aws

Panduan Administrator

AWS Client VPN

AWS Client VPN: Panduan Administrator

Table of Contents

Apa yang dimaksud dengan AWS Client VPN?

AWS Client VPN adalah layanan VPN berbasis klien terkelola yang memungkinkan Anda mengakses sumber daya AWS dan sumber daya di jaringan on-premise Anda dengan aman. Dengan Client VPN, Anda dapat mengakses sumber daya Anda dari lokasi manapun menggunakan klien VPN berbasis OpenVPN.

Daftar Isi

Fitur Client VPN

Client VPN menawarkan fitur dan fungsionalitas sebagai berikut:

- Koneksi aman — Menyediakan koneksi TLS yang aman dari lokasi manapun menggunakan klien OpenVPN.
- Layanan terkelola — Ini adalah layanan terkelola AWS, sehingga menghilangkan beban operasional dalam men-deploy dan mengelola solusi VPN akses jarak jauh pihak ketiga.
- Ketersediaan dan elastisitas tinggi — Secara otomatis menskalakan jumlah pengguna yang terhubung ke sumber daya AWS dan sumber daya on premise.
- Autentikasi — mendukung autentikasi klien menggunakan Direktori Aktif, autentikasi federasi, dan autentikasi berbasis sertifikat.
- Kontrol terperinci — Memungkinkan Anda untuk menerapkan kontrol keamanan kustom dengan mendefinisikan aturan akses berbasis jaringan. Aturan-aturan ini dapat dikonfigurasi pada granularitas grup Direktori Aktif. Anda juga dapat menerapkan kontrol akses menggunakan grup keamanan.
- Kemudahan penggunaan — Memungkinkan Anda untuk mengakses sumber daya AWS dan sumber daya on premise menggunakan satu terowongan VPN.

- Mudah dikelola — Memungkinkan Anda untuk melihat log koneksi, yang memberikan detail tentang upaya koneksi dari klien. Anda juga dapat mengelola koneksi klien yang aktif, menggunakan kemampuan untuk mengakhiri koneksi klien aktif.
- Integrasi mendalam — Terintegrasi dengan layanan AWS yang ada, termasuk AWS Directory Service dan Amazon VPC.

Komponen Client VPN

Berikut ini adalah konsep kunci untuk Client VPN:

Titik akhir Client VPN

Titik akhir Client VPN adalah sumber daya yang Anda buat dan konfigurasikan untuk mengaktifkan dan mengelola sesi Client VPN. Ini adalah titik terminasi untuk semua sesi VPN klien.

Jaringan target

Jaringan target adalah jaringan yang Anda kaitkan dengan titik akhir Client VPN. Subnet dari VPC merupakan jaringan target. Menghubungkan subnet dengan titik akhir Client VPN memungkinkan Anda untuk membuat sesi VPN. Anda dapat mengaitkan beberapa subnet dengan titik akhir Client VPN untuk ketersediaan yang tinggi. Semua subnet harus berasal dari VPC yang sama. Setiap subnet harus menjadi bagian dari Availability Zone yang berbeda.

Rute

Setiap titik akhir Client VPN memiliki tabel rute yang menjelaskan rute jaringan tujuan yang tersedia. Setiap rute dalam tabel rute menentukan jalur untuk lalu lintas ke sumber daya atau jaringan tertentu.

Aturan otorisasi

Aturan otorisasi membatasi pengguna yang dapat mengakses jaringan. Untuk jaringan yang ditentukan, Anda mengonfigurasi grup Direktori Aktif atau identitas provider (IdP) yang aksesnya diizinkan. Hanya pengguna dalam grup ini yang dapat mengakses jaringan yang ditentukan. Secara default, tidak ada aturan otorisasi dan Anda harus mengonfigurasi aturan otorisasi untuk memungkinkan pengguna mengakses sumber daya dan jaringan.

Klien

Pengguna akhir yang terhubung ke titik akhir Client VPN membuat sesi VPN. Pengguna akhir harus mengunduh klien OpenVPN dan menggunakan file konfigurasi Client VPN yang Anda buat untuk membuat sesi VPN.

Rentang CIDR klien

Rentang alamat IP tempat untuk menetapkan alamat IP klien. Setiap koneksi ke titik akhir Client VPN ditetapkan dalam alamat IP yang unik dari rentang CIDR klien. Anda memilih rentang CIDR klien, misalnya, `10.2.0.0/16`.

Port Client VPN

AWS Client VPN mendukung port 443 dan 1194 untuk TCP dan UDP. Port default adalah 443.

Antarmuka jaringan Client VPN

Ketika Anda mengaitkan subnet dengan titik akhir Client VPN Anda, kami membuat antarmuka jaringan Client VPN di subnet tersebut. Lalu lintas yang dikirim ke VPC dari titik akhir Client VPN dikirim melalui antarmuka jaringan Client VPN. Sumber terjemahan alamat jaringan (SNAT) kemudian diterapkan, di mana sumber alamat IP dari rentang CIDR klien diterjemahkan ke alamat IP antarmuka jaringan Client VPN.

Pencatatan koneksi

Anda dapat mengaktifkan pencatatan koneksi untuk titik akhir Client VPN Anda ke kejadian koneksi log. Anda dapat menggunakan informasi ini untuk menjalankan forensik, menganalisis bagaimana titik akhir Client VPN digunakan, atau men-debug masalah koneksi.

Portal layanan mandiri

Client VPN menyediakan portal swalayan sebagai halaman web untuk pengguna akhir untuk mengunduh versi terbaru AWS VPN Desktop Client dan versi terbaru dari file konfigurasi titik akhir Client VPN, yang berisi pengaturan yang diperlukan untuk terhubung ke titik akhir mereka. Administrator titik akhir Client VPN dapat mengaktifkan atau menonaktifkan portal swalayan untuk titik akhir Client VPN. Portal swalayan adalah layanan Global yang didukung oleh tumpukan layanan di Wilayah berikut: AS Timur (Virginia N.), Asia Pasifik (Tokyo), Eropa (Irlandia), dan AWS GovCloud (AS-Barat).

Bekerja dengan Client VPN

Anda dapat bekerja dengan Client VPN menggunakan salah satu dari cara berikut ini:

AWS Management Console

Konsol ini menyediakan antarmuka pengguna berbasis web untuk Client VPN. Jika Anda telah mendaftarAkun AWS, Anda dapat masuk ke konsol Amazon VPC dan memilih Client VPN di panel navigasi.

AWS Command Line Interface (AWS CLI)

Parameter AWS CLI menyediakan akses langsung ke API publik Client VPN. Hal ini didukung di Windows, macOS, dan Linux. Untuk informasi selengkapnya tentang memulai dengan AWS CLI, lihat AWS Command Line Interface Panduan Pengguna. Untuk informasi selengkapnya tentang perintah untuk Client VPN, lihat AWS CLI Referensi Perintah.

AWS Tools for Windows PowerShell

AWSmenyediakan perintah untuk serangkaian AWS penawaran yang luas bagi mereka yang membuat skrip di lingkungan. PowerShell Untuk informasi lebih lanjut tentang memulai dengan AWS Tools for Windows PowerShell, lihat AWS Tools for Windows PowerShell Panduan Pengguna. Untuk informasi selengkapnya tentang cmdlets untuk Client VPN, lihat AWS Tools for Windows PowerShell Referensi Cmdlet.

API Kueri

API Kueri HTTPS Client VPN memberikan program akses ke Client VPN dan AWS. API Kueri HTTPS memungkinkan Anda menerbitkan permintaan HTTPS secara langsung ke layanan. Saat Anda menggunakan API HTTPS, Anda harus menyertakan kode untuk menandatangani permintaan secara digital menggunakan kredensial Anda. Untuk informasi selengkapnya, lihat AWS Client VPN tindakan.

Harga untuk Client VPN

Anda dikenakan biaya untuk setiap asosiasi titik akhir dan setiap koneksi VPN setiap jam. Untuk informasi selengkapnya, lihat harga AWS Client VPN.

Anda dikenakan biaya untuk transfer data dari Amazon EC2 ke internet. Untuk informasi selengkapnya, lihat Transfer Data pada usia Harga Sesuai Permintaan Amazon EC2.

Jika Anda mengaktifkan pencatatan koneksi untuk titik akhir Client VPN, Anda harus membuat grup CloudWatch log Log di akun Anda. Biaya berlaku untuk penggunaan grup log. Untuk informasi selengkapnya, lihat CloudWatch harga Amazon (di bawah Tingkat berbayar, pilih Log).

Jika Anda mengaktifkan handler koneksi klien untuk klien titik akhir Client VPN, Anda harus mengaktifkan dan memanggil fungsi Lambda. Biaya berlaku untuk aktivasi fungsi Lambda. Untuk informasi selengkapnya, lihat AWS Lambda harga.

Titik akhir Client VPN dikaitkan dengan jaringan target, yang merupakan subnet dalam VPC. Jika VPC ini memiliki Internet Gateway, kami mengaitkan alamat IP Elastis dengan antarmuka jaringan elastis (ENI) Client VPN. Alamat IP Elastis ini dikenakan biaya sebagai alamat IPv4 publik yang sedang digunakan. Untuk informasi selengkapnya, lihat tab Alamat IPv4 Publik di halaman harga VPC.

Aturan dan praktik terbaik AWS Client VPN

Berikut ini adalah aturan dan praktik terbaik untuk AWS Client VPN

- Ada batas bandwidth 10 Mbps per koneksi pengguna.
- Rentang CIDR klien tidak dapat tumpang tindih dengan CIDR lokal dari VPC tempat subnet terkait berada, atau setiap rute secara manual ditambahkan ke tabel rute titik akhir Client VPN.
- Rentang CIDR klien harus memiliki ukuran blok minimal /22 dan tidak boleh lebih besar dari /12.
- Sebagian alamat di rentang CIDR klien digunakan untuk mendukung model ketersediaan titik akhir Client VPN, dan tidak dapat ditugaskan kepada klien. Oleh karena itu, kami rekomendasikan Anda menetapkan blok CIDR yang berisi dua kali jumlah alamat IP yang diperlukan untuk mengaktifkan jumlah maksimum koneksi bersamaan bahwa Anda berencana untuk mendukung titik akhir Client VPN.
- Rentang CIDR klien tidak dapat diubah setelah Anda membuat titik akhir Client VPN.
- Subnet yang terkait dengan titik akhir Client VPN harus berada dalam VPC yang sama.
- Anda tidak dapat mengaitkan beberapa subnet dari Availability Zone yang sama dengan titik akhir Client VPN.
- Titik Akhir Client VPN tidak mendukung asosiasi subnet di penghunian khusus VPC.
- Client VPN hanya mendukung lalu lintas IPv4. Lihat Pertimbangan IPv6 untukAWSClient VPN untuk detail tentang IPv6.
- Client VPN tidak patuh dengan Federal Information Processing Standard (FIPS).
- Portal layanan mandiri ini tidak tersedia untuk klien yang mengautentikasi menggunakan autentikasi bersama.
- Kami tidak menyarankan untuk menghubungkan ke titik akhir Client VPN menggunakan alamat IP. Karena Client VPN adalah layanan terkelola, Anda kadang-kadang akan melihat perubahan pada

alamat IP yang diselesaikan oleh nama DNS. Selain itu, Anda akan melihat antarmuka jaringan Client VPN dihapus dan dibuat ulang di log Anda CloudTrail . Sebaiknya sambungkan ke titik akhir Client VPN menggunakan nama DNS yang disediakan.

- Penerusan IP saat ini tidak didukung saat menggunakan aplikasi AWS Client VPN desktop. Penerusan IP didukung dari klien lain.
- Client VPN tidak mendukung replikasi Multi-region di. AWS Managed Microsoft AD Titik akhir Client VPN harus berada di Wilayah yang sama dengan AWS Managed Microsoft AD sumber daya.
- Jika otentikasi multi-faktor (MFA) dinonaktifkan untuk Direktori Aktif Anda, kata sandi pengguna tidak dapat menggunakan format berikut.

```
SCRV1:base64_encoded_string:base64_encoded_string
```

- Anda tidak dapat membuat koneksi VPN dari komputer jika ada beberapa pengguna yang masuk ke sistem operasi.
- Layanan Client VPN mengharuskan alamat IP yang terhubung dengan klien cocok dengan IP yang diselesaikan oleh nama DNS titik akhir Client VPN. Dengan kata lain, jika Anda menetapkan catatan DNS khusus untuk titik akhir Client VPN, lalu meneruskan lalu lintas ke alamat IP sebenarnya yang diselesaikan oleh nama DNS titik akhir, pengaturan ini tidak akan berfungsi menggunakan klien yang disediakan terbaru. AWS Aturan ini ditambahkan untuk mengurangi serangan IP server seperti yang dijelaskan di sini:. TunnelCrack
- Layanan Client VPN mensyaratkan bahwa rentang alamat IP jaringan area lokal (LAN) perangkat klien berada dalam rentang alamat IP pribadi standar berikut:`10.0.0.0/8`,`172.16.0.0/12`,`192.168.0.0/16`, atau`169.254.0.0/16`. Jika rentang alamat LAN klien terdeteksi berada di luar rentang di atas, titik akhir Client VPN akan secara otomatis mendorong arahan OpenVPN “redirect-gateway block-local” ke klien, memaksa semua lalu lintas LAN ke VPN. Oleh karena itu, jika Anda memerlukan akses LAN selama koneksi VPN, disarankan agar Anda menggunakan rentang alamat konvensional yang tercantum di atas untuk LAN Anda. Aturan ini diberlakukan untuk mengurangi kemungkinan serangan net lokal seperti yang dijelaskan di sini:. TunnelCrack

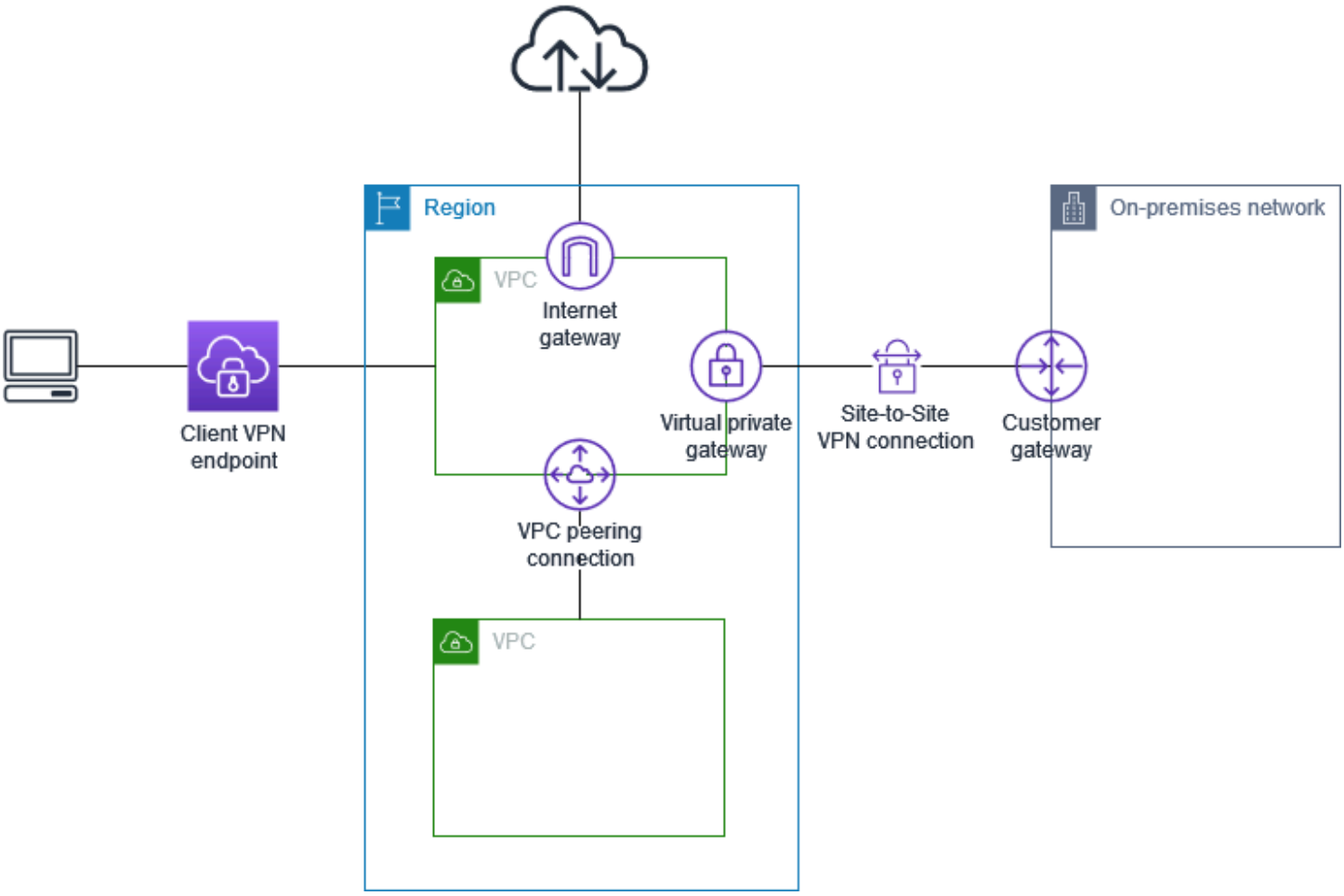
Bagaimana cara kerja AWS Client VPN

Dengan AWS Client VPN, ada dua jenis personas pengguna yang berinteraksi dengan titik akhir Client VPN: administrator dan klien.

Administrator bertanggung jawab untuk mengatur dan mengonfigurasi layanan. Melibatkan pembuatan titik akhir Client VPN, mengaitkan jaringan target, dan mengonfigurasi aturan otorisasi, dan menyiapkan rute tambahan (jika diperlukan). Setelah titik akhir Client VPN diatur dan dikonfigurasi, administrator mengunduh file konfigurasi titik akhir Client VPN dan mendistribusikannya ke klien yang membutuhkan akses. File konfigurasi titik akhir Client VPN menyertakan nama DNS titik akhir Client VPN dan informasi autentikasi yang diperlukan untuk membuat sesi VPN. Untuk informasi lebih lanjut tentang pengaturan layanan, lihat Memulai dengan AWS Client VPN.

Klien adalah pengguna akhir. Klien adalah orang yang ter-connect ke titik akhir Client VPN untuk membuat sesi VPN. Klien membuat sesi VPN dari komputer lokal atau perangkat seluler mereka menggunakan aplikasi klien VPN berbasis OpenVPN. Setelah klien membuat sesi VPN, mereka dapat dengan aman mengakses sumber daya di VPC di tempat subnet terkait berada. Klien juga dapat mengakses sumber daya lain di AWS, jaringan On-Premise, atau klien lain jika aturan rute dan otorisasi yang diperlukan telah dikonfigurasi. Untuk informasi selengkapnya tentang menghubungkan ke titik akhir Client VPN untuk membuat sesi VPN, lihat Memulai di AWS Panduan Pengguna Client VPN.

Grafis berikut menggambarkan arsitektur Client VPN basic.



Autentikasi Klien

Otentikasi klien diimplementasikan pada titik pertama masuk ke AWS Cloud. Hal ini digunakan untuk menentukan apakah klien diizinkan untuk terhubung ke titik akhir Client VPN. Jika autentikasi berhasil, klien terhubung ke titik akhir Client VPN dan membuat sesi VPN. Jika autentikasi gagal, hubungan ditolak dan klien dicegah dari membangun sesi VPN.

Client VPN menawarkan jenis autentikasi klien berikut:

- Autentikasi direktori aktif (berbasis pengguna)
- Autentikasi bersama (berbasis sertifikat)
- Sistem masuk tunggal (autentikasi federasi berbasis SAML) (berbasis pengguna)

Anda dapat menggunakan salah satu metode yang tercantum di atas saja, atau kombinasi otentikasi timbal balik dengan metode berbasis pengguna seperti berikut ini:

- Autentikasi bersama dan autentikasi federasi
- Autentikasi bersama dan autentikasi Direktori Aktif

> **Important**
>
> Untuk membuat titik akhir Client VPN, Anda harus menyediakan sertifikat server AWS Certificate Manager, terlepas dari jenis otentikasi yang Anda gunakan. Untuk informasi selengkapnya tentang pembuatan dan penyediaan sertifikat server, lihat langkah-langkah di Autentikasi bersama.

Autentikasi Direktori Aktif

Client VPN menyediakan dukungan Active Directory dengan mengintegrasikan dengan AWS Directory Service. Dengan autentikasi Direktori Aktif, klien diautentikassi terhadap kelompok Direktori Aktif yang ada. Menggunakan AWS Directory Service, Client VPN dapat terhubung ke Direktori Aktif yang ada yang disediakan di dalam AWS atau di jaringan lokal Anda. Hal ini memungkinkan Anda untuk menggunakan infrastruktur autentikasi klien yang ada. Jika Anda menggunakan Active Directory lokal dan Anda tidak memiliki Microsoft AD AWS Terkelola yang ada, Anda harus mengonfigurasi Konektor Direktori Aktif (AD Connector). Anda dapat menggunakan satu server Direktori Aktif untuk mengautentikasi pengguna. Untuk informasi selengkapnya tentang integrasi Direktori Aktif, lihat AWS Directory Service Panduan Administrasi.

Client VPN mendukung autentikasi multi-faktor (MFA) saat diaktifkan untuk AWS Dikelola Microsoft AD atau AD Connector. Jika MFA diaktifkan, klien harus memasukkan nama pengguna, kata sandi, dan kode MFA ketika mereka terhubung ke titik akhir Client VPN. Untuk informasi selengkapnya tentang mengaktifkan MFA, lihat Aktifkan Autentikasi Multi-Faktor untuk AWS Microsoft AD Terkelola dan Aktifkan Autentikasi Multi-Faktor untuk AD Connector di AWS Directory Service Panduan administrasi.

Untuk kuota dan aturan untuk mengonfigurasi pengguna dan grup di Direktori Aktif, lihat Kuota pengguna dan grup.

Autentikasi bersama

Dengan autentikasi bersama, Client VPN menggunakan sertifikat untuk melakukan autentikasi antara klien dan server. Sertifikat adalah bentuk identifikasi digital yang diterbitkan oleh otoritas sertifikat

(CA). Server menggunakan sertifikat klien untuk mengautentikasi klien ketika sertifikat tersebut mencoba untuk terhubung ke titik akhir Client VPN. Anda harus membuat sertifikat server dan kunci, dan setidaknya satu sertifikat klien dan kunci.

Anda harus mengunggah sertifikat server ke AWS Certificate Manager (ACM) dan menentukannya saat Anda membuat titik akhir Client VPN. Ketika Anda mengunggah sertifikat server untuk ACM, Anda juga menentukan otoritas sertifikat (CA). Anda hanya perlu mengunggah sertifikat klien untuk ACM ketika CA sertifikat klien berbeda dari CA sertifikat server. Untuk informasi selengkapnya tentang ACM, lihat AWS Certificate Manager Panduan Pengguna.

Anda dapat membuat sertifikat klien dan kunci terpisah untuk setiap klien yang akan terhubung ke titik akhir Client VPN. Hal ini memungkinkan Anda untuk mencabut sertifikat klien tertentu jika pengguna meninggalkan organisasi Anda. Dalam kasus ini, ketika Anda membuat titik akhir Client VPN, Anda dapat menentukan ARN sertifikat server untuk sertifikat klien, asalkan sertifikat klien telah dikeluarkan oleh CA yang sama sebagai sertifikat server.

> **Note**
>
> Titik akhir Client VPN mendukung 1024-bit dan 2048-bit RSA kunci ukuran saja. Juga, sertifikat klien harus memiliki atribut CN di bidang Subjek.
> Ketika sertifikat yang digunakan dengan layanan Client VPN diperbarui, baik melalui rotasi otomatis ACM, mengimpor sertifikat baru secara manual, atau pembaruan metadata ke Pusat Identitas IAM, layanan Client VPN akan secara otomatis memperbarui titik akhir Client VPN dengan sertifikat yang lebih baru. Ini adalah proses otomatis yang dapat memakan waktu hingga 24 jam.

Linux/macOS

Prosedur berikut menggunakan OpenVPN easy-rsa untuk membuat sertifikat dan kunci server dan klien, lalu mengunggah sertifikat dan kunci server ke ACM. Untuk informasi selengkapnya, lihat bagian Easy-RSA 3 Quickstart README.

Untuk membuat sertifikat dan kunci server serta klien dan mengunggahnya ke ACM

1. Kloning OpenVPN easy-rsa repo ke komputer lokal Anda dan navigasikan ke `easy-rsa/easyrsa3` folder tersebut.

```
$ git clone https://github.com/OpenVPN/easy-rsa.git
```

```
$ cd easy-rsa/easyrsa3
```

2. Inisialisasi lingkungan PKI baru.

```
$ ./easyrsa init-pki
```

3. Untuk membangun otoritas sertifikat baru (CA), jalankan perintah ini dan ikuti petunjuknya.

```
$ ./easyrsa build-ca nopass
```

4. Membuat sertifikat server dan kunci.

```
$ ./easyrsa --san=DNS:server build-server-full server nopass
```

5. Membuat sertifikat klien dan kunci.

   Pastikan untuk menyimpan sertifikat klien dan kunci privat klien karena Anda akan membutuhkannya ketika Anda mengonfigurasi klien.

```
$ ./easyrsa build-client-full client1.domain.tld nopass
```

   Anda dapat secara opsional mengulangi langkah ini untuk setiap klien (pengguna akhir) yang memerlukan sertifikat klien dan kunci.

6. Salin sertifikat server dan kunci serta sertifikat klien dan kunci ke folder khusus lalu kemudian navigasikan ke folder khusus.

   Sebelum Anda menyalin sertifikat dan kunci, buat folder khusus dengan menggunakan `mkdir` perintah. Contoh berikut membuat folder khusus di direktori beranda Anda.

```
$ mkdir ~/custom_folder/
$ cp pki/ca.crt ~/custom_folder/
$ cp pki/issued/server.crt ~/custom_folder/
$ cp pki/private/server.key ~/custom_folder/
$ cp pki/issued/client1.domain.tld.crt ~/custom_folder
$ cp pki/private/client1.domain.tld.key ~/custom_folder/
$ cd ~/custom_folder/
```

7. Unggah sertifikat server dan kunci serta sertifikatklien dan kunci untuk ACM. Pastikan untuk mengunggahnya di Wilayah yang sama di mana Anda ingin membuat titik akhir Client VPN.

Perintah berikut menggunakan AWS CLI untuk mengunggah sertifikat. Untuk mengunggah sertifikat menggunakan konsol ACM, lihat Impor sertifikat di AWS Certificate Manager Panduan Pengguna.

```
$ aws acm import-certificate --certificate fileb://server.crt --private-key
 fileb://server.key --certificate-chain fileb://ca.crt
```

```
$ aws acm import-certificate --certificate fileb://client1.domain.tld.crt --
private-key fileb://client1.domain.tld.key --certificate-chain fileb://ca.crt
```

Anda tidak perlu mengunggah sertifikat klien ke ACM. Jika sertifikat server dan klien telah dikeluarkan oleh Otoritas Sertifikat (CA) yang sama, Anda dapat menggunakan sertifikat server ARN untuk server dan klien saat Anda membuat titik akhir Client VPN. Pada langkah-langkah di atas, CA yang sama telah digunakan untuk membuat kedua sertifikat. Namun, langkah-langkah untuk mengunggah sertifikat klien disertakan untuk kelengkapan.

Windows

Prosedur berikut menginstal perangkat lunak Easy-RSA 3.x dan menggunakannya untuk menghasilkan sertifikat dan kunci server dan klien.

Untuk menghasilkan sertifikat dan kunci server dan klien dan mengunggahnya ke ACM

1. Buka halaman rilis EasyRSA dan unduh file ZIP untuk versi Windows Anda dan ekstrak.
2. Buka prompt perintah dan arahkan ke lokasi tempat `EasyRSA-3.x` folder diekstraksi.
3. Jalankan perintah berikut untuk membuka shell EasyRSA 3.

```
C:\Program Files\EasyRSA-3.x> .\EasyRSA-Start.bat
```

4. Inisialisasi lingkungan PKI baru.

```
# ./easyrsa init-pki
```

5. Untuk membangun otoritas sertifikat baru (CA), jalankan perintah ini dan ikuti petunjuknya.

```
# ./easyrsa build-ca nopass
```

6. Membuat sertifikat server dan kunci.

```
# ./easyrsa --san=DNS:server build-server-full server nopass
```

7. Membuat sertifikat klien dan kunci.

```
# ./easyrsa build-client-full client1.domain.tld nopass
```

Anda dapat secara opsional mengulangi langkah ini untuk setiap klien (pengguna akhir) yang memerlukan sertifikat klien dan kunci.

8. Keluar dari shell EasyRSA 3.

```
# exit
```

9. Salin sertifikat server dan kunci serta sertifikat klien dan kunci ke folder khusus lalu kemudian navigasikan ke folder khusus.

Sebelum Anda menyalin sertifikat dan kunci, buat folder khusus dengan menggunakan `mkdir` perintah. Contoh berikut membuat folder khusus di C:\ drive.

```
C:\Program Files\EasyRSA-3.x> mkdir C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\ca.crt C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\issued\server.crt C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\private\server.key C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\issued\client1.domain.tld.crt C:
\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\private\client1.domain.tld.key C:
\custom_folder
C:\Program Files\EasyRSA-3.x> cd C:\custom_folder
```

10. Unggah sertifikat server dan kunci serta sertifikat klien dan kunci untuk ACM. Pastikan untuk mengunggahnya di Wilayah yang sama di mana Anda ingin membuat titik akhir Client VPN. Perintah berikut menggunakan AWS CLI untuk meng-upload sertifikat. Untuk mengunggah sertifikat menggunakan konsol ACM, lihat Impor sertifikat di AWS Certificate Manager Panduan Pengguna.

```
aws acm import-certificate --certificate fileb://server.crt --private-key
 fileb://server.key --certificate-chain fileb://ca.crt
```

```
aws acm import-certificate --certificate fileb://client1.domain.tld.crt --
private-key fileb://client1.domain.tld.key --certificate-chain fileb://ca.crt
```

Anda tidak perlu mengunggah sertifikat klien ke ACM. Jika sertifikat server dan klien telah dikeluarkan oleh Otoritas Sertifikat (CA) yang sama, Anda dapat menggunakan sertifikat server ARN untuk server dan klien saat Anda membuat titik akhir Client VPN. Pada langkah-langkah di atas, CA yang sama telah digunakan untuk membuat kedua sertifikat. Namun, langkah-langkah untuk mengunggah sertifikat klien disertakan untuk kelengkapan.

Memperbarui sertifikat server Anda

Anda dapat memperbarui dan mengimpor sertifikat server yang telah kedaluwarsa dengan prosedur berikut.

1. Jalankan perintah perpanjangan sertifikat.

```
$ ./easyrsa renew server nopass
```

2. Buat folder khusus, salin file baru ke sana, lalu navigasikan ke folder.

```
$ mkdir ~/custom_folder2
$ cp pki/ca.crt ~/custom_folder2/
$ cp pki/issued/server.crt ~/custom_folder2/
$ cp pki/private/server.key ~/custom_folder2/
$ cd ~/custom_folder2/
```

3. Impor file baru ke ACM. Pastikan untuk mengimpornya di Wilayah yang sama dengan titik akhir Client VPN.

```
$ aws acm import-certificate --certificate fileb://server.crt --private-key
 fileb://server.key --certificate-chain fileb://ca.crt
```

Sistem masuk tunggal (autentikasi federasi berbasis SAML 2.0)

AWS Client VPN mendukung federasi identitas dengan Security Assertion Markup Language 2.0 (SAMP 2.0) untuk titik akhir Client VPN. Anda dapat menggunakan penyedia identitas (IdPs) yang mendukung SAMP 2.0 untuk membuat identitas pengguna terpusat. Kemudian Anda dapat

mengonfigurasi titik akhir Client VPN untuk menggunakan autentikasi Federasi berbasis SAML, dan mengaitkannya dengan IdP. Pengguna kemudian terhubung ke titik akhir Client VPN menggunakan kredensial terpusat.

Untuk mengaktifkan IdP berbasis SAML untuk bekerja dengan titik akhir Client VPN, Anda harus melakukan hal berikut.

