aws

Panduan Administrator

AWS Client VPN

AWS Client VPN: Panduan Administrator

Table of Contents

Apa itu AWS Client VPN?

AWS Client VPN adalah VPN layanan berbasis klien terkelola yang memungkinkan Anda mengakses AWS sumber daya dan sumber daya dengan aman di jaringan lokal Anda. Dengan KlienVPN, Anda dapat mengakses sumber daya Anda dari lokasi mana pun menggunakan VPN klien VPN berbasis Terbuka.

Topik

Fitur Klien VPN

Klien VPN menawarkan fitur dan fungsionalitas berikut:

- Koneksi aman — Ini menyediakan TLS koneksi aman dari lokasi mana pun menggunakan VPN klien Terbuka.
- Layanan terkelola - Ini adalah layanan AWS terkelola, sehingga menghilangkan beban operasional dalam menerapkan dan mengelola VPN solusi akses jarak jauh pihak ketiga.
- Ketersediaan dan elastisitas tinggi — Ini secara otomatis menskalakan jumlah pengguna yang terhubung ke AWS sumber daya dan sumber daya lokal Anda.
- 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 - Ini memungkinkan Anda mengakses AWS sumber daya dan sumber daya lokal menggunakan satu VPN terowongan.

- 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 — Ini terintegrasi dengan AWS layanan yang ada, termasuk AWS Directory Service dan AmazonVPC.

Komponen Klien VPN

Berikut ini adalah konsep kunci untuk KlienVPN:

Titik VPN akhir klien

VPNEndpoint Klien adalah sumber daya yang Anda buat dan konfigurasikan untuk mengaktifkan dan mengelola VPN sesi klien. Ini adalah titik terminasi untuk semua VPN sesi klien.

Jaringan target

Jaringan target adalah jaringan yang Anda kaitkan dengan VPN titik akhir Klien. Subnet dari a VPC adalah jaringan target. Mengaitkan subnet dengan VPN titik akhir Klien memungkinkan Anda membuat sesi. VPN Anda dapat mengaitkan beberapa subnet dengan VPN titik akhir Klien untuk ketersediaan tinggi. Semua subnet harus dari yang samaVPC. Setiap subnet harus menjadi bagian dari Availability Zone yang berbeda.

Rute

Setiap VPN titik akhir Klien 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 VPN titik akhir Klien untuk membuat VPN sesi. Pengguna akhir perlu mengunduh VPN klien Terbuka dan menggunakan file VPN konfigurasi Klien yang Anda buat untuk membuat VPN sesi.

CIDRJangkauan klien

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

VPNPort klien

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

Antarmuka VPN jaringan klien

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

Pencatatan koneksi

Anda dapat mengaktifkan pencatatan koneksi untuk VPN titik akhir Klien Anda untuk mencatat peristiwa koneksi. Anda dapat menggunakan informasi ini untuk menjalankan forensik, menganalisis bagaimana VPN titik akhir Klien Anda digunakan, atau men-debug masalah koneksi.

Portal layanan mandiri

Klien VPN menyediakan portal swalayan sebagai halaman web untuk pengguna akhir untuk mengunduh versi terbaru Klien AWS VPN Desktop dan versi terbaru dari file konfigurasi VPN titik akhir Klien, yang berisi pengaturan yang diperlukan untuk terhubung ke titik akhir mereka. Administrator VPN endpoint Klien dapat mengaktifkan atau menonaktifkan portal layanan mandiri untuk titik akhir KlienVPN. 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 Klien VPN

Anda dapat bekerja dengan Klien VPN dengan salah satu cara berikut:

AWS Management Console

Konsol menyediakan antarmuka pengguna berbasis web untuk KlienVPN. Jika Anda telah mendaftar Akun AWS, Anda dapat masuk ke VPC konsol Amazon dan memilih Klien VPN di panel navigasi.

AWS Command Line Interface (AWS CLI)

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

AWS Tools for Windows PowerShell

AWS menyediakan perintah untuk serangkaian AWS penawaran yang luas bagi mereka yang membuat skrip di lingkungan. PowerShell Untuk informasi selengkapnya tentang memulai dengan AWS Tools for Windows PowerShell, lihat AWS Tools for Windows PowerShell Panduan Pengguna. Untuk informasi selengkapnya tentang cmdlet untuk KlienVPN, lihat Referensi AWS Tools for Windows PowerShell Cmdlet.

Permintaan API

VPNHTTPSKueri Klien API memberi Anda akses terprogram ke Klien VPN dan AWS. HTTPSKueri API memungkinkan Anda mengeluarkan HTTPS permintaan langsung ke layanan. Saat Anda menggunakan HTTPSAPI, Anda harus menyertakan kode untuk menandatangani permintaan secara digital menggunakan kredensi Anda. Untuk informasi selengkapnya, lihat AWS Client VPN tindakan.

Harga untuk Klien VPN

Anda dikenakan biaya untuk setiap asosiasi titik akhir dan setiap VPN koneksi 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 EC2 Sesuai Permintaan Amazon.

Jika Anda mengaktifkan pencatatan koneksi untuk VPN titik akhir Klien, 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 pengendali koneksi klien untuk VPN titik akhir Klien Anda, Anda harus membuat dan menjalankan fungsi Lambda. Biaya berlaku untuk aktivasi fungsi Lambda. Untuk informasi selengkapnya, lihat AWS Lambda harga.

VPNEndpoint klien dikaitkan dengan jaringan target, yang merupakan subnet dalam file. VPC Jika ini VPC memiliki Internet Gateway, kami mengaitkan alamat IP Elastis dengan antarmuka jaringan VPN elastis Klien (ENIs). Alamat IP Elastis ini dibebankan sebagai IPv4 alamat publik yang sedang digunakan. Untuk informasi selengkapnya, lihat tab IPv4 Alamat Publik di halaman VPC harga.

Aturan dan praktik terbaik untuk menggunakan AWS Client VPN

Berikut ini adalah aturan dan praktik terbaik untuk menggunakan AWS Client VPN

- Bandwidth minimum 10 Mbps didukung per koneksi pengguna. Bandwidth maksimum per koneksi pengguna tergantung pada jumlah koneksi yang dibuat ke VPN titik akhir Klien.
- CIDRRentang klien tidak dapat tumpang tindih dengan lokal CIDR VPC di mana subnet terkait berada, atau rute apa pun yang ditambahkan secara manual ke tabel rute VPN titik akhir Klien.
- CIDRRentang klien harus memiliki ukuran blok minimal /22 dan tidak boleh lebih besar dari /12.
- Sebagian alamat dalam CIDR rentang klien digunakan untuk mendukung model ketersediaan VPN titik akhir Klien, dan tidak dapat ditetapkan ke klien. Oleh karena itu, kami menyarankan Anda menetapkan CIDR blok yang berisi dua kali jumlah alamat IP yang diperlukan untuk mengaktifkan jumlah maksimum koneksi bersamaan yang Anda rencanakan untuk mendukung pada titik akhir KlienVPN.
- CIDRRentang klien tidak dapat diubah setelah Anda membuat VPN titik akhir Klien.
- Subnet yang terkait dengan VPN titik akhir Klien harus sama. VPC
- Anda tidak dapat mengaitkan beberapa subnet dari Availability Zone yang sama dengan titik VPN akhir Klien.
- VPNTitik akhir Klien tidak mendukung asosiasi subnet dalam penyewaan khusus. VPC
- Klien hanya VPN mendukung IPv4 lalu lintas. Lihat IPv6pertimbangan untuk AWS Client VPN untuk detail tentangIPv6.
- Klien VPN tidak mematuhi Standar Pemrosesan Informasi Federal (FIPS).
- Portal layanan mandiri ini tidak tersedia untuk klien yang mengautentikasi menggunakan autentikasi bersama.
- Kami tidak menyarankan untuk menghubungkan ke VPN titik akhir Klien menggunakan alamat IP. Karena Client VPN adalah layanan yang dikelola, Anda kadang-kadang akan melihat perubahan

dalam alamat IP yang DNS namanya diselesaikan. Selain itu, Anda akan melihat antarmuka VPN jaringan Klien dihapus dan dibuat ulang di log Anda CloudTrail . Kami merekomendasikan untuk menghubungkan ke VPN titik akhir Klien menggunakan DNS nama yang diberikan.

- Penerusan IP saat ini tidak didukung saat menggunakan aplikasi AWS Client VPN desktop. Penerusan IP didukung dari klien lain.
- Klien VPN tidak mendukung replikasi Multi-wilayah di. AWS Managed Microsoft AD VPNTitik akhir Klien 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 VPN koneksi dari komputer jika ada beberapa pengguna yang masuk ke sistem operasi.
- VPNLayanan Klien mensyaratkan bahwa alamat IP yang terhubung dengan klien cocok dengan IP yang diselesaikan oleh DNS nama VPN titik akhir Klien. Dengan kata lain, jika Anda menetapkan DNS catatan khusus untuk VPN titik akhir Klien, lalu meneruskan lalu lintas ke alamat IP aktual yang diselesaikan oleh DNS nama 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
- VPNLayanan Klien mensyaratkan bahwa jaringan area lokal (LAN) rentang alamat IP 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 LAN alamat klien terdeteksi berada di luar rentang di atas, VPN titik akhir Klien akan secara otomatis mendorong Open VPN direktif “redirect-gateway block-local” ke klien, memaksa semua lalu lintas ke dalam. LAN VPN Oleh karena itu, jika Anda memerlukan LAN akses selama VPN koneksi, disarankan agar Anda menggunakan rentang alamat konvensional yang tercantum di atas untuk AndaLAN. Aturan ini diberlakukan untuk mengurangi kemungkinan serangan net lokal seperti yang dijelaskan di sini: TunnelCrack

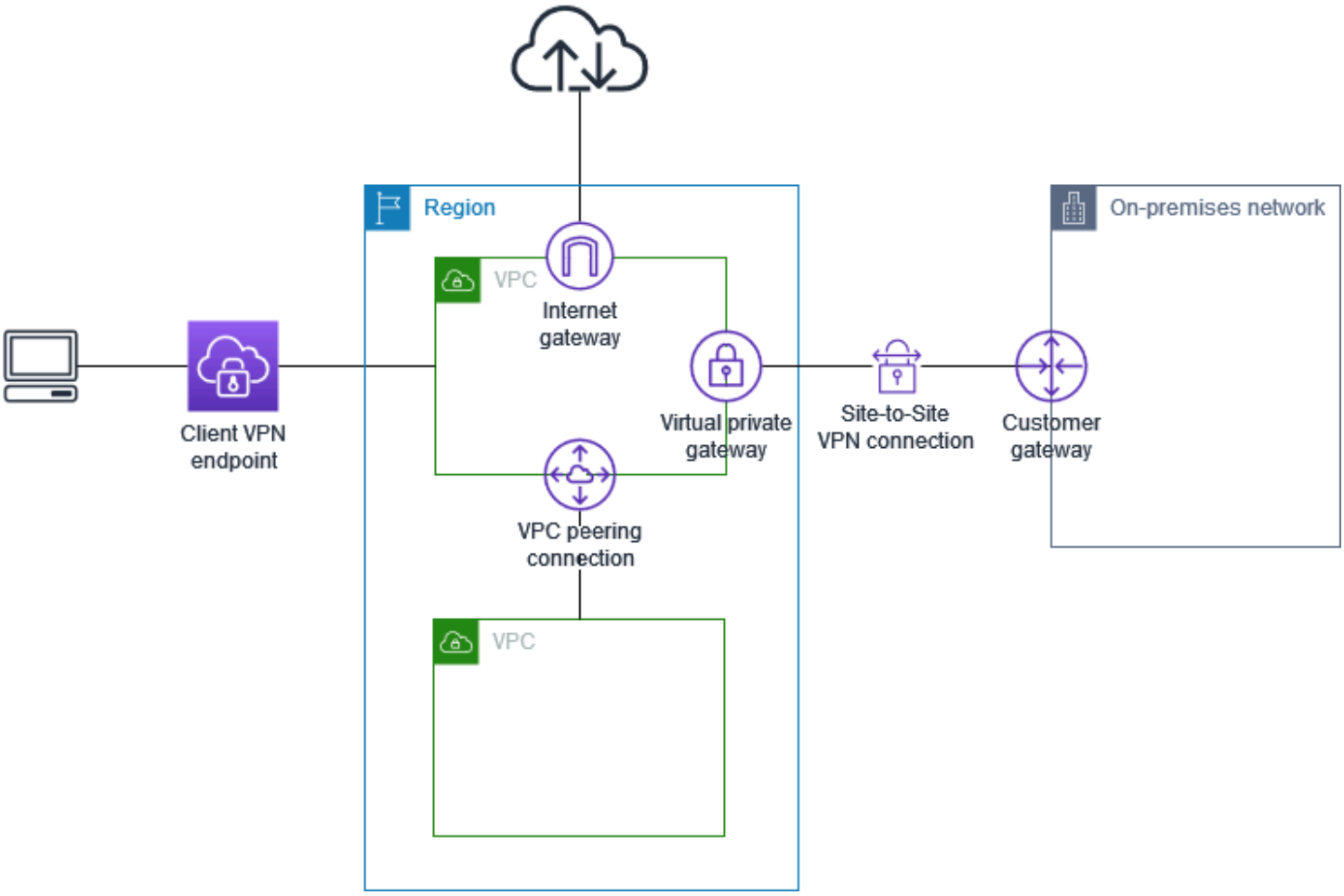
Bagaimana cara AWS Client VPN kerja

Dengan AWS Client VPN, ada dua jenis persona pengguna yang berinteraksi dengan VPN endpoint Klien: administrator dan klien.

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

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

Grafik berikut menggambarkan VPN arsitektur Klien dasar.



Skenario dan contoh untuk Klien VPN

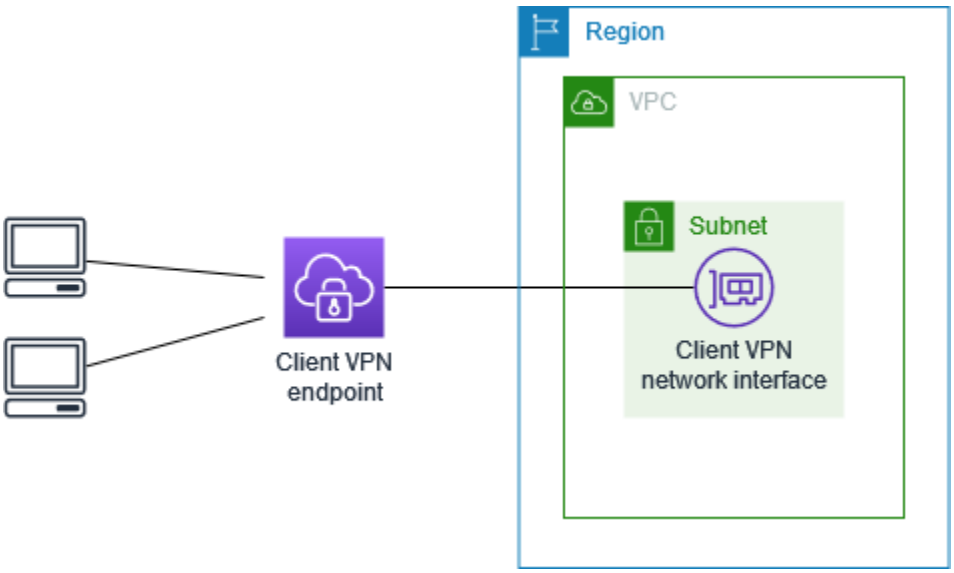
AWS Client VPN adalah VPN solusi akses jarak jauh yang dikelola sepenuhnya yang Anda gunakan untuk memungkinkan klien mengamankan akses ke sumber daya dalam keduanya AWS dan jaringan lokal Anda. Ada beberapa opsi untuk cara Anda mengonfigurasi akses. Bagian ini memberikan contoh untuk membuat dan mengonfigurasi VPN akses Klien untuk klien Anda.

Skenario

- the section called “Akses a VPC”
- the section called “Akses peered VPC”
- the section called “Mengakses jaringan lokal”
- the section called “Mengakses internet”
- the section called “lient-to-clientAkses C”
- the section called “Membatasi akses ke jaringan Anda”

Akses VPC menggunakan Klien VPN

AWS Client VPN Konfigurasi untuk skenario ini mencakup satu targetVPC. Kami merekomendasikan konfigurasi ini jika Anda perlu memberi klien akses ke sumber daya di dalam satu VPC saja.



Sebelum memulai, lakukan hal berikut:

- Buat atau identifikasi VPC dengan setidaknya satu subnet. Identifikasi subnet di VPC untuk dikaitkan dengan VPN titik akhir Klien dan catat rentangnya IPv4CIDR.
- Identifikasi CIDR rentang yang sesuai untuk alamat IP klien yang tidak tumpang tindih dengan. VPC CIDR
- Tinjau aturan dan batasan untuk VPN titik akhir Klien di[Aturan dan praktik terbaik untuk menggunakan AWS Client VPN](#).

Untuk menerapkan konfigurasi ini

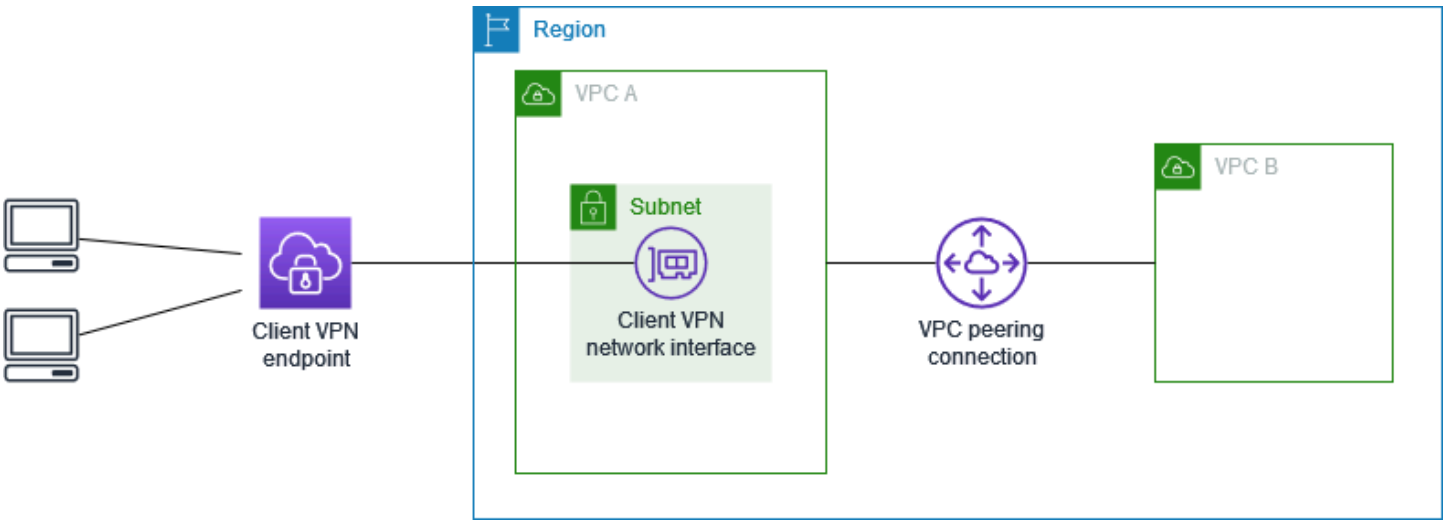
1. Buat VPN titik akhir Klien di Wilayah yang sama denganVPC. Caranya, lakukan langkah-langkah yang dijelaskan dalam [Buat titik AWS Client VPN akhir](#).
2. Kaitkan subnet dengan titik VPN akhir Klien. Untuk melakukan ini, lakukan langkah-langkah yang dijelaskan [Mengaitkan jaringan target dengan titik AWS Client VPN akhir](#) dan pilih subnet dan yang VPC Anda identifikasi sebelumnya.
3. Tambahkan aturan otorisasi untuk memberi klien akses ke file. VPC Untuk melakukan ini, lakukan langkah-langkah yang dijelaskan dalam[Tambahkan aturan otorisasi](#), dan untuk jaringan Tujuan, masukkan IPv4 CIDR rentangVPC.

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 peered VPC menggunakan Klien VPN

AWS Client VPN Konfigurasi untuk skenario ini mencakup target VPC (VPCA) yang diintip dengan tambahan VPC (VPCB). Kami merekomendasikan konfigurasi ini jika Anda perlu memberi klien akses ke sumber daya di dalam target VPC dan ke VPCs yang lain yang diintip dengannya (seperti VPC B).

> **Note**
>
> Prosedur untuk mengizinkan akses ke peered VPC (diuraikan mengikuti diagram jaringan) diperlukan hanya jika VPN titik akhir Klien dikonfigurasi untuk mode split-tunnel. Dalam mode terowongan penuh, akses ke peered diizinkan VPC secara default.



Sebelum memulai, lakukan hal berikut:

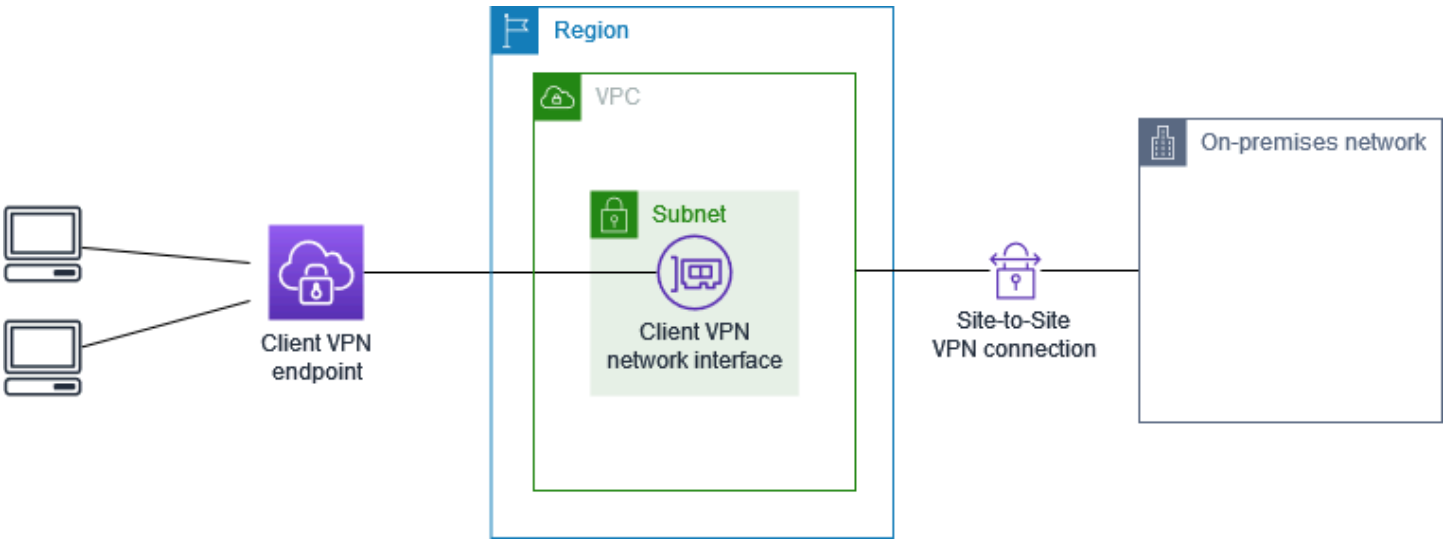
- Buat atau identifikasi VPC dengan setidaknya satu subnet. Identifikasi subnet di VPC untuk dikaitkan dengan VPN titik akhir Klien dan catat rentangnya IPv4CIDR.
- Identifikasi CIDR rentang yang sesuai untuk alamat IP klien yang tidak tumpang tindih dengan. VPC CIDR
- Tinjau aturan dan batasan untuk VPN titik akhir Klien diAturan dan praktik terbaik untuk menggunakan AWS Client VPN.

