi bahwa daftar akses sudah benar. Daftar akses contoh berikut memungkinkan semua lalu lintas internal ke VPC subnet 10.0.0.0/16.

```
access-list access-list-name extended permit ip any 10.0.0.0 255.255.0.0
```

4. Jalankan traceroute dari ASA perangkat Cisco, untuk melihat apakah itu mencapai router Amazon (misalnya, *AWS_ENDPOINT_1/AWS_ENDPOINT_2*).

Jika ini mencapai router Amazon, periksa rute statis yang Anda tambahkan di VPC konsol Amazon, dan juga grup keamanan untuk instance tertentu.

5. Untuk pemecahan masalah lebih lanjut, tinjau konfigurasi.

Memecahkan masalah konektivitas perangkat gateway IOS pelanggan Cisco

Saat Anda memecahkan masalah konektivitas perangkat gateway pelanggan Cisco, pertimbangkan empat hal: IKE, terowongan IPsec, dan BGP. Anda dapat memecahkan masalah area ini dalam urutan apa pun, tetapi kami sarankan Anda memulai dengan IKE (di bagian bawah tumpukan jaringan) dan naik.

IKE

Gunakan perintah berikut ini. Respons menunjukkan perangkat gateway pelanggan dengan IKE dikonfigurasi dengan benar.

```
router# show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
192.168.37.160 72.21.209.193 QM_IDLE        2001    0 ACTIVE
192.168.37.160 72.21.209.225 QM_IDLE        2002    0 ACTIVE
```

Anda harus melihat satu atau lebih baris yang berisi nilai `src` untuk gateway jarak jauh yang ditentukan dalam terowongan. `state` seharusnya `QM_IDLE` dan `status` seharusnya `ACTIVE`. Tidak adanya entri, atau entri apa pun di negara bagian lain, menunjukkan bahwa tidak IKE dikonfigurasi dengan benar.

Untuk pemecahan masalah lebih lanjut, jalankan perintah berikut untuk mengaktifkan pesan log yang menyediakan informasi diagnostik.

```
router# term mon
router# debug crypto isakmp
```

Untuk menonaktifkan mode debug, gunakan perintah berikut.

```
router# no debug crypto isakmp
```

IPsec

Gunakan perintah berikut ini. Respons menunjukkan perangkat gateway pelanggan dengan IPsec dikonfigurasi dengan benar.

```
router# show crypto ipsec sa
```

```
interface: Tunnel1
  Crypto map tag: Tunnel1-head-0, local addr 192.168.37.160

  protected vrf: (none)
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer 72.21.209.225 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 149, #pkts encrypt: 149, #pkts digest: 149
    #pkts decaps: 146, #pkts decrypt: 146, #pkts verify: 146
    #pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 174.78.144.73, remote crypto endpt.: 72.21.209.225
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
current outbound spi: 0xB8357C22(3090512930)

inbound esp sas:
spi: 0x6ADB173(112046451)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 1, flow_id: Motorola SEC 2.0:1, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4467148/3189)
IV size: 16 bytes
replay detection support: Y  replay window size: 128
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xB8357C22(3090512930)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2, flow_id: Motorola SEC 2.0:2, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4467148/3189)
IV size: 16 bytes
replay detection support: Y  replay window size: 128
Status: ACTIVE

outbound ah sas:

outbound pcp sas:

interface: Tunnel2
Crypto map tag: Tunnel2-head-0, local addr 174.78.144.73

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 72.21.209.193 port 500
PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
#pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 174.78.144.73, remote crypto endpt.: 72.21.209.193
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
current outbound spi: 0xF59A3FF6(4120526838)

inbound esp sas:
spi: 0xB6720137(3060924727)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 3, flow_id: Motorola SEC 2.0:3, crypto map: Tunnel2-head-0
sa timing: remaining key lifetime (k/sec): (4387273/3492)
IV size: 16 bytes
replay detection support: Y  replay window size: 128
Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:
spi: 0xF59A3FF6(4120526838)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 4, flow_id: Motorola SEC 2.0:4, crypto map: Tunnel2-head-0
sa timing: remaining key lifetime (k/sec): (4387273/3492)
IV size: 16 bytes
replay detection support: Y  replay window size: 128
Status: ACTIVE

outbound ah sas:

outbound pcg sas:
```

Untuk setiap antarmuka terowongan, Anda akan melihat, baik inbound esp sas maupun outbound esp sas. Dengan asumsi SA terdaftar (spi: 0xF95D2F3C, misalnya) dan Status isACTIVE, IPsec dikonfigurasi dengan benar.

Untuk pemecahan masalah lebih lanjut, gunakan perintah berikut untuk mengaktifkan mode debug.

```
router# debug crypto ipsec
```

Gunakan perintah berikut untuk menonaktifkan mode debug.

```
router# no debug crypto ipsec
```

Terowongan

Pertama, periksa apakah Anda memiliki aturan firewall yang diperlukan. Untuk informasi selengkapnya, lihat [Aturan firewall untuk perangkat gateway pelanggan Anda](#).

Jika aturan firewall Anda telah diatur dengan benar, maka lanjutkan pemecahan masalah dengan menggunakan perintah berikut.

```
router# show interfaces tun1
```

```
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 169.254.255.2/30
  MTU 17867 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 2/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 174.78.144.73, destination 72.21.209.225
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1427 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "ipsec-vpn-92df3bfb-0")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
    407 packets input, 30010 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

Pastikan bahwa opsi `line protocol` sudah siap. Periksa apakah alamat IP sumber terowongan, antarmuka sumber, dan tujuan masing-masing cocok dengan konfigurasi terowongan untuk perangkat gateway pelanggan di luar alamat IP, antarmuka, dan virtual private gateway di luar alamat IP. Pastikan bahwa `Tunnel protection via IPSec` ada. Jalankan perintah pada kedua antarmuka terowongan. Untuk mengatasi masalah, tinjau konfigurasi dan periksa koneksi fisik ke perangkat gateway pelanggan Anda.

Juga gunakan perintah berikut, menggantikan `169.254.255.1` dengan alamat IP di dalam virtual private gateway Anda.

```
router# ping 169.254.255.1 df-bit size 1410
```

```
Type escape sequence to abort.  
Sending 5, 1410-byte ICMP Echos to 169.254.255.1, timeout is 2 seconds:  
Packet sent with the DF bit set  
!!!!!
```

Anda akan melihat lima tanda seru.

Untuk pemecahan masalah lebih lanjut, tinjau konfigurasi.

BGP

Gunakan perintah berikut.

```
router# show ip bgp summary
```

```
BGP router identifier 192.168.37.160, local AS number 65000  
BGP table version is 8, main routing table version 8  
2 network entries using 312 bytes of memory  
2 path entries using 136 bytes of memory  
3/1 BGP path/bestpath attribute entries using 444 bytes of memory  
1 BGP AS-PATH entries using 24 bytes of memory  
0 BGP route-map cache entries using 0 bytes of memory  
0 BGP filter-list cache entries using 0 bytes of memory  
Bitfield cache entries: current 1 (at peak 2) using 32 bytes of memory  
BGP using 948 total bytes of memory  
BGP activity 4/1 prefixes, 4/1 paths, scan interval 15 secs
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
169.254.255.1	4	7224	363	323	8	0	0	00:54:21	1

```
169.254.255.5 4 7224 364 323 8 0 0 00:00:24 1
```

Kedua neighbor harus terdaftar. Untuk masing-masing, Anda akan melihat nilai State/PfxRcd adalah 1.

Jika BGP peering sudah aktif, verifikasi bahwa perangkat gateway pelanggan Anda mengiklankan rute default (0.0.0.0/0) ke VPC

```
router# show bgp all neighbors 169.254.255.1 advertised-routes
```

```
For address family: IPv4 Unicast
BGP table version is 3, local router ID is 174.78.144.73
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Originating default network 0.0.0.0

Network          Next Hop          Metric  LocPrf Weight Path
*> 10.120.0.0/16 169.254.255.1    100     0   7224   i

Total number of prefixes 1
```

Selain itu, pastikan bahwa Anda menerima awalan yang sesuai dengan Anda VPC dari gateway pribadi virtual.

```
router# show ip route bgp
```

```
10.0.0.0/16 is subnetted, 1 subnets
B       10.255.0.0 [20/0] via 169.254.255.1, 00:00:20
```

Untuk pemecahan masalah lebih lanjut, tinjau konfigurasi.

Memecahkan masalah perangkat gateway IOS pelanggan Cisco tanpa konektivitas Border Gateway Protocol

Saat Anda memecahkan masalah konektivitas perangkat gateway pelanggan Cisco, pertimbangkan tiga hal:., dan IKE terowonganIPsec. Anda dapat memecahkan masalah area ini dalam urutan apa pun, tetapi kami sarankan Anda memulai dengan IKE (di bagian bawah tumpukan jaringan) dan naik.

IKE

Gunakan perintah berikut ini. Respons menunjukkan perangkat gateway pelanggan dengan IKE dikonfigurasi dengan benar.

```
router# show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
174.78.144.73 205.251.233.121 QM_IDLE        2001    0 ACTIVE
174.78.144.73 205.251.233.122 QM_IDLE        2002    0 ACTIVE
```

Anda harus melihat satu atau lebih baris yang berisi nilai `src` untuk gateway jarak jauh yang ditentukan dalam terowongan. `state` seharusnya `QM_IDLE` dan `status` seharusnya `ACTIVE`. Tidak adanya entri, atau entri apa pun di negara bagian lain, menunjukkan bahwa tidak IKE dikonfigurasi dengan benar.

Untuk pemecahan masalah lebih lanjut, jalankan perintah berikut untuk mengaktifkan pesan log yang menyediakan informasi diagnostik.

```
router# term mon
router# debug crypto isakmp
```

Untuk menonaktifkan mode debug, gunakan perintah berikut.

```
router# no debug crypto isakmp
```

IPsec

Gunakan perintah berikut ini. Respons menunjukkan perangkat gateway pelanggan dengan IPsec dikonfigurasi dengan benar.

```
router# show crypto ipsec sa
```

```
interface: Tunnel1
  Crypto map tag: Tunnel1-head-0, local addr 174.78.144.73

  protected vrf: (none)
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
current_peer 72.21.209.225 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 149, #pkts encrypt: 149, #pkts digest: 149
#pkts decaps: 146, #pkts decrypt: 146, #pkts verify: 146
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 174.78.144.73, remote crypto endpt.:205.251.233.121
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
current outbound spi: 0xB8357C22(3090512930)

inbound esp sas:
spi: 0x6ADB173(112046451)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 1, flow_id: Motorola SEC 2.0:1, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4467148/3189)
IV size: 16 bytes
replay detection support: Y  replay window size: 128
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xB8357C22(3090512930)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2, flow_id: Motorola SEC 2.0:2, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4467148/3189)
IV size: 16 bytes
replay detection support: Y  replay window size: 128
Status: ACTIVE

outbound ah sas:

outbound pcp sas:

interface: Tunnel2
Crypto map tag: Tunnel2-head-0, local addr 205.251.233.122
```

```
protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 72.21.209.193 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
#pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 174.78.144.73, remote crypto endpt.:205.251.233.122
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
current outbound spi: 0xF59A3FF6(4120526838)

inbound esp sas:
spi: 0xB6720137(3060924727)
  transform: esp-aes esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 3, flow_id: Motorola SEC 2.0:3, crypto map: Tunnel2-head-0
  sa timing: remaining key lifetime (k/sec): (4387273/3492)
  IV size: 16 bytes
  replay detection support: Y  replay window size: 128
  Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xF59A3FF6(4120526838)
  transform: esp-aes esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 4, flow_id: Motorola SEC 2.0:4, crypto map: Tunnel2-head-0
  sa timing: remaining key lifetime (k/sec): (4387273/3492)
  IV size: 16 bytes
  replay detection support: Y  replay window size: 128
  Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

Untuk setiap antarmuka terowongan, Anda akan melihat, baik esp sas masuk dan esp sas keluar. Ini mengasumsikan bahwa SA terdaftar (misalnya, spi: 0x48B456A6), bahwa statusnya ACTIVE, dan itu IPsec dikonfigurasi dengan benar.

Untuk pemecahan masalah lebih lanjut, silahkan gunakan perintah berikut untuk mengaktifkan mode debug.

```
router# debug crypto ipsec
```

Untuk menonaktifkan mode debug, gunakan perintah berikut ini.

```
router# no debug crypto ipsec
```

Terowongan

Pertama, periksa apakah Anda memiliki aturan firewall yang diperlukan. Untuk informasi selengkapnya, lihat [Aturan firewall untuk perangkat gateway pelanggan Anda](#).

Jika aturan firewall Anda telah disiapkan dengan benar, lanjutkan pemecahan masalah dengan menggunakan perintah berikut.

```
router# show interfaces tun1
```

```
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 169.254.249.18/30
  MTU 17867 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 2/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 174.78.144.73, destination 205.251.233.121
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1427 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "ipsec-vpn-92df3bfb-0")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
```

```
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 1 packets/sec
5 minute output rate 1000 bits/sec, 1 packets/sec
 407 packets input, 30010 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

Pastikan bahwa protokol baris sudah siap. Periksa apakah alamat IP sumber terowongan, antarmuka sumber, dan tujuan masing-masing cocok dengan konfigurasi terowongan untuk perangkat gateway pelanggan di luar alamat IP, antarmuka, dan virtual private gateway di luar alamat IP. Pastikan bahwa Tunnel protection through IPsec ada. Jalankan perintah pada kedua antarmuka terowongan. Untuk mengatasi masalah, tinjau konfigurasi dan periksa koneksi fisik ke perangkat gateway pelanggan Anda.

Anda juga dapat menggunakan perintah berikut, mengganti 169.254.249.18 dengan alamat IP di dalam virtual private gateway Anda.

```
router# ping 169.254.249.18 df-bit size 1410
```

```
Type escape sequence to abort.
Sending 5, 1410-byte ICMP Echos to 169.254.249.18, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
```

Anda akan melihat lima tanda seru.

Perutean

Untuk dapat melihat tabel rute statis Anda, gunakan perintah berikut.

```
router# sh ip route static
```

```
1.0.0.0/8 is variably subnetted
S      10.0.0.0/16 is directly connected, Tunnel1
is directly connected, Tunnel2
```

Anda harus melihat bahwa rute statis untuk VPC CIDR melalui kedua terowongan ada. Jika tidak ada, silahkan tambahkan rute statis sebagai berikut.

```
router# ip route 10.0.0.0 255.255.0.0 Tunnel1 track 100
```

```
router# ip route 10.0.0.0 255.255.0.0 Tunnel2 track 200
```

Memeriksa SLA monitor

```
router# show ip sla statistics 100
```

IPSLAs Latest Operation Statistics

```
IPSLA operation id: 100
    Latest RTT: 128 milliseconds
Latest operation start time: *18:08:02.155 UTC Wed Jul 15 2012
Latest operation return code: OK
Number of successes: 3
Number of failures: 0
Operation time to live: Forever
```

```
router# show ip sla statistics 200
```

IPSLAs Latest Operation Statistics

```
IPSLA operation id: 200
    Latest RTT: 128 milliseconds
Latest operation start time: *18:08:02.155 UTC Wed Jul 15 2012
Latest operation return code: OK
Number of successes: 3
Number of failures: 0
Operation time to live: Forever
```

Nilai untuk `Number of successes` menunjukkan apakah SLA monitor telah berhasil diatur.

Untuk pemecahan masalah lebih lanjut, tinjau konfigurasi.

Pemecahan masalah konektivitas perangkat gateway pelanggan Juniper JunOS

Saat Anda memecahkan masalah konektivitas perangkat gateway pelanggan Juniper, pertimbangkan empat hal: terowongan IKEIPsec, dan BGP Anda dapat memecahkan masalah area ini dalam urutan apa pun, tetapi kami sarankan Anda memulai dengan IKE (di bagian bawah tumpukan jaringan) dan naik.

IKE

Gunakan perintah berikut ini. Respons menunjukkan perangkat gateway pelanggan dengan IKE dikonfigurasi dengan benar.

```
user@router> show security ike security-associations
```

Index	Remote Address	State	Initiator cookie	Responder cookie	Mode
4	72.21.209.225	UP	c4cd953602568b74	0d6d194993328b02	Main
3	72.21.209.193	UP	b8c8fb7dc68d9173	ca7cb0abaedeb4bb	Main

Anda akan melihat satu atau lebih baris yang berisi alamat jarak jauh dari gateway jarak jauh yang ditentukan dalam terowongan. State seharusnya UP. Tidak adanya entri, atau entri apa pun di negara bagian lain (seperti DOWN), merupakan indikasi yang tidak IKE dikonfigurasi dengan benar.

Untuk pemecahan masalah lebih lanjut, aktifkan opsi IKE pelacakan seperti yang direkomendasikan dalam file konfigurasi contoh. Kemudian jalankan perintah berikut untuk mencetak berbagai pesan debug ke layar.

```
user@router> monitor start kmd
```

Dari host eksternal, Anda dapat mengambil seluruh berkas log dengan perintah berikut.

```
scp username@router.hostname:/var/log/kmd
```

IPsec

Gunakan perintah berikut ini. Respons menunjukkan perangkat gateway pelanggan dengan IPsec dikonfigurasi dengan benar.

```
user@router> show security ipsec security-associations
```

```
Total active tunnels: 2
ID      Gateway      Port  Algorithm      SPI      Life:sec/kb  Mon  vsys
<131073 72.21.209.225 500   ESP:aes-128/sha1 df27aae4 326/ unlim   -   0
>131073 72.21.209.225 500   ESP:aes-128/sha1 5de29aa1 326/ unlim   -   0
<131074 72.21.209.193 500   ESP:aes-128/sha1 dd16c453 300/ unlim   -   0
>131074 72.21.209.193 500   ESP:aes-128/sha1 c1e0eb29 300/ unlim   -   0
```

Secara khusus, Anda akan melihat setidaknya dua baris per alamat gateway (sesuai dengan gateway jarak jauh). Tanda sisipan di awal setiap baris (< >) menunjukkan arah lalu lintas untuk entri tertentu. Output memiliki baris terpisah untuk lalu lintas masuk ("<<", lalu lintas dari virtual private gateway ke perangkat gateway pelanggan ini) dan lalu lintas keluar (">").

Untuk pemecahan masalah lebih lanjut, aktifkan IKE traceoptions (untuk informasi selengkapnya, lihat bagian sebelumnya tentang). IKE

Terowongan

Pertama, periksa kembali apakah Anda memiliki aturan firewall yang diperlukan. Untuk daftar aturan, lihat [Aturan firewall untuk perangkat gateway pelanggan Anda](#).

Jika aturan firewall Anda disiapkan dengan benar, lanjutkan pemecahan masalah dengan perintah berikut.

```
user@router> show interfaces st0.1
```

```
Logical interface st0.1 (Index 70) (SNMP ifIndex 126)
  Flags: Point-To-Point SNMP-Traps Encapsulation: Secure-Tunnel
  Input packets : 8719
  Output packets: 41841
  Security: Zone: Trust
  Allowed host-inbound traffic : bgp ping ssh traceroute
  Protocol inet, MTU: 9192
    Flags: None
    Addresses, Flags: Is-Preferred Is-Primary
    Destination: 169.254.255.0/30, Local: 169.254.255.2
```

Pastikan bahwa Security: Zone adalah benar, dan bahwa alamat Local cocok dengan terowongan perangkat gateway pelanggan di dalam alamat.