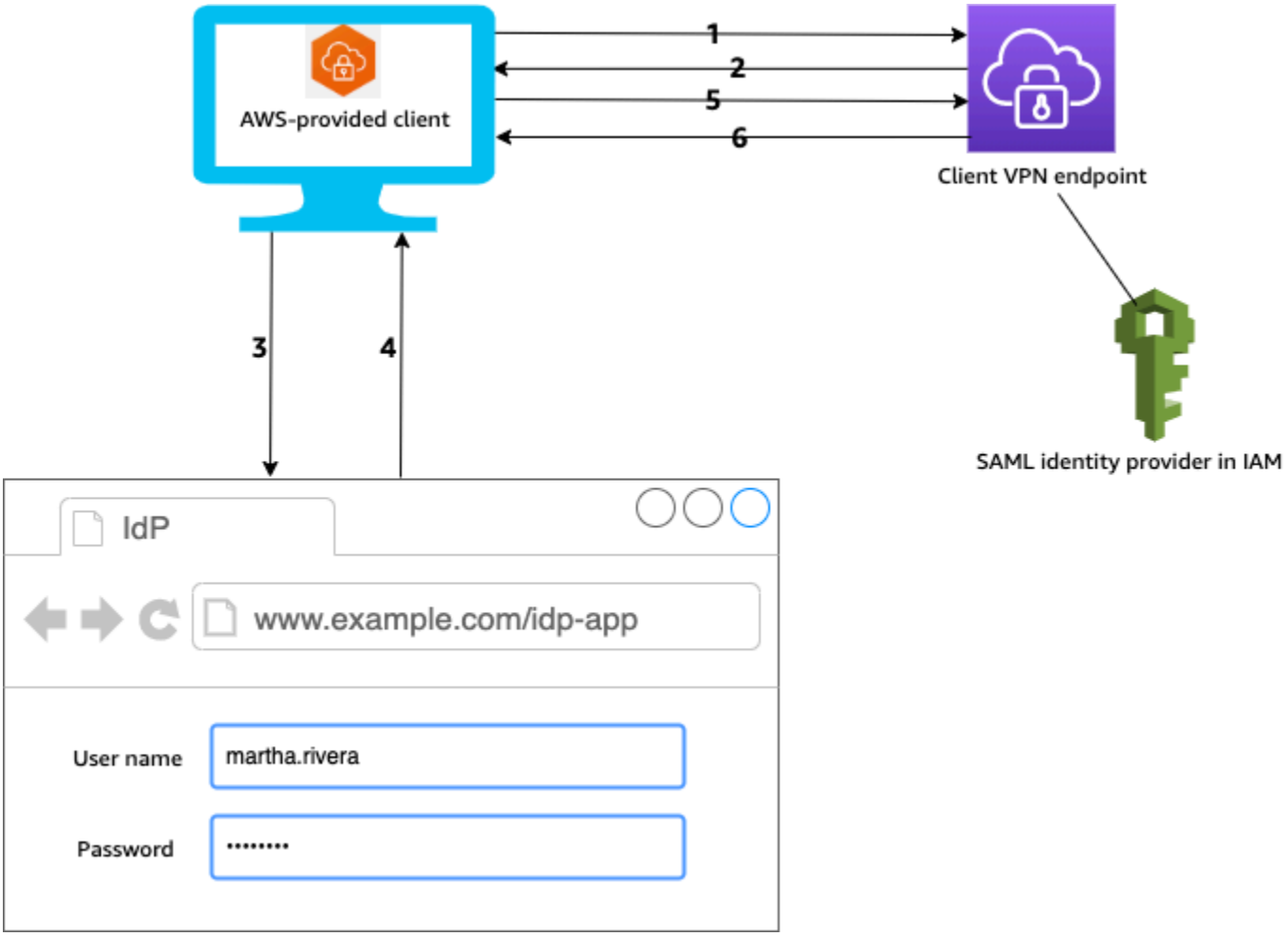
1. Buat aplikasi berbasis SAML di IDP pilihan Anda untuk digunakan AWS Client VPN, atau gunakan aplikasi yang sudah ada.
2. Konfigurasikan IdP Anda untuk membuat hubungan kepercayaan dengan AWS. Untuk sumber daya, lihat sumber daya konfigurasi IdP berbasis SAML.
3. Di IdP Anda, buat dan unduh dokumen metadata federasi yang menjelaskan organisasi Anda sebagai IdP. Dokumen XHTML yang ditandatangani ini digunakan untuk membangun hubungan kepercayaan antara AWS dan IDP.
4. Buat penyedia identitas IAM SAMP di AWS akun yang sama dengan titik akhir Client VPN. Penyedia identitas SAMP IAM mendefinisikan hubungan AWS IDP-to-trust organisasi Anda menggunakan dokumen metadata yang dihasilkan oleh IDP. Untuk informasi selengkapnya, lihat Membuat Penyedia Identitas SAML IAM dalam Panduan Pengguna IAM. Jika nanti Anda memperbarui konfigurasi aplikasi di IdP, buat dokumen metadata baru dan perbarui penyedia identitas SAML IAM Anda.

   > **Note**
   >
   > Anda tidak perlu membuat IAM role untuk menggunakan penyedia identitas SAML IAM.

5. Buat titik akhir Client VPN Tentukan autentikasi federasi sebagai jenis autentikasi, dan tentukan penyedia identitas SAML IAM yang Anda buat. Untuk informasi selengkapnya, lihat Buat titik akhir Client VPN.
6. Ekspor file konfigurasi klien dan mendistribusikannya ke pengguna Anda. Instruksikan pengguna Anda untuk mengunduh versi terbaru dari AWS klien yang disediakan, dan menggunakannya untuk memuat file konfigurasi dan terhubung ke titik akhir Client VPN. Atau, jika Anda mengaktifkan portal swalayan untuk titik akhir Client VPN Anda, instruksikan pengguna Anda untuk pergi ke portal swalayan untuk mendapatkan file konfigurasi dan klien yang disediakan. AWS Untuk informasi selengkapnya, lihat Mengakses portal layanan mandiri.

Alur kerja autentikasi

Diagram berikut memberikan gambaran umum tentang alur kerja autentikasi untuk titik akhir Client VPN yang menggunakan autentikasi federasi berbasis SAML. Ketika Anda membuat dan mengkonfigurasi titik akhir Client VPN, Anda menentukan penyedia identitas SAML IAM.



1. Pengguna membuka klien yang AWS disediakan di perangkat mereka dan memulai koneksi ke titik akhir Client VPN.
2. Titik akhir Client VPN mengirimkan URL IdP dan permintaan autentikasi kembali ke klien, berdasarkan informasi yang disediakan di penyedia identitas SAML IAM.
3. Klien yang AWS disediakan membuka jendela browser baru di perangkat pengguna. Peramban membuat permintaan ke IdP dan menampilkan halaman login.
4. Pengguna memasukkan kredensial mereka di halaman login, dan IdP mengirimkan pernyataan SAML yang ditandatangani kembali ke klien.
5. Klien AWS yang disediakan mengirimkan pernyataan SAMP ke titik akhir Client VPN.

6. Titik akhir Client VPN memvalidasi pernyataan dan mengizinkan atau menolak akses ke pengguna.

Persyaratan dan pertimbangan untuk autentikasi federasi berbasis SAML

Berikut ini merupakan persyaratan dan pertimbangan untuk autentikasi federasi berbasis SAML.

- Untuk kuota dan aturan untuk mengonfigurasi pengguna dan grup di IdP berbasis SAML, lihat Kuota pengguna dan grup.
- Pernyataan SAMP dan dokumen SAMP harus ditandatangani.
- AWS Client VPN hanya mendukung kondisi AudienceRestriction "" dan "NotBefore dan NotOnOrAfter" dalam pernyataan SAMP.
- Ukuran maksimum yang didukung untuk respons SAML adalah 128 KB.
- AWS Client VPN tidak menyediakan permintaan otentikasi yang ditandatangani.
- Logout tunggal SAML tidak didukung. Pengguna dapat keluar dengan memutuskan sambungan dari klien yang AWS disediakan, atau Anda dapat menghentikan koneksi.
- Titik akhir Client VPN mendukung satu IdP saja.
- Autentikasi Multi-Faktor (MFA) didukung bila diaktifkan di IdP Anda.
- Pengguna harus menggunakan klien yang AWS disediakan untuk terhubung ke titik akhir Client VPN. Pengguna harus menggunakan versi 1.2.0 atau lebih baru. Untuk informasi selengkapnya, lihat Connect menggunakan klien AWS yang disediakan.
- Peramban berikut didukung untuk autentikasi IdP: Apple Safari, Google Chrome, Microsoft Edge, dan Mozilla Firefox.
- Klien yang AWS disediakan mencadangkan port TCP 35001 pada perangkat pengguna untuk respons SAMP.
- Jika dokumen metadata untuk penyedia identitas SAML IAM diperbarui dengan URL yang salah atau berbahaya, hal ini dapat menyebabkan masalah autentikasi bagi pengguna, atau mengakibatkan serangan phishing. Oleh karena itu, sebaiknya gunakan AWS CloudTrail untuk memantau pembaruan yang dilakukan pada penyedia identitas SAML IAM. Untuk informasi selengkapnya, lihat Logging IAM dan AWS STS panggilan dengan AWS CloudTrail di Panduan Pengguna IAM.
- AWS Client VPN mengirimkan permintaan AuthN ke IDP melalui pengikatan HTTP Redirect. Oleh karena itu, IdP harus mendukung pengikatan Pengalihan HTTP dan harus ada dalam dokumen metadata IdP.

- Untuk pernyataan SAML, Anda harus menggunakan format alamat email untuk `NameID` atribut.

sumber daya konfigurasi IdP berbasis SAML

Tabel berikut mencantumkan berbasis SAML IdPs yang telah kami uji untuk digunakan AWS Client VPN, dan sumber daya yang dapat membantu Anda mengonfigurasi IDP.

IdP	Sumber Daya
Okta	Otentikasi AWS Client VPN pengguna dengan SAMP
Direktori Aktif Microsoft Azure	Untuk informasi selengkapnya, lihat Tutorial: Integrasi sistem masuk tunggal (SSO) Azure Active Directory dengan AWS ClientVPN di situs web dokumentasi Microsoft.
JumpCloud	Single Sign On (SSO) dengan AWS Client VPN
AWS IAM Identity Center	Menggunakan IAM Identity Center dengan AWS Client VPN untuk otentikasi dan otorisasi

Informasi penyedia layanan untuk membuat aplikasi

Untuk membuat aplikasi berbasis SAML menggunakan iDP yang tidak tercantum dalam tabel sebelumnya, gunakan informasi berikut untuk mengonfigurasi informasi penyedia layanan. AWS Client VPN

- URL Assertion Consumer Service (ACS): `http://127.0.0.1:35001`
- URI Pemirsa: `urn:amazon:webservices:clientvpn`

Setidaknya satu atribut harus disertakan dalam respons SAMP dari IDP. Berikut ini adalah contoh atribut.

Atribut	Deskripsi
`FirstName`	Nama pertama pengguna.

Atribut	Deskripsi
`LastName`	Nama terakhir pengguna.
`memberOf`	Grup atau beberapa grup tempat pengguna berada.

> **Note**
>
> `memberOf`Atribut diperlukan untuk menggunakan Active Directory atau aturan otorisasi berbasis grup SAMP IDP. Ini juga peka huruf besar/kecil, dan harus dikonfigurasi persis seperti yang ditentukan. Lihat Otorisasi berbasis jaringan dan Aturan otorisasi untuk informasi lebih lanjut.

Dukungan untuk portal layanan mandiri

Jika Anda mengaktifkan portal layanan mandiri untuk titik akhir Client VPN, pengguna masuk ke portal menggunakan kredensial IdP berbasis SAML mereka.

Jika IdP Anda mendukung beberapa URL Assertion Consumer Service (ACS), tambahkan URL ACS berikut ke aplikasi Anda.

```
https://self-service.clientvpn.amazonaws.com/api/auth/sso/saml
```

Jika Anda menggunakan titik akhir Client VPN di suatu GovCloud wilayah, gunakan URL ACS berikut sebagai gantinya. Jika Anda menggunakan aplikasi IDP yang sama untuk mengautentikasi standar dan GovCloud wilayah, Anda dapat menambahkan kedua URL.

```
https://gov.self-service.clientvpn.amazonaws.com/api/auth/sso/saml
```

Jika IdP Anda tidak mendukung beberapa URL ACS, lakukan hal berikut:

1. Buat aplikasi berbasis SAML tambahan di IdP Anda dan tentukan URL ACS berikut.

   ```
   https://self-service.clientvpn.amazonaws.com/api/auth/sso/saml
   ```

2. Buat dan unduh dokumen metadata federasi.

3. Buat penyedia identitas IAM SAMP di AWS akun yang sama dengan titik akhir Client VPN. Untuk informasi selengkapnya, lihat Membuat Penyedia Identitas SAML IAM dalam Panduan Pengguna IAM.

> **Note**
>
> Anda membuat penyedia identitas SAML IAM ini selain yang Anda buat untuk aplikasi utama.

4. Buat titik akhir Client VPN, dan tentukan kedua penyedia identitas SAML IAM yang Anda buat.

Otorisasi klien

Client VPN mendukung dua jenis otorisasi: grup keamanan dan otorisasi berbasis jaringan (menggunakan aturan otorisasi).

Grup keamanan

Saat membuat titik akhir Client VPN, Anda dapat menentukan grup keamanan dari VPC tertentu untuk diterapkan ke titik akhir Client VPN. Ketika Anda mengaitkan subnet dengan titik akhir Client VPN, kami secara otomatis menerapkan grup keamanan default VPC. Anda dapat mengubah grup keamanan setelah Anda membuat titik akhir Client VPN. Untuk informasi selengkapnya, lihat Terapkan grup keamanan ke jaringan target. Grup keamanan terkait dengan antarmuka jaringan Client VPN.

Anda dapat mengaktifkan pengguna Client VPN untuk mengakses aplikasi Anda di VPC dengan menambahkan aturan ke grup keamanan aplikasi Anda untuk mengizinkan lalu lintas dari grup keamanan yang diterapkan ke asosiasi.

Untuk menambahkan aturan yang mengizinkan lalu lintas dari grup keamanan titik akhir Client VPN

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Grup Keamanan.
3. Pilih grup keamanan yang terkait dengan sumber daya atau aplikasi Anda, dan pilih Tindakan, Edit aturan masuk.
4. Pilih Tambahkan aturan.
5. Untuk Jenis, pilih Semua lalu lintas. Atau, Anda dapat membatasi akses ke jenis lalu lintas tertentu, misalnya, SSH.

Untuk Sumber, tentukan ID grup keamanan yang terkait dengan jaringan target (subnet) untuk titik akhir Client VPN.

6. Pilih Simpan aturan.

Sebaliknya, Anda dapat membatasi akses untuk pengguna Client VPN dengan tidak menentukan grup keamanan yang diterapkan ke asosiasi, atau dengan menghapus aturan yang mereferensikan grup keamanan titik akhir Client VPN. Aturan grup keamanan yang Anda perlukan mungkin juga bergantung pada jenis akses VPN yang ingin Anda konfigurasikan. Untuk informasi selengkapnya, lihat Skenario dan contoh untuk AWS Client VPN.

Untuk informasi selengkapnya, lihat Grup Keamanan untuk VPC Anda di Panduan Pengguna Amazon VPC.

Otorisasi berbasis jaringan

Otorisasi berbasis jaringan diimplementasikan menggunakan aturan otorisasi. Untuk setiap jaringan yang ingin Anda aktifkan aksesnya, Anda harus mengonfigurasi aturan otorisasi yang membatasi pengguna yang memiliki akses. Untuk jaringan tertentu, Anda mengonfigurasi grup Direktori Aktif atau grup IdP berbasis SAML yang diizinkan mengakses. Hanya untuk pengguna grup ini yang dapat mengakses jaringan yang ditentukan. Jika Anda tidak menggunakan Direktori Aktif atau autentikasi federasi berbasis SAML, atau Anda ingin membuka akses ke semua pengguna, Anda dapat menentukan aturan yang memberikan akses ke semua klien. Untuk informasi selengkapnya, lihat Aturan otorisasi.

Otorisasi koneksi

Anda dapat mengonfigurasi handler koneksi klien Untuk titik akhir Client VPN Anda. Handler memungkinkan Anda untuk menjalankan logika kustom yang mengotorisasi koneksi baru, berdasarkan atribut perangkat, pengguna, dan koneksi. Handler koneksi klien berjalan setelah layanan Client VPN mengautentikasi perangkat dan pengguna.

Untuk mengonfigurasi handler koneksi klien ke titik akhir Client VPN Anda, buat fungsi AWS Lambda yang membutuhkan atribut perangkat, pengguna, dan koneksi sebagai input, dan menyerahkan keputusan ke layanan Client VPN untuk mengizinkan atau menolak koneksi baru. Anda menentukan fungsi Lambda di titik akhir Client VPN Anda. Ketika perangkat terhubung ke titik akhir Client VPN Anda, layanan Client VPN mengaktifkan fungsi Lambda atas nama Anda. Hanya koneksi yang diotorisasikan oleh fungsi Lambda yang diizinkan untuk terhubung ke titik akhir Client VPN.

> **Note**
>
> Saat ini, satu-satunya tipe handler koneksi klien yang didukung adalah fungsi Lambda.

Persyaratan dan pertimbangan

Berikut ini adalah persyaratan dan pertimbangan untuk handler koneksi klien:

- Nama fungsi Lambda harus diawali dengan prefiks `AWSClientVPN-`.
- Mendukung fungsi Lambda yang berkualitas.
- Fungsi Lambda harus berada di AWS Wilayah yang sama dan AWS akun yang sama dengan titik akhir Client VPN.
- Waktu fungsi Lambda habis setelah 30 detik. Nilai ini tidak dapat diubah.
- Fungsi Lambda diaktifkan secara serentak. Fungsi ini diaktifkan setelah autentikasi perangkat dan pengguna, dan sebelum aturan otorisasi dievaluasi.
- Jika fungsi Lambda diaktifkan untuk koneksi baru dan layanan Client VPN tidak mendapatkan respons yang diharapkan dari fungsi, layanan Client VPN menolak permintaan koneksi. Misalnya, hal ini dapat terjadi jika fungsi Lambda ter-throttling, waktu habis, atau menemukan kesalahan tak terduga lainnya, atau jika respons fungsi tidak dalam format yang valid.
- Kami merekomendasikan agar Anda mengonfigurasikan konkurensi yang disediakan untuk fungsi Lambda untuk mengaktifkannya agar dapat menskalakan tanpa fluktuasi dalam latensi.
- Jika Anda memperbarui fungsi Lambda, koneksi ke titik akhir Client VPN yang ada tidak akan terpengaruh. Anda dapat mengakhiri koneksi yang ada, dan kemudian menginstruksikan klien Anda untuk membuat koneksi baru. Untuk informasi selengkapnya, lihat Mengakhiri koneksi klien.
- Jika klien menggunakan klien yang AWS disediakan untuk terhubung ke titik akhir Client VPN, mereka harus menggunakan versi 1.2.6 atau yang lebih baru untuk Windows, dan versi 1.2.4 atau yang lebih baru untuk macOS. Untuk informasi selengkapnya, lihat Hubungkan menggunakan klien AWS yang disediakan.

Antarmuka Lambda

Fungsi Lambda membutuhkan atribut perangkat, atribut pengguna, dan atribut koneksi sebagai input dari layanan Client VPN. Fungsi tersebut kemudian menyerahkan keputusan ke layanan Client VPN apakah mengizinkan atau menolak koneksi.

Meminta skema

Fungsi Lambda membutuhkan blob JSON yang berisi bidang-bidang berikut sebagai input.

```
{
    "connection-id": <connection ID>,
    "endpoint-id": <client VPN endpoint ID>,
    "common-name": <cert-common-name>,
    "username": <user identifier>,
    "platform": <OS platform>,
    "platform-version": <OS version>,
    "public-ip": <public IP address>,
    "client-openvpn-version": <client OpenVPN version>,
    "aws-client-version": <AWS client version>,
    "groups": <group identifier>,
    "schema-version": "v3"
}
```

- `connection-id` — ID koneksi klien ke titik akhir Client VPN.
- `endpoint-id` — ID titik akhir Client VPN.
- `common-name` — Pengidentifikasi perangkat. Pada sertifikat klien yang Anda buat untuk perangkat, nama umum secara unik mengidentifikasi perangkat.
- `username` — Pengidentifikasi pengguna, jika ada. Untuk autentikasi Direktori Aktif, ini adalah nama pengguna. Untuk autentikasi gabungan berbasis SAML, ini adalah `NameID`. Untuk autentikasi bersama, bidang ini kosong.
- `platform` — Platform sistem operasi klien.
- `platform-version` — Versi sistem operasi. Layanan Client VPN memberikan nilai ketika arahan `--push-peer-info` hadir dalam konfigurasi klien OpenVPN saat klien terhubung ke titik akhir Client VPN, dan saat klien menjalankan platform Windows.
- `public-ip` — Alamat IP publik dari perangkat yang terhubung.
- `client-openvpn-version` — Versi OpenVPN yang digunakan klien.
- `aws-client-version`— Versi AWS klien.
- `groups` — Pengidentifikasi grup, jika ada. Untuk autentikasi Direktori Aktif, ini akan menjadi daftar grup Direktori Aktif. Untuk autentikasi gabungan berbasis SAML, ini akan menjadi daftar grup penyedia identitas (IdP). Untuk autentikasi bersama, bidang ini kosong.
- `schema-version` — Versi skema. Defaultnya adalah `v3`.

Skema respons

Fungsi Lambda harus mengembalikan bidang berikut.

```
{
    "allow": boolean,
    "error-msg-on-denied-connection": "",
    "posture-compliance-statuses": [],
    "schema-version": "v3"
}
```

- `allow` — Diperlukan. Boolean (`true` | `false`) yang menunjukkan apakah koneksi baru diizinkan atau ditolak.
- `error-msg-on-denied-connection` — Diperlukan. String dengan karakter maksimal 255 yang dapat digunakan untuk memberikan langkah-langkah dan panduan untuk klien jika koneksi ditolak oleh fungsi Lambda. Ketika terjadi kegagalan selama menjalankan fungsi Lambda (misalnya, karena throttling) pesan default berikut dikembalikan ke klien.

  ```
  Error establishing connection. Please contact your administrator.
  ```

- `posture-compliance-statuses` — Diperlukan. Jika Anda menggunakan fungsi Lambda untuk penilaian postur, ini adalah daftar status untuk perangkat yang terhubung. Anda menentukan nama status sesuai dengan kategori penilaian postur Anda untuk perangkat, misalnya, `compliant`, `quarantined`, `unknown`, dan sebagainya. Panjang setiap nama maksimal 255 karakter. Anda dapat menentukan hingga maksimal 10 status.
- `schema-version` — Diperlukan. Versi skema. Defaultnya adalah `v3`.

Anda dapat menggunakan fungsi Lambda yang sama untuk beberapa titik akhir Client VPN di Wilayah yang sama.

Untuk informasi selengkapnya tentang cara membuat fungsi Lambda, lihat Mulai dengan AWS Lambda dalam AWS Lambda Panduan Developer.

Handler koneksi klien digunakan untuk penilaian postur

Anda dapat menggunakan handler koneksi klien untuk mengintegrasikan titik akhir Client VPN Anda dengan solusi manajemen perangkat yang ada untuk mengevaluasi kepatuhan postur perangkat yang terhubung. Agar fungsi Lambda bekerja sebagai handler otorisasi perangkat, gunakan autentikasi bersama untuk titik akhir Client VPN Anda. Membuat sertifikat klien dan kunci yang unik

untuk setiap klien (perangkat) yang akan terhubung ke titik akhir Client VPN. Fungsi Lambda dapat menggunakan nama umum yang unik untuk sertifikat klien (yang diteruskan dari layanan Client VPN) untuk mengidentifikasi perangkat dan mengambil status kepatuhan postur dari solusi manajemen perangkat Anda. Anda dapat menggunakan autentikasi bersama yang dikombinasikan dengan autentikasi berbasis pengguna.

Selain itu, Anda dapat melakukan penilaian postur dasar di dalam fungsi Lambda itu sendiri. Misalnya, Anda dapat menilai bidang `platform` dan `platform-version` yang diteruskan ke fungsi Lambda oleh layanan Client VPN.

> **Note**
>
> Sementara handler koneksi dapat digunakan untuk menerapkan versi AWS Client VPN aplikasi minimum, bidang `aws-client-version` dalam handler koneksi, hanya berlaku untuk AWS Client VPN aplikasi dan sedang diisi dari variabel lingkungan pada perangkat pengguna.

Mengaktifkan handler koneksi klien

Untuk mengaktifkan handler koneksi klien, buat atau ubah titik akhir Client VPN dan tentukan Amazon Resource Name (ARN) dari fungsi Lambda. Untuk informasi selengkapnya, lihat Buat titik akhir Client VPN dan Mengubah titik akhir Client VPN.

Peran yang terhubung dengan layanan

AWS Client VPN secara otomatis membuat peran terkait layanan di akun Anda yang dipanggil. AWSServiceRoleForClientVPNConnections Peran memiliki izin untuk mengaktifkan fungsi Lambda saat koneksi dibuat ke titik akhir Client VPN. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk Client VPN.

Memantau kegagalan otorisasi koneksi

Anda dapat melihat status otorisasi koneksi dari koneksi ke titik akhir Client VPN. Untuk informasi selengkapnya, lihat Melihat koneksi klien.

Ketika handler koneksi klien digunakan untuk penilaian postur, Anda juga dapat melihat status kepatuhan postur dari perangkat yang terhubung ke titik akhir Client VPN Anda di log koneksi. Untuk informasi selengkapnya, lihat Pencatatan koneksi.

Jika perangkat gagal otorisasi koneksi, bidang `connection-attempt-failure-reason` pada log koneksi mengembalikan salah satu alasan kegagalan berikut:

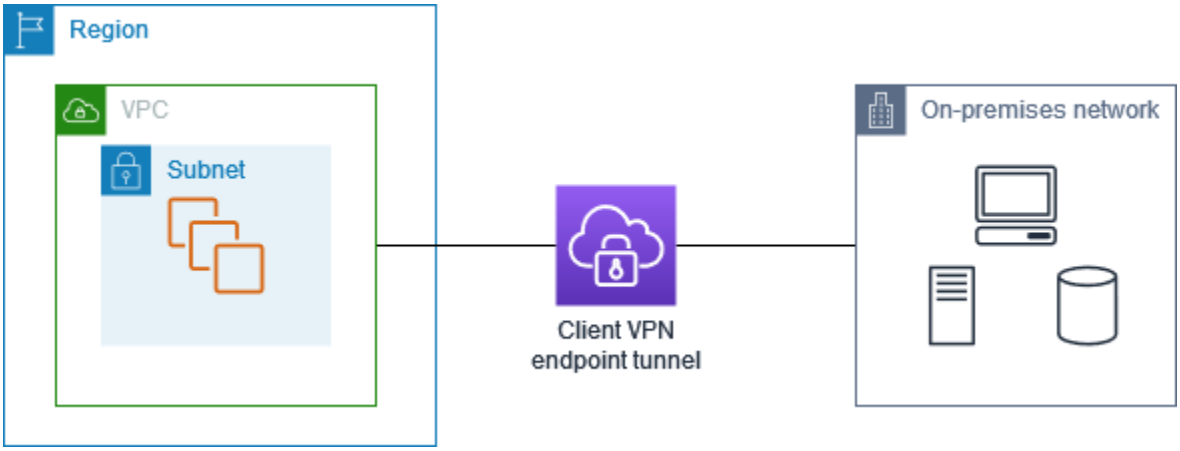
- `client-connect-failed` — Fungsi Lambda mencegah koneksi dibuat.
- `client-connect-handler-timed-out` — Waktu fungsi Lambda habis.
- `client-connect-handler-other-execution-error` — Fungsi Lambda mengalami kesalahan tak terduga.
- `client-connect-handler-throttled` — Fungsi Lambda ter-throttling.
- `client-connect-handler-invalid-response` — Fungsi Lambda mengembalikan respons yang tidak valid.
- `client-connect-handler-service-error` — Terjadi kesalahan sisi layanan selama upaya koneksi.

Terowongan terpisah pada titik akhir AWS Client VPN

Secara default, ketika Anda memiliki titik akhir Client VPN, semua lalu lintas dari klien dirutekan melalui terowongan Client VPN. Ketika Anda mengaktifkan terowongan terpisah pada titik akhir Client VPN, kami mendorong rute pada tabel rute titik akhir Client VPN ke perangkat yang terhubung ke titik akhir Client VPN. Hal ini memastikan bahwa hanya lalu lintas dengan tujuan ke jaringan yang cocok dengan rute dari tabel rute titik akhir Client VPN dirutekan melalui terowongan Client VPN.

Anda dapat menggunakan terowongan terpisah titik akhir Client VPN ketika Anda tidak ingin semua pengguna lalu lintas melewati rute melalui titik akhir Client VPN.

Dalam contoh berikut, terowongan terpisah diaktifkan pada titik akhir Client VPN. Hanya lalu lintas yang ditujukan untuk VPC (`172.31.0.0/16`) dirutekan melalui terowongan Client VPN. Lalu lintas yang ditujukan untuk sumber daya on premise tidak dirutekan melalui terowongan Client VPN.



Manfaat terowongan terpisah

Terowongan terpisah pada titik akhir Client VPN menawarkan keuntungan sebagai berikut:

- Anda dapat mengoptimalkan perutean lalu lintas dari klien dengan hanya lalu lintas AWS yang ditujukan yang akan melintasi terowongan VPN.
- Anda dapat mengurangi volume lalu lintas keluar dari AWS, sehingga mengurangi biaya transfer data.

Pertimbangan perutean

- Ketika Anda mengaktifkan terowongan terpisah, semua rute di tabel rute Client VPN ditambahkan ke tabel rute klien ketika koneksi VPN dibuat. Operasi ini berbeda dari perilaku default, yang menimpa tabel rute klien dengan entri`0.0.0.0/0`untuk merutekan semua lalu lintas melalui VPN.

  > **Note**
  >
  > Tidak disarankan untuk menambahkan`0.0.0.0/0`rute ke tabel rute titik akhir Client VPN saat menggunakan mode split-tunnel.

- Saat mode split-tunnel diaktifkan, modifikasi apa pun pada tabel rute titik akhir Client VPN akan mengakibatkan semua koneksi klien disetel ulang.

Enabling-split-tunnel

Anda dapat mengaktifkan terowongan terpisah pada titik akhir Client VPN. Untuk informasi selengkapnya, lihat topik berikut:

- Buat titik akhir Client VPN
- Mengubah titik akhir Client VPN

Pencatatan koneksi

Pencatatan koneksi adalah fitur AWS Client VPN yang mengijinkan Anda untuk menangkap catatan koneksi untuk titik akhir Client VPN Anda.

Log koneksi berisi entri log koneksi. Setiap entri log koneksi berisi informasi tentang peristiwa hubungan, yaitu saat klien (pengguna akhir) terhubung, mencoba menghubungkan, atau memutuskan hubungan dari titik akhir Client VPN Anda. Anda dapat menggunakan informasi ini untuk menjalankan forensik, menganalisis bagaimana titik akhir Client VPN Anda digunakan, atau men-debug masalah koneksi.

Pencatatan koneksi tersedia di semua Wilayah tempat AWS Client VPN tersedia. Log koneksi dipublikasikan ke CloudWatch Log di akun Anda.

> **Note**
>
> Upaya otentikasi timbal balik yang gagal tidak dicatat.

Entri log koneksi

Entri log koneksi adalah gumpalan pasangan nilai kunci yang diformat JSON. Berikut ini adalah contoh entri log koneksi.

```
{
    "connection-log-type": "connection-attempt",
    "connection-attempt-status": "successful",
    "connection-reset-status": "NA",
    "connection-attempt-failure-reason": "NA",
    "connection-id": "cvpn-connection-abc123abc123abc12",
    "client-vpn-endpoint-id": "cvpn-endpoint-aaa111bbb222ccc33",
    "transport-protocol": "udp",
    "connection-start-time": "2020-03-26 20:37:15",
    "connection-last-update-time": "2020-03-26 20:37:15",
    "client-ip": "10.0.1.2",
    "common-name": "client1",
    "device-type": "mac",
    "device-ip": "98.247.202.82",
    "port": "50096",
    "ingress-bytes": "0",
    "egress-bytes": "0",
    "ingress-packets": "0",
    "egress-packets": "0",
    "connection-end-time": "NA",
    "username": "joe"
    }
```

Entri log koneksi berisi kunci-kunci berikut:

- `connection-log-type` — Jenis entri log koneksi (`connection-attempt` atau `connection-reset`).
- `connection-attempt-status` — Status permintaan koneksi (`successful`, `failed`, `waiting-for-assertion`, atau `NA`).
- `connection-reset-status` — Status peristiwa pengaturan ulang koneksi (`NA` atau `assertion-received`).
- `connection-attempt-failure-reason` — Alasan kegagalan koneksi, jika berlaku.
- `connection-id` — Koneksi ID.
- `client-vpn-endpoint-id` — ID titik akhir Client VPN tempat koneksi dibuat.
- `transport-protocol` — Protokol transport yang digunakan untuk koneksi.
- `connection-start-time` — Waktu mulai koneksi.
- `connection-last-update-time` — Waktu pembaruan terakhir dari koneksi. Nilai ini diperbarui secara berkala di log.
- `client-ip` — Alamat IP klien, yang dialokasikan dari rentang CIDR IPv4 klien untuk titik akhir Client VPN.
- `common-name` — Nama umum sertifikat yang digunakan untuk autentikasi berbasis sertifikat.
- `device-type` — Jenis perangkat yang digunakan untuk koneksi oleh pengguna akhir.
- `device-ip` — Alamat IP publik perangkat.
- `port` — Nomor port untuk koneksi.
- `ingress-bytes` — Jumlah byte ingress (masuk) untuk koneksi. Nilai ini diperbarui secara berkala di log.
- `egress-bytes` — Jumlah byte egress (keluar) untuk koneksi. Nilai ini diperbarui secara berkala di log.
- `ingress-packets` — Jumlah paket ingress (masuk) untuk koneksi. Nilai ini diperbarui secara berkala di log.
- `egress-packets` — Jumlah paket egress (keluar) untuk koneksi. Nilai ini diperbarui secara berkala di log.
- `connection-end-time` — Waktu akhir koneksi. Nilai adalah `NA` jika koneksi masih berlangsung atau jika upaya koneksi gagal.
- `posture-compliance-statuses` — Status kepatuhan postur yang dikembalikan oleh pengendali koneksi klien, jika berlaku.

- `username`Nama pengguna dicatat ketika otentikasi berbasis pengguna (AD atau SALL) digunakan untuk titik akhir.
- `connection-duration-seconds`— Durasi koneksi dalam hitungan detik. Sama dengan perbedaan antara”connection-start-time“dan”connection-end-time“.

Untuk informasi selengkapnya tentang mengaktifkan catatan koneksi, lihat Bekerja dengan log koneksi.

Pertimbangan penskalaan Client VPN

Ketika membuat titik akhir Client VPN, pertimbangkan jumlah maksimum koneksi VPN serentak yang ingin Anda dukung. Anda harus mempertimbangkan jumlah klien yang saat ini didukung, dan apakah titik akhir Client VPN Anda dapat memenuhi permintaan tambahan jika diperlukan.

Faktor-faktor berikut memengaruhi jumlah maksimum koneksi VPN serentak yang dapat didukung di titik akhir Client VPN.

Ukuran rentang CIDR klien

Ketika Anda membuat titik akhir Client VPN, Anda harus menentukan rentang CIDR klien, yang merupakan blok CIDR IPv4 antara netmask /12 dan /22. Alamat IP yang unik dari rentang CIDR klien ditetapkan untuk setiap koneksi VPN ke titik akhir Client VPN. Sebagian alamat di rentang CIDR klien juga digunakan untuk mendukung model ketersediaan titik akhir Client VPN, dan tidak dapat ditetapkan untuk klien. Anda tidak dapat mengubah rentang CIDR klien setelah membuat titik akhir Client VPN.