Untuk menerapkan konfigurasi ini

1. Membangun koneksi VPC peering antara. VPCs Ikuti langkah-langkah di Membuat dan menerima koneksi VPC peering di Amazon VPC Peering Guide. Konfirmasikan bahwa instance di VPC A dapat berkomunikasi dengan instance di VPC B menggunakan koneksi peering.
2. Buat VPN titik akhir Klien di Wilayah yang sama dengan targetVPC. Dalam diagram, ini adalah VPC A. Lakukan langkah-langkah yang dijelaskan dalamBuat titik AWS Client VPN akhir.
3. Kaitkan subnet yang Anda identifikasi dengan VPN titik akhir Klien yang Anda buat. Untuk melakukan ini, lakukan langkah-langkah yang dijelaskan dalamMengaitkan jaringan target dengan titik AWS Client VPN akhir, memilih VPC dan subnet. Secara default, kami mengaitkan grup keamanan default VPC dengan VPN titik akhir Klien. 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 memberi klien akses ke targetVPC. Caranya, lakukan langkah-langkah yang dijelaskan dalam Tambahkan aturan otorisasi. Agar jaringan Tujuan diaktifkan, masukkan IPv4 CIDR rentang fileVPC.
5. Tambahkan rute untuk mengarahkan lalu lintas ke peeredVPC. Dalam diagram, ini adalah VPC B. Untuk melakukan ini, lakukan langkah-langkah yang dijelaskan dalamBuat rute AWS Client VPN titik akhir. Untuk tujuan Rute, masukkan IPv4 CIDR kisaran peeredVPC. Untuk ID VPC Subnet Target, pilih subnet yang Anda kaitkan dengan titik akhir KlienVPN.
6. Tambahkan aturan otorisasi untuk memberi klien akses ke VPC peered. Caranya, lakukan langkah-langkah yang dijelaskan dalam Tambahkan aturan otorisasi. Untuk jaringan Tujuan, masukkan IPv4 CIDR rentang peeredVPC.
7. Tambahkan aturan ke grup keamanan untuk instans Anda di VPC A dan VPC B untuk mengizinkan lalu lintas dari grup keamanan yang diterapkan VPN titik akhir Klien pada langkah 3. Untuk informasi selengkapnya, lihat Grup keamanan.

Mengakses jaringan lokal menggunakan Klien VPN

AWS Client VPN Konfigurasi untuk skenario ini hanya mencakup akses ke jaringan lokal. 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 setidaknya satu subnet. Identifikasi subnet di VPC untuk dikaitkan dengan VPN titik akhir Klien dan catat rentangnya IPv4CIDR.
- Identifikasi CIDR rentang yang sesuai untuk alamat IP klien yang tidak tumpang tindih dengan. VPC CIDR
- Tinjau aturan dan batasan untuk VPN titik akhir Klien diAturan dan praktik terbaik untuk menggunakan AWS Client VPN.

Untuk menerapkan konfigurasi ini

1. Aktifkan komunikasi antara jaringan lokal VPC dan jaringan lokal Anda sendiri melalui koneksi AWS VPN Site-to-Site. 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 AWS Direct Connect koneksi antara jaringan lokal Anda VPC dan jaringan lokal Anda. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS Direct Connect.

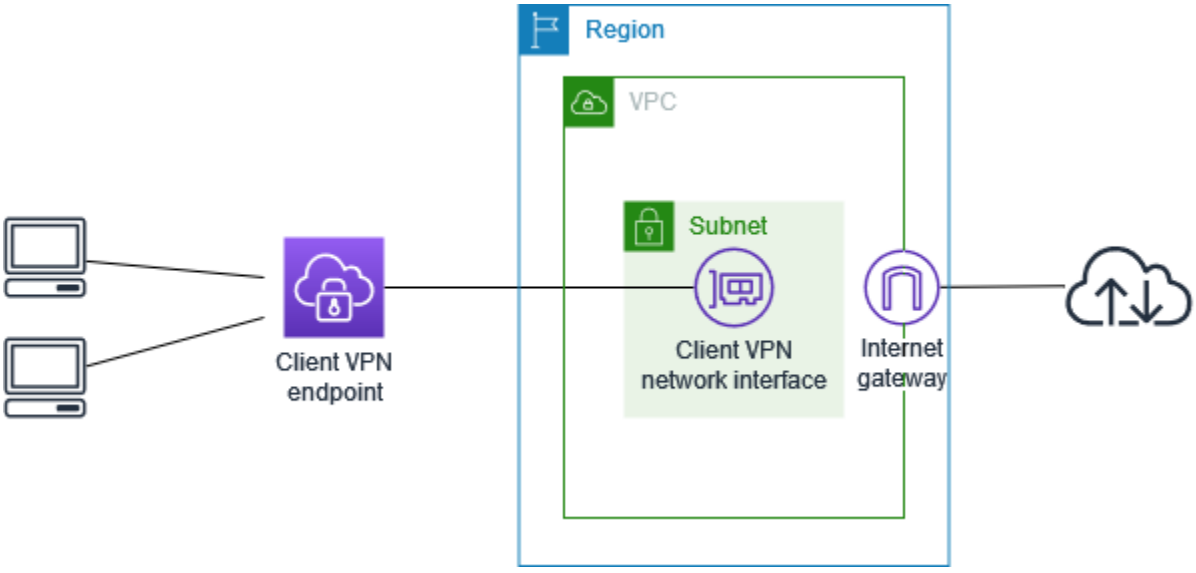
2. Uji VPN koneksi AWS Site-to-Site yang Anda buat pada langkah sebelumnya. Untuk melakukan ini, lakukan langkah-langkah yang dijelaskan dalam Menguji VPN koneksi Site-to-Site di Panduan Pengguna.AWS Site-to-Site VPN Jika VPN koneksi berfungsi seperti yang diharapkan, lanjutkan ke langkah berikutnya.

3. Buat VPN titik akhir Klien di Wilayah yang sama denganVPC. Caranya, lakukan langkah-langkah yang dijelaskan dalam Buat titik AWS Client VPN akhir.
4. Kaitkan subnet yang Anda identifikasi sebelumnya dengan titik VPN akhir Klien. Untuk melakukan ini, lakukan langkah-langkah yang dijelaskan Mengaitkan jaringan target dengan titik AWS Client VPN akhir dan pilih VPC dan subnet.
5. Tambahkan rute yang memungkinkan akses ke koneksi AWS VPN Site-to-Site. Untuk melakukan ini, lakukan langkah-langkah yang dijelaskan dalamBuat rute AWS Client VPN titik akhir; untuk tujuan Rute, masukkan IPv4 CIDR rentang VPN koneksi AWS Site-to-Site, dan untuk ID Subnet Target, pilih VPC subnet yang Anda kaitkan dengan titik akhir Klien. VPN
6. Tambahkan aturan otorisasi untuk memberi klien akses ke koneksi AWS VPN Site-to-Site. Untuk melakukan ini, lakukan langkah-langkah yang dijelaskan dalamTambahkan aturan otorisasi ke titik akhir AWS Client VPN; untuk Jaringan tujuan, masukkan rentang koneksi AWS Site-to-SiteVPN. IPv4 CIDR

Akses internet menggunakan Klien VPN

AWS Client VPN Konfigurasi untuk skenario ini mencakup satu target VPC dan akses ke internet. Kami merekomendasikan konfigurasi ini jika Anda perlu memberi klien akses ke sumber daya di dalam satu target VPC dan juga memungkinkan 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 setidaknya satu subnet. Identifikasi subnet di VPC untuk dikaitkan dengan VPN titik akhir Klien dan catat rentangnya IPv4CIDR.
- Identifikasi CIDR rentang yang sesuai untuk alamat IP klien yang tidak tumpang tindih dengan. VPC CIDR
- Tinjau aturan dan batasan untuk VPN titik akhir Klien diAturan dan praktik terbaik untuk menggunakan AWS Client VPN.

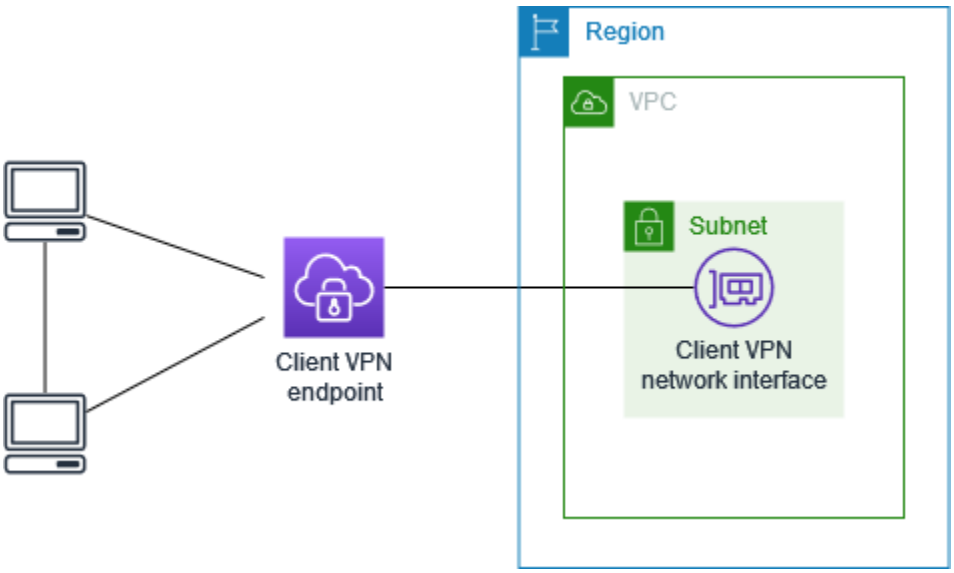
Untuk menerapkan konfigurasi ini

1. Pastikan bahwa grup keamanan yang akan Anda gunakan untuk VPN titik akhir Klien memungkinkan lalu lintas keluar ke internet. Untuk melakukan ini, tambahkan aturan keluar yang memungkinkan lalu lintas ke 0.0.0.0/0 untuk dan lalu lintas. HTTP HTTPS
2. Buat gateway internet dan lampirkan ke AndaVPC. Untuk informasi selengkapnya, lihat Membuat dan Melampirkan Internet Gateway di Panduan VPC Pengguna Amazon.
3. Buat subnet publik Anda dengan menambahkan rute ke gateway internet ke tabel rute. Di VPC konsol, pilih Subnet, pilih subnet yang ingin Anda kaitkan dengan VPN titik akhir Klien, pilih Tabel Rute, lalu 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 VPN titik akhir Klien di Wilayah yang sama denganVPC. Caranya, lakukan langkah-langkah yang dijelaskan dalam Buat titik AWS Client VPN akhir.
5. Kaitkan subnet yang Anda identifikasi sebelumnya dengan titik VPN akhir Klien. Untuk melakukan ini, lakukan langkah-langkah yang dijelaskan Mengaitkan jaringan target dengan titik AWS Client VPN akhir dan pilih VPC dan subnet.
6. Tambahkan aturan otorisasi untuk memberi klien akses ke file. VPC Untuk melakukan ini, lakukan langkah-langkah yang dijelaskan dalamTambahkan aturan otorisasi; dan untuk mengaktifkan jaringan Tujuan, masukkan IPv4 CIDR rentangVPC.
7. Tambahkan rute yang memungkinkan lalu lintas ke internet. Untuk melakukan ini, lakukan langkah-langkah yang dijelaskan diBuat rute AWS Client VPN titik akhir; untuk tujuan Rute, masukkan`0.0.0.0/0`, dan untuk ID VPC Subnet Target, pilih subnet yang Anda kaitkan dengan titik akhir KlienVPN.
8. Tambahkan aturan otorisasi untuk memberikan akses klien ke internet. Caranya, lakukan langkah-langkah yang dijelaskan dalam Tambahkan aturan otorisasi; untuk Jaringan tujuan, masukkan `0.0.0.0/0`.

9. Pastikan bahwa grup keamanan untuk sumber daya di Anda VPC memiliki aturan yang memungkinkan akses dari grup keamanan yang terkait dengan VPN titik akhir Klien. Ini memungkinkan klien Anda untuk mengakses sumber daya di AndaVPC.

C lient-to-client akses menggunakan Klien VPN

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



Sebelum memulai, lakukan hal berikut:

- Buat atau identifikasi VPC dengan setidaknya satu subnet. Identifikasi subnet di VPC untuk dikaitkan dengan VPN titik akhir Klien dan catat rentangnya IPv4CIDR.
- Identifikasi CIDR rentang yang sesuai untuk alamat IP klien yang tidak tumpang tindih dengan. VPC CIDR
- Tinjau aturan dan batasan untuk VPN titik akhir Klien diAturan dan praktik terbaik untuk menggunakan AWS Client VPN.

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

Untuk menerapkan konfigurasi ini

1. Buat VPN titik akhir Klien di Wilayah yang sama denganVPC. Caranya, lakukan langkah-langkah yang dijelaskan dalam Buat titik AWS Client VPN akhir.
2. Kaitkan subnet yang Anda identifikasi sebelumnya dengan titik VPN akhir Klien. Untuk melakukan ini, lakukan langkah-langkah yang dijelaskan Mengaitkan jaringan target dengan titik AWS Client VPN akhir dan pilih VPC dan subnet.
3. Tambahkan rute ke jaringan lokal dalam tabel rute. Caranya, lakukan langkah-langkah yang dijelaskan dalam Buat rute AWS Client VPN titik akhir. Untuk tujuan Rute, masukkan CIDR rentang klien, dan untuk ID VPC Subnet Target, tentukan`local`.
4. Tambahkan aturan otorisasi untuk memberi klien akses ke file. VPC Caranya, lakukan langkah-langkah yang dijelaskan dalam Tambahkan aturan otorisasi. Agar jaringan Tujuan diaktifkan, masukkan IPv4 CIDR rentang fileVPC.
5. Tambahkan aturan otorisasi untuk memberi klien akses ke CIDR rentang klien. Caranya, lakukan langkah-langkah yang dijelaskan dalam Tambahkan aturan otorisasi. Agar jaringan Tujuan diaktifkan, masukkan CIDR rentang klien.

Batasi akses ke jaringan Anda menggunakan Klien VPN

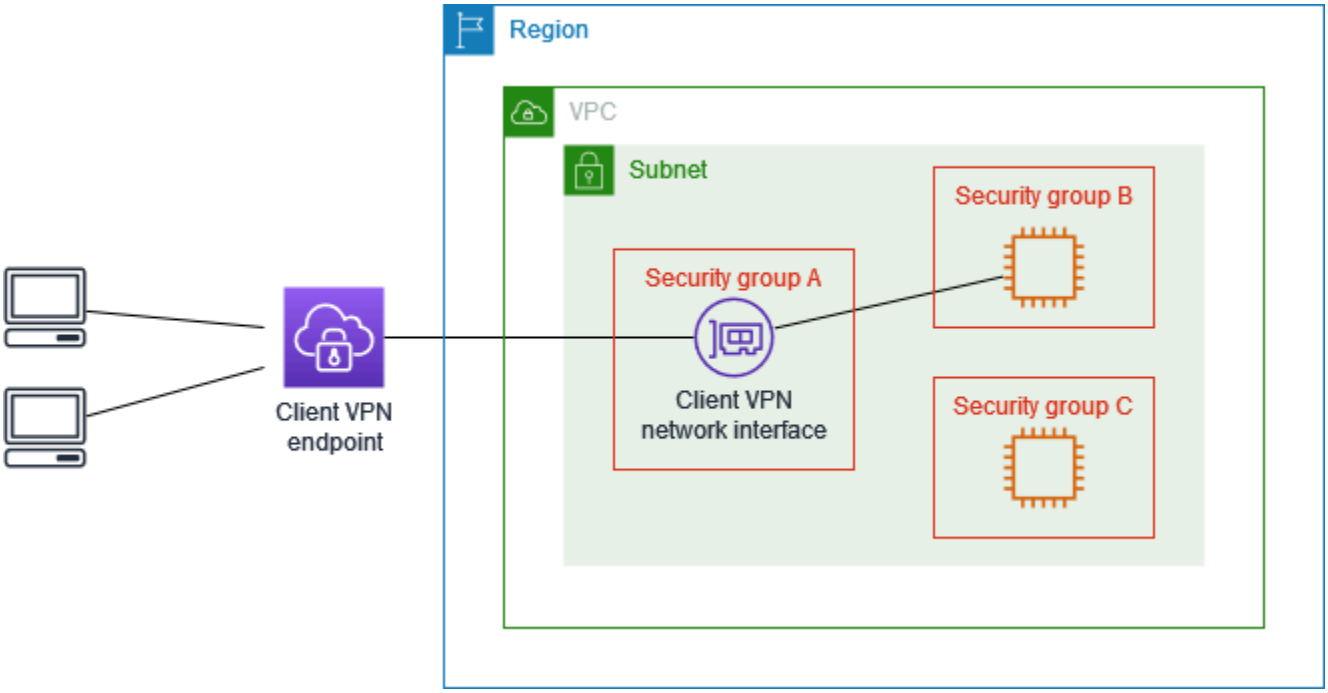
Anda dapat mengonfigurasi AWS Client VPN titik akhir Anda untuk membatasi akses ke sumber daya tertentu di Anda. VPC Untuk otentikasi berbasis pengguna, Anda juga dapat membatasi akses ke bagian jaringan Anda, berdasarkan grup pengguna yang mengakses titik akhir Klien. VPN

Membatasi akses menggunakan grup keamanan

Anda dapat memberikan atau menolak akses ke sumber daya tertentu VPC dengan menambahkan atau menghapus aturan grup keamanan yang mereferensikan grup keamanan yang diterapkan ke asosiasi jaringan target (grup VPN keamanan Klien). Konfigurasi ini diperluas pada skenario yang dijelaskan dalam Akses VPC menggunakan Klien 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 memungkinkan lalu lintas dari grup VPN keamanan Klien.

Dalam diagram berikut, grup keamanan A adalah grup VPN keamanan Klien, grup keamanan B dikaitkan dengan sebuah EC2 instance, dan grup keamanan C dikaitkan dengan sebuah EC2 instance. 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 Anda mulai, periksa apakah grup VPN keamanan Klien dikaitkan dengan sumber daya lain di AndaVPC. Jika Anda menambahkan atau menghapus aturan yang mereferensikan grup VPN keamanan Klien, Anda juga dapat memberikan atau menolak akses untuk sumber daya terkait lainnya. Untuk mencegah hal ini, gunakan grup keamanan yang dibuat khusus untuk digunakan dengan VPN titik akhir Klien Anda.

Untuk membuat aturan grup keamanan

1. Buka VPC konsol Amazon 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, lalu masukkan atau pilih ID grup VPN keamanan Klien.
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 memungkinkan lalu lintas dari grup VPN keamanan Klien, hapus.

Untuk memeriksa aturan grup keamanan Anda

1. Buka VPC konsol Amazon 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 di mana Sumber adalah grup VPN keamanan Klien, pilih Edit Aturan, dan pilih Hapus (ikon x) untuk aturan tersebut. Pilih Simpan aturan.

Membatasi akses berdasarkan grup pengguna

Jika VPN titik akhir Klien Anda dikonfigurasi untuk otentikasi berbasis pengguna, Anda dapat memberikan akses kepada grup pengguna tertentu ke bagian tertentu dari 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 di Klien VPN
   - Persyaratan dan pertimbangan untuk otentikasi federasi SAML berbasis
2. Buat aturan otorisasi untuk VPN titik akhir Klien Anda yang memungkinkan akses grup tertentu ke semua atau sebagian jaringan Anda. Untuk informasi selengkapnya, lihat AWS Client VPN aturan otorisasi.

Jika VPN titik akhir Klien Anda 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 tertentu dari jaringan

Anda, Anda dapat membuat beberapa VPN titik akhir Klien. 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 Otentikasi timbal balik di AWS Client VPN.
2. Buat VPN titik akhir Klien. Untuk informasi selengkapnya, lihat Buat titik AWS Client VPN akhir.
3. Buat aturan otorisasi yang memberikan akses ke semua atau sebagian jaringan Anda. Misalnya, untuk VPN titik akhir Klien yang digunakan oleh administrator, Anda dapat membuat aturan otorisasi yang memberikan akses ke seluruh jaringan. Untuk informasi selengkapnya, lihat Tambahkan aturan otorisasi.

Otentikasi klien di AWS Client VPN

Otentikasi klien diimplementasikan pada titik pertama masuk ke AWS Cloud. Ini digunakan untuk menentukan apakah klien diizinkan untuk terhubung ke VPN titik akhir Klien. Jika otentikasi berhasil, klien terhubung ke VPN titik akhir Klien dan membuat sesi. VPN Jika otentikasi gagal, koneksi ditolak dan klien dicegah membuat VPN sesi.

Klien VPN menawarkan jenis otentikasi klien berikut:

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

Anda dapat menggunakan salah satu metode sebelumnya saja, atau Anda dapat menggunakan 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 VPN titik akhir Klien, 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 Otentikasi timbal balik di AWS Client VPN.

Autentikasi Direktori Aktif di Klien VPN

Klien 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, Klien 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.

