관리자 안내서

AWS Client VPN

AWS Client VPN: 관리자 안내서

Table of Contents

AWS Client VPN란 무엇인가요?

AWS Client VPN 는 온프레미스 네트워크의 AWS 리소스와 리소스에 안전하게 액세스할 수 있는 관리형 클라이언트 기반 VPN 서비스입니다. Client VPN에서는 OpenVPN 기반 VPN 클라이언트를 사용하여 어떤 위치에서든 리소스에 액세스할 수 있습니다.

주제

Client VPN의 기능

Client VPN은 다음과 같은 기능을 제공합니다.

- 보안 연결 - OpenVPN 클라이언트를 통해 모든 위치에서 암호화된 TLS 연결을 설정하여 데이터 프라이버시와 무결성을 보장합니다.
- 관리형 서비스 - 완전한 AWS 관리를 통해 타사 원격 액세스 VPN 솔루션을 배포하고 유지 관리하는 운영 부담을 제거합니다.
- 고가용성 및 탄력성 - 동적으로 확장되어 수동 개입 없이도 AWS 및 온프레미스 리소스에 연결하는 다양한 수의 사용자를 수용합니다.
- 인증 - 유연한 자격 증명 관리를 위해 Active Directory 통합, 페더레이션 인증 및 인증서 기반 인증을 비롯한 여러 인증 방법을 지원합니다.
- 세분화된 제어 - Active Directory 그룹 수준에서 구성 가능한 네트워크 기반 액세스 규칙과 보안 그룹 기반 액세스 제어를 통해 정확한 보안 제어를 구현합니다.
- 사용 편의성 - 단일 VPN 터널을 통해 AWS 및 온프레미스 리소스 모두에 대한 통합 액세스를 제공하여 최종 사용자 경험을 간소화합니다.
- 관리 용이성 - 필요한 경우 활성 클라이언트 연결을 모니터링하고 종료하는 기능을 포함하여 세부 연결 로그 및 실시간 관리 기능을 통해 포괄적인 가시성을 제공합니다.
- 심층 통합 - AWS Directory Service 및 Amazon VPC를 포함한 기존 AWS 서비스와 원활하게 통합되어 클라우드 인프라의 연결 기능을 개선합니다.

- 유연한 네트워크 아키텍처 - VPC 서브넷 연결과 직접 Transit Gateway 연결을 모두 지원합니다. 자세한 내용은 Client VPN과 Transit Gateway 통합 단원을 참조하십시오.
- IPv6 지원 - Client VPN 엔드포인트에 대한 전체 IPv6 연결을 활성화하여 최신 네트워킹 요구 사항을 위해 VPC의 IPv6 리소스 및 IPv6 네트워크의 클라이언트에 대한 연결을 지원합니다.

Client VPN의 구성 요소

다음은 Client VPN의 핵심 개념입니다.

Client VPN 엔드포인트

Client VPN 엔드포인트는 Client VPN 세션을 활성화하고 관리하기 위해 생성하고 구성하는 리소스입니다. 이는 모든 Client VPN 세션의 종료 지점입니다.

대상 네트워크

대상 네트워크는 Client VPN 엔드포인트와 연결하는 네트워크입니다. VPC 서브넷을 연결하거나 AWS Transit Gateway에 직접 연결할 수 있습니다. Transit Gateway 통합에 대한 자세한 내용은 섹션을 참조하세요Client VPN과 Transit Gateway 통합.

라우팅

각 Client VPN 엔드포인트에는 사용 가능한 대상 네트워크 라우팅을 설명하는 라우팅 테이블이 있습니다. 라우팅 테이블의 각 라우팅은 특정 리소스 또는 네트워크에 대한 트래픽 경로를 지정합니다.

권한 부여 규칙

권한 부여 규칙은 네트워크에 액세스할 수 있는 사용자를 제한합니다. 지정된 네트워크의 경우 액세스가 허용되는 Active Directory 또는 자격 증명 공급자(IdP) 그룹을 구성합니다. 이 그룹에 속한 사용자만 지정된 네트워크에 액세스할 수 있습니다. 기본적으로 권한 부여 규칙이 없으므로 클라이언트가 리소스 및 네트워크에 액세스하도록 허용하는 권한 부여 규칙을 구성해야 합니다.

클라이언트

VPN 세션을 설정하기 위해 Client VPN 엔드포인트에 연결하는 최종 사용자입니다. 최종 사용자는 OpenVPN 클라이언트를 다운로드하고 사용자가 생성한 Client VPN 구성 파일을 사용하여 VPN 세션을 설정해야 합니다.

클라이언트 CIDR 범위

클라이언트 IP 주소를 할당할 IP 주소 범위입니다. Client VPN 엔드포인트에 대한 각 연결에는 클라이언트 CIDR 범위의 고유한 IP 주소가 할당됩니다. IPv4 트래픽의 경우 클라이언트 CIDR 범위(예:

10.2.0.0/16)를 선택합니다. IPv6 트래픽의 경우는 클라이언트 CIDR 범위를 AWS Client VPN 자동으로 할당합니다.

Client VPN 포트

AWS Client VPN 는 TCP 및 UDP 모두에 대해 포트 443 및 1194를 지원합니다. 기본값은 포트 443 입니다.

Client VPN 네트워크 인터페이스

서브넷을 Client VPN 엔드포인트와 연결하면 해당 서브넷에 Client VPN 네트워크 인터페이스가 생성됩니다. Client VPN 엔드포인트에서 VPC로 전송된 트래픽은 Client VPN 네트워크 인터페이스를 통해 전송됩니다. IPv4 트래픽의 경우, 소스 네트워크 주소 변환(SNAT)이 적용됩니다. 여기서 클라이언트 CIDR 범위의 소스 IP 주소는 Client VPN 네트워크 인터페이스 IP 주소로 변환됩니다. IPv6 트래픽의 경우 SNAT가 적용되지 않으므로 연결된 사용자의 IP 주소에 대한 가시성이 향상됩니다.

연결 로깅

Client VPN 엔드포인트에 대한 연결 로깅을 활성화하여 연결 이벤트를 로깅할 수 있습니다. 이 정보를 사용하여 포렌식을 실행하거나, Client VPN 엔드포인트가 어떻게 사용되고 있는지 분석하거나, 연결 문제를 디버깅할 수 있습니다.

셀프 서비스 포털

Client VPN은 엔드포인트에 연결하는 데 필요한 설정이 포함된 최신 버전의 AWS VPN Desktop Client 및 최신 버전의 Client VPN 엔드포인트 구성 파일을 최종 사용자가 다운로드할 수 있는 셀프 서비스 포털 웹 페이지를 제공합니다. Client VPN 엔드포인트 관리자는 Client VPN 엔드포인트에 대한 셀프 서비스 포털을 활성화하거나 비활성화할 수 있습니다. 셀프 서비스 포털은 미국 동부(버지니아 북부), 아시아 태평양(도쿄), 유럽(아일랜드), AWS GovCloud(미국 서부) 리전의 서비스 스택이 지원하는 글로벌 서비스입니다.

엔드포인트 IP 주소 유형

Client VPN 엔드포인트의 IP 주소 유형이며 IPv4, IPv6 또는 듀얼 스택(IPv4 및 IPv6 모두)일 수 있습니다.

트래픽 IP 주소 유형

Client VPN 엔드포인트를 통해 흐르는 트래픽의 IP 주소 유형이며 IPv4, IPv6 또는 듀얼 스택(IPv4 및 IPv6 모두)일 수 있습니다. 이는 엔드포인트당 내부 트래픽 유형(VPN 연결을 통해 터널링되는 실제 페이로드 또는 원래 트래픽), 클라이언트 CIDR 범위, 서브넷 연결, 라우팅 및 규칙을 결정합니다.

Client VPN 작업

다음 방법 중 하나를 사용하여 Client VPN으로 작업할 수 있습니다.

AWS Management Console

이 콘솔은 Client VPN을 위한 웹 기반 사용자 인터페이스를 제공합니다.

콘솔은 두 가지 설정 방법을 사용하여 Client VPN용 웹 기반 사용자 인터페이스를 제공합니다.

- 빠른 시작 설정: AWS 권장 기본값을 사용하여 엔드포인트 생성 간소화
- 표준 설정: 모든 구성 옵션에 대한 전체 제어

에 가입한 경우 Amazon VPC 콘솔에 로그인하고 탐색 창에서 Client VPN을 선택할 AWS 계정수 있습니다.

AWS Command Line Interface (AWS CLI)

는 Client VPN 퍼블릭 APIs에 대한 직접 액세스를 AWS CLI 제공합니다. 이는 Windows, macOS, Linux에서 지원됩니다. 시작하기에 대한 자세한 내용은 AWS Command Line Interface 사용 설명서를 AWS CLI참조하세요. Client VPN용 명령어에 대한 자세한 내용은 Amazon EC2 명령줄 참조의 EC2 섹션을 참조하세요.

AWS Tools for Windows PowerShell

AWS 는 PowerShell 환경에서 스크립트를 작성하는 사용자를 위해 다양한 AWS 제품에 대한 명령을 제공합니다. AWS Tools for Windows PowerShell시작하기에 대한 자세한 내용은 AWS Tools for Windows PowerShell 사용 설명서를 참조하세요. Client VPN용 cmdlet에 대한 자세한 내용은 AWS Tools for Windows PowerShell Cmdlet 참조를 참조하세요.

Query API

Client VPN HTTPS 쿼리 API를 사용하면 Client VPN 및에 프로그래밍 방식으로 액세스할 수 있습니다 AWS. HTTPS 쿼리 API를 이용하면 HTTPS 요청을 서비스에 바로 보낼 수 있습니다. HTTPS API를 사용할 때는 자격 증명을 사용하여 요청에 디지털 방식으로 서명하는 코드를 포함해야 합니다. 자세한 내용은 AWS Client VPN 작업을 참조하세요.

Client VPN의 요금

각 엔드포인트 연결 및 각 VPN 연결에 대해 시간당 요금이 부과됩니다. IPv6 또는 듀얼 스택 엔드포인트를 사용하는 데 드는 추가 비용은 없으며 IPv4 엔드포인트와 동일한 요금이 부과됩니다. 자세한 내용은 AWS Client VPN 요금을 참조하세요.

Amazon EC2에서 인터넷으로 전송되는 데이터 전송에 대한 요금이 부과됩니다. 자세한 내용은 Amazon EC2 온디맨드 요금 페이지에서 데이터 전송을 참조하세요.

Client VPN 엔드포인트에 대한 연결 로깅을 활성화하는 경우 계정에서 CloudWatch Logs 로그 그룹을 생성해야 합니다. 로그 그룹 이용 시 요금이 부과됩니다. 자세한 내용은 Amazon CloudWatch 요금(유료 티어 아래에서 로그 선택)을 참조하세요.

Client VPN 엔드포인트에 대해 클라이언트 연결 핸들러를 활성화하는 경우 Lambda 함수를 생성하고 호출해야 합니다. Lambda 함수 호출에는 요금이 적용됩니다. 자세한 내용은 AWS Lambda 요금을 참조하십시오.

Client VPN 엔드포인트는 VPC의 서브넷인 대상 네트워크와 연결됩니다. 이 VPC에 인터넷 게이트웨이가 있는 경우 탄력적 IP 주소를 Client VPN 탄력적 네트워크 인터페이스(ENI)와 연결합니다. 이러한 탄력적 IP 주소는 사용 중인 퍼블릭 IPv4 주소로 청구됩니다. 자세한 내용은 VPC 요금 페이지의 퍼블릭 IPv4 주소 탭을 참조하세요.

> **Note**
>
> Client VPN 엔드포인트는 인터넷 게이트웨이가 있는 VPC 서브넷과 연결할 때 탄력적 IP 주소가 필요합니다. 이러한 EIP는 VPN 클라이언트에 대한 직접 인터넷 연결을 활성화하기 때문입니다. Client VPN 엔드포인트를 통해 연결할 때 인터넷 리소스와 통신하려면 퍼블릭 IP 주소가 필요합니다. 탄력적 IP는 일관된 퍼블릭 엔드포인트를 제공하여 이러한 목적을 수행합니다. 이러한 EIP는 Client VPN 탄력적 네트워크 인터페이스(ENI)에 연결되며 트래픽의 적절한 라우팅을 보장하면서 VPN 클라이언트에 대한 안정적이고 안전한 인터넷 액세스를 유지하는 데 필수적입니다. 이러한 탄력적 IP 주소는 Client VPN 서비스에 할당되고 적극적으로 사용되므로는 할당된 EIP 및 연결된 EIP에 대한 표준 요금 모델에 따라 사용 중인 퍼블릭 IPv4 주소로 요금을 AWS 부과합니다. EIPs

사용에 대한 규칙 및 모범 사례 AWS Client VPN

다음 섹션에서는 AWS Client VPN사용에 대한 규칙과 모범 사례를 설명합니다.

주제

- 네트워킹 및 대역폭 요구 사항
- 서브넷 및 VPC 구성
- 보안 및 인증

- 연결 및 DNS 요구 사항
- 한계 및 제한

네트워킹 및 대역폭 요구 사항

- AWS Client VPN 는 추가 사용자 연결 및 대역폭 요구 사항을 수용하도록 자동으로 확장되는 완전 관리형 서비스입니다. 각 사용자 연결의 최대 기준 대역폭은 50Mbps입니다.

  Client VPN 엔드포인트를 통해 연결하는 실제 대역폭은 여러 요인에 따라 다를 수 있습니다. 이러한 요인에는 패킷 크기, 트래픽 구성(TCP/UDP 혼합), 중간 네트워크의 네트워크 정책(셰이핑 또는 스로틀링), 인터넷 조건, 애플리케이션별 요구 사항, 총 동시 사용자 연결 수가 포함됩니다. 최대 대역폭 한도에 도달하는 경우 AWS Support를 통해 상향을 요청할 수 있습니다.
- 클라이언트 CIDR 범위는 연결된 서브넷이 위치하는 VPC의 로컬 CIDR 또는 Client VPN 엔드포인트의 라우팅 테이블에 수동으로 추가된 라우팅과 중첩될 수 없습니다.
- 클라이언트 CIDR 범위는 블록 크기가 최소 /22여야 하며 /12를 초과할 수 없습니다.
- 클라이언트 CIDR 범위의 주소 중 일부는 Client VPN 엔드포인트의 가용성 모델을 지원하는 데 사용되며 클라이언트에 할당할 수 없습니다. 따라서 Client VPN 엔드포인트에서 지원할 최대 동시 연결 수를 활성화하는 데 필요한 IP 주소 수의 두 배가 포함된 CIDR 블록을 할당하는 것이 좋습니다.
- Client VPN 엔드포인트를 생성한 후에는 클라이언트 CIDR 범위를 변경할 수 없습니다.
- Client VPN은 IPv4, IPv6 및 듀얼 스택(IPv4 및 IPv6 모두) 트래픽을 지원합니다. IPv6 지원에 대한 자세한 내용은 AWS Client VPN에 대한 IPv6 고려 사항 섹션을 참조하세요.
- • 소스 IP 주소는 Client VPN 엔드포인트의 IP 주소로 변환됩니다.
  - 클라이언트의 원래 소스 포트 번호는 변경되지 않습니다.
- Client VPN은 동시 사용자가 동일한 대상에 연결하는 경우에만 포트 주소 변환(PAT)을 수행합니다. 포트 변환은 자동이며 동일한 VPN 엔드포인트를 통해 여러 동시 연결을 지원하는 데 필요합니다.
  - 소스 IP 변환의 경우 소스 IP 주소가 Client VPN의 IP 주소로 변환됩니다.
  - 단일 클라이언트 연결에 대한 소스 포트 변환의 경우 원래 소스 포트 번호는 변경되지 않을 수 있습니다.
  - 동일한 대상(동일한 대상 IP 주소 및 포트)에 연결하는 여러 클라이언트의 소스 포트 변환의 경우 Client VPN은 포트 변환을 수행하여 고유한 연결을 보장합니다.

  예를 들어 클라이언트 1과 클라이언트 2라는 두 클라이언트가 동일한 대상 서버에 연결하고 Client VPN 엔드포인트를 통해 포트를 연결합니다.
  - 클라이언트 1의 원래 포트(예: 9999)는 다른 포트(예: 포트 4306)로 변환될 수 있습니다.

  - 클라이언트 2의 원래 포트(예: 9999)는 클라이언트 1과 다른 고유 포트(예: 포트 63922)로 변환될 수 있습니다.
- IPv6 트래픽의 경우 Client VPN은 네트워크 주소 변환(NAT)을 수행하지 않습니다. 이렇게 하면 연결된 사용자의 IPv6 주소에 대한 가시성이 향상됩니다.

서브넷 및 VPC 구성

- Client VPN 엔드포인트와 연결된 서브넷은 동일한 VPC에 있어야 합니다.
- 동일한 가용 영역의 여러 서브넷을 한 Client VPN 엔드포인트와 연결할 수 없습니다.
- Client VPN 엔드포인트는 전용 테넌시 VPC에서 서브넷 연결을 지원하지 않습니다.
- IPv6 또는 듀얼 스택 트래픽의 경우 연결된 서브넷에 IPv6 또는 듀얼 스택 CIDR 범위가 있어야 합니다.
- 듀얼 스택 엔드포인트의 경우 가용 영역당 서브넷을 두 개 이상 연결할 수 없습니다.

보안 및 인증

- 상호 인증을 사용하여 인증하는 클라이언트에는 셀프 서비스 포털을 사용할 수 없습니다.
- Active Directory에 대해 다중 인증(MFA)이 비활성화된 경우 사용자 암호에 다음과 같은 형식을 사용할 수 없습니다.

```
SCRV1:base64_encoded_string:base64_encoded_string
```

- AWS Client VPN에 사용되는 인증서는 메모의 섹션 4.2에 지정된 인증서 확장을 포함하여 RFC 5280: Internet X.509 퍼블릭 키 인프라 인증서 및 인증서 해지 목록(CRL) 프로필을 준수해야 합니다.
- 특수 문자가 있는 사용자 이름은 연결 오류를 일으킬 수 있습니다.
- 최대 사용자 이름 길이는 1024바이트입니다. 사용자 이름이 더 긴 연결은 거부됩니다.

연결 및 DNS 요구 사항

- IP 주소를 사용하여 Client VPN 엔드포인트에 연결하지 않는 것이 좋습니다. Client VPN은 관리형 서비스이므로 때때로 DNS 이름이 확인되는 IP 주소의 변경 사항을 볼 수 있습니다. 또한 CloudTrail 로그에서 Client VPN 네트워크 인터페이스가 삭제되고 다시 생성된 것을 볼 수 있습니다. 제공된 DNS 이름을 사용하여 Client VPN 엔드포인트에 연결하는 것이 좋습니다.

- Client VPN 서비스를 사용하려면 클라이언트가 연결된 IP 주소가 Client VPN 엔드포인트의 DNS 이름이 확인된 IP와 일치해야 합니다. 즉, Client VPN 엔드포인트에 대한 사용자 지정 DNS 레코드를 설정한 다음 엔드포인트의 DNS 이름이 확인되는 실제 IP 주소로 트래픽을 전달하는 경우이 설정은 최근에 AWS 제공된 클라이언트를 사용할 수 없습니다. 이 규칙은 TunnelCrack에 설명된 대로 서버 IP 공격을 완화하기 위해 추가되었습니다.
- AWS 제공된 클라이언트를 사용하여 여러 동시 DNS 세션에 연결할 수 있습니다. 그러나 이름 확인이 올바르게 작동하려면 모든 연결의 DNS 서버에 동기화된 레코드가 있어야 합니다.
- Client VPN 서비스를 사용하려면 클라이언트 디바이스의 LAN(Local Area Network) IP 주소 범위가 `10.0.0.0/8`, `172.16.0.0/12`, `192.168.0.0/16` 또는 `169.254.0.0/16`의 표준 프라이빗 IP 주소 범위 내에 있어야 합니다. 클라이언트 LAN 주소 범위가 위의 범위를 벗어나는 것으로 감지되면 Client VPN 엔드포인트는 OpenVPN 명령 "redirect-gateway block-local"을 클라이언트에 자동으로 푸시하여 모든 LAN 트래픽을 VPN으로 강제로 보냅니다. 따라서 VPN 연결 중에 LAN 액세스가 필요한 경우 위에 나열된 기존 주소 범위를 LAN에 사용하는 것이 좋습니다. 이 규칙은 TunnelCrack에 설명된 대로 로컬 네트워크 공격 가능성을 완화하기 위해 적용됩니다.
- Windows에서 전체 터널 엔드포인트를 사용하는 경우 엔드포인트의 IP 주소 유형(IPv4 IPv6 또는 듀얼 스택)에 관계없이 모든 DNS 트래픽이 터널을 통해 강제 적용됩니다. DNS가 작동하려면 DNS 서버를 설정하고 터널 내에서 연결할 수 있어야 합니다.

한계 및 제한

- AWS Client VPN 데스크톱 애플리케이션을 사용할 때는 현재 IP 전달이 지원되지 않습니다. IP 전달은 다른 클라이언트에서 지원됩니다.
- Client VPN은 AWS Managed Microsoft AD에서 다중 리전 복제를 지원하지 않습니다. Client VPN 엔드포인트는 AWS Managed Microsoft AD 리소스와 동일한 리전에 있어야 합니다.
- 운영 체제에 로그인한 사용자가 여러 명인 경우 컴퓨터에서 VPN 연결을 설정할 수 없습니다.
- IPv6 클라이언트에는 클라이언트 간 통신이 지원되지 않습니다. IPv6 클라이언트가 다른 IPv6 클라이언트와 통신을 시도하면 트래픽이 삭제됩니다.
- IPv6 및 듀얼 스택 엔드포인트를 사용하려면 사용자 디바이스 및 인터넷 서비스 제공업체(ISP)가 해당 IP 구성을 지원해야 합니다.

AWS Client VPN 작동 방식

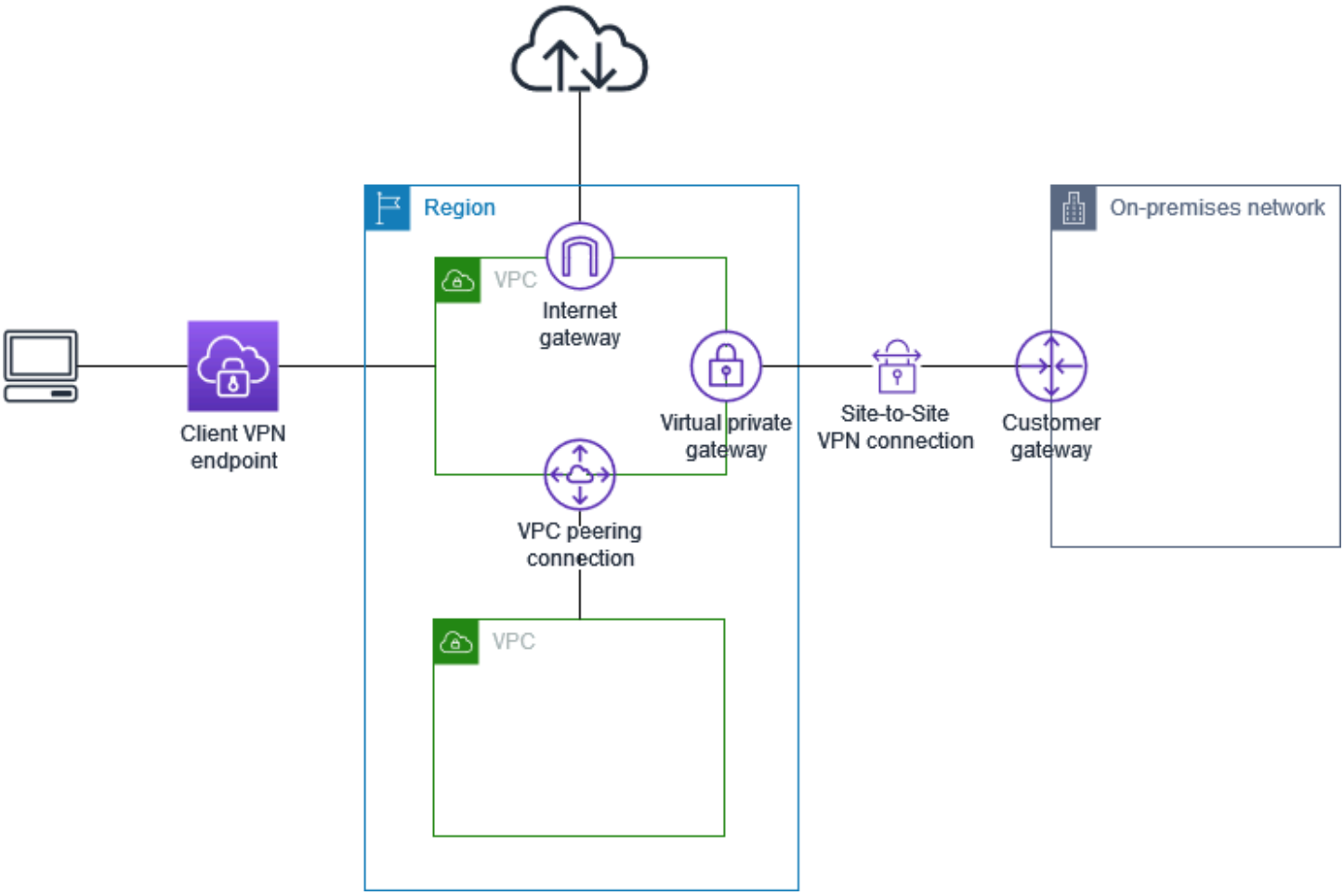
AWS Client VPN에는 Client VPN 엔드포인트와 상호 작용하는 두 가지 유형의 사용자 페르소나가 있습니다. 이 두 가지는 관리자와 클라이언트입니다.

Client VPN은 IPv4, IPv6 및 듀얼 스택(IPv4 및 IPv6 모두) 연결을 지원합니다. IPv4, IPv6 또는 둘 다를 사용하는 엔드포인트를 생성하여 VPC의 IPv6 리소스에 연결하거나 IPv6 네트워크의 클라이언트에서 연결할 수 있습니다. 이러한 유연성은 IPv6 인프라를 이미 구현했거나 IPv6 인프라로 전환하는 조직에 도움이 됩니다.

관리자는 서비스 설정 및 구성을 담당합니다. 여기에는 Client VPN 엔드포인트 생성, 대상 네트워크 연결, 권한 부여 규칙 구성, 추가 라우팅 설정(필요한 경우)이 포함됩니다. Client VPN 엔드포인트를 설정하고 구성한 후, 관리자는 Client VPN 엔드포인트 구성 파일을 다운로드하여 액세스가 필요한 클라이언트에 배포합니다. Client VPN 엔드포인트 구성 파일에는 VPN 세션을 설정하는 데 필요한 Client VPN 엔드포인트 및 인증 정보의 DNS 이름이 포함되어 있습니다. 서비스 설정에 대한 자세한 내용은 시작하기 AWS Client VPN 단원을 참조하십시오.

클라이언트가 최종 사용자입니다. 이 사용자는 Client VPN 엔드포인트에 연결하여 VPN 세션을 설정하는 사람입니다. 클라이언트는 로컬 컴퓨터 또는 모바일 디바이스에서 OpenVPN 기반 VPN 클라이언트 애플리케이션을 사용하여 VPN 세션을 설정합니다. VPN 세션이 설정되면 연결된 서브넷이 위치하는 VPC 안의 리소스에 안전하게 액세스할 수 있습니다. 필요한 경로 및 권한 부여 규칙이 구성된 경우, AWS의 다른 리소스, 온프레미스 네트워크 또는 다른 클라이언트에도 액세스할 수 있습니다. Client VPN 엔드포인트에 연결하여 VPN 세션을 설정하는 방법에 대한 자세한 내용은 AWS Client VPN 사용 설명서의 시작하기를 참조하세요.

다음 그래픽은 기본 Client VPN 아키텍처를 보여 줍니다.



Client VPN의 시나리오 및 예제

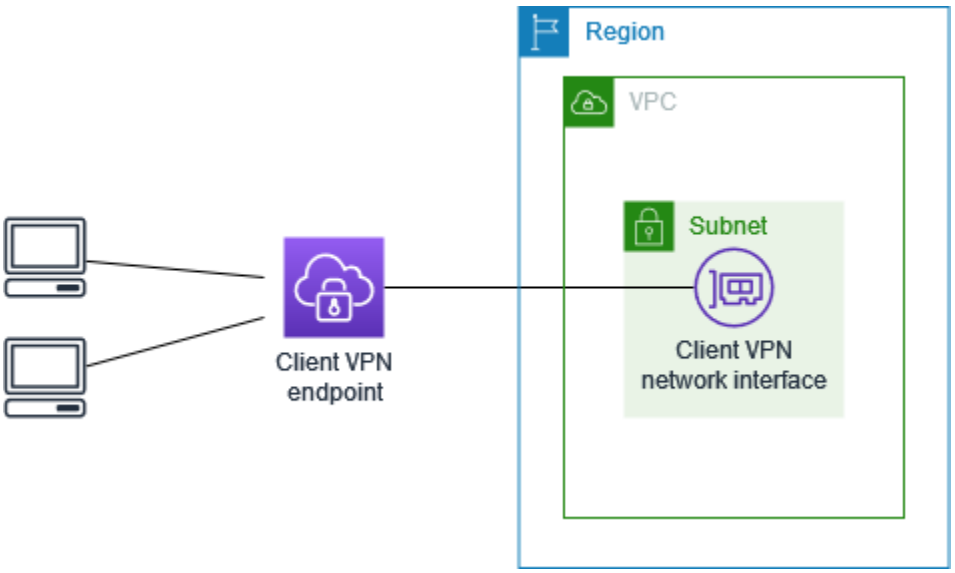
AWS Client VPN은 클라이언트가 AWS 및 온프레미스 네트워크 내 리소스에 안전하게 액세스할 수 있도록 하는 데 사용하는 완전 관리형 원격 액세스 VPN 솔루션입니다. 액세스를 구성하는 방법에는 여러 옵션이 있습니다. 이 단원에서는 클라이언트에 대한 Client VPN 액세스 권한을 생성하고 구성하는 예를 제공합니다.

시나리오

- the section called “VPC 액세스”
- the section called “피어링된 VPC 액세스”
- the section called “온프레미스 네트워크 액세스”
- the section called “인터넷 액세스”
- the section called “클라이언트 간 액세스”
- the section called “네트워크에 대한 액세스 제한”

Client VPN을 사용하여 VPC 액세스

이 시나리오의 AWS Client VPN 구성에는 단일 대상 VPC가 포함됩니다. 클라이언트에게 단일 VPC 내부의 리소스에 대한 액세스 권한만 부여하면 되는 경우 이 구성을 사용하는 것이 좋습니다.



시작하기 전에 다음을 수행하세요.

- 하나 이상의 서브넷이 있는 VPC를 생성하거나 식별합니다. VPC에서 Client VPN 엔드포인트와 연결할 서브넷을 식별하고 해당 IPv4 CIDR 범위를 기록해 둡니다.
- VPC CIDR과 겹치지 않는 클라이언트 IP 주소에 적합한 CIDR 범위를 식별합니다.
- 사용에 대한 규칙 및 모범 사례 AWS Client VPN에서 Client VPN 엔드포인트에 대한 규칙과 제한 사항을 검토합니다.

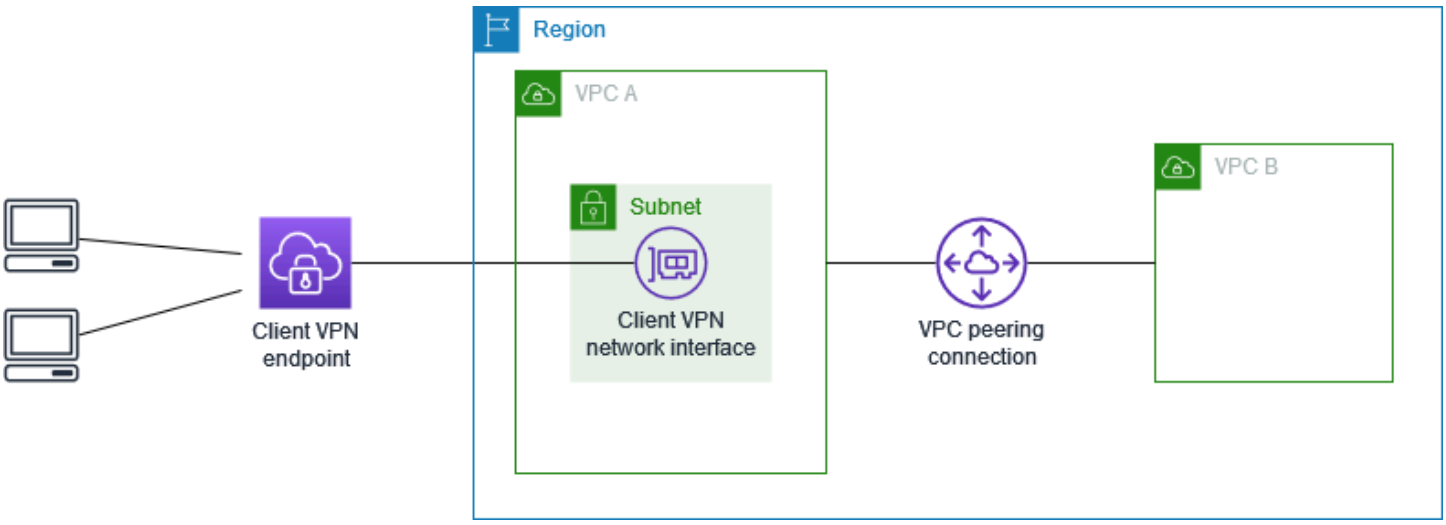
이 구성을 구현하는 방법

1. VPC와 동일한 리전에서 Client VPN 엔드포인트를 생성합니다. 이렇게 하려면 AWS Client VPN엔드포인트 생성에 설명된 단계를 수행합니다.
2. 서브넷을 Client VPN 엔드포인트와 연결합니다. 이렇게 하려면 대상 네트워크를 AWS Client VPN 엔드포인트와 연결에 설명된 단계를 수행하고 앞에서 식별한 서브넷 및 VPC를 선택합니다.
3. 권한 부여 규칙을 추가하여 클라이언트에 VPC에 대한 액세스 권한을 부여합니다. 이렇게 하려면 권한 부여 규칙 추가에 설명된 단계를 수행하고 Destination network(대상 네트워크)에 VPC의 IPv4 CIDR 범위를 입력합니다.
4. 리소스의 보안 그룹에 규칙을 추가하여 2단계에서 서브넷 연결에 적용된 보안 그룹의 트래픽을 허용합니다. 자세한 내용은 보안 그룹 섹션을 참조하세요.

Client VPN을 사용하여 피어링된 VPC 액세스

이 시나리오의 AWS Client VPN 구성에는 추가 VPC(VPC B)와 피어링되는 대상 VPC(VPC A)가 포함됩니다. 클라이언트에게 대상 VPC 및 이와 피어링된 다른 VPC(예: VPC B) 내부의 리소스에 대한 액세스 권한을 부여해야 하는 경우 이 구성을 사용하는 것이 좋습니다.

> **Note**
>
> 아래 네트워크 다이어그램에 설명된 피어링된 VPC에 대한 액세스가 가능한 절차는 Client VPN 엔드포인트가 분할 터널 모드에 대해 구성된 경우에만 필요합니다. 전체 터널 모드에서는 피어링된 VPC 대한 액세스가 기본적으로 허용됩니다.



시작하기 전에 다음을 수행하세요.

- 하나 이상의 서브넷이 있는 VPC를 생성하거나 식별합니다. VPC에서 Client VPN 엔드포인트와 연결할 서브넷을 식별하고 해당 IPv4 CIDR 범위를 기록해 둡니다.
- VPC CIDR과 겹치지 않는 클라이언트 IP 주소에 적합한 CIDR 범위를 식별합니다.
- 사용에 대한 규칙 및 모범 사례 AWS Client VPN에서 Client VPN 엔드포인트에 대한 규칙과 제한 사항을 검토합니다.

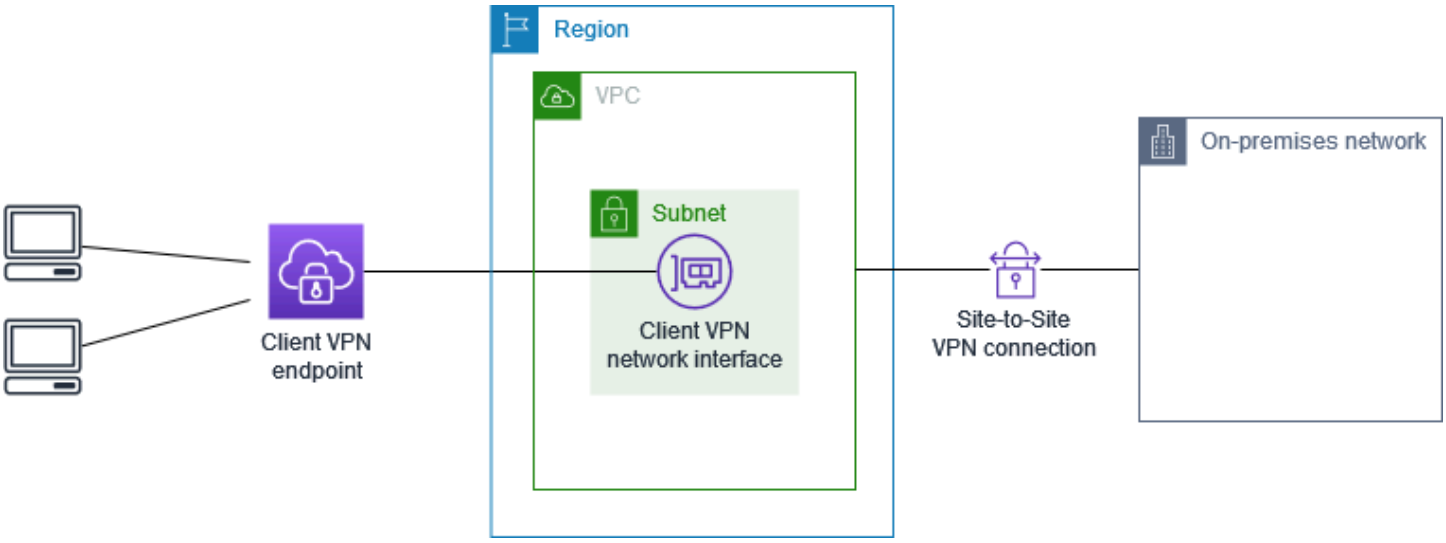
이 구성을 구현하는 방법

1. VPC 사이에 VPC 피어링 연결을 설정합니다. Amazon VPC 피어링 가이드의 VPC 피어링 연결 생성 및 수락에 있는 단계를 따릅니다. VPC A의 인스턴스에서 피어링 연결을 사용하여 VPC B의 인스턴스와 통신할 수 있는지 확인합니다.

2. 대상 VPC와 동일한 리전에서 Client VPN 엔드포인트를 생성합니다. 다이어그램에서 이것은 VPC A입니다. AWS Client VPN엔드포인트 생성에 설명된 단계를 수행합니다.
3. 식별한 서브넷을 생성한 Client VPN 엔드포인트와 연결합니다. 이렇게 하려면 대상 네트워크를 AWS Client VPN 엔드포인트와 연결에 설명된 단계를 수행하고 VPC와 서브넷을 선택합니다. 기본적으로 VPC의 기본 보안 그룹을 Client VPN 엔드포인트와 연결합니다. the section called “대상 네트워크에 보안 그룹 적용”에 설명된 단계를 사용하여 다른 보안 그룹을 연결할 수 있습니다.
4. 권한 부여 규칙을 추가하여 클라이언트에 대상 VPC에 대한 액세스 권한을 부여합니다. 이렇게 하려면 권한 부여 규칙 추가에 설명된 단계를 수행합니다. 활성화할 대상 네트워크(Destination network to enable)에 VPC의 IPv4 CIDR 범위를 입력합니다.
5. 라우팅을 추가하여 트래픽을 피어링된 VPC로 전달합니다. 다이어그램에서 이것은 VPC B입니다. 이렇게 하려면 AWS Client VPN 엔드포인트 라우팅 생성에 설명된 단계를 수행합니다. 라우팅 대상에 피어링된 VPC의 IPv4 CIDR 범위를 입력합니다. 대상 VPC 서브넷 ID에서 Client VPN 엔드포인트에 연결한 서브넷을 선택합니다.
6. 권한 부여 규칙을 추가하여 클라이언트에 피어링된 VPC에 대한 액세스 권한을 부여합니다. 이렇게 하려면 권한 부여 규칙 추가에 설명된 단계를 수행합니다. 대상 네트워크에 피어링된 VPC의 IPv4 CIDR 범위를 입력합니다.
7. VPC A 및 VPC B에 있는 인스턴스의 보안 그룹에 규칙을 추가하여 3단계에서 Client VPN 엔드포인트에 적용된 보안 그룹의 트래픽을 허용합니다. 자세한 내용은 보안 그룹 섹션을 참조하세요.

Client VPN을 사용하여 온프레미스 네트워크 액세스

이 시나리오의 AWS Client VPN 구성에는 온프레미스 네트워크에 대한 액세스만 포함됩니다. 클라이언트에게 온프레미스 네트워크 내부의 리소스에 대한 액세스 권한만 부여하면 되는 경우 이 구성을 사용하는 것이 좋습니다.



시작하기 전에 다음을 수행하세요.

- 하나 이상의 서브넷이 있는 VPC를 생성하거나 식별합니다. VPC에서 Client VPN 엔드포인트와 연결할 서브넷을 식별하고 해당 IPv4 CIDR 범위를 기록해 둡니다.
- VPC CIDR과 겹치지 않는 클라이언트 IP 주소에 적합한 CIDR 범위를 식별합니다.
- 사용에 대한 규칙 및 모범 사례 AWS Client VPN에서 Client VPN 엔드포인트에 대한 규칙과 제한 사항을 검토합니다.

이 구성을 구현하는 방법

1. AWS Site-to-Site VPN 연결을 통해 VPC와 자체 온프레미스 네트워크 간의 통신을 활성화합니다. 이렇게 하려면 AWS Site-to-Site VPN 사용 설명서의 시작하기에 설명된 단계를 수행합니다.