Umumnya, kami merekomendasikan agar Anda menentukan rentang CIDR klien yang berisi dua kali jumlah alamat IP (dan juga koneksi serentak) yang ingin Anda dukung di titik akhir Client VPN.

Jumlah subnet terkait

Ketika Anda mengaitkan subnet dengan titik akhir Client VPN, Anda memungkinkan pengguna untuk membuat sesi VPN ke titik akhir Client VPN. Anda dapat mengaitkan beberapa subnet dengan titik akhir Client VPN untuk ketersediaan tinggi, dan untuk mengaktifkan kapasitas koneksi tambahan.

Berikut adalah jumlah koneksi VPN serentak yang didukung berdasarkan jumlah asosiasi subnet untuk titik akhir Client VPN.

Asosiasi subnet	Jumlah koneksi yang didukung
1	7.000
2	36.500
3	66.500
4	96.500
5	126.000

Anda tidak dapat mengaitkan beberapa subnet dari Availability Zone yang sama dengan titik akhir Client VPN. Oleh karena itu, jumlah asosiasi subnet juga tergantung pada jumlah Availability Zones yang tersedia di Wilayah AWS.

Misalnya, jika Anda ingin mendukung 8.000 koneksi VPN ke titik akhir Client VPN Anda, tentukan ukuran rentang CIDR klien minimum /18 (16.384 alamat IP), dan kaitkan setidaknya 2 subnet dengan titik akhir Client VPN.

Jika Anda tidak yakin berapa jumlah koneksi VPN yang diharapkan untuk titik akhir Client VPN Anda, kami merekomendasikan Anda untuk menentukan ukuran blok CIDR /16 atau lebih besar.

Untuk informasi selengkapnya tentang aturan dan batasan untuk bekerja dengan rentang CIDR klien dan target jaringan, lihat Aturan dan praktik terbaik AWS Client VPN.

Untuk informasi selengkapnya tentang kuota titik akhir Client VPN, lihat Kuota AWS Client VPN.

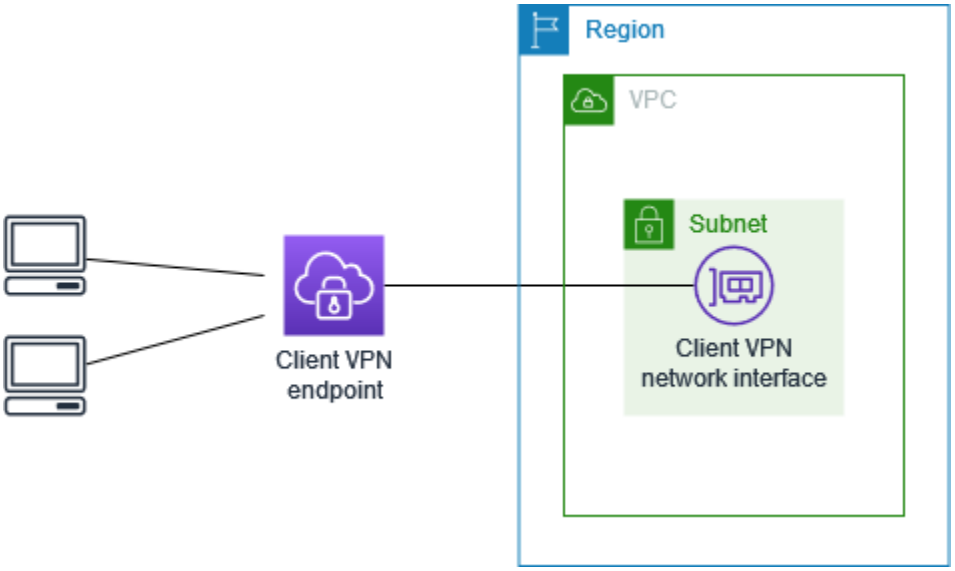
Skenario dan contoh untuk AWS Client VPN

Bagian ini memberikan contoh untuk membuat dan mengonfigurasi akses Client VPN untuk klien Anda.

Daftar Isi

Akses VPC menggunakan AWS Client VPN

Konfigurasi untuk skenario ini mencakup satu target VPC. Kami merekomendasikan konfigurasi ini jika Anda perlu memberikan akses klien ke sumber daya di dalam satu VPC saja.



Sebelum memulai, lakukan hal berikut:

- Buat atau identifikasi VPC dengan minimal satu subnet. Identifikasi subnet di VPC untuk dikaitkan dengan titik akhir Client VPN dan catat rentang IPv4 CIDR-nya.

- Identifikasi rentang CIDR yang cocok untuk alamat IP klien yang tidak tumpang tindih dengan VPC CIDR.
- Tinjau aturan dan batasan untuk titik akhir Client VPN di Aturan dan praktik terbaik AWS Client VPN.

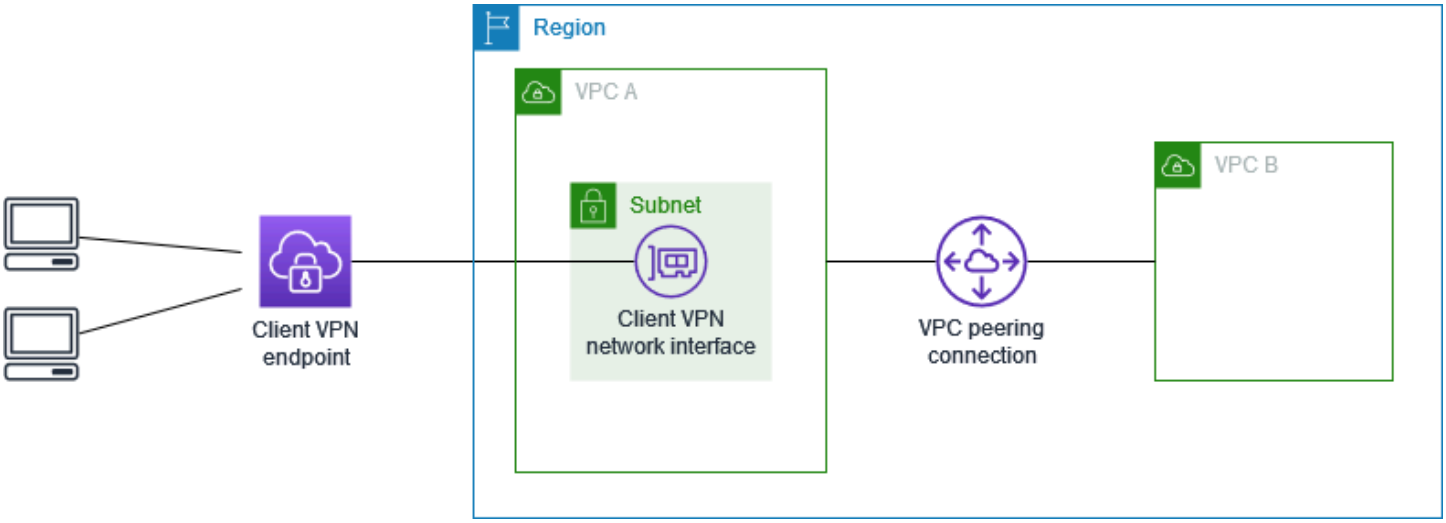
Untuk menerapkan konfigurasi ini

1. Buat titik akhir Client VPN di Wilayah yang sama dengan VPC. Caranya, lakukan langkah-langkah yang dijelaskan dalam Buat titik akhir Client VPN.
2. Kaitkan subnet dengan titik akhir Client VPN. Caranya, lakukan langkah-langkah yang dijelaskan dalam Mengaitkan jaringan target dengan titik akhir Client VPN dan pilih subnet dan VPC yang Anda identifikasi sebelumnya.
3. Tambahkan aturan otorisasi untuk memberikan akses klien ke VPC. Caranya, lakukan langkah-langkah yang dijelaskan dalam Tambahkan aturan otorisasi ke titik akhir Client VPN, dan untuk Jaringan tujuan, masukkan rentang CIDR IPv4 dari VPC.
4. Tambahkan aturan ke grup keamanan sumber daya Anda untuk mengizinkan lalu lintas dari grup keamanan yang diterapkan ke asosiasi subnet di langkah 2. Untuk informasi selengkapnya, lihat Grup keamanan.

Akses VPC AWS peered menggunakan Client VPN

Konfigurasi untuk skenario ini mencakup target VPC (VPC A) yang di-peering dengan VPC tambahan (VPC B). Kami merekomendasikan konfigurasi ini jika Anda perlu memberikan akses klien ke sumber daya dalam target VPC dan VPC lain yang di-peering dengan sumber daya tersebut (seperti VPC B).

> **Note**
>
> Prosedur untuk mengizinkan akses ke VPC peered yang diuraikan di bawah ini, hanya diperlukan jika titik akhir Client VPN dikonfigurasi untuk mode split-tunnel. Dalam mode full-tunnel, akses ke VPC peered diizinkan secara default.



Sebelum memulai, lakukan hal berikut:

- Buat atau identifikasi VPC dengan minimal satu subnet. Identifikasi subnet di VPC untuk dikaitkan dengan titik akhir Client VPN dan catat rentang IPv4 CIDR-nya.
- Identifikasi rentang CIDR yang cocok untuk alamat IP klien yang tidak tumpang tindih dengan VPC CIDR.
- Tinjau aturan dan batasan untuk titik akhir Client VPN di Aturan dan praktik terbaik AWS Client VPN.

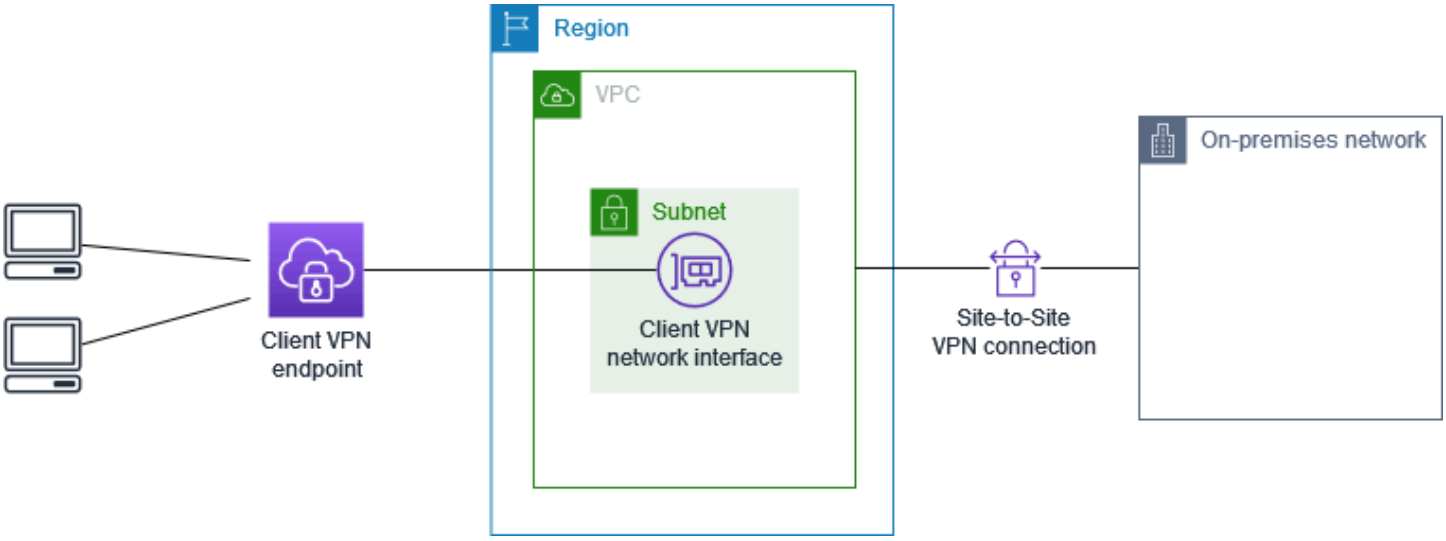
Untuk menerapkan konfigurasi ini

1. Buat koneksi peering VPC antara VPC. Ikuti langkah-langkah dalam Membuat dan menerima koneksi peering VPC di Panduan Amazon VPC Peering. Konfirmasikan bahwa instance di VPC A dapat berkomunikasi dengan instance di VPC B menggunakan koneksi peering.
2. Buat titik akhir Client VPN di Wilayah yang sama dengan target VPC. Dalam diagram, ini adalah VPC A. Lakukan langkah-langkah yang dijelaskan dalam. Buat titik akhir Client VPN
3. Kaitkan subnet yang Anda identifikasi dengan titik akhir Client VPN yang Anda buat. Untuk melakukan ini, lakukan langkah-langkah yang dijelaskan dalamMengaitkan jaringan target dengan titik akhir Client VPN, pilih VPC dan subnet. Secara default, kami mengaitkan grup keamanan default VPC dengan titik akhir Client VPN. Anda dapat mengaitkan grup keamanan yang berbeda menggunakan langkah-langkah yang dijelaskan dalamthe section called “Terapkan grup keamanan ke jaringan target”.

4. Tambahkan aturan otorisasi untuk memberikan akses klien ke target VPC. Caranya, lakukan langkah-langkah yang dijelaskan dalam Tambahkan aturan otorisasi ke titik akhir Client VPN. Untuk Jaringan tujuan yang akan diaktifkan , masukkan rentang CIDR IPv4 dari VPC.
5. Tambahkan rute untuk mengarahkan lalu lintas ke VPC yang di-peering. Dalam diagram, ini adalah VPC B. Untuk melakukan ini, lakukan langkah-langkah yang dijelaskan dalam. Membuat rute titik akhir Untuk tujuan Rute, masukkan rentang IPv4 CIDR dari VPC peered. Untuk ID Subnet VPC Target, pilih subnet yang Anda kaitkan dengan titik akhir Client VPN.
6. Tambahkan aturan otorisasi untuk memberikan akses klien ke VPC yang di-peering. Caranya, lakukan langkah-langkah yang dijelaskan dalam Tambahkan aturan otorisasi ke titik akhir Client VPN. Untuk jaringan Tujuan, masukkan rentang IPv4 CIDR dari VPC peered.
7. Tambahkan aturan ke grup keamanan untuk instans Anda di VPC A dan VPC B untuk mengizinkan lalu lintas dari grup keamanan yang diterapkan titik akhir Client VPN di langkah 3. Untuk informasi selengkapnya, lihat Grup keamanan.

Mengakses jaringan lokal menggunakan AWS Client VPN

Konfigurasi untuk skenario ini mencakup akses ke jaringan on-premise saja. Kami merekomendasikan konfigurasi ini jika Anda perlu memberikan akses klien ke sumber daya di dalam jaringan on-premise saja.



Sebelum memulai, lakukan hal berikut:

- Buat atau identifikasi VPC dengan minimal satu subnet. Identifikasi subnet di VPC untuk dikaitkan dengan titik akhir Client VPN dan catat rentang IPv4 CIDR-nya.

- Identifikasi rentang CIDR yang cocok untuk alamat IP klien yang tidak tumpang tindih dengan VPC CIDR.
- Tinjau aturan dan batasan untuk titik akhir Client VPN di Aturan dan praktik terbaik AWS Client VPN.

Untuk menerapkan konfigurasi ini

1. Aktifkan komunikasi antara VPC dan jaringan on-premise Anda sendiri melalui koneksi AWS Site-to-Site VPN. Caranya, lakukan langkah-langkah yang dijelaskan dalam Memulai di AWS Site-to-Site VPN Panduan Pengguna.

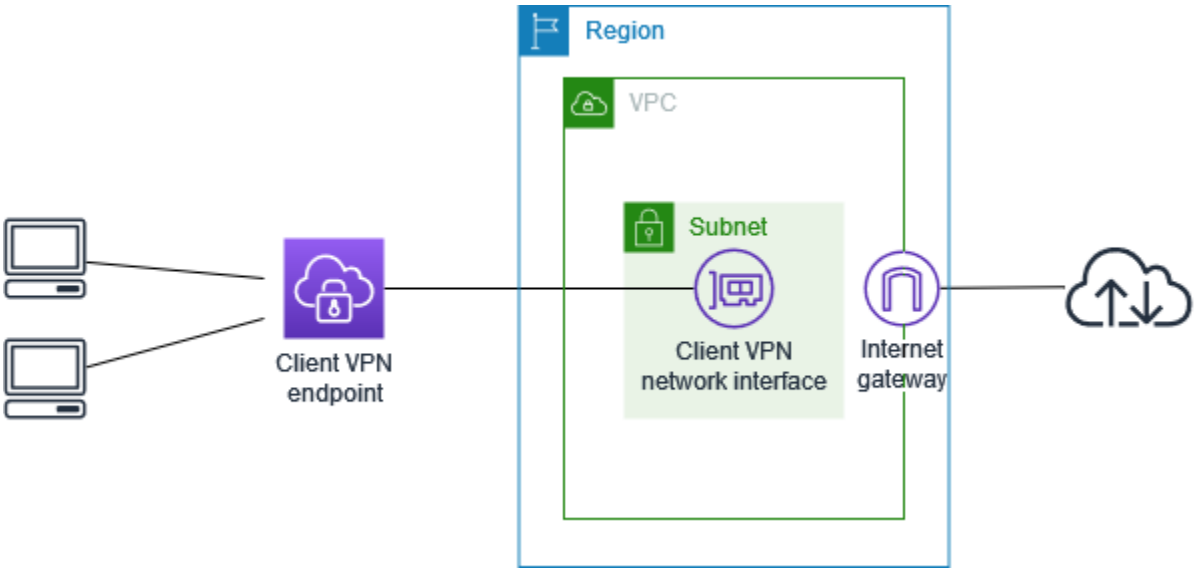
   > **Note**
   >
   > Atau, Anda dapat menerapkan skenario ini dengan menggunakan koneksi AWS Direct Connect antara VPC dan jaringan on-premise Anda. Untuk informasi selengkapnya, lihat AWS Direct Connect Panduan Pengguna.

2. Uji koneksi AWS Site-to-Site VPN yang Anda buat pada langkah sebelumnya. Caranya, lakukan langkah-langkah yang dijelaskan dalam Menguji koneksi Site-to-Site VPN di AWS Site-to-Site VPN Panduan Pengguna. Jika koneksi VPN berfungsi seperti yang diharapkan, lanjutkan ke langkah berikutnya.
3. Buat titik akhir Client VPN dalam Wilayah yang sama dengan VPC. Caranya, lakukan langkah-langkah yang dijelaskan dalam Buat titik akhir Client VPN.
4. Kaitkan subnet yang Anda identifikasi sebelumnya dengan titik akhir Client VPN. Caranya, lakukan langkah-langkah yang dijelaskan dalam Mengaitkan jaringan target dengan titik akhir Client VPN lalu pilih VPC dan subnet.
5. Tambahkan rute yang mengizinkan akses ke koneksi AWS Site-to-Site VPN. Caranya, lakukan langkah-langkah yang dijelaskan dalam Membuat rute titik akhir; untuk Tujuan rute, masukkan rentang CIDR IPv4 dari koneksi AWS Site-to-Site VPN, dan untuk ID Subnet VPC Target, pilih subnet yang Anda kaitkan dengan titik akhir Client VPN.
6. Tambahkan aturan otorisasi untuk memberikan akses klien ke koneksi AWS Site-to-Site VPN. Caranya, lakukan langkah-langkah yang dijelaskan dalam Tambahkan aturan otorisasi ke titik akhir Client VPN; untuk Jaringan tujuan, masukkan rentang CIDR IPv4 koneksi AWS Site-to-Site VPN.

Akses internet menggunakan AWS Client VPN

Konfigurasi untuk skenario ini mencakup satu target VPC dan akses ke internet. Kami merekomendasikan konfigurasi ini jika Anda perlu memberikan akses klien ke sumber daya di dalam satu target VPC dan mengizinkan akses ke internet.

Jika Anda menyelesaikan tutorial Memulai dengan AWS Client VPN, maka Anda sudah menerapkan skenario ini.



Sebelum memulai, lakukan hal berikut:

- Buat atau identifikasi VPC dengan minimal satu subnet. Identifikasi subnet di VPC untuk dikaitkan dengan titik akhir Client VPN dan catat rentang IPv4 CIDR-nya.
- Identifikasi rentang CIDR yang cocok untuk alamat IP klien yang tidak tumpang tindih dengan VPC CIDR.
- Tinjau aturan dan batasan untuk titik akhir Client VPN di Aturan dan praktik terbaik AWS Client VPN.

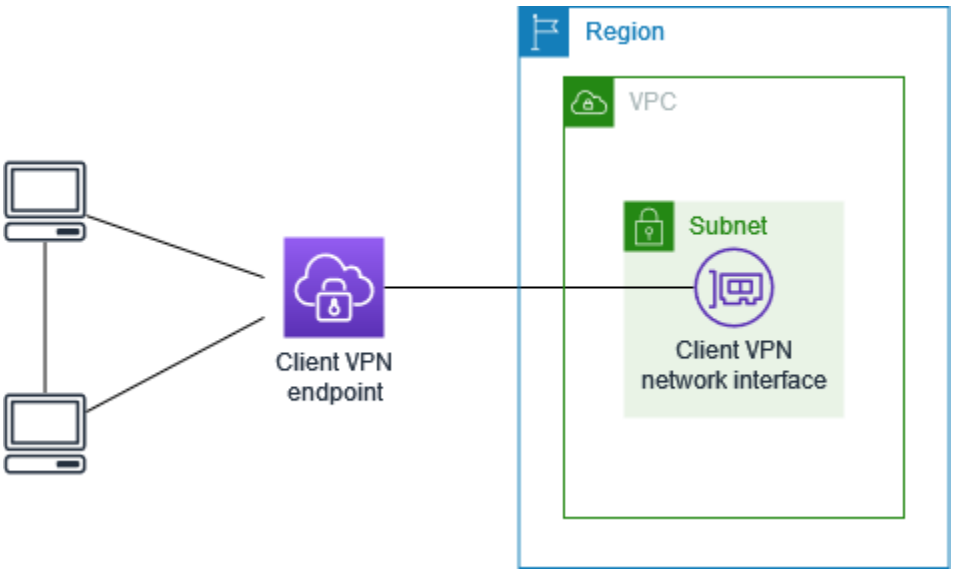
Untuk menerapkan konfigurasi ini

1. Pastikan grup keamanan yang akan Anda gunakan untuk titik akhir Client VPN memungkinkan lalu lintas keluar ke internet. Untuk melakukan ini, tambahkan aturan keluar yang memungkinkan lalu lintas ke 0.0.0.0/0 untuk lalu lintas HTTP dan HTTPS.
2. Buat gateway internet dan lampirkan ke VPC Anda. Untuk informasi selengkapnya, lihat Membuat dan melampirkan Gateway Internet di Panduan Pengguna Amazon VPC.

3. Buat subnet publik Anda dengan menambahkan rute ke gateway internet ke tabel rute. Dalam konsol VPC, pilih Subnet, pilih subnet yang ingin Anda kaitkan dengan titik akhir Client VPN, pilih Tabel Rute, dan kemudian pilih ID tabel rute. Pilih Tindakan, pilih Edit rute, dan pilih Tambahkan rute. Untuk Tujuan, masukkan `0.0.0.0/0`, dan untuk Target, pilih gateway internet dari langkah sebelumnya.
4. Buat titik akhir Client VPN di Wilayah yang sama dengan VPC. Caranya, lakukan langkah-langkah yang dijelaskan dalam Buat titik akhir Client VPN.
5. Kaitkan subnet yang Anda identifikasi sebelumnya dengan titik akhir Client VPN. Caranya, lakukan langkah-langkah yang dijelaskan dalam Mengaitkan jaringan target dengan titik akhir Client VPN lalu pilih VPC dan subnet.
6. Tambahkan aturan otorisasi untuk memberikan akses klien ke VPC. Caranya, lakukan langkah-langkah yang dijelaskan dalam Tambahkan aturan otorisasi ke titik akhir Client VPN; dan untuk Jaringan tujuan yang akan diaktifkan , masukkan rentang CIDR IPv4 dari VPC.
7. Tambahkan rute yang memungkinkan lalu lintas ke internet. Caranya, lakukan langkah-langkah yang dijelaskan dalam Membuat rute titik akhir; untuk Tujuan rute, masukkan `0.0.0.0/0`, dan untuk ID Subnet VPC Target, pilih subnet yang Anda kaitkan dengan titik akhir Client VPN.
8. Tambahkan aturan otorisasi untuk memberikan akses klien ke internet. Caranya, lakukan langkah-langkah yang dijelaskan dalam Tambahkan aturan otorisasi ke titik akhir Client VPN; untuk Jaringan tujuan, masukkan `0.0.0.0/0`.
9. Pastikan bahwa grup keamanan untuk sumber daya di VPC Anda memiliki aturan yang memungkinkan akses dari grup keamanan yang terkait dengan titik akhir Client VPN. Hal ini memungkinkan klien Anda untuk mengakses sumber daya di VPC Anda.

C lient-to-client akses menggunakan AWS Client VPN

Konfigurasi untuk skenario ini memungkinkan klien untuk mengakses VPC tunggal, dan memungkinkan klien untuk merutekan lalu lintas ke satu sama lain. Kami merekomendasikan konfigurasi ini jika klien yang terhubung ke titik akhir Client VPN yang sama juga perlu berkomunikasi satu sama lain. Klien dapat berkomunikasi satu sama lain menggunakan alamat IP unik yang ditetapkan untuk mereka dari rentang CIDR klien ketika mereka terhubung ke titik akhir Client VPN.



Sebelum memulai, lakukan hal berikut:

- Buat atau identifikasi VPC dengan minimal satu subnet. Identifikasi subnet di VPC untuk dikaitkan dengan titik akhir Client VPN dan catat rentang IPv4 CIDR-nya.
- Identifikasi rentang CIDR yang cocok untuk alamat IP klien yang tidak tumpang tindih dengan VPC CIDR.
- Tinjau aturan dan batasan untuk titik akhir Client VPN di Aturan dan praktik terbaik AWS Client VPN.

> **Note**
>
> Aturan otorisasi berbasis jaringan menggunakan grup Active Directory atau grup IDP berbasis SAML tidak didukung dalam skenario ini.

Untuk menerapkan konfigurasi ini

1. Buat titik akhir Client VPN di Wilayah yang sama dengan VPC. Caranya, lakukan langkah-langkah yang dijelaskan dalam Buat titik akhir Client VPN.
2. Kaitkan subnet yang Anda identifikasi sebelumnya dengan titik akhir Client VPN. Caranya, lakukan langkah-langkah yang dijelaskan dalam Mengaitkan jaringan target dengan titik akhir Client VPN lalu pilih VPC dan subnet.

3. Tambahkan rute ke jaringan lokal dalam tabel rute. Caranya, lakukan langkah-langkah yang dijelaskan dalam Membuat rute titik akhir. Untuk Tujuan rute, masukkan rentang CIDR klien, dan untuk ID Subnet VPC Target, tentukan `local`.
4. Tambahkan aturan otorisasi untuk memberikan akses klien ke VPC. Caranya, lakukan langkah-langkah yang dijelaskan dalam Tambahkan aturan otorisasi ke titik akhir Client VPN. Untuk Jaringan tujuan yang akan diaktifkan , masukkan rentang CIDR IPv4 dari VPC.
5. Tambahkan aturan otorisasi untuk memberikan akses klien ke rentang CIDR klien. Caranya, lakukan langkah-langkah yang dijelaskan dalam Tambahkan aturan otorisasi ke titik akhir Client VPN. Untuk Jaringan tujuan yang akan diaktifkan, masukkan rentang CIDR klien.

Batasi akses ke jaringan Anda menggunakan AWS Client VPN

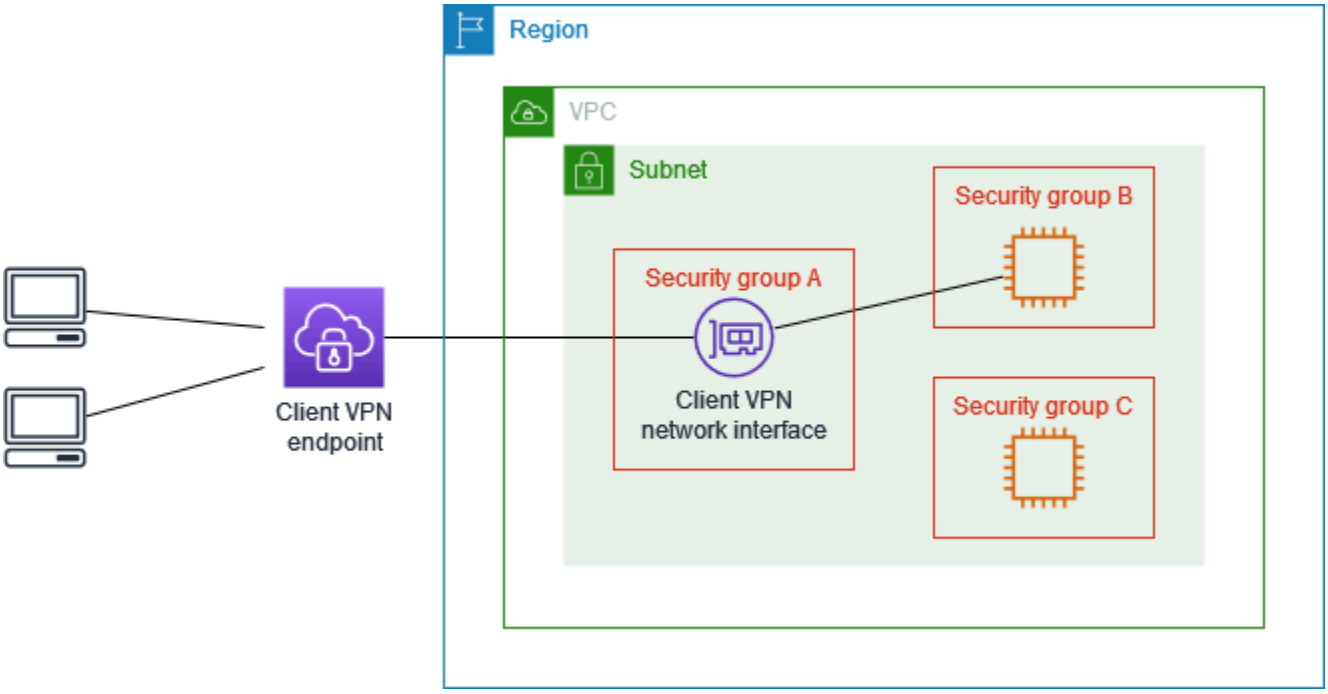
Anda dapat mengonfigurasi titik akhir Client VPN Anda untuk membatasi akses ke sumber daya tertentu di VPC Anda. Untuk autentikasi berbasis pengguna, Anda juga dapat membatasi akses ke bagian jaringan Anda, berdasarkan grup pengguna yang mengakses titik akhir Client VPN.

Membatasi akses menggunakan grup keamanan

Anda dapat memberikan atau menolak akses ke sumber daya tertentu di VPC Anda dengan menambahkan atau menghapus aturan grup keamanan yang mereferensikan grup keamanan yang diterapkan ke asosiasi jaringan target (grup keamanan Client VPN). Konfigurasi ini diperluas pada skenario yang dijelaskan dalam Akses VPC menggunakan AWS Client VPN. Konfigurasi ini diterapkan selain aturan otorisasi yang dikonfigurasi dalam skenario tersebut.

Untuk memberikan akses ke sumber daya tertentu, identifikasi grup keamanan yang terkait dengan instans di tempat sumber daya Anda berjalan. Kemudian, buat aturan yang mengizinkan lalu lintas dari grup keamanan Client VPN.

Dalam diagram berikut, grup keamanan A adalah grup keamanan Client VPN, grup keamanan B dikaitkan dengan instans EC2, dan grup keamanan C dikaitkan dengan instans EC2. Jika Anda menambahkan aturan ke grup keamanan B yang mengizinkan akses dari grup keamanan A, maka klien dapat mengakses instance yang terkait dengan grup keamanan B. Jika grup keamanan C tidak memiliki aturan yang mengizinkan akses dari grup keamanan A, maka klien tidak dapat mengakses instance yang terkait dengan grup keamanan C.



Sebelum memulai, periksa apakah grup keamanan Client VPN dikaitkan dengan sumber daya lain di VPC Anda. Jika Anda menambahkan atau menghapus aturan yang mereferensikan grup keamanan Client VPN, Anda juga dapat memberikan atau menolak akses untuk sumber daya terkait lainnya. Untuk mencegah hal ini, gunakan grup keamanan yang khusus dibuat untuk digunakan dengan titik akhir Client VPN Anda.

Untuk membuat aturan grup keamanan

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Grup Keamanan.
3. Pilih grup keamanan yang terkait dengan instans di tempat sumber daya Anda berjalan.
4. Pilih Tindakan, Edit aturan masuk.
5. Pilih Tambahkan aturan, lalu lakukan hal berikut:
   - Untuk Tipe, pilih Semua lalu lintas, atau tipe lalu lintas tertentu yang ingin Anda izinkan.
   - Untuk Sumber, pilih Kustom, dan kemudian masukkan atau pilih ID grup keamanan Client VPN.
6. Pilih Simpan aturan

Untuk menghapus akses ke sumber daya tertentu, periksa grup keamanan yang terkait dengan instans di tempat sumber daya Anda berjalan. Jika ada aturan yang mengizinkan lalu lintas dari grup keamanan Client VPN, hapus aturan tersebut.

Untuk memeriksa aturan grup keamanan Anda

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Grup Keamanan.
3. Pilih Aturan Masuk.
4. Tinjau daftar aturan. Jika ada aturan bahwa Sumber merupakan grup keamanan Client VPN, pilih Edit Aturan, dan pilih Hapus (ikon x) untuk aturan tersebut. Pilih Simpan aturan.