Klien VPN mendukung otentikasi multi-faktor (MFA) saat diaktifkan untuk Managed AWS Microsoft AD atau AD Connector. Jika MFA diaktifkan, klien harus memasukkan nama pengguna, kata sandi, dan MFA kode saat mereka terhubung ke VPN titik akhir Klien. Untuk informasi selengkapnya tentang mengaktifkanMFA, lihat Mengaktifkan Otentikasi Multi-Faktor untuk AWS Microsoft AD yang Dikelola dan Aktifkan Otentikasi Multi-Faktor untuk Konektor AD di Panduan Administrasi.AWS Directory Service

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

Otentikasi timbal balik di AWS Client VPN

Dengan otentikasi timbal balik, Klien VPN menggunakan sertifikat untuk melakukan otentikasi antara klien dan server. Sertifikat adalah bentuk identifikasi digital yang diterbitkan oleh otoritas sertifikat (CA). Server menggunakan sertifikat klien untuk mengautentikasi klien ketika mereka mencoba untuk terhubung ke titik VPN akhir Klien. 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 VPN titik akhir Klien. Saat Anda mengunggah sertifikat server keACM, Anda juga menentukan otoritas sertifikat (CA). Anda hanya perlu mengunggah sertifikat klien ACM ketika CA sertifikat klien berbeda dari CA sertifikat server. Untuk informasi selengkapnyaACM, lihat Panduan AWS Certificate Manager Pengguna.

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

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

Tugas

- Aktifkan otentikasi timbal balik untuk AWS Client VPN
- Perbarui sertifikat server Anda untuk AWS Client VPN

Aktifkan otentikasi timbal balik untuk AWS Client VPN

Anda dapat mengaktifkan otentikasi timbal balik di Klien VPN baik di Linux/macOS atau Windows.

Linux/macOS

Prosedur berikut menggunakan Open VPN easy-rsa untuk menghasilkan sertifikat dan kunci server dan klien, dan kemudian mengunggah sertifikat server dan kunci ke. ACM Untuk informasi selengkapnya, lihat Mulai Cepat README Mudah- RSA 3.

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

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

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

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

2. Menginisialisasi PKI lingkungan 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 sertifikat klien dan kunci keACM. Pastikan untuk mengunggahnya di Wilayah yang sama di mana Anda ingin membuat VPN titik akhir Klien.

Perintah berikut menggunakan AWS CLI untuk mengunggah sertifikat. Untuk mengunggah sertifikat menggunakan ACM konsol, lihat Mengimpor sertifikat di Panduan AWS Certificate Manager 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 keACM. 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 VPN titik akhir Klien. 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 RSArilis Mudah dan unduh ZIP file 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 Easy RSA 3.

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

4. Menginisialisasi PKI lingkungan 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 Easy RSA 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 keACM. Pastikan untuk mengunggahnya di Wilayah yang sama di mana Anda ingin membuat VPN titik akhir Klien. Perintah berikut menggunakan AWS CLI untuk meng-upload sertifikat. Untuk mengunggah sertifikat menggunakan ACM konsol, lihat Mengimpor sertifikat di Panduan AWS Certificate Manager 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 keACM. 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 VPN titik akhir Klien. Pada langkah-langkah di atas, CA yang sama telah digunakan untuk membuat kedua sertifikat. Namun, langkah-langkah untuk mengunggah sertifikat klien disertakan untuk kelengkapan.

Perbarui sertifikat server Anda untuk AWS Client VPN

Anda dapat memperbarui dan mengimpor ulang sertifikat VPN server Klien yang telah kedaluwarsa. Tergantung pada versi Open VPN easy-rsa yang Anda gunakan, prosedurnya akan bervariasi. Lihat Dokumentasi Pembaruan dan Pencabutan Sertifikat Mudah- RSA 3 untuk lebih jelasnya.

Untuk memperbarui sertifikat server Anda

1. Lakukan salah satu hal berikut:
   - Mudah- RSA versi 3.1.x
     - Jalankan perintah perpanjangan sertifikat.

       ```
       $ ./easyrsa renew server nopass
       ```
   - Mudah- RSA versi 3.2.x

     a. Jalankan perintah kedaluwarsa.

     ```
     $ ./easyrsa expire server
     ```

     b. Tanda tangani sertifikat baru.

     ```
     $ ./easyrsa sign-req server server
     ```
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 keACM. Pastikan untuk mengimpornya di Wilayah yang sama dengan VPN titik akhir Klien.

```
$ aws acm import-certificate \
    --certificate fileb://server.crt \
    --private-key fileb://server.key \
    --certificate-chain fileb://ca.crt \
    --certificate-arn
 arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-12345678901
```

Sistem masuk tunggal - otentikasi federasi SAML berbasis 2.0 - di Klien VPN

AWS Client VPN mendukung federasi identitas dengan Security Assertion Markup Language 2.0 (SAML2.0) untuk titik akhir Klien. VPN Anda dapat menggunakan penyedia identitas (IdPs) yang mendukung SAML 2.0 untuk membuat identitas pengguna terpusat. Anda kemudian dapat mengonfigurasi VPN titik akhir Klien untuk menggunakan otentikasi federasi SAML berbasis, dan mengaitkannya dengan IDP. Pengguna kemudian terhubung ke VPN titik akhir Klien menggunakan kredensialnya yang terpusat.

Topik

- Aktifkan SAML untuk AWS Client VPN
- Alur kerja autentikasi
- Persyaratan dan pertimbangan untuk otentikasi federasi SAML berbasis
- SAMLsumber daya konfigurasi iDP berbasis

Aktifkan SAML untuk AWS Client VPN

Untuk mengaktifkan IDP SAML berbasis Anda bekerja dengan VPN titik akhir Klien, Anda harus melakukan hal berikut.

1. Buat aplikasi SAML berbasis 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 SAMLsumber daya konfigurasi iDP berbasis.
3. Di IdP Anda, buat dan unduh dokumen metadata federasi yang menjelaskan organisasi Anda sebagai IdP.

   XMLDokumen yang ditandatangani ini digunakan untuk membangun hubungan kepercayaan antara AWS dan IDP.
4. Buat penyedia IAM SAML identitas di AWS akun yang sama dengan VPN titik akhir Klien.

   Penyedia IAM SAML identitas mendefinisikan hubungan IDP AWS untuk mempercayai organisasi Anda menggunakan dokumen metadata yang dihasilkan oleh iDP. Untuk informasi selengkapnya, lihat Membuat Penyedia IAM SAML Identitas di Panduan IAM Pengguna. Jika nanti Anda memperbarui konfigurasi aplikasi di iDP, buat dokumen metadata baru dan perbarui penyedia identitas Anda. IAM SAML

   > **Note**
   >
   > Anda tidak perlu membuat IAM peran untuk menggunakan penyedia IAM SAML identitas.
5. Buat VPN titik akhir Klien.

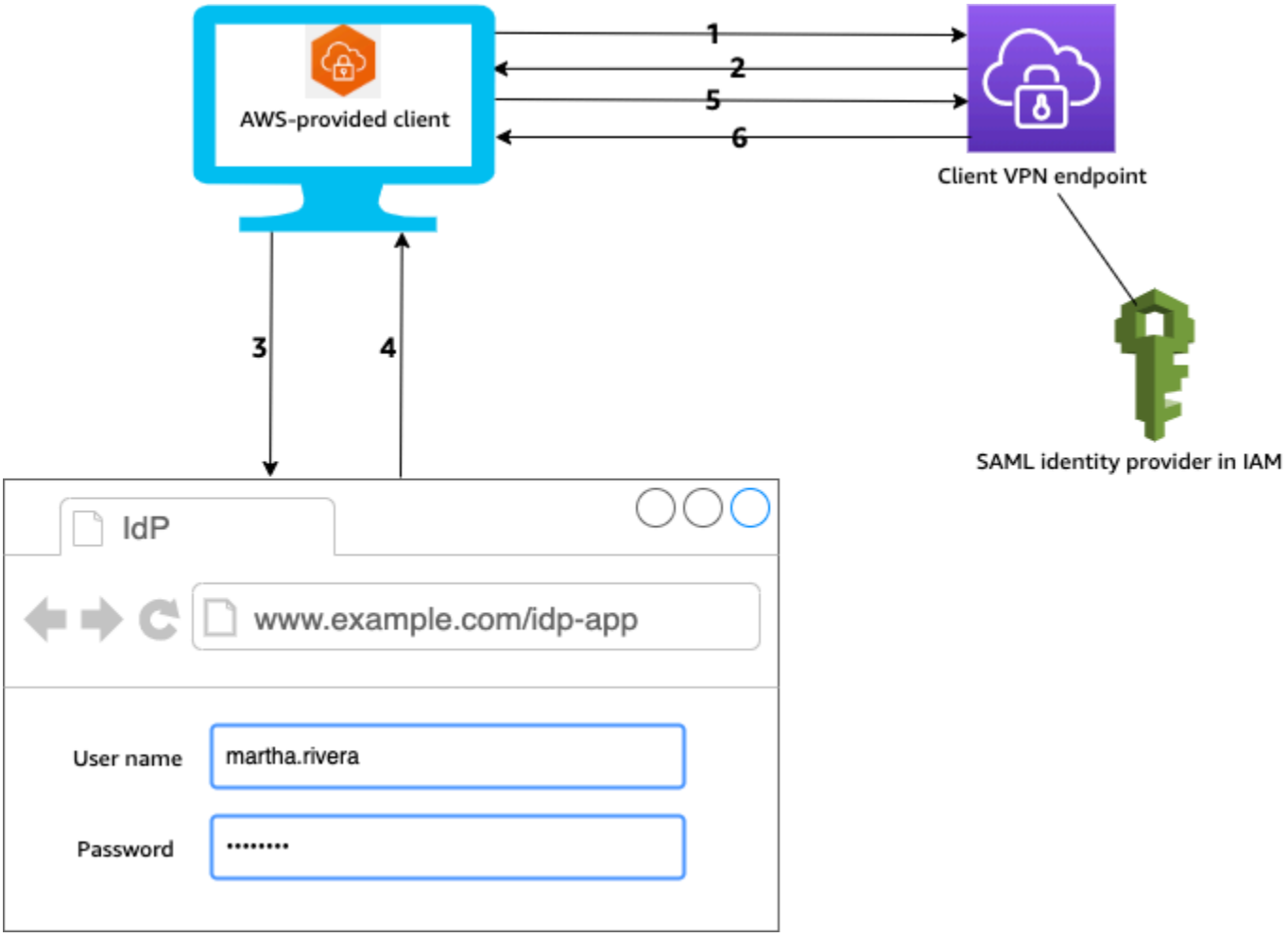
   Tentukan otentikasi federasi sebagai jenis otentikasi, dan tentukan penyedia IAM SAML identitas yang Anda buat. Untuk informasi selengkapnya, lihat Buat titik AWS Client VPN akhir.
6. Ekspor file konfigurasi klien dan mendistribusikannya ke pengguna Anda. Instruksikan pengguna Anda untuk mengunduh versi terbaru dari klien yang AWS disediakan, dan menggunakannya untuk memuat file konfigurasi dan terhubung ke titik VPN akhir Klien.

   Atau, jika Anda mengaktifkan portal swalayan untuk VPN titik akhir Klien Anda, instruksikan pengguna Anda untuk pergi ke portal swalayan untuk mendapatkan file konfigurasi dan klien

yang disediakan. AWS Untuk informasi selengkapnya, lihat AWS Client VPN akses ke portal swalayan.

Alur kerja autentikasi

Diagram berikut memberikan ikhtisar alur kerja otentikasi untuk VPN titik akhir Klien yang menggunakan otentikasi federasi SAML berbasis. Saat Anda membuat dan mengonfigurasi VPN titik akhir Klien, Anda menentukan penyedia IAM SAML identitas.



1. Pengguna membuka klien yang AWS disediakan di perangkat mereka dan memulai koneksi ke titik VPN akhir Klien.
2. VPNEndpoint Klien mengirimkan URL IDP dan permintaan otentikasi kembali ke klien, berdasarkan informasi yang diberikan dalam IAM SAML penyedia identitas.
3. Klien yang AWS disediakan membuka jendela browser baru di perangkat pengguna. Peramban membuat permintaan ke IdP dan menampilkan halaman login.

4. Pengguna memasukkan kredensialnya di halaman login, dan iDP mengirimkan SAML pernyataan yang ditandatangani kembali ke klien.
5. Klien AWS yang disediakan mengirimkan SAML pernyataan ke titik akhir KlienVPN.
6. VPNTitik akhir Klien memvalidasi pernyataan dan mengizinkan atau menolak akses ke pengguna.

Persyaratan dan pertimbangan untuk otentikasi federasi SAML berbasis

Berikut ini adalah persyaratan dan pertimbangan untuk otentikasi federasi SAML berbasis.

- Untuk kuota dan aturan untuk mengonfigurasi pengguna dan grup dalam SAML iDP berbasis, lihat. Kuota pengguna dan grup
- SAMLPernyataan dan SAML dokumen harus ditandatangani.
- AWS Client VPN hanya mendukung kondisi AudienceRestriction "" dan NotOnOrAfter "NotBefore dan" dalam SAML pernyataan.
- Ukuran maksimum yang didukung untuk SAML respons adalah 128 KB.
- AWS Client VPN tidak menyediakan permintaan otentikasi yang ditandatangani.
- SAMLlogout tunggal tidak didukung. Pengguna dapat keluar dengan memutuskan sambungan dari klien yang AWS disediakan, atau Anda dapat menghentikan koneksi.
- VPNEndpoint Klien hanya mendukung satu IDP.
- Autentikasi multi-faktor (MFA) didukung saat diaktifkan di IDP Anda.
- Pengguna harus menggunakan klien yang AWS disediakan untuk terhubung ke VPN titik akhir Klien. 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 AWS yang disediakan mencadangkan TCP port 35001 pada perangkat pengguna untuk respons. SAML
- Jika dokumen metadata untuk penyedia IAM SAML identitas diperbarui dengan salah atau berbahayaURL, ini dapat menyebabkan masalah otentikasi bagi pengguna, atau mengakibatkan serangan phishing. Oleh karena itu, kami menyarankan Anda menggunakan AWS CloudTrail untuk memantau pembaruan yang dibuat untuk penyedia IAM SAML identitas. Untuk informasi selengkapnya, lihat Logging IAM dan AWS STS panggilan dengan AWS CloudTrail di Panduan IAM Pengguna.

- AWS Client VPN mengirimkan permintaan AuthN ke IDP melalui pengikatan Pengalihan. HTTP Oleh karena itu, iDP harus mendukung pengikatan HTTP Pengalihan dan harus ada dalam dokumen metadata iDP.
- Untuk SAML pernyataan, Anda harus menggunakan format alamat email untuk atribut. `NameID`

SAMLsumber daya konfigurasi iDP berbasis

Tabel berikut mencantumkan SAML berbasis 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 SAML
Direktori Aktif Microsoft Azure	Untuk informasi selengkapnya, lihat Tutorial: Integrasi sistem masuk tunggal (SSO) Azure Active Directory dengan AWS Klien di situs VPN web dokumentasi Microsoft.
JumpCloud	Single Sign On (SSO) dengan AWS Client VPN
AWS IAM Identity Center	Menggunakan Pusat IAM Identitas dengan AWS Client VPN otentikasi dan otorisasi

Informasi penyedia layanan untuk membuat aplikasi

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

- Pernyataan Layanan Konsumen ()ACS: URL `http://127.0.0.1:35001`
- PemirsaURI: `urn:amazon:webservices:clientvpn`

Setidaknya satu atribut harus disertakan dalam SAML respon dari IDP. Berikut ini adalah contoh atribut.

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

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

Dukungan untuk portal layanan mandiri

Jika Anda mengaktifkan portal layanan mandiri untuk VPN titik akhir Klien Anda, pengguna masuk ke portal menggunakan kredensi SAML IDP berbasis mereka.

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

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

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

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

Jika IDP Anda tidak mendukung beberapa ACSURLs, lakukan hal berikut:

1. Buat aplikasi SAML berbasis tambahan di IDP Anda dan tentukan yang berikut ini. ACS URL

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

2. Buat dan unduh dokumen metadata federasi.
3. Buat penyedia IAM SAML identitas di AWS akun yang sama dengan VPN titik akhir Klien. Untuk informasi selengkapnya, lihat Membuat Penyedia IAM SAML Identitas di Panduan IAM Pengguna.

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

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

Otorisasi klien di AWS Client VPN

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

Grup keamanan

Saat Anda membuat VPN titik akhir Klien, Anda dapat menentukan grup keamanan dari yang spesifik VPC untuk diterapkan ke titik VPN akhir Klien. Saat Anda mengaitkan subnet dengan VPN titik akhir Klien, kami secara otomatis menerapkan grup VPC keamanan default. Anda dapat mengubah grup keamanan setelah membuat VPN titik akhir Klien. Untuk informasi selengkapnya, lihat Menerapkan grup keamanan ke jaringan target di AWS Client VPN. Grup keamanan dikaitkan dengan antarmuka VPN jaringan Klien.

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

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

Untuk informasi selengkapnya tentang grup keamanan, lihat Grup keamanan untuk Anda VPC di Panduan VPC Pengguna Amazon.

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 Active Directory atau grup IDP SAML berbasis yang diizinkan akses. Hanya untuk pengguna grup ini yang dapat mengakses jaringan yang ditentukan. Jika Anda tidak menggunakan Active Directory atau autentikasi federasi SAML berbasis, atau Anda ingin membuka akses ke semua pengguna, Anda dapat menentukan aturan yang memberikan akses ke semua klien. Untuk informasi selengkapnya, lihat AWS Client VPN aturan otorisasi.

Tugas

- Membuat aturan grup keamanan AWS Client VPN endpoint

Membuat aturan grup keamanan AWS Client VPN endpoint

Buat VPN aturan Klien yang mengizinkan lalu lintas dari grup keamanan VPN titik akhir Klien.

Untuk menambahkan aturan yang memungkinkan lalu lintas dari grup keamanan VPN titik akhir Klien

1. Buka VPC konsol Amazon 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 Tipe, 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 VPN akhir Klien.
6. Pilih Simpan aturan.

Otorisasi koneksi di AWS Client VPN

Anda dapat mengonfigurasi handler koneksi klien untuk titik VPN akhir Klien Anda. Handler memungkinkan Anda untuk menjalankan logika kustom yang mengotorisasi koneksi baru,

berdasarkan atribut perangkat, pengguna, dan koneksi. Client connect handler berjalan setelah VPN layanan Klien mengautentikasi perangkat dan pengguna.

Untuk mengonfigurasi pengendali koneksi klien untuk VPN titik akhir Klien Anda, buat AWS Lambda fungsi yang menggunakan atribut perangkat, pengguna, dan koneksi sebagai input, dan kembalikan keputusan ke VPN layanan Klien untuk mengizinkan atau menolak koneksi baru. Anda menentukan fungsi Lambda di titik akhir Klien VPN Anda. Saat perangkat terhubung ke VPN titik akhir Klien Anda, VPN layanan Klien akan memanggil fungsi Lambda atas nama Anda. Hanya koneksi yang diizinkan oleh fungsi Lambda yang diizinkan untuk terhubung ke titik akhir KlienVPN.

> **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 KlienVPN.
- 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 dipanggil untuk koneksi baru dan VPN layanan Klien tidak mendapatkan respons yang diharapkan dari fungsi tersebut, VPN layanan Klien 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 yang ada ke VPN titik akhir Klien tidak terpengaruh. Anda dapat mengakhiri koneksi yang ada, dan kemudian menginstruksikan klien Anda untuk membuat koneksi baru. Untuk informasi selengkapnya, lihat Mengakhiri koneksi AWS Client VPN klien.

- Jika klien menggunakan klien yang AWS disediakan untuk terhubung ke VPN titik akhir Klien, 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 mengambil atribut perangkat, atribut pengguna, dan atribut koneksi sebagai input dari layanan Klien. VPN Kemudian harus mengembalikan keputusan ke VPN layanan Klien apakah akan mengizinkan atau menolak koneksi.

Meminta skema

Fungsi Lambda mengambil JSON gumpalan yang berisi 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 VPN titik akhir Klien.
- `endpoint-id`— ID dari VPN titik akhir Klien.
- `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 otentikasi federasi SAML berbasis, ini adalah. `NameID` Untuk autentikasi bersama, bidang ini kosong.
- `platform` — Platform sistem operasi klien.

- `platform-version` — Versi sistem operasi. VPNLayanan Klien memberikan nilai ketika `--push-peer-info` direktif hadir dalam konfigurasi VPN klien Terbuka ketika klien terhubung ke VPN titik akhir Klien, dan ketika klien menjalankan platform Windows.
- `public-ip` — Alamat IP publik dari perangkat yang terhubung.
- `client-openvpn-version`— VPN Versi Terbuka 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 otentikasi federasi SAML berbasis, ini akan menjadi daftar grup penyedia identitas (iDP). Untuk autentikasi bersama, bidang ini kosong.
- `schema-version` — Versi skema. Default-nya 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. Default-nya adalah `v3`.

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

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

Gunakan penangan koneksi klien untuk penilaian postur

Anda dapat menggunakan pengendali sambungan klien untuk mengintegrasikan VPN titik akhir Klien Anda dengan solusi manajemen perangkat yang ada untuk mengevaluasi kepatuhan postur perangkat yang menghubungkan. Agar fungsi Lambda berfungsi sebagai penangan otorisasi perangkat, gunakan otentikasi timbal balik untuk titik akhir Klien Anda. VPN Buat sertifikat dan kunci klien unik untuk setiap klien (perangkat) yang akan terhubung ke VPN titik akhir Klien. Fungsi Lambda dapat menggunakan nama umum yang unik untuk sertifikat klien (yang diteruskan dari VPN layanan Klien) untuk mengidentifikasi perangkat dan mengambil status kepatuhan posturnya 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 `platform` dan `platform-version` bidang yang diteruskan ke fungsi Lambda oleh layanan KlienVPN.

> **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.

Aktifkan handler koneksi klien

Untuk mengaktifkan pengendali sambungan klien, buat atau ubah VPN titik akhir Klien dan tentukan Nama Sumber Daya Amazon (ARN) dari fungsi Lambda. Untuk informasi selengkapnya, silakan lihat Buat titik AWS Client VPN akhir dan Memodifikasi AWS Client VPN titik akhir.

Peran yang terhubung dengan layanan

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

Pantau kegagalan otorisasi koneksi

Anda dapat melihat status otorisasi koneksi koneksi ke titik VPN akhir Klien. Untuk informasi selengkapnya, lihat Lihat koneksi AWS Client VPN klien.