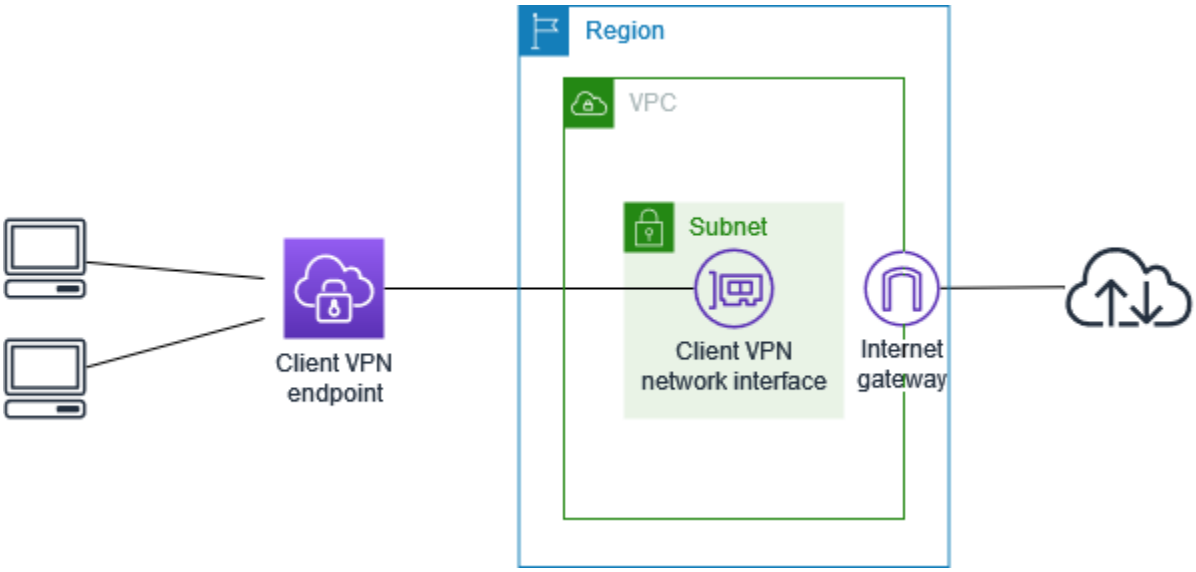
   > **Note**
   >
   > 또는 VPC와 온프레미스 네트워크 간의 Direct Connect 연결을 사용하여 이 시나리오를 구현할 수 있습니다. 자세한 내용은 Direct Connect 사용 설명서를 참조하세요.

2. 이전 단계에서 생성한 AWS Site-to-Site VPN 연결을 테스트합니다. 이렇게 하려면 AWS Site-to-Site VPN 사용 설명서의 Site-to-Site VPN 연결 테스트에 설명된 단계를 수행합니다. VPN 연결이 예상대로 작동하면 다음 단계로 이동합니다.
3. VPC와 동일한 리전에서 Client VPN 엔드포인트를 생성합니다. 이렇게 하려면 AWS Client VPN엔드포인트 생성에 설명된 단계를 수행합니다.
4. 앞에서 식별한 서브넷을 Client VPN 엔드포인트와 연결합니다. 이렇게 하려면 대상 네트워크를 AWS Client VPN 엔드포인트와 연결에 설명된 단계를 수행하고 VPC 및 서브넷을 선택합니다.
5. AWS Site-to-Site VPN 연결에 대한 액세스를 허용하는 경로를 추가합니다. 이렇게 하려면 AWS Client VPN 엔드포인트 라우팅 생성에 설명된 단계를 수행합니다. 경로 대상(Route destination)에 AWS Site-to-Site VPN 연결의 IPv4 CIDR 범위를 입력하고 대상 VPC 서브넷 ID(Target VPC Subnet ID)에서 Client VPN 엔드포인트와 연결한 서브넷을 선택합니다.
6. AWS Site-to-Site VPN 연결에 대한 액세스 권한을 클라이언트에 부여하는 권한 부여 규칙을 추가합니다. 이렇게 하려면 AWS Client VPN 엔드포인트에 권한 부여 규칙 추가에 설명된 단계를 수행하고 대상 네트워크(Destination network)에 AWS Site-to-Site VPN 연결 IPv4 CIDR 범위를 입력합니다.

Client VPN을 사용하여 인터넷 액세스

이 시나리오의 AWS Client VPN 구성에는 단일 대상 VPC와 인터넷 액세스가 포함됩니다. 클라이언트에게 단일 대상 VPC 내부의 리소스에 대한 액세스 권한을 부여하고 인터넷 액세스를 허용해야 하는 경우 이 구성을 사용하는 것이 좋습니다.

시작하기 AWS Client VPN 자습서를 완료한 경우 이 시나리오를 이미 구현한 것입니다.



시작하기 전에 다음을 수행하세요.

- 하나 이상의 서브넷이 있는 VPC를 생성하거나 식별합니다. VPC에서 Client VPN 엔드포인트와 연결할 서브넷을 식별하고 해당 IPv4 CIDR 범위를 기록해 둡니다.
- VPC CIDR과 겹치지 않는 클라이언트 IP 주소에 적합한 CIDR 범위를 식별합니다.
- 사용에 대한 규칙 및 모범 사례 AWS Client VPN에서 Client VPN 엔드포인트에 대한 규칙과 제한 사항을 검토합니다.

이 구성을 구현하는 방법

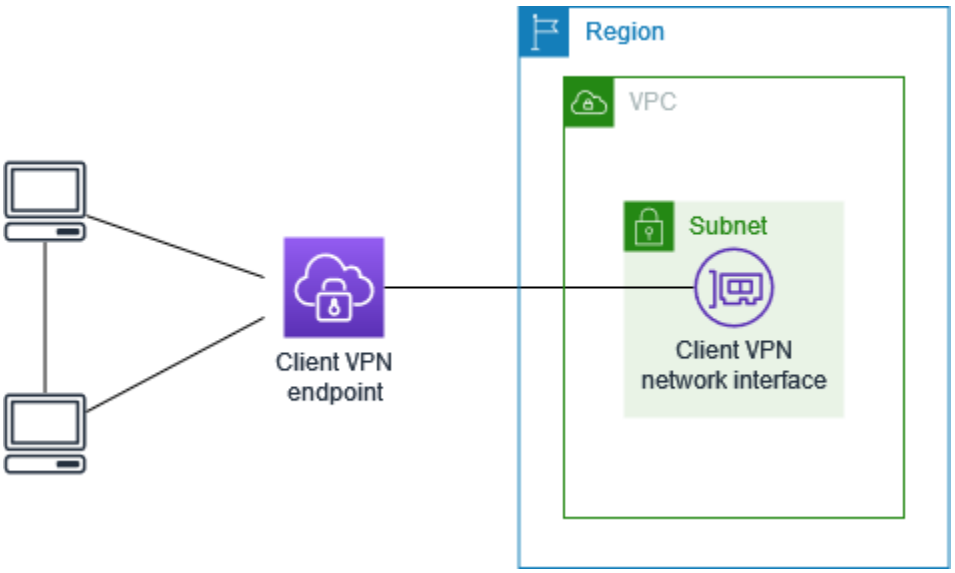
1. Client VPN 엔드포인트에 사용할 보안 그룹이 인터넷으로의 아웃바운드 트래픽을 허용하는지 확인합니다. 이렇게 하려면 HTTP 및 HTTPS 트래픽에 대해 0.0.0.0/0으로의 트래픽을 허용하는 아웃바운드 규칙을 추가합니다.
2. 인터넷 게이트웨이를 생성하여 VPC에 연결합니다. 자세한 내용은 Amazon VPC 사용 설명서의 인터넷 게이트웨이 생성 및 연결을 참조하세요.
3. 서브넷 라우팅 테이블에 인터넷 게이트웨이에 대한 라우팅을 추가하여 서브넷을 퍼블릭으로 만듭니다. VPC 콘솔에서 서브넷을 선택하고, Client VPN 엔드포인트에 연결할 서브넷을 선택한 다음,

라우팅 테이블을 선택하고, 라우팅 테이블 ID를 선택합니다. 작업을 선택하고, Edit routes(라우팅 편집)을 선택하고, Add route(라우팅 추가)를 선택합니다. 대상 주소에 `0.0.0.0/0`을 입력하고, 대상에서 이전 단계의 인터넷 게이트웨이를 선택합니다.

4. VPC와 동일한 리전에서 Client VPN 엔드포인트를 생성합니다. 이렇게 하려면 AWS Client VPN엔드포인트 생성에 설명된 단계를 수행합니다.
5. 앞에서 식별한 서브넷을 Client VPN 엔드포인트와 연결합니다. 이렇게 하려면 대상 네트워크를 AWS Client VPN 엔드포인트와 연결에 설명된 단계를 수행하고 VPC 및 서브넷을 선택합니다.
6. 권한 부여 규칙을 추가하여 클라이언트에 VPC에 대한 액세스 권한을 부여합니다. 이렇게 하려면 권한 부여 규칙 추가에 설명된 단계를 수행하고 Destination network to enable(활성화할 대상 네트워크)에 VPC의 IPv4 CIDR 범위를 입력합니다.
7. 인터넷 트래픽을 허용하는 라우팅을 추가합니다. 이렇게 하려면 AWS Client VPN 엔드포인트 라우팅 생성에 설명된 단계를 수행합니다. Route destination(라우팅 대상)에 `0.0.0.0/0`을 입력하고 Target VPC Subnet ID(대상 VPC 서브넷 ID)에서 Client VPN 엔드포인트에 연결한 서브넷을 선택합니다.
8. 권한 부여 규칙을 추가하여 클라이언트에 인터넷에 대한 액세스 권한을 부여합니다. 이렇게 하려면 권한 부여 규칙 추가에 설명된 단계를 수행하고 Destination network(대상 네트워크)에 `0.0.0.0/0`을 입력합니다.
9. VPC의 리소스에 대한 보안 그룹에 Client VPN 엔드포인트와 연결된 보안 그룹에서의 액세스를 허용하는 규칙이 있는지 확인합니다. 이렇게 하면 클라이언트가 VPC의 리소스에 액세스할 수 있습니다.

Client VPN을 사용한 클라이언트 간 액세스

이 시나리오의 AWS Client VPN 구성을 통해 클라이언트가 단일 VPC에 액세스할 수 있고 클라이언트가 서로 트래픽을 라우팅할 수 있습니다. 동일한 Client VPN 엔드포인트에 연결하는 클라이언트도 서로 통신해야 하는 경우 이 구성을 사용하는 것이 좋습니다. 클라이언트는 Client VPN 엔드포인트에 연결할 때 클라이언트 CIDR 범위에서 할당된 고유한 IP 주소를 사용하여 서로 통신할 수 있습니다.



시작하기 전에 다음을 수행하세요.

- 하나 이상의 서브넷이 있는 VPC를 생성하거나 식별합니다. VPC에서 Client VPN 엔드포인트와 연결할 서브넷을 식별하고 해당 IPv4 CIDR 범위를 기록해 둡니다.
- VPC CIDR과 겹치지 않는 클라이언트 IP 주소에 적합한 CIDR 범위를 식별합니다.
- 사용에 대한 규칙 및 모범 사례 AWS Client VPN에서 Client VPN 엔드포인트에 대한 규칙과 제한 사항을 검토합니다.

> **Note**
>
> 이 시나리오에서는 Active Directory 그룹 또는 SAML 기반 IdP 그룹을 사용하는 네트워크 기반 권한 부여 규칙을 지원하지 않습니다.

이 구성을 구현하는 방법

1. VPC와 동일한 리전에서 Client VPN 엔드포인트를 생성합니다. 이렇게 하려면 AWS Client VPN엔드포인트 생성에 설명된 단계를 수행합니다.
2. 앞에서 식별한 서브넷을 Client VPN 엔드포인트와 연결합니다. 이렇게 하려면 대상 네트워크를 AWS Client VPN 엔드포인트와 연결에 설명된 단계를 수행하고 VPC 및 서브넷을 선택합니다.
3. 라우팅 테이블의 로컬 네트워크에 대한 경로를 추가합니다. 이렇게 하려면 AWS Client VPN 엔드포인트 라우팅 생성에 설명된 단계를 수행합니다. 라우팅 대상(Route destination)에 클라이언트 CIDR 범위를 입력하고 대상 VPC 서브넷 ID(Target VPC Subnet ID)에서 `local`을 지정합니다.

4. 권한 부여 규칙을 추가하여 클라이언트에 VPC에 대한 액세스 권한을 부여합니다. 이렇게 하려면 권한 부여 규칙 추가에 설명된 단계를 수행합니다. 활성화할 대상 네트워크(Destination network to enable)에 VPC의 IPv4 CIDR 범위를 입력합니다.
5. 권한 부여 규칙을 추가하여 클라이언트에 클라이언트 CIDR 범위에 대한 액세스 권한을 부여합니다. 이렇게 하려면 권한 부여 규칙 추가에 설명된 단계를 수행합니다. 활성화할 대상 네트워크(Destination network to enable)에 클라이언트 CIDR 범위를 입력합니다.

Client VPN을 사용한 네트워크 액세스 제한

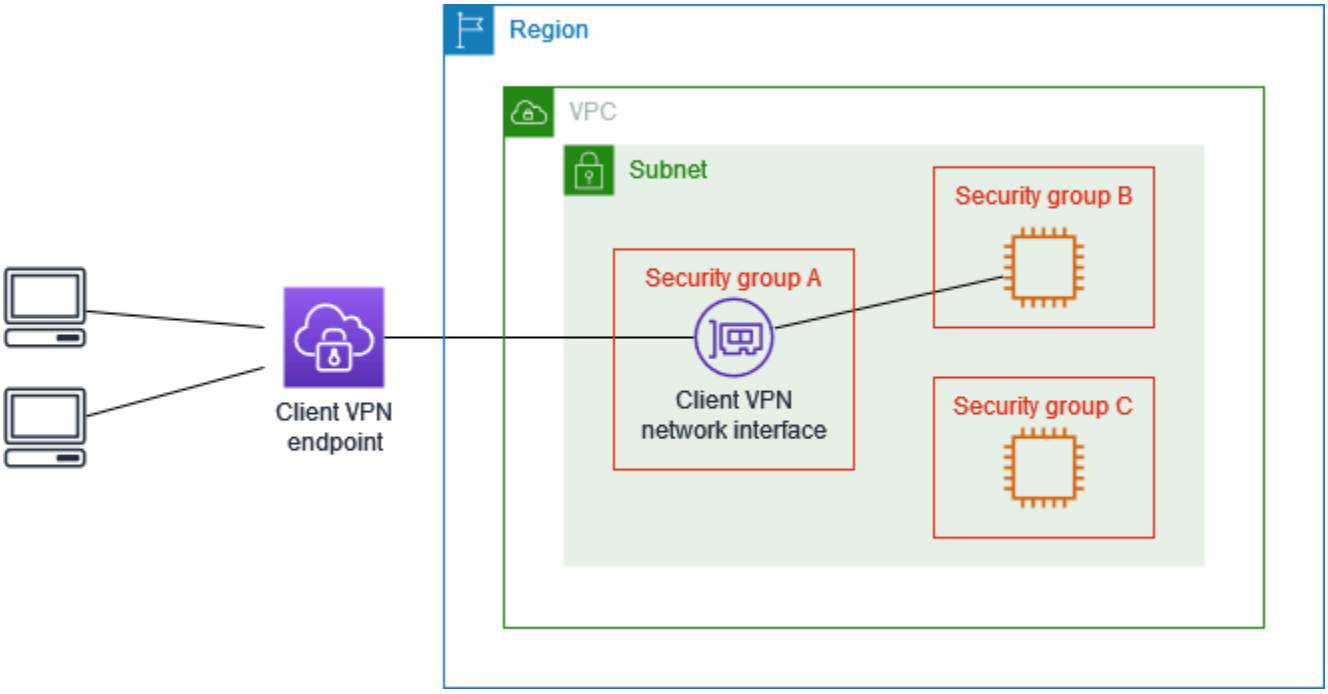
VPC의 특정 리소스에 대한 액세스를 제한하도록 AWS Client VPN 엔드포인트를 구성할 수 있습니다. 사용자 기반 인증의 경우 Client VPN 엔드포인트에 액세스하는 사용자 그룹을 기반으로 네트워크 일부에 대한 액세스를 제한할 수도 있습니다.

보안 그룹을 사용하여 액세스 제한

대상 네트워크 연결(Client VPN 보안 그룹)에 적용된 보안 그룹을 참조하는 보안 그룹 규칙을 추가하거나 제거하여 VPC의 특정 리소스에 대한 액세스를 부여하거나 거부할 수 있습니다. 이 구성은 Client VPN을 사용하여 VPC 액세스에서 설명하는 시나리오를 확장합니다. 이 구성은 그 시나리오에서 구성한 권한 부여 규칙에 추가로 적용됩니다.

특정 리소스에 대한 액세스 권한을 부여하려면 리소스가 실행 중인 인스턴스와 연결된 보안 그룹을 식별합니다. 그런 다음 Client VPN 보안 그룹의 트래픽을 허용하는 규칙을 생성합니다.

다음 다이어그램에서 보안 그룹 A는 Client VPN 보안 그룹이고, 보안 그룹 B는 EC2 인스턴스와 연결되며, 보안 그룹 C는 EC2 인스턴스와 연결됩니다. 보안 그룹 A로부터의 액세스를 허용하는 규칙을 보안 그룹 B에 추가하면 클라이언트가 보안 그룹 B와 연결된 인스턴스에 액세스할 수 있습니다. 보안 그룹 C에 보안 그룹 A로부터의 액세스를 허용하는 규칙이 없는 경우 클라이언트는 보안 그룹 C와 연결된 인스턴스에 액세스할 수 없습니다.



시작하기 전에 Client VPN 보안 그룹이 VPC의 다른 리소스와 연결되어 있는지 확인하세요. Client VPN 보안 그룹을 참조하는 규칙을 추가하거나 제거하는 경우 연결된 다른 리소스에 대한 액세스 권한도 부여하거나 거부할 수 있습니다. 이 문제를 방지하려면 Client VPN 엔드포인트에 사용하기 위해 특별히 생성된 보안 그룹을 사용합니다.

보안 그룹 규칙을 생성하는 방법

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 [Security Groups]를 선택합니다.
3. 리소스가 실행 중인 인스턴스와 연결된 보안 그룹을 선택합니다.
4. 작업, 인바운드 규칙 편집을 선택합니다.
5. Add rule(규칙 추가)를 선택하고 다음을 수행합니다.
   - 유형에서 모든 트래픽 또는 허용할 특정 트래픽 유형을 선택합니다.
   - 소스에서 사용자 지정을 선택한 다음 Client VPN 보안 그룹의 ID를 입력하거나 선택합니다.
6. 규칙 저장 선택

특정 리소스에 대한 액세스 권한을 제거하려면 리소스가 실행 중인 인스턴스와 연결된 보안 그룹을 확인합니다. Client VPN 보안 그룹의 트래픽을 허용하는 규칙이 있으면 해당 규칙을 삭제합니다.

보안 그룹 규칙을 확인하는 방법

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 [Security Groups]를 선택합니다.
3. 인바운드 규칙을 선택합니다.
4. 규칙 목록을 검토합니다. 소스가 Client VPN 보안 그룹인 규칙이 있는 경우 규칙 편집을 선택하고 규칙에 대해 삭제(x 아이콘)를 선택합니다. 규칙 저장을 선택합니다.

사용자 그룹을 기준으로 액세스 제한

Client VPN 엔드포인트가 사용자 기반 인증에 맞게 구성된 경우, 네트워크의 특정 부분에 대한 액세스 권한을 특정 사용자 그룹에 부여할 수 있습니다. 이렇게 하려면 다음 단계를 완료하세요.

1. Directory Service 또는 IdP에서 사용자 및 그룹을 구성합니다. 자세한 정보는 다음 주제를 참조하세요.
   - Client VPN에서의 Active Directory 인증
   - SAML 기반 연동 인증에 대한 요구 사항 및 고려 사항
2. 지정된 그룹이 네트워크 전체 또는 일부에 액세스할 수 있도록 허용하는 Client VPN 엔드포인트에 대한 권한 부여 규칙을 생성합니다. 자세한 내용은 AWS Client VPN 권한 부여 규칙 단원을 참조하세요.

Client VPN 엔드포인트가 상호 인증에 맞게 구성된 경우 사용자 그룹을 구성할 수 없습니다. 권한 부여 규칙을 생성할 때 모든 사용자에게 액세스 권한을 부여해야 합니다. 특정 사용자 그룹이 네트워크의 특정 부분에 액세스할 수 있도록 하려면 여러 Client VPN 엔드포인트를 생성할 수 있습니다. 예를 들어, 네트워크에 액세스하는 각 사용자 그룹에 대해 다음을 수행합니다.

1. 해당 사용자 그룹에 대한 서버 및 클라이언트 인증서 및 키 집합을 생성합니다. 자세한 내용은 의 상호 인증 AWS Client VPN 단원을 참조하세요.
2. Client VPN 엔드포인트를 생성합니다. 자세한 내용은 AWS Client VPN엔드포인트 생성 단원을 참조하세요.
3. 네트워크의 전체 또는 일부에 대한 액세스 권한을 부여하는 권한 부여 규칙을 생성합니다. 예를 들어, 관리자가 사용하는 Client VPN 엔드포인트의 경우 전체 네트워크에 대한 액세스 권한을 부여하는 권한 부여 규칙을 생성할 수 있습니다. 자세한 내용은 권한 부여 규칙 추가 섹션을 참조하세요.

의 클라이언트 인증 AWS Client VPN

클라이언트 인증은 AWS 클라우드에 처음 진입할 때 구현됩니다. 인증을 사용하여 클라이언트가 Client VPN 엔드포인트에 연결하도록 허용되는지 여부를 확인합니다. 인증이 성공하면 클라이언트가 Client VPN 엔드포인트에 연결하고 VPN 세션을 설정합니다. 인증이 실패하면 연결이 거부되고 클라이언트가 VPN 세션을 연결할 수 없습니다.

Client VPN에서는 다음과 같은 유형의 클라이언트 인증을 제공합니다.

- Active Directory 인증(사용자 기반)
- 상호 인증(인증서 기반)
- Single sign-on(SAML 기반 연동 인증)(사용자 기반)

위에 나열된 방법 중 하나만 사용하거나 다음과 같이 사용자 기반 방법과 상호 인증을 조합해 사용할 수 있습니다.

- 상호 인증 및 연동 인증
- 상호 인증 및 Active Directory 인증

> **Important**
>
> - Client VPN 엔드포인트를 생성하려면 사용하는 인증 유형에 관계없이 AWS Certificate Manager에서 서버 인증서를 프로비저닝해야 합니다. 서버 인증서를 생성하고 프로비저닝하는 방법에 대한 자세한 내용은 의 상호 인증 AWS Client VPN의 단계를 참조하십시오.
> - 상호 인증과 사용자 기반 인증의 조합을 사용하는 경우 두 방법을 모두 사용하여 VPN에서 올바르게 인증해야 합니다.

Client VPN에서의 Active Directory 인증

Client VPN은와 통합하여 Active Directory 지원을 제공합니다 Directory Service. Active Directory 인증에서는 클라이언트가 기존 Active Directory 그룹에 의해 인증됩니다. Directory Service를 사용하면 Client VPN은 AWS 또는 온프레미스 네트워크에 프로비저닝된 기존 Active Directory에 연결할 수 있습니다. 이를 통해 기존 클라이언트 인증 인프라를 사용할 수 있습니다. 온프레미스 Active Directory를 사용 중이고 기존 AWS Managed Microsoft AD가 없는 경우 Active Directory Connector(AD Connector)

를 구성해야 합니다. 하나의 Active Directory 서버를 사용하여 사용자를 인증할 수 있습니다. Active Directory 통합에 대한 자세한 내용은 AWS Directory Service 관리 안내서를 참조하세요.

Client VPN은 AWS 관리형 Microsoft AD 또는 AD Connector에 대해 활성화된 경우 멀티 팩터 인증(MFA)을 지원합니다. MFA가 활성화된 경우 클라이언트는 Client VPN 엔드포인트에 연결할 때 사용자 이름, 암호 및 MFA 코드를 입력해야 합니다. MFA 활성화에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 AWS 관리형 Microsoft AD에 대한 멀티 팩터 인증 활성화 및 AD Connector에 대한 멀티 팩터 인증 활성화를 참조하세요.

Active Directory에서 사용자와 그룹을 구성하기 위한 할당량 및 규칙은 사용자 및 그룹 할당량 단원을 참조하십시오.

의 상호 인증 AWS Client VPN

상호 인증에서는 Client VPN이 인증서를 사용하여 클라이언트와 서버 간에 인증을 수행합니다. 인증서는 인증 기관(CA)에서 발행한 디지털 형태의 ID 증명서입니다. 서버는 클라이언트 인증서를 사용하여 Client VPN 엔드포인트에 연결하려고 시도하는 클라이언트를 인증합니다. 하나의 서버 인증서 및 키와 하나 이상의 클라이언트 인증서 및 키를 생성해야 합니다.

서버 인증서를 AWS Certificate Manager (ACM)에 업로드하고 Client VPN 엔드포인트를 생성할 때 지정해야 합니다. 서버 인증서를 ACM에 업로드할 때 인증 기관(CA)도 지정합니다. 클라이언트 인증서의 CA가 서버 인증서의 CA와 다른 경우 클라이언트 인증서를 ACM에 업로드하기만 하면 됩니다. ACM에 대한 자세한 내용은 AWS Certificate Manager 사용 설명서를 참조하세요.

Client VPN 엔드포인트에 연결할 각 클라이언트에 대해 별도의 클라이언트 인증서 및 키를 생성할 수 있습니다. 이렇게 하면 사용자가 조직을 떠나는 경우 특정 클라이언트 인증서를 취소할 수 있습니다. 이 경우 클라이언트 인증서가 서버 인증서와 동일한 CA에서 발급된 경우 Client VPN 엔드포인트를 생성할 때 클라이언트 인증서에 대한 서버 인증서 ARN을 지정할 수 있습니다.

AWS Client VPN에 사용되는 인증서는 메모의 섹션 4.2에 지정된 인증서 확장을 포함하여 RFC 5280: Internet X.509 퍼블릭 키 인프라 인증서 및 인증서 해지 목록(CRL) 프로필을 준수해야 합니다.

> **Note**
>
> Client VPN 엔드포인트는 1024비트 및 2048비트 RSA 키 크기만 지원합니다. 또한 클라이언트 인증서의 제목 필드에 CN 속성이 있어야 합니다.
> Client VPN 서비스에서 사용 중인 인증서가 ACM 자동 교체를 통해 업데이트되거나 새 인증서를 수동으로 가져와 업데이트되거나 IAM Identity Center에 대한 메타데이터 업데이트를 통해

업데이트되면 Client VPN 서비스가 Client VPN 엔드포인트를 새 인증서로 자동 업데이트합니다. 이는 최대 5시간이 걸릴 수 있는 자동화된 프로세스입니다.

작업

- 에 대한 상호 인증 활성화 AWS Client VPN
- AWS Client VPN에 대한 서버 인증서 갱신

에 대한 상호 인증 활성화 AWS Client VPN

Linux/MacOS 또는 Windows의 Client VPN에서 상호 인증을 활성화할 수 있습니다.

Linux/macOS

다음 절차에서는 OpenVPN easy-rsa를 사용하여 서버 및 클라이언트 인증서와 키를 생성한 다음, 서버 인증서와 키를 ACM에 업로드합니다. 자세한 내용은 Easy-RSA 3 Quickstart README를 참조하십시오.

서버 및 클라이언트 인증서와 키를 생성하여 ACM에 업로드하려면

1. OpenVPN easy-rsa 리포지토리를 로컬 컴퓨터에 복제하고 `easy-rsa/easyrsa3` 폴더로 이동하십시오.

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

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

2. 새 PKI 환경을 시작합니다.

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

3. 새 CA(인증 기관)를 빌드하려면 이 명령을 실행하고 표시되는 메시지를 따릅니다.

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

4. 서버 인증서 및 키를 생성합니다.

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

5. 클라이언트 인증서 및 키를 생성합니다.

   클라이언트를 구성할 때 필요하므로 클라이언트 인증서와 클라이언트 프라이빗 키를 저장해야 합니다.

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

   클라이언트 인증서와 키가 필요한 각 클라이언트(최종 사용자)에 대해 이 단계를 선택적으로 반복할 수 있습니다.

6. 서버 인증서 및 키 그리고 클라이어트 인증서 및 키를 사용자 지정 폴더에 복사한 후 해당 폴더로 이동합니다.

   인증서 및 키를 복사하기 전에 `mkdir` 명령을 사용하여 사용자 지정 폴더를 만듭니다. 다음 예제에서는 홈 디렉터리에 사용자 지정 폴더를 만듭니다.

   ```
   $ 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. 서버 인증서 및 키와 클라이언트 인증서 및 키를 ACM에 업로드합니다. Client VPN 엔드포인트를 생성하려는 리전과 동일한 리전에 업로드해야 합니다. 다음 명령은 AWS CLI 를 사용하여 인증서를 업로드합니다. 대신 ACM 콘솔을 사용하여 인증서를 업로드하려면 AWS Certificate Manager 사용 설명서의 인증서 가져오기를 참조하세요.

   ```
   $ 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
   ```

   클라이언트 인증서를 반드시 ACM에 업로드하지 않아도 됩니다. 서버 및 클라이언트 인증서가 동일한 인증 기관(CA)에 의해 발급된 경우, Client VPN 엔드포인트를 생성할 때 서버 및 클라이언트 모두에 대해 서버 인증서 ARN을 사용할 수 있습니다. 위에서 설명한 단계에서는 동일한 CA를 사용하여 두 가지 인증서를 모두 생성했습니다. 그러나 완전성을 위해 클라이언트 인증서를 업로드하는 단계가 포함됩니다.

Windows

다음 절차에서는 Easy-RSA 3.x 소프트웨어를 설치하고 이 소프트웨어를 사용하여 서버 및 클라이언트 인증서와 키를 생성합니다.

서버 및 클라이언트 인증서와 키를 생성하여 ACM에 업로드하려면

1. EasyRSA 릴리스(EasyRSA releases) 페이지를 열고 사용 중인 Windows 버전에 해당하는 ZIP 파일을 다운로드한 후 압축을 풉니다.
2. 명령 프롬프트를 열고 `EasyRSA-3.x` 폴더가 추출된 위치로 이동합니다.
3. 다음 명령을 실행하여 EasyRSA 3 셸을 엽니다.

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

4. 새 PKI 환경을 시작합니다.

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

5. 새 CA(인증 기관)를 빌드하려면 이 명령을 실행하고 표시되는 메시지를 따릅니다.

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

6. 서버 인증서 및 키를 생성합니다.

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

7. 클라이언트 인증서 및 키를 생성합니다.

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

클라이언트 인증서와 키가 필요한 각 클라이언트(최종 사용자)에 대해 이 단계를 선택적으로 반복할 수 있습니다.

8. EasyRSA 3 셸을 종료합니다.

```
# exit
```

9. 서버 인증서 및 키 그리고 클라이어트 인증서 및 키를 사용자 지정 폴더에 복사한 후 해당 폴더로 이동합니다.

인증서 및 키를 복사하기 전에 mkdir 명령을 사용하여 사용자 지정 폴더를 만듭니다. 다음 예제에서는 C:\ 드라이브에 사용자 지정 폴더를 만듭니다.

```
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. 서버 인증서 및 키와 클라이언트 인증서 및 키를 ACM에 업로드합니다. Client VPN 엔드포인트를 생성하려는 리전과 동일한 리전에 업로드해야 합니다. 다음 명령은 AWS CLI 를 사용하여 인증서를 업로드합니다. 대신 ACM 콘솔을 사용하여 인증서를 업로드하려면 AWS Certificate Manager 사용 설명서의 인증서 가져오기를 참조하세요.

```
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
```

클라이언트 인증서를 반드시 ACM에 업로드하지 않아도 됩니다. 서버 및 클라이언트 인증서가 동일한 인증 기관(CA)에 의해 발급된 경우, Client VPN 엔드포인트를 생성할 때 서버 및 클라이언트 모두에 대해 서버 인증서 ARN을 사용할 수 있습니다. 위에서 설명한 단계에서는 동일한 CA를 사용하여 두 가지 인증서를 모두 생성했습니다. 그러나 완전성을 위해 클라이언트 인증서를 업로드하는 단계가 포함됩니다.

AWS Client VPN에 대한 서버 인증서 갱신

만료된 Client VPN 서버 인증서를 갱신하고 다시 가져올 수 있습니다. 사용 중인 OpenVPN easy-rsa 버전에 따라 절차가 달라집니다. 자세한 내용은 Easy-RSA 3 인증서 갱신 및 취소 설명서를 참조하세요.

서버 인증서를 갱신하려면

1. 다음 중 하나를 수행합니다.
   - Easy-RSA 버전 3.1.x
     - 인증서 갱신 명령을 실행합니다.

       ```
       $ ./easyrsa renew server nopass
       ```
   - Easy-RSA 버전 3.2.x

     a. 만료 명령을 실행합니다.

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

     b. 새 인증서에 서명합니다.

     ```
     $ ./easyrsa --san=DNS:server sign-req server server
     ```
2. 사용자 지정 폴더를 만들고 새 파일을 여기에 복사한 다음 해당 폴더로 이동합니다.