Membatasi akses berdasarkan grup pengguna

Jika titik akhir Client VPN Anda dikonfigurasi untuk autentikasi berbasis pengguna, Anda dapat memberikan grup pengguna tertentu akses ke bagian tertentu di jaringan Anda. Caranya, lakukan langkah-langkah berikut:

1. Konfigurasikan pengguna dan grup di AWS Directory Service atau IdP Anda. Untuk informasi selengkapnya, lihat topik berikut:
   - Autentikasi Direktori Aktif
   - Persyaratan dan pertimbangan untuk autentikasi federasi berbasis SAML
2. Buat aturan otorisasi untuk titik akhir Client VPN Anda yang mengizinkan akses grup tertentu ke semua atau sebagian jaringan Anda. Untuk informasi selengkapnya, lihat Aturan otorisasi.

Jika titik akhir Client VPN dikonfigurasi untuk autentikasi bersama, Anda tidak dapat mengonfigurasi grup pengguna. Saat membuat aturan otorisasi, Anda harus memberikan akses ke semua pengguna. Untuk mengaktifkan akses grup pengguna tertentu ke bagian jaringan tertentu, Anda dapat membuat beberapa titik akhir Client VPN. Misalnya, untuk setiap grup pengguna yang mengakses jaringan Anda, lakukan hal berikut:

1. Buat satu set sertifikat server dan klien serta kunci untuk grup pengguna tersebut. Untuk informasi selengkapnya, lihat Autentikasi bersama.
2. Buat titik akhir Client VPN. Untuk informasi selengkapnya, lihat Buat titik akhir Client VPN.
3. Buat aturan otorisasi yang memberikan akses ke semua atau sebagian jaringan Anda. Misalnya, untuk titik akhir Client VPN yang digunakan oleh administrator, Anda dapat membuat aturan

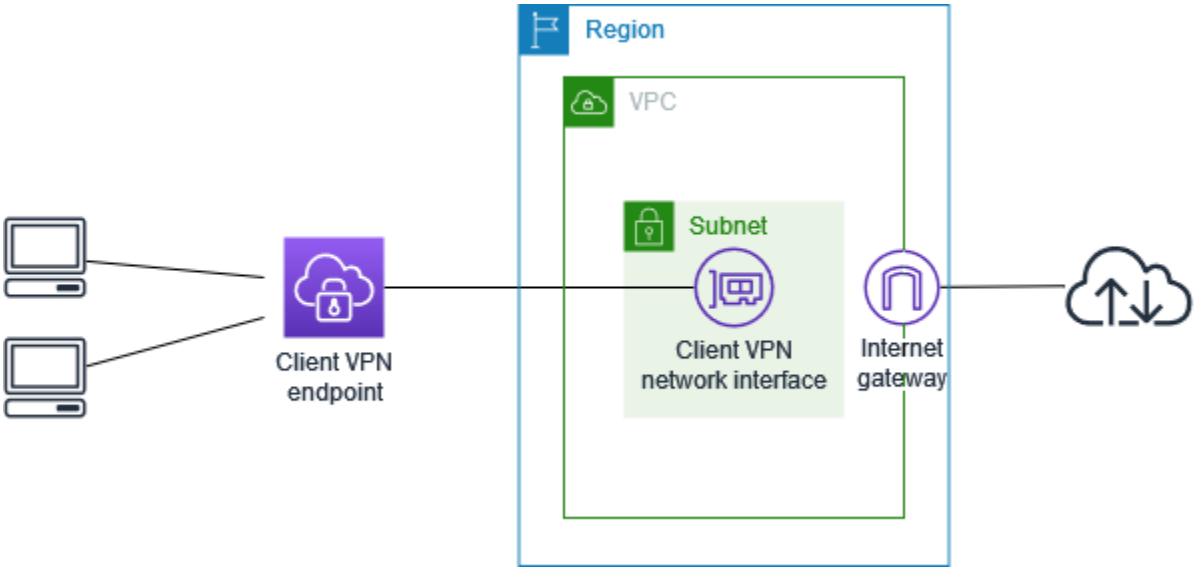
otorisasi yang memberikan akses ke seluruh jaringan. Untuk informasi selengkapnya, lihat Tambahkan aturan otorisasi ke titik akhir Client VPN.

Memulai dengan AWS Client VPN

Dalam tutorial ini Anda akan membuat endpoint Client VPN yang melakukan hal berikut:

- Menyediakan semua klien dengan akses ke satu VPC.
- Menyediakan semua klien dengan akses ke internet.
- Menggunakan autentikasi mutual.

Diagram berikut merupakan konfigurasi VPC dan titik akhir Client VPN setelah Anda menyelesaikan tutorial ini.



Langkah-langkah

- Prasyarat
- Langkah 1: Menghasilkan server, sertifikat klien, dan kunci
- Langkah 2: Buat titik akhir Client VPN
- Langkah 3: Kaitkan jaringan target
- Langkah 4: Tambahkan aturan otorisasi untuk VPC
- Langkah 5: Menyediakan akses ke internet
- Langkah 6: Verifikasi persyaratan grup keamanan
- Langkah 7: Unduh file konfigurasi titik akhir Client VPN
- Langkah 8: Connect ke endpoint Client VPN

Prasyarat

Sebelum Anda memulai tutorial memulai ini, pastikan Anda memiliki yang berikut:

- Izin yang diperlukan untuk bekerja dengan titik akhir Client VPN.
- Izin yang diperlukan untuk mengimpor sertifikat ke dalamAWS Certificate Manager.
- Sebuah VPC setidaknya dengan satu subnet dan gateway internet. Tabel rute yang terhubung dengan subnet Anda harus memiliki rute ke gateway internet.

Langkah 1: Menghasilkan server, sertifikat klien, dan kunci

Tutorial ini menggunakan autentikasi mutual. Dengan otentikasi timbal balik, Client VPN menggunakan sertifikat untuk melakukan otentikasi antara klien dan titik akhir Client VPN. Anda harus memiliki sertifikat dan kunci server, dan setidaknya satu sertifikat dan kunci klien. Minimal, sertifikat server harus diimpor ke AWS Certificate Manager (ACM) dan ditentukan saat Anda membuat titik akhir Client VPN. Mengimpor sertifikat klien ke ACM adalah opsional.

Jika Anda belum memiliki sertifikat untuk digunakan untuk tujuan ini, sertifikat tersebut dapat dibuat menggunakan utilitas easy-rsa OpenVPN. Untuk langkah-langkah mendetail untuk menghasilkan sertifikat dan kunci server dan klien menggunakan utilitas easy-rsa OpenVPN, dan mengimpornya ke ACM, lihat. Autentikasi bersama

> **Note**
>
> Sertifikat server harus disediakan dengan atau diimpor ke AWS Certificate Manager (ACM) di AWS Wilayah yang sama tempat Anda akan membuat titik akhir Client VPN.

Langkah 2: Buat titik akhir Client VPN

Titik akhir Client VPN adalah sumber daya yang Anda buat dan konfigurasikan untuk mengaktifkan dan mengelola sesi Client VPN. Ini adalah titik terminasi untuk semua sesi VPN klien.

Untuk membuat titik akhir Client VPN

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Endpoint Client VPN dan kemudian pilih Create Client VPN endpoint.

3. (Opsional) Berikan tag nama dan deskripsi untuk titik akhir Client VPN.
4. Untuk Client IPv4 CIDR, tentukan rentang alamat IP, dalam notasi CIDR, untuk menetapkan alamat IP klien.

   > **Note**
   >
   > Rentang alamat tidak dapat tumpang tindih dengan rentang alamat jaringan target, rentang alamat VPC, atau rute apa pun yang akan dikaitkan dengan titik akhir Client VPN. Rentang alamat klien harus minimal /22 dan tidak lebih besar dari/12 ukuran blok CIDR. Anda tidak dapat mengubah rentang alamat klien setelah Anda membuat titik akhir Client VPN.

5. Untuk ARN sertifikat Server, pilih ARN dari sertifikat server yang Anda buat di Langkah 1.
6. Di bawah Opsi otentikasi, pilih Gunakan otentikasi timbal balik, dan kemudian untuk ARN sertifikat klien, pilih ARN dari sertifikat yang ingin Anda gunakan sebagai sertifikat klien.

   Jika sertifikat server dan klien ditandatangani oleh otoritas sertifikat (CA) yang sama, Anda memiliki opsi untuk menentukan sertifikat server ARN untuk sertifikat klien dan server. Dalam skenario ini, sertifikat klien apa pun yang sesuai dengan sertifikat server dapat digunakan untuk mengautentikasi.
7. Simpan sisa pengaturan default, dan pilih Create Client VPN endpoint.

Setelah Anda membuat titik akhir Client VPN, statusnya adalah `pending-associate`. Klien hanya dapat membuat koneksi VPN setelah Anda mengaitkan setidaknya satu jaringan target.

Untuk informasi selengkapnya tentang opsi yang dapat Anda tentukan untuk titik akhir Client VPN, lihatBuat titik akhir Client VPN.

Langkah 3: Kaitkan jaringan target

Untuk memungkinkan klien membuat sesi VPN, Anda mengaitkan jaringan target dengan titik akhir Client VPN. Jaringan target adalah subnet dalam VPC.

Untuk mengaitkan jaringan target dengan titik akhir Client VPN

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Titik Akhir Client VPN.

3. Pilih titik akhir Client VPN yang Anda buat pada prosedur sebelumnya, lalu pilih Asosiasi jaringan target, Jaringan target asosiasi.
4. Untuk VPC, pilih VPC tempat subnet berada.
5. Untuk Pilih subnet untuk diasosiasikan, pilih subnet yang akan dikaitkan dengan titik akhir Client VPN.
6. Pilih Jaringan target asosiasi.
7. Jika aturan otorisasi mengizinkannya, satu asosiasi subnet cukup bagi klien untuk mengakses seluruh jaringan VPC. Anda dapat mengaitkan subnet tambahan untuk menyediakan ketersediaan tinggi jika Availability Zone menjadi terganggu.

Ketika Anda menghubungkan subnet pertama dengan titik akhir Client VPN, hal berikut ini akan terjadi:

- Status titik akhir Client VPN berubah menjadi `available`. Klien sekarang dapat membuat koneksi VPN, tetapi mereka tidak dapat mengakses sumber daya apa pun di VPC sampai Anda menambahkan aturan otorisasi.
- Rute lokal VPC secara otomatis ditambahkan ke tabel rute titik akhir Client VPN.
- Grup keamanan default VPC diterapkan secara otomatis untuk titik akhir Client VPN.

Langkah 4: Tambahkan aturan otorisasi untuk VPC

Agar klien dapat mengakses VPC, perlu ada rute ke VPC di tabel rute titik akhir Client VPN dan aturan otorisasi. Rute sudah ditambahkan secara otomatis pada langkah sebelumnya. Untuk tutorial ini, kami ingin memberikan semua pengguna akses ke VPC.

Untuk menambahkan aturan otorisasi untuk VPC

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Titik Akhir Client VPN.
3. Pilih titik akhir Client VPN untuk menambahkan aturan otorisasi. Pilih Aturan otorisasi, lalu pilih Tambahkan aturan otorisasi.
4. Agar jaringan Tujuan mengaktifkan akses, masukkan CIDR jaringan yang ingin Anda izinkan aksesnya. Sebagai contoh, untuk mengizinkan akses ke seluruh VPC, tentukan blok CIDR IPv4 dari VPC.

5. Untuk Memberikan akses ke, pilih Izinkan akses ke semua pengguna.
6. (Opsional) Untuk Deskripsi, masukkan deskripsi singkat tentang aturan otorisasi.
7. Pilih Tambahkan aturan otorisasi.

Langkah 5: Menyediakan akses ke internet

Anda dapat menyediakan akses ke jaringan tambahan yang terhubung ke VPC, seperti AWS layanan, VPC peered, jaringan lokal, dan internet. Untuk setiap jaringan tambahan, Anda menambahkan rute ke jaringan di tabel rute titik akhir Client VPN dan mengonfigurasi aturan otorisasi untuk memberikan akses kepada klien.

Untuk tutorial ini, kami ingin memberikan semua pengguna akses ke internet dan juga ke VPC. Anda telah mengonfigurasi akses ke VPC, jadi langkah ini adalah untuk akses ke internet.

Untuk menyediakan akses ke internet

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Titik Akhir Client VPN.
3. Pilih titik akhir Client VPN yang Anda buat untuk tutorial ini. Pilih Route Table, lalu pilih Create Route.
4. Untuk Tujuan rute, masukkan `0.0.0.0/0`. Untuk Subnet ID untuk asosiasi jaringan target, tentukan ID subnet yang digunakan untuk merutekan lalu lintas.
5. Pilih Buat Rute.
6. Pilih Aturan otorisasi, lalu pilih Tambahkan aturan otorisasi.
7. Untuk jaringan Tujuan untuk mengaktifkan akses, masukkan`0.0.0.0/0`, dan pilih Izinkan akses ke semua pengguna.
8. Pilih Tambahkan aturan otorisasi.

Langkah 6: Verifikasi persyaratan grup keamanan

Dalam tutorial ini, tidak ada grup keamanan yang ditentukan selama pembuatan titik akhir Client VPN di Langkah 2. Itu berarti bahwa grup keamanan default untuk VPC secara otomatis diterapkan ke titik akhir Client VPN ketika jaringan target dikaitkan. Akibatnya, grup keamanan default untuk VPC sekarang harus dikaitkan dengan titik akhir Client VPN.

Verifikasi persyaratan grup keamanan berikut

- Bahwa grup keamanan yang terkait dengan subnet yang Anda rutekan lalu lintas (dalam hal ini grup keamanan VPC default) memungkinkan lalu lintas keluar ke internet. Untuk melakukan ini, tambahkan aturan keluar yang memungkinkan semua lalu lintas ke tujuan`0.0.0.0/0`.
- Bahwa grup keamanan untuk sumber daya di VPC Anda memiliki aturan yang memungkinkan akses dari grup keamanan yang diterapkan ke titik akhir Client VPN (dalam hal ini grup keamanan VPC default). Hal ini memungkinkan klien Anda untuk mengakses sumber daya di VPC Anda.

Untuk informasi selengkapnya, lihat Grup keamanan.

Langkah 7: Unduh file konfigurasi titik akhir Client VPN

Langkah selanjutnya adalah mengunduh dan menyiapkan file konfigurasi titik akhir Client VPN. File konfigurasi mencakup detail titik akhir Client VPN dan informasi sertifikat yang diperlukan untuk membuat koneksi VPN. Anda memberikan file ini kepada pengguna akhir yang perlu terhubung ke titik akhir Client VPN. Pengguna akhir menggunakan file untuk mengkonfigurasi aplikasi klien VPN mereka.

Untuk mengunduh dan menyiapkan file konfigurasi titik akhir Client VPN

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Titik Akhir Client VPN.
3. Pilih endpoint Client VPN yang Anda buat untuk tutorial ini, dan pilih Unduh konfigurasi klien.
4. Cari sertifikat klien dan kunci yang dibuat pada Langkah 1. Sertifikat dan kunci klien dapat ditemukan di lokasi berikut di repo easy-rsa OpenVPN yang dikloning:
   - Sertifikat klien — `easy-rsa/easyrsa3/pki/issued/client1.domain.tld.crt`
   - Kunci klien — `easy-rsa/easyrsa3/pki/private/client1.domain.tld.key`
5. Buka file konfigurasi titik akhir Client VPN yang menggunakan teks editor pilihan Anda. Tambahkan `<cert> </cert>` dan `<key> </key>` tag ke file. Tempatkan isi sertifikat klien dan isi kunci pribadi di antara tag yang sesuai, seperti:

```
<cert>
Contents of client certificate (.crt) file
</cert>
```

```
<key>
Contents of private key (.key) file
</key>
```

6. Simpan dan tutup file konfigurasi titik akhir Client VPN.
7. Distribusikan file konfigurasi titik akhir Client VPN ke pengguna akhir Anda.

Untuk informasi selengkapnya tentang file konfigurasi titik akhir Client VPN, lihat Ekspor dan konfigurasikan file konfigurasi untuk klien.

Langkah 8: Connect ke endpoint Client VPN

Anda dapat terhubung ke titik akhir Client VPN menggunakan klien yang AWS disediakan atau aplikasi klien berbasis OpenVPN lainnya dan file konfigurasi yang baru saja Anda buat. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS Client VPN.

Bekerja denganAWSClient VPN

Topik berikut menjelaskan cara bekerja dengan Client VPN.

Konten

Mengakses portal layanan mandiri

Jika Anda mengaktifkan portal layanan mandiri untuk titik akhir Client VPN, Anda dapat menyediakan URL portal layanan mandiri untuk klien Anda. Klien dapat mengakses portal di peramban web, dan menggunakan kredensial berbasis pengguna untuk log in. Saat di portal, klien dapat mengunduh file konfigurasi titik akhir Client VPN dan mengunduh versi terbaru dari klien AWS yang telah disediakan.

Aturan berikut berlaku:

- Portal layanan mandiri ini tidak tersedia untuk klien yang mengautentikasi menggunakan autentikasi bersama.
- File konfigurasi yang tersedia di portal layanan mandiri adalah file konfigurasi yang sama yang Anda ekspor menggunakan konsol Amazon VPC atau AWS CLI. Jika Anda perlu menyesuaikan file konfigurasi sebelum mendistribusikan ke klien, Anda harus mendistribusikan sendiri file yang telah disesuaikan kepada klien.

- Anda harus mengaktifkan opsi portal layanan mandiri untuk titik akhir Client VPN Anda, atau klien tidak dapat mengakses portal. Jika opsi ini tidak diaktifkan, Anda dapat mengubah titik akhir Client VPN Anda untuk mengaktifkannya.

Setelah Anda mengaktifkan opsi portal layanan mandiri, berikan salah satu URL berikut ini kepada klien Anda:

- `https://self-service.clientvpn.amazonaws.com/`

  Jika klien mengakses portal menggunakan URL ini, mereka harus memasukkan ID titik akhir Client VPN sebelum dapat log in.
- `https://self-service.clientvpn.amazonaws.com/endpoints/<endpoint-id>`

  Ganti *<endpoint-id>* di URL sebelumnya dengan ID titik akhir Client VPN Anda, misalnya, `cvpn-endpoint-0123456abcd123456`.

Anda juga dapat melihat URL untuk portal swalayan di output describe-client-vpn-endpointsAWS CLIperintah. Atau, URL tersedia di tab Detail pada halaman Titik Akhir Client VPN di konsol VPC Amazon.

Untuk informasi selengkapnya tentang konfigurasi portal layanan mandiri untuk digunakan dengan autentikasi gabungan, lihat Dukungan untuk portal layanan mandiri.

Aturan otorisasi

Aturan otorisasi bertindak sebagai aturan firewall yang memberikan akses ke jaringan. Dengan menambahkan aturan otorisasi, Anda memberikan klien tertentu akses ke jaringan yang ditentukan. Anda harus memiliki aturan otorisasi untuk setiap jaringan yang ingin Anda akses. Anda dapat menambahkan aturan otorisasi ke titik akhir Client VPN menggunakan konsol dan AWS CLI.

> **Note**
>
> Client VPN menggunakan pencocokan awalan terpanjang saat mengevaluasi aturan otorisasi. Lihat topik pemecahan masalah Aturan otorisasi untuk grup Direktori Aktif tidak berfungsi seperti yang diharapkan dan Prioritas rute di Panduan Pengguna Amazon VPC untuk detail selengkapnya.

Daftar Isi

Tambahkan aturan otorisasi ke titik akhir Client VPN

Untuk menambahkan aturan otorisasi ke titik akhir Client VPN menggunakan AWS Management Console

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Titik Akhir Client VPN.
3. Pilih titik akhir Client VPN untuk menambahkan aturan otorisasi, pilih Aturan otorisasi, dan pilih Tambahkan aturan otorisasi.
4. Untuk jaringan Tujuan untuk mengaktifkan akses, masukkan alamat IP, dalam notasi CIDR, dari jaringan yang Anda ingin pengguna akses (misalnya, blok CIDR VPC Anda).
5. Tentukan klien mana yang diizinkan untuk mengakses jaringan yang ditentukan. Untuk Untuk memberikan akses, lakukan salah satu langkah berikut:

   - Untuk memberikan akses ke semua klien, pilih Izinkan akses ke semua pengguna.
   - Untuk membatasi akses ke klien tertentu, pilih Mengizinkan akses ke pengguna dalam grup tertentu, dan kemudian untuk akses ID grup, masukkan ID untuk grup yang akan diberi akses. Sebagai contoh, pengidentifikasi keamanan (SID) grup Direktori Aktif, atau ID/nama grup yang didefinisikan dalam penyedia identitas berbasis SAML (IdP).
     - (Direktori Aktif) Untuk mendapatkan SID, Anda dapat menggunakan Microsoft Powershell Get-ADGroup cmdlet, misalnya:

       ```
       Get-ADGroup -Filter 'Name -eq "<Name of the AD Group>"'
       ```

       Sebagai alternatif, buka alat Pengguna dan Komputer Direktori Aktif, lihat properti untuk grup, buka tab Atribut Editor, dan dapatkan nilai untuk `objectSID`. Jika perlu, pilih dulu Tampilan, Fitur lanjutan untuk mengaktifkan tab Atribut Editor.
     - (autentikasi gabungan berbasis SAML) Grup ID/nama harus sesuai dengan informasi atribut grup yang dikembalikan dalam pernyataan SAML.

6. Untuk Deskripsi, masukkan deskripsi singkat aturan otorisasi.
7. Pilih Tambahkan aturan otorisasi.

Untuk menambahkan aturan otorisasi ke titik akhir Client VPN (AWS CLI)

Gunakan perintah authorize-client-vpn-ingress.

Menghapus aturan otorisasi dari titik akhir Client VPN

Dengan menghapus aturan otorisasi, Anda menghapus akses ke jaringan yang ditentukan.

Anda dapat menghapus aturan otorisasi dari titik akhir Client VPN menggunakan konsol dan AWS CLI.

Untuk menghapus aturan otorisasi dari titik akhir Client VPN (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Titik Akhir Client VPN.
3. Pilih titik akhir Client VPN yang ditambahkan aturan otorisasi dan pilih Aturan otorisasi.
4. Pilih aturan otorisasi yang akan dihapus, pilih Hapus aturan otorisasi, dan pilih Hapus aturan otorisasi.

Untuk menghapus aturan otorisasi dari titik akhir Client VPN (AWS CLI)

Gunakan perintah revoke-client-vpn-ingress.

Melihat aturan otorisasi

Anda dapat melihat aturan otorisasi untuk titik akhir Client VPN tertentu menggunakan konsol dan AWS CLI.

Untuk melihat aturan otorisasi (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/..
2. Pada panel navigasi, pilih Titik Akhir Client VPN.
3. Pilih titik akhir Client VPN untuk melihat aturan otorisasi dan pilih Aturan otorisasi.

Untuk melihat aturan otorisasi (AWS CLI)

Gunakan perintah describe-client-vpn-authorization-rules.

Contoh skenario untuk aturan otorisasi

Bagian ini menjelaskan cara kerja aturan otorisasi. AWS Client VPN Ini mencakup poin-poin penting untuk memahami aturan otorisasi, arsitektur contoh, dan diskusi skenario contoh yang memetakan ke arsitektur contoh.

Daftar Isi

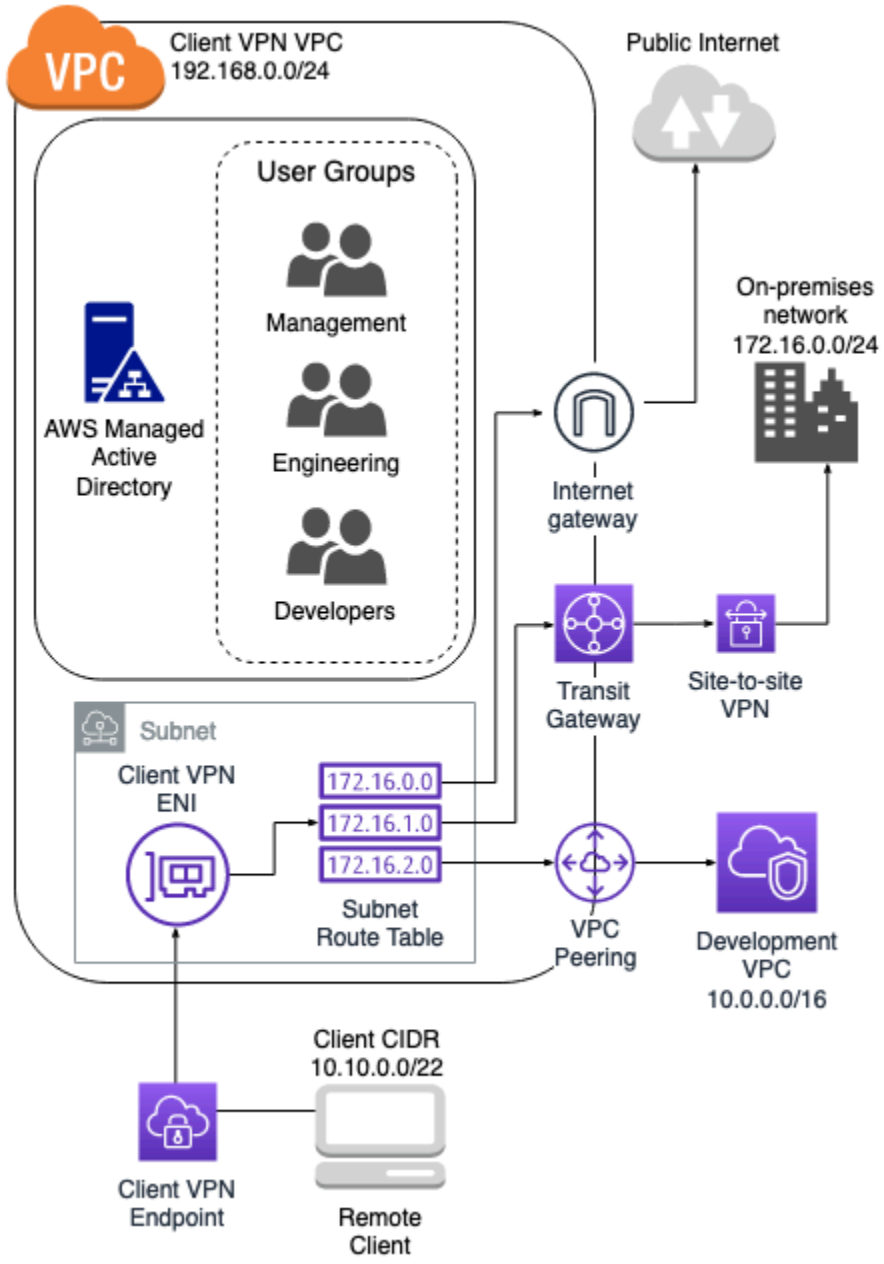
Poin penting untuk memahami aturan otorisasi

Poin-poin berikut menjelaskan beberapa perilaku aturan otorisasi:

- Untuk mengizinkan akses ke jaringan tujuan, aturan otorisasi harus ditambahkan secara eksplisit. Perilaku default adalah menolak akses.
- Anda tidak dapat menambahkan aturan otorisasi untuk membatasi akses ke jaringan tujuan.
- `0.0.0.0/0`CIDR ditangani sebagai kasus khusus. Ini diproses terakhir, terlepas dari urutan aturan otorisasi dibuat.
- `0.0.0.0/0`CIDR dapat dianggap sebagai “tujuan apa pun,” atau “tujuan apa pun yang tidak ditentukan oleh aturan otorisasi lainnya.”
- Pencocokan awalan terpanjang adalah aturan yang diutamakan.

Contoh arsitektur untuk skenario aturan otorisasi

Diagram berikut menunjukkan contoh arsitektur yang digunakan untuk skenario contoh yang ditemukan di bagian ini.



Skenario 1: Akses ke satu tujuan

Deskripsi aturan	ID Grup	Izinkan akses ke semua pengguna	Tujuan CIDR

Deskripsi aturan	ID Grup	Izinkan akses ke semua pengguna	Tujuan CIDR
Menyediakan akses grup teknik ke jaringan lokal	S-XXXXX14	Salah	172.16.0.0/24
Memberikan akses grup pengembangan ke VPC pengemban gan	S-xxxxx15	Salah	10.0.0.0/16
Berikan akses grup manajer ke Client VPN VPC	S-XXXXX16	Salah	192.168.0.0/24

Perilaku yang dihasilkan

- Kelompok teknik hanya dapat mengakses`172.16.0.0/24`.
- Grup pengembangan hanya dapat mengakses`10.0.0.0/16`.
- Grup manajer hanya dapat mengakses`192.168.0.0/24`.
- Semua lalu lintas lainnya dijatuhkan oleh titik akhir Client VPN.

> **Note**
>
> Dalam skenario ini, tidak ada grup pengguna yang memiliki akses ke internet publik.

Skenario 2: Menggunakan tujuan apa pun (0.0.0.0/0) CIDR

Deskripsi aturan	ID Grup	Izinkan akses ke semua pengguna	Tujuan CIDR
	S-XXXXX14	Salah	172.16.0.0/24

Deskripsi aturan	ID Grup	Izinkan akses ke semua pengguna	Tujuan CIDR
Menyediakan akses grup teknik ke jaringan lokal			
Memberikan akses grup pengembangan ke VPC pengemban gan	S-xxxxx15	Salah	10.0.0.0/16
Berikan akses grup manajer ke tujuan apa pun	S-XXXXX16	Salah	0.0.0.0/0

Perilaku yang dihasilkan

- Kelompok teknik hanya dapat mengakses`172.16.0.0/24`.
- Grup pengembangan hanya dapat mengakses`10.0.0.0/16`.
- Grup manajer dapat mengakses internet publik dan`192.168.0.0/24`, tetapi tidak dapat mengakses `172.16.0.0/24` atau`10.0.0.0/16`.

> **Note**
>
> Dalam skenario ini, karena tidak ada aturan yang merujuk`192.168.0.0/24`, akses ke jaringan itu juga disediakan oleh `0.0.0.0/0` aturan.
> Aturan yang mengandung selalu `0.0.0.0/0` dievaluasi terakhir terlepas dari urutan di mana aturan dibuat. Karena itu, perlu diingat bahwa aturan yang dievaluasi sebelumnya `0.0.0.0/0` berperan dalam menentukan jaringan mana yang `0.0.0.0/0` memberikan akses.

Skenario 3: Pencocokan awalan IP yang lebih panjang

Deskripsi aturan	ID Grup	Izinkan akses ke semua pengguna	Tujuan CIDR
Menyediakan akses grup teknik ke jaringan lokal	S-XXXXX14	Salah	172.16.0.0/24
Memberikan akses grup pengembangan ke VPC pengemban gan	S-xxxxx15	Salah	10.0.0.0/16
Berikan akses grup manajer ke tujuan apa pun	S-XXXXX16	Salah	0.0.0.0/0
Menyediakan akses grup manajer ke satu host dalam pengembangan VPC	S-XXXXX16	Salah	10.0.2.119/32

Perilaku yang dihasilkan

- Kelompok teknik hanya dapat mengakses`172.16.0.0/24`.
- Grup pengembangan dapat mengakses`10.0.0.0/16`, kecuali untuk host tunggal`10.0.2.119/32`.
- Grup manajer dapat mengakses internet publik,`192.168.0.0/24`, dan satu host (`10.0.2.119/32`) dalam VPC pengembangan, tetapi tidak memiliki akses ke `172.16.0.0/24` atau salah satu host yang tersisa dalam VPC pengembangan.

> **Note**
>
> Di sini Anda melihat bagaimana aturan dengan awalan IP yang lebih panjang lebih diutamakan daripada aturan dengan awalan IP yang lebih pendek. Jika Anda ingin grup pengembangan memiliki akses`10.0.2.119/32`, aturan tambahan yang memberikan akses kepada tim pengembangan `10.0.2.119/32` perlu ditambahkan.

Skenario 4: CIDR yang tumpang tindih (grup yang sama)

Deskripsi aturan	ID Grup	Izinkan akses ke semua pengguna	Tujuan CIDR
Menyediakan akses grup teknik ke jaringan lokal	S-XXXXX14	Salah	172.16.0.0/24
Memberikan akses grup pengembangan ke VPC pengemban gan	S-xxxxx15	Salah	10.0.0.0/16
Berikan akses grup manajer ke tujuan apa pun	S-XXXXX16	Salah	0.0.0.0/0
Menyediakan akses grup manajer ke host tunggal dalam pengembangan VPC	S-XXXXX16	Salah	10.0.2.119/32
Menyediakan akses grup teknik ke subnet	S-XXXXX14	Salah	172.16.0.128/25

Deskripsi aturan	ID Grup	Izinkan akses ke semua pengguna	Tujuan CIDR
yang lebih kecil dalam jaringan lokal			

Perilaku yang dihasilkan

- Grup pengembangan dapat mengakses`10.0.0.0/16`, kecuali untuk host tunggal`10.0.2.119/32`.
- Grup manajer dapat mengakses internet publik,`192.168.0.0/24`, dan satu host (`10.0.2.119/32`) dalam `10.0.0.0/16` jaringan, tetapi tidak memiliki akses ke `172.16.0.0/24` atau salah satu host yang tersisa di `10.0.0.0/16` jaringan.
- Kelompok teknik memiliki akses ke`172.16.0.0/24`, termasuk subnet `172.16.0.128/25` yang lebih spesifik.