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

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

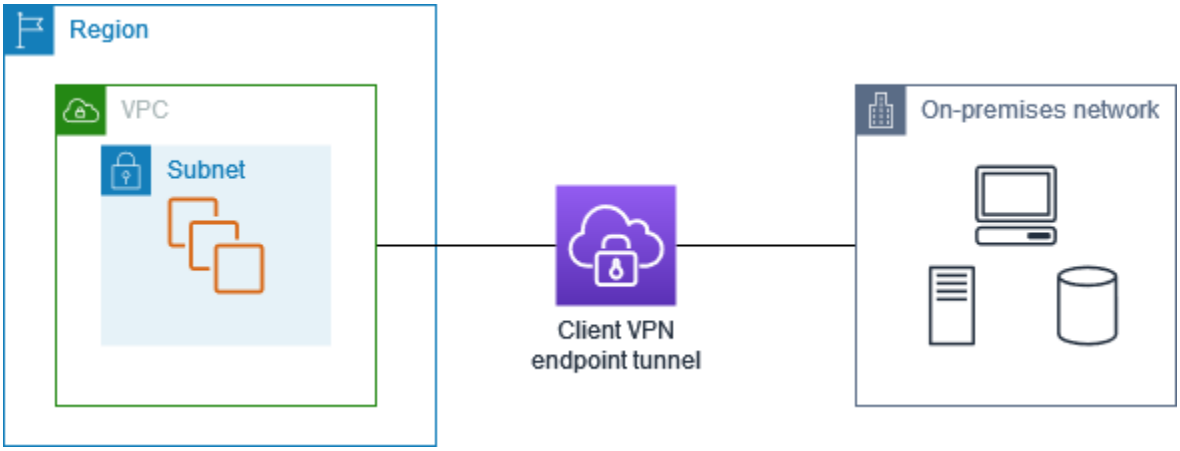
- `client-connect-failed` — Fungsi Lambda mencegah koneksi dibuat.
- `client-connect-handler-timed-out` — Waktu fungsi Lambda habis.
- `client-connect-handler-other-execution-error` — Fungsi Lambda mengalami kesalahan tak terduga.
- `client-connect-handler-throttled` — Fungsi Lambda ter-throttling.
- `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 Klien VPN

Secara default, ketika Anda memiliki VPN titik akhir Klien, semua lalu lintas dari klien dirutekan melalui terowongan KlienVPN. Saat Anda mengaktifkan split-tunnel pada VPN titik akhir Klien, kami mendorong rute pada tabel rute VPN titik akhir Klien ke perangkat yang terhubung ke titik akhir Klien. VPN Ini memastikan bahwa hanya lalu lintas dengan tujuan ke jaringan yang cocok dengan rute dari tabel rute VPN titik akhir Klien yang dirutekan melalui terowongan KlienVPN.

Anda dapat menggunakan VPN titik akhir Klien split-tunnel ketika Anda tidak ingin semua lalu lintas pengguna merutekan melalui titik akhir Klien. VPN

Dalam contoh berikut, split-tunnel diaktifkan pada titik akhir KlienVPN. Hanya lalu lintas yang ditujukan untuk VPC (`172.31.0.0/16`) yang dialihkan melalui terowongan KlienVPN. Lalu lintas yang ditujukan untuk sumber daya lokal tidak dirutekan melalui terowongan Klien. VPN



Manfaat terowongan terpisah

Split-tunnel pada VPN titik akhir Klien menawarkan manfaat berikut:

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

Pertimbangan perutean

- Saat Anda mengaktifkan mode split-tunnel, semua rute dalam tabel rute VPN titik akhir Klien ditambahkan ke tabel rute klien saat VPN koneksi dibuat. Operasi ini berbeda dari perilaku default, yang menimpa tabel rute klien dengan entri `0.0.0.0/0` untuk merutekan semua lalu lintas di atasVPN.

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

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

Mengaktifkan split-tunnel

Anda dapat mengaktifkan split-tunnel pada titik akhir Klien VPN baru atau yang sudah ada. Untuk informasi selengkapnya, lihat topik berikut.

- Buat titik AWS Client VPN akhir
- Memodifikasi AWS Client VPN titik akhir

Pencatatan koneksi untuk titik AWS Client VPN akhir

Pencatatan koneksi adalah fitur AWS Client VPN yang memungkinkan Anda untuk menangkap log koneksi untuk VPN titik akhir Klien Anda.

Log koneksi berisi entri log koneksi yang menangkap informasi tentang peristiwa koneksi, seperti ketika klien (pengguna akhir) terhubung, mencoba menghubungkan, atau memutuskan sambungan dari titik akhir Klien VPN Anda. Anda dapat menggunakan informasi ini untuk menjalankan forensik, menganalisis bagaimana VPN titik akhir Klien Anda digunakan, atau men-debug masalah koneksi.

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

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

Entri log koneksi

Entri log koneksi adalah gumpalan JSON -format pasangan kunci-nilai. 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 VPN titik akhir Klien 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 IPv4 CIDR rentang klien untuk titik VPN akhir Klien.
- `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 atauSAML) 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 AWS Client VPN log koneksi.

Pertimbangan VPN penskalaan klien

Saat Anda membuat VPN titik akhir Klien, pertimbangkan jumlah maksimum VPN koneksi bersamaan yang ingin Anda dukung. Anda harus mempertimbangkan jumlah klien yang saat ini Anda dukung, dan apakah VPN titik akhir Klien Anda dapat menskalakan untuk memenuhi permintaan tambahan jika diperlukan.

Faktor-faktor berikut mempengaruhi jumlah maksimum VPN koneksi bersamaan yang dapat didukung pada titik VPN akhir Klien:

Ukuran CIDR rentang klien

Ketika Anda membuat VPN endpoint Klien, Anda harus menentukan CIDR rentang klien, yang merupakan IPv4 CIDR blok antara netmask /12 dan /22. Setiap VPN koneksi ke VPN titik akhir

Klien diberi alamat IP unik dari CIDR rentang klien. Sebagian alamat dalam CIDR rentang klien juga digunakan untuk mendukung model ketersediaan VPN titik akhir Klien, dan tidak dapat ditetapkan ke klien. Anda tidak dapat mengubah CIDR rentang klien setelah Anda membuat VPN titik akhir Klien.

Secara umum, kami menyarankan Anda menentukan CIDR rentang klien yang berisi dua kali jumlah alamat IP (dan karena itu koneksi bersamaan) yang Anda rencanakan untuk mendukung pada titik VPN akhir Klien.

Jumlah subnet terkait

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

Berikut ini adalah jumlah VPN koneksi bersamaan yang didukung berdasarkan jumlah asosiasi subnet untuk titik akhir KlienVPN.

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 VPN akhir Klien. Oleh karena itu, jumlah asosiasi subnet juga tergantung pada jumlah Availability Zone yang tersedia di suatu AWS Wilayah.

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

Jika Anda tidak yakin berapa jumlah VPN koneksi yang diharapkan untuk VPN titik akhir Klien Anda, sebaiknya tentukan /16 CIDR blok ukuran atau lebih besar.

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

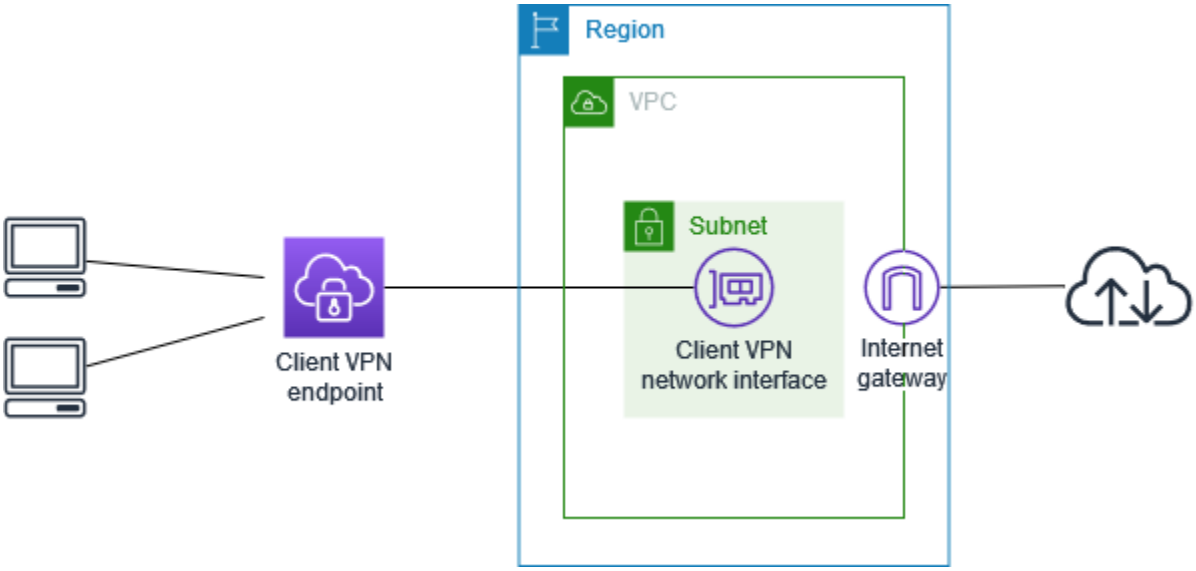
Untuk informasi selengkapnya tentang kuota untuk VPN titik akhir Klien Anda, lihat. AWS Client VPN kuota

Memulai dengan AWS Client VPN

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

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

Diagram berikut mewakili konfigurasi VPN endpoint Anda VPC dan Klien setelah Anda menyelesaikan tutorial ini.



Langkah-langkah

- Prasyarat
- Langkah 1: Menghasilkan server, sertifikat klien, dan kunci
- Langkah 2: Buat titik VPN akhir Klien
- 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 VPN titik akhir Klien
- Langkah 8: Connect ke VPN endpoint Klien

Prasyarat

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

- Izin yang diperlukan untuk bekerja dengan titik VPN akhir Klien.
- Izin yang diperlukan untuk mengimpor sertifikat ke dalam AWS Certificate Manager.
- A VPC dengan setidaknya 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, Klien VPN menggunakan sertifikat untuk melakukan otentikasi antara klien dan titik akhir KlienVPN. 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 VPN titik akhir Klien. Mengimpor sertifikat klien ke dalam ACM adalah opsional.

Jika Anda belum memiliki sertifikat untuk digunakan untuk tujuan ini, mereka dapat dibuat menggunakan utilitas Open VPN easy-rsa. Untuk langkah-langkah rinci untuk menghasilkan server dan sertifikat klien dan kunci menggunakan utilitas Open VPN easy-rsa, dan impor mereka ke ACM see. Otentikasi timbal balik di AWS Client VPN

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

Langkah 2: Buat titik VPN akhir Klien

VPNEndpoint Klien adalah sumber daya yang Anda buat dan konfigurasikan untuk mengaktifkan dan mengelola VPN sesi klien. Ini adalah titik terminasi untuk semua VPN sesi klien.

Untuk membuat titik VPN akhir Klien

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

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

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

5. Untuk sertifikat Server ARN, pilih sertifikat server yang Anda buat di Langkah 1. ARN
6. Di bawah Opsi otentikasi, pilih Gunakan otentikasi bersama, lalu untuk sertifikat Klien ARN, pilih sertifikat yang ingin Anda gunakan sebagai sertifikat klien. ARN

   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. (Opsional) Tentukan DNS server mana yang akan digunakan untuk DNS resolusi. Untuk menggunakan DNS server khusus, untuk alamat IP DNS DNS Server 1 dan alamat IP Server 2, tentukan alamat IP DNS server yang akan digunakan. Untuk menggunakan VPC DNS server, baik untuk alamat IP DNS DNS Server 1 atau alamat IP Server 2, tentukan alamat IP, dan tambahkan alamat IP VPC DNS server.

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

8. Simpan sisa pengaturan default, dan pilih Create Client VPN endpoint.

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

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

Langkah 3: Kaitkan jaringan target

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

Untuk mengaitkan jaringan target dengan titik VPN akhir Klien

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik VPNAkhir Klien.
3. Pilih VPN titik akhir Klien yang Anda buat dalam prosedur sebelumnya, lalu pilih Asosiasi jaringan target, Jaringan target asosiasi.
4. Untuk VPC, pilih VPC di mana subnet berada.
5. Untuk Pilih subnet untuk diasosiasikan, pilih subnet untuk dikaitkan dengan titik akhir KlienVPN.
6. Pilih Jaringan target asosiasi.
7. Jika aturan otorisasi mengizinkannya, satu asosiasi subnet sudah cukup bagi klien untuk mengakses seluruh jaringan. VPC Anda dapat mengaitkan subnet tambahan untuk menyediakan ketersediaan tinggi jika Availability Zone menjadi terganggu.

Ketika Anda mengaitkan subnet pertama dengan VPN titik akhir Klien, hal berikut terjadi:

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

Langkah 4: Tambahkan aturan otorisasi untuk VPC

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

Untuk menambahkan aturan otorisasi untuk VPC

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.

2. Di panel navigasi, pilih Titik VPNAkhir Klien.
3. Pilih VPN titik akhir Klien 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. Misalnya, untuk memungkinkan akses ke keseluruhanVPC, tentukan IPv4 CIDR blokVPC.
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 memberikan akses ke jaringan tambahan yang terhubung keVPC, seperti AWS layanan, peeredVPCs, jaringan lokal, dan internet. Untuk setiap jaringan tambahan, Anda menambahkan rute ke jaringan di tabel rute VPN titik akhir Klien dan mengonfigurasi aturan otorisasi untuk memberikan akses kepada klien.

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

Untuk menyediakan akses ke internet

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik VPNAkhir Klien.
3. Pilih VPN endpoint Klien 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 VPN endpoint Klien di Langkah 2. Itu berarti bahwa grup keamanan default untuk secara otomatis VPC diterapkan ke VPN titik akhir Klien ketika jaringan target dikaitkan. Akibatnya, grup keamanan default untuk sekarang VPC harus dikaitkan dengan VPN titik akhir Klien.

Verifikasi persyaratan grup keamanan berikut

- Bahwa grup keamanan yang terkait dengan subnet yang Anda rutekan lalu lintas (dalam hal ini grup VPC keamanan 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 dalam Anda VPC memiliki aturan yang mengizinkan akses dari grup keamanan yang diterapkan ke VPN titik akhir Klien (dalam hal ini grup VPC keamanan default). Ini memungkinkan klien Anda untuk mengakses sumber daya di AndaVPC.

Untuk informasi selengkapnya, lihat Grup keamanan.

Langkah 7: Unduh file konfigurasi VPN titik akhir Klien

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

Untuk mengunduh dan menyiapkan file konfigurasi VPN titik akhir Klien

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik VPNAkhir Klien.
3. Pilih VPN endpoint Klien 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 Open VPN easy-rsa kloning:
   - 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 VPN titik akhir Klien menggunakan editor teks 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 VPN titik akhir Klien.
7. Mendistribusikan file konfigurasi VPN titik akhir Klien ke pengguna akhir Anda.

Untuk informasi selengkapnya tentang file konfigurasi VPN titik akhir Klien, lihatAWS Client VPN ekspor file konfigurasi titik akhir.

Langkah 8: Connect ke VPN endpoint Klien

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

Bekerja dengan AWS Client VPN

Topik berikut menjelaskan tugas administratif utama yang diperlukan untuk bekerja dengan KlienVPN:

- Akses portal swalayan — Konfigurasikan akses ke portal VPN layanan mandiri Klien sehingga klien dapat mengunduh file konfigurasi VPN titik akhir Klien sendiri. Untuk informasi tentang mengakses portal swalayan, lihat. the section called “Akses portal swalayan”
- Aturan otorisasi - Tambahkan aturan otorisasi untuk mengontrol akses klien ke jaringan tertentu. Untuk informasi tentang menambahkan aturan otorisasi, lihatthe section called “Aturan otorisasi”.
- Daftar pencabutan sertifikat klien — Gunakan daftar pencabutan sertifikat klien untuk mencabut akses ke titik akhir Klien. VPN Untuk informasi tentang daftar pencabutan sertifikat klien, lihat. the section called “Daftar pencabutan sertifikat klien”
- Koneksi klien — Melihat atau mengakhiri koneksi klien ke titik VPN akhir Klien. Untuk informasi tentang melihat atau mengakhiri koneksi klien, lihatthe section called “Koneksi klien”.
- Spanduk login klien - Tambahkan spanduk teks pada aplikasi VPN desktop Klien saat VPN sesi dibuat. Anda dapat menggunakan spanduk teks untuk memenuhi kebutuhan peraturan dan kepatuhan Anda. Untuk informasi tentang spanduk login, lihatthe section called “Spanduk login klien”.
- VPNTitik akhir klien - Konfigurasikan VPN titik akhir Klien untuk mengelola dan mengontrol semua VPN sesi. Untuk informasi tentang mengonfigurasi titik akhir, lihat. the section called “Titik akhir”
- Log koneksi - Aktifkan pencatatan koneksi untuk VPN titik akhir Klien baru atau yang sudah ada untuk mulai menangkap log koneksi. Untuk informasi tentang pencatatan koneksi, lihatthe section called “Log koneksi”.
- Ekspor file konfigurasi klien - Konfigurasikan file konfigurasi klien yang dibutuhkan VPN klien Klien untuk membuat VPN koneksi. Setelah mengkonfigurasi file, unduh (ekspor) untuk didistribusikan ke klien. Untuk informasi selengkapnya tentang mengekspor file konfigurasi klien, lihatthe section called “Ekspor file konfigurasi klien”.
- Rute — Konfigurasikan aturan otorisasi untuk setiap VPN rute Klien untuk menentukan klien mana yang memiliki akses ke jaringan tujuan. Untuk informasi tentang mengonfigurasi aturan otorisasi, lihat the section called “Aturan otorisasi”
- Jaringan target — Mengaitkan jaringan target dengan VPN titik akhir Klien untuk memungkinkan klien terhubung dengannya dan membuat VPN koneksi. Untuk informasi tentang jaringan target, lihatthe section called “Jaringan target”.

- Durasi VPN sesi maksimum - Tetapkan opsi untuk durasi VPN sesi maksimum untuk memenuhi persyaratan keamanan dan kepatuhan Anda. Untuk informasi tentang durasi VPN sesi maksimum, lihatthe section called “Durasi VPN sesi maksimum”.

AWS Client VPN akses ke portal swalayan

Jika Anda mengaktifkan portal swalayan untuk VPN titik akhir Klien Anda, Anda dapat menyediakan portal swalayan kepada klien Anda. URL Klien dapat mengakses portal di peramban web, dan menggunakan kredensial berbasis pengguna untuk log in. Di portal, klien dapat mengunduh file konfigurasi VPN titik akhir Klien dan mereka dapat mengunduh versi terbaru dari klien yang AWS disediakan.

Aturan-aturan berikut berlaku:

- Portal layanan mandiri ini tidak tersedia untuk klien yang mengautentikasi menggunakan autentikasi bersama.
- File konfigurasi yang tersedia di portal swalayan adalah file konfigurasi yang sama dengan yang Anda ekspor menggunakan VPC konsol Amazon 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 swalayan untuk VPN titik akhir Klien Anda, atau klien tidak dapat mengakses portal. Jika opsi ini tidak diaktifkan, Anda dapat mengubah VPN titik akhir Klien Anda untuk mengaktifkannya.

Setelah Anda mengaktifkan opsi portal swalayan, berikan klien Anda salah satu dari yang berikut: URLs

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

  Jika klien mengakses portal menggunakan iniURL, mereka harus memasukkan ID VPN titik akhir Klien sebelum mereka dapat masuk.

- `https://self-service.clientvpn.amazonaws.com/endpoints/<endpoint-id>`

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

Anda juga dapat melihat portal swalayan di output describe-client-vpn-endpoints AWS CLI perintah. URL Atau, URL tersedia di tab Detail pada halaman VPNEndpoints Klien di VPC konsol Amazon.

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

AWS Client VPN 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 VPN titik akhir Klien menggunakan konsol dan. AWS CLI

> **Note**
>
> Klien VPN menggunakan pencocokan awalan terpanjang saat mengevaluasi aturan otorisasi. Lihat topik pemecahan masalah Pemecahan masalah AWS Client VPN: Aturan otorisasi untuk grup Active Directory tidak berfungsi seperti yang diharapkan dan prioritas Rute di Panduan VPC Pengguna Amazon untuk detail selengkapnya.

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 defaultnya adalah menolak akses.
- Anda tidak dapat menambahkan aturan otorisasi untuk membatasi akses ke jaringan tujuan.
- `0.0.0.0/0`CIDRIni ditangani sebagai kasus khusus. Ini diproses terakhir, terlepas dari urutan aturan otorisasi dibuat.
- Ini `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.

Topik

- Contoh skenario untuk aturan VPN otorisasi Klien

- Tambahkan aturan otorisasi ke titik akhir AWS Client VPN
- Hapus aturan otorisasi dari titik akhir AWS Client VPN
- Lihat AWS Client VPN aturan otorisasi

Contoh skenario untuk aturan VPN otorisasi Klien

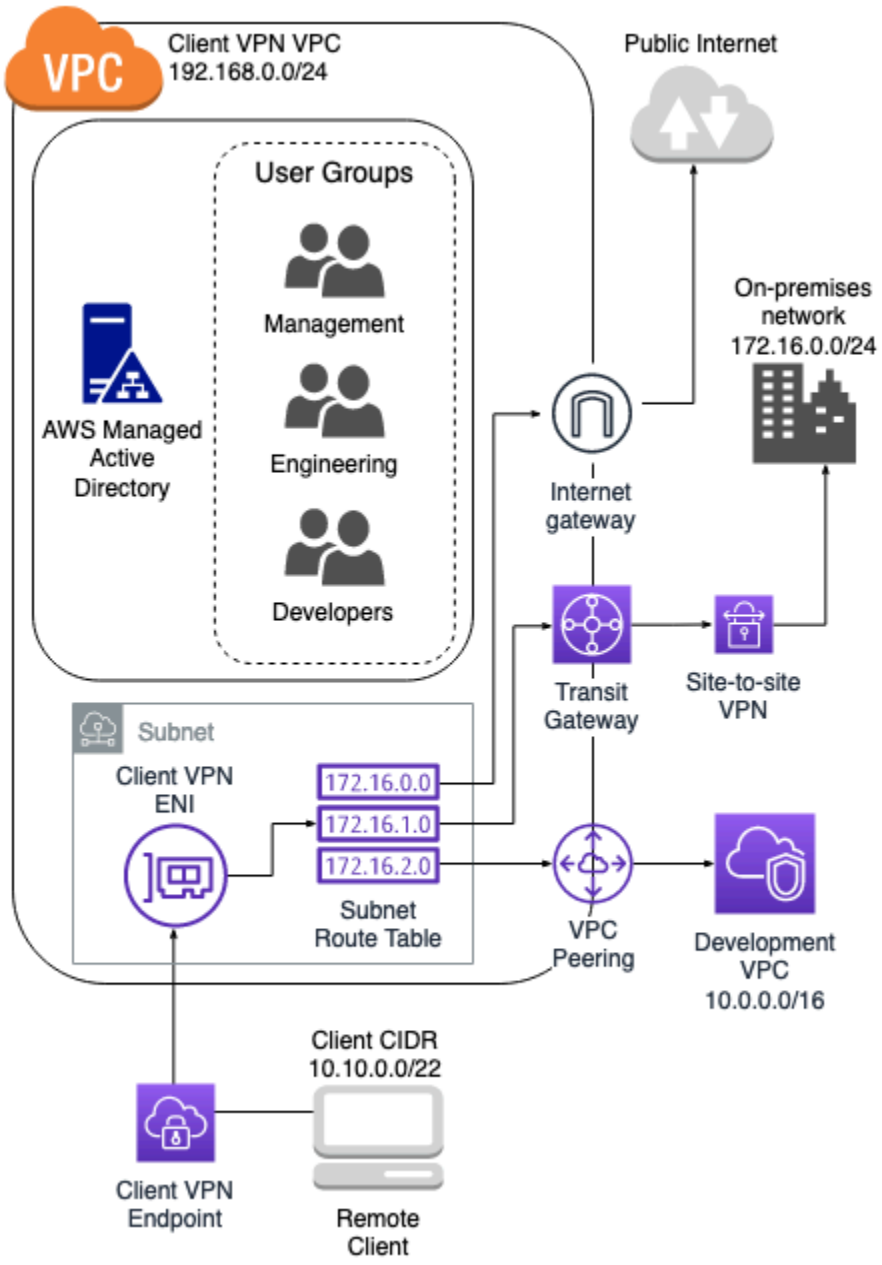
Bagian ini menjelaskan cara kerja aturan otorisasi. AWS Client VPN Ini mencakup poin-poin penting untuk memahami aturan otorisasi, arsitektur contoh, dan diskusi skenario contoh yang memetakan ke arsitektur contoh.