   ```
   $ 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. 새 파일을 ACM으로 가져옵니다. Client VPN 엔드포인트와 동일한 리전에서 가져와야 합니다.

   ```
   $ 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
   ```

Single Sign-On — SAML 2.0 기반 페더레이션 인증 — Client VPN

AWS Client VPN 는 Client VPN 엔드포인트에 대해 Security Assertion Markup Language 2.0(SAML 2.0)을 사용한 ID 페더레이션을 지원합니다. SAML 2.0을 지원하는 자격 증명 공급자(IdP)를 사용하여 중앙 집중식 사용자 자격 증명을 생성할 수 있습니다. 그런 다음 SAML 기반 연동 인증을 사용하도록 Client VPN 엔드포인트를 구성하고 IdP와 연결할 수 있습니다. 그런 다음 사용자는 중앙 집중식 자격 증명을 사용하여 Client VPN 엔드포인트에 연결합니다.

주제

에 대한 SAML 활성화 AWS Client VPN

다음 단계를 완료하여 Client VPN에 대한 Single Sign-On에 SAML을 활성화할 수 있습니다. 또는 Client VPN 엔드포인트에 대해 셀프 서비스 포털을 활성화한 경우 셀프 서비스 포털로 이동하여 구성 파일과 AWS 제공 클라이언트를 가져오도록 사용자에게 지시합니다. 자세한 내용은 셀프 서비스 포털에 대한 AWS Client VPN 액세스 단원을 참조하십시오.

SAML 기반 IdP가 Client VPN 엔드포인트에서 작동하도록 하려면 다음을 수행해야 합니다.

1. 선택한 IdP에서 SAML 기반 앱을 생성하여와 함께 사용하거나 기존 앱을 AWS Client VPN사용합니다.
2. IdP를 구성하여 와 신뢰 관계를 설정합니다 AWS리소스에 대한 자세한 내용은 SAML 기반 IdP 구성 리소스 단원을 참조하십시오.
3. 사용 중인 IdP에서 조직을 IdP로 설명하는 연동 메타데이터 문서를 생성하고 다운로드합니다.

   이 서명된 XML 문서는 AWS 와 IdP 간의 신뢰 관계를 설정하는 데 사용됩니다.
4. Client VPN 엔드포인트와 동일한 AWS 계정에 IAM SAML 자격 증명 공급자를 생성합니다.

   IAM SAML 자격 증명 공급자는 IdP에서 생성된 메타데이터 문서를 사용하여 신뢰 AWS 관계를 위한 조직의 IdP를 정의합니다. 자세한 내용은 IAM 사용 설명서의 IAM SAML 자격 증명 공급자 생성을 참조하십시오. 나중에 IdP에서 앱 구성을 업데이트하는 경우 새 메타데이터 문서를 생성하고 IAM SAML 자격 증명 공급자를 업데이트합니다.

> **Note**
>
> IAM SAML 자격 증명 공급자를 사용하기 위해 IAM 역할을 생성할 필요가 없습니다.

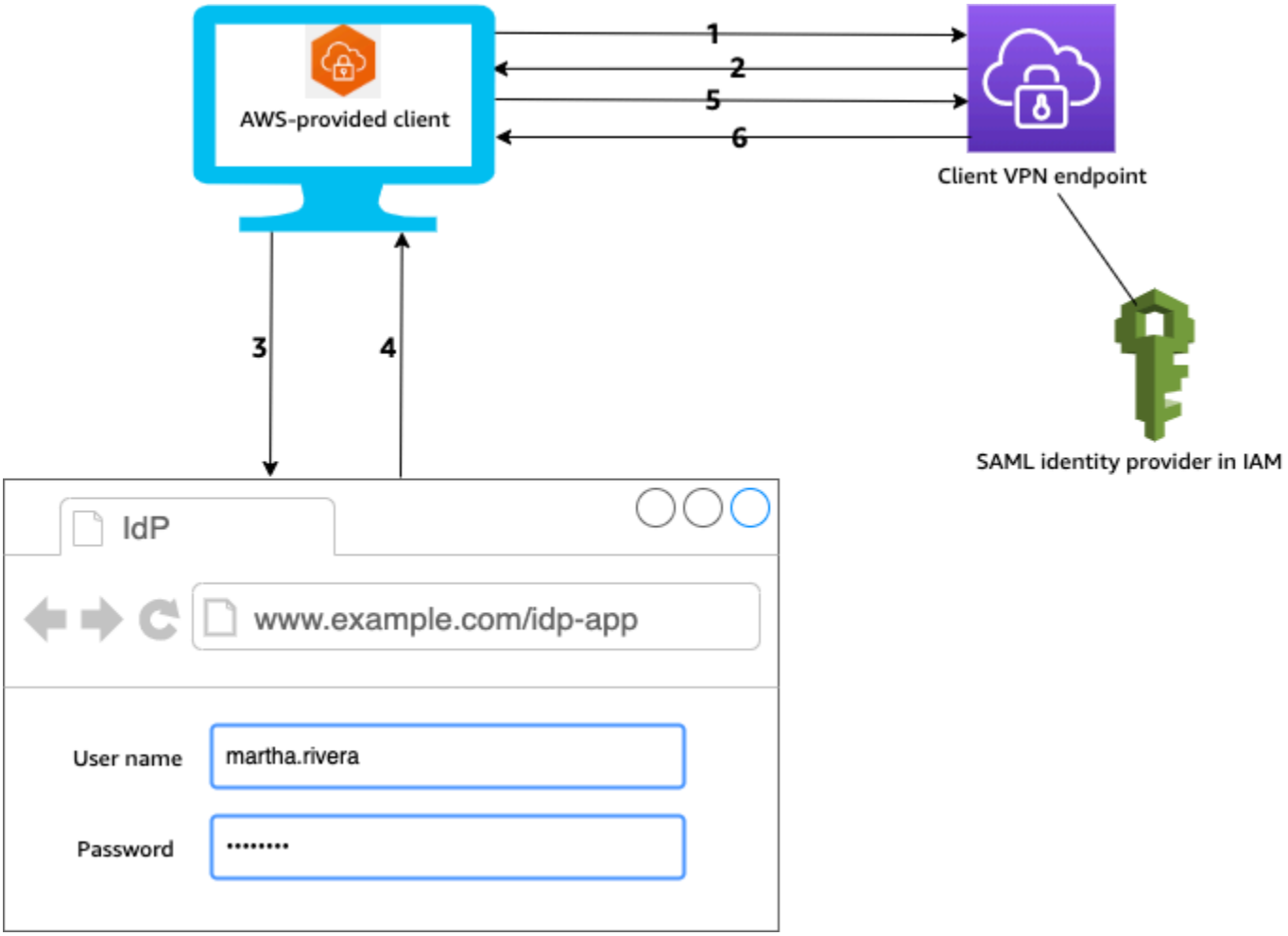
5. Client VPN 엔드포인트를 생성합니다.

   연동 인증을 인증 유형으로 지정하고 생성한 IAM SAML 자격 증명 공급자를 지정합니다. 자세한 정보는 AWS Client VPN엔드포인트 생성을 참조하십시오.

6. 클라이언트 구성 파일을 내보내고 사용자에게 배포합니다. 최신 버전의 AWS 제공 클라이언트를 다운로드하고 이 클라이언트를 사용하여 구성 파일을 로드하고 Client VPN 엔드포인트에 연결하도록 사용자에게 지시합니다.

인증 워크플로

다음 다이어그램은 SAML 기반 연동 인증을 사용하는 Client VPN 엔드포인트에 대한 인증 워크플로우의 개요를 제공합니다. Client VPN 엔드포인트를 생성하고 구성할 때 IAM SAML 자격 증명 공급자를 지정합니다.



1. 사용자는 디바이스에서 AWS 제공된 클라이언트를 열고 Client VPN 엔드포인트에 대한 연결을 시작합니다.
2. Client VPN 엔드포인트는 IAM SAML 자격 증명 공급자에 제공된 정보를 기반으로 IdP URL 및 인증 요청을 클라이언트로 다시 보냅니다.
3. AWS 제공된 클라이언트가 사용자 디바이스에서 새 브라우저 창을 엽니다. 브라우저가 IdP에 요청하고 로그인 페이지를 표시합니다.
4. 사용자가 로그인 페이지에 자격 증명을 입력하면 IdP가 서명된 SAML 어설션을 클라이언트로 다시 보냅니다.
5. AWS 제공된 클라이언트는 SAML 어설션을 Client VPN 엔드포인트로 전송합니다.
6. Client VPN 엔드포인트는 어설션의 유효성을 검사하고 사용자에 대한 액세스를 허용하거나 거부합니다.

SAML 기반 연동 인증에 대한 요구 사항 및 고려 사항

다음은 SAML 기반 연동 인증에 대한 요구 사항 및 고려 사항입니다.

- SAML 기반 IdP에서 사용자와 그룹을 구성하기 위한 할당량 및 규칙은 사용자 및 그룹 할당량 단원을 참조하십시오.
- SAML 어설션 및 응답은 서명이 필요합니다.
- AWS Client VPN 는 SAML 어설션에서 "AudienceRestriction" 및 "NotBefore and NotOnOrAfter" 조건만 지원합니다.
- SAML 응답에 대해 지원되는 최대 크기는 128KB입니다.
- AWS Client VPN 는 서명된 인증 요청을 제공하지 않습니다.
- SAML 단일 로그아웃은 지원되지 않습니다. 사용자는 AWS 제공된 클라이언트에서 연결을 해제하여 로그아웃하거나 연결을 종료할 수 있습니다.
- Client VPN 엔드포인트는 단일 IdP만 지원합니다.
- Multi-Factor Authentication(MFA)은 IdP에서 활성화될 때 지원됩니다.
- 사용자는 AWS 제공된 클라이언트를 사용하여 Client VPN 엔드포인트에 연결해야 합니다. 버전은 1.2.0 이상을 사용해야 합니다. 자세한 내용은 AWS 제공된 클라이언트를 사용하여 연결을 참조하세요.
- IdP 인증을 지원하는 브라우저로는 Apple Safari, Google Chrome, Microsoft Edge, Mozilla Firefox 등이 있습니다.
- AWS 제공된 클라이언트는 SAML 응답을 위해 사용자의 디바이스에 TCP 포트 35001을 예약합니다.
- IAM SAML 자격 증명 공급자에 대한 메타데이터 문서가 잘못되거나 악의적인 URL로 업데이트되면 사용자에게 인증 문제가 발생하거나 피싱 공격이 발생할 수 있습니다. 따라서 AWS CloudTrail 을 사용하여 IAM SAML 자격 증명 공급자에 대한 업데이트를 모니터링하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 AWS CloudTrail을 사용하여 IAM 및 AWS STS 호출 로깅을 참조하세요.
- AWS Client VPN 는 HTTP 리디렉션 바인딩을 통해 IdP에 AuthN 요청을 보냅니다. 따라서 IdP는 HTTP 리디렉션 바인딩을 지원해야 하며 IdP의 메타데이터 문서에 있어야 합니다.
- SAML 어설션의 경우 `NameID` 속성에 이메일 주소 형식을 사용해야 합니다.
- 최대 사용자 이름(`NameID`) 길이는 1024바이트입니다. 사용자 이름이 더 긴 연결은 거부됩니다.
- Client VPN 서비스에서 사용 중인 인증서가 ACM 자동 교체를 통해 업데이트되거나 새 인증서를 수동으로 가져와 업데이트되거나 IAM Identity Center에 대한 메타데이터 업데이트를 통해 업데이트되면 Client VPN 서비스가 Client VPN 엔드포인트를 새 인증서로 자동 업데이트합니다. 이는 최대 5시간이 걸릴 수 있는 자동화된 프로세스입니다.

SAML 기반 IdP 구성 리소스

다음 표에는 AWS Client VPN에서 사용하도록 테스트한 SAML 기반 IdP 및 IdP 구성에 도움이 되는 리소스가 나와 있습니다.

IdP	리소스
Okta	SAML을 사용하여 AWS Client VPN 사용자 인증
Microsoft Entra ID(이전 Azure Active Directory)	자세한 내용은 Microsoft 설명서 웹 사이트의 자습서: Microsoft Entra Single Sign-On(SSO)과 AWS ClientVPN 통합을 참조하세요.
JumpCloud	와 통합 AWS Client VPN
AWS IAM Identity Center	인증 및 권한 부여를 AWS Client VPN 위해에서 IAM Identity Center 사용

앱 생성을 위한 서비스 공급자 정보

위 표에 나열되지 않은 IdP를 사용하여 SAML 기반 앱을 생성하려면 다음 정보를 사용하여 AWS Client VPN 서비스 공급자 정보를 구성합니다.

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

IdP의 SAML 응답에는 하나 이상의 속성이 포함되어야 합니다. 다음은 속성 예시입니다.

속성	설명
`FirstName`	사용자의 이름입니다.
`LastName`	사용자의 성입니다.
`memberOf`	사용자가 속한 그룹입니다.

> **Note**
>
> `memberOf` 속성은 Active Directory 또는 SAML IdP 그룹 기반 권한 부여 규칙을 사용하는 데 필요합니다. 속성은 대/소문자를 구분하며 지정된 대로 정확하게 구성해야 합니다. 자세한 내용은 네트워크 기반 권한 부여 및 AWS Client VPN 권한 부여 규칙 섹션을 참조하세요.

셀프 서비스 포털에 대한 지원

Client VPN 엔드포인트에 대해 셀프 서비스 포털을 활성화하면 사용자는 SAML 기반 IdP 자격 증명을 사용하여 포털에 로그인합니다.

IdP가 Assertion Consumer Service(ACS) URL을 여러 개 지원하는 경우 다음 ACS URL을 앱에 추가합니다.

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

GovCloud 리전에서 Client VPN 엔드포인트를 사용하는 경우 대신 다음 ACS URL을 사용합니다. 동일한 IDP 앱을 사용하여 표준 리전과 GovCloud 리전 모두에 대해 인증하는 경우 두 URL을 추가할 수 있습니다.

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

IdP가 여러 ACS URL을 지원하지 않는 경우 다음을 수행합니다.

1. IdP에서 추가 SAML 기반 앱을 생성하고 다음 ACS URL을 지정합니다.

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

2. 연동 메타데이터 문서를 생성하고 다운로드합니다.
3. Client VPN 엔드포인트와 동일한 AWS 계정에 IAM SAML 자격 증명 공급자를 생성합니다. 자세한 내용은 IAM 사용 설명서의 IAM SAML 자격 증명 공급자 생성을 참조하십시오.

   > **Note**
   >
   > 기본 앱에 대해 생성한 자격 증명 공급자 외에도, 이 IAM SAML 자격 증명 공급자를 생성합니다.

4. Client VPN 엔드포인트를 생성하고, 생성한 IAM SAML 자격 증명 공급자를 둘 다 지정합니다.

AWS Client VPN에서 클라이언트 권한 부여

Client VPN은 두 가지 유형의 클라이언트 권한 부여를 지원합니다. 이 두 가지 유형은 보안 그룹 및 네트워크 기반 권한 부여(권한 부여 규칙 사용)입니다.

보안 그룹

Client VPN 엔드포인트를 생성할 때 Client VPN 엔드포인트에 적용할 특정 VPC의 보안 그룹을 지정할 수 있습니다. 서브넷을 Client VPN 엔드포인트와 연결하면 VPC의 기본 보안 그룹이 자동으로 적용됩니다. Client VPN 엔드포인트를 생성한 후 보안 그룹을 변경할 수 있습니다. 자세한 정보는 의 대상 네트워크에 보안 그룹 적용 AWS Client VPN을 참조하십시오. 보안 그룹은 Client VPN 네트워크 인터페이스와 연결됩니다.

연결에 적용된 보안 그룹의 트래픽을 허용하는 규칙을 애플리케이션의 보안 그룹에 추가하여 Client VPN 사용자가 VPC의 애플리케이션에 액세스하도록 허용할 수 있습니다.

반대로, 연결에 적용된 보안 그룹을 지정하지 않거나 Client VPN 엔드포인트 보안 그룹을 참조하는 규칙을 제거하여 Client VPN 사용자의 액세스를 제한할 수 있습니다. 필요한 보안 그룹 규칙은 구성하려는 VPN 액세스의 종류에 따라 달라질 수도 있습니다. 자세한 정보는 Client VPN의 시나리오 및 예제을 참조하십시오.

VPC 보안 그룹에 대한 자세한 내용은 Amazon VPC 사용 설명서의 VPC의 보안 그룹을 참조하십시오.

네트워크 기반 권한 부여

네트워크 기반 권한 부여는 권한 부여 규칙으로 구현됩니다. 액세스를 허용하려는 각 네트워크에 대해 액세스 권한을 가진 사용자를 제한하는 권한 부여 규칙을 구성해야 합니다. 지정된 네트워크에 대해 액세스가 허용되는 Active Directory 그룹 또는 SAML 기반 IdP 그룹을 구성합니다. 지정된 그룹에 속한 사용자만 지정된 네트워크에 액세스할 수 있습니다. Active Directory 인증 또는 SAML 기반 연동 인증을 사용하지 않거나 모든 사용자에게 액세스를 허용하려는 경우 모든 클라이언트에 액세스 권한을 부여하는 규칙을 지정할 수 있습니다. 자세한 내용은 AWS Client VPN 권한 부여 규칙 섹션을 참조하세요.

Tasks

- AWS Client VPN 엔드포인트 보안 그룹 규칙 생성

AWS Client VPN 엔드포인트 보안 그룹 규칙 생성

서브넷을 Client VPN에 연결할 때 적용되는 VPC의 기본 보안 그룹은 허용하려는 기본 보안 그룹 트래픽의 트래픽을 제한하는 동시에 원하지 않는 트래픽을 허용할 수 있습니다. 다음 단계를 사용하여 리소스 또는 애플리케이션과 연결된 엔드포인트 보안 그룹에 대한 트래픽을 허용하거나 제한하는 Client VPN 엔드포인트 보안 그룹 규칙을 생성합니다. 보안 그룹 규칙에 대한 자세한 내용은 Amazon VPC 사용 설명서의 VPC의 보안 그룹을 참조하세요.

Client VPN 엔드포인트 보안 그룹의 트래픽을 허용하는 규칙을 추가하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Security Groups를 선택합니다.
3. 리소스 또는 애플리케이션과 연결된 보안 그룹을 선택하고 작업, 인바운드 규칙 편집을 선택합니다.
4. [Add another rule]을 선택합니다.
5. Type에서 All traffic을 선택합니다. 또는 SSH와 같은 특정 유형의 트래픽에 대한 액세스를 제한할 수 있습니다.

   Source(소스)에서 Client VPN 엔드포인트의 대상 네트워크(서브넷)와 연결된 보안 그룹의 ID를 지정합니다.
6. 규칙 저장을 선택합니다.

의 연결 권한 부여 AWS Client VPN

Client VPN 엔드포인트에 대한 클라이언트 연결 핸들러를 구성할 수 있습니다. 핸들러를 사용하면 디바이스, 사용자 및 연결 속성을 기반으로 새 연결을 인증하는 사용자 지정 논리를 실행할 수 있습니다. Client VPN 서비스가 디바이스와 사용자를 인증한 후에 클라이언트 연결 핸들러가 실행됩니다.

Client VPN 엔드포인트에 대한 클라이언트 연결 핸들러를 구성하려면 디바이스, 사용자 및 연결 속성을 입력으로 사용하고 결정을 Client VPN 서비스에 반환하여 새 연결을 허용하거나 거부하는 AWS Lambda 함수를 생성합니다. Client VPN 엔드포인트에서 Lambda 함수를 지정합니다. 디바이스가 Client VPN 엔드포인트에 연결되면 클라이언트 VPN 서비스가 사용자를 대신하여 Lambda 함수를 호출합니다. Lambda 함수가 권한을 부여한 연결만 Client VPN 엔드포인트에 연결하도록 허용됩니다.

> **Note**
>
> 현재 지원되는 유일한 클라이언트 연결 핸들러 유형은 Lambda 함수입니다.

요구 사항 및 고려 사항

다음은 클라이언트 연결 핸들러에 대한 요구 사항 및 고려 사항입니다.

- Lambda 함수의 이름은 `AWSClientVPN-` 접두사로 시작해야 합니다.
- 정규화된 Lambda 함수가 지원됩니다.
- Lambda 함수는 Client VPN 엔드포인트와 동일한 AWS 리전 및 동일한 AWS 계정에 있어야 합니다.
- Lambda 함수는 30초 후에 시간 초과됩니다. 이 값은 변경할 수 없습니다.
- Lambda 함수는 동기식으로 호출됩니다. 이 함수는 디바이스 및 사용자 인증 후 권한 부여 규칙을 평가하기 전에 호출됩니다.
- 새 연결에 대해 Lambda 함수가 호출되고 클라이언트 VPN 서비스가 함수에서 예상 응답을 받지 못하면 클라이언트 VPN 서비스가 연결 요청을 거부합니다. 예를 들어, Lambda 함수가 제한되거나 시간 초과되거나 기타 예기치 않은 오류가 발생하거나 함수의 응답이 유효한 형식이 아닌 경우 이 문제가 발생할 수 있습니다.
- 지연 시간의 변동 없이 확장할 수 있도록 Lambda 함수에 대해 프로비저닝된 동시성을 구성하는 것이 좋습니다.
- Lambda 함수를 업데이트하더라도 Client VPN 엔드포인트에 대한 기존 연결은 영향을 받지 않습니다. 기존 연결을 종료한 다음 클라이언트에 새 연결을 설정하도록 지시할 수 있습니다. 자세한 내용은 AWS Client VPN 클라이언트 연결 종료 단원을 참조하십시오.
- 클라이언트가 AWS 제공된 클라이언트를 사용하여 Client VPN 엔드포인트에 연결하는 경우 Windows의 경우 버전 1.2.6 이상을 사용하고 macOS의 경우 버전 1.2.4 이상을 사용해야 합니다. 자세한 내용은 AWS 제공 클라이언트를 사용하여 연결을 참조하세요.

Lambda 인터페이스

Lambda 함수는 디바이스 속성, 사용자 속성 및 연결 특성을 클라이언트 VPN 서비스의 입력으로 사용합니다. 그런 다음 연결을 허용할지 또는 거부할지에 대한 결정을 Client VPN 서비스에 반환해야 합니다.

요청 스키마

Lambda 함수는 다음 필드를 포함한 JSON BLOB를 입력으로 사용합니다.

```
{
    "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` - Client VPN 엔드포인트에 대한 클라이언트 연결의 ID입니다.
- `endpoint-id` - Client VPN 엔드포인트의 ID입니다.
- `common-name` - 디바이스 식별자입니다. 디바이스에 대해 생성한 클라이언트 인증서에서 일반 이름은 디바이스를 고유하게 식별합니다.
- `username` - 해당되는 경우 사용자 식별자입니다. Active Directory 인증의 경우 이 항목은 사용자 이름입니다. SAML 기반 연동 인증의 경우 이 인증은 `NameID`입니다. 상호 인증의 경우 이 필드는 비어 있습니다.
- `platform` - 클라이언트 운영 체제 플랫폼입니다.
- `platform-version` - 운영 체제 버전입니다. 클라이언트 VPN 서비스는 클라이언트가 Client VPN 엔드포인트에 연결할 때 및 클라이언트가 Windows 플랫폼을 실행 중일 때 OpenVPN 클라이언트 구성에 `--push-peer-info` 지시문이 있을 때 값을 제공합니다.
- `public-ip` - 연결 디바이스의 퍼블릭 IP 주소입니다.
- `client-openvpn-version` - 클라이언트가 사용 중인 OpenVPN 버전입니다.
- `aws-client-version` - AWS 클라이언트 버전입니다.
- `groups` - 해당되는 경우 그룹 식별자입니다. Active Directory 인증의 경우 이 항목은 Active Directory 그룹의 목록이 됩니다. SAML 기반 페더레이션 인증의 경우 이 항목은 IdP(자격 증명 공급자) 그룹 목록이 됩니다. 상호 인증의 경우 이 필드는 비어 있습니다.
- `schema-version` - 스키마 버전입니다. 기본값은 `v3`입니다.

응답 스키마

Lambda 함수가 다음 필드를 반환해야 합니다.

```
{
```

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

- `allow` - 필수입니다. 새 연결을 허용할지 거부할지를 나타내는 부울(`true` | `false`)입니다.
- `error-msg-on-denied-connection` - 필수입니다. Lambda 함수가 연결을 거부한 경우 클라이언트에 단계 및 지침을 제공하는 데 사용할 수 있는 최대 255자의 문자열입니다. Lambda 함수를 실행하는 동안 장애가 발생할 경우(예: 스로틀링으로 인해) Client VPN 서비스에서 클라이언트에 다음과 같은 기본 메시지를 반환합니다.

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

- `posture-compliance-statuses` - 필수입니다. Lambda 함수를 태세 평가에 사용하는 경우 이 필드는 연결 디바이스의 상태 목록입니다. 디바이스의 태세 평가 범주(예: `compliant`, `quarantined`, `unknown` 등)에 따라 상태 이름을 정의합니다. 각 이름의 최대 길이는 255자입니다. 최대 10개의 상태를 지정할 수 있습니다.
- `schema-version` - 필수입니다. 스키마 버전입니다. 기본값은 `v3`입니다.

동일한 리전의 여러 Client VPN 엔드포인트에 동일한 Lambda 함수를 사용할 수 있습니다.

Lambda 함수 생성에 대한 자세한 내용은 AWS Lambda 개발자 안내서의 AWS Lambda시작하기를 참조하세요.

태세 평가에 클라이언트 연결 핸들러 사용

클라이언트 연결 핸들러를 사용하여 Client VPN 엔드포인트를 기존 디바이스 관리 솔루션과 통합하여 연결 디바이스의 규정 준수 태세를 평가할 수 있습니다. Lambda 함수가 디바이스 권한 부여 핸들러로 작동하려면 상호 인증을 Client VPN 엔드포인트에 사용합니다. Client VPN 엔드포인트에 연결할 각 클라이언트(디바이스)에 대해 고유한 클라이언트 인증서 및 키를 생성합니다. Lambda 함수는 클라이언트 VPN 서비스에서 전달된 클라이언트 인증서의 고유한 일반 이름을 사용하여 디바이스를 식별하고 디바이스 관리 솔루션에서 해당 규정 준수 태세 상태를 가져올 수 있습니다. 사용자 기반 인증과 결합된 상호 인증을 사용할 수 있습니다.

또는 Lambda 함수 자체에서 기본 태세 평가를 수행할 수 있습니다. 예를 들어 클라이언트 VPN 서비스가 Lambda 함수에 전달하는 `platform` 및 `platform-version` 필드를 평가할 수 있습니다.

> **Note**
>
> 연결 핸들러를 사용하여 최소 AWS Client VPN 애플리케이션 버전을 적용할 수 있지만 연결 핸들러`aws-client-version`의 필드는 AWS Client VPN 애플리케이션에만 적용할 수 있으며 사용자 디바이스의 환경 변수에서 채워집니다.

클라이언트 연결 핸들러 활성화

클라이언트 연결 핸들러를 활성화하려면 Client VPN 엔드포인트을 생성하거나 수정하고 Lambda 함수의 Amazon 리소스 이름(ARN)을 지정합니다. 자세한 내용은 AWS Client VPN엔드포인트 생성 및 AWS Client VPN 엔드포인트 수정 단원을 참조하십시오.

서비스 연결 역할

AWS Client VPN 는 AWSServiceRoleForClientVPNConnections라는 서비스 연결 역할을 계정에 자동으로 생성합니다. 역할에는 Client VPN 엔드포인트에 연결할 때 Lambda 함수를 호출할 수 있는 권한이 있습니다. 자세한 내용은 에 대한 서비스 연결 역할 사용 AWS Client VPN 단원을 참조하십시오.

연결 권한 부여 실패 모니터링

Client VPN 엔드포인트 연결의 연결 권한 부여 상태를 볼 수 있습니다. 자세한 정보는 AWS Client VPN 클라이언트 연결 보기을 참조하십시오.

클라이언트 연결 핸들러를 태세 평가에 사용하면 연결 로그에서 Client VPN 엔드포인트에 연결하는 디바이스의 태세 규정 준수 상태도 볼 수 있습니다. 자세한 정보는 AWS Client VPN 엔드포인트에 대한 연결 로깅을 참조하십시오.

디바이스가 연결 권한 부여에 실패하면 연결 로그의 `connection-attempt-failure-reason` 필드는 다음과 같은 실패 이유 중 하나를 반환합니다.

- `client-connect-failed` - Lambda 함수로 인해 연결을 설정할 수 없습니다.
- `client-connect-handler-timed-out` - Lambda 함수가 시간 초과되었습니다.
- `client-connect-handler-other-execution-error` - Lambda 함수에서 예기치 않은 오류가 발생했습니다.
- `client-connect-handler-throttled` - Lambda 함수가 조절되었습니다.
- `client-connect-handler-invalid-response` - Lambda 함수가 유효하지 않은 응답을 반환했습니다.

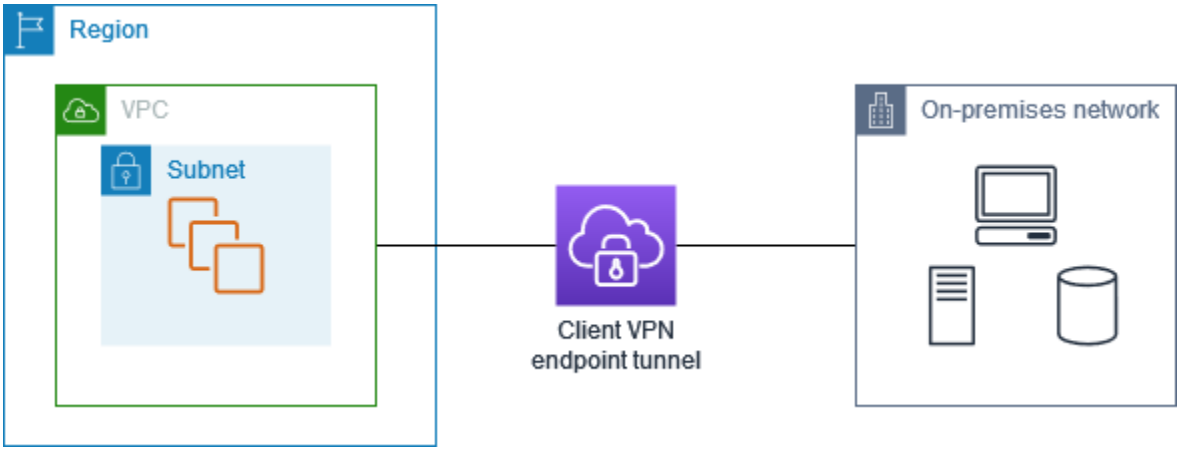
- `client-connect-handler-service-error` - 연결 시도 중에 서비스 측 오류가 발생했습니다.

AWS Client VPN 엔드포인트의 분할 터널

기본적으로 Client VPN 엔드포인트가 있는 경우 클라이언트의 모든 트래픽은 Client VPN 터널을 통해 라우팅됩니다. Client VPN 엔드포인트에서 분할 터널을 활성화하면 Client VPN 엔드포인트 라우팅 테이블의 경로가 Client VPN 엔드포인트에 연결된 디바이스로 푸시됩니다. 이렇게 하면 Client VPN 엔드포인트 라우팅 테이블의 경로와 일치하는 네트워크 대상 트래픽만 Client VPN 터널을 통해 라우팅됩니다.

모든 사용자 트래픽이 Client VPN 엔드포인트를 통해 라우팅되지 않도록 하려면 분할 터널 Client VPN 엔드포인트를 사용할 수 있습니다.

다음 예에서는 Client VPN 엔드포인트에서 분할 터널이 활성화됩니다. VPC(`172.31.0.0/16`)로 향하는 트래픽만 Client VPN 터널을 통해 라우팅됩니다. 온프레미스 리소스로 향하는 트래픽은 Client VPN 터널을 통해 라우팅되지 않습니다.



분할 터널의 이점

Client VPN 엔드포인트의 분할 터널은 다음과 같은 이점을 제공합니다.

- 목적지가 AWS인 트래픽만을 VPN 터널을 통과하도록 하여 클라이언트의 트래픽 라우팅을 최적화할 수 있습니다.
- AWS에서 송신하는 트래픽 양을 줄일 수 있고, 이에 따라 데이터 전송 비용을 절감할 수 있습니다.

라우팅 고려 사항

- 분할 터널 모드를 사용하면 VPN 연결이 설정될 때 Client VPN 엔드포인트의 라우팅 테이블에 있는 모든 경로가 클라이언트의 라우팅 테이블에 추가됩니다. 이 작업은 클라이언트의 라우팅 테이블을 `0.0.0.0/0` 항목으로 덮어써서 VPN을 통해 모든 트래픽을 라우팅하는 기본 동작과 다릅니다.

> **Note**
>
> 분할 터널 모드를 사용할 때 Client VPN 엔드포인트의 라우팅 테이블에 0.0.0.0/0 경로를 추가하면 연결이 중단될 수 있으므로 권장되지 않습니다.

- 분할 터널 모드가 활성화된 상태에서 Client VPN 엔드포인트 라우팅 테이블을 수정하면 모든 클라이언트 연결이 재설정됩니다.

분할 터널 활성화

기존 또는 새 Client VPN 엔드포인트에서 분할 터널을 활성화할 수 있습니다. 자세한 정보는 다음 주제를 참조하세요.

- AWS Client VPN엔드포인트 생성
- AWS Client VPN 엔드포인트 수정

AWS Client VPN 엔드포인트에 대한 연결 로깅

연결 로깅은 Client VPN 엔드포인트에 대한 연결 로그를 캡처할 수 있도록 해주는 AWS Client VPN의 기능입니다.

각 연결 로그에는 클라이언트(최종 사용자)가 Client VPN 엔드포인트에서 연결하거나 연결을 시도하거나 연결을 해제할 때의 연결 이벤트에 대한 정보를 캡처하는 연결 로그 항목이 포함되어 있습니다. 이 정보를 사용하여 포렌식을 실행하거나, Client VPN 엔드포인트가 어떻게 사용되고 있는지 분석하거나, 연결 문제를 디버깅할 수 있습니다.

연결 로깅은 AWS Client VPN을 사용할 수 있는 모든 리전에서 사용 가능합니다. 연결 로그는 계정의 CloudWatch Logs 로그 그룹에 게시됩니다.

> **Note**
>
> 실패한 상호 인증 시도는 로깅되지 않습니다.

연결 로그 항목

연결 로그 항목은 키-값 페어에 대한 JSON 형식 BLOB입니다. 다음은 연결 로그 항목의 예제입니다.

```
{
    "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"
    }
```

연결 로그 항목에는 다음 키가 포함되어 있습니다.

- `connection-log-type` - 연결 로그 항목의 유형입니다(`connection-attempt` 또는 `connection-reset`).
- `connection-attempt-status` - 연결 요청의 상태입니다(`successful`, `failed`, `waiting-for-assertion` 또는 `NA`).
- `connection-reset-status` - 연결 재설정 이벤트의 상태입니다(`NA` 또는 `assertion-received`).

- `connection-attempt-failure-reason` - 연결 실패의 원인입니다(해당하는 경우).
- `connection-id` - 연결의 ID입니다.
- `client-vpn-endpoint-id` - 연결이 수행된 Client VPN 엔드포인트의 ID입니다.
- `transport-protocol` - 연결에 사용된 전송 프로토콜입니다.
- `connection-start-time` - 연결의 시작 시간입니다.
- `connection-last-update-time` - 연결의 마지막 업데이트 시간입니다. (이 값은 로그에서 정기적으로 업데이트됩니다.)
- `client-ip` - Client VPN 엔드포인트에 대한 클라이언트 IPv4 CIDR 범위에서 할당되는 클라이언트의 IP 주소입니다.
- `common-name` - 인증서 기반 인증에 사용되는 인증서의 일반 이름입니다.
- `device-type` - 최종 사용자가 연결에 사용하는 디바이스의 유형입니다.
- `device-ip` - 디바이스의 퍼블릭 IP 주소입니다.
- `port` - 연결의 포트 번호입니다.
- `ingress-bytes` - 연결에 대한 수신(인바운드) 바이트 수입니다. (이 값은 로그에서 정기적으로 업데이트됩니다.)
- `egress-bytes` - 연결에 대한 송신(아웃바운드) 바이트 수입니다. (이 값은 로그에서 정기적으로 업데이트됩니다.)
- `ingress-packets` - 연결에 대한 수신(인바운드) 패킷 수입니다. (이 값은 로그에서 정기적으로 업데이트됩니다.)
- `egress-packets` - 연결에 대한 송신(아웃바운드) 패킷 수입니다. (이 값은 로그에서 정기적으로 업데이트됩니다.)
- `connection-end-time` - 연결의 종료 시간입니다. (연결이 아직 진행 중이거나 연결 시도가 실패한 경우 값은 NA입니다.)
- `posture-compliance-statuses` - 해당하는 경우 클라이언트 연결 처리기에서 반환하는 규정 준수 태세 상태입니다.
- `username` - 사용자 기반 인증(AD 또는 SAML)이 엔드포인트에 사용될 때 사용자 이름이 기록됩니다.
- `connection-duration-seconds` - 연결 기간(초)입니다. 'connection-start-time'과 'connection-end-time'의 차이와 같습니다.

연결 로깅 활성화에 대한 자세한 내용은 AWS Client VPN 연결 로그 단원을 참조하십시오.

Client VPN 확장 고려 사항

Client VPN 엔드포인트를 생성할 때, 지원하고자 하는 동시 VPN 연결의 최대 수를 고려하는 것이 좋습니다. 현재 지원하는 클라이언트 수, 그리고 필요한 경우 Client VPN 엔드포인트가 더 많은 수요에 부응하기 위해 규모를 조정할 수 있는지 여부를 고려해야 합니다.

다음은 Client VPN 엔드포인트 하나에서 지원할 수 있는 동시 VPN 연결의 최대 수에 영향을 미치는 요인입니다.

클라이언트 CIDR 범위 크기

Client VPN 엔드포인트를 생성할 때, 클라이언트 CIDR 범위를 지정해야 합니다. 이는 a/ 12부터 /22 넷마스크 사이의 IPv4 CIDR 블록입니다. Client VPN 엔드포인트에 대한 각각의 VPN 연결에 클라이언트 CIDR 범위의 고유한 IP 주소가 하나씩 할당됩니다. 클라이언트 CIDR 범위 내 주소 중 일부분은 Client VPN 엔드포인트의 가용성 모델을 지원하는 데도 사용되므로, 클라이언트에 할당될 수 없습니다. Client VPN 엔드포인트를 생성한 후에는 클라이언트 CIDR 범위를 변경할 수 없습니다.

일반적으로 Client VPN 엔드포인트에서 지원하고자 하는 IP 주소(및 그에 따른 동시 연결) 수의 두 배를 포함하는 클라이언트 CIDR 범위를 지정하는 것이 좋습니다.

연결된 서브넷 수

Client VPN 엔드포인트를 서브넷과 연결하면 사용자에게 Client VPN 엔드포인트에 대한 VPN 세션을 설정하도록 지원하는 것이 됩니다. Client VPN 엔드포인트 한 개에 여러 개의 서브넷을 연결하여 고가용성을 지향할 수 있으며, 이렇게 하면 추가적인 연결 용량을 지원할 수도 있습니다.

다음은 Client VPN 엔드포인트의 서브넷 연결 수를 바탕으로 지원되는 동시 VPN 연결 수를 나타낸 것입니다.

서브넷 연결	지원되는 연결 수
1	7,000
2	36,500
3	66,500
4	96,500
5	126,000

동일한 가용 영역의 여러 서브넷을 한 Client VPN 엔드포인트와 연결할 수 없습니다. 따라서, 서브넷 연결 수는 AWS 리전에서 이용 가능한 가용 영역의 수에도 좌우됩니다.

예를 들어 Client VPN 엔드포인트에 대하여 8,000개의 VPN 연결을 지원할 것으로 예상하는 경우, /18(IP 주소 16,384개)에 상당하는 최소 클라이언트 CIDR 범위 크기를 지정한 다음 해당 Client VPN 엔드포인트와 최소 2개의 서브넷을 연결합니다.

Client VPN 엔드포인트에 예상되는 VPN 연결 수를 잘 모르는 경우, 크기가 /16인 CIDR 블록 또는 그보다 크게 지정하는 것이 좋습니다.

클라이언트 CIDR 범위 및 대상 네트워크를 다룰 때 적용되는 규칙과 한계에 관한 자세한 내용은 사용에 대한 규칙 및 모범 사례 AWS Client VPN을(를) 참조하세요.

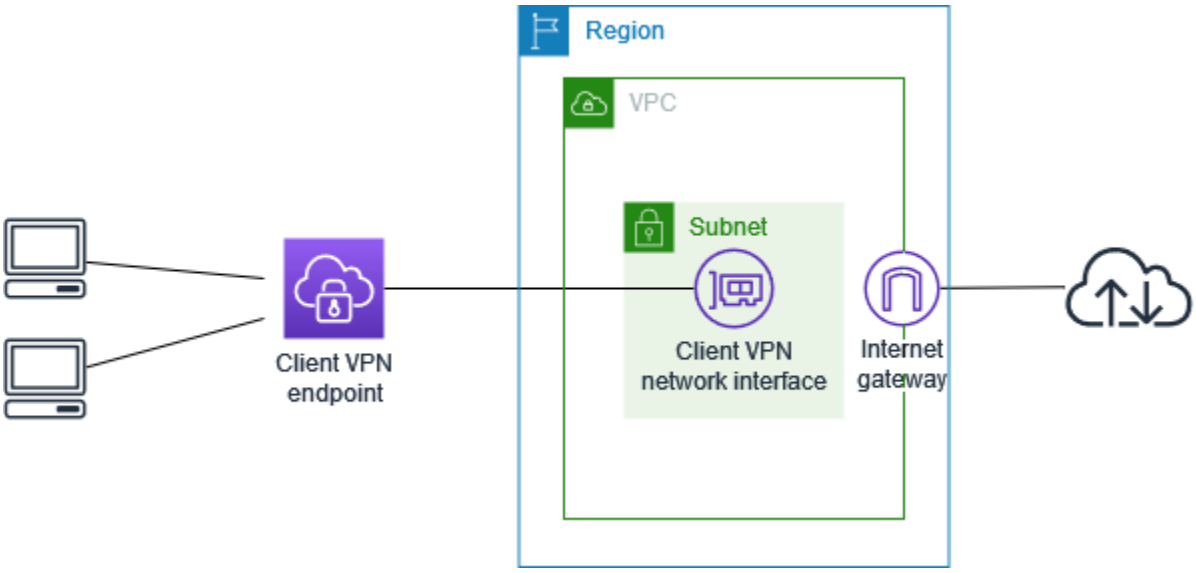
Client VPN 엔드포인트의 할당량에 대한 자세한 정보를 AWS Client VPN 할당량을(를) 참조하세요.

시작하기 AWS Client VPN

이 자습서에서는 다음을 수행하는 AWS Client VPN 엔드포인트를 생성합니다.

- 모든 클라이언트에게 단일 VPC에 대한 액세스를 제공합니다.
- 모든 클라이언트에게 인터넷에 대한 액세스를 제공합니다.
- 상호 인증을 사용합니다.

다음 다이어그램은 이 자습서를 완료한 후 VPC 및 Client VPN 엔드포인트의 구성을 나타냅니다.



단계(Steps)

- 사전 조건
- 1단계: 엔드포인트 유형 선택
- 2단계: 서버 및 클라이언트 인증서와 키 생성
- 3단계: Client VPN 엔드포인트 생성
- 4단계: 대상 네트워크 연결
- 5단계: VPC에 대한 권한 부여 규칙 추가
- 6단계: 인터넷에 대한 액세스 제공
- 7단계: 보안 그룹 요구 사항 확인
- 8단계: Client VPN 엔드포인트 구성 파일 다운로드
- 9단계: Client VPN 엔드포인트에 연결

사전 조건

이 자습서를 시작하기 전에 다음 사항을 확인해야 합니다.

- Client VPN 엔드포인트로 작업하는 데 필요한 권한.
- 인증서를 AWS Certificate Manager로 가져오는 데 필요한 권한.
- 하나 이상의 서브넷과 인터넷 게이트웨이가 있는 VPC. 서브넷과 연결된 라우팅 테이블에는 인터넷 게이트웨이에 대한 경로가 있어야 합니다.

1단계: 엔드포인트 유형 선택

Client VPN은 단일 VPC 액세스를 위한 VPC 서브넷 연결과 다중 VPC 및 하이브리드 네트워크 시나리오를 위한 Transit Gateway 연결이라는 두 가지 엔드포인트 유형을 지원합니다. 이 자습서에서는 VPC 관련 엔드포인트를 다룹니다. Transit Gateway 엔드포인트는 섹션을 참조하세요Client VPN과 Transit Gateway 통합.

2단계: 서버 및 클라이언트 인증서와 키 생성

이 자습서에서는 상호 인증을 사용합니다. 상호 인증에서는 Client VPN이 인증서를 사용하여 클라이언트와 Client VPN 엔드포인트 간에 인증을 수행합니다. 하나의 서버 인증서 및 키와 하나 이상의 클라이언트 인증서 및 키가 있어야 합니다. 최소한 서버 인증서를 AWS Certificate Manager (ACM)로 가져와서 Client VPN 엔드포인트를 생성할 때 지정해야 합니다. 클라이언트 인증서를 ACM으로 가져오는 것은 선택 사항입니다.

이 목적으로 사용할 인증서가 아직 없는 경우 OpenVPN easy-rsa 유틸리티를 사용하여 인증서를 생성할 수 있습니다. OpenVPN easy-rsa 유틸리티를 사용하여 서버 및 클라이언트 인증서와 키를 생성하고 ACM으로 가져오는 자세한 단계는 의 상호 인증 AWS Client VPN 단원을 참조하세요.

> **Note**
>
> 서버 인증서는 Client VPN 엔드포인트를 생성할 동일한 AWS 리전의 AWS Certificate Manager (ACM)으로 프로비저닝하거나 가져와야 합니다.

3단계: Client VPN 엔드포인트 생성

Client VPN 엔드포인트는 Client VPN 세션을 활성화하고 관리하기 위해 생성하고 구성하는 리소스입니다. 이는 모든 Client VPN 세션의 종료 지점입니다.

Client VPN 엔드포인트을 생성하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 클라이언트 VPN 엔드포인트(Client VPN Endpoints)를 선택한 다음 클라이언트 VPN 엔드포인트 생성(Create Client VPN endpoint)을 선택합니다.
3. (선택 사항) Client VPN 엔드포인트의 이름 태그와 설명을 입력합니다.
4. 클라이언트 IPv4 CIDR에서 클라이언트 IP 주소를 할당할 IP 주소 범위(CIDR 표기법)를 지정합니다.

   > **Note**
   >
   > 주소 범위는 Client VPN 엔드포인트와 연결될 대상 네트워크 주소 범위, VPC 주소 범위 또는 경로와 중복될 수 없습니다. 클라이언트 주소 범위는 최소 /22 이상이어야 하며 /12 CIDR 블록 크기를 넘지 않아야 합니다. Client VPN 엔드포인트를 생성한 후에는 클라이언트 주소 범위를 변경할 수 없습니다.

5. 서버 인증서 ARN에서 2단계에서 생성한 서버 인증서의 ARN을 선택합니다.
6. 인증 옵션(Authentication options)에서 상호 인증 사용(Use mutual authentication)을 선택한 다음 클라이언트 인증서 ARN(Client certificate ARN)에서 클라이언트 인증서로 사용할 인증서의 ARN을 선택합니다.

   서버 인증서와 클라이언트 인증서가 동일한 인증 기관(CA)에 의해 발급된 경우 서버 인증서 ARN을 서버 인증서와 클라이언트 인증서 모두에 지정할 수 있습니다. 이 시나리오에서는 서버 인증서에 해당하는 모든 클라이언트 인증서를 사용하여 인증할 수 있습니다.

7. (선택 사항) DNS 확인에 사용할 DNS 서버를 지정합니다. 사용자 지정 DNS 서버를 사용하려면 DNS Server 1 IP address(DNS 서버 1 IP 주소) 및 DNS Server 2 IP address(DNS 서버 2 IP 주소)에 사용할 DNS 서버의 IP 주소를 지정합니다. VPC DNS 서버를 사용하려면 DNS Server 1 IP address(DNS 서버 1 IP 주소) 또는 DNS Server 2 IP address(DNS 서버 2 IP 주소)에 IP 주소를 지정하고 VPC DNS 서버 IP 주소를 추가합니다.

> **Note**
>
> 클라이언트가 DNS 서버에 도달할 수 있는지 확인합니다.

8. 나머지 기본 설정을 그대로 두고 클라이언트 VPN 엔드포인트 생성(Create Client VPN endpoint)을 선택합니다.

Client VPN 엔드포인트을 생성한 후 상태는 `pending-associate`입니다. 하나 이상의 대상 네트워크를 연결한 이후에만 클라이언트가 VPN 연결을 설정할 수 있습니다.

Client VPN 엔드포인트에 지정할 수 있는 옵션에 대한 자세한 내용은 AWS Client VPN엔드포인트 생성 섹션을 참조하세요.

4단계: 대상 네트워크 연결

클라이언트가 VPN 세션을 설정할 수 있도록 하려면 대상 네트워크를 Client VPN 엔드포인트와 연결합니다. 대상 네트워크는 VPC 안의 서브넷입니다.

대상 네트워크를 Client VPN 엔드포인트에 연결하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 이전 절차에서 생성한 Client VPN 엔드포인트를 선택한 다음 대상 네트워크 연결(Target network associations), 대상 네트워크 연결(Associate target network)을 차례로 선택합니다.
4. VPC에서 서브넷이 있는 VPC를 선택합니다.
5. 연결할 서브넷 선택(Choose a subnet to associate)에서 Client VPN 엔드포인트에 연결할 서브넷을 선택합니다.
6. 대상 네트워크 연결(Associate target network)을 선택합니다.
7. 권한 부여 규칙에서 허용하는 경우, 하나의 서브넷 연결만으로도 클라이언트가 VPC의 전체 네트워크에 액세스할 수 있습니다. 추가 서브넷을 연결하여 가용 영역에 장애가 발생할 경우에도 고가용성을 제공할 수 있습니다.

첫 번째 서브넷을 Client VPN 엔드포인트와 연결하면 다음과 같은 결과가 발생합니다.

- Client VPN 엔드포인트의 상태가 `available`로 변경됩니다. 이제 클라이언트가 VPN 연결을 설정할 수 있지만, 권한 부여 규칙을 추가할 때까지는 VPC 내 리소스에 액세스할 수 없습니다.

- VPC의 로컬 라우팅이 Client VPN 엔드포인트 라우팅 테이블에 자동으로 추가됩니다.
- VPC의 기본 보안 그룹이 자동으로 Client VPN 엔드포인트에 적용됩니다.

5단계: VPC에 대한 권한 부여 규칙 추가

클라이언트가 VPC에 액세스하려면 Client VPN 엔드포인트의 라우팅 테이블에 VPC로 연결되는 경로가 있고 권한 부여 규칙이 있어야 합니다. 이전 단계에서 경로는 이미 자동으로 추가되었습니다. 이 자습서에서는 모든 사용자에게 VPC에 대한 액세스 권한을 부여합니다.

VPC에 대한 권한 부여 규칙을 추가하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 권한 부여 규칙을 추가할 Client VPN 엔드포인트를 선택합니다. 권한 부여 규칙(Authorization rules)을 선택한 다음 권한 부여 규칙 추가(Add authorization rule)를 선택합니다.
4. 액세스를 활성화할 대상 네트워크(Destination network to enable access)에 액세스를 허용할 네트워크의 CIDR을 입력합니다. 예를 들어, 전체 VPC에 대한 액세스를 허용하려면 VPC의 IPv4 CIDR 블록을 지정합니다.
5. 다음에 대한 액세스 권한 부여(Grant access to)에서 모든 사용자에게 액세스 허용(Allow access to all users)을 선택합니다.
6. (선택 사항) 설명(Description)에 권한 부여 규칙에 대한 간략한 설명을 입력합니다.
7. Add authorization rule(권한 부여 규칙 추가)을 선택합니다.

6단계: 인터넷에 대한 액세스 제공

AWS 서비스, 피어링된 VPC, 온프레미스 네트워크 및 인터넷과 같이 VPCs에 연결된 추가 네트워크에 대한 액세스를 제공할 수 있습니다. 각 추가 네트워크에 대해 Client VPN 엔드포인트 라우팅 테이블에 해당 네트워크 경로를 추가하고 권한 부여 규칙을 구성하여 클라이언트에 액세스 권한을 부여합니다.

이 자습서에서는 모든 사용자에게 인터넷과 VPC에 대한 액세스 권한을 부여합니다. VPC에 대한 액세스는 이미 구성했으므로 이 단계에서는 인터넷에 대한 액세스를 구성합니다.

인터넷 액세스를 제공하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.