Skenario 5: Aturan tambahan 0.0.0.0/0

Deskripsi aturan	ID Grup	Izinkan akses ke semua pengguna	Tujuan CIDR
Menyediakan akses grup teknik ke jaringan lokal	S-XXXXX14	Salah	172.16.0.0/24
Memberikan akses grup pengembangan ke VPC pengemban gan	S-xxxxx15	Salah	10.0.0.0/16
Berikan akses grup manajer ke tujuan apa pun	S-XXXXX16	Salah	0.0.0.0/0

Deskripsi aturan	ID Grup	Izinkan akses ke semua pengguna	Tujuan CIDR
Menyediakan akses grup manajer ke host tunggal dalam pengembangan VPC	S-XXXXX16	Salah	10.0.2.119/32
Menyediakan akses grup teknik ke subnet yang lebih kecil dalam jaringan lokal	S-XXXXX14	Salah	172.16.0.128/25
Menyediakan akses grup teknik ke tujuan apa pun	S-XXXXX14	Salah	0.0.0.0/0

Perilaku yang dihasilkan

- Grup pengembangan dapat mengakses`10.0.0.0/16`, kecuali untuk host tunggal`10.0.2.119/32`.
- Grup manajer dapat mengakses internet publik,`192.168.0.0/24`, dan satu host (`10.0.2.119/32`) dalam `10.0.0.0/16` jaringan, tetapi tidak memiliki akses ke `172.16.0.0/24` atau salah satu host yang tersisa di `10.0.0.0/16` jaringan.
- Kelompok teknik dapat mengakses internet publik,, dan `192.168.0.0/24``172.16.0.0/24`, termasuk subnet `172.16.0.128/25` yang lebih spesifik.

> **Note**
>
> Perhatikan bahwa kelompok teknik dan manajer sekarang dapat mengakses`192.168.0.0/24`. Ini karena kedua grup memiliki akses ke `0.0.0.0/0` (tujuan apa pun) dan tidak ada aturan lain yang merujuk`192.168.0.0/24`.

Skenario 6: Menambahkan aturan untuk 192.168.0.0/24

Deskripsi aturan	ID Grup	Izinkan akses ke semua pengguna	Tujuan CIDR
Menyediakan akses grup teknik ke jaringan lokal	S-XXXXX14	Salah	172.16.0.0/24
Memberikan akses grup pengembangan ke VPC pengemban gan	S-xxxxx15	Salah	10.0.0.0/16
Berikan akses grup manajer ke tujuan apa pun	S-XXXXX16	Salah	0.0.0.0/0
Menyediakan akses grup manajer ke host tunggal dalam pengembangan VPC	S-XXXXX16	Salah	10.0.2.119/32
Menyediakan akses grup teknik ke subnet di jaringan lokal	S-XXXXX14	Salah	172.16.0.128/25
Menyediakan akses grup teknik ke tujuan apa pun	S-XXXXX14	Salah	0.0.0.0/0
	S-XXXXX16	Salah	192.168.0.0/24

Deskripsi aturan	ID Grup	Izinkan akses ke semua pengguna	Tujuan CIDR
Berikan akses grup manajer ke Client VPN VPC			

Perilaku yang dihasilkan

- Grup pengembangan dapat mengakses`10.0.0.0/16`, kecuali untuk host tunggal`10.0.2.119/32`.
- Grup manajer dapat mengakses internet publik,`192.168.0.0/24`, dan satu host (`10.0.2.119/32`) dalam `10.0.0.0/16` jaringan, tetapi tidak memiliki akses ke `172.16.0.0/24` atau salah satu host yang tersisa di `10.0.0.0/16` jaringan.
- Kelompok teknik dapat mengakses internet publik,`172.16.0.0/24`, dan`172.16.0.128/25`.

> **Note**
>
> Perhatikan bagaimana menambahkan aturan untuk grup pengelola untuk mengakses `192.168.0.0/24` hasil dalam grup pengembangan tidak lagi memiliki akses ke jaringan tujuan tersebut.

Skenario 7: Akses untuk semua grup pengguna

Deskripsi aturan	ID Grup	Izinkan akses ke semua pengguna	Tujuan CIDR
Menyediakan akses grup teknik ke jaringan lokal	S-XXXXX14	Salah	172.16.0.0/24
Memberikan akses grup pengembangan	S-xxxxx15	Salah	10.0.0.0/16

Deskripsi aturan	ID Grup	Izinkan akses ke semua pengguna	Tujuan CIDR
ke VPC pengemban gan			
Berikan akses grup manajer ke tujuan apa pun	S-XXXXX16	Salah	0.0.0.0/0
Menyediakan akses grup manajer ke host tunggal dalam pengembangan VPC	S-XXXXX16	Salah	10.0.2.119/32
Menyediakan akses grup teknik ke subnet di jaringan lokal	S-XXXXX14	Salah	172.16.0.128/25
Menyediakan akses grup teknik ke semua jaringan	S-XXXXX14	Salah	0.0.0.0/0
Berikan akses grup manajer ke Client VPN VPC	S-XXXXX16	Salah	192.168.0.0/24
Menyediakan akses ke semua grup	T/A	Benar	0.0.0.0/0

Perilaku yang dihasilkan

- Grup pengembangan dapat mengakses`10.0.0.0/16`, kecuali untuk host tunggal`10.0.2.119/32`.

- Grup manajer dapat mengakses internet publik,`192.168.0.0/24`, dan satu host (`10.0.2.119/32`) dalam `10.0.0.0/16` jaringan, tetapi tidak memiliki akses ke `172.16.0.0/24` atau salah satu host yang tersisa di `10.0.0.0/16` jaringan.
- Kelompok teknik dapat mengakses internet publik,`172.16.0.0/24`, dan`172.16.0.128/25`.
- Grup pengguna lain, misalnya “grup admin,” dapat mengakses internet publik, tetapi tidak ada jaringan tujuan lain yang ditentukan dalam aturan lain.

Daftar pencabutan sertifikat klien

Anda dapat menggunakan daftar pencabutan sertifikat klien untuk mencabut akses ke titik akhir Client VPN untuk sertifikat klien tertentu.

> **Note**
>
> Untuk informasi selengkapnya tentang membuat sertifikat server dan klien dan kunci, lihat Autentikasi bersama

Untuk informasi selengkapnya tentang jumlah entri yang dapat Anda tambahkan ke daftar pencabutan sertifikat klien, lihat Kuota Client VPN.

Daftar Isi

Buat daftar pencabutan sertifikat klien

Linux/macOS

Dalam prosedur berikut, Anda membuat daftar pencabutan sertifikat klien menggunakan utilitas baris perintah OpenVPN easy-rsa.

Untuk membuat daftar pencabutan sertifikat klien menggunakan OpenVPN easy-rsa

1. Logon ke server hosting instalasi easyrsa yang digunakan untuk menghasilkan sertifikat.
2. Navigasikan ke folder `easy-rsa/easyrsa3` di repo lokal Anda.

```
$ cd easy-rsa/easyrsa3
```

3. Cabut sertifikat klien dan buat daftar pencabutan klien.

```
$ ./easyrsa revoke client1.domain.tld
$ ./easyrsa gen-crl
```

Ketik `yes` saat diminta.

Windows

Prosedur berikut menggunakan perangkat lunak OpenVPN untuk membuat daftar pencabutan klien. Ini mengasumsikan bahwa Anda mengikuti langkah-langkah untuk menggunakan perangkat lunak OpenVPN untuk membuat sertifikat klien dan server dan kunci.

Untuk menghasilkan daftar pencabutan sertifikat klien menggunakan EasyRSA versi 3.xx

1. Buka prompt perintah dan arahkan ke direktori EasyRSA-3.x.x, yang akan tergantung di mana ia diinstal pada sistem Anda.

```
C:\> cd c:\Users\windows\EasyRSA-3.x.x
```

2. Jalankan file "EasyRSA-Start.bat" untuk memulai shell EasyRSA.

```
C:\> .\EasyRSA-Start.bat
```

3. Di shell EasyRSA, cabut sertifikat klien.

```
# ./easyrsa revoke client_certificate_name
```

4. Ketik “ya” saat diminta.
5. Hasilkan daftar pencabutan klien.

```
# ./easyrsa gen-crl
```

6. Daftar pencabutan klien akan dibuat di lokasi berikut:

```
c:\Users\windows\EasyRSA-3.x.x\pki\crl.pem
```

Untuk menghasilkan daftar pencabutan sertifikat klien menggunakan versi EasyRSA sebelumnya

1. Buka prompt perintah dan navigasikan ke direktori OpenVPN.

```
C:\> cd \Program Files\OpenVPN\easy-rsa
```

2. Jalankan file `vars.bat`.

```
C:\> vars
```

3. Cabut sertifikat klien dan buat daftar pencabutan klien.

```
C:\> revoke-full client_certificate_name
C:\> more crl.pem
```

Impor daftar pencabutan sertifikat klien

Anda harus memiliki file daftar pencabutan sertifikat klien untuk mengimpor. Untuk informasi selengkapnya tentang membuat daftar pencabutan sertifikat klien, lihat Buat daftar pencabutan sertifikat klien.

Anda dapat mengimpor daftar pencabutan sertifikat klien menggunakan konsol dan AWS CLI.

Untuk mengimpor daftar pencabutan sertifikat klien (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir Client VPN.
3. Pilih titik akhir Client VPN untuk mengimpor daftar pencabutan sertifikat klien.
4. Pilih Tindakan, dan pilih Impor Sertifikat Klien CRL.
5. Untuk Daftar Pencabutan Sertifikat, masukkan isi file daftar pencabutan sertifikat klien, dan pilih Impor sertifikat klien CRL.

Untuk mengimpor daftar pencabutan sertifikat klien (AWS CLI)

Gunakan certificate-revocation-list perintah import-client-vpn-client-.

```
$ aws ec2 import-client-vpn-client-certificate-revocation-list --certificate-
revocation-list file://path_to_CRL_file --client-vpn-endpoint-id endpoint_id --
region region
```

Ekspor daftar pencabutan sertifikat klien

Anda dapat mengekspor daftar pencabutan sertifikat klien menggunakan konsol dan AWS CLI.

Untuk mengekspor daftar pencabutan sertifikat klien (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir Client VPN.
3. Pilih titik akhir Client VPN untuk mengekspor daftar pencabutan sertifikat klien.
4. Pilih Tindakan, pilih Ekspor Client Certificate CRL, dan pilih Ekspor Client Certificate CRL.

Untuk mengekspor daftar pencabutan sertifikat klien (AWS CLI)

Gunakan certificate-revocation-list perintah export-client-vpn-client-.

Koneksi klien

Koneksi adalah sesi VPN yang telah dibuat oleh klien. Koneksi dibuat ketika klien berhasil terhubung ke titik akhir Client VPN.

Daftar Isi

Melihat koneksi klien

Anda dapat melihat koneksi klien menggunakan konsol dan AWS CLI. Informasi koneksi mencakup alamat IP yang ditetapkan dari jangkauan CIDR klien.

Untuk melihat koneksi klien (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir Client VPN.

3. Pilih titik akhir Client VPN untuk melihat koneksi klien.
4. Pilih tab Konektivitas. Tab Konektivitas mencantumkan semua koneksi klien yang aktif dan yang diakhiri.

Untuk melihat koneksi klien (AWS CLI)

Gunakan perintah describe-client-vpn-connections.

Mengakhiri koneksi klien

Ketika Anda mengakhiri koneksi klien, sesi VPN berakhir.

Anda dapat mengakhiri koneksi klien menggunakan konsol dan AWS CLI.

Untuk mengakhiri koneksi klien (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik Akhir Client VPN.
3. Pilih titik akhir Client VPN yang terhubung dengan klien dan pilih Konektivitas.
4. Pilih koneksi untuk mengakhiri, pilih Mengakhiri Koneksi, dan pilih Mengakhiri Koneksi.

Untuk mengakhiri koneksi klien (AWS CLI)

Gunakan perintah terminate-client-vpn-connections.

Spanduk login klien

AWS Client VPNmenyediakan opsi untuk menampilkan spanduk teks pada aplikasi desktop Client VPN yang AWS disediakan saat sesi VPN dibuat. Anda dapat menentukan isi spanduk teks untuk memenuhi kebutuhan peraturan dan kepatuhan Anda. Maksimal 1400, karakter yang dikodekan UTF-8 dapat digunakan.

> **Note**
>
> Ketika banner login klien telah diaktifkan, itu akan ditampilkan pada sesi VPN yang baru dibuat saja. Sesi VPN yang ada tidak terganggu, meskipun spanduk akan ditampilkan ketika sesi yang ada dibuat kembali.

Lihat Catatan rilis untuk klien yang disediakan AWS di Panduan AWS Client VPN Pengguna untuk detail tentang aplikasi desktop klien.

Daftar Isi

Konfigurasikan banner login klien selama pembuatan endpoint Client VPN

Untuk langkah-langkah mendetail untuk mengaktifkan banner login klien selama pembuatan endpoint Client VPN, lihatBuat titik akhir Client VPN.

Konfigurasikan banner login klien untuk titik akhir Client VPN yang ada

Gunakan langkah-langkah berikut untuk mengonfigurasi banner login klien untuk titik akhir Client VPN yang ada.

Aktifkan banner login klien pada titik akhir Client VPN (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Titik Akhir Client VPN.
3. Pilih endpoint Client VPN yang ingin Anda ubah, pilih Actions, lalu pilih Modify Client VPN Endpoint.
4. Gulir ke bawah halaman ke bagian Parameter lainnya.
5. Aktifkan Aktifkan spanduk login klien.
6. Untuk teks banner login Klien, masukkan teks yang akan ditampilkan di spanduk pada klien yang AWS disediakan saat sesi VPN dibuat. Gunakan karakter yang dikodekan UTF-8 saja, dengan maksimum 1400 karakter diizinkan.
7. Pilih Ubah titik akhir Client VPN.

Aktifkan banner login klien pada titik akhir Client VPN () AWS CLI

Gunakan perintah modify-client-vpn-endpoint.

Nonaktifkan banner login klien untuk titik akhir Client VPN yang ada

Gunakan langkah-langkah berikut untuk menonaktifkan banner login klien untuk titik akhir Client VPN yang ada.

Nonaktifkan banner login klien pada titik akhir Client VPN (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Titik Akhir Client VPN.
3. Pilih endpoint Client VPN yang ingin Anda ubah, pilih Actions, lalu pilih Modify Client VPN endpoint.
4. Gulir ke bawah halaman ke bagian Parameter lainnya.
5. Matikan Aktifkan spanduk login klien? .
6. Pilih Ubah titik akhir Client VPN.

Nonaktifkan banner login klien pada titik akhir Client VPN () AWS CLI

Gunakan perintah modify-client-vpn-endpoint.

Ubah teks spanduk yang ada di titik akhir Client VPN

Gunakan langkah-langkah berikut untuk memodifikasi teks yang ada pada banner login klien.

Ubah teks spanduk yang ada di titik akhir Client VPN (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Titik Akhir Client VPN.
3. Pilih endpoint Client VPN yang ingin Anda ubah, pilih Actions, lalu pilih Modify Client VPN endpoint.
4. Untuk Aktifkan spanduk login klien? , verifikasi bahwa itu dihidupkan.
5. Untuk teks banner login Klien, ganti teks yang ada dengan teks baru yang ingin ditampilkan di spanduk pada klien yang AWS disediakan saat sesi VPN dibuat. Gunakan karakter yang dikodekan UTF-8 saja, dengan maksimal 1400 karakter.
6. Pilih Ubah titik akhir Client VPN.

Ubah spanduk login klien pada titik akhir Client VPN () AWS CLI

Gunakan perintah modify-client-vpn-endpoint.

Lihat spanduk login yang saat ini dikonfigurasi

Gunakan langkah-langkah berikut untuk melihat banner login yang saat ini dikonfigurasi.

Lihat banner login saat ini untuk titik akhir Client VPN (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Titik Akhir Client VPN.
3. Pilih titik akhir Client VPN yang ingin Anda lihat.
4. Verifikasi bahwa tab Detail dipilih.
5. Lihat teks spanduk login yang saat ini dikonfigurasi di sebelah teks spanduk login Klien.

Lihat banner login yang saat ini dikonfigurasi untuk titik akhir Client VPN () AWS CLI

Gunakan perintah describe-client-vpn-endpoints.

Titik akhir Client VPN

Semua sesi Client VPN berakhir pada titik akhir Client VPN. Anda mengonfigurasi titik akhir Client VPN untuk mengelola dan mengontrol semua sesi Client VPN.

Daftar Isi

Buat titik akhir Client VPN

Buat titik akhir Client VPN untuk memungkinkan klien Anda membuat sesi VPN.

Client VPN harus dibuat dalam akun AWS yang sama di lokasi jaringan target yang dimaksud telah ditetapkan.

Prasyarat

Sebelum memulai, pastikan Anda melakukan hal berikut:

- Meninjau aturan dan batasan di Aturan dan praktik terbaik AWS Client VPN.
- Membuat sertifikat server, dan jika diperlukan, sertifikat klien. Untuk informasi selengkapnya, lihat Autentikasi Klien.

Untuk membuat titik akhir Client VPN (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir Client VPN lalu pilih Buat Titik akhir Client VPN.
3. (Opsional) Berikan tag nama dan deskripsi untuk titik akhir Client VPN.
4. Untuk Client IPv4 CIDR, tentukan rentang alamat IP, dalam notasi CIDR, untuk menetapkan alamat IP klien. Sebagai contoh, `10.0.0.0/22`.

   > **Note**
   >
   > Rentang alamat tidak dapat tumpang tindih dengan rentang alamat jaringan target, rentang alamat VPC, atau rute apa pun yang akan dikaitkan dengan titik akhir Client VPN. Rentang alamat klien harus minimal /22 dan tidak lebih besar dari/12 ukuran blok CIDR. Anda tidak dapat mengubah rentang alamat klien setelah Anda membuat titik akhir Client VPN.

5. Untuk Sertifikat server ARN, tentukan ARN untuk sertifikat TLS yang akan digunakan oleh server. Klien menggunakan sertifikat server untuk mengautentikasi titik akhir Client VPN tempat klien terhubung.

   > **Note**
   >
   > Sertifikat server harus ada di AWS Certificate Manager (ACM) di wilayah tempat Anda membuat titik akhir Client VPN. Sertifikat dapat disediakan dengan ACM atau diimpor ke ACM.

6. Tentukan metode autentikasi yang akan digunakan untuk mengautentikasi klien ketika mereka membuat koneksi VPN. Anda harus memilih metode autentikasi.

   - Untuk menggunakan autentikasi berbasis pengguna, pilih Gunakan autentikasi berbasis pengguna, lalu pilih salah satu hal berikut ini:

- Autentikasi Direktori Aktif: Pilih opsi ini untuk autentikasi Direktori Aktif. Untuk ID Direktori, tentukan ID dari Direktori Aktif yang akan digunakan.
- Autentikasi gabungan: Pilih opsi ini untuk autentikasi gabungan berbasis SAML.

  Untuk ARN penyedia SAML, tentukan ARN dari penyedia identitas IAM SAML.

  (Opsional) ARN Penyedia SAML layanan mandiri, tentukan ARN dari penyedia identitas IAM SAML yang Anda buat untuk mendukung portal layanan mandiri, jika ada.

- Untuk menggunakan autentikasi sertifikat bersama, pilih Gunakan autentikasi bersama, lalu untuk ARN Sertifikat klien, tentukan ARN sertifikat klien yang ditetapkan di AWS Certificate Manager (ACM).

> **Note**
>
> Jika sertifikat server dan klien telah dikeluarkan oleh Otoritas Sertifikat (CA) yang sama, Anda dapat menggunakan sertifikat server ARN untuk server dan klien. Jika sertifikat klien dikeluarkan oleh CA yang berbeda, maka sertifikat klien ARN harus ditentukan.

7. (Opsional) Untuk pencatatan Koneksi, tentukan apakah akan mencatat data tentang koneksi klien menggunakan Amazon CloudWatch Logs. Aktifkan Aktifkan detail log pada koneksi klien. Untuk nama grup CloudWatch log Log, masukkan nama grup log yang akan digunakan. Untuk nama aliran CloudWatch log Log, masukkan nama aliran log yang akan digunakan, atau biarkan opsi ini kosong agar kami membuat aliran log untuk Anda.
8. (Opsional) Untuk Client Connect Handler, aktifkan Enable client connect handler untuk menjalankan kode kustom yang memungkinkan atau menolak koneksi baru ke endpoint Client VPN. Untuk ARN Client Connect Handler, tentukan untuk Amazon Resource Name (ARN) dari fungsi Lambda yang berisi logika yang mengizinkan atau menolak koneksi.
9. (Opsional) Menentukan server DNS yang akan digunakan untuk resolusi DNS. Untuk menggunakan server DNS kustom, untuk Alamat IP DNS Server 1 dan Alamat IP DNS Server 2, tentukan alamat IP dari layanan DNS yang akan digunakan. Untuk menggunakan server DNS VPC, Alamat IP DNS Server 1 atau Alamat IP DNS Server 2, tentukan alamat IP dan tambahkan alamat IP dari server DNS VPC.

> **Note**
>
> Verifikasi bahwa server DNS dapat dijangkau oleh klien.

10. (Opsional) Secara default, titik akhir Client VPN menggunakan protokol UDP transport. Untuk menggunakan protokol transportasi TCP, pada Protokol transportasi, pilih TCP.

> **Note**
>
> UDP biasanya menawarkan performa yang lebih baik daripada TCP. Anda tidak dapat mengubah protokol transportasi setelah Anda membuat titik akhir Client VPN.

11. (Opsional) Agar titik akhir menjadi titik akhir Client VPN split-tunnel, aktifkan Aktifkan split-tunnel. Secara default, split-tunnel pada titik akhir Client VPN dinonaktifkan.
12. (Opsional) Untuk ID VPC, pilih VPC agar dikaitkan dengan titik akhir Client VPN. Untuk ID Grup Keamanan, pilih satu atau beberapa grup keamanan VPC untuk diterapkan ke titik akhir Client VPN.
13. (Opsional) Pada Port VPN, pilih nomor port VPN. Default-nya adalah 443.
14. (Opsional) Untuk menghasilkan URL portal swalayan untuk klien, aktifkan Aktifkan portal swalayan.
15. (Opsional) Untuk jam tunggu Sesi, pilih waktu durasi sesi VPN maksimum yang diinginkan dalam jam dari opsi yang tersedia, atau biarkan disetel ke default 24 jam.
16. (Opsional) Tentukan apakah akan mengaktifkan teks banner login klien. Aktifkan Aktifkan spanduk login klien. Untuk teks banner login Klien, masukkan teks yang akan ditampilkan di spanduk pada klien yang disediakan AWS saat sesi VPN dibuat. Hanya karakter yang dikodekan UTF-8. Maksimal 1400 karakter.
17. Pilih Create Client VPN endpoint.

Setelah Anda membuat titik akhir Client VPN, lakukan hal berikut untuk menyelesaikan konfigurasi dan memungkinkan klien untuk terhubung:

- Keadaan awal titik akhir Client VPN adalah `pending-associate`. Klien hanya dapat terhubung ke titik akhir Client VPN setelah Anda mengaitkan jaringan target pertama.
- Buat aturan otorisasi untuk menentukan klien mana yang memiliki akses ke jaringan.
- Unduh dan siapkan file konfigurasi titik akhir Client VPN untuk didistribusikan ke klien Anda.

- Instruksikan klien Anda untuk menggunakan AWS yang disediakan klien atau aplikasi klien berbasis OpenVPN lain untuk terhubung ke titik akhir Client VPN. Untuk informasi selengkapnya, lihat AWS Client VPN Panduan Pengguna.

Untuk membuat titik akhir Client VPN (AWS CLI)

Gunakan perintah create-client-vpn-endpoint.

Mengubah titik akhir Client VPN

Setelah Client VPN dibuat, Anda dapat mengubah salah satu pengaturan berikut ini:

- Deskripsi
- Sertifikat server
- Opsi pencatatan koneksi klien
- Opsi handler koneksi klien
- Server DNS
- Opsi terowongan terpisah
- Rute (saat menggunakan opsi split-tunnel)
- Daftar Pencabutan Sertifikat (CRL)
- Aturan otorisasi
- Asosiasi VPC dan grup keamanan
- Nomor port VPN
- Opsi portal layanan mandiri
- Durasi sesi VPN maksimum
- Mengaktifkan atau menonaktifkan teks spanduk login klien
- Teks banner login klien

> **Note**
>
> Modifikasi pada titik akhir Client VPN, termasuk perubahan Daftar Pencabutan Sertifikat (CRL), akan berlaku hingga 4 jam setelah permintaan diterima oleh layanan Client VPN. Anda tidak dapat mengubah rentang IPv4 CIDR klien, opsi otentikasi, sertifikat klien atau protokol transportasi setelah titik akhir Client VPN dibuat.

Ketika Anda mengubah salah satu parameter berikut pada titik akhir Client VPN, koneksi akan diatur ulang:

- Sertifikat server
- Server DNS
- Opsi terowongan terpisah (mengaktifkan atau menonaktifkan dukungan)
- Rute (ketika Anda menggunakan opsi terowongan terpisah)
- Daftar Pencabutan Sertifikat (CRL)
- Aturan otorisasi
- Nomor port VPN

Anda dapat mengubah titik akhir Client VPN menggunakan konsol atau AWS CLI.

Untuk mengubah titik akhir Client VPN (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir Client VPN.
3. Pilih endpoint Client VPN yang akan diubah, pilih Actions, lalu pilih Modify Client VPN endpoint.
4. Untuk Deskripsi, masukkan deskripsi singkat titik akhir Client VPN.
5. Untuk Sertifikat server ARN, tentukan ARN untuk sertifikat TLS yang akan digunakan oleh server. Klien menggunakan sertifikat server untuk mengautentikasi titik akhir Client VPN tempat klien terhubung.

   > **Note**
   >
   > Sertifikat server harus ada di AWS Certificate Manager (ACM) di wilayah tempat Anda membuat titik akhir Client VPN. Sertifikat dapat disediakan dengan ACM atau diimpor ke ACM.

6. Tentukan apakah akan mencatat data tentang koneksi klien menggunakan Amazon CloudWatch Logs. Untuk Aktifkan detail log pada koneksi klien, lakukan salah satu hal berikut:

   - Untuk mengaktifkan pencatatan koneksi klien, aktifkan Aktifkan detail log pada koneksi klien. Untuk nama grup CloudWatch log Log, pilih nama grup log yang akan digunakan. Untuk nama aliran CloudWatch log Log, pilih nama aliran log yang akan digunakan, atau biarkan opsi ini kosong agar kami dapat membuat aliran log untuk Anda.

- Untuk menonaktifkan pencatatan koneksi klien, matikan Aktifkan detail log pada koneksi klien.

7. Untuk Client connect handler, untuk mengaktifkan client connect handler aktifkan Enable client connect handler. Untuk ARN Client Connect Handler, tentukan untuk Amazon Resource Name (ARN) dari fungsi Lambda yang berisi logika yang mengizinkan atau menolak koneksi.
8. Menghidupkan atau menonaktifkan Aktifkan server DNS. Untuk menggunakan server DNS kustom, untuk Alamat IP DNS Server 1 dan Alamat IP DNS Server 2, tentukan alamat IP dari layanan DNS yang akan digunakan. Untuk menggunakan server DNS VPC, Alamat IP DNS Server 1 atau Alamat IP DNS Server 2, tentukan alamat IP dan tambahkan alamat IP dari server DNS VPC.

   > **Note**
   >
   > Verifikasi bahwa server DNS dapat dijangkau oleh klien.

9. Hidupkan atau matikan Aktifkan split-tunnel. Secara default, split-tunnel pada titik akhir VPN tidak aktif.
10. Untuk ID VPC, pilih VPC yang akan diasosiasikan dengan titik akhir Client VPN. Untuk ID Grup Keamanan, pilih satu atau beberapa grup keamanan VPC untuk diterapkan ke titik akhir Client VPN.
11. Untuk Port VPN, pilih nomor port VPN. Default-nya adalah 443.
12. Untuk menghasilkan URL portal swalayan untuk klien, aktifkan Aktifkan portal swalayan.
13. Untuk jam tunggu Sesi, pilih waktu durasi sesi VPN maksimum yang diinginkan dalam jam dari opsi yang tersedia, atau biarkan disetel ke default 24 jam.
14. Menghidupkan atau menonaktifkan Aktifkan spanduk login klien. Jika Anda ingin menggunakan spanduk login klien, masukkan teks yang akan ditampilkan di spanduk pada klien yang disediakan AWS saat sesi VPN dibuat. Hanya karakter yang dikodekan UTF-8. Maksimal 1400 karakter.
15. Pilih Ubah titik akhir Client VPN.

Untuk mengubah titik akhir Client VPN (AWS CLI)

Gunakan perintah modify-client-vpn-endpoint.

Melihat titik akhir Client VPN

Anda dapat melihat informasi tentang titik akhir Client VPN menggunakan konsol atau AWS CLI.

Untuk melihat titik akhir Client VPN (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir Client VPN.
3. Pilih titik akhir Client VPN untuk melihat.
4. Gunakan tab Detail, Asosiasi jaringan target, Grup keamanan, Aturan otorisasi, Tabel rute, Koneksi, dan Tag untuk melihat informasi tentang titik akhir Client VPN yang ada.

   Anda juga dapat menggunakan filter untuk membantu menyempurnakan pencarian Anda.

Untuk melihat titik akhir Client VPN () AWS CLI

Gunakan perintah describe-client-vpn-endpoints.

Menghapus titik akhir Client VPN

Anda harus memisahkan semua jaringan target sebelum dapat menghapus titik akhir Client VPN. Ketika Anda menghapus titik akhir Client VPN, statusnya berubah menjadi `deleting` dan klien tidak bisa lagi terhubung kesana.

Anda dapat menghapus titik akhir Client VPN menggunakan konsol atau AWS CLI.

Untuk menghapus titik akhir Client VPN (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Titik Akhir Client VPN.
3. Pilih titik akhir Client VPN untuk dihapus. Pilih Tindakan, Hapus titik akhir Client VPN.
4. Masukkan hapus ke jendela konfirmasi dan pilih Hapus.

Untuk menghapus titik akhir Client VPN (AWS CLI)

Gunakan perintah delete-client-vpn-endpoint.

Bekerja dengan log koneksi

Anda dapat mengaktifkan logging koneksi untuk titik akhir Client VPN baru atau yang sudah ada, dan mulai menangkap log koneksi.

Sebelum memulai, Anda harus memiliki grup CloudWatch log Log di akun Anda. Untuk informasi selengkapnya, lihat Bekerja dengan Grup Log dan Aliran Log di Panduan Pengguna Amazon CloudWatch Logs. Biaya berlaku untuk menggunakan CloudWatch Log. Untuk informasi selengkapnya, lihat CloudWatch harga Amazon.

Bila Anda mengaktifkan logging koneksi, Anda dapat menentukan nama pengaliran log dalam grup log. Jika Anda tidak menentukan pengaliran log, layanan Client VPN akan membuat satu untuk Anda.

Aktifkan logging koneksi untuk titik akhir Client VPN baru

Anda dapat mengaktifkan logging koneksi ketika Anda membuat titik akhir Client VPN baru menggunakan konsol atau baris perintah.

Untuk mengaktifkan logging koneksi untuk titik akhir Client VPN baru menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik Akhir Client VPN, lalu pilih Create Client VPN endpoint.
3. Lengkapi opsi sampai Anda mencapai bagian Logging koneksi. Untuk informasi lebih lanjut tentang opsi, lihat Buat titik akhir Client VPN.
4. Di bawah Pencatatan koneksi, aktifkan Aktifkan detail log pada koneksi klien.
5. Untuk nama grup CloudWatch log Log, pilih nama grup CloudWatch log Log.
6. (Opsional) Untuk nama aliran CloudWatch log Log, pilih nama aliran CloudWatch log Log.
7. Pilih Create Client VPN endpoint.

Untuk mengaktifkan logging koneksi untuk titik akhir Client VPN baru menggunakan AWS CLI

Gunakan create-client-vpn-endpointperintah, dan tentukan `--connection-log-options` parameternya. Anda dapat menentukan informasi log koneksi dalam format JSON, seperti yang ditunjukkan pada contoh berikut.

```
{
    "Enabled": true,
    "CloudwatchLogGroup": "ClientVpnConnectionLogs",
    "CloudwatchLogStream": "NewYorkOfficeVPN"
}
```

Aktifkan logging koneksi untuk titik akhir Client VPN yang ada

Anda dapat mengaktifkan logging koneksi titik akhir Client VPN menggunakan konsol atau baris perintah.

Untuk mengaktifkan logging koneksi untuk titik akhir Client VPN yang ada menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir Client VPN.
3. Pilih endpoint Client VPN, pilih Actions, lalu pilih Modify Client VPN endpoint.
4. Di bawah Pencatatan koneksi, aktifkan Aktifkan detail log pada koneksi klien.
5. Untuk nama grup CloudWatch log Log, pilih nama grup CloudWatch log Log.
6. (Opsional) Untuk nama aliran CloudWatch log Log, pilih nama aliran CloudWatch log Log.
7. Pilih Ubah titik akhir Client VPN.

Untuk mengaktifkan logging koneksi untuk titik akhir Client VPN yang ada menggunakan AWS CLI

Gunakan modify-client-vpn-endpointperintah dan tentukan `--connection-log-options` parameternya. Anda dapat menentukan informasi log koneksi dalam format JSON, seperti yang ditunjukkan pada contoh berikut.

```
{
    "Enabled": true,
    "CloudwatchLogGroup": "ClientVpnConnectionLogs",
    "CloudwatchLogStream": "NewYorkOfficeVPN"
}
```

Melihat log koneksi

Anda dapat melihat log koneksi menggunakan konsol CloudWatch Log.

Untuk melihat log koneksi menggunakan konsol

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, pilih Grup log, dan pilih grup log yang berisi log koneksi Anda.
3. Pilih pengaliran log untuk titik akhir Client VPN Anda.

> **Note**
>
> Kolom Timestamp menampilkan waktu log koneksi dipublikasikan ke CloudWatch Log, bukan waktu koneksi.

Untuk informasi selengkapnya tentang penelusuran data log, lihat Cari Data Log Menggunakan Pola Filter di Panduan Pengguna CloudWatch Log Amazon.

Matikan pencatatan koneksi

Anda dapat mematikan pencatatan koneksi untuk titik akhir Client VPN dengan menggunakan konsol atau baris perintah. Saat Anda mematikan pencatatan koneksi, log koneksi yang ada di CloudWatch Log tidak akan dihapus.

Untuk mematikan logging koneksi menggunakan konsol

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir Client VPN.
3. Pilih endpoint Client VPN, pilih Actions, lalu pilih Modify Client VPN endpoint.
4. Di bawah Pencatatan koneksi, matikan Aktifkan detail log pada koneksi klien.
5. Pilih Ubah titik akhir Client VPN.