Skenario

- the section called “Contoh arsitektur”
- the section called “Akses ke satu tujuan”
- the section called “Gunakan tujuan apa pun (0.0.0.0/0) CIDR”
- the section called “Pencocokan awalan IP yang lebih panjang”
- the section called “Tumpang tindih CIDR (kelompok yang sama)”
- the section called “Aturan 0.0.0.0/0 tambahan”
- the section called “Tambahkan aturan untuk 192.168.0.0/24”
- the section called “Akses untuk semua grup pengguna”

Contoh arsitektur untuk skenario aturan otorisasi

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



Akses ke satu tujuan

Deskripsi aturan	ID Grup	Izinkan akses ke semua pengguna	Destinasi CIDR
Menyediakan akses grup teknik ke jaringan lokal	S-XXXXX14	False	172.16.0.0/24

Deskripsi aturan	ID Grup	Izinkan akses ke semua pengguna	Destinasi CIDR
Memberikan akses kelompok pengembangan ke pengembangan VPC	S-xxxxx15	False	10.0.0.0/16
Memberikan akses grup manajer ke Klien VPN VPC	S-XXXXX16	False	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 VPN titik akhir Klien.

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

Gunakan tujuan apa pun (0.0.0.0/0) CIDR

Deskripsi aturan	ID Grup	Izinkan akses ke semua pengguna	Destinasi CIDR
Menyediakan akses grup teknik ke jaringan lokal	S-XXXXX14	False	172.16.0.0/24

Deskripsi aturan	ID Grup	Izinkan akses ke semua pengguna	Destinasi CIDR
Memberikan akses kelompok pengembangan ke pengembangan VPC	S-xxxxx15	False	10.0.0.0/16
Menyediakan akses grup manajer ke tujuan apa pun	S-XXXXX16	False	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.

Pencocokan awalan IP yang lebih panjang

Deskripsi aturan	ID Grup	Izinkan akses ke semua pengguna	Destinasi CIDR

Deskripsi aturan	ID Grup	Izinkan akses ke semua pengguna	Destinasi CIDR
Menyediakan akses grup teknik ke jaringan lokal	S-XXXXX14	False	172.16.0.0/24
Memberikan akses kelompok pengembangan ke pengembangan VPC	S-xxxxx15	False	10.0.0.0/16
Menyediakan akses grup manajer ke tujuan apa pun	S-XXXXX16	False	0.0.0.0/0
Menyediakan akses grup manajer ke satu host dalam pengembangan VPC	S-XXXXX16	False	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 pengembanganVPC, tetapi tidak memiliki akses ke `172.16.0.0/24` atau salah satu host yang tersisa dalam pengembanganVPC.

> **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.

Tumpang tindih CIDR (kelompok yang sama)

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

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.

Aturan 0.0.0.0/0 tambahan

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

Deskripsi aturan	ID Grup	Izinkan akses ke semua pengguna	Destinasi CIDR
Menyediakan akses grup teknik ke subnet yang lebih kecil dalam jaringan lokal			
Menyediakan akses grup teknik ke tujuan apa pun	S-XXXXX14	False	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 `192.168.0.0/24172.16.0.0/24`, 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`.

Tambahkan aturan untuk 192.168.0.0/24

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

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

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.

Akses untuk semua grup pengguna

Deskripsi aturan	ID Grup	Izinkan akses ke semua pengguna	Destinasi CIDR
Menyediakan akses grup teknik ke jaringan lokal	S-XXXXX14	False	172.16.0.0/24
Memberikan akses kelompok pengembangan ke pengembangan VPC	S-xxxxx15	False	10.0.0.0/16
Menyediakan akses grup manajer ke tujuan apa pun	S-XXXXX16	False	0.0.0.0/0
	S-XXXXX16	False	10.0.2.119/32

Deskripsi aturan	ID Grup	Izinkan akses ke semua pengguna	Destinasi CIDR
Berikan akses grup manajer ke host tunggal dalam pengembangan VPC			
Menyediakan akses grup teknik ke subnet di jaringan lokal	S-XXXXX14	False	172.16.0.128/25
Menyediakan akses grup teknik ke semua jaringan	S-XXXXX14	False	0.0.0.0/0
Memberikan akses grup manajer ke Klien VPN VPC	S-XXXXX16	False	192.168.0.0/24
Menyediakan akses ke semua grup	N/A	True	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.

Tambahkan aturan otorisasi ke titik akhir AWS Client VPN

Anda dapat menambahkan aturan otorisasi ke VPN titik akhir Klien dengan menggunakan. AWS Management Console

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

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik VPNAkhir Klien.
3. Pilih VPN titik akhir Klien untuk menambahkan aturan otorisasi, pilih Aturan otorisasi, dan pilih Tambahkan aturan otorisasi.
4. Untuk jaringan Tujuan untuk mengaktifkan akses, masukkan alamat IP, dalam CIDR notasi, dari jaringan yang Anda ingin pengguna akses (misalnya, CIDR blok AndaVPC).
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. Misalnya, pengenal keamanan (SID) dari grup Active Directory, atau ID/nama grup yang ditentukan dalam penyedia identitas SAML berbasis (IDP).
     - (Active Directory) Untuk mendapatkanSID, 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.
     - (otentikasi federasi SAML berbasis) ID grup/nama harus cocok dengan informasi atribut grup yang dikembalikan dalam pernyataan. SAML
6. Untuk Deskripsi, masukkan deskripsi singkat tentang aturan otorisasi.
7. Pilih Tambahkan aturan otorisasi.

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

Gunakan perintah authorize-client-vpn-ingress.

Hapus aturan otorisasi dari titik akhir AWS Client VPN

Anda dapat menghapus aturan otorisasi untuk VPN titik akhir Klien tertentu menggunakan konsol dan. AWS CLI

Untuk menghapus aturan otorisasi (konsol)

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik VPNAkhir Klien.
3. Pilih VPN titik akhir Klien yang ditambahkan aturan otorisasi, lalu pilih Aturan otorisasi.
4. Pilih aturan otorisasi yang akan dihapus, pilih Hapus aturan otorisasi, lalu pilih Hapus aturan otorisasi lagi untuk mengonfirmasi penghapusan.

Untuk menghapus aturan otorisasi ()AWS CLI

Gunakan perintah revoke-client-vpn-ingress.

Lihat AWS Client VPN aturan otorisasi

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

Untuk melihat aturan otorisasi (konsol)

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

Untuk melihat aturan otorisasi (AWS CLI)

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

AWS Client VPN daftar pencabutan sertifikat klien

Daftar pencabutan sertifikat VPN klien klien digunakan untuk mencabut akses ke VPN titik akhir Klien untuk sertifikat klien tertentu. Anda dapat membuat daftar pencabutan serta impor atau daftar yang ada atau mengekspor daftar Anda saat ini file daftar pencabutan. Membuat daftar dilakukan menggunakan VPN perangkat lunak Buka di Linxu/macOS atau di Windows. Mengimpor dan mengekspor dapat dilakukan dengan menggunakan VPC Konsol Amazon atau dengan menggunakan. AWS CLI

> **Note**
>
> Untuk informasi selengkapnya tentang membuat sertifikat server dan klien dan kunci, lihat Otentikasi timbal balik di AWS Client VPN

Anda hanya dapat menambahkan sejumlah entri terbatas ke daftar pencabutan sertifikat klien. Untuk informasi selengkapnya tentang jumlah entri yang dapat Anda tambahkan ke daftar pencabutan, lihat. VPNKuota klien

Tugas

- Buat daftar pencabutan sertifikat AWS Client VPN klien
- Impor AWS Client VPN daftar pencabutan sertifikat klien
- Ekspor daftar pencabutan sertifikat AWS Client VPN klien

Buat daftar pencabutan sertifikat AWS Client VPN klien

Linux/macOS

Dalam prosedur berikut, Anda menghasilkan daftar pencabutan sertifikat klien menggunakan utilitas baris perintah Open VPN easy-rsa.

Untuk menghasilkan daftar pencabutan sertifikat klien menggunakan Open easy-rsa VPN

1. Masuk 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
```

Masuk `yes` saat diminta.

Windows

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

Untuk menghasilkan daftar pencabutan sertifikat klien menggunakan Easy RSA versi 3.xx

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

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

2. Jalankan `EasyRSA-Start.bat` file untuk memulai Easy RSA shell.

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

3. Di RSA shell Mudah, cabut sertifikat klien.

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

4. Masuk `yes` 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 Easy sebelumnya RSA

1. Buka prompt perintah dan arahkan ke VPN direktori Open.

```
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 AWS Client VPN daftar pencabutan sertifikat klien

Anda harus memiliki file daftar pencabutan sertifikat VPN klien Klien untuk diimpor. Untuk informasi selengkapnya tentang membuat daftar pencabutan sertifikat klien, lihat Buat daftar pencabutan sertifikat AWS Client VPN klien.

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

Untuk mengimpor daftar pencabutan sertifikat klien (konsol)

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik VPNAkhir Klien.
3. Pilih VPN titik akhir Klien 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 AWS Client VPN klien

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

Untuk mengekspor daftar pencabutan sertifikat klien (konsol)

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

Untuk mengekspor daftar pencabutan sertifikat klien (AWS CLI)

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

AWS Client VPN koneksi klien

AWS Client VPN koneksi adalah VPN sesi aktif yang telah ditetapkan oleh klien ke VPN titik akhir Klien tertentu serta koneksi yang telah dihentikan dalam 60 menit terakhir untuk titik akhir tersebut. Koneksi dibuat ketika klien berhasil terhubung ke VPN titik akhir Klien. Mengakhiri sesi mengakhiri koneksi klien ke titik VPN akhir Klien.

Anda dapat melihat dan mengakhiri VPN koneksi Klien. Melihat informasi koneksi mengembalikan informasi seperti alamat IP yang ditetapkan dari rentang CIDR blok klien, ID titik akhir, dan stempel waktu. Mengakhiri sesi mengakhiri VPN koneksi yang ditentukan ke titik akhir. Melihat dan mengakhiri sesi dapat dilakukan dengan menggunakan VPC Konsol Amazon atau. AWS CLI Jika Anda tidak dapat terhubung ke titik akhir, dan bergantung pada kesalahannya, lihat Pemecahan Masalah langkah-langkah yang harus diambil untuk mengatasi masalah tersebut.

Tugas

- Lihat koneksi AWS Client VPN klien
- Mengakhiri koneksi AWS Client VPN klien

Lihat koneksi AWS Client VPN klien

Anda dapat melihat VPN koneksi Klien aktif menggunakan VPC Konsol Amazon atau AWS CLI.

Untuk melihat koneksi VPN klien klien (konsol)

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik VPNAkhir Klien.
3. Pilih VPN titik akhir Klien untuk melihat koneksi klien.
4. Pilih tab Konektivitas. Tab Konektivitas mencantumkan semua koneksi klien yang aktif dan yang diakhiri.

Untuk melihat koneksi klien VPN Klien (AWS CLI)

Gunakan perintah describe-client-vpn-connections.

Mengakhiri koneksi AWS Client VPN klien

Anda dapat mengakhiri koneksi klien VPN Klien menggunakan VPC Konsol Amazon atau. AWS CLI

Untuk mengakhiri koneksi klien VPN Klien (konsol)

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik VPNAkhir Klien.
3. Pilih VPN titik akhir Klien yang terhubung dengan klien, dan pilih Koneksi.
4. Pilih koneksi yang akan dihentikan, pilih Hentikan Koneksi, lalu pilih Hentikan Koneksi lagi untuk mengonfirmasi penghentian.

Untuk mengakhiri koneksi klien VPN Klien ()AWS CLI

Gunakan perintah terminate-client-vpn-connections.

AWS Client VPN spanduk login klien

AWS Client VPN menyediakan opsi untuk menampilkan spanduk teks pada aplikasi VPN desktop Klien yang AWS disediakan saat VPN sesi dibuat. Anda dapat menentukan isi spanduk teks untuk

memenuhi kebutuhan peraturan dan kepatuhan Anda. Maksimal 1400 UTF -8 karakter yang dikodekan dapat digunakan.

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

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

Pembuatan spanduk

Spanduk login awalnya dibuat dan diaktifkan selama pembuatan VPN endpoint Klien. Untuk langkah-langkah untuk mengaktifkan banner login klien selama pembuatan VPN titik akhir Klien, lihatBuat titik AWS Client VPN akhir.

Tugas

- Konfigurasikan banner login klien untuk titik AWS Client VPN akhir yang ada
- Nonaktifkan banner login klien untuk titik akhir yang ada AWS Client VPN
- Ubah teks spanduk yang ada pada titik AWS Client VPN akhir
- Lihat spanduk AWS Client VPN login yang saat ini dikonfigurasi

Konfigurasikan banner login klien untuk titik AWS Client VPN akhir yang ada

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

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

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik VPNAkhir Klien.
3. Pilih VPN titik akhir Klien yang ingin Anda ubah, pilih Tindakan, lalu pilih Ubah Titik VPN Akhir Klien.

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 VPN sesi dibuat. Gunakan UTF -8 karakter yang dikodekan saja, dengan maksimum 1400 karakter diizinkan.
7. Pilih Ubah VPN titik akhir Klien.

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

Gunakan perintah modify-client-vpn-endpoint.

Nonaktifkan banner login klien untuk titik akhir yang ada AWS Client VPN

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

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

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

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

Gunakan perintah modify-client-vpn-endpoint.

Ubah teks spanduk yang ada pada titik AWS Client VPN akhir

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

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

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.

2. Di panel navigasi, pilih Titik VPNAkhir Klien.
3. Pilih VPN titik akhir Klien yang ingin Anda ubah, pilih Tindakan, lalu pilih Ubah titik VPN akhir Klien.
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 VPN sesi dibuat. Gunakan UTF -8 karakter yang dikodekan saja, dengan maksimal 1400 karakter.
6. Pilih Ubah VPN titik akhir Klien.

Ubah banner login klien pada VPN titik akhir Klien ()AWS CLI

Gunakan perintah modify-client-vpn-endpoint.

Lihat spanduk AWS Client VPN login yang saat ini dikonfigurasi

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

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

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik VPNAkhir Klien.
3. Pilih VPN titik akhir Klien 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 VPN titik akhir Klien ()AWS CLI

Gunakan perintah describe-client-vpn-endpoints.

AWS Client VPN titik akhir

Semua AWS Client VPN sesi menjalin komunikasi dengan VPN titik akhir Klien. Anda dapat mengelola VPN endpoint Klien untuk membuat, memodifikasi, melihat, dan menghapus VPN sesi klien dengan titik akhir tersebut. Titik akhir dapat dibuat dan dimodifikasi menggunakan VPC Konsol Amazon atau dengan menggunakan. AWS CLI

Persyaratan untuk membuat titik VPN akhir Klien

> **Important**
>
> VPNTitik akhir Klien harus dibuat di AWS akun yang sama di mana jaringan target yang dimaksud disediakan. Anda juga harus membuat sertifikat server, dan jika diperlukan, sertifikat klien. Untuk informasi selengkapnya, lihat Otentikasi klien di AWS Client VPN.

Sebelum memulai, pastikan Anda melakukan hal berikut:

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

Modifikasi titik akhir

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

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

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

Saat Anda memodifikasi salah satu parameter berikut pada VPN titik akhir Klien, koneksi akan diatur ulang:

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

Tugas

- Buat titik AWS Client VPN akhir
- Lihat titik AWS Client VPN akhir
- Memodifikasi AWS Client VPN titik akhir
- Hapus titik AWS Client VPN akhir

Buat titik AWS Client VPN akhir

Buat VPN titik akhir Klien untuk memungkinkan klien Anda membuat VPN sesi menggunakan VPC Konsol Amazon atau. AWS CLI

Sebelum membuat titik akhir, biasakan diri Anda dengan persyaratan. Untuk informasi selengkapnya tentang persyaratan titik akhir, lihatthe section called “Persyaratan untuk membuat titik VPN akhir Klien”.

Untuk membuat VPN endpoint Klien (konsol)

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

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

5. Untuk sertifikat Server ARN, tentukan ARN TLS sertifikat yang akan digunakan oleh server. Klien menggunakan sertifikat server untuk mengautentikasi VPN titik akhir Klien yang mereka sambungkan.

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

6. Tentukan metode otentikasi yang akan digunakan untuk mengautentikasi klien ketika mereka membuat VPN koneksi. 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.
     - Otentikasi federasi: Pilih opsi ini untuk otentikasi federasi SAML berbasis.

       Untuk SAMLpenyedia ARN, tentukan ARN penyedia IAM SAML identitas.

(Opsional) Untuk SAMLpenyedia layanan mandiri ARN, tentukan penyedia IAM SAML identitas yang Anda buat untuk mendukung portal swalayan, jika berlaku. ARN

- Untuk menggunakan otentikasi sertifikat timbal balik, pilih Gunakan autentikasi bersamaARN, lalu untuk sertifikat Klien, tentukan sertifikat klien yang disediakan di (). ARN 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 Klien. VPN Untuk Client Connect Handler ARN, tentukan Amazon Resource Name (ARN) dari fungsi Lambda yang berisi logika yang memungkinkan atau menolak koneksi.
9. (Opsional) Tentukan DNS server mana yang akan digunakan untuk DNS resolusi. Untuk menggunakan DNS server khusus, untuk alamat IP DNS DNS Server 1 dan alamat IP Server 2, tentukan alamat IP DNS server yang akan digunakan. Untuk menggunakan VPC DNS server, baik untuk alamat IP DNS DNS Server 1 atau alamat IP Server 2, tentukan alamat IP, dan tambahkan alamat IP VPC DNS server.

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

10. (Opsional) Secara default, VPN titik akhir Klien menggunakan protokol UDP transport. Untuk menggunakan protokol TCP transport sebagai gantinya, untuk Transport Protocol, pilih TCP.

> **Note**
>
> UDPbiasanya menawarkan kinerja yang lebih baik daripadaTCP. Anda tidak dapat mengubah protokol transport setelah Anda membuat VPN endpoint Klien.

11. (Opsional) Agar titik akhir menjadi VPN titik akhir Klien split-tunnel, aktifkan Aktifkan split-tunnel. Secara default, split-tunnel pada VPN titik akhir Klien dinonaktifkan.
12. (Opsional) Untuk VPCID, pilih VPC untuk dikaitkan dengan VPN titik akhir Klien. Untuk Grup Keamanan IDs, pilih satu atau beberapa grup keamanan untuk diterapkan ke VPN titik akhir Klien. VPC
13. (Opsional) Untuk VPNport, pilih nomor VPN port. Default-nya adalah 443.
14. (Opsional) Untuk menghasilkan portal swalayan URL untuk klien, aktifkan Aktifkan portal swalayan.
15. (Opsional) Untuk jam tunggu Sesi, pilih waktu durasi VPN sesi 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 AWS disediakan saat VPN sesi dibuat. UTF-8 karakter yang dikodekan saja. Maksimal 1400 karakter.
17. Pilih Create Client VPN endpoint.

Setelah Anda membuat VPN endpoint Klien, lakukan hal berikut untuk menyelesaikan konfigurasi dan memungkinkan klien untuk terhubung:

- Keadaan awal dari VPN titik akhir Klien adalah`pending-associate`. Klien hanya dapat terhubung ke VPN titik akhir Klien setelah Anda mengaitkan jaringan target pertama.
- Buat aturan otorisasi untuk menentukan klien mana yang memiliki akses ke jaringan.
- Unduh dan siapkan file konfigurasi VPN titik akhir Klien untuk didistribusikan ke klien Anda.
- Instruksikan klien Anda untuk menggunakan klien yang AWS disediakan atau aplikasi klien VPN berbasis Terbuka lainnya untuk terhubung ke titik VPN akhir Klien. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS Client VPN.

Untuk membuat VPN endpoint Klien ()AWS CLI

Gunakan perintah create-client-vpn-endpoint.

Lihat titik AWS Client VPN akhir

Anda dapat melihat informasi tentang VPN titik akhir Klien menggunakan VPC Konsol Amazon atau. AWS CLI

Untuk melihat VPN titik akhir Klien (konsol)

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

   Anda juga dapat menggunakan filter untuk membantu menyempurnakan pencarian Anda.

Untuk melihat VPN titik akhir Klien ()AWS CLI

Gunakan perintah describe-client-vpn-endpoints.

Memodifikasi AWS Client VPN titik akhir

Anda dapat mengubah VPN titik akhir Klien menggunakan VPC Konsol Amazon atau. AWS CLI Untuk informasi selengkapnya tentang bidang yang dapat Anda gunakan VPN Bidang klien yang dapat Anda ubah, lihatthe section called “Modifikasi titik akhir”.

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

Untuk memodifikasi VPN titik akhir Klien (konsol)

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.

2. Di panel navigasi, pilih Titik VPNAkhir Klien.
3. Pilih VPN titik akhir Klien untuk dimodifikasi, pilih Tindakan, dan kemudian pilih Ubah titik VPN akhir Klien.
4. Untuk Deskripsi, masukkan deskripsi singkat untuk VPN titik akhir Klien.
5. Untuk sertifikat Server ARN, tentukan ARN TLS sertifikat yang akan digunakan oleh server. Klien menggunakan sertifikat server untuk mengautentikasi VPN titik akhir Klien yang mereka sambungkan.