Selanjutnya, gunakan perintah berikut, menggantikan 169.254.255.1 dengan alamat IP di dalam virtual private gateway Anda. Hasil Anda akan terlihat seperti respons yang ditunjukkan di sini.

```
user@router> ping 169.254.255.1 size 1382 do-not-fragment
```

```
PING 169.254.255.1 (169.254.255.1): 1410 data bytes
64 bytes from 169.254.255.1: icmp_seq=0 ttl=64 time=71.080 ms
64 bytes from 169.254.255.1: icmp_seq=1 ttl=64 time=70.585 ms
```

Untuk pemecahan masalah lebih lanjut, tinjau konfigurasi.

BGP

Jalankan perintah berikut.

```
user@router> show bgp summary
```

```
Groups: 1 Peers: 2 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History  Damp State   Pending
inet.0         2          1          0           0         0         0
Peer           AS         InPkt    OutPkt    OutQ     Flaps Last Up/Dwn State|
#Active/Received/Accepted/Damped...
169.254.255.1  7224       9        10        0         0         1:00 1/1/1/0
           0/0/0/0
169.254.255.5  7224       8         9         0         0         56 0/1/1/0
           0/0/0/0
```

Untuk pemecahan masalah lebih lanjut, gunakan perintah berikut, mengganti 169.254.255.1 dengan alamat IP di dalam virtual private gateway Anda.

```
user@router> show bgp neighbor 169.254.255.1
```

```
Peer: 169.254.255.1+179 AS 7224 Local: 169.254.255.2+57175 AS 65000
Type: External State: Established Flags: <ImportEval Sync>
Last State: OpenConfirm Last Event: RecvKeepAlive
Last Error: None
Export: [ EXPORT-DEFAULT ]
Options: <Preference HoldTime PeerAS LocalAS Refresh>
Holdtime: 30 Preference: 170 Local AS: 65000 Local System AS: 0
Number of flaps: 0
Peer ID: 169.254.255.1 Local ID: 10.50.0.10 Active Holdtime: 30
Keepalive Interval: 10 Peer index: 0
BFD: disabled, down
Local Interface: st0.1
NLRI for restart configured on peer: inet-unicast
NLRI advertised by peer: inet-unicast
NLRI for this session: inet-unicast
Peer supports Refresh capability (2)
Restart time configured on the peer: 120
Stale routes from peer are kept for: 300
```

```

Restart time requested by this peer: 120
NLRI that peer supports restart for: inet-unicast
NLRI that restart is negotiated for: inet-unicast
NLRI of received end-of-rib markers: inet-unicast
NLRI of all end-of-rib markers sent: inet-unicast
Peer supports 4 byte AS extension (peer-as 7224)
Table inet.0 Bit: 10000
  RIB State: BGP restart is complete
  Send state: in sync
  Active prefixes:          1
  Received prefixes:       1
  Accepted prefixes:       1
  Suppressed due to damping: 0
  Advertised prefixes:     1
Last traffic (seconds): Received 4    Sent 8    Checked 4
Input messages:  Total 24    Updates 2    Refreshes 0    Octets 505
Output messages: Total 26    Updates 1    Refreshes 0    Octets 582
Output Queue[0]: 0

```

Di sini Anda akan melihat `Received prefixes` dan `Advertised prefixes` telah terdaftar masing-masing 1. Ini akan berada di dalam bagian `Table inet.0`.

Jika State bukan `Established`, periksa `Last State` dan `Last Error` untuk detail mengenai apa yang diperlukan untuk memperbaiki masalah.

Jika BGP pengintipan selesai, verifikasi bahwa perangkat gateway pelanggan Anda mengiklankan rute default (`0.0.0.0/0`) ke VPC

```
user@router> show route advertising-protocol bgp 169.254.255.1
```

```

inet.0: 10 destinations, 11 routes (10 active, 0 holddown, 0 hidden)
  Prefix          Nexthop          MED    Lclpref    AS path
* 0.0.0.0/0      Self

```

Selain itu, pastikan Anda menerima awalan yang sesuai dengan Anda VPC dari gateway pribadi virtual.

```
user@router> show route receive-protocol bgp 169.254.255.1
```

```

inet.0: 10 destinations, 11 routes (10 active, 0 holddown, 0 hidden)
  Prefix          Nexthop          MED    Lclpref    AS path

```

```
* 10.110.0.0/16          169.254.255.1      100          7224 I
```

Pemecahan masalah konektivitas perangkat gateway pelanggan Juniper ScreenOS

Saat Anda memecahkan masalah konektivitas perangkat gateway pelanggan berbasis Juniper ScreenOS, pertimbangkan empat hal: terowongan IKE, IPsec dan BGP. Anda dapat memecahkan masalah area ini dalam urutan apa pun, tetapi kami sarankan Anda memulai dengan IKE (di bagian bawah tumpukan jaringan) dan naik.

IKE dan IPsec

Gunakan perintah berikut ini. Respons menunjukkan perangkat gateway pelanggan dengan IKE dikonfigurasi dengan benar.

```
ssg5-serial-> get sa
```

```
total configured sa: 2
HEX ID   Gateway      Port Algorithm   SPI      Life:sec kb Sta   PID vsys
00000002< 72.21.209.225 500 esp:a128/sha1 80041ca4 3385 unlim A/-  -1 0
00000002> 72.21.209.225 500 esp:a128/sha1 8cdd274a 3385 unlim A/-  -1 0
00000001< 72.21.209.193 500 esp:a128/sha1 ecf0bec7 3580 unlim A/-  -1 0
00000001> 72.21.209.193 500 esp:a128/sha1 14bf7894 3580 unlim A/-  -1 0
```

Anda akan melihat satu atau lebih baris yang berisi alamat jarak jauh dari gateway jarak jauh yang ditentukan dalam terowongan. Nilai `Sta` seharusnya `A/-` dan `SPI` harus berupa angka heksadesimal selain `00000000`. Entri di negara bagian lain menunjukkan bahwa tidak IKE dikonfigurasi dengan benar.

Untuk pemecahan masalah lebih lanjut, aktifkan opsi IKE pelacakan (seperti yang direkomendasikan dalam file konfigurasi contoh).

Terowongan

Pertama, periksa kembali apakah Anda memiliki aturan firewall yang diperlukan. Untuk daftar aturan, lihat [Aturan firewall untuk perangkat gateway pelanggan Anda](#).

Jika aturan firewall Anda telah disiapkan dengan benar, lanjutkan pemecahan masalah dengan menggunakan perintah berikut.

```
ssg5-serial-> get interface tunnel.1
```

```
Interface tunnel.1:
description tunnel.1
number 20, if_info 1768, if_index 1, mode route
link ready
vsys Root, zone Trust, vr trust-vr
admin mtu 1500, operating mtu 1500, default mtu 1500
*ip 169.254.255.2/30
*manage ip 169.254.255.2
route-deny disable
bound vpn:
    IPSEC-1

Next-Hop Tunnel Binding table
Flag Status Next-Hop(IP)    tunnel-id  VPN

pmtu-v4 disabled
ping disabled, telnet disabled, SSH disabled, SNMP disabled
web disabled, ident-reset disabled, SSL disabled

OSPF disabled  BGP enabled  RIP disabled  RIPng disabled  mtrace disabled
PIM: not configured  IGMP not configured
NHRP disabled
bandwidth: physical 0kbps, configured egress [gbw 0kbps mbw 0kbps]
            configured ingress mbw 0kbps, current bw 0kbps
            total allocated gbw 0kbps
```

Pastikan bahwa Anda melihat `link:ready`, dan bahwa alamat IP cocok dengan perangkat terowongan gateway pelanggan di dalam alamat.

Selanjutnya, gunakan perintah berikut, mengganti `169.254.255.1` dengan alamat IP di dalam virtual private gateway Anda. Hasil Anda akan terlihat seperti respons yang ditunjukkan di sini.

```
ssg5-serial-> ping 169.254.255.1
```

```
Type escape sequence to abort
```

```
Sending 5, 100-byte ICMP Echos to 169.254.255.1, timeout is 1 seconds
!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=32/32/33 ms
```

Untuk pemecahan masalah lebih lanjut, tinjau konfigurasi.

BGP

Jalankan perintah berikut.

```
ssg5-serial-> get vrouter trust-vr protocol bgp neighbor
```

Peer AS	Remote IP	Local IP	Wt	Status	State	ConnID	Up/Down
7224	169.254.255.1	169.254.255.2	100	Enabled	ESTABLISH	10	00:01:01
7224	169.254.255.5	169.254.255.6	100	Enabled	ESTABLISH	11	00:00:59

Keadaan kedua BGP rekan harus ESTABLISH, yang berarti bahwa BGP koneksi ke gateway pribadi virtual aktif.

Untuk pemecahan masalah lebih lanjut, gunakan perintah berikut, mengganti 169.254.255.1 dengan alamat IP di dalam virtual private gateway Anda.

```
ssg5-serial-> get vr trust-vr prot bgp neigh 169.254.255.1
```

```
peer: 169.254.255.1, remote AS: 7224, admin status: enable
type: EBGp, multihop: 0(disable), MED: node default(0)
connection state: ESTABLISH, connection id: 18 retry interval: node default(120s), cur
  retry time 15s
configured hold time: node default(90s), configured keepalive: node default(30s)
configured adv-interval: default(30s)
designated local IP: n/a
local IP address/port: 169.254.255.2/13946, remote IP address/port: 169.254.255.1/179
router ID of peer: 169.254.255.1, remote AS: 7224
negotiated hold time: 30s, negotiated keepalive interval: 10s
route map in name: , route map out name:
weight: 100 (default)
self as next hop: disable
send default route to peer: disable
ignore default route from peer: disable
send community path attribute: no
reflector client: no
Neighbor Capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast: advertised and received
```

```
force reconnect is disable
total messages to peer: 106, from peer: 106
update messages to peer: 6, from peer: 4
Tx queue length 0, Tx queue HWM: 1
route-refresh messages to peer: 0, from peer: 0
last reset 00:05:33 ago, due to BGP send Notification(Hold Timer Expired)(code 4 :
  subcode 0)
number of total successful connections: 4
connected: 2 minutes 6 seconds
Elapsed time since last update: 2 minutes 6 seconds
```

Jika BGP pengintipan selesai, verifikasi bahwa perangkat gateway pelanggan Anda mengiklankan rute default (0.0.0.0/0) ke VPC. Perintah ini berlaku untuk ScreenOS versi 6.2.0 dan yang lebih tinggi.

```
ssg5-serial-> get vr trust-vr protocol bgp rib neighbor 169.254.255.1 advertised
```

```
i: IBGP route, e: EBGP route, >: best route, *: valid route
      Prefix          Nexthop    Wt  Pref  Med Orig  AS-Path
-----
>i      0.0.0.0/0      0.0.0.0 32768  100   0  IGP
Total IPv4 routes advertised: 1
```

Selain itu, pastikan Anda menerima awalan yang sesuai dengan Anda VPC dari gateway pribadi virtual. Perintah ini berlaku untuk ScreenOS versi 6.2.0 dan yang lebih tinggi.

```
ssg5-serial-> get vr trust-vr protocol bgp rib neighbor 169.254.255.1 received
```

```
i: IBGP route, e: EBGP route, >: best route, *: valid route
      Prefix          Nexthop    Wt  Pref  Med Orig  AS-Path
-----
>e*    10.0.0.0/16     169.254.255.1 100  100  100  IGP  7224
Total IPv4 routes received: 1
```

Pemecahan masalah konektivitas perangkat gateway pelanggan Yamaha

Saat Anda memecahkan masalah konektivitas perangkat gateway pelanggan Yamaha, pertimbangkan empat hal: terowongan IKEIPsec, dan BGP Anda dapat memecahkan masalah area ini dalam urutan apa pun, tetapi kami sarankan Anda memulai dengan IKE (di bagian bawah tumpukan jaringan) dan naik.

Note

`proxy ID` Pengaturan yang digunakan pada fase 2 dari IKE dinonaktifkan secara default pada router Yamaha. Hal ini dapat menyebabkan masalah menghubungkan ke VPN Site-to-Site. Jika tidak `proxy ID` dikonfigurasi pada router Anda, silakan lihat file konfigurasi contoh AWS yang disediakan untuk Yamaha untuk disetel dengan benar.

IKE

Jalankan perintah berikut. Respons menunjukkan perangkat gateway pelanggan dengan IKE dikonfigurasi dengan benar.

```
# show ipsec sa gateway 1
```

sgw	flags	local-id	remote-id	# of sa
1	U K	YOUR_LOCAL_NETWORK_ADDRESS	72.21.209.225	i:2 s:1 r:1

Anda akan melihat sebuah baris yang berisi nilai `remote-id` untuk gateway jarak jauh yang ditentukan dalam terowongan. Anda dapat membuat daftar semua asosiasi keamanan (SAs) dengan menghilangkan nomor terowongan.

Untuk pemecahan masalah lebih lanjut, jalankan perintah berikut untuk mengaktifkan pesan log DEBUG level yang memberikan informasi diagnostik.

```
# syslog debug on
# ipsec ike log message-info payload-info key-info
```

Untuk membatalkan item yang dicatat, jalankan perintah berikut.

```
# no ipsec ike log
# no syslog debug on
```

IPsec

Jalankan perintah berikut. Respons menunjukkan perangkat gateway pelanggan dengan IPsec dikonfigurasi dengan benar.

```
# show ipsec sa gateway 1 detail
```

```
SA[1] Duration: 10675s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Protocol: IKE
Algorithm: AES-CBC, SHA-1, MODP 1024bit

SPI: 6b ce fd 8a d5 30 9b 02 0c f3 87 52 4a 87 6e 77
Key: ** ** ** ** ** (confidential) ** ** ** ** **
-----
SA[2] Duration: 1719s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Direction: send
Protocol: ESP (Mode: tunnel)
Algorithm: AES-CBC (for Auth.: HMAC-SHA)
SPI: a6 67 47 47
Key: ** ** ** ** ** (confidential) ** ** ** ** **
-----
SA[3] Duration: 1719s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Direction: receive
Protocol: ESP (Mode: tunnel)
Algorithm: AES-CBC (for Auth.: HMAC-SHA)
SPI: 6b 98 69 2b
Key: ** ** ** ** ** (confidential) ** ** ** ** **
-----
SA[4] Duration: 10681s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Protocol: IKE
Algorithm: AES-CBC, SHA-1, MODP 1024bit
SPI: e8 45 55 38 90 45 3f 67 a8 74 ca 71 ba bb 75 ee
Key: ** ** ** ** ** (confidential) ** ** ** ** **
-----
```

Untuk setiap antarmuka terowongan, Anda akan melihat, baik `receive sas` maupun `send sas`.

Untuk pemecahan masalah lebih lanjut, gunakan perintah berikut untuk mengaktifkan mode debug.

```
# syslog debug on
# ipsec ike log message-info payload-info key-info
```

Jalankan perintah berikut untuk menonaktifkan mode debug.

```
# no ipsec ike log
# no syslog debug on
```

Terowongan

Pertama, periksa apakah Anda memiliki aturan firewall yang diperlukan. Untuk daftar aturan, lihat [Aturan firewall untuk perangkat gateway pelanggan Anda](#).

Jika aturan firewall Anda disiapkan dengan benar, lanjutkan pemecahan masalah dengan perintah berikut.

```
# show status tunnel 1
```

```
TUNNEL[1]:
Description:
  Interface type: IPsec
  Current status is Online.
  from 2011/08/15 18:19:45.
  5 hours 7 minutes 58 seconds connection.
Received:   (IPv4) 3933 packets [244941 octets]
            (IPv6) 0 packet [0 octet]
Transmitted: (IPv4) 3933 packets [241407 octets]
            (IPv6) 0 packet [0 octet]
```

Pastikan `current` status nilainya online dan `Interface type` itu IPsec. Pastikan untuk menjalankan perintah pada kedua antarmuka terowongan. Untuk mengatasi masalah apapun yang ada di sini, tinjau konfigurasi.

BGP

Jalankan perintah berikut.

```
# show status bgp neighbor
```

```
BGP neighbor is 169.254.255.1, remote AS 7224, local AS 65000, external link
```

```

BGP version 0, remote router ID 0.0.0.0
BGP state = Active
Last read 00:00:00, hold time is 0, keepalive interval is 0 seconds
Received 0 messages, 0 notifications, 0 in queue
Sent 0 messages, 0 notifications, 0 in queue
Connection established 0; dropped 0
Last reset never
Local host: unspecified
Foreign host: 169.254.255.1, Foreign port: 0

BGP neighbor is 169.254.255.5, remote AS 7224, local AS 65000, external link
BGP version 0, remote router ID 0.0.0.0
BGP state = Active
Last read 00:00:00, hold time is 0, keepalive interval is 0 seconds
Received 0 messages, 0 notifications, 0 in queue
Sent 0 messages, 0 notifications, 0 in queue
Connection established 0; dropped 0
Last reset never
Local host: unspecified
Foreign host: 169.254.255.5, Foreign port:

```

Kedua neighbor harus terdaftar. Untuk masing-masing, Anda akan melihat nilai BGP state adalah Active.

Jika BGP pengintipan selesai, verifikasi bahwa perangkat gateway pelanggan Anda mengiklankan rute default (0.0.0.0/0) ke VPC

```
# show status bgp neighbor 169.254.255.1 advertised-routes
```

```

Total routes: 1
*: valid route
  Network          Next Hop          Metric LocPrf Path
* default          0.0.0.0           0      IGP

```

Selain itu, pastikan Anda menerima awalan yang sesuai dengan Anda VPC dari gateway pribadi virtual.

```
# show ip route
```

Destination	Gateway	Interface	Kind	Additional Info.
default	***.***.***.***	LAN3(DHCP)	static	

`10.0.0.0/16``169.254.255.1``TUNNEL[1]``BGP path=10124`

Bekerja dengan Site-to-Site VPN

Anda dapat bekerja dengan sumber daya Site-to-Site VPN menggunakan konsol Amazon VPC atau AWS CLI.

Konten

- [Buat lampiran VPN Site-to-Site untuk Cloud WAN AWS](#)
- [Buat lampiran VPN gateway transit](#)
- [Uji koneksi VPN Site-to-Site](#)
- [Hapus koneksi VPN Site-to-Site](#)
- [Ubah gateway target koneksi VPN Site-to-Site](#)
- [Ubah opsi koneksi VPN Site-to-Site](#)
- [Mengubah opsi terowongan Site-to-Site VPN](#)
- [Edit rute statis untuk koneksi VPN Site-to-Site](#)
- [Ubah gateway pelanggan untuk koneksi VPN Site-to-Site](#)
- [Ganti kredensi yang disusupi untuk koneksi VPN Site-to-Site Anda](#)
- [Putar sertifikat titik akhir terowongan VPN Site-to-Site](#)
- [VPN IP pribadi dengan AWS Direct Connect](#)

Buat lampiran VPN Site-to-Site untuk Cloud WAN AWS

Ikuti prosedur di bawah ini untuk membuat lampiran VPN Site-to-Site untuk Cloud WAN. AWS

Untuk membuat lampiran VPN untuk AWS Cloud WAN menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Koneksi VPN Site-to-Site.
3. Pilih Buat koneksi VPN.
4. (Opsional) Untuk tag Nama, masukkan nama untuk koneksi. Melakukan hal itu akan menciptakan tag dengan kunci Name dan nilai yang Anda tentukan.
5. Untuk jenis gateway Target, pilih Tidak terkait.