2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 이 자습서를 위해 생성한 Client VPN 엔드포인트를 선택합니다. 라우팅 테이블(Route Table)을 선택한 다음 경로 생성(Create Route)을 선택합니다.
4. Route destination(라우팅 대상 주소)에 `0.0.0.0/0`을 입력합니다. 대상 네트워크 연결용 서브넷 ID(Subnet ID for target network association)에서 트래픽을 라우팅할 서브넷의 ID를 입력합니다.
5. Create Route(라우팅 생성)를 선택합니다.
6. 권한 부여 규칙(Authorization rules)을 선택한 다음 권한 부여 규칙 추가(Add authorization rule)를 선택합니다.
7. 액세스를 활성화할 대상 네트워크(Destination network to enable access)에 `0.0.0.0/0`을 입력하고 모든 사용자에게 액세스 허용(Allow access to all users)을 선택합니다.
8. Add authorization rule(권한 부여 규칙 추가)을 선택합니다.

7단계: 보안 그룹 요구 사항 확인

이 자습서에서는 3단계에서 Client VPN 엔드포인트를 생성하는 동안 보안 그룹이 지정되지 않았습니다. 즉, 대상 네트워크가 연결될 때 VPC의 기본 보안 그룹이 Client VPN 엔드포인트에 자동으로 적용됩니다. 따라서 VPC의 기본 보안 그룹이 Client VPN 엔드포인트에 연결됩니다.

다음 보안 그룹 요구 사항 확인

- 트래픽을 라우팅하는 서브넷과 연결된 보안 그룹(이 경우 기본 VPC 보안 그룹)이 인터넷으로의 아웃바운드 트래픽을 허용합니다. 이렇게 하려면 대상 `0.0.0.0/0`에 대한 모든 트래픽을 허용하는 아웃바운드 규칙을 추가합니다.
- VPC의 리소스에 대한 보안 그룹에 Client VPN 엔드포인트에 적용되는 보안 그룹(이 경우 기본 VPC 보안 그룹)에서의 액세스를 허용하는 규칙이 있습니다. 이렇게 하면 클라이언트가 VPC의 리소스에 액세스할 수 있습니다.

자세한 내용은 보안 그룹 단원을 참조하십시오.

8단계: Client VPN 엔드포인트 구성 파일 다운로드

다음 단계에서는 Client VPN 엔드포인트 구성 파일을 다운로드하고 준비합니다. 구성 파일에는 VPN 연결을 설정하는 데 필요한 Client VPN 엔드포인트 세부 정보 및 인증서 정보가 포함되어 있습니다. Client VPN 엔드포인트에 연결해야 하는 최종 사용자에게 이 파일을 제공합니다. 최종 사용자는 이 파일을 사용하여 VPN 클라이언트 애플리케이션을 구성합니다.

Client VPN 엔드포인트 구성 파일을 다운로드하고 준비하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 이 자습서를 위해 생성한 Client VPN 엔드포인트를 선택하고 클라이언트 구성 다운로드(Download client configuration)를 선택합니다.
4. 2단계에서 생성된 클라이언트 인증서와 키를 찾습니다. 클라이언트 인증서 및 키는 복제된 OpenVPN easy-rsa 리포지토리의 다음 위치에서 찾을 수 있습니다.

   - 클라이언트 인증서 - `easy-rsa/easyrsa3/pki/issued/client1.domain.tld.crt`
   - 클라이언트 키 - `easy-rsa/easyrsa3/pki/private/client1.domain.tld.key`
5. 원하는 텍스트 편집기를 사용하여 Client VPN 엔드포인트 구성 파일을 엽니다. `<cert></cert>` 및 `<key></key>` 태그를 파일에 추가합니다. 클라이언트 인증서의 내용과 프라이빗 키의 내용을 다음과 같이 해당 태그 사이에 배치합니다.

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

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

6. Client VPN 엔드포인트 구성 파일을 저장하고 닫습니다.
7. Client VPN 엔드포인트 구성 파일을 최종 사용자에게 배포합니다.

Client VPN 엔드포인트 구성 파일에 대한 자세한 내용은 AWS Client VPN 엔드포인트 구성 파일 내보내기 단원을 참조하십시오.

9단계: Client VPN 엔드포인트에 연결

AWS 제공된 클라이언트 또는 다른 OpenVPN 기반 클라이언트 애플리케이션과 방금 생성한 구성 파일을 사용하여 Client VPN 엔드포인트에 연결할 수 있습니다. 자세한 내용은 AWS Client VPN 사용 설명서를 참조하십시오.

작업 AWS Client VPN

다음 주제에서는 Client VPN을 사용하는 데 필요한 기본 관리 작업에 대해 설명합니다.

- 셀프 서비스 포털 액세스 — 클라이언트가 Client VPN 엔드포인트 구성 파일을 직접 다운로드할 수 있도록 Client VPN 셀프 서비스 포털에 대한 액세스를 구성합니다. 셀프 서비스 포털에 액세스하는 방법에 대한 자세한 내용은 the section called “셀프 서비스 포털 액세스” 섹션을 참조하세요.
- 권한 부여 규칙 — 지정된 네트워크에 대한 클라이언트 액세스를 제어하는 권한 부여 규칙을 추가합니다. 권한 부여 규칙 추가에 대한 자세한 내용은 the section called “권한 부여 규칙” 섹션을 참조하세요.
- 클라이언트 인증서 해지 목록 — 클라이언트 인증서 해지 목록을 사용하여 Client VPN 엔드포인트에 대한 액세스를 취소합니다. 클라이언트 인증서 해지 목록에 대한 자세한 내용은 the section called “클라이언트 인증서 해지 목록” 섹션을 참조하세요.
- 클라이언트 연결 — Client VPN 엔드포인트에 대한 클라이언트 연결을 보거나 종료합니다. 클라이언트 연결을 보거나 종료하는 방법에 대한 자세한 내용은 the section called “클라이언트 연결” 섹션을 참조하세요.
- 클라이언트 로그인 배너 — VPN 세션이 설정되면 Client VPN 데스크톱 애플리케이션에 텍스트 배너를 추가합니다. 규정 및 규정 준수 요구 사항을 충족하기 위해 텍스트 배너를 사용할 수 있습니다. 로그인 배너에 대한 자세한 내용은 the section called “클라이언트 로그인 배너” 섹션을 참조하세요.
- 클라이언트 경로 강제 적용 - VPN을 통해 연결된 디바이스에 관리자 정의 경로를 적용합니다. 클라이언트 경로 강제 적용에 대한 자세한 내용은 섹션을 참조하세요the section called “클라이언트 경로 강제 적용”.
- Client VPN 엔드포인트 — Client VPN 엔드포인트를 구성하여 모든 VPN 세션을 관리하고 제어합니다. 엔드포인트 구성에 대한 자세한 내용은 the section called “엔드포인트” 섹션을 참조하세요.
- 연결 로그 — 새 Client VPN 엔드포인트 또는 기존 Client VPN 엔드포인트에 연결 로깅을 활성화하고 연결 로그 캡처를 시작할 수 있습니다. 연결 로깅에 대한 자세한 내용은 the section called “연결 로그” 섹션을 참조하세요.
- 클라이언트 구성 파일 내보내기 — 클라이언트 VPN 클라이언트가 VPN 연결을 설정하는 데 필요한 클라이언트 구성 파일을 구성합니다. 파일을 구성한 후 클라이언트에 배포하기 위해 다운로드(내보내기)합니다. 클라이언트 구성 파일 내보내기에 대한 자세한 내용은 the section called “클라이언트 구성 파일 내보내기” 섹션을 참조하세요.
- 라우팅 — 각 Client VPN 라우팅의 권한 부여 규칙을 구성하여 대상 네트워크에 액세스할 수 있는 클라이언트를 지정합니다. 권한 부여 규칙 구성에 대한 자세한 내용은 the section called “권한 부여 규칙” 섹션을 참조하세요.

- 대상 네트워크 - VPC 서브넷을 연결하거나 AWS Transit Gateway에 직접 연결하여 클라이언트가 VPN 연결을 설정하고 연결할 수 있도록 합니다. 대상 네트워크에 대한 자세한 내용은 the section called “대상 네트워크” 섹션을 참조하세요. Transit Gateway 통합에 대한 자세한 내용은 섹션을 참조하세요the section called “Client VPN과 Transit Gateway 통합”.
- 최대 VPN 세션 기간 — 보안 및 규정 준수 요구 사항을 충족하기 위해 최대 VPN 세션 기간에 대한 옵션을 설정합니다. 최대 VPN 세션 기간에 대한 자세한 내용은 the section called “최대 VPN 세션 기간” 섹션을 참조하세요.

셀프 서비스 포털에 대한 AWS Client VPN 액세스

Client VPN 엔드포인트에 대해 셀프 서비스 포털을 활성화한 경우 클라이언트에 셀프 서비스 포털 URL을 제공할 수 있습니다. 클라이언트는 웹 브라우저에서 포털에 액세스하고 사용자 기반 자격 증명을 사용하여 로그인할 수 있습니다. 포털에서 클라이언트는 Client VPN 엔드포인트 구성 파일을 다운로드할 수 있으며 최신 버전의 AWS 제공 클라이언트를 다운로드할 수 있습니다.

다음 규칙이 적용됩니다.

- 상호 인증을 사용하여 인증하는 클라이언트에는 셀프 서비스 포털을 사용할 수 없습니다.
- 셀프 서비스 포털에서 사용할 수 있는 구성 파일은 Amazon VPC 콘솔 또는 를 사용하여 내보내는 구성 파일과 동일합니다AWS CLI 구성 파일을 클라이언트에 배포하기 전에 사용자 지정해야 하는 경우 사용자 지정된 파일을 클라이언트에 직접 배포해야 합니다.
- Client VPN 엔드포인트에 대해 셀프 서비스 포털 옵션을 활성화해야 합니다. 그렇지 않으면 클라이언트가 포털에 액세스할 수 없습니다. 이 옵션을 활성화하지 않은 경우 Client VPN 엔드포인트를 수정하여 활성화할 수 있습니다.

셀프 서비스 포털 옵션을 활성화한 후 클라이언트에 다음 URL 중 하나를 제공합니다.

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

  클라이언트가 이 URL을 사용하여 포털에 액세스하는 경우 로그인하려면 먼저 Client VPN 엔드포인트의 ID를 입력해야 합니다.

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

  이전 URL의 *<endpoint-id>*를 Client VPN 엔드포인트의 ID로 바꿉니다(예: `cvpn-endpoint-0123456abcd123456`).

describe-client-vpn-endpoints AWS CLI 명령의 출력에서 셀프 서비스 포털의 URL도 볼 수 있습니다. 또는 Amazon VPC 콘솔의 클라이언트 VPN 엔드포인트(Client VPN Endpoints) 페이지에 있는 세부 정보(Details) 탭에서 URL을 사용할 수 있습니다.

연동 인증에 사용할 셀프 서비스 포털을 구성하는 방법에 대한 자세한 내용은 셀프 서비스 포털에 대한 지원 단원을 참조하십시오

AWS Client VPN 권한 부여 규칙

권한 부여 규칙은 네트워크에 대한 액세스 권한을 부여하는 방화벽의 역할을 합니다. 권한 부여 규칙을 추가하여 특정 클라이언트에게 지정된 네트워크에 대한 액세스 권한을 부여합니다. 액세스 권한을 부여할 각 네트워크마다 권한 부여 규칙이 있어야 합니다. 콘솔과 AWS CLI를 사용하여 Client VPN 엔드포인트에 권한 부여 규칙을 추가할 수 있습니다.

> **Note**
>
> Client VPN에서는 권한 부여 규칙을 평가할 때 가장 긴 접두사 일치를 사용합니다. 자세한 내용은 Amazon VPC 사용 설명서의 문제 해결 주제 문제 해결 AWS Client VPN: Active Directory 그룹에 대한 권한 부여 규칙이 예상대로 작동하지 않음 및 경로 우선 순위를 참조하십시오.

권한 부여 규칙을 이해하기 위한 중요 사항

다음은 권한 부여 규칙의 몇 가지 동작에 대한 설명입니다.

- 대상 네트워크에 대한 액세스를 허용하려면 권한 부여 규칙을 명시적으로 추가해야 합니다. 기본 동작은 액세스를 거부하는 것입니다.
- 대상 네트워크에 대한 액세스를 제한하는 권한 부여 규칙은 추가할 수 없습니다.
- `0.0.0.0/0` CIDR은 특수한 경우로 처리됩니다. 이것은 권한 부여 규칙이 생성된 순서에 관계없이 마지막으로 처리됩니다.
- `0.0.0.0/0` CIDR은 '모든 대상' 또는 '다른 권한 부여 규칙에 의해 정의되지 않은 대상'으로 생각할 수 있습니다.
- 가장 긴 접두사 일치가 우선적으로 적용되는 규칙입니다.

주제

- Client VPN 권한 부여 규칙에 대한 예제 시나리오

- AWS Client VPN 엔드포인트에 권한 부여 규칙 추가
- AWS Client VPN 엔드포인트에서 권한 부여 규칙 제거
- AWS Client VPN 권한 부여 규칙 보기

Client VPN 권한 부여 규칙에 대한 예제 시나리오

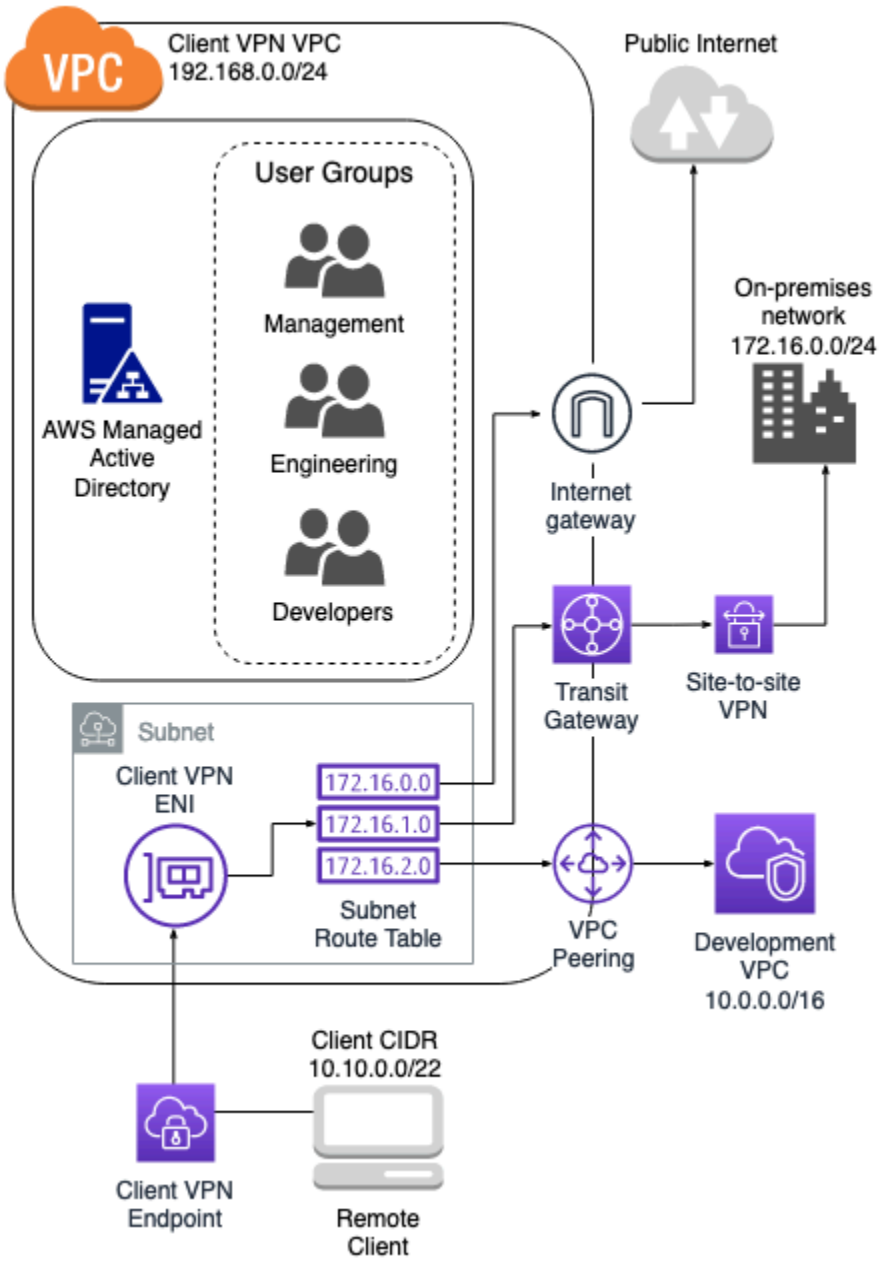
이 섹션에서는 권한 부여 규칙의 작동 방식을 설명합니다 AWS Client VPN. 여기에는 권한 부여 규칙을 이해하기 위한 중요 사항, 예제 아키텍처 및 예제 아키텍처에 매핑되는 예제 시나리오에 대한 설명이 포함됩니다.

시나리오

- the section called “아키텍처 예”
- the section called “단일 대상에 대한 액세스”
- the section called “대상(0.0.0.0/0) CIDR 사용”
- the section called “더 긴 IP 접두사 일치”
- the section called “겹치는 CIDR(동일한 그룹)”
- the section called “추가 0.0.0.0/0 규칙”
- the section called “192.168.0.0/24에 대한 규칙 추가”
- the section called “SAML 연동 인증”
- the section called “모든 사용자 그룹의 액세스”

권한 부여 규칙 시나리오의 아키텍처 예

다음 다이어그램은 이 섹션에 있는 예제 시나리오에 사용되는 아키텍처의 예를 보여줍니다.



단일 대상에 대한 액세스

규칙 설명	그룹 ID	모든 사용자에게 액세스 허용	대상 CIDR
엔지니어링 그룹에 온프레미스 네트워크에 대한 액세스 제공	S-xxxxx14	False	172.16.0.0/24

규칙 설명	그룹 ID	모든 사용자에게 액세스 허용	대상 CIDR
개발 그룹에 개발 VPC에 대한 액세스 제공	S-xxxxx15	False	10.0.0.0/16
관리자 그룹에 Client VPN VPC에 대한 액세스 제공	S-xxxxx16	False	192.168.0.0/24

결과적 동작

- 엔지니어링 그룹은 `172.16.0.0/24`에만 액세스할 수 있습니다.
- 개발 그룹은 `10.0.0.0/16`에만 액세스할 수 있습니다.
- 관리자 그룹은 `192.168.0.0/24`에만 액세스할 수 있습니다.
- 다른 모든 트래픽은 Client VPN 엔드포인트에 의해 삭제됩니다.

> **Note**
>
> 이 시나리오에서는 어떤 사용자 그룹도 퍼블릭 인터넷에 액세스할 수 없습니다.

대상(0.0.0.0/0) CIDR 사용

규칙 설명	그룹 ID	모든 사용자에게 액세스 허용	대상 CIDR
엔지니어링 그룹에 온프레미스 네트워크에 대한 액세스 제공	S-xxxxx14	False	172.16.0.0/24
개발 그룹에 개발 VPC에 대한 액세스 제공	S-xxxxx15	False	10.0.0.0/16

규칙 설명	그룹 ID	모든 사용자에게 액세스 허용	대상 CIDR
관리자 그룹에 모든 대상에 대한 액세스 제공	S-xxxxx16	False	0.0.0.0/0

결과적 동작

- 엔지니어링 그룹은 `172.16.0.0/24`에만 액세스할 수 있습니다.
- 개발 그룹은 `10.0.0.0/16`에만 액세스할 수 있습니다.
- 관리자 그룹은 퍼블릭 인터넷 및 `192.168.0.0/24`에 액세스할 수 있지만 `172.16.0.0/24` 또는 `10.0.0/16`에는 액세스할 수 없습니다.

> **Note**
>
> 이 시나리오에서는 `192.168.0.0/24`를 참조하는 규칙이 없기 때문에 해당 네트워크에 대한 액세스도 `0.0.0.0/0` 규칙에 의해 제공됩니다.
> `0.0.0.0/0`을 포함하는 규칙은 규칙이 생성된 순서에 관계없이 항상 마지막으로 평가됩니다. 이 때문에 `0.0.0.0/0` 이전에 평가된 규칙은 `0.0.0.0/0`이 액세스 권한을 부여하는 네트워크를 결정하는 역할을 합니다.

더 긴 IP 접두사 일치

규칙 설명	그룹 ID	모든 사용자에게 액세스 허용	대상 CIDR
엔지니어링 그룹에 온프레미스 네트워크에 대한 액세스 제공	S-xxxxx14	False	172.16.0.0/24
개발 그룹에 개발 VPC에 대한 액세스 제공	S-xxxxx15	False	10.0.0.0/16

규칙 설명	그룹 ID	모든 사용자에게 액세스 허용	대상 CIDR
관리자 그룹에 모든 대상에 대한 액세스 제공	S-xxxxx16	False	0.0.0.0/0
관리자 그룹에 개발 VPC의 단일 호스트에 대한 액세스 제공	S-xxxxx16	False	10.0.2.119/32

결과적 동작

- 엔지니어링 그룹은 `172.16.0.0/24`에만 액세스할 수 있습니다.
- 개발 그룹은 단일 호스트 `10.0.2.119/32`를 제외하고 `10.0.0.0/16`에 액세스할 수 있습니다.
- 관리자 그룹은 퍼블릭 인터넷, `192.168.0.0/24` 및 개발 VPC 내의 단일 호스트(`10.0.2.119/32`)에 액세스할 수 있지만 `172.16.0.0/24` 또는 개발 VPC의 나머지 호스트에는 액세스할 수 없습니다.

> **Note**
>
> 여기서는 긴 IP 접두사를 가진 규칙이 더 짧은 IP 접두사를 가진 규칙보다 우선적으로 적용되는 방식을 볼 수 있습니다. 개발 그룹이 `10.0.2.119/32`에 액세스할 수 있도록 하려면 개발 팀에 `10.0.2.119/32`에 대한 액세스 권한을 부여하는 규칙을 추가해야 합니다.

겹치는 CIDR(동일한 그룹)

규칙 설명	그룹 ID	모든 사용자에게 액세스 허용	대상 CIDR
엔지니어링 그룹에 온프레미스 네트워크에 대한 액세스 제공	S-xxxxx14	False	172.16.0.0/24
	S-xxxxx15	False	10.0.0.0/16

규칙 설명	그룹 ID	모든 사용자에게 액세스 허용	대상 CIDR
개발 그룹에 개발 VPC에 대한 액세스 제공			
관리자 그룹에 모든 대상에 대한 액세스 제공	S-xxxxx16	False	0.0.0.0/0
관리자 그룹에 개발 VPC의 단일 호스트에 대한 액세스 제공	S-xxxxx16	False	10.0.2.119/32
엔지니어링 그룹에 온프레미스 네트워크 내 소규모 서브넷에 대한 액세스 제공	S-xxxxx14	False	172.16.0.128/25

결과적 동작

- 개발 그룹은 단일 호스트 `10.0.2.119/32`를 제외하고 `10.0.0.0/16`에 액세스할 수 있습니다.
- 관리자 그룹은 퍼블릭 인터넷, `192.168.0.0/24` 및 `10.0.0.0/16` 네트워크 내의 단일 호스트(`10.0.2.119/32`)에 액세스할 수 있지만 `172.16.0.0/24` 또는 `10.0.0.0/16` 네트워크의 나머지 호스트에는 액세스할 수 없습니다.
- 엔지니어링 그룹은 보다 구체적인 서브넷 `172.16.0.128/25`를 포함하여 `172.16.0.0/24`에 액세스할 수 있습니다.

추가 0.0.0.0/0 규칙

규칙 설명	그룹 ID	모든 사용자에게 액세스 허용	대상 CIDR
	S-xxxxx14	False	172.16.0.0/24

규칙 설명	그룹 ID	모든 사용자에게 액세스 허용	대상 CIDR
엔지니어링 그룹에 온프레미스 네트워크에 대한 액세스 제공			
개발 그룹에 개발 VPC에 대한 액세스 제공	S-xxxxx15	False	10.0.0.0/16
관리자 그룹에 모든 대상에 대한 액세스 제공	S-xxxxx16	False	0.0.0.0/0
관리자 그룹에 개발 VPC의 단일 호스트에 대한 액세스 제공	S-xxxxx16	False	10.0.2.119/32
엔지니어링 그룹에 온프레미스 네트워크 내 소규모 서브넷에 대한 액세스 제공	S-xxxxx14	False	172.16.0.128/25
엔지니어링 그룹에 모든 대상에 대한 액세스 제공	S-xxxxx14	False	0.0.0.0/0

결과적 동작

- 개발 그룹은 단일 호스트 10.0.2.119/32를 제외하고 10.0.0.0/16에 액세스할 수 있습니다.
- 관리자 그룹은 퍼블릭 인터넷, 192.168.0.0/24 및 10.0.0.0/16 네트워크 내의 단일 호스트(10.0.2.119/32)에 액세스할 수 있지만 172.16.0.0/24 또는 10.0.0.0/16 네트워크의 나머지 호스트에는 액세스할 수 없습니다.
- 엔지니어링 그룹은 보다 구체적인 서브넷 172.16.0.128/25를 포함하여 퍼블릭 인터넷, 192.168.0.0/24 및 172.16.0.0/24에 액세스할 수 있습니다.

> **Note**
>
> 이제 엔지니어링 그룹과 관리자 그룹 모두 192.168.0.0/24에 액세스할 수 있습니다. 두 그룹 모두 0.0.0.0/0(모든 대상)에 액세스할 수 있는 동시에 192.168.0.0/24를 참조하는 다른 규칙이 없기 때문입니다.

192.168.0.0/24에 대한 규칙 추가

규칙 설명	그룹 ID	모든 사용자에게 액세스 허용	대상 CIDR
엔지니어링 그룹에 온프레미스 네트워크에 대한 액세스 제공	S-xxxxx14	False	172.16.0.0/24
개발 그룹에 개발 VPC에 대한 액세스 제공	S-xxxxx15	False	10.0.0.0/16
관리자 그룹에 모든 대상에 대한 액세스 제공	S-xxxxx16	False	0.0.0.0/0
관리자 그룹에 개발 VPC의 단일 호스트에 대한 액세스 제공	S-xxxxx16	False	10.0.2.119/32
엔지니어링 그룹에 온프레미스 네트워크의 서브넷에 대한 액세스 제공	S-xxxxx14	False	172.16.0.128/25
엔지니어링 그룹에 모든 대상에 대한 액세스 제공	S-xxxxx14	False	0.0.0.0/0

규칙 설명	그룹 ID	모든 사용자에게 액세스 허용	대상 CIDR
관리자 그룹에 Client VPN VPC에 대한 액세스 제공	S-xxxxx16	False	192.168.0.0/24

결과적 동작

- 개발 그룹은 단일 호스트 `10.0.2.119/32`를 제외하고 `10.0.0.0/16`에 액세스할 수 있습니다.
- 관리자 그룹은 퍼블릭 인터넷, `192.168.0.0/24` 및 `10.0.0.0/16` 네트워크 내의 단일 호스트(`10.0.2.119/32`)에 액세스할 수 있지만 `172.16.0.0/24` 또는 `10.0.0.0/16` 네트워크의 나머지 호스트에는 액세스할 수 없습니다.
- 엔지니어링 그룹은 퍼블릭 인터넷, `172.16.0.0/24` 및 `172.16.0.128/25`에 액세스할 수 있습니다.

> **Note**
>
> 관리자 그룹이 `192.168.0.0/24`에 액세스하도록 규칙을 추가하면 개발 그룹이 해당 대상 네트워크에 더 이상 액세스할 수 없게 됩니다.

SAML 연동 인증

규칙 설명	그룹 ID	모든 사용자에게 액세스 허용	대상 CIDR
엔지니어링 그룹에 온프레미스 네트워크에 대한 액세스 제공	엔지니어링	False	172.16.0.0/24
개발 그룹에 개발 VPC에 대한 액세스 제공	개발자	False	10.0.0.0/16

규칙 설명	그룹 ID	모든 사용자에게 액세스 허용	대상 CIDR
관리자 그룹에 Client VPN VPC에 대한 액세스 제공	관리자	False	192.168.0.0/24

결과적 동작

- '엔지니어링' 그룹 속성으로 SAML을 통해 인증된 사용자는 `172.16.0.0/24`에만 액세스할 수 있습니다.
- '개발자' 그룹 속성으로 SAML을 통해 인증된 사용자는 `10.0.0.0/16`에만 액세스할 수 있습니다.
- '관리자' 그룹 속성으로 SAML을 통해 인증된 사용자는 `192.168.0.0/24`에만 액세스할 수 있습니다.
- 다른 모든 트래픽은 Client VPN 엔드포인트에 의해 삭제됩니다.

> **Note**
>
> SAML 연동 인증을 사용하는 경우 그룹 ID 필드는 사용자의 그룹 멤버십을 식별하는 SAML 속성 값에 해당합니다. 이 속성은 SAML ID 공급자에서 구성되며 인증 중에 Client VPN으로 전달됩니다.

모든 사용자 그룹의 액세스

규칙 설명	그룹 ID	모든 사용자에게 액세스 허용	대상 CIDR
엔지니어링 그룹에 온프레미스 네트워크에 대한 액세스 제공	S-xxxxx14	False	172.16.0.0/24
개발 그룹에 개발 VPC에 대한 액세스 제공	S-xxxxx15	False	10.0.0.0/16

규칙 설명	그룹 ID	모든 사용자에게 액세스 허용	대상 CIDR
관리자 그룹에 모든 대상에 대한 액세스 제공	S-xxxxx16	False	0.0.0.0/0
관리자 그룹에 개발 VPC의 단일 호스트에 대한 액세스 제공	S-xxxxx16	False	10.0.2.119/32
엔지니어링 그룹에 온프레미스 네트워크의 서브넷에 대한 액세스 제공	S-xxxxx14	False	172.16.0.128/25
엔지니어링 그룹에 모든 네트워크에 대한 액세스 제공	S-xxxxx14	False	0.0.0.0/0
관리자 그룹에 Client VPN VPC에 대한 액세스 제공	S-xxxxx16	False	192.168.0.0/24
모든 그룹에 액세스 제공	해당 사항 없음	True	0.0.0.0/0

결과적 동작

- 개발 그룹은 단일 호스트 `10.0.2.119/32`를 제외하고 `10.0.0.0/16`에 액세스할 수 있습니다.
- 관리자 그룹은 퍼블릭 인터넷, `192.168.0.0/24` 및 `10.0.0.0/16` 네트워크 내의 단일 호스트(`10.0.2.119/32`)에 액세스할 수 있지만 `172.16.0.0/24` 또는 `10.0.0.0/16` 네트워크의 나머지 호스트에는 액세스할 수 없습니다.
- 엔지니어링 그룹은 퍼블릭 인터넷, `172.16.0.0/24` 및 `172.16.0.128/25`에 액세스할 수 있습니다.

- 다른 모든 사용자 그룹(예: '관리자 그룹')은 퍼블릭 인터넷에 액세스할 수 있지만 다른 규칙에 정의된 다른 대상 네트워크에는 액세스할 수 없습니다.

AWS Client VPN 엔드포인트에 권한 부여 규칙 추가

AWS Management Console을 사용하여 Client VPN 엔드포인트에 대한 액세스 권한을 부여하거나 제한하는 권한 부여 규칙을 추가할 수 있습니다. 권한 부여 규칙은 Amazon VPC 콘솔을 사용하거나 명령줄 또는 API를 사용하여 Client VPN 엔드포인트에 추가할 수 있습니다.

를 사용하여 Client VPN 엔드포인트에 권한 부여 규칙을 추가하려면 AWS Management Console

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 권한 부여 규칙을 추가할 Client VPN 엔드포인트를 선택하고 권한 부여 규칙(Authorization rules), 권한 부여 규칙 추가(Add authorization rule)를 차례로 선택합니다.
4. 액세스를 활성화할 대상 네트워크(Destination network to enable access)에서 사용자가 액세스하려는 네트워크의 IP 주소(예: VPC의 CIDR 블록)를 CIDR 표기법으로 입력합니다.
5. 지정된 네트워크에 액세스하도록 허용되는 클라이언트를 지정합니다. For grant access to(액세스 권한 부여)에서 다음 중 하나를 수행합니다.

   - 모든 클라이언트에게 액세스 권한을 부여하려면 Allow access to all users(모든 사용자에게 액세스 허용)를 선택합니다.
   - 특정 클라이언트에 대한 액세스를 제한하려면 특정 액세스 그룹의 사용자에게 액세스 허용을 선택한 다음 액세스 그룹 ID에 액세스 권한을 부여할 그룹의 ID를 입력합니다. 예를 들어, Active Directory 그룹의 보안 식별자(SID) 또는 SAML 기반 자격 증명 공급자(IdP)에 정의된 그룹의 ID/이름입니다.
     - (Active Directory) SID를 가져오려면 Microsoft Powershell Get-ADGroup cmdlet를 사용합니다. 예를 들면 다음과 같습니다.

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

       또는 Active Directory 사용자 및 컴퓨터 도구를 열고 그룹의 속성을 보고 속성 편집기 탭으로 이동한 다음 `objectSID`에 대한 값을 가져옵니다. 필요한 경우 먼저 뷰, 고급 기능을 선택하여 속성 편집기 탭을 활성화합니다.
     - (SAML 기반 연동 인증) 그룹 ID/이름은 SAML 어설션에 반환된 그룹 속성 정보와 일치해야 합니다.

6. 설명에 권한 부여 규칙에 대한 간략한 설명을 입력합니다.
7. Add authorization rule(권한 부여 규칙 추가)을 선택합니다.

Client VPN 엔드포인트에 권한 부여 규칙을 추가하려면(AWS CLI)

authorize-client-vpn-ingress 명령을 사용합니다.

AWS Client VPN 엔드포인트에서 권한 부여 규칙 제거

콘솔 및 AWS CLI를 사용하여 특정 Client VPN 엔드포인트의 권한 부여 규칙을 제거할 수 있습니다.

권한 부여 규칙을 제거하려면(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 권한 부여 규칙이 추가된 Client VPN 엔드포인트를 선택하고 권한 부여 규칙을 선택합니다.
4. 삭제할 권한 부여 규칙을 선택한 다음 권한 부여 규칙 제거를 선택한 다음, 다시 권한 부여 규칙 제거를 선택하여 삭제를 확인합니다.

권한 부여 규칙을 제거하려면(AWS CLI)

revoke-client-vpn-ingress 명령을 사용합니다.

AWS Client VPN 권한 부여 규칙 보기

콘솔 및 를 사용하여 특정 Client VPN 엔드포인트의 권한 부여 규칙을 볼 수 있습니다AWS CLI

권한 부여 규칙을 보는 방법(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 권한 부여 규칙을 볼 Client VPN 엔드포인트를 선택하고 권한 부여 규칙(Authorization rules)을 선택합니다.

권한 부여 규칙을 보려면(AWS CLI)

describe-client-vpn-authorization-rules 명령을 사용합니다.

AWS Client VPN 클라이언트 인증서 해지 목록

Client VPN 클라이언트 인증서 해지 목록을 사용하여 특정 클라이언트 인증서의 Client VPN 엔드포인트에 대한 액세스를 취소합니다. 해지 목록을 생성하거나 기존 목록을 가져올 수 있습니다. 현재 목록을 해지 목록 파일로 내보낼 수도 있습니다. 목록 생성은 Linux/macOS 또는 Windows에서 OpenVPN 소프트웨어를 사용하여 수행됩니다. Amazon VPC 콘솔 또는 AWS CLI를 사용하여 가져오기 및 내보내기를 수행할 수 있습니다.

서버와 클라이언트 인증서 및 키 생성에 대한 자세한 내용은 의 상호 인증 AWS Client VPN 단원을 참조하십시오.

> **Note**
>
> 클라이언트 인증서 취소 목록이 만료된 경우 Client VPN 엔드포인트에 연결할 수 없습니다. 새 항목을 생성하여 Client VPN 엔드포인트로 가져와야 합니다.

클라이언트 인증서 해지 목록에는 제한된 수의 항목만 추가할 수 있습니다. 해지 목록에 추가할 수 있는 항목 수에 대한 자세한 내용은 Client VPN 할당량 섹션을 참조하세요.

태스크

- AWS Client VPN 클라이언트 인증서 해지 목록 생성
- AWS Client VPN 클라이언트 인증서 해지 목록 가져오기
- AWS Client VPN 클라이언트 인증서 해지 목록 내보내기

AWS Client VPN 클라이언트 인증서 해지 목록 생성

Linux/macOS 또는 Windows 운영 체제에서 Client VPN 인증서 해지 목록을 생성할 수 있습니다. 해지 목록을 사용하여 특정 인증서의 Client VPN 엔드포인트에 대한 액세스를 취소합니다. 클라이언트 인증서 해지 목록에 대한 자세한 내용은 클라이언트 인증서 해지 목록 섹션을 참조하세요.

Linux/macOS

다음 절차에서는 OpenVPN easy-rsa 명령줄 유틸리티를 사용하여 클라이언트 인증서 해지 목록을 생성합니다.

OpenVPN easy-rsa를 사용하여 클라이언트 인증서 해지 목록을 생성하려면

1. 인증서를 생성하는 데 사용한 easyrsa 설치를 호스팅하는 서버에 로그인합니다.

2. 로컬 리포지토리의 `easy-rsa/easyrsa3` 폴더로 이동합니다.

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

3. 클라이언트 인증서를 취소하고 클라이언트 취소 목록을 생성합니다.

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

메시지가 표시되면 `yes`를 입력합니다.

Windows

다음 절차에서는 OpenVPN 소프트웨어를 사용하여 클라이언트 해지 목록을 생성합니다. 클라이언트 및 서버 인증서와 키를 생성하는 데 OpenVPN 소프트웨어를 사용하기 위한 단계를 수행했다고 가정합니다.

EasyRSA 버전 3.x.x를 사용하여 클라이언트 인증서 해지 목록을 생성하려면

1. 명령 프롬프트를 열고 EasyRSA-3.x.x 디렉토리로 이동합니다. 이 디렉토리는 시스템에 설치된 위치에 따라 다릅니다.

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

2. `EasyRSA-Start.bat` 파일을 실행하여 EasyRSA 쉘을 시작합니다.

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

3. EasyRSA 셸에서 클라이언트 인증서를 해지합니다.

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

4. 메시지가 표시되면 `yes`를 입력합니다.
5. 클라이언트 해지 목록을 생성합니다.

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

6. 클라이언트 해지 목록은 다음 위치에 생성됩니다.

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

이전 EasyRSA 버전을 사용하여 클라이언트 인증서 해지 목록을 생성하려면

1. 명령 프롬프트를 열고 OpenVPN 디렉터리로 이동합니다.

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

2. `vars.bat` 파일을 실행합니다.

```
C:\> vars
```

3. 클라이언트 인증서를 취소하고 클라이언트 취소 목록을 생성합니다.

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

AWS Client VPN 클라이언트 인증서 해지 목록 가져오기

가져올 Client VPN 클라이언트 인증서 해지 목록 파일이 있어야 합니다. 클라이언트 인증서 해지 목록 생성에 대한 자세한 내용은 AWS Client VPN 클라이언트 인증서 해지 목록 생성 단원을 참조하십시오.

콘솔 및 AWS CLI를 사용하여 클라이언트 인증서 해지 목록을 가져올 수 있습니다.

클라이언트 인증서 해지 목록을 가져오는 방법(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 클라이언트 인증서 해지 목록을 가져올 Client VPN 엔드포인트를 선택합니다.
4. 작업을 선택하고 Import Client Certificate CRL(클라이언트 인증성 CRL 가져오기)을 선택합니다.
5. 인증서 해지 목록(Certificate Revocation List)에 클라이언트 인증서 해지 목록 파일의 내용을 입력하고 클라이언트 인증서 CRL 가져오기(Import client certificate CRL)를 선택합니다.

클라이언트 인증서 해지 목록을 가져오려면(AWS CLI)

import-client-vpn-client-certificate-revocation-list 명령을 사용합니다.

```
$ 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
```

AWS Client VPN 클라이언트 인증서 해지 목록 내보내기

콘솔 및 AWS CLI를 사용하여 Client VPN 클라이언트 인증서 해지 목록을 내보낼 수 있습니다.

클라이언트 인증서 해지 목록을 내보내는 방법(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 클라이언트 인증서 해지 목록을 내보낼 Client VPN 엔드포인트를 선택합니다.
4. 작업(Actions)을 선택하고 클라이언트 인증서 CRL 내보내기(Export Client Certificate CRL), 클라이언트 인증서 CRL 내보내기(Export Client Certificate CRL)를 차례로 선택합니다.

클라이언트 인증서 해지 목록을 내보내려면(AWS CLI)

export-client-vpn-client-certificate-revocation-list 명령을 사용합니다.

AWS Client VPN 클라이언트 연결

AWS Client VPN 연결은 클라이언트가 특정 Client VPN 엔드포인트에 설정한 활성 VPN 세션과 해당 엔드포인트에 대해 지난 60분 이내에 종료된 연결입니다. 클라이언트가 성공적으로 Client VPN 엔드포인트에 연결하면 연결이 설정됩니다. 세션을 종료하면 Client VPN 엔드포인트에 대한 클라이언트 연결이 종료됩니다.

Client VPN 연결을 보고 종료할 수 있습니다. 연결 정보를 보면 클라이언트 CIDR 블록 범위에서 할당된 IP 주소, 엔드포인트 ID 및 타임스탬프와 같은 정보가 반환됩니다. 세션을 종료하면 엔드포인트에 대한 지정된 VPN 연결이 종료됩니다. Amazon VPC 콘솔 또는 AWS CLI를 사용하여 세션을 보고 종료할 수 있습니다. 엔드포인트에 연결할 수 없는 경우 오류에 따라 문제를 해결하기 위해 취해야 할 단계는 문제 해결 섹션을 참조하세요.

Tasks

- AWS Client VPN 클라이언트 연결 보기
- AWS Client VPN 클라이언트 연결 종료

AWS Client VPN 클라이언트 연결 보기

Amazon VPC 콘솔 또는 AWS CLI를 사용하여 활성 Client VPN 연결을 볼 수 있습니다.

Client VPN 클라이언트 연결을 보는 방법(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 클라이언트 연결을 볼 Client VPN 엔드포인트를 선택합니다.
4. 연결 탭을 선택합니다. 연결 탭에 모든 활성 및 종료된 클라이언트 연결이 나열됩니다.

Client VPN 클라이언트 연결을 보는 방법(AWS CLI)

describe-client-vpn-connections 명령을 사용합니다.

AWS Client VPN 클라이언트 연결 종료

Amazon VPC 콘솔 또는 AWS CLI를 사용하여 Client VPN 클라이언트 연결을 종료할 수 있습니다.

Client VPN 클라이언트 연결을 종료하는 방법(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 클라이언트가 연결된 Client VPN 엔드포인트를 선택하고 연결을 선택합니다.
4. 종료할 연결을 선택하고 연결 종료를 선택한 다음, 연결 종료를 다시 선택하여 종료를 확인합니다.

Client VPN 클라이언트 연결을 종료하는 방법(AWS CLI)

terminate-client-vpn-connections 명령을 사용합니다.