   > **Note**
   >
   > Sertifikat server harus ada di AWS Certificate Manager (ACM) di wilayah tempat Anda membuat VPN titik akhir Klien. 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 Client Connect Handler ARN, tentukan Amazon Resource Name (ARN) dari fungsi Lambda yang berisi logika yang memungkinkan atau menolak koneksi.
8. Hidupkan atau matikan Aktifkan DNS server. Untuk menggunakan DNS server khusus, untuk alamat IP DNS DNS Server 1 dan alamat IP Server 2, tentukan alamat IP DNS server yang akan digunakan. Untuk menggunakan VPC DNS server, baik untuk alamat IP DNS DNS Server 1 atau alamat IP Server 2, tentukan alamat IP, dan tambahkan alamat IP VPC DNS server.

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

9. Hidupkan atau matikan Aktifkan split-tunnel. Secara default, split-tunnel pada VPN titik akhir tidak aktif.

10. Untuk VPCID, pilih yang akan VPC dikaitkan dengan VPN titik akhir Klien. Untuk Grup Keamanan IDs, pilih satu atau beberapa grup keamanan untuk diterapkan ke VPN titik akhir Klien. VPC
11. Untuk VPNport, pilih nomor VPN port. Default-nya adalah 443.
12. Untuk menghasilkan portal swalayan URL untuk klien, aktifkan Aktifkan portal swalayan.
13. Untuk jam tunggu sesi, pilih waktu durasi VPN sesi 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 AWS disediakan saat VPN sesi dibuat. UTF-8 karakter yang dikodekan saja. Maksimal 1400 karakter.
15. Pilih Ubah VPN titik akhir Klien.

Untuk memodifikasi VPN titik akhir Klien ()AWS CLI

Gunakan perintah modify-client-vpn-endpoint.

Hapus titik AWS Client VPN akhir

Anda harus memisahkan semua jaringan target sebelum Anda dapat menghapus titik VPN akhir Klien. Saat Anda menghapus VPN titik akhir Klien, statusnya diubah `deleting` dan klien tidak dapat lagi terhubung dengannya.

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

Untuk menghapus VPN titik akhir Klien (konsol)

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

Untuk menghapus VPN titik akhir Klien ()AWS CLI

Gunakan perintah delete-client-vpn-endpoint.

AWS Client VPN log koneksi

Anda dapat mengaktifkan pencatatan koneksi untuk VPN titik akhir Klien baru atau yang sudah ada, dan mulai menangkap log koneksi. Log koneksi menunjukkan urutan peristiwa log untuk VPN titik akhir Klien. Bila Anda mengaktifkan logging koneksi, Anda dapat menentukan nama pengaliran log dalam grup log. Jika Anda tidak menentukan aliran log, VPN layanan Klien membuatnya untuk Anda. Pencatatan koneksi kemudian mencatat informasi berikut: permintaan koneksi klien, hasil koneksi klien (berhasil atau tidak berhasil), alasan hasil koneksi yang tidak berhasil, dan waktu penghentian klien dari titik akhir.

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.

Log VPN koneksi klien dapat dibuat menggunakan VPC Konsol Amazon atau file AWS CLI.

Tugas

- Aktifkan pencatatan koneksi untuk titik AWS Client VPN akhir baru
- Aktifkan pencatatan koneksi untuk titik AWS Client VPN akhir yang ada
- Lihat log AWS Client VPN koneksi
- Matikan pencatatan AWS Client VPN koneksi

Aktifkan pencatatan koneksi untuk titik AWS Client VPN akhir baru

Anda dapat mengaktifkan pencatatan koneksi saat membuat VPN titik akhir Klien baru dengan menggunakan konsol atau baris perintah.

Untuk mengaktifkan pencatatan koneksi untuk VPN titik akhir Klien baru menggunakan konsol

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih VPNTitik Akhir Klien, lalu pilih Create Client VPN endpoint.
3. Lengkapi opsi sampai Anda mencapai bagian Logging koneksi. Untuk informasi lebih lanjut tentang opsi, lihat Buat titik AWS Client VPN akhir.
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 Buat VPN titik akhir Klien.

Untuk mengaktifkan pencatatan koneksi untuk VPN titik akhir Klien baru menggunakan AWS CLI

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

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

Aktifkan pencatatan koneksi untuk titik AWS Client VPN akhir yang ada

Anda dapat mengaktifkan pencatatan koneksi untuk VPN titik akhir Klien yang ada dengan menggunakan konsol atau baris perintah.

Untuk mengaktifkan pencatatan koneksi untuk VPN titik akhir Klien yang ada menggunakan konsol

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik VPNAkhir Klien.
3. Pilih VPN titik akhir Klien, pilih Tindakan, lalu pilih Ubah titik VPN akhir Klien.
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 VPN titik akhir Klien.

Untuk mengaktifkan pencatatan koneksi untuk VPN titik akhir Klien yang ada menggunakan AWS CLI

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

```
{
```

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

Lihat log AWS Client VPN koneksi

Anda dapat melihat log VPN koneksi Klien 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 aliran log untuk VPN titik akhir Klien 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 AWS Client VPN koneksi

Anda dapat menonaktifkan pencatatan koneksi untuk VPN titik akhir Klien 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 VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik VPNAkhir Klien.
3. Pilih VPN titik akhir Klien, pilih Tindakan, lalu pilih Ubah titik VPN akhir Klien.
4. Di bawah Pencatatan koneksi, matikan Aktifkan detail log pada koneksi klien.
5. Pilih Ubah VPN titik akhir Klien.

Untuk mematikan log koneksi menggunakan AWS CLI

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

AWS Client VPN ekspor file konfigurasi titik akhir

File konfigurasi AWS Client VPN endpoint adalah file yang digunakan klien (pengguna) untuk membuat VPN koneksi dengan titik VPN akhir Klien. Anda harus mengunduh (mengekspor) file ini dan mendistribusikannya ke semua klien yang membutuhkan akses ke fileVPN. Atau, jika Anda mengaktifkan portal swalayan untuk VPN titik akhir Klien Anda, klien dapat masuk ke portal dan mengunduh file konfigurasi sendiri. Untuk informasi selengkapnya, lihat AWS Client VPN akses ke portal swalayan.

Jika VPN titik akhir Klien Anda menggunakan otentikasi timbal balik, Anda harus menambahkan sertifikat klien dan kunci pribadi klien ke file konfigurasi.ovpn yang Anda unduh. Setelah Anda menambahkan informasi, klien dapat mengimpor file.ovpn ke dalam perangkat lunak VPN klien Terbuka.

> **Important**
>
> Jika Anda tidak menambahkan sertifikat klien dan informasi kunci pribadi klien ke file, klien yang mengautentikasi menggunakan otentikasi timbal balik tidak dapat terhubung ke titik akhir KlienVPN.

Secara default, opsi “remote-random-hostname” dalam konfigurasi VPN klien Buka mengaktifkan wildcardDNS. Karena wildcard DNS diaktifkan, klien tidak menyimpan alamat IP titik akhir dan Anda tidak akan dapat melakukan ping DNS nama titik akhir.

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

Tugas

- Ekspor file konfigurasi AWS Client VPN klien
- Tambahkan sertifikat AWS Client VPN klien dan informasi kunci untuk otentikasi timbal balik

Ekspor file konfigurasi AWS Client VPN klien

Anda dapat mengekspor konfigurasi VPN klien Klien dengan menggunakan konsol atau AWS CLI.

Untuk mengekspor konfigurasi klien (konsol)

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik VPNAkhir Klien.
3. Pilih VPN titik akhir Klien 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
```

Tambahkan sertifikat AWS Client VPN klien dan informasi kunci untuk otentikasi timbal balik

Jika VPN titik akhir Klien Anda menggunakan otentikasi timbal balik, Anda harus menambahkan sertifikat klien dan kunci pribadi klien ke file konfigurasi.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) Mendistribusikan sertifikat klien dan kunci ke klien bersama dengan file konfigurasi VPN titik akhir Klien. 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 dan kunci klien (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 dan kunci klien terpisah untuk setiap pengguna yang akan terhubung ke VPN titik akhir Klien, ulangi langkah ini untuk setiap pengguna.

Berikut ini adalah contoh format file VPN konfigurasi Klien yang mencakup sertifikat klien dan 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
```

AWS Client VPN rute

Setiap AWS Client VPN titik akhir 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 VPN titik akhir Klien untuk menentukan klien mana yang memiliki akses ke jaringan tujuan.

Saat Anda mengaitkan subnet dari VPN titik akhir Klien VPC dengan Klien, rute untuk secara otomatis VPC ditambahkan ke tabel rute VPN titik akhir Klien. Untuk mengaktifkan akses untuk jaringan tambahan, seperti peeredVPCs, jaringan lokal, jaringan lokal (untuk memungkinkan klien berkomunikasi satu sama lain), atau internet, Anda harus menambahkan rute secara manual ke tabel rute VPN titik akhir Klien.

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

Pertimbangan untuk menggunakan split-tunnel pada titik akhir Klien VPN

Saat Anda menggunakan split-tunnel pada VPN titik akhir Klien, semua rute yang ada di tabel VPN rute Klien ditambahkan ke tabel rute klien saat dibuat. VPN Jika Anda menambahkan rute setelah VPN dibuat, Anda harus mengatur ulang koneksi sehingga rute baru dikirim ke klien.

Kami menyarankan Anda memperhitungkan jumlah rute yang dapat ditangani perangkat klien sebelum Anda memodifikasi tabel rute VPN titik akhir Klien.

Tugas

- Buat rute AWS Client VPN titik akhir
- Lihat AWS Client VPN rute titik akhir
- Hapus rute AWS Client VPN titik akhir

Buat rute AWS Client VPN titik akhir

Saat Anda membuat rute VPN titik akhir Klien, 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 VPN titik akhir Klien dengan menggunakan konsol dan. AWS CLI

Untuk membuat rute VPN titik akhir Klien (konsol)

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik VPNAkhir Klien.
3. Pilih VPN titik akhir Klien yang akan ditambahkan rute, pilih tabel Rute, lalu pilih Buat rute.
4. Untuk tujuan Rute, tentukan IPv4 CIDR rentang untuk jaringan tujuan. Sebagai contoh:
   - Untuk menambahkan rute untuk VPN titik VPC akhir Klien, masukkan VPC IPv4 CIDR rentang.
   - Untuk menambahkan rute akses internet, masukkan `0.0.0.0/0`.
   - Untuk menambahkan rute untuk peeredVPC, masukkan rentang peeredVPC. IPv4 CIDR
   - Untuk menambahkan rute untuk jaringan lokal, masukkan rentang koneksi AWS Site-to-SiteVPN. IPv4 CIDR
5. Untuk Subnet ID untuk asosiasi jaringan target, pilih subnet yang terkait dengan titik akhir KlienVPN.

   Atau, jika Anda menambahkan rute untuk jaringan VPN endpoint Klien lokal, pilih`local`.
6. (Opsional) Untuk Deskripsi, masukkan deskripsi singkat untuk rute tersebut.
7. Pilih Buat rute.

Untuk membuat rute VPN titik akhir Klien ()AWS CLI

Gunakan perintah create-client-vpn-route.

Lihat AWS Client VPN rute titik akhir

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

Untuk melihat rute VPN titik akhir Klien (konsol)

1. Di panel navigasi, pilih Titik VPNAkhir Klien.
2. Pilih VPN titik akhir Klien untuk melihat rute dan pilih tabel Rute.

Untuk melihat rute VPN titik akhir Klien ()AWS CLI

Gunakan perintah describe-client-vpn-routes.

Hapus rute AWS Client VPN titik akhir

Anda hanya dapat menghapus VPN rute Klien yang Anda tambahkan secara manual. Anda tidak dapat menghapus rute yang ditambahkan secara otomatis saat Anda mengaitkan subnet dengan titik VPN akhir Klien. Untuk menghapus rute yang ditambahkan secara otomatis, Anda harus memisahkan subnet yang memulai pembuatannya dari titik akhir Klien. VPN

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

Untuk menghapus rute VPN titik akhir Klien (konsol)

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

Untuk menghapus rute VPN titik akhir Klien ()AWS CLI

Gunakan perintah delete-client-vpn-route.

AWS Client VPN jaringan target

Jaringan target adalah subnet dalam aVPC. AWS Client VPN Endpoint harus memiliki setidaknya satu jaringan target untuk memungkinkan klien terhubung ke sana dan membuat VPN koneksi.

Untuk informasi selengkapnya tentang jenis akses yang dapat Anda konfigurasikan (seperti memungkinkan klien Anda mengakses internet), lihatSkenario dan contoh untuk Klien VPN.

Persyaratan jaringan VPN target klien

Saat membuat jaringan target, aturan berikut berlaku:

- Subnet harus memiliki CIDR blok dengan setidaknya /27 bitmask, misalnya 10.0.0.0/27. Subnet juga harus memiliki setidaknya 20 alamat IP yang tersedia setiap saat.
- CIDRBlok subnet tidak dapat tumpang tindih dengan CIDR rentang klien dari titik akhir KlienVPN.
- Jika Anda mengaitkan lebih dari satu subnet dengan VPN titik akhir Klien, setiap subnet harus berada di Availability Zone yang berbeda. Kami merekomendasikan Anda mengaitkan setidaknya dua subnet untuk menyediakan redundansi Availability Zone.

- Jika Anda menentukan VPC saat Anda membuat VPN titik akhir Klien, subnet harus sama. VPC Jika Anda belum mengaitkan VPC dengan VPN titik akhir Klien, Anda dapat memilih subnet apa pun di mana pun. VPC

  Semua asosiasi subnet lebih lanjut harus dari yang samaVPC. Untuk mengaitkan subnet dari yang berbedaVPC, Anda harus terlebih dahulu memodifikasi VPN titik akhir Klien dan mengubah VPC yang terkait dengannya. Untuk informasi selengkapnya, lihat Memodifikasi AWS Client VPN titik akhir.

Saat Anda mengaitkan subnet dengan VPN titik akhir Klien, kami secara otomatis menambahkan rute lokal VPC tempat subnet terkait disediakan ke tabel rute titik akhir KlienVPN.

> **Note**
>
> Setelah jaringan target Anda dikaitkan, ketika Anda menambah atau menghapus tambahan CIDRs ke lampiran AndaVPC, Anda harus melakukan salah satu operasi berikut untuk memperbarui rute lokal untuk tabel rute VPN titik akhir Klien Anda:
>
> - Putuskan hubungan VPN titik akhir Klien Anda dari jaringan target, lalu kaitkan VPN titik akhir Klien ke jaringan target.
> - Tambahkan rute secara manual, atau hapus rute dari tabel rute VPN titik akhir Klien.

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

Tugas

- Mengaitkan jaringan target dengan titik AWS Client VPN akhir
- Menerapkan grup keamanan ke jaringan target di AWS Client VPN
- Lihat jaringan AWS Client VPN target
- Putuskan hubungan jaringan target dari titik akhir AWS Client VPN

Mengaitkan jaringan target dengan titik AWS Client VPN akhir

Anda dapat mengaitkan satu atau beberapa jaringan target (subnet) dengan VPN titik akhir Klien menggunakan VPC Konsol Amazon atau. AWS CLI Sebelum Anda mengaitkan jaringan target

dengan VPN titik akhir Klien, biasakan diri Anda dengan persyaratan. Lihat Persyaratan untuk membuat jaringan target.

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

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik VPNAkhir Klien.
3. Pilih VPN titik akhir Klien untuk mengaitkan jaringan target, pilih Asosiasi jaringan target, lalu pilih Jaringan target asosiasi.
4. Untuk VPC, pilih VPC di mana subnet berada. Jika Anda menentukan VPC kapan Anda membuat VPN titik akhir Klien atau jika Anda memiliki asosiasi subnet sebelumnya, itu harus sama. VPC
5. Untuk Pilih subnet untuk diasosiasikan, pilih subnet untuk dikaitkan dengan titik akhir KlienVPN.
6. Pilih Jaringan target asosiasi.

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

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

Menerapkan grup keamanan ke jaringan target di AWS Client VPN

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

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

Untuk menerapkan grup keamanan ke jaringan target (konsol)

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

6. Pilih Terapkan Grup Keamanan.

Untuk menerapkan grup keamanan ke jaringan target (AWS CLI)

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

Lihat jaringan AWS Client VPN target

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

Untuk melihat jaringan target (konsol)

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

Untuk melihat jaringan target menggunakan AWS CLI

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

Putuskan hubungan jaringan target dari titik akhir AWS Client VPN

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

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

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik VPNAkhir Klien.
3. Pilih VPN titik akhir Klien 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 VPN titik akhir Klien ()AWS CLI

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

AWS Client VPN durasi VPN sesi maksimum

AWS Client VPN menyediakan beberapa opsi untuk durasi VPN sesi maksimum, yang merupakan waktu maksimum yang diizinkan untuk koneksi klien ke VPN titik akhir Klien. Anda dapat mengonfigurasi durasi VPN sesi maksimum yang lebih pendek untuk memenuhi persyaratan keamanan dan kepatuhan. Secara default, durasi VPN sesi maksimum adalah 24 jam.

> **Note**
>
> Ketika nilai durasi VPN sesi maksimum dikurangi dari nilai saat ini, setiap VPN sesi aktif yang terhubung ke titik akhir untuk jangka waktu yang lebih lama dari durasi yang baru ditetapkan akan terputus. Sesi baru perlu dimulai.

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

Konfigurasikan VPN sesi maksimum selama pembuatan titik AWS Client VPN akhir

Durasi VPN sesi dikonfigurasi selama pembuatan VPN titik akhir Klien. Lihat langkah-langkah Buat titik AWS Client VPN akhir untuk membuat VPN titik akhir Klien dan mengatur durasi sesi maksimum.

Tugas

- Lihat durasi VPN sesi maksimum AWS Client VPN saat ini
- Ubah durasi AWS Client VPN sesi maksimum

Lihat durasi VPN sesi maksimum AWS Client VPN saat ini

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

Melihat durasi VPN sesi maksimum saat ini untuk VPN titik akhir Klien (konsol)

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

3. Pilih VPN titik akhir Klien yang ingin Anda lihat.
4. Verifikasi bahwa tab Detail dipilih.
5. Lihat durasi VPN sesi maksimum saat ini di samping Jam tunggu sesi.

Melihat durasi VPN sesi maksimum saat ini untuk VPN titik akhir Klien ()AWS CLI

Gunakan perintah describe-client-vpn-endpoints.

Ubah durasi AWS Client VPN sesi maksimum

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

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

1. Buka VPC konsol Amazon di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Titik VPNakhir Klien.
3. Pilih VPN titik akhir Klien yang ingin Anda ubah, pilih Tindakan, lalu pilih Ubah Titik VPN Akhir Klien.
4. Untuk jam tunggu sesi, pilih waktu durasi VPN sesi maksimum yang diinginkan dalam jam.
5. Pilih Ubah VPN titik akhir Klien.

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

Gunakan perintah modify-client-vpn-endpoint.

Keamanan di AWS Client VPN

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

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku AWS Client VPN, lihat AWS Layanan dalam Lingkup oleh AWS Layanan Program Kepatuhan .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

AWS Client VPN adalah bagian dari VPC layanan Amazon. Untuk informasi selengkapnya tentang keamanan di AmazonVPC, lihat Keamanan di Panduan VPC Pengguna Amazon.

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

Topik

Perlindungan data di AWS Client VPN

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS KlienVPN. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk AWS layanan yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat Privasi Data FAQ. Untuk informasi tentang perlindungan data di Eropa, lihat Model Tanggung Jawab AWS Bersama dan posting GDPR blog di Blog AWS Keamanan.

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensi dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management ()IAM. Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan otentikasi multi-faktor (MFA) dengan setiap akun.
- GunakanSSL/TLSuntuk berkomunikasi dengan AWS sumber daya. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya AWS layanan.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan FIPS 140-3 modul kriptografi yang divalidasi saat mengakses AWS melalui antarmuka baris perintah atau, gunakan titik akhir. API FIPS Untuk informasi selengkapnya tentang FIPS titik akhir yang tersedia, lihat Federal Information Processing Standard (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk ketika Anda bekerja dengan Klien VPN atau lainnya AWS layanan menggunakan konsol,API, AWS CLI, atau AWS SDKs. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Jika Anda memberikan URL ke server eksternal, kami sangat menyarankan agar

Anda tidak menyertakan informasi kredensional dalam URL untuk memvalidasi permintaan Anda ke server tersebut.

Enkripsi bergerak

AWS Client VPN menyediakan koneksi aman dari lokasi manapun menggunakan Transport Layer Security (TLS) 1.2 atau yang lebih baru.

Privasi lalu lintas antar jaringan

Mengaktifkan akses antarjaringan

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

Pembatasan akses ke jaringan

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

Autentikasi klien

Autentikasi diimplementasikan pada titik pertama masuk ke dalam AWS Cloud. Ini digunakan untuk menentukan apakah klien diizinkan untuk terhubung ke VPN titik akhir Klien. Jika otentikasi berhasil, klien terhubung ke VPN titik akhir Klien dan membuat sesi. VPN Jika otentikasi gagal, koneksi ditolak dan klien dicegah membuat VPN sesi.

Klien VPN menawarkan jenis otentikasi klien berikut:

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

Identitas dan manajemen akses untuk AWS Client VPN

AWS Identity and Access Management (IAM) adalah AWS layanan yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. IAMadministrator mengontrol siapa yang

dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Klien. VPN IAMadalah AWS layanan yang dapat Anda gunakan tanpa biaya tambahan.

Topik

Audiens

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

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

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

IAMadministrator - Jika Anda seorang IAM administrator, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke KlienVPN. Untuk melihat contoh Kebijakan VPN berbasis identitas klien yang dapat Anda gunakan, lihat. IAM Contoh kebijakan berbasis identitas untuk AWS Client VPN

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai IAM pengguna, atau dengan mengambil peranIAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensi yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (Pusat IAM Identitas), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas federasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan IAM peran. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

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

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang menggunakan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani AWS API permintaan di Panduan IAM Pengguna.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari lebih lanjut, lihat Autentikasi multi-faktor di Panduan AWS IAM Identity Center Pengguna dan Menggunakan otentikasi multi-faktor (MFA) AWS di Panduan Pengguna. IAM

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua AWS layanan dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas

yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensi pengguna root di IAMPanduan Pengguna.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS layanan dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses AWS layanan dengan menggunakan kredensi yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

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

Pengguna dan grup IAM

IAMPengguna adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya mengandalkan kredensi sementara daripada membuat IAM pengguna yang memiliki kredensi jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensi jangka panjang dengan IAM pengguna, kami sarankan Anda memutar kunci akses. Untuk informasi selengkapnya, lihat Memutar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensi jangka panjang di IAMPanduan Pengguna.