6. Untuk gateway Pelanggan, lakukan salah satu hal berikut:
 - Untuk menggunakan gateway pelanggan yang ada, pilih Existing, lalu pilih gateway pelanggan.
 - Untuk membuat gateway pelanggan, pilih Baru. Untuk alamat IP, masukkan alamat IP publik statis. Untuk Sertifikat ARN, pilih ARN dari sertifikat privat Anda (jika menggunakan autentikasi berbasis sertifikat). Untuk BGP ASN, masukkan Border Gateway Protocol (BGP) Autonomous System Number (ASN) dari gateway pelanggan Anda. Untuk informasi selengkapnya, lihat [Opsi gateway pelanggan](#).
7. Untuk opsi Routing, pilih Dinamis atau Statis.
8. Untuk Tunnel dalam versi IP, pilih IPv4 atau IPv6.
9. (Opsional) Untuk Aktifkan akselerasi, pilih kotak centang untuk mengaktifkan akselerasi. Untuk informasi selengkapnya, lihat [Koneksi VPN yang dipercepat](#).

Jika Anda mengaktifkan akselerasi, kami buat dua akselerator yang digunakan oleh koneksi VPN Anda. Berlaku biaya tambahan.

10. (Opsional) Untuk CIDR jaringan IPv4 lokal, tentukan rentang IPv4 CIDR di sisi gateway pelanggan (lokal) yang diizinkan untuk berkomunikasi melalui terowongan VPN. Defaultnya adalah `0.0.0.0/0`.

Untuk CIDR jaringan IPv4 Jarak Jauh, tentukan rentang IPv4 CIDR di AWS sisi yang diizinkan untuk berkomunikasi melalui terowongan VPN. Nilai default-nya `0.0.0.0/0`.

Jika Anda menentukan IPv6 untuk Tunnel di dalam versi IP, maka tentukan rentang IPv6 CIDR di sisi dan AWS sisi gateway pelanggan yang diizinkan untuk berkomunikasi melalui terowongan VPN. Default untuk kedua rentang tersebut adalah `::/0`.

11. (Opsional) Untuk opsi Tunnel, Anda dapat menentukan informasi berikut untuk setiap terowongan:
 - Sebuah blok CIDR berukuran /30 IPv4 dari rentang `169.254.0.0/16` untuk alamat IPv4 terowongan dalam.
 - Jika Anda menentukan IPv6 untuk Tunnel di dalam versi IP, blok CIDR /126 IPv6 dari `fd00::/8` rentang untuk alamat IPv6 terowongan di dalam.
 - Kunci pra-berbagi IKE (PSK). Versi berikut telah didukung: IKEv1 atau IKEv2.
 - Untuk mengedit opsi lanjutan untuk terowongan Anda, pilih opsi Edit terowongan. Untuk informasi selengkapnya, lihat [Opsi terowongan VPN](#).

12. Pilih Buat koneksi VPN.

Untuk membuat koneksi Site-to-Site VPN menggunakan baris perintah atau API

- [CreateVpnConnection](#) (Amazon EC2 Query API)
- [create-vpn-connection](#) (AWS CLI)

Buat lampiran VPN gateway transit

Untuk membuat lampiran VPN pada gateway transit, Anda harus menentukan gateway transit dan gateway pelanggan. Gateway transit harus dibuat sebelum mengikuti prosedur ini. Untuk informasi selengkapnya tentang pembuatan transit gateway, lihat [Transit Gateway](#) di Amazon VPC Transit Gateway.

Untuk membuat lampiran VPN pada gateway transit menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Koneksi VPN Site-to-Site.
3. Pilih Buat koneksi VPN.
4. (Opsional) Untuk tag Nama, masukkan nama untuk koneksi. Melakukan hal itu akan menciptakan tag dengan kunci Name dan nilai yang Anda tentukan.
5. Untuk jenis gateway Target, pilih Transit gateway, lalu pilih gateway transit.
6. Untuk gateway Pelanggan, lakukan salah satu hal berikut:
 - Untuk menggunakan gateway pelanggan yang ada, pilih Existing, lalu pilih gateway pelanggan.

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

- Untuk membuat gateway pelanggan, pilih Baru. Untuk Alamat IP, masukkan alamat IP publik statis. Untuk Sertifikat ARN, pilih ARN dari sertifikat privat Anda (jika menggunakan autentikasi berbasis sertifikat). Untuk BGP ASN, masukkan Border Gateway Protocol (BGP) Autonomous System Number (ASN) dari gateway pelanggan Anda. Untuk informasi selengkapnya, lihat [Opsi gateway pelanggan](#).
7. Untuk opsi Routing, pilih Dinamis atau Statis.

8. Untuk Tunnel dalam versi IP, tentukan apakah terowongan VPN mendukung lalu lintas IPv4 atau IPv6. Lalu lintas IPv6 hanya didukung untuk koneksi VPN pada transit gateway.
9. (Opsional) Untuk Aktifkan akselerasi, pilih kotak centang untuk mengaktifkan akselerasi. Untuk informasi selengkapnya, lihat [Koneksi VPN yang dipercepat](#).

Jika Anda mengaktifkan akselerasi, kami buat dua akselerator yang digunakan oleh koneksi VPN Anda. Berlaku biaya tambahan.

10. (Opsional) Untuk CIDR jaringan IPv4 lokal, tentukan rentang IPv4 CIDR di sisi gateway pelanggan (lokal) yang diizinkan untuk berkomunikasi melalui terowongan VPN. Defaultnya adalah `0.0.0.0/0`.

Untuk CIDR jaringan IPv4 Jarak Jauh, tentukan rentang IPv4 CIDR di AWS sisi yang diizinkan untuk berkomunikasi melalui terowongan VPN. Nilai default-nya `0.0.0.0/0`.

Jika Anda menentukan IPv6 untuk Tunnel di dalam versi IP, maka tentukan rentang IPv6 CIDR di sisi dan AWS sisi gateway pelanggan yang diizinkan untuk berkomunikasi melalui terowongan VPN. Default untuk kedua rentang tersebut adalah `::/0`.

11. (Opsional) Untuk opsi Tunnel, Anda dapat menentukan informasi berikut untuk setiap terowongan:
 - Sebuah blok CIDR berukuran /30 IPv4 dari rentang `169.254.0.0/16` untuk alamat IPv4 terowongan dalam.
 - Jika Anda menentukan IPv6 untuk Tunnel di dalam versi IP, blok CIDR /126 IPv6 dari `fd00::/8` rentang untuk alamat IPv6 terowongan di dalam.
 - Kunci pra-berbagi IKE (PSK). Versi berikut telah didukung: IKEv1 atau IKEv2.
 - Untuk mengedit opsi lanjutan untuk terowongan Anda, pilih opsi Edit terowongan. Untuk informasi selengkapnya, lihat [Opsional terowongan VPN](#).

12. Pilih Buat koneksi VPN.

Untuk membuat lampiran VPN menggunakan AWS CLI

Gunakan [create-vpn-connection](#) perintah dan tentukan ID gateway transit untuk `--transit-gateway-id` opsi tersebut.

Uji koneksi VPN Site-to-Site

Setelah membuat AWS Site-to-Site VPN koneksi dan mengonfigurasi gateway pelanggan, Anda dapat meluncurkan instance dan menguji koneksi dengan melakukan ping ke instance.

Sebelum memulai, pastikan hal-hal berikut:

- Gunakan AMI yang merespons permintaan ping. Kami merekomendasikan agar Anda menggunakan salah satu AMI Amazon Linux.
- Konfigurasi grup keamanan atau ACL jaringan apa pun di VPC Anda yang memfilter lalu lintas ke instans untuk mengizinkan lalu lintas ICMP masuk dan keluar. Hal ini memungkinkan instans untuk menerima permintaan ping.
- Jika Anda menggunakan instans yang menjalankan Windows Server, sambungkan ke instans dan aktifkan ICMPv4 masuk pada firewall Windows untuk melakukan ping ke instans.
- (Perutean statis) Pastikan perangkat gateway pelanggan memiliki rute statis ke VPC Anda, dan koneksi VPN Anda memiliki rute statis sehingga lalu lintas dapat kembali ke perangkat gateway pelanggan Anda.
- (Perutean dinamis) Pastikan status BGP pada perangkat gateway pelanggan Anda telah ditetapkan. Dibutuhkan sekitar 30 detik untuk membuat sesi peering BGP. Pastikan bahwa rute yang diiklankan dengan BGP dengan benar dan ditampilkan di tabel rute subnet, sehingga lalu lintas dapat kembali ke gateway pelanggan Anda. Pastikan bahwa kedua terowongan dikonfigurasi dengan perutean BGP.
- Pastikan Anda telah mengonfigurasi perutean di tabel rute subnet Anda untuk koneksi VPN.

Untuk menguji konektivitas

1. Buka konsol Amazon EC2 di <https://console.aws.amazon.com/ec2/>.
2. Pada dasbor, pilih Luncurkan instans.
3. (Opsional) Untuk Nama, masukkan nama deskriptif untuk instance Anda.
4. Untuk Gambar Aplikasi dan OS (Amazon Machine Image), pilih Mulai Cepat, lalu pilih sistem operasi untuk instans Anda.
5. Untuk nama Key pair, pilih key pair yang ada atau buat yang baru.
6. Untuk Pengaturan jaringan, pilih Pilih grup keamanan yang ada, lalu pilih grup keamanan yang Anda konfigurasi.
7. Di panel Ringkasan, pilih Luncurkan instans.

- Setelah instance berjalan, dapatkan alamat IP pribadinya (misalnya, 10.0.0.4). Konsol Amazon EC2 menampilkan alamat sebagai bagian dari detail instans.
- Dari komputer di jaringan Anda yang berada di belakang perangkat gateway pelanggan, gunakan ping perintah dengan alamat IP privat instans.

```
ping 10.0.0.4
```