Untuk mematikan log koneksi menggunakan AWS CLI

Gunakan modify-client-vpn-endpointperintah, dan tentukan `--connection-log-options` parameternya. Pastikan bahwa `Enabled` diatur ke `false`.

Ekspor dan konfigurasikan file konfigurasi untuk klien

Konfigurasi file titik akhir Client VPN adalah file yang digunakan klien (pengguna) untuk membuat koneksi VPN dengan titik akhir Client VPN. Anda harus mengunduh (mengekspor) file ini dan mendistribusikan ke semua klien yang membutuhkan akses VPN. Atau, jika Anda telah mengaktifkan portal layanan mandiri untuk titik akhir Client VPN Anda, klien dapat log in ke portal dan mengunduh file konfigurasi sendiri. Untuk informasi selengkapnya, lihat Mengakses portal layanan mandiri.

Jika titik akhir Client VPN Anda menggunakan autentikasi bersama, Anda harus menambahkan sertifikat klien dan kunci privat klien ke konfigurasi file .ovpn yang diunduh. Setelah Anda menambahkan informasi, klien dapat mengimpor file .ovpn ke perangkat lunak klien OpenVPN.

> **Important**
>
> Jika Anda tidak menambahkan sertifikat klien dan informasi kunci privat klien ke dalam file, autentikasi klien yang menggunakan autentikasi bersama tidak dapat terhubung ke titik akhir Client VPN.

Secara default, opsi “remote-random-hostname” dalam konfigurasi klien OpenVPN memungkinkan DNS wildcard. Karena wildcard DNS diaktifkan, klien tidak membuat cache titik akhir alamat IP dan Anda tidak akan dapat mengirim ping titik akhir nama DNS.

Jika titik akhir Client VPN menggunakan autentikasi Direktori Aktif dan jika Anda mengaktifkan autentikasi multi-faktor (MFA) pada direktori Anda setelah mendistribusikan file konfigurasi klien, Anda harus mengunduh file baru dan mendistribusikan kembali ke klien Anda. Klien tidak dapat menggunakan file konfigurasi sebelumnya untuk terhubung ke titik akhir Client VPN.

Ekspor file konfigurasi klien

Anda dapat mengekspor konfigurasi klien menggunakan konsol atau AWS CLI.

Untuk mengekspor konfigurasi klien (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir Client VPN.
3. Pilih titik akhir Client VPN untuk mengunduh konfigurasi klien dan pilih Unduh Konfigurasi Klien.

Untuk mengekspor konfigurasi klien (AWS CLI)

Gunakan perintah export-client-vpn-client-configuration dan tentukan nama file output.

```
$ aws ec2 export-client-vpn-client-configuration --client-vpn-endpoint-id endpoint_id
 --output text>config_filename.ovpn
```

Menambahkan sertifikat klien dan informasi kunci (autentikasi bersama)

Jika titik akhir Client VPN Anda menggunakan autentikasi bersama, Anda harus menambahkan sertifikat klien dan kunci privat klien ke konfigurasi file .ovpn yang Anda unduh.

Anda tidak dapat mengubah sertifikat klien ketika Anda menggunakan autentikasi bersama.

Untuk menambahkan sertifikat klien dan informasi kunci (autentikasi bersama)

Anda dapat menggunakan salah satu opsi berikut.

(Opsi 1) Distribusikan sertifikat klien dan kunci untuk klien bersama dengan konfigurasi file titik akhir Client VPN. Dalam hal ini, tentukan jalur ke sertifikat dan kunci di dalam file konfigurasi. Buka file konfigurasi menggunakan editor teks pilihan Anda dan tambahkan berikut ini di akhir file. Ganti */path/* dengan lokasi sertifikat klien dan kunci (lokasi relatif terhadap klien yang terhubung ke titik akhir).

```
cert /path/client1.domain.tld.crt
key /path/client1.domain.tld.key
```

(Opsi 2) Tambahkan isi sertifikat klien antara tanda `<cert></cert>` dan isi dari kunci privat antara tanda `<key></key>` ke file konfigurasi. Jika Anda memilih opsi ini, Anda hanya mendistiribusikan file konfigurasi untuk klien Anda.

Jika Anda membuat sertifikat klien dan kunci secara terpisah untuk setiap pengguna yang akan terhubung ke titik akhir Client VPN, ulangi langkah ini untuk setiap pengguna.

Berikut ini adalah contoh format file konfigurasi Client VPN yang mencakup sertifikat klien beserta kunci.

```
client
dev tun
proto udp
remote cvpn-endpoint-0011abcabcabcabc1.prod.clientvpn.eu-west-2.amazonaws.com 443
remote-random-hostname
resolv-retry infinite
nobind
remote-cert-tls server
cipher AES-256-GCM
verb 3
```

```
<ca>
Contents of CA
</ca>

<cert>
Contents of client certificate (.crt) file
</cert>

<key>
Contents of private key (.key) file
</key>

reneg-sec 0
```

Rute

Setiap titik akhir Client VPN memiliki tabel rute yang menjelaskan rute jaringan tujuan yang tersedia. Setiap rute dalam tabel rute menentukan tempat lalu lintas jaringan diarahkan. Anda harus mengonfigurasi aturan otorisasi untuk setiap rute titik akhir Client VPN untuk menentukan klien yang memiliki akses ke jaringan tujuan.

Ketika Anda mengaitkan subnet dari VPC dengan titik akhir Client VPN, rute untuk VPC secara otomatis ditambahkan ke tabel rute titik akhir Client VPN. Untuk mengaktifkan akses jaringan tambahan, seperti VPC ter-peering, jaringan on-premise, jaringan lokal (untuk memungkinkan klien berkomunikasi satu sama lain), atau internet, Anda harus menambahkan rute ke tabel rute titik akhir Client VPN secara manual.

> **Note**
>
> Jika Anda mengaitkan beberapa subnet ke titik akhir Client VPN, Anda harus memastikan untuk membuat rute untuk setiap subnet seperti yang dijelaskan di sini. Akses ke VPC yang di-peering, Amazon S3, atau internet terputus-putus Setiap subnet terkait harus memiliki serangkaian rute yang identik.

Daftar Isi

- Melihat rute titik akhir
- Menghapus rute titik akhir

Terowongan terpisah pada pertimbangan titik akhir Client VPN

Ketika Anda menggunakan terowongan terpisah pada titik akhir Client VPN, semua rute yang ada di tabel rute Client VPN ditambahkan ke tabel rute klien ketika VPN dibuat. Jika Anda menambahkan rute setelah VPN dibuat, Anda harus mengatur ulang koneksi sehingga rute baru dikirim ke klien.

Kami merekomendasikan Anda untuk memperhitungkan jumlah rute yang dapat ditangani perangkat klien sebelum Anda mengubah tabel rute titik akhir Client VPN.

Membuat rute titik akhir

Ketika membuat rute, Anda menentukan bagaimana lalu lintas untuk jaringan tujuan harus diarahkan.

Untuk mengizinkan klien mengakses internet, tambahkan rute `0.0.0.0/0` tujuan.

Anda dapat menambahkan rute ke titik akhir Client VPN dengan menggunakan konsol tersebut dan AWS CLI.

Untuk membuat rute titik akhir Client VPN (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Titik Akhir Client VPN.
3. Pilih titik akhir Client VPN yang akan ditambahkan rute, pilih tabel Rute, lalu pilih Buat rute.
4. Untuk Tujuan rute, tentukan rentang CIDR IPv4 untuk jaringan tujuan. Misalnya:
   - Untuk menambahkan rute untuk VPC titik akhir Client VPN, masukkan rentang CIDR IPv4 VPC.
   - Untuk menambahkan rute akses internet, masukkan `0.0.0.0/0`.
   - Untuk menambahkan rute untuk VPC ter-peering, masukkan rentang CIDR IPv4 VPC ter-peering.
   - Untuk menambahkan rute jaringan on-premise, masukkan rentang CIDR IPv4 koneksi AWS Site-to-Site VPN.
5. Untuk Subnet ID untuk asosiasi jaringan target, pilih subnet yang terkait dengan titik akhir Client VPN.

Atau, jika Anda menambahkan rute untuk jaringan endpoint Client VPN lokal, pilih`local`.

6. (Opsional) Untuk Deskripsi, masukkan deskripsi singkat untuk rute tersebut.
7. Pilih Buat rute.

Untuk membuat rute titik akhir Client VPN (AWS CLI)

Gunakan perintah create-client-vpn-route.

Melihat rute titik akhir

Anda dapat melihat rute untuk titik akhir Client VPN tertentu dengan menggunakan konsol tersebut atau AWS CLI.

Untuk melihat rute titik akhir Client VPN (konsol)

1. Pada panel navigasi, pilih Titik Akhir Client VPN.
2. Pilih titik akhir Client VPN untuk melihat rute dan pilih tabel Rute.

Untuk melihat rute titik akhir Client VPN (AWS CLI)

Gunakan perintah describe-client-vpn-routes.

Menghapus rute titik akhir

Anda hanya dapat menghapus rute yang ditambahkan secara manual. Anda tidak dapat menghapus rute yang ditambahkan secara otomatis ketika Anda mengaitkan subnet dengan titik akhir Client VPN. Untuk menghapus rute yang ditambahkan secara otomatis, Anda harus memisahkan subnet yang pembuatannya dimulai dari titik akhir Client VPN.

Anda dapat menghapus rute dari titik akhir Client VPN dengan menggunakan konsol tersebut atau AWS CLI.

Untuk menghapus rute titik akhir Client VPN (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Titik akhir Client VPN.
3. Pilih titik akhir Client VPN untuk menghapus rute dan pilih tabel Route.
4. Pilih rute yang akan dihapus, pilih Hapus rute, dan pilih Hapus rute.

Untuk menghapus rute titik akhir Client VPN (AWS CLI)

Gunakan perintah delete-client-vpn-route.

Jaringan target

Subnet dari VPC merupakan jaringan target. Titik akhir Client VPN harus memiliki setidaknya satu jaringan target untuk memungkinkan klien terhubung dan membuat koneksi VPN.

Untuk informasi selengkapnya tentang jenis akses yang dapat Anda konfigurasi (seperti mengaktifkan klien Anda untuk mengakses internet), lihat Skenario dan contoh untuk AWS Client VPN.

Konten

Mengaitkan jaringan target dengan titik akhir Client VPN

Anda dapat mengaitkan satu atau lebih jaringan target (subnet) dengan titik akhir Client VPN.

Aturan berikut berlaku:

- Subnet harus memiliki blok CIDR dengan setidaknya bitmask /27, misalnya 10.0.0.0/27. Subnet juga harus memiliki setidaknya 20 alamat IP yang tersedia setiap saat.
- Blok CIDR subnet tidak dapat tumpang tindih dengan kisaran CIDR klien titik akhir Client VPN.
- Jika Anda mengaitkan lebih dari satu subnet dengan titik akhir Client VPN, setiap subnet harus berada di Availability Zone yang berbeda. Kami merekomendasikan Anda mengaitkan setidaknya dua subnet untuk menyediakan redundansi Availability Zone.
- Jika Anda menetapkan VPC ketika Anda membuat titik akhir Client VPN, subnet harus dalam VPC yang sama. Jika Anda belum mengaitkan VPC dengan titik akhir Client VPN, Anda dapat memilih subnet apa pun di VPC manapun.

  Semua asosiasi subnet selanjutnya harus berasal dari VPC yang sama. Untuk mengaitkan subnet dari VPC yang berbeda, Anda harus terlebih dahulu memodifikasi titik akhir Client VPN dan

mengubah VPC yang terkait dengannya. Untuk informasi selengkapnya, lihat Mengubah titik akhir Client VPN.

Ketika Anda mengaitkan subnet dengan titik akhir Client VPN, kami secara otomatis menambahkan rute lokal VPC di mana subnet terkait disediakan ke tabel rute titik akhir Client VPN.

> **Note**
>
> Setelah jaringan target Anda dikaitkan, saat Anda menambahkan atau menghapus CIDR tambahan ke VPC terlampir, Anda harus melakukan salah satu operasi berikut untuk memperbarui rute lokal untuk tabel rute titik akhir Client VPN Anda:
>
> - Pisahkan titik akhir Client VPN Anda dari jaringan target, lalu kaitkan titik akhir Client VPN ke jaringan target.
> - Secara manual menambahkan rute ke, atau menghapus rute dari titik akhir Client VPN tabel rute.

Setelah Anda mengaitkan subnet pertama dengan titik akhir Client VPN, status titik akhir Client VPN berubah `pending-associate` dari `available` ke dan klien dapat membuat koneksi VPN.

Untuk mengaitkan jaringan target dengan titik akhir Client VPN (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Titik Akhir Client VPN.
3. Pilih titik akhir Client VPN untuk mengaitkan jaringan target, pilih Asosiasi jaringan target, lalu pilih Associate target network.
4. Untuk VPC, pilih VPC tempat subnet berada. Jika Anda menetapkan VPC ketika Anda membuat titik akhir Client VPN atau jika Anda memiliki asosiasi subnet sebelumnya, subnet harus dalam VPC yang sama.
5. Untuk Pilih subnet untuk diasosiasikan, pilih subnet yang akan dikaitkan dengan titik akhir Client VPN.
6. Pilih Jaringan target asosiasi.

Untuk mengaitkan jaringan target dengan titik akhir Client VPN (AWS CLI)

Gunakan perintah associate-client-vpn-target-network.

Terapkan grup keamanan ke jaringan target

Saat Anda membuat titik akhir Client VPN, Anda dapat menentukan grup keamanan untuk diterapkan ke jaringan target. Saat Anda mengaitkan jaringan target pertama dengan titik akhir Client VPN, kami secara otomatis menerapkan grup keamanan default VPC tempat subnet terkait berada. Untuk informasi selengkapnya, lihat Grup keamanan.

Anda dapat mengubah grup keamanan untuk akhir Client VPN. Aturan grup keamanan yang Anda perlukan bergantung pada jenis akses VPN yang ingin Anda konfigurasikan. Untuk informasi selengkapnya, lihat Skenario dan contoh untuk AWS Client VPN.

Untuk menerapkan grup keamanan ke jaringan target (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik akhir Client VPN.
3. Pilih titik akhir Client VPN untuk menerapkan grup keamanan.
4. Pilih Grup Keamanan, lalu pilih Terapkan Grup Keamanan.
5. Pilih grup keamanan yang sesuai dari ID grup Keamanan.
6. Pilih Terapkan Grup Keamanan.

Untuk menerapkan grup keamanan ke jaringan target (AWS CLI)

Gunakan client-vpn-target-network perintah apply-security-groups-to-.

Pisahkan jaringan target dari titik akhir Client VPN

Saat Anda memisahkan jaringan target, rute apa pun yang ditambahkan secara manual ke tabel rute titik akhir Client VPN akan dihapus, serta rute yang dibuat secara otomatis saat asosiasi jaringan target dibuat (rute lokal VPC). Jika Anda memisahkan semua jaringan target dari titik akhir Client VPN, klien tidak dapat lagi membuat koneksi VPN.

Untuk memisahkan jaringan target dari titik akhir Client VPN (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Titik Akhir Client VPN.
3. Pilih titik akhir Client VPN yang terkait dengan jaringan target dan pilih Asosiasi jaringan target.
4. Pilih jaringan target untuk memisahkan, pilih Disassociate, dan kemudian pilih Disassociate target network.

Untuk memisahkan jaringan target dari titik akhir Client VPN (AWS CLI)

Gunakan perintah disassociate-client-vpn-target-network.

Lihat jaringan target

Anda dapat melihat target yang terkait dengan titik akhir Client VPN menggunakan konsol atau AWS CLI.

Untuk melihat jaringan target (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Titik Akhir Client VPN.
3. Pilih titik akhir Client VPN yang sesuai dan pilih Asosiasi jaringan target.

Untuk melihat jaringan target menggunakan AWS CLI

Gunakan perintah describe-client-vpn-target-networks.

Durasi maksimum sesi VPN

AWS Client VPNmenyediakan beberapa opsi untuk durasi sesi VPN maksimum. Anda dapat mengonfigurasi durasi sesi VPN maksimum yang lebih pendek untuk memenuhi persyaratan keamanan dan kepatuhan. Secara default, durasi sesi VPN maksimum adalah 24 jam.

> **Note**
>
> Ketika nilai durasi sesi VPN maksimum berkurang, sesi VPN aktif yang lebih lama dari nilai batas waktu baru akan terputus.

Lihat Catatan rilis untuk klien yang disediakan AWS di Panduan AWS Client VPN Pengguna untuk detail tentang aplikasi desktop klien.

Daftar Isi

Konfigurasikan sesi VPN maksimum selama pembuatan titik akhir Client VPN

Untuk langkah-langkah mendetail untuk mengonfigurasi sesi VPN maksimum selama pembuatan titik akhir Client VPN, lihat. Buat titik akhir Client VPN

Lihat durasi sesi VPN maksimum saat ini

Gunakan langkah-langkah berikut untuk melihat durasi sesi VPN maksimum saat ini.

Lihat durasi sesi VPN maksimum saat ini untuk titik akhir Client VPN (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Pada panel navigasi, pilih Titik Akhir Client VPN.
3. Pilih titik akhir Client VPN yang ingin Anda lihat.
4. Verifikasi bahwa tab Detail dipilih.
5. Lihat durasi sesi VPN maksimum saat ini di samping Jam tunggu sesi.

Lihat durasi sesi VPN maksimum saat ini untuk titik akhir Client VPN () AWS CLI

Gunakan perintah describe-client-vpn-endpoints.

Ubah durasi sesi VPN maksimum

Gunakan langkah-langkah berikut untuk mengubah durasi sesi VPN maksimum yang ada.

Ubah durasi sesi VPN maksimum yang ada untuk titik akhir Client VPN (konsol)

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih titik akhir Client VPN.
3. Pilih endpoint Client VPN yang ingin Anda ubah, pilih Actions, lalu pilih Modify Client VPN Endpoint.
4. Untuk jam tunggu sesi, pilih durasi sesi VPN maksimum yang diinginkan dalam jam.
5. Pilih Ubah titik akhir Client VPN.

Ubah durasi sesi VPN maksimum yang ada untuk titik akhir Client VPN () AWS CLI

Gunakan perintah modify-client-vpn-endpoint.

Keamanan di AWS Client VPN

Keamanan cloud di AWS merupakan prioritas tertinggi. Sebagai pelanggan AWS, Anda mendapatkan manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara AWS dan Anda. Model tanggung jawab bersama menggambarkan ini sebagai keamanan dari cloud dan keamanan di dalam cloud:

- Keamanan cloud – AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan layanan-layanan AWS di dalam AWS Cloud. AWS juga memberikan Anda layanan yang dapat digunakan dengan aman. Auditor pihak ketiga menguji dan memverifikasi secara berkala efektivitas keamanan kami sebagai bagian dari Program Kepatuhan AWS. Untuk mempelajari tentang program kepatuhan yang berlaku untukAWS Client VPN, lihatAWSLayanan dalam Lingkup oleh Program Kepatuhan.
- Keamanan di cloud – Tanggung jawab Anda ditentukan oleh layanan AWS yang digunakan. Anda juga bertanggung jawab atas faktor lain termasuk sensitivitas data Anda, persyaratan perusahaan Anda, serta hukum dan peraturan yang berlaku.

AWS Client VPNadalah bagian dari layanan Amazon VPC. Untuk informasi selengkapnya tentang aturan keamanan dalam Amazon VPC, lihat Keamanan dalam Panduan Pengguna Amazon VPC.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Client VPN. Topik berikut menunjukkan kepada Anda cara mengonfigurasi Client VPN agar memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan layanan AWS lain yang membantu Anda untuk memantau dan mengamankan sumber daya Client VPN.

Daftar Isi

Perlindungan data di AWS Client VPN

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS Client VPN. Sebagaimana diuraikan dalam model ini, AWS bertanggung jawab untuk memberikan perlindungan terhadap infrastruktur global yang menjalankan semua AWS Cloud. Anda harus bertanggung jawab untuk memelihara kendali terhadap konten yang di-hosting pada infrastruktur ini. Anda juga bertanggung jawab atas konfigurasi keamanan dan tugas manajemen untuk Layanan AWS yang Anda gunakan. Untuk informasi lebih lanjut tentang privasi data, lihat FAQ tentang Privasi Data. Untuk informasi tentang perlindungan data di Eropa, lihat postingan blog Model Tanggung Jawab Bersama AWS dan GDPR di Blog Keamanan AWS.

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensyal dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara tersebut, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tugas pekerjaan mereka. Kami juga merekomendasikan agar Anda mengamankan data Anda dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk melakukan komunikasi dengan sumber daya AWS. 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 dalamnyaLayanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 ketika mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Untuk informasi lebih lanjut tentang titik akhir FIPS yang tersedia, lihat Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Kami sangat menyarankan agar Anda tidak pernah memasukkan informasi rahasia atau sensitif, seperti alamat email pelanggan Anda, ke dalam tag atau bidang teks bentuk bebas seperti bidang Nama. Ini termasuk ketika Anda bekerja dengan Client VPN atau lainnya Layanan AWS menggunakan konsol, APIAWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tag atau bidang teks bentuk bebas yang digunakan untuk nama dapat digunakan untuk penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, sebaiknya Anda

tidak menyertakan informasi kredensial di URL untuk memvalidasi permintaan Anda ke server tersebut.

Enkripsi dalam transit

AWS Client VPNmenyediakan koneksi aman dari lokasi mana pun menggunakan Transport Layer Security (TLS) 1.2 atau yang lebih baru.

Privasi lalu lintas jaringan Internet

Mengaktifkan akses antarjaringan

Anda dapat mengaktifkan klien untuk terhubung ke VPC Anda dan jaringan lainnya melalui titik akhir Client VPN. Untuk informasi selengkapnya dan contoh tambahan, lihat Skenario dan contoh untuk AWS Client VPN.

Pembatasan akses ke jaringan

Anda dapat mengonfigurasi titik akhir Client VPN Anda untuk membatasi akses ke sumber daya tertentu di VPC Anda. Untuk autentikasi berbasis pengguna, Anda juga dapat membatasi akses ke bagian jaringan Anda, berdasarkan grup pengguna yang mengakses titik akhir Client VPN. Untuk informasi selengkapnya, lihat Batasi akses ke jaringan Anda menggunakan AWS Client VPN.

Autentikasi klien

Autentikasi diimplementasikan pada titik pertama masuk ke dalam AWS Cloud. Hal ini digunakan untuk menentukan apakah klien diizinkan untuk terhubung ke titik akhir Client VPN. Jika autentikasi berhasil, klien terhubung ke titik akhir Client VPN dan membuat sesi VPN. Jika autentikasi gagal, hubungan ditolak dan klien dicegah dari membangun sesi VPN.

Client VPN menawarkan jenis autentikasi klien berikut:

- Autentikasi direktori aktif (berbasis pengguna)
- Autentikasi bersama (berbasis sertifikat)
- Sistem masuk tunggal (autentikasi federasi berbasis SAML) (berbasis pengguna)

Manajemen identitas dan akses untuk AWS Client VPN

(IAM) AWS Identity and Access Management adalah Layanan AWS yang membantu seorang administrator dalam mengendalikan akses ke sumber daya AWS secara aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Client VPN. IAM adalah sebuah layanan Layanan AWS yang dapat Anda gunakan tanpa dikenakan biaya tambahan.

Topik

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Client VPN.

Pengguna layanan — Jika Anda menggunakan layanan Client VPN untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensyal dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Client VPN 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 Client VPN, lihatMemecahkan masalah identitas dan AWS akses Client VPN.

Administrator layanan — Jika Anda bertanggung jawab atas sumber daya Client VPN di perusahaan Anda, Anda mungkin memiliki akses penuh ke Client VPN. Tugas Anda adalah menentukan fitur dan sumber daya Client VPN mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Client VPN, lihatBagaimana AWS Client VPN bekerja dengan IAM.

Administrator IAM — Jika Anda seorang administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Client VPN. Untuk melihat contoh

kebijakan berbasis identitas Client VPN yang dapat Anda gunakan di IAM, lihat. Contoh kebijakan berbasis identitas untuk Client VPN AWS

Mengautentikasi dengan identitas

Autentikasi merupakan cara Anda untuk masuk ke AWS dengan menggunakan kredensial identitas Anda. Anda harus terautentikasi (masuk keAWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengambil peran IAM.

Anda dapat masuk ke AWS sebagai identitas terfederasi dengan menggunakan kredensial yang disediakan melalui sumber identitas. AWS IAM Identity Center Para pengguna (Pusat Identitas IAM), otentikasi sign-on tunggal perusahaan Anda, dan kredensial Google atau Facebook Anda merupakan contoh identitas terfederasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas dengan menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil suatu peran.

Tergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal akses AWS. Untuk informasi selengkapnya tentang masuk ke AWS, silakan lihat Cara masuk ke Akun AWS Anda di Panduan Pengguna AWS Sign-In.

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 peralatan AWS, maka Anda harus menandatangani sendiri permintaan tersebut. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, silakan lihat Menandatangani permintaan API AWS di Panduan Pengguna IAM.

Terlepas dari metode autentikasi yang Anda gunakan, Anda mungkin juga diminta untuk menyediakan informasi keamanan tambahan. Sebagai contoh, AWS menyarankan supaya Anda menggunakan autentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, silakan lihat Autentikasi multi-faktor di Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) di AWS di Panduan Pengguna IAM.

Pengguna root Akun AWS

Ketika Anda membuat Akun AWS, Anda memulai dengan satu identitas masuk yang memiliki akses ke semua Layanan AWS dan sumber daya di akun tersebut. Identitas ini disebut pengguna root Akun AWS dan diakses dengan cara masuk ke alamat email dan kata sandi yang Anda gunakan

untuk membuat akun. Kami sangat menyarankan 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, silakan lihat Tugas yang memerlukan kredensial pengguna root di Panduan Pengguna IAM.

Identitas terfederasi

Praktik terbaiknya berupa, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensial temporer.

Identitas terfederasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, dikenal sebagai AWS Directory Service, direktori Pusat Identitas, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensial yang disediakan melalui sumber identitas. Ketika identitas terfederasi mengakses Akun AWS, identitas tersebut mengambil peran, dan peran memberikan kredensial temporer.

Untuk pengelolaan akses terpusat, kami sarankan Anda menggunakanAWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua Akun AWS Anda dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, silakan lihat Apakah Pusat Identitas IAM itu? di User Guide AWS IAM Identity Center.

Pengguna dan Grup IAM

Pengguna IAM adalah identitas dalam Akun AWS Anda yang memiliki izin khusus untuk satu orang atau aplikasi. Apabila memungkinkan, kami menyarankan untuk mengandalkan pada kredensial temporer alih-alih membuat pengguna IAM yang memiliki kredensyal jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami menyarankan Anda memutar kunci akses. Untuk informasi selengkapnya, silakan lihat Memutar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang di Panduan Pengguna IAM.

Grup IAM adalah identitas yang menerangkan secara spesifik kumpulan pengguna IAM. Anda tidak dapat masuk sebagai kelompok. Anda dapat menggunakan grup untuk menerangkan secara spesifik izin untuk beberapa pengguna sekaligus. Grup membuat izin lebih mudah dikelola untuk sekelompok besar pengguna. Sebagai contoh, Anda dapat memiliki grup yang diberi nama AdminIAM dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran tersebut dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial temporer. Untuk mempelajari selengkapnya, silakan lihat Kapan harus membuat pengguna IAM (alih-alih peran) di Panduan Pengguna IAM.

Peran IAM

Peran IAM merupakan identitas dalam Akun AWS Anda yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat menggunakan peran IAM untuk sementara dalam AWS Management Console dengan berganti peran. Anda dapat mengambil peran dengan cara memanggil operasi API AWS CLI atau AWS atau menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, silakan lihat menggunakan peran IAM di Panduan Pengguna IAM.

IAM role dengan kredensial temporer berguna dalam situasi berikut:

- Akses pengguna gabungan – Untuk menetapkan izin ke sebuah identitas terfederasi, Anda harus membuat sebuah peran dan menentukan izin untuk peran tersebut. Ketika identitas gabungan terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberikan izin yang ditentukan oleh peran. Untuk informasi tentang peran-peran untuk federasi, silakan lihat Membuat sebuah peran untuk Penyedia Identitas pihak ketiga di Panduan Pengguna IAM. Jika Anda menggunakan Pusat Identitas IAM, Anda mengonfigurasi serangkain izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM mengkorelasikan izin yang diatur ke peran dalam IAM. Untuk informasi tentang rangkaian izin, silakan lihat Rangkaian izin di Panduan Pengguna AWS IAM Identity Center.
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM untuk sementara mengambil izin berbeda untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (pengguna utama tepercaya) di akun berbeda untuk mengakses sumber daya yang ada di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, pada beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan suatu peran sebagai proksi). Untuk mempelajari perbedaan antara kebijakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, silakan lihat Bagaimana peran IAM role berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.
- Akses lintas layanan – Sebagian Layanan AWS menggunakan fitur di Layanan AWS lainnya. Sebagai contoh, ketika Anda melakukan panggilan dalam suatu layanan, lazim pada layanan

tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Suatu layanan mungkin melakukan hal tersebut menggunakan izin pengguna utama panggilan, menggunakan peran layanan, atau peran tertaut layanan.

- Sesi akses maju (FAS) – Ketika Anda menggunakan pengguna IAM atau peran IAM untuk melakukan tindakan-tindakan di AWS, Anda akan dianggap sebagai seorang pengguna utama. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian dilanjutkan oleh tindakan lain pada layanan yang berbeda. FAS menggunakan izin dari pengguna utama untuk memanggil Layanan AWS, yang dikombinasikan dengan Layanan AWS yang diminta untuk membuat pengajuan ke layanan hilir. Permintaan FAS hanya diajukan ketika sebuah layanan menerima pengajuan yang memerlukan interaksi dengan Layanan AWS lain atau sumber daya lain untuk diselesaikan. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, silakan lihat Meneruskan sesi akses.
- Peran layanan – Sebuah peran layanan adalah sebuah peran IAM yang dijalankan oleh suatu layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, silakan lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
- Peran tertaut layanan – Peran tertaut layanan adalah tipe peran layanan yang tertaut dengan Layanan AWS. Layanan tersebut dapat menjalankan peran untuk melakukan sebuah tindakan atas nama Anda. Peran tertaut layanan akan muncul di Akun AWS Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran tertaut layanan.

- Aplikasi yang berjalan di Amazon EC2 – Anda dapat menggunakan peran IAM untuk mengelola kredensial temporer untuk aplikasi yang berjalan di instans EC2 dan mengajukan permintaan AWS CLI atau API AWS. Cara ini lebih baik daripada menyimpan kunci akses dalam instans EC2. Untuk menugaskan sebuah peran AWS ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda dapat membuat sebuah profil instans yang dilampirkan ke instans. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 untuk mendapatkan kredensial sementara. Untuk informasi selengkapnya, silakan lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di instans Amazon EC2 di Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, silakan lihat Kapan harus membuat peran IAM (alih-alih pengguna) di Panduan Pengguna IAM.

Mengelola kebijakan menggunakan akses

Anda mengendalikan akses di AWS dengan membuat kebijakan dan melampirkannya ke identitas atau sumber daya AWS. Kebijakan adalah objek di AWS yang, ketika terkait dengan identitas atau sumber daya, akan menentukan izinnya. AWS mengevaluasi kebijakan-kebijakan tersebut ketika seorang pengguna utama (pengguna, root user, atau sesi peran) mengajukan permintaan. Izin dalam kebijakan menentukan apakah permintaan diberikan atau ditolak. Sebagian besar kebijakan disimpan di AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, silakan lihat Gambaran Umum kebijakan JSON di Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses pada apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

Secara bawaan, para pengguna dan peran tidak memiliki izin. Untuk mengabulkan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian akan dapat menambahkan kebijakan IAM ke peran, dan para pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk pengoperasiannya. Sebagai contoh, anggap saja Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole` . Pengguna dengan kebijakan tersebut dapat memperoleh informasi peran dari AWS Management Console, AWS CLI, atau APIAWS.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, misalnya pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol apa yang pengguna tindakan dan peran dapat kerjakan, pada sumber daya mana, dan dalam keadaan apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, silakan lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan terkelola. Kebijakan inline ditanam secara langsung ke pengguna tunggal, grup, atau peran. Kebijakan terkelola adalah kebijakan yang berdiri sendiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran di Akun AWS Anda. Kebijakan terkelola mencakup kebijakan terkelola AWS dan kebijakan terkelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan inline, silakan lihat Memilih antara kebijakan terkelola dan kebijakan inline diPanduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan-kebijakan berbasis sumber daya adalah kebijakan terpercaya peran IAM 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 yang dilampiri kebijakan, kebijakan tersebut menentkan tindakan apa yang dapat dilakukan oleh pengguna utama yang ditentukan di sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan pengguna utama dalam kebijakan berbasis sumber daya. Pengguna utama dapat mencakup akun, pengguna, peran, pengguna gabungan, atau Layanan AWS.

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan terkelola AWS dari IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACL)

Daftar kontrol akses (ACL) mengendalikan pengguna utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan-kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh-contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, silakan lihat Gambaran umum daftar kontrol akses (ACL) di Panduan Pengembang Layanan Penyimpanan Ringkas Amazon.

Tipe-tipe kebijakan lain

AWS mendukung tipe kebijakan tambahan, yang kurang umum. Tipe-tipe kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh tipe kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batas 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 menindihi izin. Untuk informasi selengkapnya tentang batasan izin, silakan lihat Batasan izin untuk entitas IAM di Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) – SCP adalah kebijakan JSON yang menentukan izin maksimum untuk sebuah organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations

adalah layanan untuk mengelompokkan dan secara terpusat mengelola beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di suatu organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau ke semua akun Anda. SCP membatasi izin untuk entitas dalam akun anggota, termasuk setiap Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organisasi dan SCP, silakan lihat Cara kerja SCP di Panduan Pengguna AWS Organizations.

- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara terprogram untuk peran atau pengguna gabungan. Izin sesi yang dihasilkan adalah perpotongan kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga dapat berasal dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini menindihi izin. Untuk informasi selengkapnya, silakan lihat Kebijakan sesi di Panduan Pengguna IAM.

Berbagai tipe kebijakan

Ketika beberapa tipe kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan ketika beberapa tipe kebijakan dilibatkan, silakan lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana AWS Client VPN bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Client VPN, pelajari fitur IAM apa saja yang tersedia untuk digunakan dengan Client VPN.

Fitur IAM yang dapat Anda gunakan dengan AWS Client VPN

Fitur IAM	Dukungan Client VPN
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya

Fitur IAM	Dukungan Client VPN
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
ACL	Tidak
ABAC (tag dalam kebijakan)	Tidak
Kredensial temporer	Ya
Izin-izin pengguna utama	Ya
Peran layanan	Ya
Peran tertaut layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Client VPN dan AWS layanan lainnya dengan sebagian besar fitur IAM, lihat AWSlayanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk Client VPN

Mendukung kebijakan berbasis identitas	Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, misalnya pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol apa yang pengguna tindakan dan peran dapat kerjakan, pada sumber daya mana, dan dalam keadaan apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, silakan lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta persyaratan yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Anda tidak dapat menentukan secara spesifik pengguna utama dalam sebuah kebijakan berbasis identitas karena pengguna utama berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, silakan lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk Client VPN

Untuk melihat contoh kebijakan berbasis identitas Client VPN, lihat. Contoh kebijakan berbasis identitas untuk Client VPN AWS

Kebijakan berbasis sumber daya dalam Client VPN

Mendukung kebijakan berbasis sumber daya	Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan-kebijakan berbasis sumber daya adalah kebijakan terpercaya peran IAM 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 yang dilampiri kebijakan, kebijakan tersebut menentkan tindakan apa yang dapat dilakukan oleh pengguna utama yang ditentukan di sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan pengguna utama dalam kebijakan berbasis sumber daya. Pengguna utama dapat mencakup akun, pengguna, peran, pengguna gabungan, atau Layanan AWS.

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai pengguna utama dalam kebijakan berbasis sumber daya. Menambahkan pengguna utama akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika pengguna utama dan sumber daya berada dalam Akun AWS yang berbeda, Administrator IAM di akun tepercaya juga harus memberikan izin kepada entitas pengguna utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses kepada pengguna utama dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, silakan lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Tindakan kebijakan untuk Client VPN

Mendukung tindakan kebijakan	Ya

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses pada apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan-tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan-tindakan kebijakan biasanya memiliki nama yang sama sebagaimana operasi API AWS yang dikaitkan padanya. Ada beberapa pengecualian, misalnya tindakan yang memiliki izin saja yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam sebuah kebijakan. Tindakan-tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam suatu kebijakan untuk memberikan izin guna melakukan operasi yang terkait.

Untuk melihat daftar tindakan Client VPN, lihat Tindakan yang ditentukan oleh AWS Client VPN di Referensi Otorisasi Layanan.

Tindakan kebijakan di Client VPN menggunakan awalan berikut sebelum tindakan:

```
ec2
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan-tindakan tersebut dengan koma.

```
"Action": [
      "ec2:action1",
      "ec2:action2"
         ]
```

Untuk melihat contoh kebijakan berbasis identitas Client VPN, lihat. Contoh kebijakan berbasis identitas untuk Client VPN AWS

Sumber daya kebijakan untuk Client VPN

Mendukung sumber daya kebijakan	Ya

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses pada apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

Elemen kebijakan JSON `Resource` menentukan objek atau objek-objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan entah elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan-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 mengindikasikan bahwa pernyataan tersebut berlaku bagi semua sumber daya.

```
"Resource": "*"
```

Untuk melihat daftar jenis sumber daya Client VPN dan ARNnya, lihat Sumber daya yang ditentukan oleh AWS Client VPN dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang ditentukan oleh AWS Client VPN.

Untuk melihat contoh kebijakan berbasis identitas Client VPN, lihat. Contoh kebijakan berbasis identitas untuk Client VPN AWS

Kunci kondisi kebijakan untuk Client VPN

Mendukung kunci-kunci persyaratan kebijakan spesifik layanan	Ya

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses pada apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan syarat yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator syarat, misalnya sama dengan atau kurang dari, untuk mencocokkan syarat 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 dengan menggunakan

operasi AND yang logis. Jika Anda menentukan beberapa niilai untuk satu kunci persyaratan, maka AWS akan mengevaluasi syarat tersebut menggunakan operasi OR yang logis. Semua persyaratan harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan syarat. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tag yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, silakan lihat Elemen kebijakan IAM: variabel dan tag di Panduan Pengguna IAM.

AWS mendukung kunci-kunci syarat global dan kunci-kunci syarat spesifik layanan. Untuk melihat semua kunci persyaratan global AWS, silakan lihat kunci konteks syarat global AWS di Panduan Pengguna IAM.

Untuk melihat daftar kunci kondisi Client VPN, lihat Kunci kondisi untuk AWS Client VPN di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh AWS Client VPN.

Untuk melihat contoh kebijakan berbasis identitas Client VPN, lihat. Contoh kebijakan berbasis identitas untuk Client VPN AWS

ACL di Client VPN

Mendukung ACL	Tidak

Daftar kontrol akses (ACL) mengendalikan pengguna utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan-kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

ABAC dengan Client VPN

Mendukung ABAC (tag dalam kebijakan)	Tidak

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Di AWS, atribut-atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak sumber daya AWS. Pemberian tag ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi-

operasi ketika tag milik pengguna utama cocok dengan tag yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi dimana pengelolaan kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tag di elemen syarat dari sebuh kebijakan dengan menggunakan kunci-kunci persyaratan `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci-kunci persyaratan untuk setiap jenis sumber daya, maka nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci persyaratan untuk hanya beberapa jenis sumber daya, maka nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, silakan lihat Apa itu ABAC? di Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, silakan lihat Menggunakan kontrol akses berbasis atribut (ABAC) di Panduan Pengguna IAM.

Menggunakan kredensyal sementara dengan Client VPN

Mendukung kredensial temporer	Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk dengan menggunakan kredensial temporer. Sebagai informasi tambahan, termasuk tentang Layanan AWS mana saja yang berfungsi dengan kredensial temporer, silakan lihat Layanan AWS yang berfungsi dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredensial temporer jika Anda masuk ke AWS Management Console dengan menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Sebagai contoh, ketika Anda mengakses AWS dengan menggunakan tautan masuk tunggal (SSO) milik perusahaan Anda, proses itu secara otomatis akan membuat kredensial temporer. Anda juga akan secara otomatis membuat kredensial temporer ketika Anda masuk ke konsol sebagai seorang pengguna dan kemudian beralih peran. Untuk informasi selengkapnya tentang peralihan peran, silakan lihat Peralihan peran (konsol) di Panduan Pengguna IAM.

Anda dapat secara manual membuat kredensial temporer menggunakan AWS CLI atau API AWS. Anda kemudian dapat menggunakan kredensial temporer tersebut untuk mengakses AWS. AWS menyarankan agar Anda secara dinamis membuat kredensial temporer alih-alih menggunakan kunci

akses jangka panjang. Untuk informasi selengkapnya, silakan lihat Kredensial keamanan temporer di IAM.

Izin utama lintas layanan untuk Client VPN

Mendukung sesi akses maju (FAS)	Ya

Saat Anda menggunakan pengguna IAM atau peran IAM untuk mengerjakan tindakan di AWS, Anda akan dianggap sebagai pengguna utama. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian dilanjutkan oleh tindakan lain pada layanan yang berbeda. FAS menggunakan izin dari pengguna utama untuk memanggil Layanan AWS, yang dikombinasikan dengan Layanan AWS yang diminta untuk membuat pengajuan ke layanan hilir. Permintaan FAS hanya diajukan ketika sebuah layanan menerima pengajuan yang memerlukan interaksi dengan Layanan AWS lain atau sumber daya lain untuk diselesaikan. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, silakan lihat Meneruskan sesi akses.

Peran layanan untuk Client VPN

Mendukung peran layanan	Ya

Peran layanan adalah sebuah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak fungsionalitas Client VPN. Edit peran layanan hanya jika Client VPN memberikan panduan untuk melakukannya.

Peran terkait layanan untuk Client VPN

Mendukung peran yang terhubung dengan layanan	Ya

Peran yang tertaut layanan adalah jenis peran layanan yang tertaut dengan Layanan AWS. Layanan tersebut dapat menjalankan peran untuk melakukan sebuah tindakan atas nama Anda. Peran tertaut layanan akan muncul di Akun AWS Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran tertaut layanan.

Untuk detail tentang pembuatan atau pengelolaan peran yang terhubung dengan layanan, lihat Layanan AWS yang bekerja dengan IAM. Cari layanan dalam tabel yang memiliki `Yes` di kolom Service-linked role (Peran yang terhubung dengan layanan). Pilih tautan Ya untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Contoh kebijakan berbasis identitas untuk Client VPN AWS

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Client VPN. Pengguan dan peran tersebut juga tidak dapat melakukan tugas dengan menggunakan API AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS. Untuk mengabulkan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian akan dapat menambahkan kebijakan IAM ke peran, dan para pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, silakan lihat Membuat kebijakan IAM di Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Client VPN, termasuk format ARN untuk setiap jenis sumber daya, lihat Tindakan, sumber daya, dan kunci kondisi untuk AWS Client VPN dalam Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Izinkan para pengguna untuk melihat izin mereka sendiri

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Client VPN di akun Anda. Tindakan ini mengenakan biaya kepada Anda Akun AWS. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan terkelola AWS dan beralih ke izin dengan hak akses paling rendah – Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan terkelola AWS yang memberikan izin untuk banyak kasus penggunaan umum. Kebijakan tedapat di Akun AWS Anda. Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan AWS yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, silakan lihat kebijakan-kebijakan terkelola AWS atau kebijakan-kebijakan terkelola AWS untuk fungsi tugas di Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukan ini dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan pengguna IAM untuk mengajukan izin, silakan lihat Kebijakan dan izin di IAM di Panduan Pengguna IAM.
- Gunakan syarat dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu syarat ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis syarat kebijakan untuk menentukan bahwa semua pengajuan harus dikirim menggunakan SSL. Anda juga dapat menggunakan syarat untuk memberi akses ke tindakan layanan jika digunakan melalui Layanan AWS yang spesifk, sepertiAWS CloudFormation. Untuk informasi selengkapnya, silakan lihat Elemen kebijakan JSON IAM: Syarat di Panduan Pengguna IAM.
- Gunakan Analizer Akses IAM untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – Analizer Akses IAM memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. Analizer Akses IAM menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, silakan lihat validasi kebijakan Analizer Akses IAM di Panduan Pengguna IAM.
- Memerlukan autentikasi multi-faktor (MFA) – Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Akun AWS Anda, aktifkan MFA untuk keamanan tambahan.

Untuk meminta MFA ketika operasi API dipanggil, tambahkan syarat MFA pada kebijakan Anda. Untuk informasi selengkapnya, silakan lihat Mengonfigurasi akses API yang diproteksi MFA di Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, silakan lihat Praktik terbaik keamanan di IAM di Panduan Pengguna IAM.

Izinkan para pengguna untuk melihat izin mereka sendiri

Contoh ini menunjukkan cara Anda dapat membuat kebijakan yang mengizinkan para pengguna IAM untuk melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan pada konsol atau secara terprogram menggunakan API AWS CLI atau AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

Memecahkan masalah identitas dan AWS akses Client VPN

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Client VPN dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di Client VPN
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Client VPN saya

Saya tidak berwenang untuk melakukan tindakan di Client VPN

Jika Anda menerima pesan galat bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh galat berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya *`my-example-widget`* rekaan, tetapi tidak memiliki izin `ec2:`*`GetWidget`* rekaan.

```
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 membutuhkan bantuan, hubungi administrator AWS Anda. Administrator Anda adalah orang yang memberikan kredensial masuk Anda.

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 Client VPN.

Sebagian Layanan AWS mengizinkan Anda untuk memberikan peran yang sudah ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran tertaut-layanan. Untuk melakukan tindakan tersebut, Anda harus memiliki izin untuk memberikan peran pada layanan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Client VPN. 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 membutuhkan bantuan, hubungi administrator AWS Anda. Administrator Anda adalah orang yang memberikan kredensial masuk Anda.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Client VPN saya

Anda dapat membuat peran yang dapat digunakan para pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi akses kepada orang ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa hal berikut:

- Untuk mengetahui apakah Client VPN mendukung fitur-fitur ini, lihatBagaimana AWS Client VPN bekerja dengan IAM.
- Untuk mempelajari cara memberikan akses ke sumber daya di seluruh Akun AWS yang Anda miliki, silakan lihat Menyediakan akses ke pengguna IAM di Akun AWS lainnya yang Anda miliki di Panduan Pengguna IAM.

- Untuk mempelajari cara memberikan akses ke sumber daya Anda ke pihak ketiga Akun AWS, silakan lihat Menyediakan akses ke akun Akun AWS yang dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, silakan lihat Menyediakan akses ke pengguna terautentikasi eksternal (gabungan identitas) di Panduan Pengguna IAM .
- Untuk mempelajari perbedaan antara penggunaan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Perbedaan IAM role dan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Menggunakan peran terkait layanan untuk Client VPN

AWSClient VPN menggunakanAWS Identity and Access Management(SAYA)peran terkait layanan. peran terkait layanan adalah peran terkait layanan yang terkait layanan, terkait layanan, terkait layanan. peran terkait layanan ditentukan sebelumnya oleh Client VPN, termasuk izin yang diperlukan layanan untuk mengasumsikan layananAWSlayanan atas nama Anda.

Topik

- Menggunakan peran untuk Client VPN
- Menggunakan peran untuk otorisasi koneksi

Menggunakan peran untuk Client VPN

AWSClient VPN menggunakanAWS Identity and Access Management(SAYA)peran terkait layanan. peran terkait layanan adalah peran terkait layanan yang terkait layanan, terkait layanan, terkait layanan. peran terkait layanan ditentukan sebelumnya oleh Client VPN, termasuk izin yang diperlukan layanan untuk mengasumsikan layananAWSlayanan atas nama Anda.

Perannya terkait layanan membuat pengaturan Client VPN lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan. Client VPN menentukan izin peran terkait layanan, kecuali jika ditentukan berbeda, hanya Client yang dapat mengasumsikan perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi sumber daya Client VPN karena Anda tidak dapat secara tidak sengaja mengasumsikan izin untuk mengakses sumber.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat Layanan AWS yang Bekerja bersama IAM dan mencari layanan yang memiliki Ya dalam Peran Terkait Layanan. Pilih Ya dengan tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Izin peran terkait layanan untuk Client VPN

Client VPN menggunakan peran terkait layananAWSServiceRoleForClientVPN— Izinkan Client VPN untuk membuat dan mengelola sumber daya yang terkait dengan koneksi VPN Anda.

AWSServiceRoleForClientVPN peran terkait layanan mempercayakan layanan berikut untuk menjalankan peran tersebut:

- `clientvpn.amazonaws.com`

Kebijakan izin peran terkait peran terkait peranClientVPNServiceRolePolicymemungkinkan Client VPN untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: `ec2:CreateNetworkInterface` pada `Resource: "*"`
- Tindakan: `ec2:CreateNetworkInterfacePermission` pada `Resource: "*"`
- Tindakan: `ec2:DescribeSecurityGroups` pada `Resource: "*"`
- Tindakan: `ec2:DescribeVpcs` pada `Resource: "*"`
- Tindakan: `ec2:DescribeSubnets` pada `Resource: "*"`
- Tindakan: `ec2:DescribeInternetGateways` pada `Resource: "*"`
- Tindakan: `ec2:ModifyNetworkInterfaceAttribute` pada `Resource: "*"`
- Tindakan: `ec2:DeleteNetworkInterface` pada `Resource: "*"`
- Tindakan: `ec2:DescribeAccountAttributes` pada `Resource: "*"`
- Tindakan: `ds:AuthorizeApplication` pada `Resource: "*"`
- Tindakan: `ds:DescribeDirectories` pada `Resource: "*"`
- Tindakan: `ds:GetDirectoryLimits` pada `Resource: "*"`
- Tindakan: `ds:UnauthorizeApplication` pada `Resource: "*"`
- Tindakan: `logs:DescribeLogStreams` pada `Resource: "*"`
- Tindakan: `logs:CreateLogStream` pada `Resource: "*"`
- Tindakan: `logs:PutLogEvents` pada `Resource: "*"`

- Tindakan: `logs:DescribeLogGroups` pada `Resource: "*"`
- Tindakan: `acm:GetCertificate` pada `Resource: "*"`
- Tindakan: `acm:DescribeCertificate` pada `Resource: "*"`
- Tindakan: `iam:GetSAMLProvider` pada `Resource: "*"`
- Tindakan: `lambda:GetFunctionConfiguration` pada `Resource: "*"`

Anda harus mengonfigurasikan izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, menyunting, atau menghapus peran terhubung dengan layanan. Untuk informasi selengkapnya, lihat Izin peran tertaut layanan dalam Panduan Pengguna IAM.

Membuat peran terkait layanan untuk Client VPN

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat titik akhir Client VPN pertama di akun Anda denganAWS Management Console,AWS CLI, atauAWSAPI, Client VPN membuat peran terkait layanan untuk Anda.

Jika Anda menghapus peran tertaut layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda membuat titik akhir Client VPN di akun, Client VPN membuat peran terkait layanan untuk Anda.

Mengedit peran terkait layanan untuk Client VPN

Client VPN tidak memungkinkan Anda mengasumsikan AWSServiceRoleForClientVPN peran terkait layanan. Setelah Anda membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran yang terkait dengan layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Client VPN

Jika Anda tidak perlu lagi menggunakan Client VPN, sebaiknya Anda mengasumsikanAWSServiceRoleForClientVPNperan terkait layanan.

Anda harus terlebih dahulu menghapus sumber daya Client VPN yang terkait. Ini memastikan bahwa Anda tidak menghapus izin untuk mengakses sumber daya secara tidak sengaja.

Gunakan konsol IAM, CLI IAM, atau API IAM untuk menghapus peran layanan terkait. Untuk informasi lebih lanjut, lihat Menghapus Peran Terkait Layanan di Panduan Pengguna IAM.

Wilayah terkait layanan Client VPN

Client VPN mendukung peran terkait layanan di semua wilayah tempat layanan tersedia. Untuk informasi selengkapnya, lihatAWSdaerah dan titik akhir.

Menggunakan peran untuk otorisasi koneksi

AWSClient VPN menggunakanAWS Identity and Access Management(SAYA)peran terkait layanan. peran terkait layanan adalah peran terkait layanan yang terkait layanan, terkait layanan, terkait layanan. peran terkait layanan ditentukan sebelumnya oleh Client VPN, termasuk izin yang diperlukan layanan untuk mengasumsikan layananAWSlayanan atas nama Anda.

Perannya terkait layanan membuat pengaturan Client VPN lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan. Client VPN menentukan izin peran terkait layanan, kecuali jika ditentukan berbeda, hanya Client yang dapat mengasumsikan perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi sumber daya Client VPN karena Anda tidak dapat secara tidak sengaja mengasumsikan izin untuk mengakses sumber.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat Layanan AWS yang Bekerja bersama IAM dan mencari layanan yang memiliki Ya dalam Peran Terkait Layanan. Pilih Ya dengan tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Izin peran terkait layanan untuk Client VPN

Client VPN menggunakan peran terkait layananAWSServiceRoleForClientVPNConnections— Peran Tertaut Layanan untuk koneksi Client VPN.

The AWSServiceRoleForClientVPNConnections peran terkait layanan mempercayai layanan untuk mengasumsikan peran terkait layanan:

- `clientvpn-connections.amazonaws.com`

Kebijakan izin peran bernama ClientVPNServiceConnectionsRolePolicy memungkinkan Client VPN untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: `lambda:InvokeFunction` pada `arn:aws:lambda:*:*:function:AWSClientVPN-*`

Anda harus mengonfigurasikan izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, menyunting, atau menghapus peran terhubung dengan layanan. Untuk informasi selengkapnya, lihat Izin peran tertaut layanan dalam Panduan Pengguna IAM.

Membuat peran terkait layanan untuk Client VPN

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat titik akhir Client VPN pertama di akun Anda denganAWS Management Console,AWS CLI, atauAWSAPI, Client VPN membuat peran terkait layanan untuk Anda.

Jika Anda menghapus peran tertaut layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda membuat titik akhir Client VPN di akun, Client VPN membuat peran terkait layanan untuk Anda.

Mengedit peran terkait layanan untuk Client VPN

Client VPN tidak memungkinkan Anda mengasumsikan AWSServiceRoleForClientVPNConnections peran terkait layanan. Setelah Anda membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran yang terkait dengan layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Client VPN

Jika Anda tidak perlu lagi menggunakan Client VPN, sebaiknya Anda mengasumsikanAWSServiceRoleForClientVPNConnectionsperan terkait layanan.

Anda harus terlebih dahulu menghapus sumber daya Client VPN yang terkait. Ini memastikan bahwa Anda tidak menghapus izin untuk mengakses sumber daya secara tidak sengaja.

Gunakan konsol IAM, CLI IAM, atau API IAM untuk menghapus peran layanan terkait. Untuk informasi lebih lanjut, lihat Menghapus Peran Terkait Layanan di Panduan Pengguna IAM.

Wilayah terkait layanan Client VPN

Client VPN mendukung peran terkait layanan di semua wilayah tempat layanan tersedia. Untuk informasi selengkapnya, lihatAWSdaerah dan titik akhir.

Ketahanan di AWS Client VPN

Infrastruktur global AWS dibangun di sekitar Wilayah dan Availability Zone AWS. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung

dengan jaringan berlatensi rendah, throughput yang tinggi, dan sangat redundan. Dengan Availability Zone, Anda dapat mendesain dan mengoperasikan aplikasi dan basis data yang secara otomatis mengalami kegagalan di antara zona tanpa gangguan. Availability Zone lebih tersedia, memiliki toleransi kesalahan, dan dapat diskalakan dibandingkan dengan satu atau beberapa infrastruktur pusat data tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zones, lihat Infrastruktur Global AWS.

Terlebih lagi pada infrastruktur global AWS, AWS Client VPN menawarkan beberapa fitur yang dapat membantu dalam mendukung ketahanan serta kebutuhan cadangan data Anda.

Beberapa jaringan target untuk ketersediaan yang tinggi

Anda mengaitkan jaringan target dengan titik akhir Client VPN untuk memungkinkan klien membuat sesi VPN. Jaringan target adalah subnet di VPC Anda. Setiap subnet yang Anda kaitkan dengan titik akhir Client VPN harus dimiliki oleh Availability Zone yang berbeda. Anda dapat mengaitkan beberapa subnet dengan titik akhir Client VPN untuk ketersediaan yang tinggi.

Keamanan infrastruktur dalam AWS Client VPN

Sebagai layanan yang dikelola,AWSClient VPN dilindungi olehAWSkeamanan jaringan global. Untuk informasi tentangAWSLayanan keamanan dan bagaimanaAWSmelindungi infrastruktur, lihatAWSKeamanan Cloud. Untuk mendesainAWSlingkungan menggunakan praktik terbaik untuk keamanan infrastruktur, lihatPerlindungan InfrastrukturdiPilar KeamananAWSKerangka Kerja yang Diarsiteksikan dengan Baik.

Anda menggunakan panggilan API yang dipublikasikan AWS untuk mengakses Client VPN melalui jaringan. Klien harus mendukung hal-hal berikut:

- Transport Layer Secrecy (TLS). Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- suite cipher dengan Perfect Forward Secrecy (PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan sistem yang lebih baru mendukung mode ini.

Selain itu, permintaan harus ditandatangani menggunakan access key ID dan secret access key yang terkait dengan principal IAM. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Praktik keamanan terbaik untuk AWS Client VPN

AWS Client VPN menyediakan sejumlah fitur keamanan yang dapat dipertimbangkan ketika Anda mengembangkan dan menerapkan kebijakan keamanan Anda sendiri. Praktik terbaik berikut adalah pedoman umum dan tidak mewakili solusi keamanan yang lengkap. Karena praktik terbaik ini mungkin tidak sesuai atau cukup untuk lingkungan Anda, jadikan sebagai pertimbangan dan bukan sebagai rekomendasi.

Aturan otorisasi

Gunakan aturan otorisasi untuk membatasi pengguna mana yang dapat mengakses jaringan Anda. Untuk informasi selengkapnya, lihat Aturan otorisasi.

Grup keamanan

Gunakan grup keamanan untuk mengontrol sumber daya mana yang dapat diakses pengguna di VPC Anda. Untuk informasi selengkapnya, lihat Grup keamanan.

Daftar pencabutan sertifikat klien

Gunakan daftar pencabutan sertifikat klien untuk mencabut akses ke titik akhir Client VPN untuk sertifikat klien tertentu. Misalnya, saat pengguna keluar dari organisasi Anda. Untuk informasi selengkapnya, lihat Daftar pencabutan sertifikat klien.

Alat pemantauan

Gunakan alat pemantauan untuk melacak ketersediaan dan performa titik akhir Client VPN Anda. Untuk informasi selengkapnya, lihat PemantauanAWSClient VPN.

Identity and access management

Kelola akses ke sumber daya Client VPN dan API dengan menggunakan kebijakan IAM untuk pengguna IAM dan IAM role Anda. Untuk informasi selengkapnya, lihat Manajemen identitas dan akses untuk AWS Client VPN.

Pertimbangan IPv6 untukAWSClient VPN

Saat ini layanan Client VPN tidak mendukung perutean lalu lintas IPv6 melalui terowongan VPN. Namun, ada beberapa kasus ketika lalu lintas IPv6 harus diarahkan ke terowongan VPN untuk mencegah kebocoran IPv6. Kebocoran IPv6 dapat terjadi ketika IPv4 dan IPv6 diaktifkan dan

terhubung ke VPN, tetapi VPN tidak mengarahkan lalu lintas IPv6 ke terowongannya. Dalam hal ini, saat menghubungkan ke tujuan yang diaktifkan IPv6, Anda sebenarnya masih terhubung dengan alamat IPv6 yang disediakan oleh ISP Anda. Ini akan membocorkan alamat IPv6 asli. Petunjuk di bawah ini menjelaskan cara merutekan lalu lintas IPv6 ke terowongan VPN.

Arahan terkait IPv6 berikut harus ditambahkan ke file konfigurasi Client VPN Anda untuk mencegah kebocoran IPv6:

```
ifconfig-ipv6 arg0 arg1
route-ipv6 arg0
```

Contohnya mungkin:

```
ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1
route-ipv6 2000::/4
```

Dalam contoh ini,`ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1`akan mengatur alamat IPv6 perangkat terowongan lokal menjadi`fd15:53b6:dead::2`dan alamat IPv6 titik akhir VPN jarak jauh`fd15:53b6:dead::1`.

Perintah berikutnya,`route-ipv6 2000::/4`akan merutekan alamat IPv6.`2000:0000:0000:0000:0000:0000:0000:0000`kepada`2fff:ffff:ffff:ffff:ffff:ffff:ff`koneksi VPN.

> **Note**
>
> Untuk perutean perangkat “TAP” di Windows misalnya, parameter kedua`ifconfig-ipv6`akan digunakan sebagai target rute untuk`--route-ipv6`.

Organizations harus mengkonfigurasi dua parameter`ifconfig-ipv6`sendiri, dan dapat menggunakan alamat di`100::/64`(dari`0100:0000:0000:0000:0000:0000:0000:0000`kepada`0100:0000:0000:0000:fff`atau`fc00::/7`(dari`fc00:0000:0000:0000:0000:0000:0000:0000`kepada`fdff:ffff:ffff:ffff:f`Blok Alamat Hanya Buang, dan`fc00::/7`adalah Unik-Lokal.

Contoh lain:

```
ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1
```

```
route-ipv6 2000::/3
route-ipv6 fc00::/7
```

Dalam contoh ini, konfigurasi akan merutekan semua lalu lintas IPv6 yang saat ini dialokasikan ke koneksi VPN.

Verifikasi

Organisasi Anda kemungkinan akan memiliki tes sendiri. Verifikasi dasar adalah mengatur koneksi VPN terowongan penuh, lalu jalankan ping6 ke server IPv6 menggunakan alamat IPv6. Alamat IPv6 server harus berada dalam kisaran yang ditentukan oleh`route-ipv6`perintah. Tes ping ini seharusnya gagal. Namun, ini dapat berubah jika dukungan IPv6 ditambahkan ke layanan Client VPN di masa mendatang. Jika ping berhasil dan Anda dapat mengakses situs publik saat terhubung dalam mode terowongan penuh, Anda mungkin perlu melakukan pemecahan masalah lebih lanjut. Anda juga dapat menguji dengan menggunakan beberapa alat yang tersedia untuk umum seperti[ipleak.org](ipleak.org)juga.

PemantauanAWSClient VPN

Pemantauan adalah bagian penting dari pemeliharaan keandalan, ketersediaan, dan performa AWS Client VPN dan solusi AWS Anda lainnya. Anda dapat menggunakan fitur berikut ini untuk memantau titik akhir Client VPN Anda, menganalisis pola lalu lintas, dan memecahkan masalah dengan titik akhir Client VPN Anda.

Amazon CloudWatch

Memantau AWS sumber daya dan aplikasi yang Anda jalankan di AWS secara waktu nyata. Anda dapat mengumpulkan dan melacak metrik, membuat dasbor yang disesuaikan, dan mengatur alarm yang memberi tahu Anda atau mengambil tindakan saat metrik tertentu mencapai ambang batas yang ditentukan. Misalnya, Anda dapat memiliki CloudWatch melacak penggunaan CPU atau metrik lain dari instans Amazon EC2 Anda dan memulai instans baru secara otomatis jika diperlukan. Untuk informasi lebih lanjut, lihatAmazon CloudWatch Panduan Pengguna.

AWS CloudTrail

Menangkap panggilan API dan kejadian terkait yang dibuat atas nama Anda di akun AWS Anda dan kemudian mengirimkan berkas log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang memanggil AWS, alamat IP sumber yang melakukan panggilan, dan kapan panggilan tersebut terjadi. Untuk mengetahui informasi selengkapnya, lihat Panduan Pengguna AWS CloudTrail.

Amazon CloudWatch Log

Memungkinkan Anda untuk memantau upaya koneksi yang dilakukan pada titik akhir AWS Client VPN Anda. Anda dapat melihat upaya koneksi dan pengaturan ulang untuk koneksi Client VPN. Untuk upaya koneksi, Anda dapat melihat upaya koneksi yang berhasil dan gagal. Anda dapat menentukan CloudWatch Log aliran untuk mencatat detail koneksi. Untuk informasi selengkapnya, lihatPencatatan koneksidanAmazon CloudWatch Panduan Pengguna Log.

CloudWatch metrik untukAWS Client VPN

AWSClient VPN menerbitkan metrik berikut ke Amazon CloudWatch untuk titik akhir Client VPN Anda. Metrik dipublikasikan ke Amazon CloudWatch setiap lima menit.

Metrik	Deskripsi
ActiveConnectionsCount	Jumlah koneksi aktif ke titik akhir Client VPN. Unit: Count (Jumlah)
AuthenticationFailures	Jumlah kegagalan autentikasi untuk titik akhir Client VPN. Unit: Count (Jumlah)
CrlDaysToExpiry	Jumlah hari hingga Certificate Revocation List (CRL) yang dikonfigurasi pada titik akhir Client VPN berakhir. Unit: Hari
EgressBytes	Jumlah byte yang dikirim dari titik akhir Client VPN. Unit: Bita
EgressPackets	Jumlah paket yang dikirim dari titik akhir Client VPN. Unit: Count (Jumlah)
IngressBytes	Jumlah byte yang diterima oleh titik akhir Client VPN. Unit: Bita
IngressPackets	Jumlah paket yang diterima oleh titik akhir Client VPN. Unit: Count (Jumlah)
SelfServicePortalClientConfigurationDownloads	Jumlah unduhan file konfigurasi titik akhir Client VPN dari portal layanan mandiri. Unit: Jumlah

AWS Client VPN memublikasikan metrik penilaian postur berikut untuk titik akhir Client VPN Anda.

Metrik	Deskripsi
ClientConnectHandlerTimeouts	Jumlah permintaan waktu habis pada handler koneksi klien untuk koneksi ke titik akhir Client VPN. Unit: Count (Jumlah)
ClientConnectHandlerInvalidResponses	Jumlah respons tidak valid yang dikembalikan pada handler koneksi klien untuk koneksi ke titik akhir Client VPN. Unit: Count (Jumlah)
ClientConnectHandlerOtherExecutionErrors	Jumlah kesalahan tak terduga saat menjalank an handler koneksi klien untuk koneksi ke titik akhir Client VPN. Unit: Count (Jumlah)
ClientConnectHandlerThrottlingErrors	Jumlah pemanggilan kesalahan throttling pada handler koneksi klien untuk koneksi ke titik akhir Client VPN. Unit: Count (Jumlah)
ClientConnectHandlerDeniedConnections	Jumlah koneksi yang ditolak pada handler koneksi klien untuk koneksi ke titik akhir Client VPN. Unit: Count (Jumlah)
ClientConnectHandlerFailedServiceErrors	Jumlah kesalahan sisi layanan saat berjalan pada handler koneksi klien untuk koneksi ke titik akhir Client VPN. Unit: Jumlah

Anda dapat memfilter metrik untuk titik akhir Client VPN Anda berdasarkan titik akhir.

CloudWatch memungkinkan Anda untuk mengambil statistik tentang titik-titik data tersebut sebagai kumpulan data deret waktu yang menurut Anda metrik. Anggap metrik sebagai variabel untuk memantau, dan titik data sebagai nilai variabel tersebut dari waktu ke waktu. Setiap titik data memiliki timestamp terkait dan pengukuran unit opsional.