IAMGrup adalah identitas yang menentukan kumpulan IAM pengguna. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup bernama IAMAdminsdan memberikan izin grup tersebut untuk mengelola sumber dayaIAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara.

Untuk mempelajari lebih lanjut, lihat Kapan membuat IAM pengguna (bukan peran) di Panduan IAM Pengguna.

IAMperan

IAMPeran adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Ini mirip dengan IAM pengguna, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil IAM peran sementara AWS Management Console dengan beralih peran. Anda dapat mengambil peran dengan memanggil AWS CLI atau AWS API operasi atau dengan menggunakan kustomURL. Untuk informasi selengkapnya tentang metode penggunaan peran, lihat Menggunakan IAM peran di Panduan IAM Pengguna.

IAMperan dengan kredensi sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga di Panduan IAM Pengguna. Jika Anda menggunakan Pusat IAM Identitas, Anda mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah diautentikasi, Pusat IAM Identitas menghubungkan izin yang disetel ke peran. IAM Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin IAM pengguna sementara — IAM Pengguna atau peran dapat mengambil IAM peran untuk sementara mengambil izin yang berbeda untuk tugas tertentu.
- Akses lintas akun — Anda dapat menggunakan IAM peran untuk memungkinkan seseorang (prinsipal tepercaya) di akun lain mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa AWS layanan, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM Panduan Pengguna. IAM
- Akses lintas layanan — Beberapa AWS layanan menggunakan fitur lain AWS layanan. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan

beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FASmenggunakan izin dari pemanggilan utama AWS layanan, dikombinasikan dengan permintaan AWS layanan untuk membuat permintaan ke layanan hilir. FASPermintaan hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain AWS layanan atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat Meneruskan sesi akses.

- Peran layanan — Peran layanan adalah IAMperan yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalamIAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke AWS layanan dalam IAMPanduan Pengguna.
- Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. AWS layanan Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. IAMAdministrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.

- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan IAM peran untuk mengelola kredenal sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS API meminta. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensi sementara. Untuk informasi selengkapnya, lihat Menggunakan IAM peran untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di IAMPanduan Pengguna.

Untuk mempelajari apakah akan menggunakan IAM peran atau IAM pengguna, lihat Kapan membuat IAM peran (bukan pengguna) di Panduan IAM Pengguna.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai JSON dokumen. Untuk informasi selengkapnya tentang struktur dan isi dokumen JSON kebijakan, lihat Ringkasan JSON kebijakan di Panduan IAM Pengguna.

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka butuhkan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

IAMkebijakan menentukan izin untuk tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasi. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan itu bisa mendapatkan informasi peran dari AWS Management Console, AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat Anda lampirkan ke identitas, seperti pengguna, grup IAM pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat IAM kebijakan di Panduan Pengguna. IAM

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan sebaris, lihat Memilih antara kebijakan terkelola dan kebijakan sebaris di IAMPanduan Pengguna.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. AWS layanan

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

Daftar kontrol akses (ACLs)

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLsmirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung. ACLs Untuk mempelajari selengkapnyaACLs, lihat Ikhtisar daftar kontrol akses (ACL) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batas izin — Batas izin adalah fitur lanjutan tempat Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas (pengguna atau peran). IAM IAM Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batas izin, lihat Batas izin untuk IAM entitas di IAMPanduan Pengguna.
- Kebijakan kontrol layanan (SCPs) — SCPs adalah JSON kebijakan yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCPMembatasi izin untuk entitas di akun anggota, termasuk masing-masing Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organizations danSCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan

secara tegas dalam salah satu kebijakan ini membatalkan izin. Untuk informasi selengkapnya, lihat Kebijakan sesi di Panduan IAM Pengguna.

Berbagai jenis kebijakan

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

Bagaimana AWS Client VPN bekerja dengan IAM

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

IAMfitur yang dapat Anda gunakan dengan AWS Klien VPN

IAMfitur	VPNDukungan klien
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
ACLs	Tidak
ABAC(tag dalam kebijakan)	Tidak
Kredensial sementara	Ya
Izin prinsipal	Ya
Peran layanan	Ya
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang bagaimana Klien VPN dan AWS layanan lain bekerja dengan sebagian besar IAM fitur, lihat AWS layanan yang bekerja dengan IAM dalam Panduan IAM Pengguna.

Kebijakan berbasis identitas untuk Klien VPN

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat Anda lampirkan ke identitas, seperti pengguna, grup IAM pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat IAM kebijakan di Panduan Pengguna. IAM

Dengan kebijakan IAM berbasis identitas, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak serta kondisi di mana tindakan diizinkan atau ditolak. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam JSON kebijakan, lihat referensi elemen IAM JSON kebijakan di Panduan IAM Pengguna.

Contoh kebijakan berbasis identitas untuk Klien VPN

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

Kebijakan berbasis sumber daya dalam Klien VPN

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. AWS layanan

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

Tindakan kebijakan untuk Klien VPN

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

`Action`Elemen JSON kebijakan menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan AWS API operasi terkait. Ada beberapa pengecualian, seperti tindakan khusus izin yang tidak memiliki operasi yang cocok. API Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

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

Tindakan kebijakan di Klien VPN menggunakan awalan berikut sebelum tindakan:

```
ec2
```

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

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

```
        ]
```

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

Sumber daya kebijakan untuk Klien VPN

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Resource` JSON kebijakan menentukan objek atau objek yang tindakan tersebut berlaku. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Sebagai praktik terbaik, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

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

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

Kunci kondisi kebijakan untuk Klien VPN

Mendukung kunci kondisi kebijakan khusus layanan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

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

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi `AND` logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Misalnya, Anda dapat memberikan izin IAM pengguna untuk mengakses sumber daya hanya jika ditandai dengan nama IAM pengguna mereka. Untuk informasi selengkapnya, lihat elemen IAM kebijakan: variabel dan tag di Panduan IAM Pengguna.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan IAM Pengguna.

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

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

ACLsdi Klien VPN

MendukungACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLsmirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

ABACdengan Klien VPN

Mendukung ABAC (tag dalam kebijakan): Tidak

Attribute-based access control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke IAM entitas (pengguna atau peran) dan ke banyak AWS sumber daya. Menandai entitas dan sumber daya adalah langkah pertama dari. ABAC Kemudian Anda merancang ABAC kebijakan untuk mengizinkan operasi ketika tag prinsipal cocok dengan tag pada sumber daya yang mereka coba akses.

ABACmembantu dalam lingkungan yang berkembang pesat dan membantu dengan situasi di mana manajemen kebijakan menjadi rumit.

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

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

Untuk informasi lebih lanjut tentangABAC, lihat Apa ituABAC? dalam IAMUser Guide. Untuk melihat tutorial dengan langkah-langkah penyiapanABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) di IAMPanduan Pengguna.

Menggunakan kredensi sementara dengan Klien VPN

Mendukung kredensi sementara: Ya

Beberapa AWS layanan tidak berfungsi saat Anda masuk menggunakan kredensi sementara. Untuk informasi tambahan, termasuk yang AWS layanan bekerja dengan kredensil sementara, lihat AWS layanan yang berfungsi IAM di IAMPanduan Pengguna.

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan link sign-on (SSO) tunggal perusahaan Anda, proses tersebut secara otomatis membuat kredensi sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang beralih peran, lihat Beralih ke peran (konsol) di Panduan IAM Pengguna.

Anda dapat secara manual membuat kredensi sementara menggunakan atau. AWS CLI AWS API Anda kemudian dapat menggunakan kredensi sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih

menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensi keamanan sementara di. IAM

Izin utama lintas layanan untuk Klien VPN

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FASmenggunakan izin dari pemanggilan utama AWS layanan, dikombinasikan dengan permintaan AWS layanan untuk membuat permintaan ke layanan hilir. FASPermintaan hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain AWS layanan atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat Meneruskan sesi akses.

Peran layanan untuk Klien VPN

Mendukung peran layanan: Ya

Peran layanan adalah IAMperan yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalamIAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke AWS layanan dalam IAMPanduan Pengguna.

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

Peran terkait layanan untuk Klien VPN

Mendukung peran terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. AWS layanan Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. IAMAdministrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.

Untuk detail tentang membuat atau mengelola peran terkait layanan, lihat AWS layanan yang berfungsi dengannya. IAM Cari layanan dalam tabel yang memiliki `Yes` di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Contoh kebijakan berbasis identitas untuk AWS Client VPN

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi VPN sumber daya Klien. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka butuhkan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

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

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

Topik

- Praktik terbaik kebijakan
- Mengizinkan pengguna melihat izin mereka sendiri

Praktik terbaik kebijakan

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

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan AWSAWS terkelola atau kebijakan terkelola untuk fungsi pekerjaan di Panduan IAM Pengguna.

- Menerapkan izin hak istimewa paling sedikit — Saat Anda menetapkan izin dengan IAM kebijakan, berikan hanya izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang penggunaan IAM untuk menerapkan izin, lihat Kebijakan dan izin IAM di IAM Panduan Pengguna.
- Gunakan ketentuan dalam IAM kebijakan untuk membatasi akses lebih lanjut — Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakanSSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik AWS layanan, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat elemen IAM JSON kebijakan: Kondisi dalam Panduan IAM Pengguna.
- Gunakan IAM Access Analyzer untuk memvalidasi IAM kebijakan Anda guna memastikan izin yang aman dan fungsional — IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan mematuhi bahasa IAM kebijakan () JSON dan praktik terbaik. IAM IAMAccess Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan IAM Access Analyzer di IAMPanduan Pengguna.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan IAM pengguna atau pengguna root di Anda Akun AWS, aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA kapan API operasi dipanggil, tambahkan MFA kondisi ke kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi API akses MFA yang dilindungi di IAMPanduan Pengguna.

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

Mengizinkan pengguna melihat izin mereka sendiri

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

```
{
    "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 AWS Client VPN identitas dan akses

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

Topik

- Saya tidak berwenang untuk melakukan tindakan di Klien VPN
- Saya tidak berwenang untuk melakukan iam: PassRole

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

Saya tidak berwenang untuk melakukan tindakan di Klien VPN

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

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

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya *`my-example-widget`* dengan menggunakan tindakan `ec2:`*`GetWidget`*.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran kepada KlienVPN.

Beberapa AWS layanan memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika IAM pengguna bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di KlienVPN. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

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

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

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah Klien VPN mendukung fitur ini, lihatBagaimana AWS Client VPN bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke IAM pengguna lain Akun AWS yang Anda miliki di Panduan IAM Pengguna.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan IAM Pengguna.
- Untuk mempelajari cara menyediakan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna yang diautentikasi secara eksternal (federasi identitas) di Panduan Pengguna. IAM
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM Panduan Pengguna. IAM

Menggunakan peran terkait layanan untuk AWS Client VPN

AWS Client VPN menggunakan AWS Identity and Access Management (IAM) peran terkait layanan. Peran terkait layanan adalah jenis peran unik yang ditautkan langsung ke Klien. IAM VPN Peran terkait layanan telah ditentukan sebelumnya oleh Klien VPN dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Topik

- Menggunakan peran untuk AWS Client VPN

- Menggunakan peran untuk otorisasi koneksi di KlienVPN;

Menggunakan peran untuk AWS Client VPN

AWS Client VPN menggunakan AWS Identity and Access Management (IAM) peran terkait layanan. Peran terkait layanan adalah jenis peran unik yang ditautkan langsung ke Klien. IAM VPN Peran terkait layanan telah ditentukan sebelumnya oleh Klien VPN dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan Klien VPN lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Klien VPN mendefinisikan izin dari peran terkait layanannya, dan kecuali ditentukan lain, hanya Klien yang VPN dapat mengambil perannya. Izin yang ditetapkan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas lain mana pun. IAM

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

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat AWS layanan yang bekerja dengan IAM dan cari layanan yang memiliki Ya di kolom Peran terkait layanan. Pilih Ya bersama tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Izin peran terkait layanan untuk Klien VPN

Klien VPN menggunakan peran terkait layanan bernama AWSServiceRoleForClientVPN— Izinkan Klien VPN membuat dan mengelola sumber daya yang terkait dengan koneksi AndaVPN.

Peran AWSServiceRoleForClientVPNterkait layanan mempercayai layanan berikut untuk mengambil peran:

- `clientvpn.amazonaws.com`

Kebijakan izin peran bernama C lientVPNService RolePolicy memungkinkan Klien 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 mengonfigurasi izin untuk mengizinkan IAM entitas (seperti pengguna, grup, atau peran) membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran terkait layanan di Panduan Pengguna. IAM

Membuat peran terkait layanan untuk Klien VPN

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat VPN titik akhir Klien pertama di akun Anda dengan AWS Management Console, Klien AWS CLI, atau AWS API, Klien 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 VPN titik akhir Klien pertama di akun Anda, Klien VPN membuat peran terkait layanan untuk Anda lagi.

Mengedit peran terkait layanan untuk Klien VPN

Klien VPN tidak mengizinkan Anda mengedit peran AWSServiceRoleForClientVPN 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 deskripsi peran menggunakanIAM. Untuk informasi selengkapnya, lihat Mengedit peran terkait layanan di IAMPanduan Pengguna.

Menghapus peran terkait layanan untuk Klien VPN

Jika Anda tidak perlu lagi menggunakan KlienVPN, kami sarankan Anda menghapus peran AWSServiceRoleForClientVPNterkait layanan.

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

Gunakan IAM konsol, the IAMCLI, atau IAM API untuk menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Menghapus Peran Tertaut Layanan di Panduan Pengguna. IAM

Wilayah yang Didukung untuk peran VPN terkait layanan Klien

Klien VPN mendukung penggunaan peran terkait layanan di semua Wilayah tempat layanan tersedia. Untuk informasi selengkapnya, silakan lihat Wilayah AWS dan titik akhir.

Menggunakan peran untuk otorisasi koneksi di KlienVPN;

AWS Client VPN menggunakan AWS Identity and Access Management (IAM) peran terkait layanan. Peran terkait layanan adalah jenis peran unik yang ditautkan langsung ke Klien. IAM VPN Peran terkait layanan telah ditentukan sebelumnya oleh Klien VPN dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan Klien VPN lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Klien VPN mendefinisikan izin dari peran terkait layanannya, dan kecuali ditentukan lain, hanya Klien yang VPN dapat mengambil perannya. Izin yang ditetapkan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas lain mana pun. IAM

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

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat AWS layanan yang bekerja dengan IAM dan cari layanan yang memiliki Ya di kolom Peran terkait layanan. Pilih Ya bersama tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Izin peran terkait layanan untuk Klien VPN

Klien VPN menggunakan peran terkait layanan bernama AWSServiceRoleForClientVPNConnections— Peran Tertaut Layanan untuk koneksi KlienVPN.

Peran AWSServiceRoleForClientVPNConnections terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `clientvpn-connections.amazonaws.com`

Kebijakan izin peran bernama C lientVPNService ConnectionsRolePolicy memungkinkan Klien VPN untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

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

Anda harus mengonfigurasi izin untuk mengizinkan IAM entitas (seperti pengguna, grup, atau peran) membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran terkait layanan di Panduan Pengguna. IAM

Membuat peran terkait layanan untuk Klien VPN

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat VPN titik akhir Klien pertama di akun Anda dengan AWS Management Console, Klien AWS CLI, atau AWS API, Klien 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 VPN titik akhir Klien pertama di akun Anda, Klien VPN membuat peran terkait layanan untuk Anda lagi.

Mengedit peran terkait layanan untuk Klien VPN

Klien VPN tidak mengizinkan Anda mengedit peran AWSServiceRoleForClientVPNConnections 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 deskripsi peran menggunakanIAM. Untuk informasi selengkapnya, lihat Mengedit peran terkait layanan di IAMPanduan Pengguna.

Menghapus peran terkait layanan untuk Klien VPN

Jika Anda tidak perlu lagi menggunakan KlienVPN, kami sarankan Anda menghapus peran AWSServiceRoleForClientVPNConnectionsterkait layanan.

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

Gunakan IAM konsol, the IAMCLI, atau IAM API untuk menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Menghapus Peran Tertaut Layanan di Panduan Pengguna. IAM

Wilayah yang Didukung untuk peran VPN terkait layanan Klien

Klien VPN mendukung penggunaan peran terkait layanan di semua Wilayah tempat layanan tersedia. Untuk informasi selengkapnya, silakan lihat Wilayah AWS dan titik akhir.

Ketahanan di AWS Client VPN

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

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

Selain infrastruktur AWS global, AWS Client VPN menawarkan fitur untuk membantu mendukung ketahanan data dan kebutuhan cadangan Anda.

Beberapa jaringan target untuk ketersediaan yang tinggi

Anda mengaitkan jaringan target dengan VPN titik akhir Klien untuk memungkinkan klien membuat VPN sesi. Jaringan target adalah subnet di AndaVPC. Setiap subnet yang Anda kaitkan dengan VPN

titik akhir Klien harus dimiliki oleh Availability Zone yang berbeda. Anda dapat mengaitkan beberapa subnet dengan VPN titik akhir Klien untuk ketersediaan tinggi.

Keamanan infrastruktur di AWS Client VPN

Sebagai layanan terkelola, AWS Klien VPN dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

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

- Keamanan Lapisan Transportasi (TLS). Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Suite cipher dengan kerahasiaan maju yang sempurna (PFS) seperti (Ephemeral Diffie-Hellman) atau DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani dengan menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan IAM prinsipal. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Praktik terbaik keamanan untuk AWS Client VPN

AWS Client VPN menyediakan sejumlah fitur keamanan untuk dipertimbangkan saat 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 AWS Client VPN aturan otorisasi.

Grup keamanan

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

Daftar pencabutan sertifikat klien

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

Alat pemantauan

Gunakan alat pemantauan untuk melacak ketersediaan dan kinerja VPN titik akhir Klien Anda. Untuk informasi selengkapnya, lihat Pemantauan AWS Client VPN.

Pengelolaan identitas dan akses

Kelola akses ke VPN sumber daya Klien dan APIs dengan menggunakan IAM kebijakan untuk IAM pengguna dan IAM peran Anda. Untuk informasi selengkapnya, lihat Identitas dan manajemen akses untuk AWS Client VPN.

IPv6pertimbangan untuk AWS Client VPN

Saat ini VPN layanan Klien tidak mendukung IPv6 lalu lintas routing melalui VPN terowongan. Namun, ada beberapa kasus ketika IPv6 lalu lintas harus diarahkan ke VPN terowongan untuk mencegah IPv6 kebocoran. IPv6kebocoran dapat terjadi ketika keduanya IPv4 dan IPv6 diaktifkan dan terhubung keVPN, tetapi VPN tidak mengarahkan IPv6 lalu lintas ke terowongannya. Dalam hal ini, saat menghubungkan ke tujuan yang IPv6 diaktifkan, Anda sebenarnya masih terhubung dengan IPv6 alamat yang disediakan oleh AndaISP. Ini akan membocorkan IPv6 alamat asli Anda. Petunjuk di bawah ini menjelaskan cara mengarahkan IPv6 lalu lintas ke VPN terowongan.

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

```
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 IPv6 alamat perangkat terowongan lokal menjadi `fd15:53b6:dead::2` dan IPv6 alamat VPN endpoint jarak jauh menjadi`fd15:53b6:dead::1`.

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

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

Organizations harus mengkonfigurasi dua parameter `ifconfig-ipv6` itu sendiri, dan dapat menggunakan alamat di `100::/64` (dari `0100:0000:0000:0000:0000:0000:0000:0000` ke`0100:0000:0000:0000:ffff:ffff:ffff:ffff`) atau `fc00::/7` (dari `fc00:0000:0000:0000:0000:0000:0000:0000` ke`fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff`). `100::/64`adalah Blok Alamat Hanya Buang, dan `fc00::/7` 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 IPv6 lalu lintas yang saat ini dialokasikan ke VPN koneksi.

Verifikasi

Organisasi Anda kemungkinan akan memiliki tes sendiri. Verifikasi dasar adalah mengatur VPN koneksi terowongan penuh, lalu jalankan ping6 ke IPv6 server menggunakan alamat. IPv6 IPv6Alamat server harus dalam kisaran yang ditentukan oleh `route-ipv6` perintah. Tes ping ini seharusnya gagal. Namun, ini dapat berubah jika IPv6 dukungan ditambahkan ke VPN layanan Klien

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. Ada juga beberapa alat yang tersedia untuk umum.

Pemantauan AWS Client VPN

Pemantauan adalah bagian penting dari menjaga keandalan, ketersediaan, dan kinerja AWS Client VPN dan AWS solusi Anda yang lain. Anda dapat menggunakan fitur berikut untuk memantau VPN titik akhir Klien Anda, menganalisis pola lalu lintas, dan memecahkan masalah dengan titik akhir Klien Anda. VPN

Amazon CloudWatch

Memantau AWS sumber daya Anda dan aplikasi yang Anda jalankan AWS secara real time. 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 CloudWatch melacak CPU penggunaan atau metrik lain dari EC2 instans Amazon Anda dan secara otomatis meluncurkan instans baru bila diperlukan. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

AWS CloudTrail

Menangkap API panggilan dan peristiwa terkait yang dilakukan oleh atau atas nama AWS akun Anda dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS CloudTrail.

CloudWatch Log Amazon

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

Topik

CloudWatch Metrik Amazon untuk AWS Client VPN

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

Metrik	Deskripsi
ActiveConnectionsCount	Jumlah koneksi aktif ke VPN titik akhir Klien. Unit: Jumlah
AuthenticationFailures	Jumlah kegagalan otentikasi untuk titik VPN akhir Klien. Unit: Jumlah
CrlDaysToExpiry	Jumlah hari sampai Daftar Pencabutan Sertifika t (CRL) yang dikonfigurasi pada titik VPN akhir Klien berakhir. Unit: Hari
EgressBytes	Jumlah byte yang dikirim dari titik VPN akhir Klien. Unit: Bita
EgressPackets	Jumlah paket yang dikirim dari titik VPN akhir Klien. Unit: Jumlah
IngressBytes	Jumlah byte yang diterima oleh titik VPN akhir Klien. Unit: Bita
IngressPackets	Jumlah paket yang diterima oleh titik VPN akhir Klien.