AWS Client VPN 클라이언트 로그인 배너

AWS Client VPN에서는 VPN 세션이 설정될 때 AWS 제공 Client VPN 데스크톱 애플리케이션에 텍스트 배너를 표시할 수 있는 옵션을 제공합니다. 규정 및 규정 준수 요구 사항을 충족하기 위해 텍스트 배너의 내용을 정의할 수 있습니다. 최대 1,400자의 UTF-8 인코딩 문자를 사용할 수 있습니다.

> **Note**
>
> 클라이언트 로그인 배너가 활성화되면 새로 생성된 VPN 세션에만 해당 배너가 표시됩니다. 기존 VPN 세션은 중단되지 않지만 배너는 기존 세션이 다시 설정했을 때 표시됩니다.

배너 생성

Client VPN 엔드포인트를 생성하는 동안 로그인 배너가 처음에 생성되고 활성화됩니다. Client VPN 엔드포인트 생성 중에 클라이언트 로그인 배너를 활성화하는 자세한 단계는 AWS Client VPN엔드포인트 생성 섹션을 참조하세요.

Tasks

- 기존 AWS Client VPN 엔드포인트에 대한 클라이언트 로그인 배너 구성
- 기존 AWS Client VPN 엔드포인트에 대한 클라이언트 로그인 배너 비활성화
- AWS Client VPN 엔드포인트의 기존 배너 텍스트 수정
- 현재 구성된 AWS Client VPN 로그인 배너 보기

기존 AWS Client VPN 엔드포인트에 대한 클라이언트 로그인 배너 구성

기존 Client VPN 엔드포인트에 대한 클라이언트 로그인 배너를 구성하려면 다음 단계를 사용합니다.

Client VPN 엔드포인트에서 클라이언트 로그인 배너 활성화(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 수정할 Client VPN 엔드포인트를 선택하고 작업(Actions)을 선택한 다음 Client VPN 엔드포인트 수정(Modify Client VPN Endpoint)을 선택합니다.
4. 페이지를 아래의 기타 파라미터(Other parameters) 섹션으로 스크롤합니다.
5. 클라이언트 로그인 배너 활성화(Enable client login banner)를 켭니다.
6. 클라이언트 로그인 배너 텍스트에 VPN 세션이 설정될 때 AWS 제공된 클라이언트의 배너에 표시될 텍스트를 입력합니다. UTF-8로 인코딩된 문자만 사용할 수 있으며 최대 1,400자까지 사용할 수 있습니다.
7. 클라이언트 VPN 엔드포인트 수정(Modify Client VPN endpoint)을 선택합니다.

Client VPN 엔드포인트에서 클라이언트 로그인 배너 활성화(AWS CLI)

modify-client-vpn-endpoint 명령을 사용합니다.

기존 AWS Client VPN 엔드포인트에 대한 클라이언트 로그인 배너 비활성화

기존 Client VPN 엔드포인트에 대한 클라이언트 로그인 배너를 비활성화하려면 다음 단계를 사용합니다.

Client VPN 엔드포인트에서 클라이언트 로그인 배너 비활성화(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 수정할 Client VPN 엔드포인트를 선택하고 작업(Actions)을 선택한 다음 클라이언트 VPN 엔드포인트 수정(Modify Client VPN Endpoint)을 선택합니다.
4. 페이지를 아래의 기타 파라미터(Other parameters) 섹션으로 스크롤합니다.
5. 클라이언트 로그인 배너 활성화(Enable client login banner)를 켜거나 끕니다.
6. 클라이언트 VPN 엔드포인트 수정(Modify Client VPN endpoint)을 선택합니다.

Client VPN 엔드포인트에서 클라이언트 로그인 배너 비활성화(AWS CLI)

modify-client-vpn-endpoint 명령을 사용합니다.

AWS Client VPN 엔드포인트의 기존 배너 텍스트 수정

Client VPN 클라이언트 로그인 배너의 기존 텍스트를 수정하려면 다음 단계를 사용합니다.

Client VPN 엔드포인트의 기존 배너 텍스트 수정(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 수정할 Client VPN 엔드포인트를 선택하고 작업(Actions)을 선택한 다음 클라이언트 VPN 엔드포인트 수정(Modify Client VPN Endpoint)을 선택합니다.
4. 클라이언트 로그인 배너 활성화(Enable client login banner)가 켜져 있는지 확인합니다.
5. 클라이언트 로그인 배너 텍스트의 경우 VPN 세션이 설정될 때 AWS 제공된 클라이언트의 배너에 표시할 새 텍스트로 기존 텍스트를 바꿉니다. UTF-8로 인코딩된 문자만 사용할 수 있으며 최대 1,400자까지 허용됩니다.
6. 클라이언트 VPN 엔드포인트 수정(Modify Client VPN endpoint)을 선택합니다.

Client VPN 엔드포인트에서 클라이언트 로그인 배너 수정(AWS CLI)

modify-client-vpn-endpoint 명령을 사용합니다.

현재 구성된 AWS Client VPN 로그인 배너 보기

현재 구성된 Client VPN 로그인 배너를 보려면 다음 단계를 사용합니다.

Client VPN 엔드포인트에 대한 현재 로그인 배너 보기(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 보려는 Client VPN 엔드포인트를 선택합니다.
4. 세부 정보(Details) 탭이 선택되어 있는지 확인합니다.
5. 클라이언트 로그인 배너 텍스트(Client login banner text) 옆에 현재 구성된 로그인 배너 텍스트를 봅니다.

Client VPN 엔드포인트에 대해 현재 구성된 로그인 배너 보기(AWS CLI)

describe-client-vpn-endpoints 명령을 사용합니다.

AWS Client VPN 클라이언트 라우팅 적용

클라이언트 경로 강제 적용은 VPN을 통해 연결된 디바이스에서 관리자가 정의한 경로를 적용하는 데 도움이 됩니다. 이 기능은 연결된 클라이언트에서 발생하는 네트워크 트래픽이 실수로 VPN 터널 외부로 전송되지 않게 함으로써 보안 태세를 개선하는 데 도움이 됩니다.

클라이언트 경로 강제 적용은 연결된 디바이스의 기본 라우팅 테이블을 모니터링하고 클라이언트 VPN 엔드포인트에 구성된 네트워크 경로에 따라 아웃바운드 네트워크 트래픽이 VPN 터널로 전달되도록 합니다. 여기에는 VPN 터널과 충돌하는 경로가 감지되는 경우 디바이스의 라우팅 테이블 수정이 포함됩니다. 클라이언트 경로 강제 적용은 IPv4 및 IPv6 주소 패밀리를 모두 지원합니다.

요구 사항

클라이언트 라우팅 적용은 다음 AWS 제공 Client VPN 버전에서만 작동합니다.

- Windows 버전 5.2.0 이상(IPv4 지원)
- macOS 버전 5.2.0 이상(IPv4 지원)
- Ubuntu 버전 5.2.0 이상(IPv4 지원)

- Windows 버전 5.3.0 이상(IPv6 지원)
- macOS 버전 5.3.0 이상(IPv6 지원)
- Ubuntu 버전 5.3.0 이상(IPv6 지원)

듀얼 스택 엔드포인트의 경우 클라이언트 경로 강제 적용 설정은 IPv4 스택과 IPv6 스택 모두에 동시에 적용됩니다. 하나의 스택에만 클라이언트 경로 강제 적용을 활성화할 수는 없습니다.

라우팅 충돌

클라이언트가 VPN에 연결되어 있는 동안 클라이언트의 로컬 라우팅 테이블과 엔드포인트의 네트워크 라우팅을 비교합니다. 두 라우팅 테이블 항목 간에 네트워크 중복이 있는 경우 라우팅 충돌이 발생합니다. 중첩 네트워크의 예는 다음과 같습니다.

- `172.31.0.0/16`
- `172.31.1.0/24`

이 예에서 이러한 CIDR 블록은 라우팅 충돌을 구성합니다. 예를 들어 `172.31.0.0/16`은 VPN 터널 CIDR일 수 있습니다. `172.31.1.0/24`는 접두사가 더 길기 때문에 더 구체적이며, 일반적으로 우선 순위를 가지며 `172.31.1.0/24` IP 범위 내의 VPN 트래픽을 다른 대상으로 잠재적으로 리디렉션합니다. 이로 인해 의도하지 않은 라우팅 동작이 발생할 수 있습니다. 그러나 클라이언트 경로 강제 적용이 활성화되면 후자의 CIDR이 제거됩니다. 이 기능을 사용할 때는 잠재적 라우팅 충돌을 고려해야 합니다.

전체 터널 VPN 연결은 VPN 연결을 통해 모든 네트워크 트래픽을 전달합니다. 따라서 클라이언트 경로 강제 적용 기능이 활성화된 경우 VPN에 연결된 디바이스는 로컬 네트워크(LAN) 리소스에 액세스할 수 없습니다. 로컬 LAN 액세스가 필요한 경우 전체 터널 모드 대신 분할 터널 모드를 사용하는 것이 좋습니다. 분할 터널에 대한 자세한 내용은 분할 터널 Client VPN 섹션을 참조하세요.

고려 사항

클라이언트 경로 강제 적용을 활성화하기 전에 다음 정보를 고려해야 합니다.

- 연결 시 라우팅 충돌이 감지되면 이 기능은 클라이언트의 라우팅 테이블을 업데이트하여 트래픽을 VPN 터널로 보냅니다. 연결이 설정되기 전에 존재했던 경로 중 이 기능으로 삭제된 경로는 복원됩니다.
- 이 기능은 기본 라우팅 테이블에만 적용되며 다른 라우팅 메커니즘에는 적용되지 않습니다. 예를 들어 다음에는 적용되지 않습니다.

  - 정책 기반 라우팅
  - 인터페이스 범위 라우팅
- 클라이언트 경로 강제 적용은 VPN 터널이 열려 있는 동안 VPN 터널을 보호합니다. 터널이 연결 해제되거나 클라이언트가 다시 연결되는 동안에는 보호되지 않습니다.

OpenVPN 명령이 클라우드 경로 강제 적용에 미치는 영향

OpenVPN 구성 파일의 일부 사용자 지정 명령은 클라이언트 경로 강제 적용과 특정 상호 작용을 합니다.

- `route` 지시문
  - VPN 게이트웨이에 경로를 추가할 때. 예를 들어 VPN 게이트웨이에 경로 `192.168.100.0 255.255.255.0`을 추가합니다.

    VPN 게이트웨이에 추가된 경로는 다른 VPN 경로와 유사하게 클라이언트 경로 강제 적용에 의해 모니터링됩니다. 해당 경로 내에서 충돌하는 모든 경로가 감지되고 제거됩니다.
  - 비VPN 게이트웨이에 경로를 추가할 때. 예를 들어 경로 `192.168.200.0 255.255.255.0 net_gateway`를 추가합니다.

    비VPN 게이트웨이에 추가된 경로는 VPN 터널을 우회하므로 클라이언트 경로 강제 적용에서 제외됩니다. 충돌하는 경로는 해당 경로 내에서 허용됩니다. 위 예제의 경로는 클라이언트 경로 강제 적용의 모니터링에서 제외됩니다.
  - IPv4 경로와 마찬가지로 VPN 게이트웨이에 추가된 IPv6 경로는 클라이언트 경로 강제 적용에서 모니터링되는 반면, 비VPN 게이트웨이에 추가된 경로는 모니터링에서 제외됩니다.

무시된 경로

다음 IPv4 네트워크에 대한 라우팅은 클라이언트 경로 강제 적용에서 무시됩니다.

- `127.0.0.0/8` - 로컬 호스트용으로 예약됨
- `169.254.0.0/16` - 링크-로컬 주소용으로 예약됨
- `224.0.0.0/4` - 멀티캐스트용으로 예약됨
- `255.255.255.255/32` - 브로드캐스트용으로 예약됨

다음 IPv6 네트워크에 대한 라우팅은 클라이언트 경로 강제 적용에서 무시됩니다.

- `::1/128` - 루프백용으로 예약됨
- `fe80::/10` - 링크-로컬 주소용으로 예약됨
- `ff00::/8` - 멀티캐스트용으로 예약됨

주제

- AWS Client VPN 엔드포인트에 대한 클라이언트 라우팅 적용 활성화
- AWS Client VPN 엔드포인트에서 클라이언트 라우팅 적용 비활성화
- IPv6 클라이언트 경로 강제 적용 문제 해결

AWS Client VPN 엔드포인트에 대한 클라이언트 라우팅 적용 활성화

콘솔 또는 AWS CLI를 사용하여 기존 Client VPN 엔드포인트에서 클라이언트 경로 강제 적용을 활성화할 수 있습니다.

콘솔을 사용하여 클라이언트 경로 강제 적용을 활성화하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 클라이언트 VPN 엔드포인트(Client VPN endpoints)를 선택합니다.
3. 수정할 Client VPN 엔드포인트를 선택하고 작업을 선택한 다음 클라이언트 VPN 엔드포인트 수정을 선택합니다.
4. 페이지를 아래의 기타 파라미터(Other parameters) 섹션으로 스크롤합니다.
5. 클라이언트 경로 강제 적용을 켭니다.
6. 클라이언트 VPN 엔드포인트 수정(Modify Client VPN endpoint)을 선택합니다.

AWS CLI를 사용하여 클라이언트 경로 강제 적용을 활성화하려면

- modify-client-vpn-endpoint 명령을 사용합니다.

AWS Client VPN 엔드포인트에서 클라이언트 라우팅 적용 비활성화

콘솔 또는 AWS CLI를 사용하여 Client VPN 엔드포인트에서 클라이언트 경로 강제 적용을 비활성화할 수 있습니다.

콘솔을 사용하여 클라이언트 경로 강제 적용을 비활성화하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 클라이언트 VPN 엔드포인트(Client VPN endpoints)를 선택합니다.
3. 수정할 Client VPN 엔드포인트를 선택하고 작업을 선택한 다음 클라이언트 VPN 엔드포인트 수정을 선택합니다.
4. 페이지를 아래의 기타 파라미터(Other parameters) 섹션으로 스크롤합니다.
5. 클라이언트 경로 강제 적용을 끕니다.
6. 클라이언트 VPN 엔드포인트 수정(Modify Client VPN endpoint)을 선택합니다.

를 사용하여 클라이언트 라우팅 적용을 비활성화하려면 AWS CLI

- modify-client-vpn-endpoint 명령을 사용합니다.

IPv6 클라이언트 경로 강제 적용 문제 해결

IPv6 클라이언트 경로 강제 적용에 문제가 발생하면 다음 문제 해결 단계를 고려하세요.

클라이언트 버전 확인

IPv6 클라이언트 경로 강제 적용 지원에 필요한 AWS VPN 클라이언트 버전 5.3.0 이상을 사용하고 있는지 확인합니다.

엔드포인트 구성 확인

엔드포인트에 클라이언트 경로 강제 적용이 활성화되어 있고 IPv6 또는 듀얼 스택 트래픽에 맞춰 구성되어 있는지 확인합니다.

클라이언트 로그 검사

AWS VPN 클라이언트 로그에서 IPv6 클라이언트 경로 강제 적용과 관련된 오류 메시지를 검토합니다. 'IPv6' 및 '클라이언트 경로 강제 적용' 또는 'CRM'이 포함된 항목을 찾습니다.

라우팅 테이블 검사

운영 체제에 적합한 명령을 사용하여 IPv6 라우팅 테이블을 봅니다.

- Windows: `netsh interface ipv6 show route`
- macOS: `netstat -rn -f inet6`
- Linux: `ip -6 route`

충돌하는 경로 확인

VPN 경로와 충돌할 수 있는 IPv6 경로를 찾습니다. 대상은 동일하지만 게이트웨이는 다른 경로에 특히 주의하세요.

ISP IPv6 지원 확인

인터넷 서비스 제공업체(ISP)가 IPv6를 제대로 지원하는지 확인합니다.

이러한 문제 해결 단계를 시도한 후에도 IPv6 클라이언트 경로 강제 적용에 문제가 계속 발생하면 AWS Support에 문의하여 추가 지원을 받으세요.

AWS Client VPN 엔드포인트

모든 AWS Client VPN 세션은 Client VPN 엔드포인트와 통신을 설정합니다. Client VPN 엔드포인트를 관리하여 해당 엔드포인트로 Client VPN 세션을 생성, 수정, 보기 및 삭제할 수 있습니다. 엔드포인트는 Amazon VPC 콘솔 또는 AWS CLI를 사용하여 생성하고 수정할 수 있습니다.

Client VPN 엔드포인트 생성 요구 사항

> **Important**
>
> Client VPN 엔드포인트는 의도한 대상 네트워크가 프로비저닝된 동일한 AWS 계정에 생성해야 합니다. 또한 서버 인증서와 필요한 경우 클라이언트 인증서를 생성해야 합니다. 자세한 내용은 의 클라이언트 인증 AWS Client VPN 단원을 참조하십시오.

시작하기 전에 다음이 있는지 확인하십시오.

- 사용에 대한 규칙 및 모범 사례 AWS Client VPN에서 규칙 및 제한 사항을 검토합니다.
- 서버 인증서를 생성하고, 필요한 경우 클라이언트 인증서를 생성합니다. 자세한 내용은 의 클라이언트 인증 AWS Client VPN 단원을 참조하십시오.

IP 주소 유형

AWS Client VPN 는 엔드포인트 연결 및 트래픽 라우팅 모두에 대해 IPv4-only, IPv6-only 및 듀얼 스택 구성을 지원합니다. 다음 지침은 클라이언트 디바이스 기능, 네트워크 인프라 및 애플리케이션 요구 사항에 따라 적절한 IP 주소 유형을 선택하는 데 도움이 됩니다.

엔드포인트 주소 유형

엔드포인트 주소 유형에 따라 Client VPN 엔드포인트가 클라이언트 연결에 지원하는 IP 프로토콜이 결정됩니다. 엔드포인트 생성 후에는 이 설정을 변경할 수 없습니다.

다음과 같은 경우 IPv4 전용을 선택합니다.

- 클라이언트 디바이스는 IPv4 VPN 연결만 지원하는 경우
- 보안 도구가 IPv4 트래픽 검사에 최적화되어 있는 경우

다음과 같은 경우 IPv6 전용을 선택합니다.

- 모든 클라이언트 디바이스가 IPv6 연결을 완전히 지원하는 경우
- IPv4 주소가 고갈된 네트워크에 있는 경우

다음과 같은 경우 듀얼 스택을 선택합니다.

- 다양한 IP 기능을 갖춘 클라이언트 디바이스가 혼합되어 있는 경우
- IPv4에서 IPv6로 점진적으로 전환 중인 경우

트래픽 IP 주소 유형

트래픽 IP 주소 유형은 엔드포인트의 지원되는 프로토콜과 관계없이 Client VPN이 클라이언트와 VPC 리소스 간의 트래픽을 라우팅하는 방법을 제어합니다.

다음과 같은 경우 트래픽을 IPv4로 라우팅합니다.

- VPC의 대상 애플리케이션이 IPv4만 지원하는 경우
- IPv4 보안 그룹 및 네트워크 ACL가 복잡한 경우
- 레거시 시스템에 연결 중인 경우

다음과 같은 경우 트래픽을 IPv6로 라우팅합니다.

- VPC 인프라는 주로 IPv6인 경우
- 향후 네트워크 아키텍처에 대비하려는 경우
- IPv6용으로 구축된 최신 애플리케이션이 있는 경우

엔드포인트 수정

> **Note**
>
> 빠른 시작 설정을 사용하여 생성된 Client VPN 엔드포인트는 표준 설정으로 생성된 엔드포인트와 동일한 절차를 사용하여 수정할 수 있습니다. 모든 구성 옵션은 생성 중에 사용되는 설정 방법에 관계없이 사용할 수 있습니다.

Client VPN이 생성된 후에는 다음 설정을 수정할 수 있습니다.

- 설명
- 서버 인증서
- 클라이언트 연결 로깅 옵션
- 클라이언트 연결 핸들러 옵션
- DNS 서버
- 분할 터널 옵션
- 경로(분할 터널 옵션을 사용하는 경우)
- 인증서 취소 목록(CRL)
- 권한 부여 규칙
- VPC 및 보안 그룹 연결
- VPN 포트 번호
- 셀프 서비스 포털 옵션
- 최대 VPN 세션 시간
- 세션 제한 시간에 자동 재연결 활성화 또는 비활성화
- 클라이언트 로그인 배너 텍스트 사용 또는 사용 중지
- 클라이언트 로그인 배너 텍스트

> **Note**
>
> 인증서 취소 목록(CRL) 변경 사항을 포함하여 Client VPN 엔드포인트에 대한 수정 사항은 Client VPN 서비스에서 요청을 수락한 후 최대 4시간 이내에 적용됩니다.

Client VPN 엔드포인트가 생성된 이후에는 클라이언트 IPv4 CIDR 범위, 인증 옵션, 클라이언트 인증서 또는 전송 프로토콜을 수정할 수 없습니다.

Client VPN 엔드포인트에서 다음과 같은 파라미터 중 아무 것이라도 변경하면, 연결이 재설정됩니다.

- 서버 인증서
- DNS 서버
- 분할 터널 옵션(지원 켜기 또는 끄기)
- 경로(분할 터널 옵션을 사용하는 경우)
- 인증서 취소 목록(CRL)
- 권한 부여 규칙
- VPN 포트 번호

태스크

- AWS Client VPN엔드포인트 생성
- AWS Client VPN 엔드포인트 보기
- AWS Client VPN 엔드포인트 수정
- AWS Client VPN 엔드포인트 삭제

AWS Client VPN엔드포인트 생성

AWS Client VPN엔드포인트를 생성하여 클라이언트가 Amazon VPC 콘솔 또는를 사용하여 VPN 세션을 설정할 수 있도록 합니다AWS CLI.Client VPN은 초기 생성 중에 엔드포인트 유형(분할 터널 및 전체 터널)과 트래픽 유형(IPv4, IPv6 및 듀얼 스택)의 모든 조합을 지원합니다.

엔드포인트를 생성하기 전에 요구 사항을 숙지하세요. 자세한 내용은 the section called “Client VPN 엔드포인트 생성 요구 사항” 단원을 참조하십시오.

콘솔을 사용하여 Client VPN 엔드포인트를 생성하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN Endpoints(Client VPN 엔드포인트)를 선택한 다음 Create Client VPN Endpoint(Client VPN 엔드포인트 생성)를 선택합니다.
3. "설정 방법 선택"에서 다음 중 하나를 선택합니다.

- 빠른 시작 - AWS 권장 기본값으로 엔드포인트 생성
- 표준 - 엔드포인트에 대한 모든 설정을 수동으로 구성

빠른 시작 설정:

1. “설정 방법 선택”에서 빠른 시작을 선택합니다.
2. "클라이언트 IPv4 CIDR"에 클라이언트 IP 주소를 할당할 IP 주소 범위를 입력합니다. AWS는 /22 CIDR 블록(예: 10.0.0.0/22)을 사용할 것을 권장합니다.
3. "VPC"에서 Client VPN 엔드포인트와 연결할 VPC를 선택합니다.
4. “서브넷”에서 VPC에서 하나 이상의 서브넷을 선택합니다. 이러한 서브넷은 대상 네트워크 연결에 사용됩니다.
5. Server certificate ARN(서버 인증서 ARN)에 서버에서 사용할 TLS 인증서의 ARN을 지정합니다. 클라이언트는 서버 인증서를 사용하여 연결할 Client VPN 엔드포인트를 인증합니다.
6. "Client VPN 엔드포인트 생성"을 선택합니다.

AWS는 다음 리소스를 자동으로 생성합니다.

- 모든 사용자가 VPC CIDR에 액세스하도록 허용하는 권한 부여 규칙
- 선택한 VPC 서브넷과의 대상 네트워크 연결
- VPC CIDR에 대한 라우팅 테이블 항목

엔드포인트가 생성되면 엔드포인트 세부 정보 페이지에서 클라이언트 구성 파일을 다운로드하여 클라이언트 인증서 및 키와 함께 사용자에게 배포할 수 있습니다.

표준 설정:

1. "설정 방법 선택"에서 표준을 선택합니다.
2. (선택 사항) Client VPN 엔드포인트의 이름 태그와 설명을 입력합니다.
3. 엔드포인트 IP 주소 유형에서 엔드포인트의 IP 주소 유형을 선택합니다.
   - IPv4: 엔드포인트가 외부 VPN 터널 트래픽에 IPv4 주소를 사용합니다.
   - IPv6: 엔드포인트가 외부 VPN 터널 트래픽에 IPv6 주소를 사용합니다.
   - 듀얼 스택: 엔드포인트가 외부 VPN 터널 트래픽에 IPv4 및 IPv6 주소를 모두 사용합니다.
4. 트래픽 IP 주소 유형에서 엔드포인트를 통해 흐르는 트래픽의 IP 주소 유형을 선택합니다.

- IPv4: 엔드포인트가 IPv4 트래픽만 지원합니다.
- IPv6: 엔드포인트가 IPv6 트래픽만 지원합니다.
- 듀얼 스택: 엔드포인트가 IPv4 트래픽과 IPv6 트래픽을 모두 지원합니다.

5. 클라이언트 IPv4 CIDR에서 클라이언트 IP 주소를 할당할 IP 주소 범위(CIDR 표기법)를 지정합니다. 예를 들어 `10.0.0.0/22`입니다. 트래픽 IP 주소 유형에 IPv4 또는 듀얼 스택을 선택한 경우 필수입니다.

> **Note**
>
> - 주소 범위는 Client VPN 엔드포인트와 연결될 대상 네트워크 주소 범위, VPC 주소 범위 또는 경로와 중복될 수 없습니다. 클라이언트 주소 범위는 최소 /22 이상이어야 하며 /12 CIDR 블록 크기를 넘지 않아야 합니다. Client VPN 엔드포인트를 생성한 후에는 클라이언트 주소 범위를 변경할 수 없습니다.
> - IPv6를 엔드포인트 IP 주소 유형으로 선택하면 클라이언트 IPv4 CIDR 필드가 비활성화됩니다. Client VPN 엔드포인트는 연결된 서브넷에서 클라이언트 IPv6 주소를 할당하며 엔드포인트를 생성한 후 서브넷을 연결할 수 있습니다.

> **Note**
>
> IPv6 트래픽의 경우 클라이언트 CIDR 범위를 지정할 필요가 없습니다. Amazon은 클라이언트에 IPv6 CIDR 범위를 자동으로 할당합니다.

6. Server certificate ARN(서버 인증서 ARN)에 서버에서 사용할 TLS 인증서의 ARN을 지정합니다. 클라이언트는 서버 인증서를 사용하여 연결할 Client VPN 엔드포인트를 인증합니다.

> **Note**
>
> 서버 인증서는 Client VPN 엔드포인트를 생성하는 리전의AWS Certificate Manager(ACM)에 있어야 합니다. 인증서는 ACM을 사용하여 프로비저닝하거나 ACM으로 가져올 수 있습니다.
> ACM에 인증서를 프로비저닝하거나 가져오는 단계는 AWS Certificate Manager사용 설명서의 AWS Certificate Manager인증서를 참조하세요.

7. 클라이언트가 VPN 연결을 설정할 때 클라이언트를 인증하는 데 사용할 인증 방법을 지정합니다. 인증 방법을 선택해야 합니다.

   - 사용자 기반 인증을 사용하려면 사용자 기반 인증 사용을 선택하고 다음 중 하나를 선택합니다.
     - Active Directory 인증: Active Directory 인증을 사용하려면 이 옵션을 선택합니다. 디렉터리 ID에는 사용할 Active Directory의 ID를 지정합니다.
     - 연동 인증: SAML 기반 연동 인증을 사용하려면 이 옵션을 선택합니다.

       SAML 제공업체 ARN에는 IAM SAML 자격 증명 공급자의 ARN을 지정합니다.

       (선택 사항) Self-service SAML provider ARN(셀프 서비스 SAML 공급자 ARN)에서 셀프 서비스 포털을 지원하기 위해 생성한 IAM SAML 자격 증명 공급자의 ARN을 지정합니다(해당하는 경우).
   - 상호 인증서 인증을 사용하려면 상호 인증 사용을 선택한 다음 클라이언트 인증서 ARN에AWS Certificate Manager(ACM)에 프로비저닝된 클라이언트 인증서의 ARN을 지정합니다.

   > **Note**
   >
   > 서버 및 클라이언트 인증서가 동일한 CA(인증 기관)에 의해 발급된 경우 서버 인증서 ARN을 서버 및 클라이언트 모두에 사용할 수 있습니다. 클라이언트 인증서가 다른 CA에 의해 발급된 경우 클라이언트 인증서 ARN이 지정되어야 합니다.

8. (선택 사항) 연결 로깅(Connection logging)에서 Amazon CloudWatch Logs를 사용하여 클라이언트 연결에 대한 데이터를 로그할지 여부를 지정합니다. 클라이언트 연결에 대한 로그 세부 정보 활성화(Enable log details on client connections)를 켭니다. CloudWatch Logs log group name(CloudWatch Logs 로그 그룹 이름)에 사용할 로그 그룹의 이름을 입력합니다. CloudWatch Logs log stream name(CloudWatch Logs 로그 스트림 이름)에 사용할 로그 스트림의 이름을 입력하거나 사용자 대신 자동으로 로그 스트림을 생성할 수 있도록 이 옵션을 비워 둡니다.

9. (선택 사항) 클라이언트 연결 핸들러(Client Connect Handler)에서 클라이언트 연결 핸들러 활성화(Enable client connect handler)를 켜서 Client VPN 엔드포인트에 대한 새 연결을 허용하거나 거부하는 사용자 지정 코드를 실행합니다. Client Connect Handler ARN(클라이언트 연결 처리기 ARN)에서 연결을 허용하거나 거부하는 논리가 포함된 Lambda 함수의 Amazon 리소스 이름(ARN)을 지정합니다.

10. (선택 사항) DNS 확인에 사용할 DNS 서버를 지정합니다. 사용자 지정 DNS 서버를 사용하려면 DNS 서버 1 IP 주소 및 DNS 서버 2 IP 주소에 사용할 DNS 서버의 IPv4 주소를 지정합니다. IPv6 또는 듀얼 스택 엔드포인트의 경우 DNS 서버 IPv6 1 및 DNS 서버 IPv6 2 주소를 지정할 수도 있습니다. VPC DNS 서버를 사용하려면 DNS Server 1 IP address(DNS 서버 1 IP 주소) 또는 DNS

Server 2 IP address(DNS 서버 2 IP 주소)에 IP 주소를 지정하고 VPC DNS 서버 IP 주소를 추가합니다.

> **Note**
>
> 클라이언트가 DNS 서버에 도달할 수 있는지 확인합니다.

11. (선택 사항) 기본적으로 Client VPN 엔드포인트는 UDP 전송 프로토콜을 사용합니다. TCP 전송 프로토콜을 대신 사용하려면 Transport Protocol에서 TCP를 선택합니다.

> **Note**
>
> 일반적으로 UDP가 TCP보다 뛰어난 성능을 제공합니다. Client VPN 엔드포인트를 생성한 후에는 전송 프로토콜을 변경할 수 없습니다.

12. (선택 사항) 엔드포인트를 분할 터널 Client VPN 엔드포인트로 사용하려면 분할 터널 활성화(Enable split-tunnel)를 켭니다. 기본적으로 Client VPN 엔드포인트의 분할 터널은 비활성화됩니다.
13. (선택 사항) VPC ID에서 Client VPN 엔드포인트와 연결할 VPC를 선택합니다. Security Group IDs(보안 그룹 ID)에서 Client VPN 엔드포인트에 적용할 VPC의 보안 그룹을 하나 이상 선택합니다.
14. (선택 사항) VPN 포트의 경우 VPN 포트 번호를 선택합니다. 기본값은 443입니다.
15. (선택 사항) 클라이언트에 대한 셀프 서비스 포털 URL을 생성하려면 셀프 서비스 포털 활성화(Enable self-service portal)를 켭니다.
16. (선택 사항) 세션 제한 시간(Session timeout hours)에서 사용 가능한 옵션에서 원하는 최대 VPN 세션 기간(시간)을 선택하거나 기본값 24시간으로 설정된 상태로 둡니다.
17. (선택 사항) 세션 제한 시간 도달 시 연결 해제에서 최대 세션 시간에 도달할 때 세션을 종료할지 여부를 선택합니다. 이 옵션을 선택하면 세션 시간이 초과한 경우 사용자가 엔드포인트에 수동으로 다시 연결해야 합니다. 그렇지 않으면 Client VPN이 자동으로 다시 연결을 시도합니다.
18. (선택 사항) 클라이언트 로그인 배너 텍스트를 사용 설정할지 여부를 지정합니다. 클라이언트 로그인 배너 활성화(Enable client login banner)를 켭니다. 클라이언트 로그인 배너 텍스트(Client login banner text)에 VPN 세션이 설정될 때 AWS 제공 클라이언트의 배너에 표시될 텍스트를 입력합니다. UTF-8로 인코딩된 문자만 허용됩니다. 최대 1,400자입니다.
19. 클라이언트 VPN엔드포인트 생성(Create Client VPN endpoint)을 선택합니다.

Client VPN 엔드포인트를 생성한 후, 다음을 수행하여 구성을 완료하고 클라이언트가 연결할 수 있도록 합니다.

- Client VPN 엔드포인트의 초기 상태는 `pending-associate`입니다. 첫 번째 대상 네트워크를 연결한 이후에만 클라이언트가 Client VPN 엔드포인트에 연결할 수 있습니다.
- 네트워크에 액세스할 수 있는 클라이언트를 지정하려면 권한 부여 규칙을 생성합니다.
- 클라이언트에 배포할 Client VPN 엔드포인트 구성 파일을 다운로드하고 준비합니다.
- 클라이언트에게AWS제공된 클라이언트 또는 다른 OpenVPN 기반 클라이언트 애플리케이션을 사용하여 Client VPN 엔드포인트에 연결하도록 지시합니다. 자세한 내용은 AWS Client VPN사용 설명서를 참조하십시오.

를 사용하여 Client VPN 엔드포인트를 생성하려면AWS CLI

create-client-vpn-endpoint 명령을 사용합니다.

IPv4 엔드포인트 생성 예제:

```
aws ec2 create-client-vpn-endpoint \
  --client-cidr-block "172.31.0.0/16" \
  --server-certificate-arn arn:aws:acm:ap-south-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
  --authentication-options Type=certificate-
authentication,MutualAuthentication={ClientRootCertificateChainArn=arn:aws:acm:ap-
south-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE} \
  --connection-log-options Enabled=false
```

IPv6 엔드포인트 생성 예제:

```
aws ec2 create-client-vpn-endpoint \
  --endpoint-ip-address-type "ipv6" \
  --traffic-ip-address-type "ipv6" \
  --server-certificate-arn arn:aws:acm:ap-south-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
  --authentication-options Type=certificate-
authentication,MutualAuthentication={ClientRootCertificateChainArn=arn:aws:acm:ap-
south-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE} \
  --connection-log-options Enabled=false
```

듀얼 스택 엔드포인트 생성 예제:

```
aws ec2 create-client-vpn-endpoint \
  --endpoint-ip-address-type "dual-stack" \
  --traffic-ip-address-type "dual-stack" \
  --client-cidr-block "172.31.0.0/16" \
  --server-certificate-arn arn:aws:acm:ap-south-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
  --authentication-options Type=certificate-
authentication,MutualAuthentication={ClientRootCertificateChainArn=arn:aws:acm:ap-
south-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE} \
  --connection-log-options Enabled=false
```

AWS Client VPN 엔드포인트 보기

Amazon VPC 콘솔 또는 AWS CLI를 사용하여 Client VPN 엔드포인트에 대한 정보를 볼 수 있습니다.

Client VPN 엔드포인트를 보려면(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 보려는 Client VPN 엔드포인트를 선택합니다.
4. 세부 정보, 대상 네트워크 연결, 보안 그룹, 권한 부여 규칙, 라우팅 테이블, 연결 및 태그 탭을 사용하여 기존 Client VPN 엔드포인트에 대한 정보를 봅니다.

   필터를 사용하여 검색을 구체화할 수도 있습니다.

Client VPN 엔드포인트를 보려면(AWS CLI)

describe-client-vpn-endpoints 명령을 사용합니다.

AWS Client VPN 엔드포인트 수정

Amazon VPC 콘솔 또는 AWS CLI를 사용하여 Client VPN 엔드포인트를 수정할 수 있습니다. 수정할 수 있는 Client VPN 필드에 대한 자세한 내용은 the section called “엔드포인트 수정” 섹션을 참조하세요.

제한 사항

엔드포인트를 수정할 때 다음과 같은 제한 사항이 적용됩니다.

- 인증서 취소 목록(CRL) 변경 사항을 포함하여 Client VPN 엔드포인트에 대한 수정 사항은 Client VPN 서비스에서 요청을 수락한 후 최대 4시간 이내에 적용됩니다.
- Client VPN 엔드포인트가 생성된 이후에는 클라이언트 IPv4 CIDR 범위, 인증 옵션, 클라이언트 인증서 또는 전송 프로토콜을 수정할 수 없습니다.
- 엔드포인트 IP 유형과 트래픽 IP 유형 모두에 대해 기존 IPv4 엔드포인트를 듀얼 스택으로 수정할 수 있습니다. 엔드포인트 IP 및 트래픽 IP에 IPv6 전용이 필요한 경우 새 엔드포인트를 생성해야 합니다.
- Client VPN은 생성 후 엔드포인트 유형(IPv4, IPv6, 듀얼 스택) 또는 트래픽 유형(IPv4, IPv6, 듀얼 스택)의 수정을 지원하지 않습니다.
- 엔드포인트 유형과 트래픽 유형의 특정 조합으로 Client VPN을 수정하는 것은 지원되지 않습니다. 다른 조합으로 변경할 수 없습니다. 엔드포인트를 삭제하고 원하는 구성으로 다시 생성해야 합니다.
- IPv6 트래픽에 대한 Client-to-client 통신은 지원되지 않습니다.

Client VPN 엔드포인트를 수정합니다.

콘솔 또는 AWS CLI를 사용하여 Client VPN 엔드포인트를 수정할 수 있습니다.

콘솔을 사용하여 Client VPN 엔드포인트를 수정하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 수정할 Client VPN 엔드포인트를 선택하고 작업(Actions)을 선택한 다음 클라이언트 VPN 엔드포인트 수정(Modify Client VPN endpoint)을 선택합니다.
4. 설명(Description)에 Client VPN 엔드포인트에 대한 간략한 설명을 입력합니다.
5. 엔드포인트 IP 주소 유형의 경우 기존 IPv4 엔드포인트를 듀얼 스택으로 수정할 수 있습니다. 이 옵션은 IPv4 엔드포인트에만 사용할 수 있습니다.
6. 트래픽 IP 주소 유형의 경우 기존 IPv4 엔드포인트를 듀얼 스택으로 수정할 수 있습니다. 이 옵션은 IPv4 엔드포인트에만 사용할 수 있습니다.
7. Server certificate ARN(서버 인증서 ARN)에 서버에서 사용할 TLS 인증서의 ARN을 지정합니다. 클라이언트는 서버 인증서를 사용하여 연결할 Client VPN 엔드포인트를 인증합니다.

> **Note**
>
> 서버 인증서는 Client VPN 엔드포인트를 생성하는 리전의 AWS Certificate Manager(ACM)에 위치해야 합니다. 인증서는 ACM을 사용하여 프로비저닝하거나 ACM으로 가져올 수 있습니다.

8. Amazon CloudWatch Logs를 사용하여 클라이언트 연결에 대한 데이터를 로깅할지 여부를 지정합니다. 클라이언트 연결에 대한 로그 세부 정보 활성화(Enable log details on client connections)에서 다음 중 하나를 수행합니다.

   - 클라이언트 연결 로깅을 활성화하려면 클라이언트 연결에 대한 로그 세부 정보 활성화(Enable log details on client connections)를 켭니다. CloudWatch Logs 로그 그룹 이름(CloudWatch Logs log group name)에 사용할 로그 그룹의 이름을 선택합니다. CloudWatch Logs 로그 스트림 이름(CloudWatch Logs log stream name)에 사용할 로그 스트림의 이름을 선택하거나 사용자 대신 자동으로 로그 스트림을 생성할 수 있도록 이 옵션을 비워 둡니다.
   - 클라이언트 연결 로깅을 비활성화하려면 클라이언트 연결에 대한 로그 세부 정보 활성화(Enable log details on client connections)를 끕니다.

9. 클라이언트 연결 핸들러(Client connect handler)에서 클라이언트 연결 핸들러를 활성화하려면 클라이언트 연결 핸들러 활성화(Enable client connect handler)를 켭니다. Client Connect Handler ARN(클라이언트 연결 처리기 ARN)에서 연결을 허용하거나 거부하는 논리가 포함된 Lambda 함수의 Amazon 리소스 이름(ARN)을 지정합니다.

10. DNS 서버 활성화(Enable DNS servers)를 켜거나 끕니다. 사용자 지정 DNS 서버를 사용하려면 DNS 서버 1 IP 주소 및 DNS 서버 2 IP 주소에 사용할 DNS 서버의 IPv4 주소를 지정합니다. IPv6 또는 듀얼 스택 엔드포인트의 경우 DNS 서버 IPv6 1 및 DNS 서버 IPv6 2 주소를 지정할 수도 있습니다. VPC DNS 서버를 사용하려면 DNS Server 1 IP address(DNS 서버 1 IP 주소) 또는 DNS Server 2 IP address(DNS 서버 2 IP 주소)에 IP 주소를 지정하고 VPC DNS 서버 IP 주소를 추가합니다.

> **Note**
>
> 클라이언트가 DNS 서버에 도달할 수 있는지 확인합니다.

11. 분할 터널 활성화(Enable split-tunnel)를 켜거나 끕니다. 기본적으로 VPN 엔드포인트에서 분할 터널은 꺼져 있습니다.

12. VPC ID에서 Client VPN 엔드포인트와 연결할 VPC를 선택합니다. Security Group IDs(보안 그룹 ID)에서 Client VPN 엔드포인트에 적용할 VPC의 보안 그룹을 하나 이상 선택합니다.

13. VPN 포트의 경우 VPN 포트 번호를 선택합니다. 기본값은 443입니다.
14. 클라이언트에 대한 셀프 서비스 포털 URL을 생성하려면 셀프 서비스 포털 활성화(Enable self-service portal)를 켭니다.
15. 세션 제한 시간(Session timeout hours)에서 사용 가능한 옵션에서 원하는 최대 VPN 세션 기간(시간)을 선택하거나 기본값 24시간으로 설정된 상태로 둡니다.
16. 세션 제한 시간 도달 시 연결 해제에서 최대 세션 시간에 도달할 때 세션을 종료할지 여부를 선택합니다. 이 옵션을 선택하면 세션 시간이 초과한 경우 사용자가 엔드포인트에 수동으로 다시 연결해야 합니다. 그렇지 않으면 Client VPN이 자동으로 다시 연결을 시도합니다.
17. 클라이언트 로그인 배너 활성화(Enable client login banner)를 켜거나 끕니다. 클라이언트 로그인 배너를 사용하려면 VPN 세션이 설정될 때 AWS 제공 클라이언트의 배너에 표시될 텍스트를 입력합니다. UTF-8로 인코딩된 문자만 허용됩니다. 최대 1,400자입니다.
18. 클라이언트 VPN 엔드포인트 수정(Modify Client VPN endpoint)을 선택합니다.