Respon yang sukses mirip dengan yang berikut ini.

```
Pinging 10.0.0.4 with 32 bytes of data:

Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.4:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

    Approximate round trip times in milliseconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Untuk menguji failover terowongan, Anda dapat menonaktifkan sementara salah satu terowongan pada perangkat gateway pelanggan Anda dan kemudian ulangi langkah ini. Anda tidak dapat menonaktifkan terowongan di AWS sisi koneksi VPN.

- Untuk menguji koneksi dari AWS ke jaringan lokal, Anda dapat menggunakan SSH atau RDP untuk menyambung ke instans dari jaringan Anda. Kemudian Anda dapat menjalankan ping perintah dengan alamat IP privat dari komputer lain di jaringan Anda, untuk memverifikasi bahwa kedua sisi sambungan dapat memulai dan menerima permintaan.

Untuk informasi selengkapnya tentang cara menyambung ke instans Linux, lihat [Connect ke instans Linux Anda](#) di Panduan Pengguna Amazon EC2. Untuk informasi selengkapnya tentang cara menyambung ke instans Windows, lihat [Connect to Windows Anda](#) di Panduan Pengguna Amazon EC2.

Hapus koneksi VPN Site-to-Site

Jika Anda tidak lagi membutuhkan AWS Site-to-Site VPN koneksi, Anda dapat menghapusnya. Ketika Anda menghapus koneksi Site-to-Site VPN, kami tidak menghapus gateway pelanggan atau

gateway privat virtual yang berhubungan dengan koneksi Site-to-Site VPN. Jika Anda tidak lagi memerlukan gateway pelanggan dan gateway privat virtual, Anda dapat menghapusnya.

Warning

Jika Anda menghapus koneksi VPN Site-to-Site dan kemudian membuat yang baru, Anda harus mengunduh file konfigurasi baru dan mengkonfigurasi ulang perangkat gateway pelanggan.

Tugas

- [Hapus koneksi VPN](#)
- [Hapus gateway pelanggan](#)
- [Lepaskan dan hapus gateway pribadi virtual](#)

Hapus koneksi VPN

Setelah Anda menghapus koneksi Site-to-Site VPN, koneksi tersebut akan tetap terlihat selama beberapa saat dengan status `deleted`, dan kemudian entri akan dihapus secara otomatis.

Untuk menghapus koneksi VPN menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Koneksi VPN Site-to-Site.
3. Pilih koneksi VPN dan pilih Tindakan, Hapus koneksi VPN.
4. Saat diminta konfirmasi, masukkan **delete**, lalu pilih Hapus.

Untuk menghapus koneksi VPN menggunakan baris perintah atau API

- [DeleteVpnConnection](#) (Amazon EC2 Query API)
- [delete-vpn-connection](#) (AWS CLI)
- [Remove-EC2VpnConnection](#) (AWS Tools for Windows PowerShell)

Hapus gateway pelanggan

Jika Anda tidak lagi memerlukan gateway pelanggan, Anda dapat menghapusnya. Anda tidak dapat menghapus gateway pelanggan yang digunakan dalam koneksi Site-to-Site VPN.

Untuk menghapus gateway pelanggan gunakan konsol tersebut

1. Di panel navigasi, pilih gateway Pelanggan.
2. Pilih gateway pelanggan dan pilih Tindakan, Hapus gateway pelanggan.
3. Saat diminta konfirmasi, masukkan **delete**, lalu pilih Hapus.

Untuk menghapus gateway pelanggan gunakan baris perintah atau API

- [DeleteCustomerGateway](#) (Amazon EC2 Query API)
- [delete-customer-gateway](#) (AWS CLI)
- [Remove-EC2CustomerGateway](#) (AWS Tools for Windows PowerShell)

Lepaskan dan hapus gateway pribadi virtual

Jika Anda tidak lagi memerlukan gateway privat virtual untuk VPC Anda, Anda dapat melepaskannya dari VPC.

Untuk melepaskan gateway privat virtual menggunakan konsol tersebut

1. Di panel navigasi, pilih Gateway pribadi virtual.
2. Pilih gateway privat virtual dan kemudian pilih Tindakan, Lepaskan dari VPC.
3. Pilih Lepaskan gateway pribadi virtual.

Jika Anda tidak lagi memerlukan gateway privat virtual yang dilepaskan, Anda dapat menghapusnya. Anda tidak dapat menghapus gateway privat virtual yang masih terlampir pada VPC. Setelah Anda menghapus gateway pribadi virtual Anda, itu tetap terlihat untuk sementara waktu dengan status `deleted`, dan kemudian entri dihapus secara otomatis.

Untuk menghapus gateway privat virtual menggunakan konsol tersebut

1. Di panel navigasi, pilih Gateway pribadi virtual.
2. Pilih gateway pribadi virtual dan pilih Tindakan, Hapus gateway pribadi virtual.

3. Saat diminta konfirmasi, masukkan **delete**, lalu pilih Hapus.

Untuk melepaskan gateway privat virtual gunakan baris perintah atau API

- [DetachVpnGateway](#) (Amazon EC2 Query API)
- [detach-vpn-gateway](#) (AWS CLI)
- [Dismount-EC2VpnGateway](#) (AWS Tools for Windows PowerShell)

Untuk menghapus gateway privat virtual gunakan baris perintah atau API

- [DeleteVpnGateway](#) (Amazon EC2 Query API)
- [delete-vpn-gateway](#) (AWS CLI)
- [Remove-EC2VpnGateway](#) (AWS Tools for Windows PowerShell)

Ubah gateway target koneksi VPN Site-to-Site

Anda dapat memodifikasi gateway target AWS Site-to-Site VPN koneksi. Berikut ini adalah opsi migrasi yang tersedia:

- Gateway privat virtual yang sudah ada ke transit gateway
- Gateway privat virtual yang sudah ada ke gateway privat virtual lainnya
- Transit gateway yang sudah ada ke transit gateway lainnya
- Transit gateway yang sudah ada ke gateway privat virtual

Setelah Anda mengubah gateway target, koneksi Site-to-Site VPN Anda sementara tidak akan tersedia untuk jangka waktu singkat ketika kami menyediakan titik akhir baru.

Tugas berikut membantu Anda menyelesaikan migrasi ke gateway baru.

Tugas

- [Langkah 1: Buat gateway target baru](#)
- [Langkah 2: Hapus rute statis Anda \(bersyarat\)](#)
- [Langkah 3: Migrasi ke gateway baru](#)
- [Langkah 4: Perbarui tabel rute VPC](#)

- [Langkah 5: Perbarui perutean gateway target \(bersyarat\)](#)
- [Langkah 6: Perbarui gateway pelanggan ASN \(bersyarat\)](#)

Langkah 1: Buat gateway target baru

Sebelum Anda melakukan migrasi ke gateway target baru, Anda harus terlebih dahulu mengkonfigurasi gateway baru. Untuk informasi tentang menambahkan gateway privat virtual, lihat [the section called “Buat gateway privat virtual”](#). Untuk informasi selengkapnya tentang menambahkan transit gateway, lihat [Buat transit gateway](#) di Amazon VPC Transit Gateways.

Jika gateway target baru adalah transit gateway, lampirkan VPC ke transit gateway. Untuk informasi tentang lampiran VPC, lihat [Lampiran transit gateway ke VPC](#) di Amazon VPC Transit Gateway.

Ketika mengubah target dari gateway privat virtual ke transit gateway, Anda secara opsional dapat mengatur ASN transit gateway menjadi nilai yang sama dengan ASN gateway privat virtual. Jika Anda memilih untuk memiliki ASN yang berbeda, maka Anda harus mengatur ASN di perangkat gateway pelanggan Anda ke transit gateway ASN. Untuk informasi selengkapnya, lihat [the section called “Langkah 6: Perbarui gateway pelanggan ASN \(bersyarat\)”](#).

Langkah 2: Hapus rute statis Anda (bersyarat)

Langkah ini diperlukan ketika Anda bermigrasi dari gateway privat virtual dengan rute statis ke transit gateway.

Anda harus menghapus rute statis sebelum bermigrasi ke gateway baru.

Tip

Simpan salinan rute statis sebelum Anda menghapusnya. Anda harus menambahkan kembali rute ini ke transit gateway setelah migrasi koneksi VPN selesai.

Untuk menghapus rute dari tabel rute

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Tabel rute, lalu pilih tabel rute.
3. Di tab Rute, pilih Edit rute.

4. Pilih Hapus untuk rute statis ke gateway pribadi virtual.
5. Pilih Simpan perubahan.

Langkah 3: Migrasi ke gateway baru

Untuk mengubah gateway target

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Koneksi VPN Site-to-Site.
3. Pilih koneksi VPN dan pilih Tindakan, Ubah koneksi VPN.
4. Untuk tipe Target, pilih jenis gateway.
 - a. Jika gateway target baru adalah gateway pribadi virtual, pilih gateway VPN.
 - b. Jika gateway target baru adalah gateway transit, pilih Transit gateway.
5. Pilih Simpan perubahan.

Untuk mengubah koneksi Site-to-Site VPN menggunakan baris perintah atau API

- [ModifyVpnConnection](#) (Amazon EC2 Query API)
- [modify-vpn-connection](#) (AWS CLI)

Langkah 4: Perbarui tabel rute VPC

Setelah bermigrasi ke gateway baru, Anda mungkin perlu mengubah tabel rute VPC Anda. Untuk informasi selengkapnya, lihat [Rutekan tabel](#) di Panduan Pengguna Amazon VPC.

Tabel berikut memberikan informasi tentang pembaruan tabel rute VPC yang akan dilakukan setelah Anda memodifikasi target gateway VPN.

Gateway yang sudah ada	Gateway baru	Perubahan tabel rute VPC
Gateway privat virtual dengan rute dipropagasi	Transit gateway	Tambahkan rute yang berisi ID gateway transit.
Gateway privat virtual dengan rute dipropagasi	Gateway privat virtual dengan rute dipropagasi	Tidak ada tindakan yang diperlukan.

Gateway yang sudah ada	Gateway baru	Perubahan tabel rute VPC
Gateway privat virtual dengan rute dipropagasi	Gateway privat virtual dengan rute statis	Tambahkan rute yang berisi ID gateway pribadi virtual baru.
Gateway privat virtual dengan rute statis	Gateway transit	Perbarui rute yang berisi ID gateway pribadi virtual ke ID gateway transit.
Gateway privat virtual dengan rute statis	Gateway privat virtual dengan rute statis	Perbarui rute yang berisi ID gateway pribadi virtual ke ID gateway pribadi virtual baru.
Gateway privat virtual dengan rute statis	Gateway privat virtual dengan rute dipropagasi	Hapus rute yang berisi ID gateway pribadi virtual.
Gateway transit	Gateway privat virtual dengan rute statis	Perbarui rute yang berisi ID gateway transit ke ID gateway pribadi virtual.
Gateway transit	Gateway privat virtual dengan rute dipropagasi	Hapus rute yang berisi ID gateway transit.
Gateway transit	Gateway transit	Perbarui rute yang berisi ID gateway transit ke ID gateway transit baru.

Langkah 5: Perbarui perutean gateway target (bersyarat)

Ketika gateway baru adalah transit gateway, ubah tabel rute transit gateway untuk mengizinkan lalu lintas antara VPC dan Site-to-Site VPN. Untuk informasi selengkapnya, lihat [Tabel rute gateway transit](#) di Amazon VPC Transit Gateways.

Jika Anda menghapus rute statis VPN, Anda harus menambahkan rute statis ke tabel rute transit gateway.

Tidak seperti gateway pribadi virtual, gateway transit menetapkan nilai yang sama untuk multi-exit diskriminator (MED) di semua terowongan pada lampiran VPN. Jika Anda bermigrasi dari gateway pribadi virtual ke gateway transit dan mengandalkan nilai MED untuk pemilihan terowongan, kami

sarankan Anda membuat perubahan perutean untuk menghindari masalah koneksi. Misalnya, Anda dapat mengiklankan rute yang lebih spesifik di gateway transit Anda. Untuk informasi selengkapnya, lihat [Tabel rute dan prioritas VPN rute](#).

Langkah 6: Perbarui gateway pelanggan ASN (bersyarat)

Ketika gateway baru memiliki ASN yang berbeda dari gateway lama, Anda harus memperbarui ASN di perangkat gateway pelanggan Anda untuk diarahkan ke ASN baru. Lihat [Opsinya gateway pelanggan untuk koneksi Site-to-Site VPN](#) untuk informasi selengkapnya.

Ubah opsi koneksi VPN Site-to-Site

Anda dapat mengubah opsi koneksi untuk koneksi Site-to-Site VPN Anda. Anda dapat mengubah opsi berikut:

- Rentang CIDR IPv4 di sisi (gateway pelanggan) lokal dan sisi (AWS) jarak jauh dari koneksi VPN yang dapat berkomunikasi melalui terowongan VPN. Default-nya adalah $0.0.0.0/0$ untuk kedua rentang.
- Rentang CIDR IPv6 di sisi (gateway pelanggan) lokal dan sisi (AWS) jarak jauh dari koneksi VPN yang dapat berkomunikasi melalui terowongan VPN. Default-nya adalah $::/0$ untuk kedua rentang.

Saat Anda memodifikasi opsi koneksi VPN, alamat IP titik akhir VPN di AWS samping tidak berubah, dan opsi terowongan tidak berubah. Koneksi VPN Anda sementara tidak akan tersedia untuk jangka waktu yang singkat ketika koneksi VPN diperbarui.

Untuk mengubah opsi koneksi VPN menggunakan konsol tersebut

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Koneksi VPN Site-to-Site.
3. Pilih koneksi VPN Anda, dan pilih Tindakan, Ubah opsi koneksi VPN.
4. Masukkan rentang CIDR baru sesuai kebutuhan.
5. Pilih Simpan perubahan.

Untuk mengubah opsi koneksi VPN menggunakan baris perintah atau API

- [modify-vpn-connection-options](#) (AWS CLI)

- [ModifyVpnConnectionOptions](#) (Amazon EC2 Query API)

Mengubah opsi terowongan Site-to-Site VPN

Anda dapat mengubah opsi terowongan VPN untuk terowongan VPN di koneksi Site-to-Site VPN Anda. Anda dapat mengubah satu terowongan VPN pada satu waktu.

Important

Ketika Anda mengubah terowongan VPN, konektivitas melalui terowongan terganggu selama beberapa menit. Pastikan Anda merencanakan waktu henti yang diharapkan.

Untuk mengubah opsi terowongan VPN menggunakan konsol tersebut

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Koneksi VPN Site-to-Site.
3. Pilih koneksi VPN Site-to-Site, dan pilih Actions, Modify VPN tunnel options.
4. Untuk terowongan VPN di luar alamat IP, pilih IP titik akhir terowongan VPN.
5. Pilih atau masukkan nilai baru untuk opsi terowongan sesuai kebutuhan. Untuk informasi selengkapnya, lihat [Opsi terowongan VPN](#).
6. Pilih Simpan perubahan.

Untuk mengubah opsi terowongan VPN menggunakan baris perintah atau API

- (AWS CLI) Gunakan [describe-vpn-connections](#) untuk melihat opsi terowongan saat ini, dan [modify-vpn-tunnel-options](#) untuk memodifikasi opsi terowongan.
- (Amazon EC2 Query API) Gunakan [DescribeVpnConnections](#) untuk melihat opsi terowongan saat ini, dan [ModifyVpnTunnelOptions](#) untuk memodifikasi opsi terowongan.

Edit rute statis untuk koneksi VPN Site-to-Site

Untuk koneksi VPN Site-to-Site pada gateway pribadi virtual yang dikonfigurasi untuk perutean statis, Anda dapat menambah atau menghapus rute statis dari konfigurasi VPN Anda.

Untuk menambah atau menghapus rute statis menggunakan konsol

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Koneksi VPN Site-to-Site.
3. Pilih koneksi VPN.
4. Pilih Edit rute statis.
5. Tambahkan atau hapus rute sesuai kebutuhan.
6. Pilih Simpan perubahan.
7. Jika Anda belum mengaktifkan propagasi rute untuk tabel rute Anda, Anda harus memperbarui rute secara manual di tabel rute Anda untuk mencerminkan awalan IP statis yang diperbarui dalam koneksi VPN Anda. Untuk informasi selengkapnya, lihat [\(Gateway privat virtual\) Aktifkan propagasi rute di tabel rute Anda](#).
8. Untuk koneksi VPN pada gateway transit, Anda menambahkan, memodifikasi, atau menghapus rute statis dalam tabel rute gateway transit. Untuk informasi selengkapnya, lihat [Tabel rute gateway transit](#) di Amazon VPC Transit Gateways.

Untuk menambahkan rute statis menggunakan baris perintah atau API

- [CreateVpnConnectionRoute](#) (Amazon EC2 Query API)
- [create-vpn-connection-route](#) (AWS CLI)
- [New-EC2VpnConnectionRoute](#) (AWS Tools for Windows PowerShell)

Untuk menghapus rute statis menggunakan baris perintah atau API

- [DeleteVpnConnectionRoute](#) (Amazon EC2 Query API)
- [delete-vpn-connection-route](#) (AWS CLI)
- [Remove-EC2VpnConnectionRoute](#) (AWS Tools for Windows PowerShell)

Ubah gateway pelanggan untuk koneksi VPN Site-to-Site

Anda dapat mengubah gateway pelanggan dari koneksi Site-to-Site VPN Anda dengan menggunakan konsol Amazon VPC atau alat baris perintah.

Setelah Anda mengubah gateway pelanggan, koneksi VPN Anda akan sementara tidak tersedia untuk waktu yang singkat sementara kami menyediakan titik akhir baru.

Untuk mengubah gateway pelanggan menggunakan konsol tersebut

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Koneksi VPN Site-to-Site.
3. Pilih koneksi VPN.
4. Pilih Tindakan, Ubah koneksi VPN.
5. Untuk tipe Target, pilih gateway Pelanggan.
6. Untuk gateway pelanggan Target, pilih gateway pelanggan baru.
7. Pilih Simpan perubahan.

Untuk mengubah gateway pelanggan menggunakan baris perintah atau API

- [ModifyVpnConnection](#) (Amazon EC2 Query API)
- [modify-vpn-connection](#) (AWS CLI)

Ganti kredensi yang disusupi untuk koneksi VPN Site-to-Site Anda

Jika Anda yakin bahwa kredensial terowongan untuk koneksi Site-to-Site VPN Anda telah disusupi, Anda dapat mengubah kunci pra-berbagi IKE atau mengubah sertifikat ACM. Metode yang Anda gunakan tergantung pada opsi autentikasi yang Anda gunakan untuk terowongan VPN Anda. Untuk informasi selengkapnya, lihat [Opsis otentikasi terowongan situs-ke-situs VPN](#).

Untuk mengubah kunci pra-berbagi IKE

Anda dapat memodifikasi opsi terowongan untuk koneksi VPN dan menentukan kunci pra-bersama IKE baru untuk setiap terowongan. Untuk informasi selengkapnya, lihat [Mengubah opsi terowongan Site-to-Site VPN](#).

Atau, Anda dapat menghapus koneksi VPN. Untuk informasi selengkapnya, lihat [Hapus koneksi VPN](#). Anda tidak perlu menghapus VPC atau gateway privat virtual. Kemudian, buat koneksi VPN baru menggunakan gateway pribadi virtual yang sama, dan konfigurasi kunci baru pada perangkat gateway pelanggan Anda. Anda dapat menentukan kunci pra-bersama Anda sendiri untuk terowongan atau membiarkan AWS menghasilkan kunci pra-bersama baru untuk Anda. Untuk informasi selengkapnya, lihat [Membuat koneksi VPN](#). Alamat terowongan di dalam dan di luar mungkin berubah saat Anda membuat ulang koneksi VPN.

Untuk mengubah sertifikat untuk AWS sisi titik akhir terowongan

Putar sertifikatnya. Untuk informasi selengkapnya, lihat [Putar sertifikat titik akhir terowongan VPN](#).

Untuk mengubah sertifikat pada perangkat gateway pelanggan

1. Buat sertifikat baru. Untuk selengkapnya, lihat [Menerbitkan dan mengelola sertifikat](#) di Panduan AWS Certificate Manager Pengguna.
2. Tambahkan sertifikat ke perangkat gateway pelanggan.

Putar sertifikat titik akhir terowongan VPN Site-to-Site

Anda dapat memutar sertifikat pada titik akhir terowongan di AWS samping dengan menggunakan konsol VPC Amazon. Ketika sertifikat titik akhir terowongan mendekati kedaluwarsa, AWS secara otomatis memutar sertifikat menggunakan peran terkait layanan. Untuk informasi selengkapnya, lihat [the section called “Peran terkait layanan”](#).

Untuk merotasi sertifikat titik akhir terowongan Site-to-Site VPN menggunakan konsol tersebut

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Koneksi VPN Site-to-Site.
3. Pilih koneksi VPN Site-to-Site, lalu pilih Actions, Modify VPN tunnel certificate.
4. Pilih titik akhir terowongan.
5. Pilih Simpan.

Untuk memutar sertifikat titik akhir terowongan Site-to-Site VPN menggunakan AWS CLI

Gunakan perintah [modify-vpn-tunnel-certificate](#).

VPN IP pribadi dengan AWS Direct Connect

Dengan VPN IP pribadi, Anda dapat menyebarkan VPN IPsec melalui AWS Direct Connect, mengenkripsi lalu lintas antara jaringan lokal Anda dan AWS, tanpa menggunakan alamat IP publik atau peralatan VPN pihak ketiga tambahan.

Salah satu kasus penggunaan utama untuk VPN IP pribadi AWS Direct Connect adalah membantu pelanggan di industri keuangan, perawatan kesehatan, dan federal memenuhi tujuan peraturan dan kepatuhan. Private IP VPN over AWS Direct Connect memastikan bahwa lalu lintas antara AWS dan

jaringan lokal aman dan pribadi, memungkinkan pelanggan untuk mematuhi mandat peraturan dan keamanan mereka.

Daftar Isi

- [Manfaat VPN IP Pribadi](#)
- [Cara kerja VPN IP pribadi](#)
- [Prasyarat](#)
- [Buat gateway pelanggan](#)
- [Siapkan gerbang transit](#)
- [Buat AWS Direct Connect gateway](#)
- [Buat asosiasi gateway transit](#)
- [Buat koneksi VPN](#)

Manfaat VPN IP Pribadi

- Manajemen dan operasi jaringan yang disederhanakan: Tanpa VPN IP pribadi, pelanggan harus menggunakan VPN dan router pihak ketiga untuk mengimplementasikan VPN pribadi melalui jaringan. AWS Direct Connect Dengan kemampuan VPN IP pribadi, pelanggan tidak perlu menggunakan dan mengelola infrastruktur VPN mereka sendiri. Ini mengarah pada operasi jaringan yang disederhanakan dan pengurangan biaya.
- Postur keamanan yang ditingkatkan: Sebelumnya, pelanggan harus menggunakan antarmuka AWS Direct Connect virtual publik (VIF) untuk mengenkripsi lalu lintas AWS Direct Connect, yang memerlukan alamat IP publik untuk titik akhir VPN. Menggunakan IP publik meningkatkan kemungkinan serangan eksternal (DOS), yang pada gilirannya memaksa pelanggan untuk menggunakan peralatan keamanan tambahan untuk perlindungan jaringan. Selain itu, VIF publik membuka akses antara semua layanan AWS publik dan jaringan lokal pelanggan, meningkatkan tingkat keparahan risiko. Fitur VPN IP pribadi memungkinkan enkripsi melalui VIF AWS Direct Connect transit (bukan VIF publik), ditambah dengan kemampuan untuk mengkonfigurasi IP pribadi. Ini menyediakan konektivitas end-to-end pribadi selain enkripsi, meningkatkan postur keamanan secara keseluruhan.
- Skala rute yang lebih tinggi: Koneksi VPN IP pribadi menawarkan batas rute yang lebih tinggi (5000 rute keluar dan 1000 rute masuk) dibandingkan dengan AWS Direct Connect sendiri, yang saat ini memiliki batas 200 rute keluar dan 100 rute masuk.

Cara kerja VPN IP pribadi

IP Pribadi Site-to-Site VPN bekerja melalui AWS Direct Connect antarmuka virtual transit (VIF). Ini menggunakan AWS Direct Connect gateway dan gateway transit untuk menghubungkan jaringan lokal Anda dengan AWS VPC. Koneksi VPN IP pribadi memiliki titik penghentian di gateway transit di AWS samping, dan di perangkat gateway pelanggan Anda di sisi lokal. Anda harus menetapkan alamat IP pribadi ke gateway transit dan ujung perangkat gateway pelanggan dari terowongan IPsec. Anda dapat menggunakan alamat IP pribadi dari rentang alamat IPv4 pribadi RFC1918 atau RFC6598.

Anda melampirkan koneksi VPN IP pribadi ke gateway transit. Anda kemudian merutekan lalu lintas antara lampiran VPN dan VPC apa pun (atau jaringan lain) yang juga dilampirkan ke gateway transit. Anda melakukannya dengan mengaitkan tabel rute dengan lampiran VPN. Dalam arah sebaliknya, Anda dapat merutekan lalu lintas dari VPC Anda ke lampiran VPN IP pribadi dengan menggunakan tabel rute yang terkait dengan VPC.

Tabel rute yang terkait dengan lampiran VPN bisa sama atau berbeda dari yang terkait dengan AWS Direct Connect lampiran yang mendasarinya. Ini memberi Anda kemampuan untuk merutekan lalu lintas terenkripsi dan tidak terenkripsi secara bersamaan antara VPC Anda dan jaringan lokal Anda.

Untuk detail selengkapnya tentang jalur lalu lintas yang meninggalkan VPN, lihat [Antarmuka virtual pribadi dan kebijakan perutean antarmuka virtual transit](#) di Panduan AWS Direct Connect Pengguna.

Prasyarat

Sumber daya berikut diperlukan untuk menyelesaikan pengaturan VPN IP pribadi melalui AWS Direct Connect:

- AWS Direct Connect Koneksi antara jaringan lokal Anda dan AWS
- AWS Direct Connect Gateway dengan asosiasi dengan gateway transit yang sesuai
- Gateway transit dengan blok CIDR IP pribadi yang tersedia
- Perangkat gateway pelanggan di jaringan lokal Anda dan gateway AWS pelanggan terkait

Buat gateway pelanggan

Gateway pelanggan adalah sumber daya yang Anda buat AWS. Ini mewakili perangkat gateway pelanggan di jaringan lokal Anda. Saat Anda membuat gateway pelanggan, Anda memberikan informasi tentang perangkat Anda AWS. Untuk detail selengkapnya, lihat [Gateway pelanggan](#).

Untuk membuat gateway pelanggan menggunakan konsol tersebut

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih gateway Pelanggan.
3. Pilih Buat gateway pelanggan.
4. (Opsional) Untuk tag Nama, masukkan nama untuk gateway pelanggan Anda. Melakukan hal itu akan menciptakan tag dengan kunci Name dan nilai yang Anda tentukan.
5. Untuk BGP ASN, masukkan Border Gateway Protocol (BGP) Autonomous System Number (ASN) untuk gateway pelanggan Anda.
6. Untuk alamat IP, masukkan alamat IP pribadi untuk perangkat gateway pelanggan Anda.
7. (Opsional) Untuk Perangkat, masukkan nama untuk perangkat yang menghosting gateway pelanggan ini.
8. Pilih Buat gateway pelanggan.

Untuk membuat gateway pelanggan menggunakan baris perintah atau API

- [CreateCustomerGateway](#) (Amazon EC2 Query API)
- [create-customer-gateway](#) (AWS CLI)

Siapkan gerbang transit

Transit gateway adalah hub transit jaringan yang dapat Anda gunakan untuk saling menghubungkan VPC Anda dan jaringan on-premise. Anda dapat membuat gateway transit baru atau menggunakan yang sudah ada untuk koneksi VPN IP pribadi. Saat Anda membuat gateway transit, atau memodifikasi gateway transit yang ada, Anda menentukan blok CIDR IP pribadi untuk koneksi.

Note

Saat menentukan blok CIDR gateway transit yang akan dikaitkan dengan VPN IP Pribadi Anda, pastikan blok CIDR tidak tumpang tindih dengan alamat IP apa pun untuk lampiran jaringan lain di gateway transit. Jika ada blok IP CIDR yang tumpang tindih, ini dapat menyebabkan masalah konfigurasi dengan perangkat gateway pelanggan Anda.

Untuk langkah-langkah AWS konsol tertentu untuk membuat atau memodifikasi gateway transit yang akan digunakan untuk VPN IP pribadi, lihat Gateway [transit di Panduan Gateway Transit VPC Amazon](#).

Untuk membuat gateway transit menggunakan command line atau API

- [CreateTransitGateway](#) (Amazon EC2 Query API)
- [create-transit-gateway](#) (AWS CLI)

Buat AWS Direct Connect gateway

Buat AWS Direct Connect gateway dengan mengikuti prosedur [gateway Creating a Direct Connect](#) di Panduan AWS Direct Connect Pengguna.

Untuk membuat AWS Direct Connect gateway menggunakan command line atau API

- [CreateDirectConnectGateway](#)(API AWS Direct Connect Kueri)
- [create-direct-connect-gateway](#) (AWS CLI)

Buat asosiasi gateway transit

Setelah membuat AWS Direct Connect gateway, buat asosiasi gateway transit untuk AWS Direct Connect gateway. Tentukan CIDR IP pribadi untuk gateway transit yang diidentifikasi sebelumnya dalam daftar awalan yang diizinkan.

Untuk informasi selengkapnya, lihat [asosiasi Transit Gateway](#) di Panduan AWS Direct Connect Pengguna.

Untuk membuat asosiasi AWS Direct Connect gateway menggunakan baris perintah atau API

- [CreateDirectConnectGatewayAssociation](#)(API AWS Direct Connect Kueri)
- [create-direct-connect-gateway-asosiasi](#) ()AWS CLI

Buat koneksi VPN

Untuk membuat koneksi VPN menggunakan alamat IP pribadi

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

2. Di panel navigasi, pilih Koneksi VPN Site-to-Site.
3. Pilih Buat koneksi VPN.
4. (Opsional) Untuk Tanda nama, masukkan sebuah nama untuk koneksi Site-to-Site VPN. Dengan melakukan hal tersebut akan menciptakan tanda dengan kunci Name dan nilai yang Anda tentukan.
5. Untuk jenis gateway Target, pilih Transit gateway. Kemudian, pilih gateway transit yang Anda identifikasi sebelumnya.
6. Untuk gateway Pelanggan, pilih Existing. Kemudian, pilih gateway pelanggan yang Anda buat sebelumnya.
7. Pilih salah satu opsi perutean berdasarkan apakah perangkat gateway pelanggan Anda mendukung Border Gateway Protocol (BGP):
 - Jika perangkat gateway pelanggan Anda mendukung BGP, pilih Dinamis (membutuhkan BGP).
 - Jika perangkat gateway pelanggan Anda tidak mendukung BGP, pilih Statis.
8. Untuk Tunnel dalam versi IP, tentukan apakah terowongan VPN mendukung lalu lintas IPv4 atau IPv6.
9. (Opsional) Jika Anda menentukan IPv4 untuk Tunnel di dalam Versi IP, Anda dapat secara opsional menentukan rentang IPv4 CIDR untuk gateway pelanggan dan AWS sisi yang diizinkan untuk berkomunikasi melalui terowongan VPN. Nilai default-nya `0.0.0.0/0`.

Jika Anda menentukan IPv6 untuk Tunnel di dalam versi IP, Anda dapat secara opsional menentukan rentang IPv6 CIDR untuk gateway pelanggan dan AWS sisi yang diizinkan untuk berkomunikasi melalui terowongan VPN. Default untuk kedua rentang tersebut adalah `::/0`.
10. Untuk jenis alamat IP Luar, pilih PrivateIpv4.
11. Untuk ID lampiran Transport, pilih lampiran gateway transit untuk AWS Direct Connect gateway yang sesuai.
12. Pilih Buat koneksi VPN.

 Note

Opsi Aktifkan akselerasi tidak berlaku untuk koneksi VPN AWS Direct Connect.

Keamanan di AWS Site-to-Site VPN

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. [Model tanggung jawab bersama](#) menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari [Program AWS Kepatuhan Program AWS Kepatuhan](#). Untuk mempelajari tentang program kepatuhan yang berlaku untuk AWS Situs-ke-SitusVPN, lihat [AWS Layanan dalam Lingkup oleh Program Kepatuhan dalam Lingkup oleh Program Kepatuhan](#).
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan VPN Site-to-Site. Topik berikut menunjukkan cara mengonfigurasi Site-to-Site VPN untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Site-to-Site VPN Anda.

Daftar Isi

- [Perlindungan data di AWS Situs-ke-Situs VPN](#)
- [Manajemen identitas dan akses untuk AWS Site-to-Site VPN](#)
- [Ketahanan di AWS Site-to-Site VPN](#)
- [Keamanan infrastruktur di AWS Situs-ke-Situs VPN](#)

Perlindungan data di AWS Situs-ke-Situs VPN

[Model tanggung jawab AWS bersama model tanggung](#) berlaku untuk perlindungan data di AWS VPN Site-to-Site. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk

melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk AWS layanan yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat [Privasi Data FAQ](#). Untuk informasi tentang perlindungan data di Eropa, lihat [Model Tanggung Jawab AWS Bersama dan](#) posting GDPR blog di Blog AWS Keamanan.

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensial dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan otentikasi multi-faktor (MFA) dengan setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API dan log aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya AWS layanan.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan FIPS 140-3 modul kriptografi yang divalidasi saat mengakses AWS melalui antarmuka baris perintah atau, gunakan titik akhir. API FIPS Untuk informasi selengkapnya tentang FIPS titik akhir yang tersedia, lihat [Standar Pemrosesan Informasi Federal \(FIPS\) 140-3](#).

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk ketika Anda bekerja dengan Site-to-Site VPN atau lainnya AWS layanan menggunakan konsol, API, AWS CLI atau. AWS SDKs Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Jika Anda memberikan URL ke server eksternal, kami sangat menyarankan agar Anda tidak menyertakan informasi kredensial dalam URL untuk memvalidasi permintaan Anda ke server tersebut.

Privasi lalu lintas antar jaringan

VPN Koneksi Site-to-Site secara pribadi menghubungkan Anda VPC ke jaringan lokal Anda. Data yang ditransfer antara rute jaringan Anda VPC dan Anda melalui VPN koneksi terenkripsi untuk membantu menjaga kerahasiaan dan integritas data dalam perjalanan. Amazon mendukung koneksi keamanan Protokol Internet (IPsec) VPN. IPsec adalah suite protokol untuk mengamankan komunikasi IP dengan mengautentikasi dan mengenkripsi setiap paket IP dalam aliran data.

Setiap VPN koneksi Site-to-Site terdiri dari dua IPsec VPN terowongan terenkripsi yang menghubungkan dan jaringan Anda. AWS Lalu lintas di setiap terowongan dapat dienkripsi dengan AES128 atau AES256 dan menggunakan grup Diffie-Hellman untuk pertukaran kunci, memberikan Perfect Forward Secrecy. AWS mengautentikasi dengan SHA1 atau fungsi SHA2 hashing.

Contoh di Anda VPC tidak memerlukan alamat IP publik untuk terhubung ke sumber daya di sisi lain koneksi Site-to-Site VPN Anda. Instans dapat merutekan lalu lintas internet mereka melalui VPN koneksi Site-to-Site ke jaringan lokal Anda. Mereka kemudian dapat mengakses internet melalui titik lalu lintas keluar yang ada serta keamanan jaringan dan perangkat pemantauan Anda.

Lihat topik berikut untuk informasi selengkapnya:

- [Opsinya terowongan untuk koneksi Site-to-Site VPN Anda](#): Menyediakan informasi tentang IPsec dan opsi Internet Key Exchange (IKE) yang tersedia untuk setiap terowongan.
- [Opsinya otentikasi terowongan situs-ke-situs VPN](#): Menyediakan informasi tentang opsi otentikasi untuk titik akhir VPN terowongan Anda.
- [Persyaratan untuk perangkat gateway pelanggan Anda](#): Memberikan informasi tentang persyaratan untuk perangkat gateway pelanggan di sisi VPN koneksi Anda.
- [Menyediakan komunikasi yang aman antar situs menggunakan VPN CloudHub](#): Jika Anda memiliki beberapa VPN koneksi Site-to-Site, Anda dapat menyediakan komunikasi yang aman antara situs lokal Anda dengan menggunakan AWS VPN CloudHub.

Manajemen identitas dan akses untuk AWS Site-to-Site VPN

AWS Identity and Access Management (IAM) adalah AWS layanan yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. IAM administrator mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Situs-ke-Situs. VPN IAM adalah AWS layanan yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- [Audiens](#)
- [Mengautentikasi dengan identitas](#)
- [Mengelola akses menggunakan kebijakan](#)
- [Bagaimana AWS VPN Site-to-Site bekerja dengan IAM](#)
- [Contoh kebijakan berbasis identitas untuk Site-to-Site AWS VPN](#)
- [Pemecahan masalah Identitas dan akses AWS situs-ke-situs VPN](#)
- [Menggunakan peran terkait layanan untuk Site-to-Site VPN](#)

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di VPN Site-to-Site.

Pengguna layanan — Jika Anda menggunakan VPN layanan Site-to-Site untuk melakukan pekerjaan Anda, maka administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak VPN fitur Site-to-Site untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Site-to-SiteVPN, lihat. [Pemecahan masalah Identitas dan akses AWS situs-ke-situs VPN](#)

Administrator layanan — Jika Anda bertanggung jawab atas VPN sumber daya Situs-ke-Situs di perusahaan Anda, Anda mungkin memiliki akses penuh ke Site-to-Site. VPN Tugas Anda adalah menentukan VPN fitur dan sumber daya Site-to-Site mana yang harus diakses pengguna layanan Anda. Anda kemudian harus mengirimkan permintaan ke IAM administrator Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasarIAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM Site-to-SiteVPN, lihat. [Bagaimana AWS VPN Site-to-Site bekerja dengan IAM](#)

IAM administrator - Jika Anda seorang IAM administrator, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke VPN Site-to-Site. Untuk melihat contoh kebijakan VPN berbasis identitas situs ke situs yang dapat Anda gunakan, lihat. IAM [Contoh kebijakan berbasis identitas untuk Site-to-Site AWS VPN](#)

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai IAM pengguna, atau dengan mengambil peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensi yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (Pusat IAM Identitas), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas federasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan IAM peran. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat [Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS](#).

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensial Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang menggunakan metode yang disarankan untuk menandatangani permintaan sendiri, lihat [Menandatangani AWS API permintaan](#) di Panduan IAM Pengguna.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari lebih lanjut, lihat [Autentikasi multi-faktor](#) di Panduan AWS IAM Identity Center Pengguna dan [Menggunakan otentikasi multi-faktor \(MFA\) AWS](#) di Panduan Pengguna. IAM

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua AWS layanan dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas

yang mengharuskan Anda masuk sebagai pengguna root, lihat [Tugas yang memerlukan kredensi pengguna root](#) di IAMPanduan Pengguna.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS layanan dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses AWS layanan dengan menggunakan kredensial yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat IAM Identitas, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat IAM Identitas, lihat [Apa itu Pusat IAM Identitas?](#) dalam AWS IAM Identity Center User Guide.

Pengguna dan grup IAM

[IAMPengguna](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya mengandalkan kredensi sementara daripada membuat IAM pengguna yang memiliki kredensi jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensial jangka panjang dengan IAM pengguna, kami sarankan Anda memutar kunci akses. Untuk informasi selengkapnya, lihat [Memutar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensi jangka panjang](#) di IAMPanduan Pengguna.

[IAMGrup](#) adalah identitas yang menentukan kumpulan IAM pengguna. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup bernama IAMAdmins dan memberikan izin grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara.

Untuk mempelajari lebih lanjut, lihat [Kapan membuat IAM pengguna \(bukan peran\)](#) di Panduan IAM Pengguna.

IAMperan

[IAMPeran](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Ini mirip dengan IAM pengguna, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil IAM peran sementara AWS Management Console dengan [beralih peran](#). Anda dapat mengambil peran dengan memanggil AWS CLI atau AWS API operasi atau dengan menggunakan kustomURL. Untuk informasi selengkapnya tentang metode penggunaan peran, lihat [Menggunakan IAM peran](#) di Panduan IAM Pengguna.

IAMperan dengan kredensi sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat [Membuat peran untuk Penyedia Identitas pihak ketiga](#) di Panduan IAM Pengguna. Jika Anda menggunakan Pusat IAM Identitas, Anda mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah diautentikasi, Pusat IAM Identitas menghubungkan izin yang disetel ke peran. Untuk informasi tentang set izin, lihat [Set izin](#) dalam Panduan Pengguna AWS IAM Identity Center .
- Izin IAM pengguna sementara — IAM Pengguna atau peran dapat mengambil IAM peran untuk sementara mengambil izin yang berbeda untuk tugas tertentu.
- Akses lintas akun — Anda dapat menggunakan IAM peran untuk memungkinkan seseorang (prinsipal tepercaya) di akun lain mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa AWS layanan, Anda dapat melampirkan kebijakan langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM](#) Panduan Pengguna. IAM
- Akses lintas layanan — Beberapa AWS layanan menggunakan fitur lain AWS layanan. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
 - Sesi akses teruskan (FAS) — Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan

beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama AWS layanan, dikombinasikan dengan permintaan AWS layanan untuk membuat permintaan ke layanan hilir. FAS permintaan hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain AWS layanan atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat [Meneruskan sesi akses](#).

- Peran layanan — Peran layanan adalah [IAM peran](#) yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAM Administrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Membuat peran untuk mendelegasikan izin ke AWS layanan](#) dalam IAM Panduan Pengguna.
- Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke AWS layanan. Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. IAM Administrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan IAM peran untuk mengelola kredensial sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS API meminta. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat [Menggunakan IAM peran untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon](#) di IAM Panduan Pengguna.

Untuk mempelajari apakah akan menggunakan IAM peran atau IAM pengguna, lihat [Kapan membuat IAM peran \(bukan pengguna\)](#) di Panduan IAM Pengguna.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai JSON dokumen. Untuk informasi selengkapnya tentang struktur dan isi dokumen JSON kebijakan, lihat [Ringkasan JSON kebijakan](#) di Panduan IAM Pengguna.

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka butuhkan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

IAMkebijakan menentukan izin untuk tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasi. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan itu bisa mendapatkan informasi peran dari AWS Management Console, AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat dilampirkan ke identitas, seperti pengguna, grup IAM pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Membuat IAM kebijakan di Panduan Pengguna](#). IAM

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat dilampirkan ke beberapa pengguna, grup, dan peran dalam akun AWS. Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan sebaris, lihat [Memilih antara kebijakan terkelola dan kebijakan sebaris](#) di IAMPanduan Pengguna.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan prinsipal](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau AWS layanan

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACLs)

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACLs. Untuk mempelajari selengkapnya ACLs, lihat [Ikhtisar daftar kontrol akses \(ACL\)](#) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- **Batas izin** — Batas izin adalah fitur lanjutan tempat Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas (pengguna atau peran). IAM Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batas izin, lihat [Batas izin untuk IAM entitas](#) di IAM Panduan Pengguna.
- **Kebijakan kontrol layanan (SCPs)** — SCPs adalah JSON kebijakan yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCPs membatasi izin untuk entitas di akun anggota, termasuk masing-masing Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organizations dan SCPs, lihat [Kebijakan kontrol layanan](#) di Panduan AWS Organizations Pengguna.
- **Kebijakan sesi** – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan

secara tegas dalam salah satu kebijakan ini membatalkan izin. Untuk informasi selengkapnya, lihat [Kebijakan sesi](#) di Panduan IAM Pengguna.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat [Logika evaluasi kebijakan](#) di Panduan IAM Pengguna.

Bagaimana AWS VPN Site-to-Site bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Site-to-SiteVPN, pelajari IAM fitur apa saja yang tersedia untuk digunakan dengan Site-to-Site. VPN

IAMfitur yang dapat Anda gunakan dengan AWS Site-to-Site VPN

IAMfitur	Dukungan situs-ke-situs VPN
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
ACLs	Tidak
ABAC(tag dalam kebijakan)	Tidak
Kredensial sementara	Ya
Izin prinsipal	Ya
Peran layanan	Ya
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Situs-ke-Situs VPN dan AWS layanan lainnya dengan sebagian besar IAM fitur, lihat [AWS layanan yang berfungsi IAM di Panduan Pengguna](#). IAM

Kebijakan berbasis identitas untuk Situs-ke-Situs VPN

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat dilampirkan ke identitas, seperti pengguna, grup IAM pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Membuat IAM kebijakan di Panduan Pengguna](#). IAM

Dengan kebijakan IAM berbasis identitas, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak serta kondisi di mana tindakan diizinkan atau ditolak. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam JSON kebijakan, lihat [referensi elemen IAM JSON kebijakan](#) di Panduan IAM Pengguna.

Contoh kebijakan berbasis identitas untuk Site-to-Site VPN

Untuk melihat contoh kebijakan berbasis VPN identitas Site-to-Site, lihat. [Contoh kebijakan berbasis identitas untuk Site-to-Site AWS VPN](#)

Kebijakan berbasis sumber daya dalam Situs-ke-Situs VPN

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan prinsipal](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. AWS layanan

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan seluruh akun atau IAM entitas di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, IAM administrator di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke prinsipal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun IAM di](#) Panduan IAM Pengguna.

Tindakan kebijakan untuk Situs-ke-Situs VPN

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

ActionElemen JSON kebijakan menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan AWS API operasi terkait. Ada beberapa pengecualian, seperti tindakan khusus izin yang tidak memiliki operasi yang cocok. API Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar tindakan Situs-ke-Situs, lihat VPN [Tindakan yang ditentukan oleh AWS Situs-ke-Situs VPN](#) dalam Referensi Otorisasi Layanan.

Tindakan kebijakan di Situs-ke-Situs VPN menggunakan awalan berikut sebelum tindakan:

```
ec2
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [  
  "ec2:action1",  
  "ec2:action2"
```

```
] ]
```

Untuk melihat contoh kebijakan berbasis VPN identitas Site-to-Site, lihat. [Contoh kebijakan berbasis identitas untuk Site-to-Site AWS VPN](#)

Sumber daya kebijakan untuk Site-to-Site VPN

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Resource` JSON kebijakan menentukan objek atau objek yang tindakan tersebut berlaku. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Sebagai praktik terbaik, tentukan sumber daya menggunakan [Amazon Resource Name \(ARN\)](#). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*" ]
```

Untuk melihat daftar jenis sumber daya Situs-ke-Situs dan jenisnya ARNs, lihat VPN Sumber Daya yang [ditentukan oleh AWS Site-to-Site VPN](#) dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat [Tindakan yang ditentukan oleh AWS VPN Site-to-Site](#).

Untuk melihat contoh kebijakan berbasis VPN identitas Site-to-Site, lihat. [Contoh kebijakan berbasis identitas untuk Site-to-Site AWS VPN](#)

Kunci kondisi kebijakan untuk Site-to-Site VPN

Mendukung kunci kondisi kebijakan khusus layanan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan [operator kondisi](#), misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi AND logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan OR operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Misalnya, Anda dapat memberikan izin IAM pengguna untuk mengakses sumber daya hanya jika ditandai dengan nama IAM pengguna mereka. Untuk informasi selengkapnya, lihat [elemen IAM kebijakan: variabel dan tag](#) di Panduan IAM Pengguna.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat [kunci konteks kondisi AWS global](#) di Panduan IAM Pengguna.