Metrik	Deskripsi
	Unit: Jumlah
SelfServicePortalClientConfigurationDownloads	Jumlah unduhan file konfigurasi VPN titik akhir Klien dari portal swalayan. Unit: Jumlah

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

Metrik	Deskripsi
ClientConnectHandlerTimeouts	Jumlah batas waktu saat memanggil handler koneksi klien untuk koneksi ke titik akhir Klien. VPN Unit: Jumlah
ClientConnectHandlerInvalidResponses	Jumlah tanggapan tidak valid yang dikembali kan oleh handler koneksi klien untuk koneksi ke titik akhir Klien. VPN Unit: Jumlah
ClientConnectHandlerOtherExecutionErrors	Jumlah kesalahan tak terduga saat menjalank an handler koneksi klien untuk koneksi ke titik VPN akhir Klien. Unit: Jumlah
ClientConnectHandlerThrottlingErrors	Jumlah kesalahan pelambatan saat memanggil handler koneksi klien untuk koneksi ke titik akhir Klien. VPN Unit: Jumlah

Metrik	Deskripsi
ClientConnectHandlerDeniedConnections	Jumlah koneksi yang ditolak oleh handler koneksi klien untuk koneksi ke titik VPN akhir Klien. Unit: Jumlah
ClientConnectHandlerFailedServiceErrors	Jumlah kesalahan sisi layanan saat menjalankan handler koneksi klien untuk koneksi ke titik VPN akhir Klien. Unit: Jumlah

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

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

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

Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

Tugas

- Lihat metrik VPN titik akhir Klien di Amazon CloudWatch

Lihat metrik VPN titik akhir Klien di Amazon CloudWatch

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

Untuk melihat metrik menggunakan konsol CloudWatch

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

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

Untuk melihat metrik menggunakan AWS CLI

Pada prompt perintah, gunakan perintah berikut untuk membuat daftar metrik yang tersedia untuk Klien VPN

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

AWS CloudTrail log untuk AWS Client VPN

AWS Client VPN terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di KlienVPN. CloudTrail menangkap semua API panggilan untuk Klien VPN sebagai acara. Panggilan yang diambil termasuk panggilan dari VPN konsol Klien dan panggilan kode ke VPN API operasi Klien. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk acara untuk Klien. VPN Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Gunakan informasi yang dikumpulkan oleh CloudTrail untuk menentukan permintaan yang dibuat untuk KlienVPN, alamat IP yang meminta, pemohon, kapan dibuat, dan rincian tambahan.

Untuk informasi selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

VPNInformasi klien di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Ketika aktivitas terjadi di KlienVPN, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di AWS akun Anda. Untuk informasi selengkapnya, lihat Melihat Acara dengan Riwayat CloudTrail Acara.

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk KlienVPN, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon

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

- Gambaran Umum untuk Membuat Jejak
- CloudTrail Layanan dan Integrasi yang Didukung
- Mengkonfigurasi SNS Pemberitahuan Amazon untuk CloudTrail
- Menerima File CloudTrail Log dari Beberapa Wilayah dan Menerima File CloudTrail Log dari Beberapa Akun

Semua VPN tindakan Klien dicatat oleh CloudTrail dan didokumentasikan dalam EC2APIReferensi Amazon. Misalnya, panggilan ke`CreateClientVpnEndpoint`,`AssociateClientVpnTargetNetwork`, dan `AuthorizeClientVpnIngress` tindakan menghasilkan entri dalam file CloudTrail log.

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

- Apakah permintaan dibuat dengan root atau AWS Identity and Access Management (IAM) kredensional pengguna.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna terfederasi.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat CloudTrail userIdentity Elemen.

Memahami entri berkas VPN log Klien

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa merepresentasikan satu permintaan dari sumber apa pun dan menyertakan informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari API panggilan publik, sehingga tidak muncul dalam urutan tertentu.

Untuk informasi selengkapnya, lihat Mencatat VPC API panggilan Amazon EC2EBS, Amazon, dan Amazon AWS CloudTrail di EC2APIReferensi Amazon.

AWS Client VPN kuota

AWS Akun Anda memiliki kuota berikut, sebelumnya disebut sebagai batas, terkait dengan titik akhir Klien. VPN Kecuali dinyatakan lain, setiap kuota bersifat khusus per Wilayah. Anda dapat meminta peningkatan untuk beberapa kuota dan kuota lainnya tidak dapat ditingkatkan.

Untuk meminta peningkatan kuota untuk kuota yang dapat disesuaikan, pilih Ya di kolom Adjustable. Untuk informasi selengkapnya, lihat Meminta peningkatan kuota di Panduan Pengguna Service Quotas.

VPNKuota klien

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

Saat Anda mengonfigurasi pengguna dan grup untuk Active Directory atau iDP SAML berbasis, 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-hal berikut saat Anda menggunakan VPN titik akhir Klien:

- Jika Anda menggunakan Active Directory untuk mengautentikasi pengguna, VPN titik akhir Klien harus milik akun yang sama dengan AWS Directory Service sumber daya yang digunakan untuk otentikasi Active Directory.
- Jika Anda menggunakan otentikasi federasi SAML berbasis untuk mengautentikasi pengguna, VPN titik akhir Klien harus memiliki akun yang sama dengan penyedia IAM SAML identitas yang Anda buat untuk menentukan hubungan IDP dengan kepercayaan. AWS Penyedia IAM SAML identitas dapat dibagikan di beberapa VPN titik akhir Klien di AWS akun yang sama.

Pemecahan masalah AWS Client VPN

Bagian berikut dapat membantu Anda memecahkan masalah yang mungkin Anda miliki dengan titik akhir KlienVPN.

Untuk informasi selengkapnya tentang pemecahan masalah Perangkat lunak VPN berbasis terbuka yang digunakan klien untuk terhubung ke KlienVPN, lihat Memecahkan Masalah VPN Koneksi Klien Anda di Panduan Pengguna.AWS Client VPN

Masalah umum

- Pemecahan masalah AWS Client VPN: Tidak dapat menyelesaikan nama titik akhir Klien VPN DNS
- Pemecahan masalah AWS Client VPN: Lalu lintas tidak dibagi antara subnet
- Pemecahan masalah AWS Client VPN: Aturan otorisasi untuk grup Active Directory tidak berfungsi seperti yang diharapkan
- Pemecahan masalah AWS Client VPN: Klien tidak dapat mengakses peered, Amazon VPC S3, atau internet
- Pemecahan masalah AWS Client VPN: Akses ke peered, Amazon VPC S3, atau internet terputus-putus
- Pemecahan masalah AWS Client VPN: Perangkat lunak klien mengembalikan TLS kesalahan saat mencoba terhubung ke Klien VPN
- Pemecahan masalah AWS Client VPN: Perangkat lunak klien mengembalikan kesalahan nama pengguna dan kata sandi — Otentikasi Direktori Aktif
- Pemecahan masalah AWS Client VPN: Perangkat lunak klien mengembalikan kesalahan nama pengguna dan kata sandi - otentikasi federasi
- Pemecahan masalah AWS Client VPN: Klien tidak dapat terhubung — otentikasi timbal balik
- Pemecahan masalah AWS Client VPN: Klien mengembalikan kredensi melebihi kesalahan ukuran maksimal di Klien - otentikasi federasi VPN
- Pemecahan masalah AWS Client VPN: Klien tidak membuka browser untuk titik akhir — otentikasi federasi
- Pemecahan masalah AWS Client VPN: Klien tidak mengembalikan kesalahan port yang tersedia - otentikasi federasi
- Pemecahan masalah AWS Client VPN: Koneksi dihentikan karena ketidakcocokan IP

- Pemecahan masalah AWS Client VPN: Merutekan lalu lintas ke LAN tidak berfungsi seperti yang diharapkan
- Pemecahan masalah AWS Client VPN: Verifikasi batas bandwidth untuk titik akhir Klien VPN

Pemecahan masalah AWS Client VPN: Tidak dapat menyelesaikan nama titik akhir Klien VPN DNS

Masalah

Saya tidak dapat menyelesaikan DNS nama VPN titik akhir Klien.

Penyebab

File konfigurasi VPN titik akhir Klien menyertakan parameter yang disebut`remote-random-hostname`. Parameter ini memaksa klien untuk menambahkan string acak ke DNS nama untuk mencegah DNS caching. Beberapa klien tidak mengenali parameter ini dan oleh karena itu, mereka tidak menambahkan string acak yang diperlukan ke namanya. DNS

Solusi

Buka file konfigurasi VPN titik akhir Klien menggunakan editor teks pilihan Anda. Temukan baris yang menentukan DNS nama VPN endpoint Klien, dan menambahkan string acak ke dalamnya sehingga formatnya *`random_string.displayed_DNS_name`*. Sebagai contoh:

- DNSNama asli: `cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`
- DNSNama yang dimodifikasi: `asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`

Pemecahan masalah AWS Client VPN: Lalu lintas tidak dibagi 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 VPN titik akhir Klien.

Penyebab

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

Klien terhubung ke VPN titik akhir Klien berdasarkan algoritma DNS round-robin. 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 VPN titik akhir Klien memiliki entri rute yang sama dengan target untuk setiap jaringan terkait. Ini memastikan bahwa klien memiliki akses ke semua rute terlepas dari subnet mana yang dirutekan untuk lalu lintas mereka.

Pemecahan masalah AWS Client VPN: Aturan otorisasi untuk grup Active Directory 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 untuk `0.0.0.0/0` mengotorisasi lalu lintas untuk semua jaringan, tetapi lalu lintas masih gagal untuk tujuan tertentu. CIDRs

Penyebab

Aturan otorisasi diindeks di jaringan. CIDRs Aturan otorisasi harus memberikan akses grup Active Directory ke jaringan CIDRs 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.

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

Solusi

Verifikasi bahwa Anda membuat aturan otorisasi yang secara eksplisit memberikan akses grup Active Directory ke jaringan tertentu. CIDRs 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.

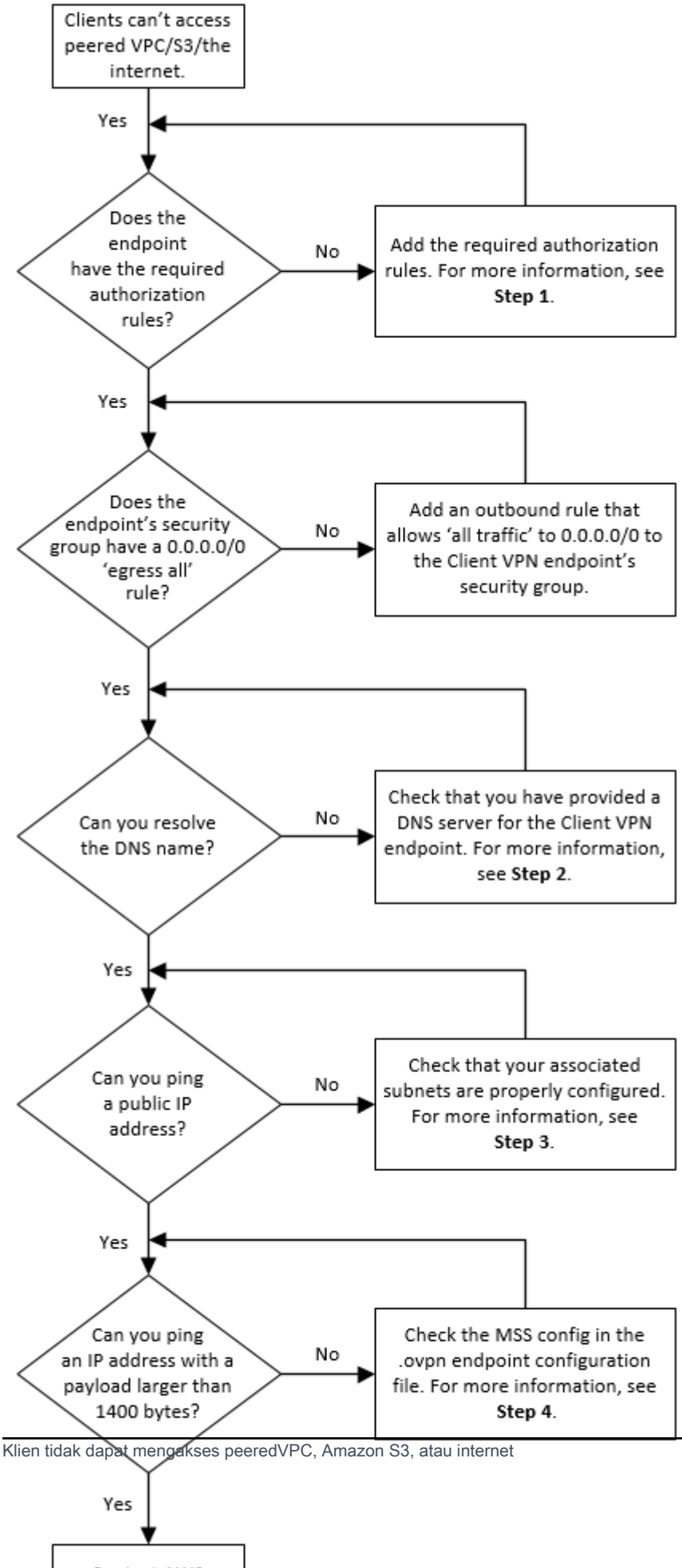
Pemecahan masalah AWS Client VPN: Klien tidak dapat mengakses peered, Amazon VPC S3, atau internet

Masalah

Saya telah mengonfigurasi rute VPN titik akhir Klien saya dengan benar, tetapi klien saya tidak dapat mengakses peeredVPC, Amazon S3, atau internet.

Solusi

Diagram alir berikut berisi langkah-langkah untuk mendiagnosis masalah konektivitas internet, peeredVPC, 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 peeredVPC, tambahkan aturan otorisasi untuk IPv4 CIDR rentang. VPC

   Untuk akses menuju S3, tentukan alamat IP dari titik akhir Amazon S3.

2. Periksa apakah Anda dapat menyelesaikan DNS nama.

   Jika Anda tidak dapat menyelesaikan DNS nama, verifikasi bahwa Anda telah menentukan DNS server untuk VPN titik akhir Klien. Jika Anda mengelola DNS server Anda sendiri, tentukan alamat IP-nya. Verifikasi bahwa DNS server dapat diakses dariVPC.

   Jika Anda tidak yakin tentang alamat IP mana yang akan ditentukan untuk DNS server, tentukan VPC DNS resolver di alamat IP .2 di alamat IP Anda. VPC

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 bahwa tabel rute untuk subnet terkait memiliki rute default yang menargetkan gateway internet atau NAT gateway. 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 mencapai peeredVPC, verifikasi bahwa tabel rute subnet terkait memiliki entri rute untuk peered. VPC

   Jika Anda tidak dapat mencapai Amazon S3, verifikasi bahwa tabel rute subnet terkait memiliki entri rute untuk titik akhir gateway. VPC

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 melakukan ping ke alamat IP dengan muatan yang lebih besar dari 1400 byte, buka file `.ovpn` konfigurasi VPN titik akhir Klien menggunakan editor teks pilihan Anda, dan tambahkan yang berikut ini.

```
mssfix 1328
```

Pemecahan masalah AWS Client VPN: Akses ke peered, Amazon VPC S3, atau internet terputus-putus

Masalah

Saya memiliki masalah konektivitas intermiten saat menghubungkan ke peered, Amazon VPC 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 VPN titik akhir Klien berdasarkan algoritma DNS round-robin. 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 VPN titik akhir Klien 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, katakan bahwa VPN titik akhir Klien Anda memiliki tiga subnet terkait (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

Pemecahan masalah AWS Client VPN: Perangkat lunak klien mengembalikan TLS kesalahan saat mencoba terhubung ke Klien VPN

Masalah

Saya dulu VPN berhasil menghubungkan klien saya ke Klien, tetapi sekarang klien VPN berbasis Terbuka 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 otentikasi, VPN titik akhir Klien memeriksa sertifikat klien terhadap daftar pencabutan sertifikat klien yang Anda impor. Jika daftar pencabutan sertifikat klien telah kedaluwarsa, Anda tidak dapat terhubung ke titik akhir Klien. VPN

Solusi #1

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

```
$ 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 yang baru dan mengimpornya ke titik akhir Klien. VPN Untuk informasi selengkapnya, lihat AWS Client VPN daftar pencabutan sertifikat klien.

Kemungkinan penyebabnya #2

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

Solusi #2

Periksa status sertifikat server Anda di AWS Certificate Manager konsol atau dengan menggunakan file AWS CLI. Jika sertifikat server kedaluwarsa, buat sertifikat baru dan unggah keACM. Untuk langkah-langkah rinci untuk menghasilkan server dan sertifikat klien dan kunci menggunakan utilitas Open VPN easy-rsa, dan impor mereka ke ACM see. Otentikasi timbal balik di AWS Client VPN

Atau, mungkin ada masalah dengan perangkat lunak VPN berbasis Terbuka yang digunakan klien untuk terhubung ke KlienVPN. Untuk informasi selengkapnya tentang pemecahan masalah Perangkat lunak VPN berbasis terbuka, lihat Memecahkan Masalah VPN Koneksi Klien Anda di Panduan Pengguna.AWS Client VPN

Pemecahan masalah AWS Client VPN: Perangkat lunak klien mengembalikan kesalahan nama pengguna dan kata sandi — Otentikasi Direktori Aktif

Masalah

Saya menggunakan otentikasi Active Directory untuk VPN titik akhir Klien saya dan saya dulu dapat menghubungkan klien saya ke Klien VPN dengan sukses. Tapi sekarang, klien mendapatkan galat nama pengguna dan kata sandi tidak valid.

Kemungkinan penyebab

Jika Anda menggunakan otentikasi Active Directory dan jika Anda mengaktifkan otentikasi multi-faktor (MFA) setelah Anda mendistribusikan file konfigurasi klien, file tersebut tidak berisi informasi yang diperlukan untuk meminta pengguna memasukkan kode mereka. MFA 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 AWS Client VPN ekspor file konfigurasi titik akhir. Uji MFA konfigurasi untuk Active Directory Anda tanpa menggunakan VPN endpoint Klien untuk memverifikasi bahwa MFA berfungsi seperti yang diharapkan.

Pemecahan masalah AWS Client VPN: 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 SAML respons dari iDP.

Solusi

Pastikan setidaknya satu atribut disertakan dalam SAML respon dari IDP. Lihat SAMLsumber daya konfigurasi iDP berbasis untuk informasi selengkapnya.

Pemecahan masalah AWS Client VPN: Klien tidak dapat terhubung — otentikasi timbal balik

Masalah

Saya menggunakan otentikasi timbal balik untuk titik VPN akhir Klien saya. Klien mendapatkan kesalahan gagal negosiasi TLS kunci dan kesalahan batas waktu.

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 AWS Client VPN ekspor file konfigurasi titik akhir.

Pemecahan masalah AWS Client VPN: Klien mengembalikan kredensi melebihi kesalahan ukuran maksimal di Klien - otentikasi federasi VPN

Masalah

Saya menggunakan otentikasi federasi untuk titik akhir Klien VPN saya. Ketika klien memasukkan nama pengguna dan kata sandi mereka di jendela browser penyedia identitas SAML berbasis (iDP), mereka mendapatkan kesalahan bahwa kredensialnya melebihi ukuran maksimum yang didukung.

Penyebab

SAMLRespons yang dikembalikan oleh iDP melebihi ukuran maksimum yang didukung. Untuk informasi selengkapnya, lihat Persyaratan dan pertimbangan untuk otentikasi federasi SAML berbasis.

Solusi

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

Pemecahan masalah AWS Client VPN: Klien tidak membuka browser untuk titik akhir — otentikasi federasi

Masalah

Saya menggunakan otentikasi federasi untuk titik akhir Klien 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.

Pemecahan masalah AWS Client VPN: Klien tidak mengembalikan kesalahan port yang tersedia - otentikasi federasi

Masalah

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

Solusi

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

Pemecahan masalah AWS Client VPN: Koneksi dihentikan karena ketidakcocokan IP

Masalah

VPNkoneksi 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 mensyaratkan bahwa alamat IP yang terhubung untuk cocok dengan IP VPN server yang mendukung titik VPN akhir Klien. Untuk informasi selengkapnya, lihat Aturan dan praktik terbaik untuk menggunakan AWS Client VPN.

Solusi

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

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

Solusi

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

Pemecahan masalah AWS Client VPN: Verifikasi batas bandwidth untuk titik akhir Klien VPN

Masalah

Saya perlu memverifikasi batas bandwidth untuk VPN titik akhir Klien.

Penyebab

Throughput tergantung pada beberapa faktor, seperti kapasitas koneksi Anda dari lokasi Anda, dan latensi jaringan antara aplikasi VPN desktop Klien di komputer Anda dan titik akhirVPC. 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 VPN Pengguna Klien

Tabel berikut menjelaskan pembaruan Panduan AWS Client VPN Administrator.

Perubahan	Deskripsi	Tanggal
Contoh aturan otorisasi	Penambahan contoh skenario untuk aturan otorisasi.	15 September 2022
VPNdurasi maksimum sesi	Anda dapat mengonfigurasi durasi VPN sesi maksimum yang lebih pendek untuk memenuhi persyaratan keamanan dan kepatuhan.	20 Januari 2022
Spanduk login klien	Anda dapat mengaktifkan spanduk teks pada aplikasi VPN desktop Klien yang AWS disediakan saat VPN sesi dibuat untuk memenuhi kebutuhan peraturan dan kepatuhan.	20 Januari 2022
Client connect handler	Anda dapat mengaktifkan pengendali koneksi klien untuk VPN titik akhir Klien Anda untuk menjalankan logika kustom yang mengotorisasi koneksi baru.	4 November 2020
Portal swalayan	Anda dapat mengaktifkan portal swalayan di VPN titik akhir Klien Anda untuk klien Anda.	29 Oktober 2020
lient-to-client Akses C	Anda dapat mengaktifkan klien yang terhubung ke VPN titik	29 September 2020

	akhir Klien untuk terhubung satu sama lain.	
SAMLOtentikasi federasi berbasis 2.0	Anda dapat mengauten tikasi VPN pengguna Klien menggunakan otentikasi federasi SAML berbasis 2.0.	19 Mei 2020
Tentukan grup keamanan selama pembuatan	Anda dapat menentukan grup keamanan VPC dan keamanan saat membuat AWS Client VPN titik akhir.	5 Maret 2020
Port yang dapat dikonfigurasi VPN	Anda dapat menentuka n nomor VPN port yang didukung untuk AWS Client VPN titik akhir Anda.	16 Januari 2020
Support untuk otentikasi multi-faktor () MFA	AWS Client VPN Endpoint Anda mendukung MFA jika diaktifkan untuk Active Directory Anda.	30 September 2019
Support untuk split-tunnel	Anda dapat mengaktifkan split-tunnel di endpoint Anda AWS Client VPN .	24 Juli 2019
Rilis awal	Rilis 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.