AWS CLI를 사용하여 Client VPN 엔드포인트를 수정하려면

modify-client-vpn-endpoint 명령을 사용합니다.

IPv4 엔드포인트를 듀얼 스택으로 수정하는 예:

```
aws ec2 modify-client-vpn-endpoint \
  --client-vpn-endpoint-id cvpn-endpoint-123456789123abcde \
  --endpoint-ip-address-type "dual-stack" \
  --traffic-ip-address-type "dual-stack" \
  --client-cidr-block "172.31.0.0/16"
```

AWS Client VPN 엔드포인트 삭제

Client VPN 엔드포인트를 삭제하려면 먼저 모든 대상 네트워크를 연결 해제해야 합니다. Client VPN 엔드포인트를 삭제하면 상태가 `deleting`으로 전환되고 클라이언트가 더 이상 해당 엔드포인트에 연결할 수 없습니다.

콘솔 또는 를 사용하여 Client VPN 엔드포인트를 삭제할 수 있습니다AWS CLI

Client VPN 엔드포인트를 삭제하려면(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.

3. 삭제할 Client VPN 엔드포인트를 선택합니다. 작업(Actions), 클라이언트 VPN 엔드포인트 삭제(Delete Client VPN endpoint)를 선택합니다.
4. 확인 창에 delete를 입력한 다음 삭제(Delete)를 선택합니다.

Client VPN 엔드포인트를 삭제하려면(AWS CLI)

delete-client-vpn-endpoint 명령을 사용합니다.

AWS Client VPN 연결 로그

새 Client VPN 엔드포인트 또는 기존 Client VPN 엔드포인트에 연결 로깅을 활성화하고 연결 로그 캡처를 시작할 수 있습니다. 연결 로그는 Client VPN 엔드포인트에 대한 로그 이벤트 시퀀스를 보여줍니다. 연결 로깅을 활성화하면 로그 그룹에서 로그 스트림의 이름을 지정할 수 있습니다. 로그 스트림을 지정하지 않으면 Client VPN 서비스에서 자동으로 로그 스트림을 생성합니다. 그런 다음 연결 로깅은 클라이언트 연결 요청, 클라이언트 연결 결과(성공 또는 실패), 연결 실패 원인, 엔드포인트의 클라이언트 종료 시간을 기록합니다.

시작하기 전에 계정에 CloudWatch Logs 로그 그룹이 있어야 합니다. 자세한 내용은 Amazon CloudWatch Logs 사용 설명서의 로그 그룹 및 로그 스트림 작업을 참조하십시오. CloudWatch Logs 이용 시 요금이 부과됩니다. 자세한 내용은 Amazon CloudWatch 요금을 참조하세요.

Client VPN 연결 로그는 Amazon VPC 콘솔 또는 AWS CLI를 사용하여 생성할 수 있습니다.

Tasks

- 새 AWS Client VPN 엔드포인트에 대한 연결 로깅 활성화
- 기존 AWS Client VPN 엔드포인트에 대한 연결 로깅 활성화
- AWS Client VPN 연결 로그 보기
- AWS Client VPN 연결 로깅 끄기

새 AWS Client VPN 엔드포인트에 대한 연결 로깅 활성화

콘솔 또는 명령줄을 사용하여 새 Client VPN 엔드포인트를 생성할 때 연결 로깅을 활성화할 수 있습니다.

콘솔을 사용하여 새 Client VPN 엔드포인트에 연결 로깅을 활성화하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.

2. 탐색 창에서 클라이언트 VPN 엔드포인트(Client VPN Endpoints)를 선택한 다음 클라이언트 VPN 엔드포인트 생성(Create Client VPN endpoint)을 선택합니다.
3. Connection Logging(연결 로깅) 섹션에 도달할 때까지 옵션을 완료합니다. 이러한 옵션에 대한 자세한 내용은 AWS Client VPN엔드포인트 생성을 참조하세요.
4. 연결 로깅(Connection logging)에서 클라이언트 연결에 대한 로그 세부 정보 사용(Enable log details on client connections)을 설정합니다.
5. CloudWatch Logs 로그 그룹 이름(CloudWatch Logs log group name)에서 CloudWatch Logs 로그 그룹의 이름을 선택합니다.
6. (선택 사항) CloudWatch Logs 로그 스트림 이름(CloudWatch Logs log stream name)에서 CloudWatch Logs 로그 스트림의 이름을 선택합니다.
7. 클라이언트 VPN엔드포인트 생성(Create Client VPN endpoint)을 선택합니다.

를 사용하여 새 Client VPN 엔드포인트에 대한 연결 로깅을 활성화하려면 AWS CLI

create-client-vpn-endpoint 명령을 사용하고 `--connection-log-options` 파라미터를 지정합니다. 다음 예제와 같이 JSON 형식으로 연결 로그 정보를 지정할 수 있습니다.

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

기존 AWS Client VPN 엔드포인트에 대한 연결 로깅 활성화

콘솔 또는 명령줄을 사용하여 기존 Client VPN 엔드포인트에 연결 로깅을 활성화할 수 있습니다.

콘솔을 사용하여 기존 Client VPN 엔드포인트에 연결 로깅을 활성화하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. Client VPN 엔드포인트를 선택하고 작업(Actions)을 선택한 다음 클라이언트 VPN 엔드포인트 수정(Modify Client VPN endpoint)을 선택합니다.
4. 연결 로깅(Connection logging)에서 클라이언트 연결에 대한 로그 세부 정보 사용(Enable log details on client connections)을 설정합니다.
5. CloudWatch Logs 로그 그룹 이름(CloudWatch Logs log group name)에서 CloudWatch Logs 로그 그룹의 이름을 선택합니다.

6. (선택 사항) CloudWatch Logs 로그 스트림 이름(CloudWatch Logs log stream name)에서 CloudWatch Logs 로그 스트림의 이름을 선택합니다.
7. 클라이언트 VPN 엔드포인트 수정(Modify Client VPN endpoint)을 선택합니다.

를 사용하여 기존 Client VPN 엔드포인트에 대한 연결 로깅을 활성화하려면 AWS CLI

modify-client-vpn-endpoint 명령을 사용하고 `--connection-log-options` 파라미터를 지정합니다. 다음 예제와 같이 JSON 형식으로 연결 로그 정보를 지정할 수 있습니다.

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

AWS Client VPN 연결 로그 보기

CloudWatch Logs 콘솔을 사용하여 Client VPN 연결 로그를 볼 수 있습니다.

콘솔을 사용하여 연결 로그를 보려면

1. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 Log groups(로그 그룹)을 선택하고 연결 로그가 포함된 로그 그룹을 선택합니다.
3. Client VPN 엔드포인트에 대한 로그 스트림을 선택합니다.

> **Note**
>
> 타임스탬프(Timestamp) 열에는 연결 시간이 아니라 연결 로그가 CloudWatch Logs에 게시된 시간이 표시됩니다.

로그 데이터 검색에 대한 자세한 내용은 Amazon CloudWatch Logs 사용 설명서의 필터 패턴을 사용하여 로그 데이터 검색을 참조하세요.

AWS Client VPN 연결 로깅 끄기

콘솔 또는 명령줄을 사용하여 Client VPN 엔드포인트에 대한 연결 로깅을 끌 수 있습니다. 연결 로깅을 꺼도 CloudWatch Logs의 기존 연결 로그는 삭제되지 않습니다.

콘솔을 사용하여 연결 로깅을 끄려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. Client VPN 엔드포인트를 선택하고 작업(Actions)을 선택한 다음 클라이언트 VPN 엔드포인트 수정(Modify Client VPN endpoint)을 선택합니다.
4. 연결 로깅(Connection logging)에서 클라이언트 연결에 대한 로그 세부 정보 활성화(Enable log details on client connections)를 끕니다.
5. 클라이언트 VPN 엔드포인트 수정(Modify Client VPN endpoint)을 선택합니다.

AWS CLI를 사용하여 연결 로깅을 끄려면

modify-client-vpn-endpoint 명령을 사용하고 `--connection-log-options` 파라미터를 지정합니다. `Enabled`가 `false`로 설정되어 있는지 확인합니다.

AWS Client VPN 엔드포인트 구성 파일 내보내기

AWS Client VPN 엔드포인트 구성 파일은 클라이언트(사용자)가 Client VPN 엔드포인트와의 VPN 연결을 설정하는 데 사용하는 파일입니다. 이 파일을 다운로드(내보내기)하여 VPN에 액세스해야 하는 모든 클라이언트에게 배포해야 합니다. 또는 Client VPN 엔드포인트에 대해 셀프 서비스 포털을 활성화한 경우 클라이언트가 포털에 로그인하여 구성 파일을 직접 다운로드할 수 있습니다. 자세한 내용은 셀프 서비스 포털에 대한 AWS Client VPN 액세스 단원을 참조하십시오.

Client VPN 엔드포인트가 상호 인증을 사용하는 경우 다운로드한 .ovpn 구성 파일에 클라이언트 인증서와 클라이언트 프라이빗 키를 추가해야 합니다. 정보를 추가한 다음, 클라이언트는 .ovpn 파일을 OpenVPN 클라이언트 소프트웨어로 가져올 수 있습니다.

> **Important**
>
> 클라이언트 인증서 및 클라이언트 프라이빗 키 정보를 파일에 추가하지 않으면 상호 인증을 사용하여 인증하는 클라이언트가 Client VPN 엔드포인트에 연결할 수 없습니다.

기본적으로 OpenVPN 클라이언트 구성의 "remote-random-hostname" 옵션은 와일드 카드 DNS를 활성화합니다. 와일드 카드 DNS가 활성화되므로 클라이언트가 엔드포인트의 IP 주소를 캐싱하지 않으며 엔드포인트의 DNS 이름을 ping할 수 없습니다.

Client VPN 엔드포인트가 Active Directory 인증을 사용하고 클라이언트 구성 파일을 배포한 후 디렉터리에서 Multi-Factor Authentication(MFA)을 활성화한 경우 새 파일을 다운로드하여 클라이언트에 다시 배포해야 합니다. 클라이언트는 이전 구성 파일을 사용하여 Client VPN 엔드포인트에 연결할 수 없습니다.

태스크

- AWS Client VPN 클라이언트 구성 파일 내보내기
- 상호 인증을 위한 AWS Client VPN 클라이언트 인증서 및 키 정보 추가

AWS Client VPN 클라이언트 구성 파일 내보내기

콘솔 또는 AWS CLI를 사용하여 Client VPN 클라이언트 구성을 내보낼 수 있습니다.

클라이언트 구성을 내보내는 방법(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 클라이언트 구성을 다운로드할 Client VPN 엔드포인트를 선택하고 Download Client Configuration(클라이언트 구성 다운로드)을 선택합니다.

클라이언트 구성을 내보내려면(AWS CLI)

export-client-vpn-client-configuration 명령을 사용하고 출력 파일 이름을 지정합니다.

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

상호 인증을 위한 AWS Client VPN 클라이언트 인증서 및 키 정보 추가

Client VPN 엔드포인트가 상호 인증을 사용하는 경우 다운로드한 .ovpn 구성 파일에 클라이언트 인증서와 클라이언트 프라이빗 키를 추가해야 합니다.

상호 인증을 사용할 때는 클라이언트 인증서를 수정할 수 없습니다.

클라이언트 인증서 및 키 정보를 추가하려면(상호 인증)

다음 옵션 중 하나를 사용할 수 있습니다.

(옵션 1) 클라이언트 인증서 및 키를 Client VPN 엔드포인트 구성 파일과 함께 클라이언트에 배포합니다. 이 경우 구성 파일에 인증서 및 키의 경로를 지정합니다. 선호하는 텍스트 편집기를 사용하여 구성 파일을 열고 파일 끝부분에 다음을 추가합니다. */path/*를 클라이언트 인증서 및 키의 위치로 바꿉니다(위치는 엔드포인트에 연결하는 클라이언트를 기준으로 함).

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

(옵션 2) 구성 파일에 <cert></cert> 태그 사이에 클라이언트 인증서의 내용을 추가하고 <key></key> 태그 사이에 프라이빗 키의 내용을 추가합니다. 이 옵션을 선택하면 구성 파일만 클라이언트에 배포됩니다.

Client VPN 엔드포인트에 연결할 각 사용자에 대해 별도의 클라이언트 인증서 및 키를 생성한 경우 각 사용자에 대해 이 단계를 반복합니다.

다음은 클라이언트 인증서 및 키를 포함하는 Client VPN 구성 파일 형식의 예입니다.

```
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 경로

각 AWS Client VPN 엔드포인트에는 사용 가능한 대상 네트워크 경로를 설명하는 라우팅 테이블이 있습니다. 라우팅 테이블의 각 라우팅은 네트워크 트래픽이 전달되는 위치를 결정합니다. 각 Client VPN 엔드포인트 라우팅의 권한 부여 규칙을 구성하여 대상 네트워크에 액세스할 수 있는 클라이언트를 지정해야 합니다.

Client VPN 엔드포인트에 VPC의 서브넷을 연결하면 해당 VPC에 대한 라우팅이 자동으로 Client VPN 엔드포인트의 라우팅 테이블에 추가됩니다. 피어링된 VPC, 온프레미스 네트워크, 로컬 네트워크(클라이언트가 서로 통신할 수 있도록) 또는 인터넷과 같은 추가 네트워크에 대한 액세스를 활성화하려면 Client VPN 엔드포인트의 라우팅 테이블에 경로를 수동으로 추가해야 합니다.

> **Note**
>
> 여러 서브넷을 Client VPN 엔드포인트에 연결 중인 경우 여기 문제 해결 AWS Client VPN: 피어링된 VPC, Amazon S3 또는 인터넷에 대한 액세스가 간헐적임에 설명된 대로 각 서브넷에 대한 경로를 생성해야 합니다. 연결된 각 서브넷에는 동일한 경로 집합이 있어야 합니다.

Client VPN 엔드포인트에서 분할 터널을 사용하기 위한 고려 사항

Client VPN 엔드포인트에서 분할 터널을 사용하면 VPN이 설정될 때 Client VPN 라우팅 테이블에 있는 모든 경로가 클라이언트 라우팅 테이블에 추가됩니다. VPN을 설정한 후 라우팅을 추가하는 경우 새 라우팅이 클라이언트로 전송되도록 연결을 재설정해야 합니다.

Client VPN 엔드포인트 라우팅 테이블을 수정하기 전에 클라이언트 디바이스가 처리할 수 있는 라우팅 수를 고려하는 것이 좋습니다.

태스크

- AWS Client VPN 엔드포인트 라우팅 생성
- AWS Client VPN 엔드포인트 라우팅 보기
- AWS Client VPN 엔드포인트 라우팅 삭제

AWS Client VPN 엔드포인트 라우팅 생성

Client VPN 엔드포인트 라우팅을 생성할 때 대상 네트워크의 트래픽이 어떻게 전달될지 지정합니다.

클라이언트에게 인터넷 액세스를 허용하려면 대상 `0.0.0.0/0` 라우팅을 추가합니다.

콘솔과 를 사용하여 Client VPN 엔드포인트에 경로를 추가할 수 있습니다AWS CLI

Client VPN 엔드포인트 라우팅을 생성하려면(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 라우팅을 추가할 Client VPN 엔드포인트를 선택하고 라우팅 테이블(Route table)을 선택한 다음 경로 생성(Create route)을 선택합니다.
4. Route destination(라우팅 대상 주소)에 대상 네트워크의 IPv4 CIDR 범위를 지정합니다. 예:
   - Client VPN 엔드포인트의 VPC에 대한 경로를 추가하려면 VPC의 IPv4 CIDR 범위를 입력합니다.
   - 인터넷 액세스용 라우팅을 추가하려면 `0.0.0.0/0`을 입력합니다.
   - 피어링된 VPC에 대한 라우팅을 추가하려면 피어링된 VPC의 IPv4 CIDR 범위를 입력합니다.
   - 온프레미스 네트워크에 대한 경로를 추가하려면 AWS Site-to-Site VPN 연결의 IPv4 CIDR 범위를 입력합니다.
5. 대상 네트워크 연결용 서브넷 ID(Subnet ID for target network association)에서 Client VPN 엔드포인트에 연결된 서브넷을 선택합니다.

   또는 로컬 Client VPN 엔드포인트 네트워크에 대한 경로를 추가하려는 경우 `local`을 선택합니다.
6. (선택 사항) 설명(Description)에 스냅샷에 대한 간략한 설명을 입력합니다.
7. 경로 생성(Create route)을 선택합니다.

Client VPN 엔드포인트 경로를 생성하려면(AWS CLI)

create-client-vpn-route 명령을 사용합니다.

AWS Client VPN 엔드포인트 라우팅 보기

콘솔 또는 를 사용하여 특정 Client VPN 엔드포인트의 경로를 볼 수 있습니다AWS CLI

Client VPN 엔드포인트 라우팅을 보려면(콘솔)

1. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
2. 라우팅을 보려는 Client VPN 엔드포인트를 선택하고 라우팅 테이블(Route table)을 선택합니다.

Client VPN 엔드포인트 경로를 보려면(AWS CLI)

describe-client-vpn-routes 명령을 사용합니다.

AWS Client VPN 엔드포인트 라우팅 삭제

수동으로 추가한 Client VPN 라우팅만 삭제할 수 있습니다. 서브넷을 Client VPN 엔드포인트에 연결할 때 자동으로 추가된 라우팅은 삭제할 수 없습니다. 자동으로 추가된 라우팅을 삭제하려면 해당 라우팅을 생성한 서브넷을 Client VPN 엔드포인트에서 연결 해제해야 합니다.

콘솔 또는 를 사용하여 Client VPN 엔드포인트에서 경로를 삭제할 수 있습니다AWS CLI

Client VPN 엔드포인트 라우팅을 삭제하려면(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 라우팅을 삭제할 Client VPN 엔드포인트를 선택하고 라우팅 테이블(Route table)을 선택합니다.
4. 삭제할 경로를 선택하고 Delete route(경로 삭제), Delete route(경로 삭제)를 선택합니다.

Client VPN 엔드포인트 경로를 삭제하려면(AWS CLI)

delete-client-vpn-route 명령을 사용합니다.

AWS Client VPN 대상 네트워크

대상 네트워크는 VPC 안의 서브넷입니다. 클라이언트가 연결하여 VPN 연결을 설정할 수 있도록 AWS Client VPN 엔드포인트에 하나 이상의 대상 네트워크가 있어야 합니다.

구성할 수 있는 액세스 종류(예: 클라이언트가 인터넷에 액세스할 수 있도록 설정)에 대한 자세한 내용은 Client VPN의 시나리오 및 예제 섹션을 참조하세요.

Client VPN 대상 네트워크 요구 사항

대상 네트워크를 생성할 때 다음 규칙이 적용됩니다.

- 서브넷에는 /27 비트마스크(예: 10.0.0.0/27)가 있는 CIDR 블록이 있어야 합니다. 또한 서브넷에는 항상 최소 20개의 사용 가능한 IP 주소가 있어야 합니다.
- 서브넷의 CIDR 블록은 Client VPN 엔드포인트의 클라이언트 CIDR 범위와 겹칠 수 없습니다.
- 하나 이상의 서브넷을 Client VPN 엔드포인트에 연결하는 경우 각 서브넷은 서로 다른 가용 영역에 있어야 합니다. 서브넷을 2개 이상 연결하여 가용 영역 중복성을 제공하는 것이 좋습니다.

- Client VPN 엔드포인트를 생성할 때 VPC를 지정한 경우 서브넷은 동일한 VPC에 있어야 합니다. 아직 VPC를 Client VPN 엔드포인트에 연결하지 않은 경우 모든 VPC에서 서브넷을 선택할 수 있습니다.

  이후의 모든 서브넷 연결은 동일한 VPC에서 이루어져야 합니다. 다른 VPC의 서브넷을 연결하려면 먼저 Client VPN 엔드포인트를 수정하고 연결된 VPC를 변경해야 합니다. 자세한 내용은 AWS Client VPN 엔드포인트 수정 섹션을 참조하세요.

Client VPN 엔드포인트에 서브넷을 연결하면 연결된 서브넷이 프로비저닝되는 VPC의 로컬 경로가 자동으로 Client VPN 엔드포인트의 라우팅 테이블에 추가됩니다.

> **Note**
>
> 대상 네트워크가 연결된 후 연결된 VPC에 CIDR을 추가하거나 제거할 때 다음 작업 중 하나를 수행하여 Client VPN 엔드포인트 라우팅 테이블의 로컬 경로를 업데이트해야 합니다.
>
> - 대상 네트워크에서 Client VPN 엔드포인트를 분리한 다음 Client VPN 엔드포인트를 대상 네트워크에 연결합니다.
> - 수동으로 경로를 추가하거나 Client VPN 엔드포인트 라우팅 테이블에서 경로를 제거합니다.

Client VPN 엔드포인트에 첫 번째 서브넷을 연결하면 Client VPN 엔드포인트의 상태가 `pending-associate`에서 `available`로 전환되고 클라이언트가 VPN 연결을 설정할 수 있게 됩니다.

Tasks

- 대상 네트워크를 AWS Client VPN 엔드포인트와 연결
- 의 대상 네트워크에 보안 그룹 적용 AWS Client VPN
- AWS Client VPN 대상 네트워크 보기
- AWS Client VPN 엔드포인트에서 대상 네트워크 연결 해제

대상 네트워크를 AWS Client VPN 엔드포인트와 연결

Amazon VPC 콘솔 또는 AWS CLI를 사용하여 하나 이상의 대상 네트워크(서브넷)를 Client VPN 엔드포인트와 연결할 수 있습니다. 대상 네트워크를 Client VPN 엔드포인트에 연결하기 전에 요구 사항을 숙지하세요. 대상 네트워크 생성 요구 사항을(를) 참조하세요.

Client VPN 엔드포인트에 대상 네트워크를 연결하려면(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 대상 네트워크를 연결할 Client VPN 엔드포인트를 선택하고 대상 네트워크 연결(Target network associations), 대상 네트워크 연결(Associate target network)을 차례로 선택합니다.
4. VPC에서 서브넷이 있는 VPC를 선택합니다. Client VPN 엔드포인트를 생성할 때 VPC를 지정했거나 이전 서브넷 연결이 있는 경우 동일한 VPC여야 합니다.
5. 연결할 서브넷 선택(Choose a subnet to associate)에서 Client VPN 엔드포인트에 연결할 서브넷을 선택합니다.
6. 대상 네트워크 연결(Associate target network)을 선택합니다.

대상 네트워크를 Client VPN 엔드포인트에 연결하려면(AWS CLI)

associate-client-vpn-target-network 명령을 사용합니다.

의 대상 네트워크에 보안 그룹 적용 AWS Client VPN

Client VPN 엔드포인트를 만들 때 대상 네트워크에 적용할 보안 그룹을 지정할 수 있습니다. 첫 번째 대상 네트워크를 Client VPN 엔드포인트에 연결하면 연결된 서브넷이 위치하는 VPC의 기본 보안 그룹이 자동으로 적용됩니다. 자세한 내용은 보안 그룹 단원을 참조하십시오.

Client VPN 엔드포인트의 보안 그룹을 변경할 수 있습니다. 필요한 보안 그룹 규칙은 구성하려는 VPN 액세스의 종류에 따라 다릅니다. 자세한 내용은 Client VPN의 시나리오 및 예제 단원을 참조하십시오.

대상 네트워크에 보안 그룹을 적용하는 방법(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 보안 그룹을 적용할 Client VPN 엔드포인트를 선택합니다.
4. 보안 그룹(Security Groups)을 선택한 다음, 보안 그룹 적용(Apply Security Groups)을 선택합니다.
5. 보안 그룹 ID(Security group IDs)에서 해당 보안 그룹을 선택합니다.
6. 보안 그룹 적용(Apply Security Groups)을 선택합니다.

대상 네트워크에 보안 그룹을 적용하려면(AWS CLI)

apply-security-groups-to-client-vpn-target-network 명령을 사용합니다.

AWS Client VPN 대상 네트워크 보기

콘솔 또는 를 사용하여 Client VPN 엔드포인트에 연결된 대상을 볼 수 있습니다AWS CLI

대상 네트워크를 보는 방법(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 해당 Client VPN 엔드포인트를 선택하고 대상 네트워크 연결(Target network associations)을 선택합니다.

를 사용하여 대상 네트워크를 보려면AWS CLI

describe-client-vpn-target-networks 명령을 사용합니다.

AWS Client VPN 엔드포인트에서 대상 네트워크 연결 해제

대상 네트워크의 연결을 해제하면 대상 네트워크 연결 시 자동으로 생성된 경로(VPC의 로컬 경로)뿐만 아니라 Client VPN 엔드포인트의 라우팅 테이블에 수동으로 추가된 모든 경로가 삭제됩니다. Client VPN 엔드포인트에서 모든 대상 네트워크를 연결 해제하면 클라이언트가 더 이상 VPN 연결을 설정할 수 없습니다.

Client VPN 엔드포인트에서 대상 네트워크를 연결 해제하려면(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 대상 네트워크가 연결된 Client VPN 엔드포인트를 선택하고 대상 네트워크 연결(Target network associations)을 선택합니다.
4. 연결 해제할 대상 네트워크를 선택하고 연결 해제(Disassociate)를 선택한 다음 대상 네트워크 연결 해제(Disassociate target network)를 선택합니다.

Client VPN 엔드포인트에서 대상 네트워크를 연결 해제하려면(AWS CLI)

disassociate-client-vpn-target-network 명령을 선택합니다.

AWS Client VPN 최대 VPN 세션 기간 제한 시간

AWS Client VPN 는 Client VPN 엔드포인트에 대한 클라이언트 연결에 허용되는 최대 시간인 최대 VPN 세션 기간에 대한 몇 가지 옵션을 제공합니다. 보안 및 규정 준수 요구 사항을 충족하도록 지원하기 위해 더 짧은 최대 VPN 세션 기간을 구성할 수 있습니다. 기본적으로 최대 VPN 세션 기간은 24시간입니다. 최대 세션 기간을 설정하면 해당 제한 시간에 도달했을 때 해당 세션에서 무엇을 할지 제어할 수 있습니다. 세션 제한 시간 도달 시 연결 해제 옵션을 사용하면 세션을 종료하거나 엔드포인트에 대한 재연결을 자동으로 시도할 수 있습니다. 세션을 종료하면 최대 VPN 세션 기간을 적용하여 엔드포인트 보안을 더 잘 제어할 수 있습니다. 최대 시간에 도달했을 때 세션이 종료되도록 설정된 경우 VPN 연결을 다시 설정하려면 사용자가 다시 연결하고 인증 자격 증명을 제공해야 합니다.

세션 제한 시간 도달 시 연결 해제 설정이 자동 재연결로 설정된 경우, 최대 세션 시간에 도달하면

- 캐시된 사용자 자격 증명(Active Directory) 또는 인증서 기반 인증(상호 인증) 시 새로운 세션이 자동으로 설정됩니다. 연결을 완전히 해제하고 자동으로 다시 연결하지 않으려면 이러한 사용자는 수동으로 연결을 해제해야 합니다.
- 연동 인증(SAML)의 경우 새 세션이 자동으로 설정되지 않습니다. 이러한 사용자는 세션 제한 시간이 만료된 후 다시 인증하여 VPN 연결을 다시 설정해야 합니다.

> **Note**
>
> - 최대 VPN 세션 지속 시간 값이 현재 값에서 감소하면 새로 설정된 지속 시간보다 긴 기간 동안 엔드포인트에 연결된 모든 활성 VPN 세션이 연결 해제됩니다.
> - 세션 제한 시간 도달 시 연결 해제 옵션을 변경하면 현재 열려 있는 모든 세션에 새 설정이 적용됩니다.

AWS Client VPN 엔드포인트 생성 중 최대 VPN 세션 구성

VPN 세션 기간은 Client VPN 엔드포인트를 생성하는 동안 구성됩니다. Client VPN 엔드포인트를 생성하고 최대 세션 기간을 설정하는 단계는 AWS Client VPN엔드포인트 생성 섹션을 참조하세요.

태스크

- AWS Client VPN 현재 최대 VPN 세션 기간 보기
- 최대 AWS Client VPN 세션 기간 및 제한 시간 동작 수정

AWS Client VPN 현재 최대 VPN 세션 기간 보기

현재 Client VPN 최대 VPN 세션 기간을 보려면 다음 단계를 사용합니다.

Client VPN 엔드포인트에 대한 현재 최대 VPN 세션 기간 보기(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 보려는 Client VPN 엔드포인트를 선택합니다.
4. 세부 정보(Details) 탭이 선택되어 있는지 확인합니다.
5. 세션 제한 시간 옆의 현재 최대 VPN 세션 기간과 제한 시간 연결 해제가 활성화 또는 비활성화되어 있는지 확인합니다.

Client VPN 엔드포인트에 대한 현재 최대 VPN 세션 기간 보기(AWS CLI)

describe-client-vpn-endpoints 명령을 사용합니다.

최대 AWS Client VPN 세션 기간 및 제한 시간 동작 수정

기존 클라이언트 VPN의 최대 VPN 세션 기간을 수정하고 세션 시간 초과 시 연결 해제 동작을 변경하려면 다음 단계를 따릅니다.

Client VPN 엔드포인트에 대한 기존 최대 VPN 세션 기간 수정(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 클라이언트 VPN 엔드포인트(Client VPN endpoints)를 선택합니다.
3. 수정할 Client VPN 엔드포인트를 선택하고 작업(Actions)을 선택한 다음 Client VPN 엔드포인트 수정(Modify Client VPN Endpoint)을 선택합니다.
4. 세션 제한 시간(Session timeout hours)에서 원하는 최대 VPN 세션 기간(시간)을 선택합니다.
5. 세션 제한 시간 도달 시 연결 해제에서 최대 세션 제한 시간에 도달했을 때 세션 연결을 해제할지 여부를 선택합니다. 기본적으로 엔드포인트를 처음 수정할 때 이 기능이 해제됩니다.
6. 클라이언트 VPN 엔드포인트 수정(Modify Client VPN endpoint)을 선택합니다.

Client VPN 엔드포인트에 대한 기존 최대 VPN 세션 기간 수정(AWS CLI)

modify-client-vpn-endpoint 명령을 사용합니다.

Client VPN과 Transit Gateway 통합

Client VPN 엔드포인트를 기본적으로 Transit Gateway에 연결하여 여러 VPCs, 온프레미스 네트워크 및 Transit Gateway에 연결된 기타 리소스에 안전하게 원격 액세스할 수 있습니다. 따라서 각 VPC에 대해 별도의 VPN 엔드포인트를 생성하거나 중간 VPCs.

주제

개요

Transit Gateway를 Client VPN 엔드포인트와 연결하면 Client VPN 엔드포인트에 적절한 경로 및 권한 부여 규칙이 구성된 경우 연결된 VPN 클라이언트가 Transit Gateway에 연결된 모든 리소스에 액세스할 수 있습니다.

Transit Gateway 관련 엔드포인트는 클라이언트 소스 IP 주소를 보존합니다. 소스 네트워크 주소 변환(SNAT)은 적용되지 않으므로 클라이언트 트래픽에 대한 가시성이 향상됩니다.

> **Important**
>
> VPC 서브넷 연결과 Transit Gateway 연결을 단일 Client VPN 엔드포인트에서 혼합할 수 없습니다. 엔드포인트를 생성할 때 연결 유형 하나를 선택합니다.

이점

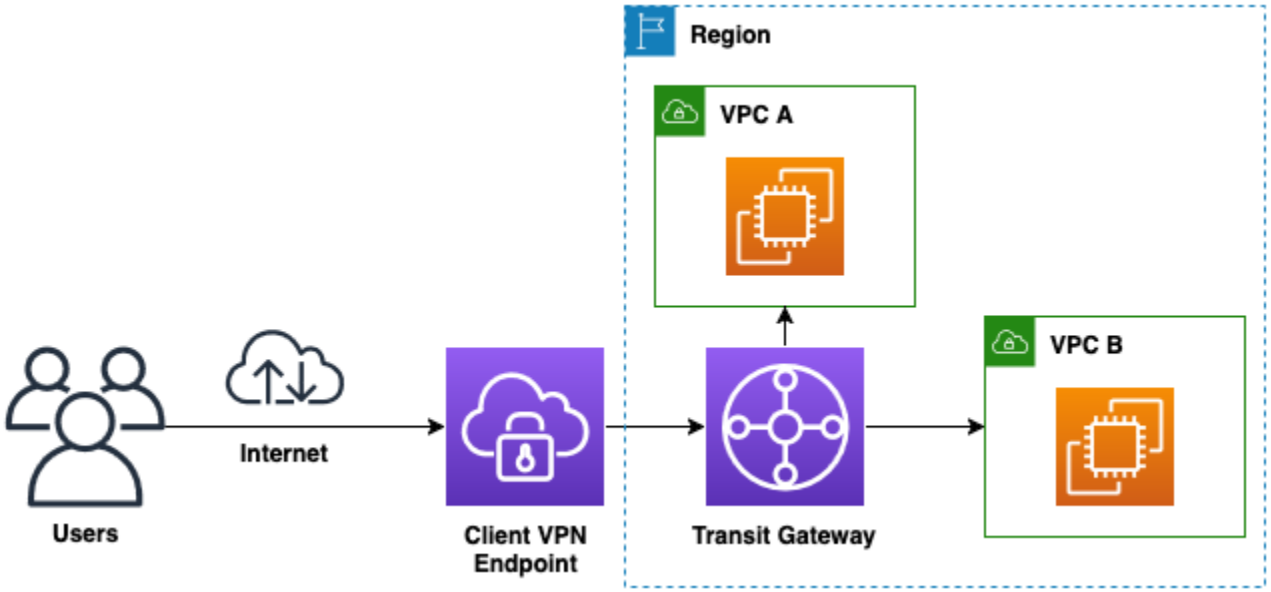
Client VPN과의 Transit Gateway 통합은 다음과 같은 이점을 제공합니다.

- 간소화된 관리 - VPC당 별도의 VPN 엔드포인트가 필요하지 않습니다. VPN 종료를 위해서만 중간 VPCs 생성할 필요가 없습니다.
- 중앙 집중식 라우팅 - Transit Gateway를 중앙 라우팅 허브로 활용합니다. 네트워크 전체에서 라우팅 관리를 간소화합니다.
- 향상된 가시성 - 클라이언트 소스 IP 주소(SNSAT 없음)를 보존합니다. Client VPN에 대한 흐름 로그 지원을 제공합니다.
- 확장성 - Client VPN을 통해 액세스할 수 있는 Transit Gateway에 새 VPCs를 쉽게 추가합니다. 대규모 원격 작업 인력 및 사업부를 지원하도록 확장합니다.
- 중앙 집중식 보안 - 연결된 모든 네트워크에서 일관된 보안 정책을 구현합니다. 포괄적인 감사 추적을 유지 관리합니다.

Transit Gateway 통합 작동 방식

다음은 Client VPN이 Transit Gateway와 작동하는 방법을 설명합니다.

1. 엔드포인트 생성 - Client VPN 엔드포인트를 생성하고 Transit Gateway ID를 지정합니다.
2. 연결 생성 - AWS 엔드포인트에 `client-vpn` 대한 유형의 Transit Gateway 연결을 자동으로 생성합니다.
3. 가용 영역 선택 - 사용할 가용 영역을 지정하거나 2개의 가용 영역을 자동으로 AWS 선택합니다.
4. 라우팅 구성 - Client VPN 엔드포인트 라우팅 테이블에 경로를 추가하여 Transit Gateway를 통해 클라이언트 트래픽을 대상 네트워크로 보냅니다.
5. 클라이언트 연결 흐름 - 클라이언트가 연결되면 트래픽이 클라이언트 VPN 엔드포인트를 통해 Transit Gateway로 흐른 다음 Transit Gateway 라우팅 테이블에 따라 대상 네트워크로 흐릅니다.



사전 조건

Transit Gateway 연결 Client VPN 엔드포인트를 생성하기 전에 다음 요구 사항을 확인합니다.

전송 게이트웨이 요구 사항

- Client VPN 엔드포인트와 동일한 리전의 기존 Transit Gateway입니다.
- 교차 계정 액세스의 경우 Transit Gateway를 계정과 공유해야 합니다 AWS Resource Access Manager.
- Transit Gateway에는 IPv4 CIDR 블록이 할당되어 있어야 합니다. IPv6 또는 듀얼 스택 구성을 사용하려는 경우 IPv6 CIDR 블록도 할당합니다.

네트워크 요구 사항

- 클라이언트 CIDR 범위는 Transit Gateway에 연결된 VPCs의 CIDR 범위와 겹치지 않아야 합니다.
- 선택한 가용 영역은 Transit Gateway에서 지원해야 합니다.
- VPC 라우팅 테이블에서 반환 경로를 구성하여 클라이언트 CIDR 범위로 향하는 트래픽을 Transit Gateway로 전달해야 합니다.

인증서 요구 사항

- Client VPN 엔드포인트와 동일한 리전의 AWS Certificate Manager (ACM)에 프로비저닝된 서버 인증서입니다.
- 상호 인증을 사용하는 경우 ACM에 프로비저닝된 클라이언트 인증서입니다.

Transit Gateway Client VPN 엔드포인트 생성

콘솔 또는를 사용하여 Transit Gateway와 연결된 Client VPN 엔드포인트를 생성할 수 있습니다 AWS CLI.

Transit Gateway Client VPN 엔드포인트를 생성하려면(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN Endpoints(Client VPN 엔드포인트)를 선택한 다음 Create Client VPN Endpoint(Client VPN 엔드포인트 생성)를 선택합니다.
3. (선택 사항) 이름 태그 및 설명에 엔드포인트의 이름과 설명을 입력합니다.
4. 트래픽 IP 주소 유형에서 다음 중 하나를 선택합니다.
   - IPv4 - 클라이언트 IPv4 CIDR 범위(예: `10.0.0.0/22`)를 지정합니다.
   - IPv6 - 클라이언트 IPv6 CIDR 범위를 AWS 자동으로 할당합니다.
   - 듀얼 스택 - 클라이언트 IPv4 CIDR 범위를 지정합니다.는 클라이언트 IPv6 CIDR 범위를 AWS 자동으로 할당합니다.
5. 서버 인증서 ARN에서 ACM에 프로비저닝된 TLS 인증서의 ARN을 지정합니다.
6. 인증 방법을 선택합니다. 자세한 내용은 의 클라이언트 인증 AWS Client VPN 단원을 참조하십시오.
7. (선택 사항) 연결 로깅에서 클라이언트 연결에 대한 로그 세부 정보 활성화를 켜고 CloudWatch Logs 로그 그룹 및 로그 스트림을 지정합니다.
8. 네트워크 인프라에서 전송 게이트웨이를 선택합니다.
9. Transit Gateway ID의 드롭다운 목록에서 Transit Gateway를 선택합니다.
10. (선택 사항) 가용 영역에서 최대 5개의 가용 영역을 선택합니다. 가용 영역을 선택하지 않으면가 자동으로 2를 AWS 선택합니다.
11. (선택 사항) DNS 서버, 전송 프로토콜, 분할 터널, VPN 포트, 세션 제한 시간 및 로그인 배너와 같은 추가 설정을 구성합니다.
12. 클라이언트 VPN엔드포인트 생성(Create Client VPN endpoint)을 선택합니다.

> **Note**
>
> 생성 후 엔드포인트 상태는 입니다`pending-associate`. Transit Gateway 연결은 자동으로 생성됩니다. 클라이언트는 연결을 사용할 수 있게 된 후 연결할 수 있습니다.

Transit Gateway Client VPN 엔드포인트를 생성하려면(AWS CLI)

create-client-vpn-endpoint 명령을 `--transit-gateway-id` 파라미터와 함께 사용합니다.

다음 예시에서는 특정 가용 영역이 있는 Client VPN 엔드포인트를 생성합니다.

```
aws ec2 create-client-vpn-endpoint \
    --client-cidr-block 10.0.0.0/22 \
    --server-certificate-arn arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
    --authentication-options Type=certificate-
authentication,MutualAuthentication={ClientRootCertificateChainArn=arn:aws:acm:us-
east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE} \
    --connection-log-options Enabled=false \
    --transit-gateway-id tgw-0a1b2c3d4e5f6EXAMPLE \
    --availability-zone-list us-east-1a us-east-1b us-east-1c
```

출력 예시:

```
{
    "ClientVpnEndpointId": "cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE",
    "Status": {
        "Code": "pending-associate"
    },
    "DnsName": "cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE.prod.clientvpn.us-
east-1.amazonaws.com"
}
```

가 2개의 가용 영역을 AWS 자동으로 선택하도록 하려면 `--availability-zone-list` 파라미터를 생략합니다.

```
aws ec2 create-client-vpn-endpoint \
    --client-cidr-block 10.0.0.0/22 \
    --server-certificate-arn arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
    --authentication-options Type=certificate-
authentication,MutualAuthentication={ClientRootCertificateChainArn=arn:aws:acm:us-
east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE} \
    --connection-log-options Enabled=false \
    --transit-gateway-id tgw-0a1b2c3d4e5f6EXAMPLE
```

Transit Gateway 연결 확인

엔드포인트를 생성한 후 Transit Gateway 연결이 생성되었는지 확인합니다.

Transit Gateway 연결을 확인하려면(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Attachment를 선택합니다.
3. 리소스 유형 = `client-vpn` 및 Client VPN 엔드포인트 ID와 일치하는 리소스 ID가 있는 연결을 찾습니다.
4. 상태가 인지 확인합니다`available`.

Transit Gateway 연결을 확인하려면(AWS CLI)

describe-transit-gateway-attachments 명령을 사용합니다.

```
aws ec2 describe-transit-gateway-attachments \
    --filters Name=transit-gateway-id,Values=tgw-0a1b2c3d4e5f6EXAMPLE Name=resource-
type,Values=client-vpn
```

엔드포인트에 대한 Transit Gateway 구성을 보려면 describe-client-vpn-endpoints 명령을 사용합니다.

```
aws ec2 describe-client-vpn-endpoints \
    --client-vpn-endpoint-ids cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE
```

출력에는 Transit Gateway ID 및 연결된 가용 영역이 있는 `TransitGatewayConfiguration` 객체가 포함됩니다.

경로 관리

> **Important**
>
> Transit Gateway 관련 엔드포인트의 경우 경로를 생성할 때 대상 서브넷 ID를 지정하지 않습니다. 트래픽은 Transit Gateway 연결을 통해 자동으로 전달됩니다.

경로를 추가하려면(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.

2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. Client VPN 엔드포인트를 선택하고 라우팅 테이블을 선택한 다음 라우팅 생성을 선택합니다.
4. 라우팅 대상에 대상 CIDR 범위(예: VPC 또는 `0.0.0.0/0` 모든 트래픽)`10.1.0.0/16`를 입력합니다.
5. (선택 사항) 설명에 경로에 대한 설명을 입력합니다.
6. 경로 생성(Create route)을 선택합니다.

경로를 추가하려면(AWS CLI)

`--target-vpc-subnet-id` 파라미터 없이 create-client-vpn-route 명령을 사용합니다.