Anda dapat menggunakan metrik untuk memverifikasi bahwa sistem Anda bekerja sesuai harapan. Misalnya, Anda dapat membuat CloudWatch alarm untuk memantau metrik tertentu dan memulai tindakan (seperti mengirim notifikasi ke alamat email) jika metrik berada di luar rentang yang menurut Anda dapat diterima.

Untuk informasi lebih lanjut, lihatAmazon CloudWatch Panduan Pengguna.

Melihat metrik CloudWatch

Anda dapat melihat metrik untuk titik akhir Client VPN Anda sebagai berikut.

Untuk melihat metrik menggunakan CloudWatch konsol

Metrik dikelompokkan terlebih dahulu berdasarkan namespace layanan, kemudian berdasarkan berbagai kombinasi dimensi dalam setiap namespace.

1. Buka CloudWatch konsol dihttps://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, pilih Metrik.
3. Di bawah Semua metrik, pilih namespace metrik ClientVPN.
4. Untuk melihat metrik, pilih dimensi metrik berdasarkan titik akhir.

Untuk melihat metrik menggunakan AWS CLI

Pada prompt perintah, gunakan perintah berikut untuk mencantumkan metrik yang tersedia untuk Client VPN

```
aws cloudwatch list-metrics --namespace "AWS/ClientVPN"
```

CloudTrail log untukAWSClient VPN

AWSClient VPN terintegrasi denganAWS CloudTrailLayanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atauAWSlayanan di Client VPN. CloudTrail menangkap semua

panggilan API untuk Client VPN sebagai acara. Panggilan yang direkam mencakup panggilan dari konsol Client VPN dan panggilan kode ke operasi API Client VPN. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrailperistiwa ke bucket Amazon S3, termasuk acara untuk Client VPN. Jika Anda tidak mengonfigurasi jejak, Anda dapat melihat peristiwa terbaru di CloudTrail konsol diRiwayat acara. Gunakan informasi yang dikumpulkan oleh CloudTrail untuk menentukan permintaan yang dibuat untuk Client VPN, alamat IP yang meminta, pemohon, kapan dibuat, dan detail tambahan.

Untuk informasi lebih lanjut tentang CloudTrail, lihatAWS CloudTrailPanduan Pengguna.

Informasi Client VPN di CloudTrail

CloudTrail diaktifkan pada AndaAWSakun saat Anda membuat akun. Ketika aktivitas terjadi di Client VPN, aktivitas tersebut dicatat dalam CloudTrail Event bersama dengan lainnyaAWSacara layanan diRiwayat acara. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun AWS Anda. Untuk informasi selengkapnya, lihatMelihat Acara dengan CloudTrail Riwayat Acara.

Untuk catatan kejadian yang sedang berlangsung di akun AWS Anda, termasuk kejadian untuk Client VPN, buatlah jejak. SEBUAHjejakmenyalakan CloudTrail untuk mengirim file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di dalam konsol tersebut, jejak diterapkan ke semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Misalnya, Anda dapat mengonfigurasi lainnyaAWSLayanan untuk menganalisis dan bertindak atas data acara yang dikumpulkan di CloudTrail log. Untuk informasi selengkapnya, lihat yang berikut:

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

Semua tindakan Client VPN dicatat oleh CloudTrail dan didokumentasikan dalamReferensi API Amazon EC2. Misalnya, panggilan keCreateClientVpnEndpoint,AssociateClientVpnTargetNetwork, danAuthorizeClientVpnIngresstindakan menghasilkan entri di CloudTrail file log.

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

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

Untuk informasi lebih lanjut, lihat CloudTrail Elemen UserIdentity.

Memahami entri berkas log Client VPN

Jejak adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai berkas log ke bucket Amazon S3 yang Anda tentukan. CloudTrail File log berisi satu atau beberapa entri log. Peristuwa mewakili satu permintaan dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail File log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, sehingga file tersebut tidak muncul dalam urutan tertentu.

Untuk informasi lebih lanjut, lihat Mencatat panggilan API Amazon EC2, Amazon EBS, dan Amazon VPC dengan AWS CloudTrail di Referensi API Amazon EC2.

Kuota AWS Client VPN

AndaAWSAkun memiliki kuota berikut, yang sebelumnya disebut sebagai batasan, terkait dengan kuota berikut, yang sebelumnya disebut sebagai batasan, terkait dengan Client 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 kuota kuota untuk kuota yang dapat disesuaikan, pilih.yadiDapat disesuaikankolom. Untuk informasi lebih lanjut, lihat Meminta peningkatan kuota di Panduan Pengguna Service Quotas.

Kuota Client VPN

Nama	Default	Dapat Disesuaikan
Aturan otorisasi per titik akhir Client VPN	50	Ya
Titik akhir Client VPN per Wilayah	5	Ya
Koneksi klien bersamaan per titik akhir Client VPN	Nilai ini tergantung pada jumlah asosiasi subnet per titik akhir. • 1 — 7,000 • 2 — 36,500 • 3 — 66,500 • 4 — 96,500 • 5 — 126,000	Ya
Operasi bersamaan per Client VPN.	10	Tidak
Entri dalam daftar pencabutan sertifikat klien untuk titik akhir Client VPN	20.000	Tidak
Rute per titik akhir Client VPN	10	Ya

† Operasi meliputi:

- Mengaitkan atau memisahkan subnet
- Membuat atau menghapus rute
- Membuat atau menghapus aturan masuk dan keluar
- Membuat atau menghapus grup keamanan

Kuota pengguna dan grup

Jika Anda mengonfigurasi pengguna dan grup untuk Direktori aktif atau IdP berbasis SAML, kuota berikut berlaku:

- Pengguna dapat tergabung dalam grup maksimal sebanyak 200. Kami mengabaikan grup apa pun sesudah grup ke-200.
- Panjang maksimum ID grup adalah 255 karakter.
- Panjang maksimum ID nama adalah 255 karakter. Kami memotong karakter sesudah karakter ke-255.

Pertimbangan umum

Pertimbangkan hal berikut ini saat Anda menggunakan titik akhir Client VPN:

- Jika Anda menggunakan Direktori Aktif untuk mengautentikasi pengguna, titik akhir Client VPN harus milik akun yang sama sebagai sumber daya AWS Directory Service yang digunakan untuk autentikasi Direktori Aktif.
- Jika Anda menggunakan autentikasi gabungan berbasis SAML untuk mengautentikasi pengguna, titik akhir Client VPN harus milik akun yang sama sebagai penyedia identitas IAM SAML yang Anda buat untuk menentukan IdP ke hubungan kepercayaan AWS. Penyedia identitas IAM SAML dapat dibagikan ke beberapa titik akhir Client VPN di akun AWS yang sama.

Pemecahan Masalah Client VPN AWS

Topik berikut dapat membantu Anda memecahkan masalah yang mungkin terjadi terhadap titik akhir Client VPN.

Untuk informasi selengkapnya tentang pemecahan masalah perangkat lunak yang berbasis OpenVPN yang digunakan klien untuk mengoneksikan ke Client VPN, lihat Pemecahan Masalah Client VPN Anda di Panduan Pengguna AWS Client VPN .

Masalah umum

- Tidak dapat mengatasi nama DNS titik akhir Client VPN
- Lalu lintas tidak dibagi di antara subnet
- Aturan otorisasi untuk grup Direktori Aktif tidak berfungsi seperti yang diharapkan
- Klien tidak dapat mengakses VPC yang di-peering, Amazon S3, atau internet
- Akses ke VPC yang di-peering, Amazon S3, atau internet terputus-putus
- Perangkat lunak klien mengembalikan galat TLS
- Perangkat lunak klien mengembalikan galat nama pengguna dan kata sandi (Autentikasi Direktori Aktif)
- Perangkat lunak klien mengembalikan kesalahan nama pengguna dan kata sandi (otentikasi federasi)
- Klien tidak dapat terkoneksi (autentikasi bersama)
- Klien mengembalikan kredensial yang telah melebihi ukuran maksimal galat (autentikasi gabungan)
- Klien tidak membuka peramban (autentikasi gabungan)
- Klien mengembalikan tidak ada galat port yang tersedia (autentikasi gabungan)
- Koneksi VPN dihentikan karena ketidakcocokan IP
- Merutekan lalu lintas ke LAN tidak berfungsi seperti yang diharapkan
- Verifikasi batas bandwidth untuk titik akhir Client VPN

Tidak dapat mengatasi nama DNS titik akhir Client VPN

Masalah

Saya tidak dapat menyelesaikan nama DNS titik akhir Client VPN.

Penyebab

File konfigurasi titik akhir Client VPN mencakup parameter yang disebut `remote-random-hostname`. Parameter ini memaksa klien untuk menambahkan string acak ke nama DNS untuk mencegah DNS menyimpan cache. Beberapa klien tidak mengenali parameter ini, dan oleh karenanya, mereka tidak menambahkan string acak yang diperlukan untuk nama DNS.

Solusi

Buka file konfigurasi titik akhir Client VPN yang menggunakan teks editor pilihan Anda. Cari baris yang menentukan nama DNS titik akhir Client VPN, serta tambahkan string acak pada titik akhir tersebut sehingga formatnya menjadi *`random_string.displayed_DNS_name`*. Sebagai contoh:

- Nama DNS asli: `cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`
- Nama DNS yang diubah: `asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`

Lalu lintas tidak dibagi di antara subnet

Masalah

Saya mencoba untuk membagi lalu lintas jaringan diantara dua subnet. Lalu lintas privat harus dirutekan melalui subnet privat, sedangkan lalu lintas internet harus dirutekan melalui subnet publik. Namun, hanya satu rute yang digunakan meskipun saya telah menambahkan kedua rute ke tabel rute titik akhir Client VPN.

Penyebab

Anda dapat mengaitkan beberapa subnet menggunakan titik akhir Client VPN, tetapi Anda hanya dapat mengaitkan satu subnet saja ke setiap Availability Zone. Tujuan dari beberapa asosiasi subnet adalah untuk menyediakan ketersediaan yang tinggi serta ketersediaan Availability Zone bagi klien. Namun, Client VPN tidak memungkinkan Anda untuk secara selektif membagi lalu lintas antara subnet yang terkait dengan titik akhir Client VPN.

Klien terhubung ke titik akhir Client VPN berdasarkan pada algoritme round-robin DNS. Ini berarti bahwa lalu lintas mereka dapat dirutekan melalui salah satu subnet terkait ketika membuat koneksi.

Oleh karena itu, mereka mungkin mengalami masalah konektivitas jika mendarat di subnet terkait yang tidak memiliki entri rute yang diperlukan.

Misalnya, Anda mengonfigurasi asosiasi dan rute subnet berikut:

- Asosiasi subnet
  - Asosiasi 1: Subnet-A (us-east-1a)
  - Asosiasi 2: Subnet-B (us-east-1b)
- Rute
  - Rute 1: 10.0.0.0/16 dirutekan ke Subnet-A
  - Rute 2: 172.31.0.0/16 dirutekan ke Subnet-B

Dalam contoh ini, klien yang mendarat di Subnet-A saat mereka terkoneksi tidak dapat mengakses Rute 2, sementara klien yang mendarat di Subnet-B saat mereka terkoneksi tidak dapat mengakses Rute 1.

Solusi

Verifikasi bahwa titik akhir Client VPN memiliki entri rute yang sama dengan target untuk setiap jaringan yang terkait. Ini memastikan bahwa klien memiliki akses ke semua rute terlepas dari subnet mana yang dirutekan untuk lalu lintas mereka.

Aturan otorisasi untuk grup Direktori Aktif tidak berfungsi seperti yang diharapkan

Masalah

Saya telah mengonfigurasi aturan otorisasi untuk grup Direktori Aktif saya, akan tetapi grup Direktori Aktif tidak berfungsi sesuai dengan harapan saya. Saya telah menambahkan aturan otorisasi pada `0.0.0.0/0` untuk mengotorisasi lalu lintas pada semua jaringan, akan tetapi lalu lintas tidak dapat berjalan pada CIDR untuk tujuan tertentu.

Penyebab

Aturan otorisasi diindekskan pada jaringan CIDR. Aturan otorisasi harus memberikan akses kepada grup Direktori Aktif menuju jaringan CIDR tertentu. Aturan otorisasi untuk `0.0.0.0/0` telah ditangani sebagai kasus yang spesial, dan karena itu dievaluasi terakhir, terlepas dari urutan pembuatan aturan otorisasi.

Misalnya, anggap saja jika Anda membuat lima aturan otorisasi dengan urutan berikut ini:

- Aturan 1: Akses Grup 1 menuju `10.1.0.0/16`
- Aturan 2: Akses Grup 1 menuju `0.0.0.0/0`
- Aturan 3: Akses Grup 2 menuju `0.0.0.0/0`
- Aturan 4: Akses Grup 3 menuju `0.0.0.0/0`
- Aturan 5: Akses Grup 2 menuju `172.131.0.0/16`

Pada contoh ini, aturan 2, aturan 3, dan aturan 4 akan dievaluasi terakhir. Grup 1 memiliki akses menuju `10.1.0.0/16` saja, dan Grup 2 memiliki akses menuju `172.131.0.0/16` saja. Grup 3 tidak memiliki akses menuju `10.1.0.0/16` atau `172.131.0.0/16`, namun memiliki akses ke semua jaringan lainnya. Jika Anda menghilangkan Aturan 1 dan 5, ketiga grup sisanya memiliki akses ke semua jaringan.

Client VPN menggunakan pencocokan awalan terpanjang saat mengevaluasi aturan otorisasi. Lihat Prioritas rute di Panduan Pengguna Amazon VPC untuk detail selengkapnya.

Solusi

Verifikasi bahwa Anda membuat aturan otorisasi yang secara eksplisit memberikan akses grup Direktori Aktif ke CIDR jaringan tertentu. Jika Anda menambahkan aturan otorisasi untuk `0.0.0.0/0`, perlu diingat bahwa aturan otorisasi akan dievaluasi terakhir, dan aturan otorisasi sebelumnya mungkin dapat membatasi jaringan dimana otorisasi tersebut dapat memberikan akses.

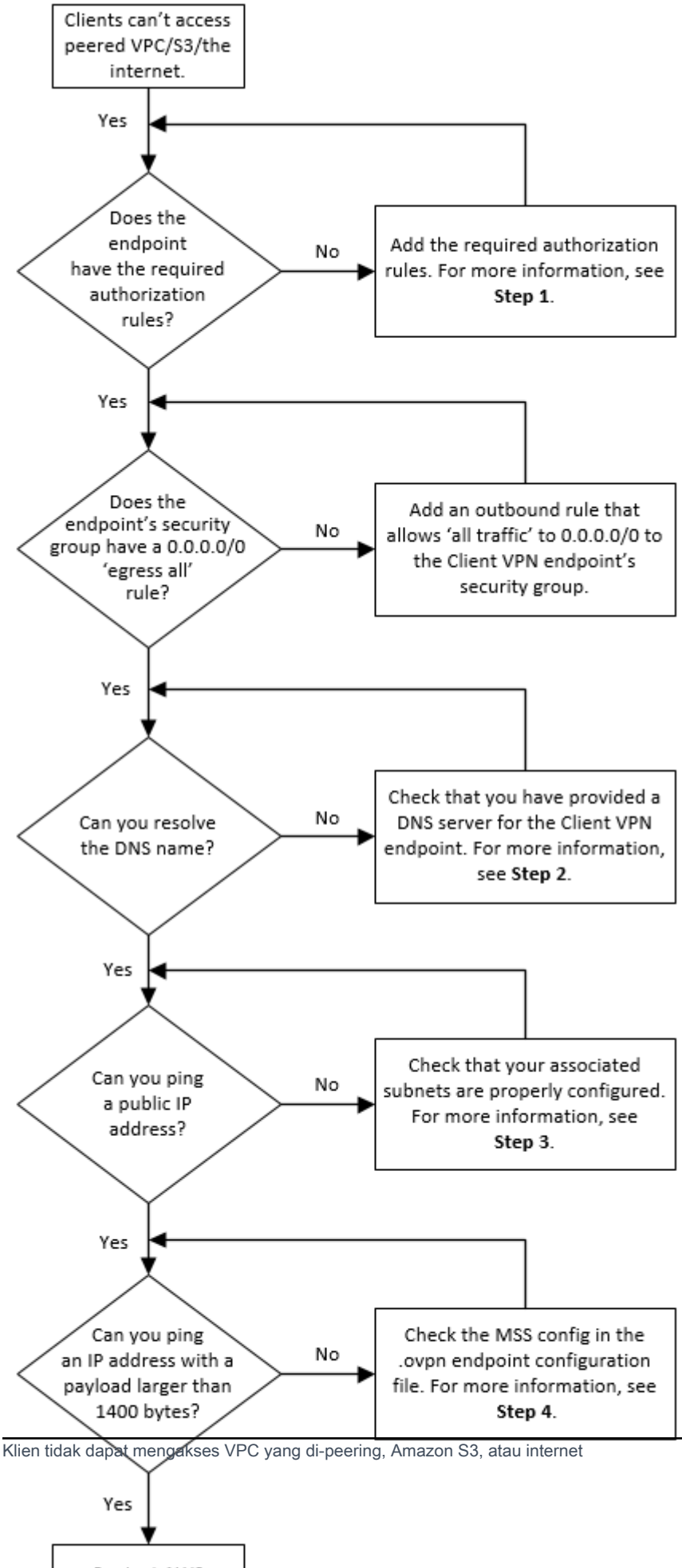
Klien tidak dapat mengakses VPC yang di-peering, Amazon S3, atau internet

Masalah

Saya telah mengonfigurasi rute titik akhir Client VPN milik saya dengan benar, namun klien saya tidak dapat mengakses VPC yang di-peering, Amazon S3, atau internet.

Solusi

Bagan alur berikut berisi langkah-langkah untuk mendiagnosis masalah konektivitas internet, VPC yang di-peering, dan Amazon S3.


Clients can't access peered VPC/S3/the internet.
Yes
Does the endpoint have the required authorization rules?
No
Add the required authorization rules. For more information, see **Step 1**.
Yes
Does the endpoint's security group have a 0.0.0.0/0 'egress all' rule?
No
Add an outbound rule that allows 'all traffic' to 0.0.0.0/0 to the Client VPN endpoint's security group.
Yes
Can you resolve the DNS name?
No
Check that you have provided a DNS server for the Client VPN endpoint. For more information, see **Step 2**.
Yes
Can you ping a public IP address?
No
Check that your associated subnets are properly configured. For more information, see **Step 3**.
Yes
Can you ping an IP address with a payload larger than 1400 bytes?
No
Check the MSS config in the .ovpn endpoint configuration file. For more information, see **Step 4**.
Yes

1. Untuk akses menuju internet, tambahkan aturan otorisasi untuk `0.0.0.0/0`.

   Untuk akses ke VPC yang di-peering, tambahkan aturan otorisasi untuk rentang IPv4 CIDR dari VPC.

   Untuk akses menuju S3, tentukan alamat IP dari titik akhir Amazon S3.
2. Anda perlu memeriksa jika Anda dapat menyelesaikan nama DNS.

   Jika Anda tidak dapat menyelesaikan nama DNS, verifikasi bahwa Anda telah menentukan server DNS untuk titik akhir Client VPN. Jika Anda mengelola server DNS milik Anda sendiri, mohon tentukan alamat IP-nya. Verifikasi bahwa server DNS dapat diakses dari VPC.

   Jika Anda tidak yakin tentang alamat IP mana yang harus ditentukan untuk server DNS, tentukan DNS VPC resolver di alamat IP .2 di VPC Anda.
3. Untuk akses internet, periksa apakah Anda dapat melakukan ping pada sebuah alamat IP publik atau situs web publik, misalnya, `amazon.com`. Jika Anda tidak mendapatkan respons, pastikan tabel rute untuk subnet terkait memiliki rute default yang menargetkan gateway internet atau gateway NAT. Jika rute sudah berada pada tempatnya, verifikasi bahwa subnet terkait tidak memiliki aturan daftar kontrol akses jaringan yang memblokir lalu lintas masuk dan keluar.

   Jika Anda tidak dapat menjangkau VPC yang di-peering, verifikasi bahwa tabel rute subnet terkait memiliki entri rute untuk VPC yang di-peering.

   Jika Anda tidak dapat menjangkau Amazon S3, verifikasi bahwa tabel rute subnet terkait memiliki entri rute untuk gateway VPC endpoint.
4. Peeriksa apakah Anda dapat menge-ping alamat IP publik dengan muatan yang lebih besar dari 1400 byte. Gunakan salah satu perintah berikut:

   - Windows

     ```
     C:\> ping  8.8.8.8 -l 1480 -f
     ```

   - Linux

     ```
     $ ping -s 1480 8.8.8.8 -M do
     ```

Jika Anda tidak dapat menge-ping alamat IP dengan muatan yang lebih besar dari 1400 byte, buka file konfigurasi `.ovpn` titik akhir Client VPN dengan menggunakan teks editor pilihan Anda, dan tambahkan hal berikut.

```
mssfix 1328
```

Akses ke VPC yang di-peering, Amazon S3, atau internet terputus-putus

Masalah

Saya mengalami masalah konektivitas yang terputus-putus saat mengoneksikan ke VPC yang di-peering, Amazon S3, atau internet, tetapi akses ke subnet terkait tidak terpengaruh. Saya harus memutuskan hubungan dan menghubungkan kembali untuk menyelesaikan masalah konektivitas.

Penyebab

Klien terhubung ke titik akhir Client VPN berdasarkan pada algoritme round-robin DNS. Ini berarti bahwa lalu lintas mereka dapat dirutekan melalui salah satu subnet terkait ketika membuat koneksi. Oleh karena itu, mereka mungkin mengalami masalah konektivitas jika mendarat di subnet terkait yang tidak memiliki entri rute yang diperlukan.

Solusi

Verifikasi bahwa titik akhir Client VPN memiliki entri rute yang sama dengan target untuk setiap jaringan terkait. Ini memastikan bahwa klien memiliki akses ke semua rute, terlepas dari subnet terkait mana yang dirutekan untuk lalu lintas mereka.

Misalnya, anggap bahwa titik akhir Client VPN Anda memiliki tiga asosiasi subnet (Subnet A, B, dan C), dan Anda ingin mengaktifkan akses internet untuk klien Anda. Untuk melakukannya, Anda harus menambahkan tiga rute `0.0.0.0/0` - satu menargetkan setiap subnet terkait:

- Rute 1: `0.0.0.0/0` untuk Subnet A
- Rute 2: `0.0.0.0/0` untuk Subnet B
- Rute 3: `0.0.0.0/0` untuk Subnet C

Perangkat lunak klien mengembalikan galat TLS

Masalah

Dulu saya berhasil menghubungkan klien saya ke Client VPN, tetapi sekarang klien berbasis OpenVPN mengembalikan salah satu kesalahan berikut ketika mencoba menghubungkan:

```
TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network
 connectivity)
TLS Error: TLS handshake failed
```

```
Connection failed because of a TLS handshake error. Contact your IT administrator.
```

Kemungkinan penyebabnya #1

Jika Anda menggunakan autentikasi bersama dan Anda mengimpor daftar pencabutan sertifikat klien, maka daftar pencabutan sertifikat klien tersebut mungkin telah kedaluwarsa. Selama fase autentikasi, titik akhir Client VPN memeriksa sertifikat klien yang tidak sesuai dengan daftar pencabutan sertifikat klien yang Anda impor. Jika daftar pencabutan sertifikat klien telah kedaluwarsa, maka Anda tidak dapat terkoneksi dengan titik akhir Client VPN.

Solusi #1

Periksa tanggal kedaluwarsa daftar pencabutan sertifikat klien Anda dengan menggunakan alat OpenSSL.

```
$ openssl crl -in path_to_crl_pem_file -noout -nextupdate
```

Output menampilkan tanggal dan waktu kedaluwarsa. Jika daftar pencabutan sertifikat klien telah kedaluwarsa, Anda harus membuat daftar yang baru dan mengimpornya ke titik akhir Client VPN. Untuk informasi selengkapnya, lihat Daftar pencabutan sertifikat klien.

Kemungkinan penyebabnya #2

Sertifikat server yang digunakan untuk titik akhir Client VPN telah kedaluwarsa.

Solusi #2

Periksa status sertifikat server Anda di AWS Certificate Manager konsol atau dengan menggunakan AWS CLI. Jika sertifikat server kedaluwarsa, buat sertifikat baru dan unggah ke ACM. Untuk langkah-

langkah mendetail untuk menghasilkan sertifikat dan kunci server dan klien menggunakan utilitas easy-rsa OpenVPN, dan mengimpornya ke ACM, lihat. Autentikasi bersama

Atau, mungkin ada masalah dengan perangkat lunak berbasis OpenVPN yang digunakan klien untuk terkoneksi ke Client VPN. Untuk informasi selengkapnya tentang pemecahan masalah perangkat lunak berbasis OpenVPN, lihat Memecahkan Masalah Koneksi Client VPN Anda dalam Panduan Pengguna AWS Client VPN .

Perangkat lunak klien mengembalikan galat nama pengguna dan kata sandi (Autentikasi Direktori Aktif)

Masalah

Saya menggunakan autentikasi Direktori Aktif untuk titik akhir Client VPN saya dan biasanya saya berhasil mengoneksikan klien saya ke Client VPN. Tapi sekarang, klien mendapatkan galat nama pengguna dan kata sandi tidak valid.

Kemungkinan penyebab

Jika Anda menggunakan autentikasi direktori aktif dan mengaktifkan Autentikasi Multi-Faktor (MFA) setelah Anda mendistribusikan file konfigurasi milik klien, file tidak berisi informasi yang diperlukan untuk meminta pengguna memasukkan kode MFA mereka. Pengguna hanya diminta untuk memasukkan nama pengguna dan kata sandi, dan kemudian autentikasi gagal.

Solusi

Unduh file konfigurasi klien yang baru dan distribusikan kepada klien Anda. Verifikasi bahwa file yang baru tersebut berisi baris berikut.

```
static-challenge "Enter MFA code " 1
```

Untuk informasi selengkapnya, lihat Ekspor dan konfigurasikan file konfigurasi untuk klien. Uji konfigurasi MFA untuk Direktori Aktif Anda tanpa menggunakan titik akhir Client VPN ketika memverifikasi bahwa MFA bekerja sesuai yang diharapkan.

Perangkat lunak klien mengembalikan kesalahan nama pengguna dan kata sandi (otentikasi federasi)

Masalah

Mencoba masuk dengan nama pengguna dan kata sandi dengan otentikasi federasi dan mendapatkan kesalahan “Kredensi yang diterima tidak benar. Hubungi administrator TI Anda.”

Penyebab

Kesalahan ini dapat disebabkan oleh tidak memiliki setidaknya satu atribut yang disertakan dalam respons SAMP dari IDP.

Solusi

Pastikan setidaknya satu atribut disertakan dalam respons SAMP dari iDP. Untuk informasi selengkapnya, lihat sumber daya konfigurasi IdP berbasis SAML.

Klien tidak dapat terkoneksi (autentikasi bersama)

Masalah

Saya menggunakan autentikasi bersama untuk titik akhir Client VPN saya. Klien mendapatkan galat negosiasi kunci TLS dan galat waktu habis.

Kemungkinan penyebab

File konfigurasi yang disediakan untuk klien tidak berisi sertifikat serta kunci privat klien, atau sertifikat dan kunci tidak benar.

Solusi

Pastikan bahwa file konfigurasi berisi sertifikat dan kunci klien yang benar. Jika perlu, perbaiki file konfigurasi dan distribusikan kembali ke klien Anda. Untuk informasi selengkapnya, lihat Ekspor dan konfigurasikan file konfigurasi untuk klien.

Klien mengembalikan kredensial yang telah melebihi ukuran maksimal galat (autentikasi gabungan)

Masalah

Saya menggunakan autentikasi gabungan untuk titik akhir Client VPN saya. Ketika klien memasukkan nama pengguna dan kata sandi di jendela peramban penyedia identitas (IdP) berbasis SAML, mereka mendapatkan galat bahwa kredensial melebihi ukuran maksimum yang didukung.

Penyebab

Respon SAML yang dikembalikan oleh IdP melebihi ukuran maksimum yang didukung. Untuk informasi selengkapnya, lihat Persyaratan dan pertimbangan untuk autentikasi federasi berbasis SAML.

Solusi

Coba untuk mengurangi jumlah grup yang dimiliki pengguna di IdP, dan coba untuk mengoneksikan kembali.

Klien tidak membuka peramban (autentikasi gabungan)

Masalah

Saya menggunakan autentikasi gabungan untuk titik akhir Client VPN saya. Saat klien mencoba terkoneksi ke titik akhir, perangkat lunak klien tidak membuka jendela peramban, dan malah menampilkan jendela popup nama pengguna dan kata sandi.

Penyebab

File konfigurasi yang disediakan untuk klien tidak berisi tanda `auth-federate`.

Solusi

Ekspor file konfigurasi terbaru, impor ke klien yang AWS disediakan, dan coba sambungkan lagi.

Klien mengembalikan tidak ada galat port yang tersedia (autentikasi gabungan)

Masalah

Saya menggunakan autentikasi gabungan untuk titik akhir Client VPN saya. Saat klien mencoba untuk terkoneksi ke titik akhir, perangkat lunak klien mengembalikan galat berikut ini:

```
The authentication flow could not be initiated. There are no available ports.
```

Penyebab

Klien yang AWS disediakan memerlukan penggunaan port TCP 35001 untuk menyelesaikan otentikasi. Untuk informasi selengkapnya, lihat Persyaratan dan pertimbangan untuk autentikasi federasi berbasis SAML.

Solusi

Verifikasi bahwa perangkat klien tidak memblokir TCP port 35001 atau menggunakannya untuk proses yang berbeda.

Koneksi VPN dihentikan karena ketidakcocokan IP

Masalah

Koneksi VPN dihentikan dan perangkat lunak klien mengembalikan kesalahan berikut: `"The VPN connection is being terminated due to a discrepancy between the IP address of the connected server and the expected VPN server IP. Please contact your network administrator for assistance in resolving this issue."`

Penyebab

Klien yang AWS disediakan mengharuskan alamat IP yang terhubung cocok dengan IP server VPN yang mendukung titik akhir Client VPN. Untuk informasi selengkapnya, lihat Aturan dan praktik terbaik AWS Client VPN.

Solusi

Verifikasi bahwa tidak ada proxy DNS antara klien yang AWS disediakan dan titik akhir Client VPN.

Merutekan lalu lintas ke LAN tidak berfungsi seperti yang diharapkan

Masalah

Mencoba merutekan lalu lintas ke jaringan area lokal (LAN) tidak berfungsi seperti yang diharapkan ketika rentang alamat IP LAN tidak berada dalam rentang alamat IP pribadi standar berikut:`10.0.0.0/8`,`172.16.0.0/12`,`192.168.0.0/16`, atau`169.254.0.0/16`.

Penyebab

Jika rentang alamat LAN klien terdeteksi berada di luar rentang standar di atas, titik akhir Client VPN akan secara otomatis mendorong arahan OpenVPN “redirect-gateway block-local” ke klien, memaksa semua lalu lintas LAN ke VPN. Untuk informasi selengkapnya, lihat Aturan dan praktik terbaik AWS Client VPN.

Solusi

Jika Anda memerlukan akses LAN selama koneksi VPN, disarankan agar Anda menggunakan rentang alamat konvensional yang tercantum di atas untuk LAN Anda.

Verifikasi batas bandwidth untuk titik akhir Client VPN

Masalah

Saya perlu memverifikasi batas bandwidth untuk titik akhir Client VPN.

Penyebab

Throughput tergantung pada beberapa faktor, seperti kapasitas koneksi dari lokasi Anda, dan latensi jaringan antara aplikasi desktop Client VPN di komputer Anda dengan VPC endpoint. Ada juga batas bandwidth 10 Mbps per koneksi pengguna.

Solusi

Jalankan perintah berikut untuk memverifikasi bandwidth.

```
sudo iperf3 -s -V
```

Pada klien:

```
sudo iperf -c server IP address -p port -w 512k -P 60
```

Riwayat dokumen untuk Panduan Pengguna

Tabel berikut menjelaskan pembaruan Panduan Administrator AWS Client VPN.

Perubahan	Deskripsi	Tanggal
Riwayat aturan otorisasi	Penambahan contoh skenario untuk aturan otorisasi.	September 15, 2022
Durasi maksimum sesi VPN	Anda dapat mengonfigurasi durasi sesi VPN maksimum yang lebih pendek untuk memenuhi persyaratan keamanan dan kepatuhan.	Januari 20, 2022
Spanduk login klien	Anda dapat mengaktifkan spanduk teks diAWSmeny ediakan aplikasi desktop Client VPN saat sesi VPN dibuat untuk memenuhi kebutuhan peraturan dan kepatuhan.	Januari 20, 2022
Handler koneksi klien	Anda dapat mengaktifkan handler koneksi klien untuk titik akhir Client VPN agar menjalankan logika kustom yang mengotorisasi koneksi baru.	4 November 2020
Porayat swalayan	Anda dapat mengaktifkan portal layanan mandiri di titik akhir Client VPN untuk klien Anda.	29 Oktober 2020
Client-to-client akses	Anda dapat mengaktifkan klien yang terhubung ke titik akhir	29 September 2020

	Client VPN agar terhubung satu sama lain.	
Autentikasi gabungan berbasis SAML 2.0	Anda dapat mengautentikasi pengguna Client VPN menggunakan autentikasi gabungan berbasis SAML 2.0.	19 Mei 2020
Menentukan grup keamanan selama pembuatan	Anda dapat menentukan VPC dan grup keamanan saat membuat titik akhir AWS Client VPN Anda.	5 Maret 2020
Port VPN yang dapat dikonfigurasi	Anda dapat menentukan nomor port VPN yang didukung untuk titik akhir AWS Client VPN Anda.	16 Januari 2020
Dukungan untuk autentikasi multi-faktor (MFA)	Titik akhir AWS Client VPN Anda mendukung MFA jika diaktifkan untuk Direktori Aktif.	30 September 2019
Dukungan untuk terowongan terpisah	Anda dapat mengaktifkan terowongan terpisah di titik akhir AWS Client VPN Anda.	24 Juli 2019
Riwayat awal	Perilisan ini memperkenalkan AWS Client VPN.	18 Desember 2018

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