Untuk melihat daftar kunci kondisi Site-to-Site, lihat Kunci VPN kondisi [untuk AWS Site-to-Site VPN dalam Referensi](#) Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat [Tindakan yang ditentukan oleh AWS VPN Site-to-Site](#).

Untuk melihat contoh kebijakan berbasis VPN identitas Site-to-Site, lihat. [Contoh kebijakan berbasis identitas untuk Site-to-Site AWS VPN](#)

ACLs di Site-to-site VPN

Mendukung ACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

ABAC dengan Site-to-Site VPN

Mendukung ABAC (tag dalam kebijakan): Tidak

Attribute-based access control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke IAM entitas (pengguna atau peran) dan ke banyak AWS sumber daya. Menandai entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian Anda merancang ABAC kebijakan untuk mengizinkan operasi ketika tag prinsipal cocok dengan tag pada sumber daya yang mereka coba akses.

ABAC membantu dalam lingkungan yang berkembang pesat dan membantu dengan situasi di mana manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tag di [elemen kondisi](#) dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi lebih lanjut tentang ABAC, lihat [Apa itu ABAC?](#) dalam IAM User Guide. Untuk melihat tutorial dengan langkah-langkah persiapan ABAC, lihat [Menggunakan kontrol akses berbasis atribut \(ABAC\)](#) di IAM Panduan Pengguna.

Menggunakan kredensi sementara dengan Site-to-Site VPN

Mendukung kredensi sementara: Ya

Beberapa AWS layanan tidak berfungsi saat Anda masuk menggunakan kredensi sementara. Untuk informasi tambahan, termasuk yang AWS layanan bekerja dengan kredensi sementara, lihat [AWS layanan yang berfungsi IAM](#) di IAM Panduan Pengguna.

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan link sign-on (SSO) tunggal perusahaan Anda, proses tersebut secara otomatis membuat kredensi sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang beralih peran, lihat [Beralih ke peran \(konsol\)](#) di Panduan IAM Pengguna.

Anda dapat secara manual membuat kredensi sementara menggunakan `awscli` atau `awscli` API. Anda kemudian dapat menggunakan kredensi sementara tersebut untuk mengakses AWS. AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih

menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat [Kredensi keamanan sementara](#) di IAM

Izin utama lintas layanan untuk Site-to-Site VPN

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama AWS layanan, dikombinasikan dengan permintaan AWS layanan untuk membuat permintaan ke layanan hilir. FAS permintaan hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain AWS layanan atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat [Meneruskan sesi akses](#).

Peran layanan untuk Site-to-Site VPN

Mendukung peran layanan: Ya

Peran layanan adalah [IAM peran](#) yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAM Administrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Membuat peran untuk mendelegasikan izin ke AWS layanan](#) dalam IAMPanduan Pengguna.

Warning

Mengubah izin untuk peran layanan dapat merusak fungsionalitas VPN Site-to-Site. Edit peran layanan hanya jika Site-to-Site VPN memberikan panduan untuk melakukannya.

Peran terkait layanan untuk Site-to-Site VPN

Mendukung peran terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke AWS layanan Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. IAM Administrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.

Untuk detail tentang membuat atau mengelola peran terkait layanan, lihat [AWS layanan yang berfungsi](#) dengannya. IAM Cari layanan dalam tabel yang memiliki Yes di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Contoh kebijakan berbasis identitas untuk Site-to-Site AWS VPN

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya VPN Site-to-Site. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka butuhkan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan IAM berbasis identitas menggunakan contoh dokumen kebijakan ini, lihat [Membuat JSON IAM kebijakan di Panduan Pengguna](#). IAM

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Situs-ke-SitusVPN, termasuk format ARNs untuk setiap jenis sumber daya, lihat [Tindakan, sumber daya, dan kunci kondisi untuk AWS Situs-ke-Situs VPN](#) dalam Referensi Otorisasi Layanan.

Topik

- [Praktik terbaik kebijakan](#)
- [Menggunakan konsol Site-to-Site VPN](#)
- [Jelaskan koneksi Site-to-site VPN tertentu](#)
- [Buat dan jelaskan sumber daya yang dibutuhkan untuk AWS Site-to-Site VPN koneksi](#)

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya VPN Situs-ke-Situs di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan

yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat [kebijakan AWSAWS terkelola](#) atau [kebijakan terkelola untuk fungsi pekerjaan](#) di Panduan IAM Pengguna.

- Menerapkan izin hak istimewa paling sedikit — Saat Anda menetapkan izin dengan IAM kebijakan, berikan hanya izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang penggunaan IAM untuk menerapkan izin, lihat [Kebijakan dan izin IAM di IAM](#) Panduan Pengguna.
- Gunakan ketentuan dalam IAM kebijakan untuk membatasi akses lebih lanjut — Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik AWS layanan, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat [elemen IAM JSON kebijakan: Kondisi](#) dalam Panduan IAM Pengguna.
- Gunakan IAM Access Analyzer untuk memvalidasi IAM kebijakan Anda guna memastikan izin yang aman dan fungsional — IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan mematuhi bahasa IAM kebijakan () JSON dan praktik terbaik. IAM IAMAccess Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat [Validasi kebijakan IAM Access Analyzer](#) di IAMPanduan Pengguna.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan IAM pengguna atau pengguna root di Anda Akun AWS, aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA kapan API operasi dipanggil, tambahkan MFA kondisi ke kebijakan Anda. Untuk informasi selengkapnya, lihat [Mengonfigurasi API akses MFA yang dilindungi](#) di IAMPanduan Pengguna.

Untuk informasi selengkapnya tentang praktik terbaik diIAM, lihat [Praktik terbaik keamanan IAM di](#) Panduan IAM Pengguna.

Menggunakan konsol Site-to-Site VPN

Untuk mengakses VPN konsol AWS Site-to-Site, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Situs-ke-Situs di situs VPN Anda. Akun AWS Jika Anda membuat kebijakan berbasis identitas yang lebih ketat

daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang cocok dengan API operasi yang mereka coba lakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan VPN konsol Site-to-Site, lampirkan juga kebijakan Site-to-Site VPN `AmazonVPCFullAccess` atau `AmazonVPCReadOnlyAccess` AWS managed ke entitas. Untuk informasi selengkapnya, lihat [Menambahkan izin ke pengguna](#) di Panduan IAM Pengguna.

Jelaskan koneksi Site-to-site VPN tertentu

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpnConnections"
      ],
      "Resource": [
        "arn:aws:ec2:us-west-2:123456789012:vpn-connection/vpn-04d5cc9b88example",
        "arn:aws:ec2:us-west-2:123456789012:vpn-connection/vpn-903004f88example"
      ]
    }
  ]
}
```

Buat dan jelaskan sumber daya yang dibutuhkan untuk AWS Site-to-Site VPN koneksi

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

```

```

    "ec2:CreateCustomerGateway",
    "ec2:CreateVpnGateway",
    "ec2:CreateVpnConnection"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Effect": "Allow",
  "Action": "iam:CreateServiceLinkedRole",
  "Resource": "arn:aws:iam::*:role/aws-service-role/s2svpn.amazonaws.com/
AWSServiceRoleForVPCS2SVPNInternal",
  "Condition": {
    "StringLike": {
      "iam:AWSServiceName": "s2svpn.amazonaws.com"
    }
  }
}
]
}

```

Pemecahan masalah Identitas dan akses AWS situs-ke-situs VPN

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan VPN Site-to-Site dan IAM

Topik

- [Saya tidak berwenang untuk melakukan tindakan di Site-to-Site VPN](#)
- [Saya tidak berwenang untuk melakukan iam: PassRole](#)
- [Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses sumber daya Site-to-Site VPN saya](#)

Saya tidak berwenang untuk melakukan tindakan di Site-to-Site VPN

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika `mateojackson` IAM pengguna mencoba menggunakan konsol untuk melihat detail tentang `my-example-widget` sumber daya fiksi tetapi tidak memiliki izin `ec2:GetWidget` fiksi.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
ec2:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya `my-example-widget` dengan menggunakan tindakan `ec2:GetWidget`.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan `iam:PassRole`

Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke VPN Site-to-Site.

Beberapa AWS layanan memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika IAM pengguna bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di VPN Site-to-Site. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses sumber daya Site-to-Site VPN saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang

dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah Site-to-Site VPN mendukung fitur-fitur ini, lihat [Bagaimana AWS VPN Site-to-Site bekerja dengan IAM](#)
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat [Menyediakan akses ke IAM pengguna lain Akun AWS yang Anda miliki](#) di Panduan IAM Pengguna.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat [Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga](#) dalam Panduan IAM Pengguna.
- Untuk mempelajari cara menyediakan akses melalui federasi identitas, lihat [Menyediakan akses ke pengguna yang diautentikasi secara eksternal \(federasi identitas\) di Panduan Pengguna](#). IAM
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM](#) Panduan Pengguna. IAM

Menggunakan peran terkait layanan untuk Site-to-Site VPN

AWS [Site-to-site VPN menggunakan AWS Identity and Access Management \(IAM\) peran terkait layanan](#). Peran terkait layanan adalah jenis peran unik yang ditautkan langsung ke Site-to-Site. IAM VPN Peran terkait layanan telah ditentukan sebelumnya oleh Site-to-Site VPN dan mencakup semua izin yang diperlukan layanan untuk memanggil layanan lain atas nama Anda. AWS

Peran terkait layanan membuat pengaturan Site-to-Site VPN lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Site-to-Site VPN mendefinisikan izin dari peran terkait layanannya, dan kecuali ditentukan lain, hanya Site-to-Site yang dapat mengambil perannya. VPN Izin yang ditetapkan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas lain. IAM

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi VPN sumber daya Site-to-Site Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat [AWS Layanan yang Bekerja dengan IAM](#) dan cari layanan yang memiliki Ya di kolom Peran terkait layanan. Pilih Ya bersama tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Izin peran terkait layanan untuk Site-to-Site VPN

Site-to-Site VPN menggunakan peran terkait layanan bernama `AWSServiceRoleForVPCS2SVPN`—Izinkan Site-to-Site VPN untuk membuat dan mengelola sumber daya yang terkait dengan koneksi Anda. VPN

Peran `AWSServiceRoleForVPCS2SVPN` terkait layanan mempercayai layanan berikut untuk mengambil peran:

- AWS Certificate Manager
- AWS Private Certificate Authority

Kebijakan izin peran bernama `AWSVPCS2SVpnServiceRolePolicy` memungkinkan Site-to-Site VPN untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: `acm:ExportCertificate` pada Resource: `"*"`
- Tindakan: `acm:DescribeCertificate` pada Resource: `"*"`
- Tindakan: `acm:ListCertificates` pada Resource: `"*"`
- Tindakan: `acm-pca:DescribeCertificateAuthority` pada Resource: `"*"`

Anda harus mengonfigurasi izin untuk mengizinkan IAM entitas (seperti pengguna, grup, atau peran) membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat [Izin peran terkait layanan di Panduan Pengguna IAM](#).

Membuat peran terkait layanan untuk Site-to-Site VPN

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat gateway pelanggan dengan sertifikat ACM pribadi terkait di, atau AWS Management Console AWS CLI AWS API, Site-to-Site VPN membuat peran terkait layanan untuk Anda.

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda membuat gateway pelanggan dengan sertifikat ACM pribadi terkait, Site-to-Site akan VPN membuat peran terkait layanan untuk Anda lagi.

Mengedit peran terkait layanan untuk Site-to-Site VPN

Site-to-site VPN tidak memungkinkan Anda untuk mengedit peran terkait layanan.

`AWSServiceRoleForVPCs2SVPN` Setelah Anda membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengedit deskripsi peran menggunakan IAM. Untuk informasi selengkapnya, lihat [Mengedit peran terkait layanan](#) di [IAM Panduan Pengguna](#).

Menghapus peran terkait layanan untuk Site-to-Site VPN

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami merekomendasikan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Tetapi, Anda harus membersihkan sumber daya peran yang terhubung dengan layanan sebelum menghapusnya secara manual.

Note

Jika VPN layanan Site-to-Site menggunakan peran saat Anda mencoba menghapus sumber daya, maka penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus VPN sumber daya Site-to-Site yang digunakan oleh `AWSServiceRoleForVPCs2SVPN`

Anda dapat menghapus peran terkait layanan ini hanya setelah Anda menghapus semua gateway pelanggan yang memiliki sertifikat pribadi terkait. ACM Ini memastikan bahwa Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses ACM sertifikat yang digunakan oleh koneksi Site-to-Site. VPN

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan IAM konsol, AWS CLI, atau AWS API untuk menghapus peran `AWSServiceRoleForVPCs2SVPN` terkait layanan. Untuk informasi selengkapnya, lihat [Menghapus peran terkait layanan di Panduan Pengguna](#). IAM

Ketahanan di AWS Site-to-Site VPN

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat [Infrastruktur AWS Global](#).

Selain infrastruktur AWS global, Site-to-Site VPN menawarkan fitur untuk membantu mendukung ketahanan data dan kebutuhan cadangan Anda.

Dua terowongan per koneksi VPN

VPN Koneksi Site-to-Site terdiri dari dua terowongan, masing-masing berakhir di Availability Zone yang berbeda, untuk memberikan peningkatan ketersediaan bagi Anda. VPC Jika ada kegagalan perangkat di dalam AWS, VPN koneksi Anda secara otomatis gagal ke terowongan kedua sehingga akses Anda tidak terganggu. Dari waktu ke waktu, AWS juga melakukan pemeliharaan rutin pada VPN koneksi Anda, yang secara singkat dapat menonaktifkan salah satu dari dua terowongan VPN koneksi Anda. Untuk informasi selengkapnya, lihat [Penggantian titik akhir terowongan Site-to-Site VPN](#). Ketika Anda mengonfigurasi gateway pelanggan Anda, oleh karena itu penting untuk Anda mengonfigurasi kedua terowongan.

Redundansi

Untuk melindungi dari hilangnya konektivitas jika gateway pelanggan Anda tidak tersedia, Anda dapat mengatur koneksi Site-to-Site VPN kedua. Untuk informasi selengkapnya, lihat dokumentasi berikut ini:

- [Menggunakan koneksi Site-to-Site VPN berlebih untuk memberikan failover](#)
- [Opsi Konektivitas Amazon Virtual Private Cloud](#)
- [Membangun Infrastruktur Multi VPC AWS Jaringan yang Skalabel dan Aman](#)

Keamanan infrastruktur di AWS Situs-ke-Situs VPN

Sebagai layanan terkelola, AWS Site-to-Site VPN dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat [Keamanan AWS Cloud](#). Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat [Perlindungan Infrastruktur dalam Kerangka Kerja](#) yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan API panggilan yang AWS dipublikasikan untuk mengakses Site-to-Site VPN melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Transportasi (TLS). Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Suite cipher dengan kerahasiaan maju yang sempurna (PFS) seperti (Ephemeral Diffie-Hellman) atau DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani dengan menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan IAM prinsipal. Atau Anda bisa menggunakan [AWS Security Token Service](#) (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Memantau koneksi Site-to-Site VPN Anda

Pemantauan adalah bagian penting untuk menjaga keandalan, ketersediaan, dan kinerja AWS Site-to-Site VPN koneksi Anda. Anda harus mengumpulkan data pemantauan dari semua bagian dari solusi Anda sehingga Anda dapat lebih mudah men-debug kegagalan multi-titik jika terjadi. Sebelum Anda mulai memantau koneksi Site-to-Site VPN Anda; bagaimanapun, Anda harus membuat rencana pemantauan yang mencakup jawaban atas pertanyaan-pertanyaan berikut:

- Apa sasaran pemantauan Anda?
- Sumber daya apa yang akan Anda pantau?
- Seberapa sering Anda akan memantau sumber daya ini?
- Alat pemantauan apa yang akan Anda gunakan?
- Siapa yang akan melakukan tugas pemantauan?
- Siapa yang harus diberi tahu saat terjadi kesalahan?

Langkah berikutnya adalah menetapkan baseline untuk performa normal VPN di lingkungan Anda, dengan mengukur performa di berbagai waktu dan di bawah kondisi beban yang berbeda. Saat memantau VPN Anda, simpan data pemantauan historis sehingga Anda dapat membandingkannya dengan data performa saat ini, mengidentifikasi pola performa normal dan anomali performa, dan merancang metode untuk mengatasi masalah tersebut.

Untuk menetapkan baseline, Anda harus memantau item berikut:

- Status terowongan VPN Anda
- Data masuk ke dalam terowongan
- Data keluar dari terowongan

Daftar Isi

- [Alat pemantauan](#)
- [AWS Site-to-Site VPN log](#)
- [Memantau terowongan VPN menggunakan Amazon CloudWatch](#)
- [Memantau koneksi VPN menggunakan AWS Health acara](#)

Alat pemantauan

AWS menyediakan berbagai alat yang dapat Anda gunakan untuk memantau koneksi VPN Site-to-Site. Anda dapat mengonfigurasi beberapa alat ini untuk melakukan pemantauan untuk Anda, sementara beberapa alat memerlukan intervensi manual. Kami menyarankan agar Anda mengotomatiskan tugas pemantauan sebanyak mungkin.

Alat pemantauan otomatis

Anda dapat menggunakan alat pemantauan otomatis berikut untuk koneksi Site-to-Site VPN dan melaporkan saat terjadi kesalahan:

- CloudWatch Alarm Amazon — Tonton satu metrik selama periode waktu yang Anda tentukan, dan lakukan satu atau beberapa tindakan berdasarkan nilai metrik relatif terhadap ambang batas tertentu selama beberapa periode waktu. Tindakannya adalah pemberitahuan yang dikirim ke topik Amazon SNS. CloudWatch alarm tidak memanggil tindakan hanya karena mereka berada dalam keadaan tertentu; negara harus telah berubah dan dipertahankan untuk sejumlah periode tertentu. Untuk informasi selengkapnya, lihat [Memantau terowongan VPN menggunakan Amazon CloudWatch](#).
- AWS CloudTrail Pemantauan Log - Bagikan file log antar akun, pantau file CloudTrail log secara real time dengan mengirimkannya ke CloudWatch Log, menulis aplikasi pemrosesan log di Java, dan validasi bahwa file log Anda tidak berubah setelah pengiriman oleh CloudTrail. Untuk informasi selengkapnya, lihat [Mencatat Panggilan API Menggunakan AWS CloudTrail](#) Referensi API Amazon EC2 dan [Bekerja dengan file CloudTrail log](#) di AWS CloudTrail Panduan Pengguna.
- AWS Health event — Menerima peringatan dan pemberitahuan terkait perubahan kesehatan terowongan VPN Site-to-Site Anda, rekomendasi konfigurasi praktik terbaik, atau saat mendekati batas penskalaan. Gunakan kejadian di [Personal Health Dashboard](#) untuk memicu failover otomatis, mengurangi waktu pemecahan masalah, atau mengoptimalkan koneksi untuk ketersediaan tinggi. Untuk informasi selengkapnya, lihat [Memantau koneksi VPN menggunakan AWS Health acara](#).

Alat pemantauan manual

Bagian penting lainnya dari pemantauan koneksi VPN Site-to-Site melibatkan pemantauan secara manual item yang CloudWatch tidak tercakup oleh alarm. Dasbor VPC dan CloudWatch konsol Amazon memberikan at-a-glance tampilan keadaan lingkungan Anda. AWS

Note

Di konsol VPC Amazon, parameter status terowongan VPN Site-to-Site seperti “Status” dan “Perubahan status terakhir”, mungkin tidak mencerminkan perubahan status sementara atau penutup terowongan sesaat. Disarankan untuk menggunakan CloudWatch metrik dan log untuk pembaruan perubahan status terowongan granular.

- Dasbor Amazon VPC menunjukkan:
 - Kondisi layanan menurut Wilayah
 - Koneksi Site-to-Site VPN
 - Status terowongan VPN (Di panel navigasi, pilih Koneksi Site-to-Site VPN, pilih koneksi Site-to-Site VPN, dan kemudian pilih Detail Terowongan)
- CloudWatch Halaman beranda menunjukkan:
 - Alarm dan status saat ini
 - Grafik alarm dan sumber daya
 - Status kesehatan layanan

Selain itu, Anda dapat menggunakan CloudWatch untuk melakukan hal berikut:

- Membuat [dasbor yang disesuaikan](#) untuk memantau layanan yang penting bagi Anda
- Data metrik grafik untuk memecahkan masalah dan mengungkap tren
- Cari dan telusuri semua metrik AWS sumber daya Anda
- Membuat dan mengedit alarm untuk menerima notifikasi terkait masalah

AWS Site-to-Site VPN log

AWS Site-to-Site VPN log memberi Anda visibilitas yang lebih dalam ke penerapan VPN Site-to-Site Anda. Dengan fitur ini, Anda memiliki akses ke log koneksi VPN Site-to-Site yang memberikan rincian tentang pembentukan terowongan IP Security (IPsec), negosiasi Internet Key Exchange (IKE), dan pesan protokol deteksi rekan mati (DPD).

Log VPN Site-to-Site dapat dipublikasikan ke Amazon Logs. CloudWatch Fitur ini memberi pelanggan satu cara konsisten untuk mengakses dan menganalisis log terperinci untuk semua koneksi VPN Site-to-Site mereka.

Daftar Isi

- [Manfaat log VPN Site-to-Site](#)
- [Pembatasan ukuran kebijakan sumber daya Amazon CloudWatch Logs](#)
- [Isi log VPN Site-to-Site](#)
- [Persyaratan IAM untuk mempublikasikan ke CloudWatch Log](#)
- [Lihat konfigurasi log VPN Site-to-Site](#)
- [Aktifkan log VPN Site-to-Site](#)
- [Nonaktifkan log VPN Site-to-Site](#)

Manfaat log VPN Site-to-Site

- Pemecahan masalah VPN yang disederhanakan: Log VPN Site-to-Site membantu Anda menentukan AWS ketidakcocokan konfigurasi antara dan perangkat gateway pelanggan Anda, dan mengatasi masalah konektivitas VPN awal. Koneksi VPN dapat sebentar-sebentar menutup dari waktu ke waktu karena pengaturan yang salah konfigurasi (seperti batas waktu yang disetel dengan buruk), mungkin ada masalah di jaringan transportasi yang mendasarinya (seperti cuaca internet), atau perubahan perutean atau kegagalan jalur dapat menyebabkan gangguan konektivitas melalui VPN. Fitur ini memungkinkan Anda untuk secara akurat mendiagnosis penyebab kegagalan koneksi intermiten dan menyempurnakan konfigurasi terowongan tingkat rendah untuk operasi yang andal.
- AWS Site-to-Site VPN Visibilitas terpusat: Log VPN Site-to-Site dapat menyediakan log aktivitas terowongan untuk semua cara berbeda yang terhubung dengan Site-to-Site VPN: Virtual Gateway, Transit Gateway, dan, menggunakan internet dan sebagai transportasi. CloudHub AWS Direct Connect Fitur ini memberi pelanggan satu cara konsisten untuk mengakses dan menganalisis log terperinci untuk semua koneksi VPN Site-to-Site mereka.
- Keamanan dan kepatuhan: Log VPN Site-to-Site dapat dikirim ke CloudWatch Amazon Logs untuk analisis retrospektif status dan aktivitas koneksi VPN dari waktu ke waktu. Ini dapat membantu Anda memenuhi persyaratan kepatuhan dan peraturan.

Pembatasan ukuran kebijakan sumber daya Amazon CloudWatch Logs

CloudWatch Kebijakan sumber daya log dibatasi hingga 5120 karakter. Ketika CloudWatch Log mendeteksi bahwa kebijakan mendekati batas ukuran ini, secara otomatis mengaktifkan grup log yang memulai `/aws/vendedLogs/`. Saat Anda mengaktifkan logging, Site-to-Site VPN harus

memperbarui kebijakan sumber daya Log CloudWatch Anda dengan grup log yang Anda tentukan. Untuk menghindari mencapai batas ukuran kebijakan sumber daya CloudWatch Log, awali nama grup log Anda dengan `/aws/vendedlogs/`.

Isi log VPN Site-to-Site

Informasi berikut disertakan dalam log aktivitas terowongan VPN Site-to-Site.

Bidang	Deskripsi
VpnLogCreationTimestamp	Stempel waktu pembuatan log dalam format yang dapat dibaca manusia.
VpnConnectionId	Pengidentifikasi koneksi VPN.
TunnelOutsideIPAddress	IP eksternal dari terowongan VPN yang menghasilkan entri log.
TunnelDpdEnabled	Status Diaktifkan Protokol Deteksi Rekan Mati (Benar/Salah).
TerowongCGWNATT DetectionStatus	NAT-T terdeteksi pada perangkat gateway pelanggan (Benar/Salah).
TunnelikepHase1state	Status Protokol Fase 1 IKE (Didirikan Rekeying Negosiasi Turun).
TunnelikepHase2state	Status Protokol IKE Fase 2 (Didirikan Rekeying Negosiasi Turun).
VpnLogDetail	Pesan verbose untuk protokol IPsec, IKE dan DPD.

Daftar Isi

- [Pesan Kesalahan IKEv1](#)
- [Pesan Kesalahan IKEv2](#)
- [Pesan Negosiasi IKEv2](#)

Pesan Kesalahan IKEv1

Pesan	Penjelasan
Peer tidak responsif - Mendeklarasikan rekan mati	Sebaya belum menanggapi Pesan DPD, menegakkan aksi time-out DPD.
AWS Dekripsi payload terowongan tidak berhasil karena Kunci Pra-bersama yang tidak valid	Kunci Pra-Bersama yang sama perlu dikonfigurasi pada kedua Peer IKE.
Tidak Ada Pencocokan Proposal Ditemukan oleh AWS	Atribut yang Diusulkan untuk Fase 1 (Enkripsi, Hashing, dan Grup DH) tidak didukung oleh AWS VPN Endpoint. misalnya 3DES
Tidak Ada Pencocokan Proposal yang Ditemukan. Memberi tahu dengan "Tidak ada proposal yang dipilih"	Tidak ada Proposal Pesan kesalahan yang dipilih dipertukarkan antara Rekan untuk menginformasikan bahwa Proposal/Kebijakan yang benar harus dikonfigurasi untuk fase 2 di IKE Peers.
AWS terowongan menerima DELETE untuk Fase 2 SA dengan SPI: xxxx	CGW telah mengirim pesan Delete_SA untuk Fase 2
AWS terowongan menerima DELETE untuk IKE_SA dari CGW	CGW telah mengirim pesan Delete_SA untuk Fase 1

Pesan Kesalahan IKEv2

Pesan	Penjelasan
AWS terowongan DPD habis setelah {retry_count} mentransmisikan ulang	Sebaya belum menanggapi Pesan DPD, menegakkan aksi time-out DPD.
AWS terowongan menerima DELETE untuk IKE_SA dari CGW	Peer telah mengirim pesan Delete_SA untuk orang tua/IKE_SA

Pesan	Penjelasan
AWS terowongan menerima DELETE untuk Fase 2 SA dengan SPI: xxxx	Peer telah mengirim pesan Delete_SA untuk CHILD_SA
AWS terowongan mendeteksi tabrakan (CHILD_REKEY) sebagai CHILD_DELETE	CGW telah mengirim pesan Delete_SA untuk SA Aktif, yang sedang di-rekeyed.
AWS tunnel (CHILD_SA) SA redundan sedang dihapus karena tabrakan yang terdeteksi	Karena Tabrakan, Jika SA redundan dihasilkan, Peer akan menutup SA redundan setelah mencocokkan nilai nonce sesuai RFC
AWS terowongan Fase 2 tidak dapat dibangun sambil mempertahankan Fase 1	Peer tidak dapat membuat CHILD_SA karena kesalahan negosiasi misalnya proposal yang salah.
AWS: Pemilih Lalu Lintas: TS_UNACCEPTABLE: diterima dari responden	Peer telah mengusulkan Pemilih Lalu Lintas/Domain Enkripsi yang Salah. Peer harus dikonfigurasi dengan CIDR yang identik dan benar.
AWS terowongan mengirim AUTHENTICATION_FAILED sebagai respons	Peer tidak dapat Mengautentikasi Peer dengan memverifikasi isi pesan IKE_AUTH
AWS terowongan mendeteksi ketidakcocokan kunci yang telah dibagikan sebelumnya dengan cgw: xxxx	Kunci Pra-Bersama yang sama perlu dikonfigurasi pada kedua Peer IKE.
AWS tunnel Timeout: menghapus Fase 1 IKE_SA yang tidak ditetapkan dengan cgw: xxxx	Menghapus IKE_SA yang setengah terbuka karena rekan belum melanjutkan negosiasi
Tidak Ada Pencocokan Proposal yang Ditemukan. Memberi tahu dengan "Tidak ada proposal yang dipilih"	Tidak ada Proposal Pesan kesalahan yang dipilih dipertukarkan antara Rekan untuk menginformasikan bahwa Proposal yang benar harus dikonfigurasi pada Rekan IKE.
Tidak Ada Pencocokan Proposal Ditemukan oleh AWS	Atribut yang Diusulkan untuk Fase 1 (Enkripsi, Hashing, dan Grup DH) tidak didukung oleh Titik Akhir AWS VPN. Misalnya 3DES

Pesan Negosiasi IKEv2

Pesan	Penjelasan
AWS permintaan yang diproses terowongan (id=xxx) untuk CREATE_CHILD_SA	AWS telah menerima permintaan CREATE_CHILD_SA dari CGW
AWS terowongan mengirimkan respons (id=xxx) untuk CREATE_CHILD_SA	AWS mengirim respons CREATE_CHILD_SA ke CGW
AWS terowongan mengirim permintaan (id=xxx) untuk CREATE_CHILD_SA	AWS mengirim permintaan CREATE_CHILD_SA ke CGW
AWS respons yang diproses terowongan (id=xxx) untuk CREATE_CHILD_SA	AWS telah menerima formulir respons CREATE_CHILD_SA CGW

Persyaratan IAM untuk mempublikasikan ke CloudWatch Log

Agar fitur logging berfungsi dengan baik, kebijakan IAM yang dilampirkan pada prinsipal IAM yang digunakan untuk mengonfigurasi fitur, minimal harus menyertakan izin berikut. Detail selengkapnya juga dapat ditemukan di bagian [Mengaktifkan logging dari AWS layanan tertentu](#) di Panduan Pengguna Amazon CloudWatch Logs.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs>ListLogDeliveries"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow",
      "Sid": "S2SVPNLogging"
    }
  ]
}
```

```
    },
    {
      "Sid": "S2SVPNLoggingCWL",
      "Action": [
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Lihat konfigurasi log VPN Site-to-Site

Untuk melihat setelan pencatatan terowongan saat ini

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Koneksi Site-to-Site VPN.
3. Pilih koneksi VPN yang ingin Anda lihat dari daftar koneksi VPN.
4. Pilih tab Detail terowongan.
5. Perluas opsi Tunnel 1 dan bagian opsi Tunnel 2 untuk melihat semua detail konfigurasi terowongan.
6. Anda dapat melihat status fitur logging saat ini di bawah log Tunnel VPN, dan grup CloudWatch log yang saat ini dikonfigurasi (jika ada) di bawah grup CloudWatch log.

Untuk melihat pengaturan pencatatan terowongan saat ini pada koneksi VPN Site-to-Site menggunakan baris perintah atau API AWS

- [DescribeVpnConnections](#) (Amazon EC2 Query API)
- [describe-vpn-connections](#) (AWS CLI)

Aktifkan log VPN Site-to-Site

Note

Saat Anda mengaktifkan log VPN Site-to-Site untuk terowongan koneksi VPN yang ada, konektivitas Anda melalui terowongan itu dapat terganggu selama beberapa menit. Namun, setiap koneksi VPN menawarkan dua terowongan untuk ketersediaan tinggi, sehingga Anda dapat mengaktifkan logging pada satu terowongan pada satu waktu sambil mempertahankan konektivitas melalui terowongan yang tidak dimodifikasi. Untuk informasi selengkapnya, lihat [Penggantian titik akhir terowongan Site-to-Site VPN](#).

Untuk mengaktifkan logging VPN selama pembuatan koneksi VPN Site-to-Site baru

Ikuti prosedur [Langkah 5: Buat koneksi VPN](#). Selama Langkah 9 Opsi Tunnel, Anda dapat menentukan semua opsi yang ingin Anda gunakan untuk kedua terowongan, termasuk opsi pencatatan VPN. Untuk informasi selengkapnya tentang opsi ini, lihat [Opsi terowongan untuk koneksi Site-to-Site VPN Anda](#).

Untuk mengaktifkan pencatatan terowongan pada koneksi VPN Site-to-Site baru menggunakan baris perintah atau API AWS

- [CreateVpnConnection](#) (Amazon EC2 Query API)
- [create-vpn-connection](#) (AWS CLI)

Untuk mengaktifkan pencatatan terowongan pada koneksi VPN Site-to-Site yang ada

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Koneksi Site-to-Site VPN.
3. Pilih koneksi VPN yang ingin Anda modifikasi dari daftar koneksi VPN.
4. Pilih Tindakan, Ubah opsi terowongan VPN.
5. Pilih terowongan yang ingin Anda modifikasi dengan memilih alamat IP yang sesuai dari terowongan VPN di luar daftar alamat IP.
6. Di bawah Log aktivitas terowongan, pilih Aktifkan.
7. Di bawah grup CloudWatch log Amazon, pilih grup CloudWatch log Amazon tempat Anda ingin log dikirim.

8. (Opsional) Di bawah Format output, pilih format yang diinginkan untuk output log, baik json atau teks.
9. Pilih Simpan perubahan.
10. (Opsional) Ulangi langkah 4 hingga 9 untuk terowongan lain jika diinginkan.

Untuk mengaktifkan pencatatan terowongan pada koneksi VPN Site-to-Site yang ada menggunakan baris perintah atau API AWS

- [ModifyVpnTunnelOptions](#) (Amazon EC2 Query API)
- [modify-vpn-tunnel-options](#) (AWS CLI)

Nonaktifkan log VPN Site-to-Site

Untuk menonaktifkan pencatatan terowongan pada koneksi VPN Site-to-Site

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Koneksi Site-to-Site VPN.
3. Pilih koneksi VPN yang ingin Anda modifikasi dari daftar koneksi VPN.
4. Pilih Tindakan, Ubah opsi terowongan VPN.
5. Pilih terowongan yang ingin Anda modifikasi dengan memilih alamat IP yang sesuai dari terowongan VPN di luar daftar alamat IP.
6. Di bawah Log aktivitas terowongan, hapus Aktifkan.
7. Pilih Simpan perubahan.
8. (Opsional) Ulangi langkah 4 hingga 7 untuk terowongan lain jika diinginkan.

Untuk menonaktifkan pencatatan terowongan pada koneksi VPN Site-to-Site menggunakan baris perintah atau API AWS

- [ModifyVpnTunnelOptions](#) (Amazon EC2 Query API)
- [modify-vpn-tunnel-options](#) (AWS CLI)

Memantau terowongan VPN menggunakan Amazon CloudWatch

Anda dapat memantau terowongan VPN menggunakan CloudWatch, yang mengumpulkan dan memproses data mentah dari layanan VPN menjadi metrik yang dapat dibaca, mendekati waktu nyata. Statistik ini dicatat untuk jangka waktu 15 bulan, sehingga Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang performa aplikasi atau layanan web Anda. Data metrik VPN dikirim secara otomatis CloudWatch saat tersedia.

Untuk informasi selengkapnya, lihat [Panduan CloudWatch Pengguna Amazon](#).

Daftar Isi

- [Metrik dan dimensi VPN](#)
- [Melihat CloudWatch metrik VPN](#)
- [Membuat CloudWatch alarm untuk memantau terowongan VPN](#)

Metrik dan dimensi VPN

CloudWatch Metrik berikut tersedia untuk koneksi VPN Site-to-Site Anda.

Metrik	Deskripsi
TunnelState	Status terowongan. Untuk VPN statis, 0 menunjukkan TURUN dan 1 menunjukkan NAIK. Untuk VPN BGP, 1 menunjukkan DITETAPKAN dan 0 digunakan untuk semua status lainnya. Untuk kedua jenis VPN, nilai antara 0 dan 1 menunjukkan setidaknya satu terowongan tidak NAIK. Unit: nilai pecahan antara 0 dan 1
TunnelDataIn †	Byte yang diterima di AWS sisi koneksi melalui terowongan VPN dari gateway pelanggan. Setiap titik data metrik mewakili jumlah byte yang diterima setelah titik data sebelumnya. Menggunakan statistik Sum untuk menunjukk

Metrik	Deskripsi
	<p>an jumlah total byte yang diterima selama periode tersebut.</p> <p>Metrik ini menghitung data setelah dekripsi.</p> <p>Unit: Bit</p>
TunnelDataOut †	<p>Byte dikirim dari AWS sisi koneksi melalui terowongan VPN ke gateway pelanggan. Setiap titik data metrik mewakili jumlah byte yang dikirim setelah titik data sebelumnya. Menggunakan Statistik Sum untuk menunjukkan jumlah total byte yang dikirimkan selama periode tersebut.</p> <p>Metrik ini menghitung data sebelum enkripsi.</p> <p>Unit: Bit</p>

† Metrik ini dapat melaporkan penggunaan jaringan bahkan ketika terowongan sedang down. Ini karena pemeriksaan status berkala yang dilakukan di terowongan, dan permintaan ARP dan BGP latar belakang.

Untuk memfilter data metrik, gunakan dimensi berikut.

Dimensi	Deskripsi
VpnId	Memfilter data metrik berdasarkan ID koneksi Site-to-Site VPN.
TunnelIpAddress	Mem-filter data metrik berdasarkan alamat IP terowongan untuk virtual private gateway.

Melihat CloudWatch metrik VPN

Saat Anda membuat koneksi VPN Site-to-Site, layanan VPN mengirimkan metrik tentang koneksi CloudWatch VPN Anda, saat tersedia. Anda dapat melihat metrik untuk koneksi VPN Anda sebagai berikut.

Untuk melihat metrik menggunakan konsol CloudWatch

Metrik dikelompokkan terlebih dahulu berdasarkan namespace layanan, lalu berdasarkan berbagai kombinasi dimensi dalam setiap namespace.

1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Pada panel navigasi, silakan pilih Metrik.
3. Di bawah Semua metrik, pilih namespace metrik VPN.
4. Pilih dimensi metrik untuk melihat metrik (misalnya, Metrik Terowongan VPN).

Note

Namespace VPN tidak akan muncul di CloudWatch konsol sampai setelah koneksi VPN Site-to-Site dibuat di wilayah yang Anda lihat. AWS

Untuk melihat metrik menggunakan AWS CLI

Pada prompt perintah, gunakan perintah berikut:

```
aws cloudwatch list-metrics --namespace "AWS/VPN"
```

Membuat CloudWatch alarm untuk memantau terowongan VPN

Anda dapat membuat CloudWatch alarm yang mengirimkan pesan Amazon SNS saat alarm berubah status. Alarm mengawasi satu metrik selama periode waktu yang Anda tentukan, dan mengirimkan notifikasi ke topik Amazon SNS berdasarkan nilai metrik relatif terhadap ambang batas tertentu selama beberapa periode waktu.

Misalnya, Anda dapat membuat alarm yang memantau status terowongan VPN tunggal, dan mengirimkan pemberitahuan ketika status terowongan TURUN selama 3 titik data dalam waktu 15 menit.

Untuk membuat alarm untuk status terowongan tunggal

1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Di panel navigasi, perluas Alarm, lalu pilih Semua alarm.
3. Pilih Buat alarm, lalu pilih Pilih metrik.
4. Pilih VPN, lalu Metrik Terowongan VPN.
5. Pilih alamat IP terowongan yang diinginkan, pada baris yang sama dengan TunnelStatemetrik. Pilih Pilih Metrik.
6. Untuk Kapan TunnelState pun... , pilih Turunkan, lalu masukkan "1" di bidang input di bawah dari... .
7. Di bawah Konfigurasi tambahan, atur input ke "3 dari 3" untuk titik data ke alarm.
8. Pilih Selanjutnya.
9. Di bawah Kirim pemberitahuan ke topik SNS berikut, pilih daftar notifikasi yang ada atau buat yang baru.
10. Pilih Selanjutnya.
11. Masukkan nama untuk alarm Anda. Pilih Selanjutnya.
12. Periksa pengaturan untuk alarm Anda, dan kemudian pilih Buat alarm.

Anda dapat membuat alarm yang memantau status koneksi Site-to-Site VPN. Misalnya, Anda dapat membuat alarm yang mengirimkan notifikasi saat salah satu atau kedua status terowongan tersebut TURUN selama satu periode 5 menit.

Membuat alarm untuk status koneksi Site-to-Site VPN

1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Di panel navigasi, perluas Alarm, lalu pilih Semua alarm.
3. Pilih Buat alarm, lalu pilih Pilih metrik.
4. Pilih VPN dan kemudian pilih Metrik Koneksi VPN.
5. Pilih koneksi VPN Site-to-Site Anda dan metriknya. TunnelState Pilih Pilih Metrik.
6. Untuk Statistik, tentukan Maksimum.

Atau, jika Anda telah mengonfigurasi koneksi Site-to-Site VPN sehingga kedua terowongan naik, Anda dapat menentukan statistik Minimum untuk mengirim notifikasi setidaknya saat satu terowongan yang turun.

7. Untuk Kapan pun, pilih Lebih rendah/sama (\leq) dan masukkan 0 (atau 0,5 untuk setidaknya saat satu terowongan turun). Pilih Selanjutnya.
8. Di bawah Pilih topik SNS, pilih daftar notifikasi yang ada atau pilih Daftar baru untuk membuat yang baru. Pilih Selanjutnya.
9. Masukkan nama dan deskripsi untuk alarm. Pilih Selanjutnya.
10. Periksa pengaturan untuk alarm Anda, dan kemudian pilih Buat alarm.

Anda juga dapat membuat alarm yang memantau jumlah lalu lintas yang masuk atau meninggalkan terowongan VPN. Misalnya, alarm berikut memantau jumlah lalu lintas yang masuk ke terowongan VPN dari jaringan Anda, dan mengirimkan notifikasi ketika jumlah byte mencapai ambang batas 5.000.000 selama periode 15 menit.

Membuat alarm untuk lalu lintas jaringan masuk

1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Di panel navigasi, perluas Alarm, lalu pilih Semua alarm.
3. Pilih Buat alarm, lalu pilih Pilih metrik.
4. Pilih VPN, lalu pilih Metrik Terowongan VPN.
5. Pilih alamat IP terowongan VPN dan TunnelDataInmetrik. Pilih Pilih Metrik.
6. Untuk Statistik, tentukan Jumlah.
7. Untuk Periode, pilih 15 Menit.
8. Untuk Kapan pun, pilih Besar/Sama (\geq) dan masukkan 5000000. Pilih Selanjutnya.
9. Di bawah Pilih topik SNS, pilih daftar notifikasi yang ada atau pilih Daftar baru untuk membuat yang baru. Pilih Selanjutnya.
10. Masukkan nama dan deskripsi untuk alarm. Pilih Selanjutnya.
11. Periksa pengaturan untuk alarm Anda, dan kemudian pilih Buat alarm.

Alarm berikut memantau jumlah lalu lintas yang meninggalkan terowongan VPN ke jaringan Anda, dan mengirimkan notifikasi ketika jumlah byte kurang dari 1.000.000 selama periode 15 menit.

Membuat alarm untuk lalu lintas jaringan keluar

1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Di panel navigasi, perluas Alarm, lalu pilih Semua alarm.

3. Pilih Buat alarm, lalu pilih Pilih metrik.
4. Pilih VPN, lalu pilih Metrik Terowongan VPN.
5. Pilih alamat IP terowongan VPN dan TunnelDataOutmetrik. Pilih Pilih Metrik.
6. Untuk Statistik, tentukan Jumlah.
7. Untuk Periode, pilih 15 Menit.
8. Untuk Kapan pun, pilih Lebih Rendah/Sama (\leq) dan masukkan 1000000. Pilih Selanjutnya.
9. Di bawah Pilih topik SNS, pilih daftar notifikasi yang ada atau pilih Daftar baru untuk membuat yang baru. Pilih Selanjutnya.
10. Masukkan nama dan deskripsi untuk alarm. Pilih Selanjutnya.
11. Periksa pengaturan untuk alarm Anda, dan kemudian pilih Buat alarm.

Untuk lebih banyak contoh pembuatan alarm, lihat [Membuat CloudWatch alarm Amazon](#) di CloudWatch Panduan Pengguna Amazon.

Memantau koneksi VPN menggunakan AWS Health acara

AWS Site-to-Site VPN secara otomatis mengirimkan pemberitahuan ke AWS [AWS Health Dashboard](#)(PHD), yang didukung oleh AWS Health API. Dasbor ini tidak memerlukan pengaturan, dan siap digunakan untuk AWS pengguna yang diautentikasi. Anda dapat mengonfigurasi beberapa tindakan dalam menanggapi notifikasi kejadian melalui AWS Health Dashboard.

AWS Health Dashboard Ini menyediakan jenis notifikasi berikut untuk koneksi VPN Anda:

- [Notifikasi penggantian titik akhir terowongan](#)
- [Notifikasi VPN terowongan tunggal](#)

Notifikasi penggantian titik akhir terowongan

Anda menerima pemberitahuan penggantian titik akhir Tunnel AWS Health Dashboard ketika salah satu atau kedua titik akhir terowongan VPN di koneksi VPN Anda diganti. Sebuah titik akhir terowongan diganti ketika AWS melakukan pembaruan terowongan, atau saat Anda mengubah koneksi VPN Anda. Untuk informasi selengkapnya, lihat [Penggantian titik akhir terowongan Site-to-Site VPN](#).

Ketika penggantian titik akhir terowongan selesai, AWS mengirimkan pemberitahuan penggantian titik akhir Tunnel melalui acara. AWS Health Dashboard

Notifikasi VPN terowongan tunggal

Koneksi Site-to-Site VPN terdiri dari dua terowongan untuk lebih. Kami sangat menyarankan agar Anda mengonfigurasi kedua terowongan untuk menyediakan banyak tempat. Jika koneksi VPN Anda memiliki satu terowongan ke atas tetapi yang lain tidak aktif selama lebih dari satu jam dalam sehari, Anda menerima pemberitahuan terowongan tunggal VPN bulanan melalui sebuah AWS Health Dashboard acara. Acara ini akan diperbarui setiap hari dengan koneksi VPN baru yang terdeteksi sebagai terowongan tunggal, dengan pemberitahuan dikirim setiap minggu. Acara baru akan dibuat setiap bulan, yang akan menghapus koneksi VPN yang tidak lagi terdeteksi sebagai terowongan tunggal.

Kuota Site-to-Site VPN

AWS Akun Anda memiliki kuota berikut, sebelumnya disebut sebagai batas, terkait dengan Site-to-Site VPN. Kecuali dinyatakan lain, setiap kuota bersifat khusus per Wilayah. Anda dapat meminta peningkatan untuk beberapa kuota dan kuota lainnya tidak dapat ditingkatkan.

Untuk meminta peningkatan kuota untuk kuota yang dapat disesuaikan, pilih Ya di kolom Adjustable. Untuk informasi selengkapnya, lihat [Meminta peningkatan kuota](#) di Panduan Pengguna Service Quotas.

Sumber daya Site-to-Site VPN

Nama	Default	Dapat disesuaikan
Gateway pelanggan per Wilayah	50	Ya
Gateway pribadi virtual per Wilayah	5	Ya
Koneksi VPN Site-to-Site per Wilayah	50	Ya
Koneksi VPN Site-to-Site per gateway pribadi virtual	10	Ya
Koneksi VPN Site-to-Site yang dipercepat per Wilayah	10	Ya
Koneksi VPN Site-to-Site yang tidak terkait per Wilayah	10	Ya

Note

Koneksi Akselerasi dan Tidak Terkait dihitung terhadap total koneksi VPN Site-to-Site per kuota Wilayah.

Anda dapat melampirkan satu gateway pribadi virtual ke VPC sekaligus. Untuk menghubungkan koneksi Site-to-Site VPN yang sama ke beberapa VPC, kami merekomendasikan Anda untuk

menjelajahi menggunakan transit gateway. Untuk informasi selengkapnya, lihat [Transit gateway](#) di Amazon VPC Transit Gateway.

Koneksi Site-to-Site VPN pada transit gateway tunduk pada batas total transit gateway attachments. Untuk informasi selengkapnya, lihat [Kuota gateway transit](#).

Rute

Sumber rute yang diiklankan mencakup rute VPC, rute VPN lainnya, dan rute dari antarmuka virtual AWS Direct Connect . Rute yang diiklankan berasal dari tabel rute yang terkait dengan lampiran VPN.

Note

Jika Anda menggunakan gateway pribadi virtual dan propagasi rute diaktifkan pada tabel rute VPC Anda, rute dinamis dan statis akan secara otomatis ditambahkan untuk koneksi VPN Anda, hingga batas tabel rute VPC. Lihat [kuota VPC Amazon](#) di Panduan Pengguna Amazon VPC untuk detail lebih lanjut.

Nama	Default	Dapat disesuaikan
Rute dinamis yang diiklankan dari perangkat gateway pelanggan ke koneksi VPN Site-to-Site pada gateway pribadi virtual	100	Tidak
Rute yang diiklankan dari koneksi VPN Site-to-Site pada gateway pribadi virtual ke perangkat gateway pelanggan	1.000	Tidak
Rute dinamis yang diiklankan dari perangkat gateway pelanggan ke koneksi VPN Site-to-Site pada gateway transit	1.000	Tidak
Rute yang diiklankan dari koneksi VPN Site-to-Site pada gateway transit ke perangkat gateway pelanggan	5.000	Tidak

Nama	Default	Dapat disesuaikan
Rute statis dari perangkat gateway pelanggan ke koneksi VPN Site-to-Site pada gateway pribadi virtual	100	Tidak

Bandwidth dan throughput

Ada banyak faktor yang dapat memengaruhi bandwidth terealisasi melalui koneksi VPN Site-to-Site, termasuk namun tidak terbatas pada: ukuran paket, bauran lalu lintas (TCP/UDP), kebijakan pembentukan atau pelambatan pada jaringan perantara, cuaca internet, dan persyaratan aplikasi tertentu.

Nama	Default	Dapat disesuaikan
Bandwidth maksimum per terowongan VPN	Hingga 1,25 Gbps	Tidak
Paket maksimum per detik (PPS) per terowongan VPN	Hingga 140.000	Tidak

Untuk koneksi Site-to-Site VPN pada transit gateway, Anda dapat menggunakan ECMP untuk mendapatkan bandwidth VPN yang lebih tinggi dengan menggabungkan beberapa terowongan VPN. Untuk menggunakan ECMP, koneksi VPN harus dikonfigurasi untuk perutean dinamis. ECMP tidak didukung pada koneksi VPN yang menggunakan perutean statis. Untuk informasi selengkapnya, lihat [Transit gateway](#).

Unit transmisi maksimum (MTU)

Site-to-Site VPN mendukung unit transmisi maksimum (MTU) 1446 byte dan ukuran segmen maksimum (MSS) yang sesuai sebesar 1406 byte. Namun, algoritme tertentu yang menggunakan header TCP yang lebih besar dapat secara efektif mengurangi nilai maksimum itu. Untuk menghindari fragmentasi, kami sarankan Anda mengatur MTU dan MSS berdasarkan algoritma yang dipilih. Untuk detail lebih lanjut tentang MTU, MSS, dan nilai optimal, lihat [Praktik terbaik untuk perangkat gateway pelanggan Anda](#)

Frame jumbo tidak didukung. Untuk informasi selengkapnya, lihat [Frame jumbo](#) di Panduan Pengguna Amazon EC2.

Koneksi Site-to-Site VPN tidak mendukung Path MTU Discovery.

Sumber daya kuota tambahan

Untuk kuota yang terkait dengan transit gateway, termasuk jumlah lampiran pada transit gateway, lihat [Kuota untuk transit gateway Anda](#) di Panduan Amazon VPC Transit Gateway.

Untuk kuota VPC tambahan, lihat [Kuota Amazon VPC](#) di Panduan Pengguna Amazon VPC.

Riwayat dokumen untuk Panduan Pengguna VPN Site-to-Site

Tabel berikut menjelaskan pembaruan Panduan AWS Site-to-Site VPN Pengguna.

Perubahan	Deskripsi	Tanggal
Info VPN klasik dihapus	Menghapus info tentang VPN klasik dari panduan.	19 Januari 2023
Pesan contoh log VPN	Contoh log ditambahkan untuk koneksi VPN Site-to-Site.	Desember 9, 2022
Utilitas Konfigurasi Unduhan yang Diperbarui	Pelanggan VPN Site-to-Site dapat membuat templat konfigurasi untuk perangkat Customer Gateway (CGW) yang kompatibel, sehingga memudahkan untuk membuat koneksi VPN. AWS Pembaruan ini menambahkan dukungan untuk parameter Internet Key Exchange versi 2 (IKEv2) untuk banyak perangkat CGW populer dan mencakup dua API baru — dan. <code>GetVpnConnectionDeviceTypes</code> <code>GetVpnConnectionDeviceSampleConfiguration</code>	September 21, 2021
Pemberitahuan koneksi VPN	Site-to-Site VPN secara otomatis mengirimkan notifikasi koneksi VPN Anda ke AWS Health Dashboard.	29 Oktober 2020

Inisiasi terowongan VPN	Anda dapat mengonfigurasi terowongan VPN Anda sehingga AWS memunculkan terowongan.	27 Agustus 2020
Ubah opsi koneksi VPN	Anda dapat mengubah opsi koneksi untuk koneksi Site-to-Site VPN Anda.	27 Agustus 2020
Algoritma keamanan tambahan	Anda dapat menerapkan algoritme keamanan tambahan untuk terowongan VPN Anda.	14 Agustus 2020
Dukungan IPv6	Terowongan VPN Anda dapat mendukung lalu lintas IPv6 di dalam terowongan.	12 Agustus 2020
Gabung panduan AWS Site-to-Site VPN	Rilis ini menggabungkan isi Panduan Administrator AWS Site-to-Site VPN Jaringan ke dalam panduan ini.	31 Maret 2020
AWS Site-to-Site VPN Koneksi yang dipercepat	Anda dapat mengaktifkan akselerasi untuk AWS Site-to-Site VPN koneksi Anda.	3 Desember 2019
Ubah opsi AWS Site-to-Site VPN terowongan	Anda dapat memodifikasi opsi untuk terowongan VPN dalam AWS Site-to-Site VPN koneksi. Anda juga dapat mengonfigurasi opsi terowongan tambahan.	29 Agustus 2019
AWS Private Certificate Authority dukungan sertifikat pribadi	Anda dapat menggunakan sertifikat pribadi AWS Private Certificate Authority untuk mengautentikasi VPN Anda.	15 Agustus 2019

Panduan Pengguna VPN Site-to-Site Baru	Rilis ini memisahkan konten AWS Site-to-Site VPN (sebelumnya dikenal sebagai AWS Managed VPN) dari Panduan Pengguna Amazon VPC.	18 Desember 2018
Ubah gateway target	Anda dapat memodifikasi gateway target AWS Site-to-Site VPN koneksi.	18 Desember 2018
Kustom ASN	Ketika Anda membuat virtual private gateway, Anda dapat menentukan Nomor Sistem Mandiri (ASN) privat untuk sisi gateway Amazon.	10 Oktober 2017
Opsi terowongan VPN	Anda dapat menentukan blok CIDR terowongan dalam dan kunci pre-shared kustom untuk terowongan VPN Anda.	3 Oktober 2017
Metrik VPN	Anda dapat melihat CloudWatch metrik untuk koneksi VPN Anda.	15 Mei 2017

Penyempurnaan VPN

Koneksi VPN sekarang mendukung fungsi enkripsi AES 256-bit, fungsi hashing SHA-256, NAT traversal, dan grup Diffie-Hellman tambahan selama koneksi Tahap 1 dan Tahap 2. Selain itu, sekarang Anda dapat menggunakan alamat IP gateway pelanggan yang sama untuk setiap koneksi VPN yang menggunakan perangkat gateway pelanggan yang sama.

28 Oktober 2015

Koneksi VPN menggunakan konfigurasi perutean statis

Anda dapat membuat koneksi VPN IPsec ke Amazon VPC menggunakan konfigurasi perutean statis. Sebelumnya, koneksi VPN memerlukan penggunaan Border Gateway Protocol (BGP). Kami sekarang mendukung kedua jenis koneksi dan Anda sekarang dapat membuat konektivitas dari perangkat yang tidak mendukung BGP, termasuk Cisco ASA dan Microsoft Windows Server 2008 R2.

13 September 2012

[Perbanyakkan rute otomatis](#)

Anda sekarang dapat mengonfigurasi propagasi otomatis rute dari VPN Anda dan AWS Direct Connect tautan ke tabel perutean VPC Anda.

13 September 2012

[AWS VPN CloudHub dan koneksi VPN yang berlebihan](#)

Anda dapat berkomunikasi dengan aman dari satu situs ke situs lain dengan atau tanpa VPC. Anda dapat menggunakan koneksi VPN yang berlebihan untuk menyediakan koneksi toleransi kesalahan ke VPC Anda.

29 September 2011

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