```
aws ec2 create-client-vpn-route \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --destination-cidr-block 10.1.0.0/16
```

여러 경로를 추가하려면 각 대상 CIDR 범위에 대해 명령을 실행합니다.

```
# Route to VPC 1
aws ec2 create-client-vpn-route \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --destination-cidr-block 10.1.0.0/16

# Route to VPC 2
aws ec2 create-client-vpn-route \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --destination-cidr-block 10.2.0.0/16

# Route to on-premises network
aws ec2 create-client-vpn-route \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --destination-cidr-block 192.168.0.0/16
```

경로를 삭제하려면(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. Client VPN 엔드포인트를 선택하고 라우팅 테이블을 선택한 다음 라우팅을 선택한 다음 라우팅 삭제를 선택합니다.

4. 라우팅 삭제를 선택하여 확인합니다.

경로를 삭제하려면(AWS CLI)

delete-client-vpn-route 명령을 사용합니다.

```
aws ec2 delete-client-vpn-route \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --destination-cidr-block 10.1.0.0/16
```

권한 부여 구성

> **Important**
>
> Transit Gateway 관련 Client VPN 엔드포인트에는 보안 그룹 기반 권한 부여가 지원되지 않습니다. 네트워크 기반 권한 부여 규칙을 사용하여 클라이언트 액세스를 제어해야 합니다.

권한 부여 규칙을 추가하려면(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. Client VPN 엔드포인트를 선택하고 권한 부여 규칙을 선택한 다음 권한 부여 규칙 추가를 선택합니다.
4. 대상 네트워크에서 액세스를 활성화하려면 대상 CIDR 범위(예: `10.1.0.0/16`)를 입력합니다.
5. 에 대한 액세스 권한 부여에서 다음 중 하나를 선택합니다.
   - 모든 사용자에게 액세스 허용 - 인증된 모든 클라이언트가 대상 네트워크에 액세스할 수 있습니다.
   - 특정 액세스 그룹의 사용자에게 액세스 허용 - 액세스 그룹 ID에 Active Directory 그룹 SID 또는 IdP 그룹 이름을 입력합니다.
6. Add authorization rule(권한 부여 규칙 추가)을 선택합니다.

권한 부여 규칙을 추가하려면(AWS CLI)

authorize-client-vpn-ingress 명령을 사용합니다.

다음 예제에서는 모든 사용자에게 10.1.0.0/16 네트워크에 액세스할 수 있는 권한을 부여합니다.

```
aws ec2 authorize-client-vpn-ingress \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --target-network-cidr 10.1.0.0/16 \
    --authorize-all-groups
```

다음 예시에서는 특정 Active Directory 그룹에 권한을 부여합니다.

```
aws ec2 authorize-client-vpn-ingress \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --target-network-cidr 10.1.0.0/16 \
    --access-group-id S-1-2-34-1234567890-1234567890-1234567890-1234
```

가용 영역 관리

생성 후 Transit Gateway 관련 Client VPN 엔드포인트의 가용 영역을 수정할 수 있습니다.

단일 가용 영역을 추가하려면(AWS CLI)

associate-client-vpn-target-network 명령을 --availability-zone 파라미터와 함께 사용합니다.

```
aws ec2 associate-client-vpn-target-network \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --availability-zone us-east-1c
```

단일 가용 영역을 제거하려면(AWS CLI)

먼저 describe-client-vpn-target-networks 명령을 사용하여 가용 영역의 연결 ID를 찾습니다.

```
aws ec2 describe-client-vpn-target-networks \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE
```

그런 다음 연결 ID와 함께 disassociate-client-vpn-target-network 명령을 사용합니다.

```
aws ec2 disassociate-client-vpn-target-network \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --association-id cvpn-assoc-0a1b2c3d4e5f6EXAMPLE
```

교차 계정 전송 게이트웨이 액세스

다른 AWS 계정이 소유한 Transit Gateway와 연결된 Client VPN 엔드포인트를 생성할 수 있습니다. 이렇게 하려면 Transit Gateway 소유자가 Transit Gateway를 계정과 공유해야 합니다 AWS Resource Access Manager.

사전 조건

- Transit Gateway 소유자 계정 - 기존 Transit Gateway 및 리소스 공유를 생성할 수 있는 권한입니다 AWS Resource Access Manager.
- Client VPN 엔드포인트 계정 - Client VPN 엔드포인트를 생성하고 AWS Resource Access Manager 리소스 공유를 수락할 수 있는 권한입니다.

Client VPN 엔드포인트 계정에서 AWS Resource Access Manager 콘솔에서 또는 accept-resource-share-invitation 명령을 사용하여 리소스 공유를 수락합니다. 공유를 수락하면 Client VPN 엔드포인트를 생성할 때 Transit Gateway ID 드롭다운에 Transit Gateway가 나타납니다.

고려 사항 및 제한 사항

Client VPN과 Transit Gateway 통합을 사용할 때는 다음 사항을 고려하세요.

- 연결 제한
  - VPC 서브넷 연결과 Transit Gateway 연결을 단일 엔드포인트에서 혼합할 수 없습니다.
  - 각 엔드포인트는 하나의 연결 유형만 사용해야 합니다.
- 보안 그룹
  - Transit Gateway 엔드포인트에는 보안 그룹 기반 권한 부여가 지원되지 않습니다.
  - 네트워크 기반 권한 부여 규칙만 사용합니다.
- 라우팅 관리
  - Transit Gateway의 자동 라우팅 전파는 지원되지 않습니다.
  - 대상 네트워크의 경로를 수동으로 정의해야 합니다.
- CIDR 중첩
  - Client VPN CIDR 블록은 다른 Transit Gateway 연결 또는 Transit Gateway CIDR 블록과 겹치지 않아야 합니다.
  - Transit Gateway는 연결된 VPCs 간에 중복되는 CIDR 범위를 지원하지 않습니다.
- 리전 제한

  - Client VPN 엔드포인트와 Transit Gateway는 동일한 AWS 리전에 있어야 합니다.
  - Client VPN에는 교차 리전 Transit Gateway 피어링이 지원되지 않습니다.
- 가용 영역
  - 엔드포인트당 최대 5개의 가용 영역을 지정할 수 있습니다.
  - 지정하지 않으면가 2개의 가용 영역을 AWS 자동으로 할당합니다.
  - 지정된 모든 가용 영역은 Client VPN과 Transit Gateway 모두에서 지원되어야 합니다.
- 반환 라우팅
  - Transit Gateway에 연결된 VPCs에는 Client VPN CIDR로 향하는 트래픽을 Transit Gateway로 다시 라우팅하도록 구성된 반환 경로가 있어야 합니다.
  - 적절한 반환 라우팅이 없으면 VPN 클라이언트VPCs의 리소스에 액세스할 수 없습니다.
    - IPv4의 경우: 엔드포인트 생성 시 Client VPN CIDR이 알려져 있습니다.
    - IPv6의 경우: IPv6 클라이언트 CIDR 범위가에 의해 자동으로 할당되므로 Client VPN 엔드포인트에 할당된 IPv6 CIDR 범위(Client VPN 엔드포인트와 연결된 Transit Gateway 라우팅 테이블에서 가장 큰 CIDR 범위)를 확인하려면 Transit Gateway 라우팅 테이블을 설명해야 합니다 AWS Client VPN.
- 연결 및 흐름 로그
  - Transit Gateway 흐름 로그를 활성화하여 Transit Gateway로 들어오고 나가는 IP 트래픽에 대한 정보를 캡처할 수 있습니다. Client VPN 연결 로그를 활성화하여 Client VPN 연결 이벤트에 대한 정보를 캡처할 수 있습니다.
  - Transit Gateway 흐름 로그 이벤트의 클라이언트 IP 및 타임스탬프를 Client VPN 연결 로그의 동일한 클라이언트 IP 및 기간과 비교하여 Transit Gateway 흐름 로그 이벤트를 Client VPN 연결과 상호 연관시킬 수 있습니다.
- 인터넷 연결
  - 분할 터널 없이 Transit Gateway가 있는 Client VPN을 통해 인터넷에 액세스하려면 연결된 VPC에 NAT가 구성되어 있어야 합니다.
    - IPv4의 경우: Client VPN 클라이언트 IPs를 퍼블릭 IP 주소로 대체하도록 NAT 게이트웨이를 구성합니다.
    - IPv6의 경우: IPv6를 사용한 중앙 집중식 인터넷 아웃바운드 트래픽을 참조하세요.

AWS Client VPN의 보안

AWS에서 클라우드 보안은 가장 중요합니다. AWS 고객은 보안에 가장 보안에 민감한 조직의 요구 사항에 부합하도록 빌드된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 AWS와 사용자의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드의 보안: AWS는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다. AWS는 안전하게 사용할 수 있는 서비스 또한 제공합니다. 서드 파티 감사자는 AWS 규정 준수 프로그램의 일환으로 보안 효과를 정기적으로 테스트하고 검증합니다. AWS Client VPN에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램의 범위에 속하는 AWS 서비스를 참조하세요.
- 클라우드의 보안 – 귀하의 책임은 귀하가 사용하는 AWS 서비스에 의해 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

AWS Client VPN은 Amazon VPC 서비스의 일부입니다. Amazon VPC의 보안에 대한 자세한 내용은 Amazon VPC 사용 설명서의 보안을 참조하세요.

이 설명서는 Client VPN을 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표를 충족하도록 Client VPN을 구성하는 방법을 보여줍니다. 또한 Client VPN 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

- AWS Client VPN의 데이터 보호
- 에 대한 자격 증명 및 액세스 관리 AWS Client VPN
- AWS Client VPN의 복원성
- 의 인프라 보안AWS Client VPN
- 의 보안 모범 사례AWS Client VPN
- AWS Client VPN에 대한 IPv6 고려 사항

AWS Client VPN의 데이터 보호

AWS Shared Responsibility Model은 AWS Client VPN의 데이터 보호에 적용됩니다. 이 모델에서 설명하는 것처럼 AWS는 모든 AWS 클라우드를 실행하는 글로벌 인프라를 보호할 책임이 있습니다. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터를 보호하려면 AWS 계정 자격 증명을 보호하고 AWS IAM Identity Center 또는 AWS Identity and Access Management(IAM)를 통해 개별 사용자 계정을 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신하세요. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- AWS CloudTrail로 API 및 사용자 활동 로깅을 설정하세요. AWS 활동 캡처에 CloudTrail 추적을 사용하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- AWS 암호화 솔루션을 AWS 서비스 내의 모든 기본 보안 컨트롤과 함께 사용하세요.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 통해 AWS에 액세스할 때 FIPS 140-3 검증된 암호화 모듈이 필요한 경우, FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 Client VPN 또는 기타 AWS 서비스에서 콘솔, API, AWS CLI 또는 AWS SDK를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명을 URL에 포함해서는 안 됩니다.

전송 중 암호화

AWS Client VPN에서는 전송 계층 보안(TLS) 1.2 이상을 사용하여 모든 위치에서 보안 연결을 제공합니다.

인터네트워크 트래픽 개인 정보

인터네트워크 액세스 활성화

클라이언트가 Client VPN 엔드포인트를 통해 VPC 및 기타 네트워크에 연결하도록 할 수 있습니다. 자세한 정보와 지침은 Client VPN의 시나리오 및 예제 단원을 참조하십시오.

네트워크에 대한 액세스 제한

VPC의 특정 리소스에 대한 액세스를 제한하도록 Client VPN 엔드포인트를 구성할 수 있습니다. 사용자 기반 인증의 경우 Client VPN 엔드포인트에 액세스하는 사용자 그룹을 기반으로 네트워크 일부에 대한 액세스를 제한할 수도 있습니다. 자세한 정보는 Client VPN을 사용한 네트워크 액세스 제한을 참조하십시오.

클라이언트 인증

인증은 AWS 클라우드의 첫 번째 진입 지점에서 구현됩니다. 인증을 사용하여 클라이언트가 Client VPN 엔드포인트에 연결하도록 허용되는지 여부를 확인합니다. 인증이 성공하면 클라이언트가 Client VPN 엔드포인트에 연결하고 VPN 세션을 설정합니다. 인증이 실패하면 연결이 거부되고 클라이언트가 VPN 세션을 연결할 수 없습니다.

Client VPN에서는 다음과 같은 유형의 클라이언트 인증을 제공합니다.

- Active Directory 인증(사용자 기반)
- 상호 인증(인증서 기반)
- Single sign-on(SAML 기반 연동 인증)(사용자 기반)

에 대한 자격 증명 및 액세스 관리 AWS Client VPN

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. IAM 관리자는 누가 Client VPN 리소스를 사용하도록 인증되고(로그인됨) 권한이 부여되는지(권한 있음)를 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

- 대상
- ID를 통한 인증
- 정책을 사용하여 액세스 관리
- AWS Client VPN 에서 IAM을 사용하는 방법

- 에 대한 자격 증명 기반 정책 예제 AWS Client VPN
- AWS Client VPN 자격 증명 및 액세스 문제 해결
- 에 대한 서비스 연결 역할 사용 AWS Client VPN

대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 역할에 따라 다릅니다.

- 서비스 사용자 - 기능에 액세스할 수 없는 경우 관리자에게 권한 요청(참조AWS Client VPN 자격 증명 및 액세스 문제 해결)
- 서비스 관리자 - 사용자 액세스 결정 및 권한 요청 제출(AWS Client VPN 에서 IAM을 사용하는 방법 참조)
- IAM 관리자 - 액세스를 관리하기 위한 정책 작성(에 대한 자격 증명 기반 정책 예제 AWS Client VPN 참조)

ID를 통한 인증

인증은 자격 증명 자격 증명을 AWS 사용하여에 로그인하는 방법입니다. AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할을 수임하여 인증되어야 합니다.

AWS IAM Identity Center (IAM Identity Center), Single Sign-On 인증 또는 Google/Facebook 자격 증명과 같은 자격 증명 소스의 자격 증명을 사용하여 페더레이션 자격 증명으로 로그인할 수 있습니다. 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 AWS 계정에 로그인하는 방법 섹션을 참조하세요.

프로그래밍 방식 액세스를 위해는 요청에 암호화 방식으로 서명할 수 있는 SDK 및 CLI를 AWS 제공합니다. 자세한 내용은 IAM 사용 설명서의 API 요청용AWS Signature Version 4 섹션을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 AWS 계정 theroot 사용자라는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명이 필요한 작업은 IAM 사용 설명서의 루트 사용자 자격 증명이 필요한 작업 섹션을 참조하세요.

페더레이션 ID

가장 좋은 방법은 인간 사용자에게 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 서비스 사용하여에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 디렉터리, 웹 자격 증명 공급자 또는 자격 증명 소스의 자격 증명을 AWS 서비스 사용하여 Directory Service 에 액세스하는 사용자입니다. 페더레이션 ID는 임시 자격 증명을 제공하는 역할을 수임합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center를 추천합니다. 자세한 정보는 AWS IAM Identity Center 사용 설명서의 What is IAM Identity Center?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 개인 또는 애플리케이션에 대한 특정 권한을 가진 ID입니다. 장기 자격 증명이 있는 IAM 사용자 대신 임시 자격 증명을 사용하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 사용하여에 액세스하도록 인간 사용자에게 요구하기를 참조하세요.

IAM 그룹은 IAM 사용자 모음을 지정하고 대규모 사용자 집합에 대한 관리 권한을 더 쉽게 만듭니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자 사용 사례 섹션을 참조하세요.

IAM 역할

IAM 역할은 임시 자격 증명을 제공하는 특정 권한이 있는 자격 증명입니다. 사용자에서 IAM 역할(콘솔)로 전환하거나 또는 API 작업을 호출하여 역할을 수임할 수 있습니다. AWS CLI AWS 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

IAM 역할은 페더레이션 사용자 액세스, 임시 IAM 사용자 권한, 교차 계정 액세스, 교차 서비스 액세스 및 Amazon EC2에서 실행되는 애플리케이션에 유용합니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결될 때 권한을 정의합니다.는 보안 주체가 요청할 때 이러한 정책을 AWS 평가합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요 섹션을 참조하세요.

정책을 사용하여 관리자는 어떤 보안 주체가 어떤 리소스에 대해 어떤 조건에서 작업을 수행할 수 있는지 정의하여 누가 무엇을 액세스할 수 있는지 지정합니다.

기본적으로 사용자 및 역할에는 어떠한 권한도 없습니다. IAM 관리자는 IAM 정책을 생성하고 사용자가 수임할 수 있는 역할에 추가합니다. IAM 정책은 작업을 수행하기 위해 사용하는 방법과 관계없이 작업에 대한 권한을 정의합니다.

ID 기반 정책

ID 기반 정책은 ID(사용자, 사용자 그룹 또는 역할)에 연결하는 JSON 권한 정책 문서입니다. 이러한 정책은 자격 증명이 수행할 수 있는 작업, 대상 리소스 및 이에 관한 조건을 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

ID 기반 정책은 인라인 정책(단일 ID에 직접 포함) 또는 관리형 정책(여러 ID에 연결된 독립 실행형 정책)일 수 있습니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택 섹션을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 예를 들어 IAM 역할 신뢰 정책 및 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 사용할 수 없습니다.

기타 정책 유형

AWS 는 보다 일반적인 정책 유형에서 부여한 최대 권한을 설정할 수 있는 추가 정책 유형을 지원합니다.

- 권한 경계 - ID 기반 정책에서 IAM 엔터티에 부여할 수 있는 최대 권한을 설정합니다. 자세한 정보는 IAM 사용 설명서의 IAM 엔터티의 권한 범위를 참조하세요.
- 서비스 제어 정책(SCP) - AWS Organizations내 조직 또는 조직 단위에 대한 최대 권한을 지정합니다. 자세한 내용은AWS Organizations 사용 설명서의 서비스 제어 정책을 참조하세요.
- 리소스 제어 정책(RCP) – 계정의 리소스에 사용할 수 있는 최대 권한을 설정합니다. 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCP)을 참조하세요.
- 세션 정책 – 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

AWS Client VPN 에서 IAM을 사용하는 방법

IAM을 사용하여 Client VPN에 대한 액세스를 관리하기 전에 Client VPN과 함께 사용할 수 있는 IAM 기능을 알아보세요.

AWS Client VPN과 함께 사용할 수 있는 IAM 기능

IAM 특성	Client VPN 지원
자격 증명 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	예
ACL	아니요
ABAC(정책의 태그)	예
임시 보안 인증	예
엔터티 권한	예
서비스 역할	예
서비스 연결 역할	예

Client VPN에 대한 자격 증명 기반 정책

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. JSON 정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

Client VPN 자격 증명 기반 정책 예제

Client VPN 자격 증명 기반 정책의 예를 보려면 에 대한 자격 증명 기반 정책 예제 AWS Client VPN 섹션을 참조하세요.

Client VPN 내 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는가 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM에서 교차 계정 리소스 액세스를 참조하세요.

Client VPN에 대한 정책 작업

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

Client VPN 작업 목록을 보려면 서비스 승인 참조의 AWS Client VPN에서 정의한 작업을 참조하세요.

Client VPN의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
ec2
```

단일 문에서 여러 작업을 지정하려면 쉼표로 구분합니다.

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

Client VPN 자격 증명 기반 정책의 예를 보려면 에 대한 자격 증명 기반 정책 예제 AWS Client VPN 섹션을 참조하세요.

Client VPN의 정책 리소스

정책 리소스 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

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

Client VPN 리소스 유형 및 해당 ARNs 목록을 보려면 서비스 승인 참조의 AWS Client VPN에서 정의한 리소스를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 AWS Client VPN에서 정의한 작업을 참조하세요.

Client VPN 자격 증명 기반 정책의 예를 보려면 에 대한 자격 증명 기반 정책 예제 AWS Client VPN 섹션을 참조하세요.

Client VPN 정책 조건 키

서비스별 정책 조건 키 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소는 정의된 기준에 따라 문이 실행되는 시기를 지정합니다. 같음(equals) 또는 미만(less than)과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수

있습니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

Client VPN 조건 키 목록을 보려면 서비스 승인 참조의 AWS Client VPN에 사용되는 조건 키를 참조하세요. 조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 AWS Client VPN에서 정의한 작업을 참조하세요.

Client VPN 자격 증명 기반 정책의 예를 보려면 에 대한 자격 증명 기반 정책 예제 AWS Client VPN 섹션을 참조하세요.

Client VPN의 ACL

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Client VPN의 ABAC

ABAC 지원(정책의 태그): 예

속성 기반 액세스 제어(ABAC)는 태그라고 불리는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. IAM 엔터티 및 AWS 리소스에 태그를 연결한 다음 보안 주체의 태그가 리소스의 태그와 일치할 때 작업을 허용하는 ABAC 정책을 설계할 수 있습니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`또는 `aws:TagKeys`조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 ABAC 권한 부여를 통한 권한 정의를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

Client VPN에서 임시 보안 인증 정보 사용

임시 자격 증명 지원: 예

임시 자격 증명은 AWS 리소스에 대한 단기 액세스를 제공하며 페더레이션 또는 전환 역할을 사용할 때 자동으로 생성됩니다. 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 것이

AWS 좋습니다. 자세한 내용은 IAM 사용 설명서의 IAM의 임시 보안 자격 증명 및 IAM으로 작업하는 AWS 서비스 섹션을 참조하세요.

Client VPN의 서비스 간 보안 주체 권한

전달 액세스 세션(FAS) 지원: 예

전달 액세스 세션(FAS)은를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

Client VPN의 서비스 역할

서비스 역할 지원: 예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스 AWS에 권한을 위임할 역할 생성을 참조하세요.

Client VPN의 서비스 연결 역할

서비스 연결 역할 지원: 예

서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

에 대한 자격 증명 기반 정책 예제 AWS Client VPN

기본적으로 사용자 및 역할은 Client VPN 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성(콘솔)을 참조하세요.

각 리소스 유형에 대한 ARNs 형식을 포함하여 Client VPN에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 AWS Client VPN에 사용되는 작업, 리소스 및 조건 키를 참조하세요.

주제

- 정책 모범 사례
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용

정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Client VPN 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. AWS 서비스와 같은 특정를 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 CloudFormation. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정켭니다. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "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": "*"
        }
    ]
}
```

AWS Client VPN 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 Client VPN 및 IAM에서 발생할 수 있는 공통적인 문제를 진단하고 수정할 수 있습니다.

주제

- Client VPN에서 작업을 수행할 권한이 없음
- iam:PassRole을 수행하도록 인증되지 않음

- 내 외부의 사람이 내 Client VPN 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

Client VPN에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 표시되면 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음의 예제 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 가상 *my-example-widget* 리소스에 대한 세부 정보를 보려고 하지만 가상 ec2:*GetWidget* 권한이 없을 때 발생합니다.

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

이 경우, ec2:*GetWidget* 작업을 사용하여 *my-example-widget* 리소스에 액세스할 수 있도록 mateojackson 사용자 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

iam:PassRole을 수행하도록 인증되지 않음

iam:PassRole 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 Client VPN에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 역할을 서비스에 전달할 권한이 있어야 합니다.

다음 예시 오류는 marymajor라는 IAM 사용자가 콘솔을 사용하여 Client VPN에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 권한이 없습니다.

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

이 경우, Mary가 iam:PassRole작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 외부의 사람이 내 Client VPN 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제

어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세한 내용은 다음을 참조하세요.

- Client VPN에서 이러한 기능을 지원하는지 여부를 알아보려면 AWS Client VPN 에서 IAM을 사용하는 방법 섹션을 참조하세요.
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유한 다른의 IAM 사용자에게 액세스 권한 제공을 참조 AWS 계정 하세요.
- 리소스에 대한 액세스 권한을 타사에 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정 소유에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

에 대한 서비스 연결 역할 사용 AWS Client VPN

AWS Client VPN 는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 Client VPN에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 Client VPN에서 사전 정의하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

주제

- 에 역할 사용 AWS Client VPN
- Client VPN에서 연결 권한 부여를 위한 역할 사용;

에 역할 사용 AWS Client VPN

AWS Client VPN 는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 Client VPN에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 Client VPN에서 사전 정의하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 Client VPN을 더 쉽게 설정할 수 있습니다. Client VPN에서 서비스 연결 역할의 권한을 정의하므로 다르게 정의되지 않은 한,

Client VPN만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제한 후에만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 부주의로 삭제할 수 없기 때문에 Client VPN 리소스가 보호됩니다.

Client VPN에 대한 서비스 연결 역할 권한

Client VPN은 VPN 연결과 관련된 리소스를 생성하고 관리할 수 있도록 AWSServiceRoleForClientVPN이라는 서비스 연결 역할을 사용합니다.

AWSServiceRoleForClientVPN 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `clientvpn.amazonaws.com`

서비스 연결 역할은 관리형 정책 ClientVPNServiceRolePolicy를 사용합니다. 이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조의 ClientVPNServiceRolePolicy를 참조하세요.

Client VPN에 대한 서비스 연결 역할 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. AWS CLI, 또는 AWS API를 사용하여 계정에 첫 번째 Client VPN 엔드포인트 AWS Management Console를 생성하면 Client VPN이 서비스 연결 역할을 생성합니다.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 계정에서 첫 번째 Client VPN 엔드포인트를 만들 때 Client VPN은 자동으로 서비스 연결 역할을 다시 생성합니다.

Client VPN에 대한 서비스 연결 역할 편집

Client VPN은 AWSServiceRoleForClientVPN 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 설명 편집을 참조하세요.

Client VPN에 대한 서비스 연결 역할 삭제

Client VPN을 더 이상 사용할 필요 없는 경우 AWSServiceRoleForClientVPN 서비스 연결 역할을 삭제하는 것이 좋습니다.

먼저 관련 Client VPN 리소스를 삭제해야 합니다. 이렇게 하면 리소스에 대한 액세스 권한을 실수로 제거할 염려가 없습니다.

IAM 콘솔, IAM CLI 또는 IAM API를 사용하여 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하세요.

Client VPN에서 연결 권한 부여를 위한 역할 사용;

AWS Client VPN 는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 Client VPN에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 Client VPN에서 사전 정의하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 Client VPN을 더 쉽게 설정할 수 있습니다. Client VPN에서 서비스 연결 역할의 권한을 정의하므로 다르게 정의되지 않은 한, Client VPN만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제한 후에만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 부주의로 삭제할 수 없기 때문에 Client VPN 리소스가 보호됩니다.

Client VPN에 대한 서비스 연결 역할 권한

Client VPN은 클라이언트 VPN 연결을 위한 서비스 연결 역할인 AWSServiceRoleForClientVPNConnections라는 서비스 연결 역할을 사용합니다.

AWSServiceRoleForClientVPNConnections 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `clientvpn-connections.amazonaws.com`

이름이 ClientVPNServiceConnectionsRolePolicy인 역할 권한 정책은 Client VPN이 지정된 리소스에서 다음 작업을 완료하도록 허용합니다.

- 작업: `arn:aws:lambda:*:*:function:AWSClientVPN-*`에 대한 `lambda:InvokeFunction`

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 링크 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

Client VPN에 대한 서비스 연결 역할 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. AWS CLI, 또는 AWS API를 사용하여 계정에 첫 번째 Client VPN 엔드포인트 AWS Management Console를 생성하면 Client VPN이 서비스 연결 역할을 생성합니다.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 계정에서 첫 번째 Client VPN 엔드포인트를 만들 때 Client VPN은 자동으로 서비스 연결 역할을 다시 생성합니다.

Client VPN에 대한 서비스 연결 역할 편집

Client VPN은 AWSServiceRoleForClientVPNConnections 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 설명 편집을 참조하세요.

Client VPN에 대한 서비스 연결 역할 삭제

Client VPN을 더 이상 사용할 필요 없는 경우 AWSServiceRoleForClientVPNConnections 서비스 연결 역할을 삭제하는 것이 좋습니다.

먼저 관련 Client VPN 리소스를 삭제해야 합니다. 이렇게 하면 리소스에 대한 액세스 권한을 실수로 제거할 염려가 없습니다.

IAM 콘솔, IAM CLI 또는 IAM API를 사용하여 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하세요.

AWS Client VPN의 복원성

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. AWS 리전은 물리적으로 분리되고 격리된 다수의 가용 리전을 제공하며 이러한 가용 리전은 짧은 지연 시간, 높은 처리량 및 높은 중복성을 갖춘 네트워크에 연결되어 있습니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

AWS 글로벌 인프라 외에 AWS Client VPN도 데이터 복원성과 백업 요구 사항을 지원하는 여러 가지 기능을 제공합니다.

고가용성을 위한 다중 대상 네트워크

대상 네트워크를 Client VPN 엔드포인트와 연결하여 클라이언트가 VPN 세션을 설정할 수 있도록 합니다. 대상 네트워크는 VPC의 서브넷입니다. Client VPN 엔드포인트와 연결하는 각 서브넷은 서로 다른 가용 영역에 속해야 합니다. 고가용성을 위해 여러 서브넷을 하나의 Client VPN 엔드포인트와 연결할 수 있습니다.

의 인프라 보안AWS Client VPN

관리형 서비스인AWS Client VPN은AWS글로벌 네트워크 보안으로 보호됩니다.AWS보안 서비스 및가 인프라를AWS보호하는 방법에 대한 자세한 내용은 AWS클라우드 보안을 참조하세요. 인프라 보안 모범 사례를 사용하여 환경을 설계하려면 보안 원칙AWS Well-Architected Framework의 인프라 보호를 참조하세요AWS.

AWS게시된 API 호출을 사용하여 네트워크를 통해 Client VPN에 액세스합니다. 클라이언트는 다음을 지원해야 합니다.

- Transport Layer Security(TLS). TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

의 보안 모범 사례AWS Client VPN

AWS Client VPN는 자체 보안 정책을 개발하고 구현할 때 고려해야 할 여러 보안 기능을 제공합니다. 다음 모범 사례는 일반적인 지침이며 완벽한 보안 솔루션을 나타내지는 않습니다. 이러한 모범 사례는 환경에 적절하지 않거나 충분하지 않을 수 있으므로 참고용으로만 사용해 주세요.

권한 부여 규칙

권한 부여 규칙을 사용하여 네트워크에 액세스할 수 있는 사용자를 제한합니다. 자세한 내용은 권한 부여 규칙 섹션을 참조하세요.

보안 그룹

보안 그룹을 사용하여 사용자가 VPC에서 액세스할 수 있는 리소스를 제어합니다. 자세한 내용은 보안 그룹 섹션을 참조하세요.

클라이언트 인증서 해지 목록

클라이언트 인증서 해지 목록을 사용하여 특정 클라이언트 인증서의 Client VPN 엔드포인트에 대한 액세스를 취소합니다. 예를 들어 사용자가 조직을 떠나는 경우입니다. 자세한 내용은 클라이언트 인증서 해지 목록 섹션을 참조하세요.

세션 시간 초과 시 연결 해제

최대 Client VPN 세션 시간에 도달하면 세션을 연결 해제하여 최대 VPN 세션 기간을 강제 적용합니다. 자세한 내용은 최대 VPN 세션 기간 섹션을 참조하세요.

모니터링 도구

모니터링 도구를 사용하여 Client VPN 엔드포인트의 가용성과 성능을 추적합니다. 자세한 내용은 Client VPN 모니터링 섹션을 참조하세요.

자격 증명 및 액세스 관리

IAM 사용자 및 IAM 역할에 IAM 정책을 사용하여 Client VPN 리소스 및 API에 대한 액세스를 관리합니다. 자세한 내용은 에 대한 자격 증명 및 액세스 관리 AWS Client VPN 섹션을 참조하세요.

AWS Client VPN에 대한 IPv6 고려 사항

Client VPN은 이제 기존 IPv4 기능과 함께 네이티브 IPv6 연결을 지원합니다. 네트워킹 요구 사항을 충족하기 위해 IPv6 전용, IPv4 전용 또는 듀얼 스택(IPv4 및 IPv6 모두) 엔드포인트를 생성할 수 있습니다.

IPv6 지원의 주요 구성 요소

Client VPN에서 IPv6로 작업하는 경우 두 가지 주요 구성 파라미터가 있습니다.

엔드포인트 IP 주소 유형

이 파라미터는 엔드포인트에 프로비저닝된 EC2 인스턴스 유형을 결정하는 엔드포인트 관리 IP 유형을 정의합니다. 이 IP 유형은 외부 VPN 터널 트래픽(퍼블릭 인터넷을 통해 OpenVPN 클라이언트와 서버 간에 흐르는 암호화된 트래픽)을 관리하는 데 사용됩니다.

트래픽 IP 주소 유형

이 파라미터는 VPN 터널을 통해 흐르는 트래픽 유형을 정의합니다. 이 IP 유형은 암호화된 내부 트래픽(실제 페이로드), 클라이언트 CIDR 범위, 서브넷 연결, 경로 및 엔드포인트당 규칙을 관리하는 데 사용됩니다.

IPv6 클라이언트 CIDR 할당

IPv6 클라이언트 CIDR의 경우 CIDR 블록을 지정할 필요가 없습니다. Amazon은 IPv6 클라이언트에 CIDR 범위를 자동으로 할당합니다. 이 자동 할당을 사용하면 IPv6 터널 트래픽에 대해 SNATing할 수 없으므로 연결된 사용자의 IPv6 주소에 대한 가시성이 향상됩니다.

호환성 요구 사항

IPv6 및 듀얼 스택 엔드포인트는 사용자 기기와 인터넷 서비스 공급자(ISP)에 의존합니다.

- CVPN 클라이언트를 실행하는 사용자 디바이스는 아래 호환성 표에 표시된 대로 필요한 IP 구성을 지원해야 합니다.
- 연결이 제대로 작동하려면 ISP가 필요한 IP 구성을 지원해야 합니다.
- IPv6 또는 듀얼 스택 트래픽의 경우 연결된 VPC 서브넷에 IPv6 또는 듀얼 스택 CIDR 범위가 있어야 합니다.

DNS 지원

DNS는 IPv4, IPv6, 듀얼 스택 등 모든 유형의 엔드포인트에서 지원됩니다. IPv6 엔드포인트의 경우 `--dns-server-ipv6` 파라미터를 사용하여 IPv6 DNS 서버를 구성할 수 있습니다. AAAA DNS 레코드는 서비스와 클라이언트 종단 모두에서 지원됩니다.

제한 사항

다음은 IPv6의 제한 사항입니다.

- Client-to-client(C2C) 통신은 IPv6 클라이언트에서 지원되지 않습니다. IPv6 클라이언트가 다른 IPv6 클라이언트와 통신을 시도하면 트래픽이 삭제됩니다.

IPv6에 대한 클라이언트 라우팅 적용

Client VPN은 이제 IPv6 트래픽에 대한 클라이언트 라우팅 적용을 지원합니다. 이 기능은 연결된 클라이언트의 IPv6 네트워크 트래픽이 관리자가 정의한 경로를 따르고 실수로 VPN 터널 외부로 전송되지 않도록 하는 데 도움이 됩니다.

IPv6 클라이언트 경로 강제 적용 지원의 주요 측면은 다음과 같습니다.

- 기존 `ClientRouteEnforcementOptions.enforced` 플래그는 IPv4 스택과 IPv6 스택 모두에 대해 CRE를 활성화합니다.
- IPv6 클라이언트 경로 강제 적용은 중요한 IPv6 기능을 유지하기 위해 특정 IPv6 범위를 제외합니다.
  - `::1/128` - 루프백용으로 예약됨
  - `fe80::/10` - 링크-로컬 주소용으로 예약됨
  - `ff00::/8` - 멀티캐스트용으로 예약됨
- IPv6 클라이언트 경로 강제 적용은 Windows, macOS 및 Ubuntu의 AWS VPN 클라이언트 버전 5.3.0 이상에서 사용할 수 있습니다.

CRE에 대한 자세한 정보(활성화 및 구성 방법 포함)는 the section called “클라이언트 경로 강제 적용”을 참조하세요.

IPv6 누수 방지(레거시 정보)

네이티브 IPv6 지원을 사용하지 않는 이전 구성의 경우 IPv6 누수를 방지해야 할 수 있습니다. IPv6 누수는 IPv4 및 IPv6이 둘 다 활성화되고 VPN에 연결될 때 발생할 수 있지만 VPN은 IPv6 트래픽을 터널로 라우팅하지 않습니다. 이 경우 IPv6 활성화 대상에 연결할 때 실제로는 ISP에서 제공한 IPv6 주소로 계속 연결되어 있습니다. 그러면 실제 IPv6 주소가 유출됩니다. 아래 지침은 IPv6 트래픽을 VPN 터널로 라우팅하는 방법에 대해 설명합니다.

IPv6 유출을 방지하려면 다음 IPv6 관련 지시문을 Client VPN 구성 파일에 추가해야 합니다.

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

예를 들면 다음과 같습니다.

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

이 예시에서 `ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1`은 로컬 터널 디바이스 IPv6 주소를 `fd15:53b6:dead::2`로, 원격 VPN 엔드포인트 IPv6 주소를 `fd15:53b6:dead::1`로 설정합니다.

다음 명령인 `route-ipv6 2000::/4`는 IPv6 주소 (`2000:0000:0000:0000:0000:0000:0000:0000~2fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff` 사이)를 VPN 연결로 라우팅합니다.

> **Note**
>
> 예를 들어 Windows에서 'TAP' 디바이스를 라우팅할 경우 `ifconfig-ipv6`에 대한 두 번째 파라미터는 `--route-ipv6`에 대한 라우팅 대상으로 사용됩니다.

조직들은 `ifconfig-ipv6`의 파라미터 두 개를 직접 구성해야 하며 `100::/64`의 주소 (`0100:0000:0000:0000:0000:0000:0000:0000~0100:0000:0000:0000:ffff:ffff:ffff:ffff` 사이) 또는 `fc00::/7`(`fc00:0000:0000:0000:0000:0000:0000:0000~fdff:ffff:ffff:ffff:ffff:ffff:ff` 사이) 주소를 사용할 수 있습니다. `100::/64`는 Discard-Only 주소 블록이고 `fc00::/7`은 Unique-Local입니다.

또 다른 예시:

```
ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1
route-ipv6 2000::/3
route-ipv6 fc00::/7
```

이 예시에서 구성은 현재 할당된 모든 IPv6 트래픽을 VPN 연결로 라우팅합니다.

Verification(확인)

조직에는 자체 테스트가 있을 수 있습니다. 기본 확인은 전체 터널 VPN 연결을 설정한 다음 IPv6 주소를 사용하여 IPv6 서버를 향해 ping6을 실행하는 것입니다. 서버의 IPv6 주소는 `route-ipv6` 명령에 의해 지정된 범위에 있어야 합니다. 이 ping 테스트는 실패해야 합니다. 그러나 나중에 IPv6 지원이 Client VPN 서비스에 추가되는 경우 이는 변경될 수 있습니다. ping이 성공하고 전체 터널 모드로 연결되었을 때 퍼블릭 사이트에 액세스할 수 있는 경우 문제 해결을 추가로 수행해야 할 수도 있습니다. 공개적으로 사용할 수 있는 도구도 몇 가지 있습니다.

AWS Client VPN 모니터링

모니터링은 AWS Client VPN과 사용자의 기타 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 중요한 역할을 합니다. 다음 기능을 사용하여 Client VPN 엔드포인트를 모니터링하고 트래픽 패턴을 분석하며 Client VPN 엔드포인트의 문제를 해결할 수 있습니다.

Amazon CloudWatch

AWS 리소스와 AWS에서 실행 중인 애플리케이션을 실시간으로 모니터링합니다. 지표를 수집 및 추적하고, 사용자 지정 대시보드를 생성할 수 있으며, 지정된 지표가 지정한 임곗값에 도달하면 사용자에게 알리거나 조치를 취하도록 경보를 설정할 수 있습니다. 예를 들어 CloudWatch에서 Amazon EC2 인스턴스의 CPU 사용량 또는 기타 지표를 추적하고 필요할 때 자동으로 새 인스턴스를 시작할 수 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하세요.

AWS CloudTrail

직접 수행하거나 AWS 계정을 대신하여 수행한 API 호출 및 관련 이벤트를 캡처하고 지정한 Amazon S3 버킷에 로그 파일을 전송합니다. 어떤 사용자 및 계정이 AWS를 호출했는지 어떤 소스 IP 주소에 호출이 이루어졌는지 언제 호출이 발생했는지 확인할 수 있습니다. 모든 Client VPN 작업은 CloudTrail에서 기록되며 Amazon EC2 API 참조에 설명되어 있습니다.

Amazon CloudWatch Logs

AWS Client VPN 엔드포인트에 대한 연결 시도를 모니터링하도록 합니다. Client VPN 연결에 대한 연결 시도 및 연결 재설정을 볼 수 있습니다. 연결 시도의 경우 성공 및 실패한 연결 시도를 모두 볼 수 있습니다. CloudWatch Logs 로그 스트림을 지정하여 연결 세부 정보를 기록할 수 있습니다. 자세한 내용은 AWS Client VPN 엔드포인트에 대한 연결 로깅 및 Amazon CloudWatch Logs 사용 설명서를 참조하십시오.

주제

- AWS Client VPN에 대한 Amazon CloudWatch 지표

AWS Client VPN에 대한 Amazon CloudWatch 지표

AWS Client VPN은 Client VPN 엔드포인트에 대한 Amazon CloudWatch에 다음 지표를 게시합니다. 지표는 5분마다 Amazon CloudWatch에 게시됩니다.

지표	설명
ActiveConnectionsCount	Client VPN 엔드포인트에 대한 활성 연결 수입니다. 단위: 개
AuthenticationFailures	Client VPN 엔드포인트에 대한 인증 실패 수입니다. 단위: 개
CrlDaysToExpiry	Client VPN 엔드포인트에 구성된 CRL(인증서 해지 목록)이 만료될 때까지 남은 기간(일)입니다. 단위: 일
EgressBytes	Client VPN 엔드포인트에서 전송된 바이트 수입니다. 단위: 바이트
EgressPackets	Client VPN 엔드포인트에서 전송된 패킷 수입니다. 단위: 개
IngressBytes	Client VPN 엔드포인트에서 수신된 바이트 수입니다. 단위: 바이트
IngressPackets	Client VPN 엔드포인트에서 수신된 패킷 수입니다. 단위: 개
SelfServicePortalClientConfigurationDownloads	셀프 서비스 포털에서 Client VPN 엔드포인트 구성 파일의 다운로드 수입니다.

지표	설명
	단위: 개

AWS Client VPN은 Client VPN 엔드포인트에 대한 다음과 같은 태세 평가 지표를 게시합니다.

지표	설명
ClientConnectHandlerTimeouts	Client VPN 엔드포인트 연결에 대해 클라이언트 연결 핸들러를 호출할 때 발생하는 시간 초과 수입니다. 단위: 개
ClientConnectHandlerInvalidResponses	Client VPN 엔드포인트 연결에 대해 클라이언트 연결 핸들러가 반환하는 잘못된 응답 수입니다. 단위: 개
ClientConnectHandlerOtherExecutionErrors	Client VPN 엔드포인트 연결에 대해 클라이언트 연결 핸들러를 실행하는 중에 발생한 예상치 못한 오류 수입니다. 단위: 개
ClientConnectHandlerThrottlingErrors	Client VPN 엔드포인트 연결에 대해 클라이언트 연결 핸들러를 호출할 때 발생하는 제한 오류 수입니다. 단위: 개
ClientConnectHandlerDeniedConnections	Client VPN 엔드포인트 연결에 대해 클라이언트 연결 핸들러가 거부한 연결 수입니다. 단위: 개
ClientConnectHandlerFailedServiceErrors	Client VPN 엔드포인트 연결에 대해 클라이언트 연결 핸들러를 실행하는 중에 발생한 서비스측 오류 수입니다.

지표	설명
	단위: 개

Client VPN 엔드포인트에 대한 지표를 엔드포인트별로 필터링할 수 있습니다.

CloudWatch를 사용하면 이러한 데이터 요소에 대한 통계를 정렬된 시계열 데이터 세트로 검색할 수 있습니다. 이러한 통계를 지표라고 합니다. 지표를 모니터링할 변수로 생각하면 데이터 요소는 시간에 따른 변수의 값을 나타냅니다. 각 데이터 포인트에는 연결된 타임스탬프와 측정 단위(선택 사항)가 있습니다.

지표를 사용하여 시스템이 예상대로 수행되고 있는지 확인할 수 있습니다. 예를 들어 CloudWatch 경보를 생성하여 지정된 지표를 모니터링할 수 있으며, 지표가 허용 범위를 벗어난다고 간주되는 경우 작업(예: 이메일 주소로 알림 전송)을 시작할 수 있습니다.

자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하세요.

Tasks

- Amazon CloudWatch에서 Client VPN 엔드포인트 지표 보기

Amazon CloudWatch에서 Client VPN 엔드포인트 지표 보기

Client VPN 엔드포인트에 대한 지표를 다음과 같이 볼 수 있습니다.

CloudWatch 콘솔을 사용하여 지표를 보려면

지표는 먼저 서비스 네임스페이스별로 그룹화된 다음 각 네임스페이스 내에서 다양한 차원 조합별로 그룹화됩니다.

1. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 지표를 선택합니다.
3. 전체 지표(All metrics)에서 Client VPN 지표 네임스페이스를 선택합니다.
4. 지표를 보려면 엔드포인트 기준 지표 측정 기준을 선택합니다.

AWS CLI을(를) 사용하여 지표를 보려면

명령 프롬프트에서 다음 명령을 사용하여 Client VPN에 사용 가능한 지표 목록을 확인합니다.

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

AWS Client VPN 할당량

AWS 계정에는 Client VPN 엔드포인트에 관련된 다음과 같은 할당량(이전에는 제한이라고 함)이 있습니다. 다르게 표시되지 않는 한, 리전별로 각 할당량이 적용됩니다. 일부 할당량에 대한 증가를 요청할 수 있으며 다른 할당량은 늘릴 수 없습니다.

조정 가능한 할당량에 대해 할당량 증가를 요청하려면 조정 가능(Adjustable) 열에서 예(Yes)를 선택하세요. 자세한 내용은 Service Quotas 사용 설명서의 할당량 증가 요청을 참조하세요.

Client VPN 할당량

이름	기본값	조정 가능
Client VPN 엔드포인트당 권한 부여 규칙	200 듀얼 스택 엔드포인트의 경우 이 제한은 IPv4와 IPv6 경로 간에 공유됩니다.	예
리전당 Client VPN 엔드포인트	5	예
Client VPN 엔드포인트당 클라이언트 동시 연결	이 값은 엔드포인트당 서브넷 연결 수에 따라 다릅니다. • 1~7,000 • 2~36,500 • 3~66,500 • 4~96,500 • 5~126,000 듀얼 스택 엔드포인트의 경우 이 제한은 IPv4와 IPv6 연결 간에 공유됩니다.	예

이름	기본값	조정 가능
Client VPN 엔드포인트당 동시 작업 †	10	아니요
Client VPN 엔드포인트용 클라이언트 인증서 해지 목록의 항목	20,000건	아니요
Client VPN 대상 네트워크 연결당 라우팅	100 듀얼 스택 엔드포인트의 경우 이 제한은 IPv4와 IPv6 경로 간에 공유됩니다.	예

† 작업에는 다음이 포함됩니다.

- 서브넷 연결 또는 연결 해제
- 보안 그룹 생성 또는 삭제

사용자 및 그룹 할당량

Active Directory 또는 SAML 기반 IdP에 대한 사용자 및 그룹을 구성하는 경우 다음 할당량이 적용됩니다.

- 사용자는 최대 200개의 그룹에 속할 수 있습니다. 여기서는 200번째 그룹 이후의 모든 그룹을 무시합니다.
- 그룹 ID의 최대 길이는 255자입니다.
- 이름 ID의 최대 길이는 255자입니다. 255번째 이후의 문자는 자릅니다.

일반적인 고려 사항

Client VPN 엔드포인트를 사용할 때는 다음 사항을 고려하세요.

- Active Directory를 사용하여 사용자를 인증하는 경우 Client VPN 엔드포인트는 Active Directory 인증에 사용되는 AWS Directory Service 리소스와 동일한 계정에 속해야 합니다.

- IAM SAML 기반 연동 인증을 사용하여 사용자를 인증하는 경우 Client VPN 엔드포인트는 Idp-to-AWS 간 신뢰 관계를 정의하기 위해 생성한 IAM SAML 자격 증명 공급자와 동일한 계정에 속해야 합니다. IAM SAML 자격 증명 공급자는 동일한 AWS 계정의 여러 Client VPN 엔드포인트에서 공유할 수 있습니다.

AWS Client VPN 문제 해결

다음 섹션은 Client VPN 엔드포인트 관련 문제를 해결하는 데 도움이 될 수 있습니다.

클라이언트가 Client VPN에 연결하는 데 사용하는 OpenVPN 기반 소프트웨어의 문제 해결에 대한 자세한 내용은 AWS Client VPN 사용 설명서의 Client VPN 연결 문제 해결을 참조하십시오.

공통 문제

- 문제 해결 AWS Client VPN: Client VPN 엔드포인트 DNS 이름을 확인할 수 없음
- 문제 해결 AWS Client VPN: 트래픽이 서브넷 간에 분할되지 않음
- 문제 해결 AWS Client VPN: Active Directory 그룹에 대한 권한 부여 규칙이 예상대로 작동하지 않음
- 문제 해결 AWS Client VPN: 클라이언트가 피어링된 VPC, Amazon S3 또는 인터넷에 액세스할 수 없음
- 문제 해결 AWS Client VPN: 피어링된 VPC, Amazon S3 또는 인터넷에 대한 액세스가 간헐적임
- 문제 해결 AWS Client VPN: Client VPN에 연결하려고 할 때 클라이언트 소프트웨어가 TLS 오류를 반환합니다.
- 문제 해결 AWS Client VPN: 클라이언트 소프트웨어에서 사용자 이름 및 암호 오류 반환 - Active Directory 인증
- 문제 해결 AWS Client VPN: 클라이언트 소프트웨어에서 사용자 이름 및 암호 오류 반환 - 페더레이션 인증
- 문제 해결 AWS Client VPN: 클라이언트가 연결할 수 없음 - 상호 인증
- 문제 해결 AWS Client VPN: 클라이언트가 Client VPN에서 자격 증명이 최대 크기 초과 오류를 반환함 - 페더레이션 인증
- 문제 해결 AWS Client VPN: 클라이언트가 엔드포인트에 대한 브라우저를 열지 않음 - 페더레이션 인증
- 문제 해결 AWS Client VPN: 클라이언트가 사용 가능한 포트 없음 오류 반환 - 페더레이션 인증
- 문제 해결 AWS Client VPN: IP 불일치로 인해 연결이 종료됩니다.
- 문제 해결 AWS Client VPN: LAN으로 트래픽 라우팅이 예상대로 작동하지 않음
- 문제 해결 AWS Client VPN: Client VPN 엔드포인트의 대역폭 제한 확인
- AWS Client VPN 문제 해결: VPC에 대한 터널 연결 문제

문제 해결 AWS Client VPN: Client VPN 엔드포인트 DNS 이름을 확인할 수 없음

문제

Client VPN 엔드포인트의 DNS 이름을 확인할 수 없습니다.

원인

Client VPN 엔드포인트 구성 파일에는 `remote-random-hostname`이라는 파라미터가 포함되어 있습니다. 이 파라미터는 DNS 캐싱을 방지하기 위해 클라이언트가 DNS 이름 앞에 임의의 문자열을 붙이도록 강제합니다. 일부 클라이언트는 이 파라미터를 인식하지 못하므로 DNS 이름 앞에 필요한 임의의 문자열을 붙이지 않습니다.

Solution

원하는 텍스트 편집기를 사용하여 Client VPN 엔드포인트 구성 파일을 엽니다. Client VPN 엔드포인트 DNS 이름을 지정하는 행을 찾은 다음 임의의 문자열을 앞에 붙여 형식이 *`random_string.displayed_DNS_name`*이 되도록 합니다. 예:

- 원래 DNS 이름: `cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`
- 수정된 DNS 이름: `asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`

문제 해결 AWS Client VPN: 트래픽이 서브넷 간에 분할되지 않음

문제

두 서브넷 간에 네트워크 트래픽을 분할하려고 합니다. 프라이빗 트래픽은 프라이빗 서브넷을 통해 라우팅되고 인터넷 트래픽은 퍼블릭 서브넷을 통해 라우팅되어야 합니다. 그러나 Client VPN 엔드포인트 라우팅 테이블에 두 경로를 모두 추가했더라도 하나의 경로만 사용되고 있습니다.

원인

여러 서브넷을 Client VPN 엔드포인트와 연결할 수 있지만 가용 영역당 하나의 서브넷만 연결할 수 있습니다. 여러 서브넷 연결의 목적은 클라이언트에 고가용성 및 가용 영역 중복성을 제공하는 것입니다. 그러나 Client VPN을 사용하면 Client VPN 엔드포인트와 연결된 서브넷 간에 트래픽을 선택적으로 분할할 수 없습니다.

클라이언트는 DNS 라운드 로빈 알고리즘을 기반으로 Client VPN 엔드포인트에 연결합니다. 즉, 연결을 설정할 때 연결된 서브넷을 통해 트래픽이 라우팅될 수 있습니다. 따라서 필요한 경로 항목이 없는 연결된 서브넷에 도달하면 연결 문제가 발생할 수 있습니다.

예를 들어 다음과 같은 서브넷 연결 및 경로를 구성한다고 가정합니다.

- 서브넷 연결
  - 연결 1: 서브넷-A(us-east-1a)
  - 연결 2: 서브넷-B(us-east-1b)
- Routes
  - 경로 1: 서브넷-A로 라우팅된 10.0.0.0/16
  - 경로 2: 서브넷-B로 라우팅된 172.31.0.0/16

이 예에서 연결될 때 서브넷-A에 도달한 클라이언트는 루트 2에 액세스할 수 없고, 연결될 때 서브넷-B에 도달한 클라이언트는 루트 1에 액세스할 수 없습니다.

Solution

Client VPN 엔드포인트에 연결된 각 네트워크의 대상이 있는 동일한 경로 항목이 있는지 확인합니다. 이렇게 하면 트래픽이 라우팅되는 서브넷에 관계없이 클라이언트가 모든 경로에 액세스할 수 있습니다.

문제 해결 AWS Client VPN: Active Directory 그룹에 대한 권한 부여 규칙이 예상대로 작동하지 않음

문제

Active Directory 그룹에 대한 권한 부여 규칙을 구성했지만 예상대로 작동하지 않습니다. 모든 네트워크의 트래픽을 승인하는 `0.0.0.0/0`에 대한 권한 부여 규칙을 추가했지만 특정 대상 CIDR에 대한 트래픽은 여전히 실패합니다.

원인

권한 부여 규칙은 네트워크 CIDR에서 인덱싱됩니다. 권한 부여 규칙은 Active Directory 그룹에 특정 네트워크 CIDR에 대한 액세스 권한을 부여해야 합니다. `0.0.0.0/0`에 대한 권한 부여 규칙은 특별한 경우로 간주되므로, 권한 부여 규칙이 만들어진 순서에 관계없이 마지막으로 평가됩니다.

예를 들어 다음과 같은 순서로 다섯 가지 권한 부여 규칙을 만들 수 있다고 가정합니다.

- 규칙 1: 10.1.0.0/16에 액세스하는 그룹 1
- 규칙 2: 0.0.0.0/0에 액세스하는 그룹 1
- 규칙 3: 0.0.0.0/0에 액세스하는 그룹 2
- 규칙 4: 0.0.0.0/0에 액세스하는 그룹 3
- 규칙 5: 172.131.0.0/16에 액세스하는 그룹 2

이 예시에서는 규칙 2, 규칙 3과 규칙 4를 마지막으로 평가합니다. 그룹 1은 10.1.0.0/16에 대한 액세스 권한만 있고 그룹 2는 172.131.0.0/16에 대한 액세스 권한만 가집니다. 그룹 3은 10.1.0.0/16 또는 172.131.0.0/16에 액세스할 수 없지만 다른 모든 네트워크에 액세스할 수 있습니다. 규칙 1과 5를 제거하면 세 그룹 모두 모든 네트워크에 액세스할 수 있습니다.

Client VPN에서는 권한 부여 규칙을 평가할 때 가장 긴 접두사 일치를 사용합니다. 자세한 내용은 Amazon VPC 사용 설명서의 경로 우선 순위를 참조하십시오.

Solution

Active Directory 그룹에 특정 네트워크 CIDR에 대한 액세스 권한을 명시적으로 부여하는 권한 부여 규칙을 만들어야 합니다. 0.0.0.0/0에 대한 권한 부여 규칙을 추가하는 경우 마지막으로 평가되며 이전 권한 부여 규칙에 따라 액세스 권한을 부여하는 네트워크가 제한될 수 있습니다.

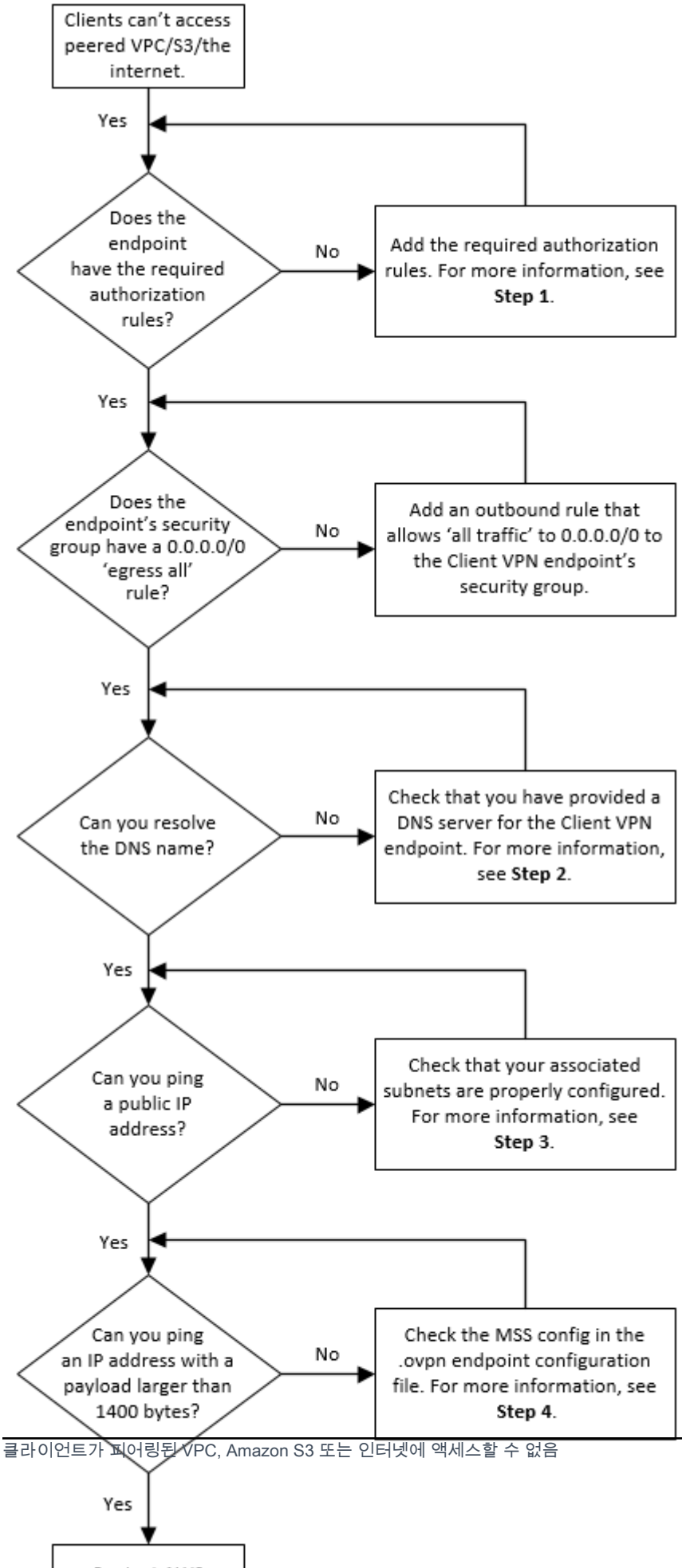
문제 해결 AWS Client VPN: 클라이언트가 피어링된 VPC, Amazon S3 또는 인터넷에 액세스할 수 없음

문제

Client VPN 엔드포인트 경로를 올바르게 구성했지만 클라이언트가 피어링된 VPC, Amazon S3 또는 인터넷에 액세스할 수 없습니다.

Solution

다음 순서도에는 인터넷, 피어링된 VPC 및 Amazon S3 연결 문제를 진단하는 단계가 나와 있습니다.


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. 인터넷에 액세스하려면 `0.0.0.0/0`에 대한 권한 부여 규칙을 추가합니다.

   피어링된 VPC에 액세스하려면 VPC의 IPv4 CIDR 범위에 대한 권한 부여 규칙을 추가합니다.

   S3에 액세스하려면 Amazon S3 엔드포인트의 IP 주소를 지정합니다.

2. DNS 이름을 확인할 수 있는지 확인합니다.

   DNS 이름을 확인할 수 없는 경우 Client VPN 엔드포인트에 대해 DNS 서버를 지정했는지 확인합니다. 자체 DNS 서버를 관리하는 경우 IP 주소를 지정하십시오. VPC에서 DNS 서버에 액세스할 수 있는지 확인합니다.

   DNS 서버에 지정할 IP 주소가 확실하지 않은 경우 VPC의 .2 IP 주소에 VPC DNS 해석기를 지정합니다.

3. 인터넷 액세스의 경우 퍼블릭 IP 주소 또는 퍼블릭 웹 사이트 (예: `amazon.com`)를 Ping할 수 있는지 확인합니다. 응답을 받지 못하면 연결된 서브넷의 라우팅 테이블에 인터넷 게이트웨이 또는 NAT 게이트웨이를 대상으로 하는 기본 경로가 있는지 확인합니다. 경로가 설정되어 있으면 연결된 서브넷에 인바운드 및 아웃바운드 트래픽을 차단하는 네트워크 액세스 제어 목록 규칙이 없는지 확인합니다.

   피어링된 VPC에 도달할 수 없는 경우 연결된 서브넷의 라우팅 테이블에 피어링된 VPC에 대한 라우팅 항목이 있는지 확인합니다.

   Amazon S3에 도달할 수 없는 경우 연결된 서브넷의 라우팅 테이블에 게이트웨이 VPC 엔드포인트에 대한 라우팅 항목이 있는지 확인합니다.

4. 1400바이트보다 큰 페이로드를 사용하여 퍼블릭 IP 주소를 Ping할 수 있는지 확인합니다. 다음 명령 중 하나를 사용합니다.

   - Windows

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

   - Linux

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

   1400바이트보다 큰 페이로드를 사용하여 IP 주소를 Ping할 수 없는 경우 원하는 텍스트 편집기를 사용하여 Client VPN 엔드포인트 `.ovpn` 구성 파일을 열고 다음을 추가합니다.

```
mssfix 1328
```

문제 해결 AWS Client VPN: 피어링된 VPC, Amazon S3 또는 인터넷에 대한 액세스가 간헐적임

문제

피어링된 VPC, Amazon S3 또는 인터넷에 연결할 때 간헐적인 연결 문제가 발생하지만 연결된 서브넷에 대한 액세스는 영향을 받지 않습니다. 연결 문제를 해결하려면 연결을 끊었다가 다시 연결해야 합니다.

원인

클라이언트는 DNS 라운드 로빈 알고리즘을 기반으로 Client VPN 엔드포인트에 연결합니다. 즉, 연결을 설정할 때 연결된 서브넷을 통해 트래픽이 라우팅될 수 있습니다. 따라서 필요한 경로 항목이 없는 연결된 서브넷에 도달하면 연결 문제가 발생할 수 있습니다.

Solution

Client VPN 엔드포인트에 연결된 각 네트워크의 대상이 있는 동일한 경로 항목이 있는지 확인합니다. 이렇게 하면 트래픽이 라우팅되는 연결된 서브넷에 관계없이 클라이언트가 모든 경로에 액세스할 수 있습니다.

예를 들어 Client VPN 엔드포인트에 세 개의 연결된 서브넷(서브넷 A, B, C)이 있고 클라이언트에 인터넷 액세스를 활성화한다고 가정합니다. 이렇게 하려면 연결된 각 서브넷을 대상으로 하는 세 개의 `0.0.0.0/0` 경로를 추가해야 합니다.

- 루트 1: 서브넷 A의 경우 `0.0.0.0/0`
- 루트 2: 서브넷 B의 경우 `0.0.0.0/0`
- 루트 3: 서브넷 C의 경우 `0.0.0.0/0`

문제 해결 AWS Client VPN: Client VPN에 연결하려고 할 때 클라이언트 소프트웨어가 TLS 오류를 반환합니다.

문제

이전에는 클라이언트를 Client VPN에 성공적으로 연결할 수 있었지만 이제는 OpenVPN 기반 클라이언트가 연결을 시도할 때 다음 오류 중 하나를 반환합니다.

```
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.
```

가능한 원인 #1

상호 인증을 사용하고 클라이언트 인증서 취소 목록을 가져온 경우 클라이언트 인증서 취소 목록이 만료되었을 수 있습니다. 인증 단계에서 Client VPN 엔드포인트는 가져온 클라이언트 인증서 취소 목록과 비교하여 클라이언트 인증서를 확인합니다. 클라이언트 인증서 취소 목록이 만료된 경우 Client VPN 엔드포인트에 연결할 수 없습니다.

해결 방법 #1

OpenSSL 도구를 사용하여 클라이언트 인증서 취소 목록의 만료 날짜를 확인합니다.

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

출력에 만료 날짜와 시간이 표시됩니다. 클라이언트 인증서 취소 목록이 만료된 경우 새 목록을 만들어 Client VPN 엔드포인트로 가져와야 합니다. 자세한 내용은 AWS Client VPN 클라이언트 인증서 해지 목록 단원을 참조하십시오.

가능한 원인 #2

Client VPN 엔드포인트에 사용 중인 서버 인증서가 만료되었습니다.

해결 방법 #2

AWS Certificate Manager 콘솔에서 또는 AWS CLI를 사용하여 서버 인증서의 상태를 확인합니다. 서버 인증서가 만료된 경우 새 인증서를 생성하여 ACM에 업로드합니다. OpenVPN easy-rsa 유틸리티를 사용하여 서버 및 클라이언트 인증서와 키를 생성하고 ACM으로 가져오는 자세한 단계는 의 상호 인증 AWS Client VPN 단원을 참조하세요.

또는 클라이언트가 Client VPN에 연결하는 데 사용하는 OpenVPN 기반 소프트웨어에 문제가 있을 수 있습니다. OpenVPN 기반 소프트웨어 문제 해결에 대한 자세한 내용은 AWS Client VPN 사용 설명서의 Client VPN 연결 문제 해결을 참조하십시오.

문제 해결 AWS Client VPN: 클라이언트 소프트웨어에서 사용자 이름 및 암호 오류 반환 - Active Directory 인증

문제

나는 Client VPN 엔드포인트에 Active Directory 인증을 사용하고, 내 클라이언트를 Client VPN에 성공적으로 연결할 수 있었습니다. 하지만 이제 클라이언트가 잘못된 사용자 이름과 암호 오류를 수신합니다.

가능한 원인

Active Directory 인증을 사용하고 클라이언트 구성 파일을 배포한 후 Multi-Factor Authentication(MFA)을 활성화한 경우, 이 파일에는 MFA 코드를 입력하라는 메시지를 표시하는 데 필요한 정보가 들어 있지 않습니다. 사용자 이름과 암호만 입력하라는 메시지가 표시되고 인증이 실패합니다.

Solution

새 클라이언트 구성 파일을 다운로드하여 클라이언트에 배포합니다. 새 파일이 다음 라인을 포함하고 있는지 확인합니다.

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

자세한 내용은 AWS Client VPN 엔드포인트 구성 파일 내보내기 단원을 참조하십시오. Client VPN 엔드포인트를 사용하지 않고 Active Directory의 MFA 구성을 테스트하여 MFA가 예상대로 작동하는지 확인합니다.

문제 해결 AWS Client VPN: 클라이언트 소프트웨어에서 사용자 이름 및 암호 오류 반환 - 페더레이션 인증

문제

페더레이션 인증을 사용하여 사용자 이름과 암호로 로그인하려고 하고 “수신된 자격 증명이 올바르지 않습니다. IT 관리자에게 문의하세요." 오류가 발생함

원인

이 오류는 IdP 의 SAML 응답에 포함된 속성이 하나 이상 없기 때문에 발생할 수 있습니다.

Solution

IdP의 SAML 응답에는 하나 이상의 속성이 포함되어야 합니다. 자세한 내용은 SAML 기반 IdP 구성 리소스를 참조하세요.

문제 해결 AWS Client VPN: 클라이언트가 연결할 수 없음 - 상호 인증

문제

Client VPN 엔드포인트에 대해 상호 인증을 사용합니다. 클라이언트가 TLS 키 협상 실패 오류 및 제한 시간 오류를 수신하는 중입니다.

가능한 원인

클라이언트에 제공된 구성 파일에 클라이언트 인증서 및 클라이언트 프라이빗 키가 포함되어 있지 않거나, 인증서 및 키가 올바르지 않습니다.

Solution

구성 파일에 올바른 클라이언트 인증서와 키가 포함되어 있는지 확인합니다. 필요한 경우 구성 파일을 수정하여 클라이언트에 재배포합니다. 자세한 내용은 AWS Client VPN 엔드포인트 구성 파일 내보내기 단원을 참조하십시오.

문제 해결 AWS Client VPN: 클라이언트가 Client VPN에서 자격 증명이 최대 크기 초과 오류를 반환함 - 페더레이션 인증

문제

Client VPN 엔드포인트에 연동 인증을 사용합니다. 클라이언트가 SAML 기반 자격 증명 공급자(IdP) 브라우저 창에 사용자 이름과 암호를 입력하면 자격 증명이 지원되는 최대 크기를 초과한다는 오류가 발생합니다.

원인

IdP에서 반환한 SAML 응답이 지원되는 최대 크기를 초과합니다. 자세한 내용은 SAML 기반 연동 인증에 대한 요구 사항 및 고려 사항 단원을 참조하십시오.

Solution

IdP에서 사용자가 속한 그룹 수를 줄이고 다시 연결해 보십시오.

문제 해결 AWS Client VPN: 클라이언트가 엔드포인트에 대한 브라우저를 열지 않음 - 페더레이션 인증

문제

Client VPN 엔드포인트에 연동 인증을 사용합니다. 클라이언트가 엔드포인트에 연결하려고 하면 클라이언트 소프트웨어에서 브라우저 창을 열지 않고 대신 사용자 이름 및 암호 팝업 창을 표시합니다.

원인

클라이언트에 제공된 구성 파일에 `auth-federate` 플래그가 포함되어 있지 않습니다.

Solution

최신 구성 파일을 내보내고 AWS 제공된 클라이언트로 가져온 다음 다시 연결을 시도합니다.

문제 해결 AWS Client VPN: 클라이언트가 사용 가능한 포트 없음 오류 반환 - 페더레이션 인증

문제

Client VPN 엔드포인트에 연동 인증을 사용합니다. 클라이언트가 엔드포인트에 연결하려고 하면 클라이언트 소프트웨어에서 다음 오류를 반환합니다.

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

원인

AWS 제공된 클라이언트는 TCP 포트 35001을 사용하여 인증을 완료해야 합니다. 자세한 내용은 SAML 기반 연동 인증에 대한 요구 사항 및 고려 사항 단원을 참조하십시오.

Solution

클라이언트의 디바이스가 TCP 포트 35001을 차단하거나 다른 프로세스에서 사용하고 있지 않은지 확인하십시오.

문제 해결 AWS Client VPN: IP 불일치로 인해 연결이 종료됩니다.

문제

VPN 연결이 종료되고 클라이언트 소프트웨어가 다음 오류를 반환합니다. `"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."`

원인

AWS 제공된 클라이언트는 연결된 IP 주소가 Client VPN 엔드포인트를 지원하는 VPN 서버의 IP와 일치해야 합니다. 자세한 내용은 사용에 대한 규칙 및 모범 사례 AWS Client VPN 단원을 참조하십시오.

Solution

AWS 제공된 클라이언트와 Client VPN 엔드포인트 사이에 DNS 프록시가 없는지 확인합니다.

문제 해결 AWS Client VPN: LAN으로 트래픽 라우팅이 예상대로 작동하지 않음

문제

LAN IP 주소 범위가 `10.0.0.0/8`, `172.16.0.0/12`, `192.168.0.0/16` 또는 `169.254.0.0/16` 표준 프라이빗 IP 주소 범위 내에 있지 않을 때 예상대로 작동하지 않는 LAN(Local Area Network)으로 트래픽을 라우팅하려고 시도합니다.

원인

클라이언트 LAN 주소 범위가 위의 표준 범위를 벗어나는 것으로 감지되면 Client VPN 엔드포인트는 OpenVPN 명령 'redirect-gateway block-local'을 클라이언트에 자동으로 푸시하여 모든 LAN 트래픽을 VPN으로 강제로 보냅니다. 자세한 내용은 사용에 대한 규칙 및 모범 사례 AWS Client VPN 단원을 참조하십시오.

Solution

VPN 연결 중에 LAN 액세스가 필요한 경우 위에 나열된 기존 주소 범위를 LAN에 사용하는 것이 좋습니다.

문제 해결 AWS Client VPN: Client VPN 엔드포인트의 대역폭 제한 확인

문제

Client VPN 엔드포인트에 대한 대역폭 제한을 확인해야 합니다.

원인

처리량은 사용자 위치에서의 연결 용량, 컴퓨터의 Client VPN 데스크톱 애플리케이션과 VPC 엔드포인트 간의 네트워크 지연 시간 등 여러 요소에 따라 달라집니다. 사용자 연결당 최소 대역폭 10Mbps가 지원됩니다.

Solution

다음 명령을 실행하여 대역폭을 확인하십시오.

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

클라이언트에서 다음을 수행합니다.

```
sudo iperf -c server IP address -p port -w 512k -P 60
```

AWS Client VPN 문제 해결: VPC에 대한 터널 연결 문제

AWS Client VPN 연결에 연결 문제가 발생하는 경우, 이 체계적인 문제 해결 접근 방식에 따라 문제를 식별하고 해결합니다. 이 섹션에서는 원격 클라이언트와 Amazon VPC 리소스 간의 일반적인 Client VPN 연결 문제를 진단하는 단계별 절차를 제공합니다.

주제

- 네트워크 연결 사전 조건
- Client VPN 엔드포인트 상태 확인
- 클라이언트 연결 확인
- 클라이언트 인증 확인
- 권한 부여 규칙 확인
- Client VPN 경로 검증
- 보안 그룹 및 네트워크 ACL 확인

- 클라이언트 연결 테스트
- 클라이언트 디바이스 진단
- DNS 확인 문제 해결
- 성능 문제 해결
- Client VPN 지표 모니터링
- Client VPN 로그 확인
- 일반적인 문제 및 해결 방법

네트워크 연결 사전 조건

Client VPN 연결 문제를 해결하기 전에 다음 네트워크 사전 조건을 확인합니다.

- Client VPN 엔드포인트 서브넷에 인터넷 연결이 있는지 확인합니다(인터넷 게이트웨이 또는 NAT 게이트웨이를 통해).
- Client VPN 엔드포인트가 고가용성을 위해 서로 다른 가용성 영역의 서브넷과 연결되어 있는지 확인합니다.
- VPC에 충분한 IP 주소 공간이 있고 클라이언트 CIDR 블록과 충돌하지 않는지 확인합니다.
- 대상 서브넷에 적절한 라우팅 테이블 연결이 있는지 확인합니다.

Client VPN 엔드포인트 상태 확인

먼저 다음과 같이 Client VPN 엔드포인트가 올바른 상태인지 확인합니다.

1. AWS CLI를 사용하여 Client VPN 엔드포인트의 상태를 확인합니다.

   ```
   aws ec2 describe-client-vpn-endpoints --region your-region
   ```

2. 출력에서 엔드포인트 상태를 찾습니다. 상태는 `available`이어야 합니다.
3. 엔드포인트에 연결된 대상 네트워크(서브넷)가 있는지 확인합니다.
4. 상태가 `available`이 아닌 경우, 구성 문제를 나타낼 수 있는 오류 메시지 또는 보류 중 상태가 있는지 확인합니다.

클라이언트 연결 확인

Client VPN 엔드포인트에 대한 클라이언트 연결 상태를 확인합니다.

1. 활성 클라이언트 연결 확인:

```
aws ec2 describe-client-vpn-connections --client-vpn-endpoint-id cvpn-endpoint-id
 --region your-region
```

2. 출력의 연결 상태 및 오류 메시지를 검토합니다.
3. 클라이언트 인증 로그에 실패한 인증 시도가 있는지 확인합니다.
4. 클라이언트가 구성된 클라이언트 CIDR 블록에서 IP 주소를 수신하고 있는지 확인합니다.

> **Note**
>
> 클라이언트가 연결할 수 없는 경우 인증 구성, 권한 부여 규칙 또는 네트워크 연결에 문제가 있을 수 있습니다.

클라이언트 인증 확인

인증 문제는 Client VPN 연결 문제의 일반적인 원인입니다.

- 상호 인증을 위해 클라이언트 인증서가 유효하며 만료되지 않았는지 확인합니다.
- Active Directory 인증의 경우 사용자 자격 증명 및 도메인 연결을 확인합니다.
- SAML 기반 페더레이션 인증의 경우 IdP 구성 및 사용자 권한을 확인합니다.
- 자세한 오류 정보는 CloudWatch의 인증 로그를 검토하세요.
- 엔드포인트에 구성된 인증 방법이 클라이언트 구성과 일치하는지 확인합니다.

권한 부여 규칙 확인

권한 부여 규칙은 클라이언트가 액세스할 수 있는 네트워크 리소스를 제어합니다.

1. 현재 권한 부여 규칙 나열:

```
aws ec2 describe-client-vpn-authorization-rules --client-vpn-endpoint-id cvpn-
endpoint-id --region your-region
```

2. 클라이언트가 액세스해야 하는 대상 네트워크에 대한 규칙이 있는지 확인합니다.
3. 규칙이 올바른 Active Directory 그룹을 지정하는지 확인합니다(AD 인증을 사용하는 경우).

4. 권한 부여 규칙이 `active` 상태인지 확인합니다.

Client VPN 경로 검증

Client VPN 연결에는 적절한 라우팅 구성이 필수적입니다.

1. Client VPN 엔드포인트 라우팅 확인:

```
aws ec2 describe-client-vpn-routes --client-vpn-endpoint-id cvpn-endpoint-id --
region your-region
```

2. 클라이언트가 액세스해야 하는 대상 네트워크에 경로가 있는지 확인합니다.
3. Amazon VPC 라우팅 테이블을 확인하여 반환 트래픽이 Client VPN 엔드포인트에 도달할 수 있는지 확인합니다.

```
aws ec2 describe-route-tables --filters "Name=vpc-id,Values=vpc-id" --region your-
region
```

4. 대상 네트워크 연결이 올바르게 구성되었는지 확인합니다.

보안 그룹 및 네트워크 ACL 확인

보안 그룹 및 네트워크 ACLs Client VPN 트래픽을 차단할 수 있습니다.

1. 대상 EC2 인스턴스의 보안 그룹을 확인합니다.

```
aws ec2 describe-security-groups --group-ids sg-xxxxxxxxx --region your-region
```

2. 인바운드 규칙이 Client VPN CIDR 블록의 트래픽을 허용하는지 확인합니다.
   - Client VPN CIDR의 SSH(포트 22): `10.0.0.0/16`
   - Client VPN CIDR의 HTTP(포트 80): `10.0.0.0/16`
   - Client VPN CIDR의 HTTPS(포트 443): `10.0.0.0/16`
   - 필요에 따라 사용자 지정 애플리케이션 포트
3. Client VPN 엔드포인트 보안 그룹(해당하는 경우)에서 다음을 허용하는지 확인합니다.
   - 0.0.0.0/0의 UDP 포트 443(OpenVPN)
   - VPC CIDR 블록으로 아웃바운드되는 모든 트래픽

4. 네트워크 ACL 트래픽을 차단하지 않는지 확인합니다. 네트워크 ACL은 상태 비저장이므로 인바운드 및 아웃바운드 규칙을 모두 구성해야 합니다.
5. 전송하려는 특정 트래픽에 대한 인바운드 및 아웃바운드 규칙을 모두 확인합니다.

클라이언트 연결 테스트

Client VPN 클라이언트에서 Amazon VPC 리소스로의 연결을 테스트합니다.

1. 연결된 Client VPN 클라이언트에서 Amazon VPC 리소스에 대한 연결을 테스트합니다.

```
ping vpc-resource-ip
traceroute vpc-resource-ip
```

2. 지정된 애플리케이션 연결성 테스트:

```
telnet vpc-resource-ip port
```

3. 프라이빗 DNS 이름을 사용하는 경우 DNS 확인을 확인합니다.

```
nslookup private-dns-name
```

4. 분할 터널링이 활성화된 경우 인터넷 리소스에 대한 연결을 테스트합니다.

클라이언트 디바이스 진단

클라이언트 디바이스에서 다음 검사를 수행합니다.

1. 클라이언트 구성 파일(.ovpn)에 올바른 설정이 포함되어 있는지 확인합니다.
   - 올바른 서버 엔드포인트 URL
   - 유효한 클라이언트 인증서 및 프라이빗 키
   - 적절한 인증 방법 구성
2. 클라이언트 로그에서 연결 오류를 확인합니다.
   - Windows: 이벤트 뷰어 → 애플리케이션 및 서비스 로그 → OpenVPN
   - macOS: 콘솔 앱, 'Tunnelblick' 또는 'OpenVPN' 검색
   - Linux: `/var/log/openvpn/` 또는 시스템 저널
3. 클라이언트의 기본 네트워크 연결을 테스트합니다.

```
ping 8.8.8.8
nslookup cvpn-endpoint-id.cvpn.region.amazonaws.com
```

DNS 확인 문제 해결

DNS 문제는 프라이빗 DNS 이름을 사용한 리소스 액세스를 방해할 수 있습니다.

1. Client VPN 엔드포인트에 DNS 서버가 구성되어 있는지 확인합니다.

```
aws ec2 describe-client-vpn-endpoints --client-vpn-endpoint-ids cvpn-endpoint-id --
query 'ClientVpnEndpoints[0].DnsServers'
```

2. 클라이언트에서 DNS 확인을 테스트합니다.

```
nslookup private-resource.internal
dig private-resource.internal
```

3. 사용자 지정 DNS 확인을 사용하는 경우 Route 53 Resolver 규칙을 확인합니다.
4. 보안 그룹이 Client VPN CIDR에서 DNS 서버로의 DNS 트래픽(UDP/TCP 포트 53)을 허용하는지 확인합니다.

성능 문제 해결

Client VPN 연결의 성능 문제를 해결합니다.

- CloudWatch 지표를 사용하여 수신/송신 바이트에 대한 대역폭 사용률을 모니터링합니다.
- 클라이언트의 지속적 ping 테스트를 사용하여 패킷 손실을 확인합니다.
- Client VPN 엔드포인트가 연결 제한에 도달하지 않는지 확인합니다.
- 로드 배포에 여러 Client VPN 엔드포인트를 사용하는 것이 좋습니다.
- 다양한 클라이언트 위치로 테스트하여 리전별 성능 문제를 식별합니다.

Client VPN 지표 모니터링

CloudWatch를 사용하여 Client VPN 엔드포인트 지표를 모니터링합니다.

1. 활성 연결 지표 확인:

```
aws cloudwatch get-metric-statistics \
  --namespace AWS/ClientVPN \
  --metric-name ActiveConnectionsCount \
  --dimensions Name=Endpoint,Value=cvpn-endpoint-id \
  --start-time start-time \
  --end-time end-time \
  --period 300 \
  --statistics Average
```

2. 인증 실패 지표 검토:

```
aws cloudwatch get-metric-statistics \
  --namespace AWS/ClientVPN \
  --metric-name AuthenticationFailures \
  --dimensions Name=Endpoint,Value=cvpn-endpoint-id \
  --start-time start-time \
  --end-time end-time \
  --period 300 \
  --statistics Sum
```

3. 수신/송신 바이트 및 패킷과 같은 기타 사용 가능한 지표를 검토합니다.

Client VPN 로그 확인

Client VPN 연결 로그는 연결 시도 및 오류에 대한 자세한 정보를 제공합니다.

- 아직 구성되지 않은 경우 Client VPN 연결 로깅을 활성화합니다.
- CloudWatch 로그에서 연결 시도, 인증 실패 및 권한 부여 오류를 검토합니다.
- 연결 문제의 근본 원인을 나타내는 특정 오류 코드와 메시지를 찾습니다.
- 실패한 연결에서 구성 문제를 나타낼 수 있는 패턴이 있는지 확인합니다.

일반적인 문제 및 해결 방법

Client VPN 연결에 영향을 미칠 수 있는 일반적인 문제:

인증 실패 횟수

클라이언트 인증서가 만료되었거나 유효하지 않거나 Active Directory 자격 증명이 잘못되었습니다. 인증 구성 및 자격 증명 유효성을 확인합니다.

권한 부여 규칙 누락

누락되거나 잘못된 권한 부여 규칙으로 인해 클라이언트가 대상 네트워크에 액세스할 수 없습니다. 필요한 네트워크에 적절한 권한 부여 규칙을 추가합니다.

분할 터널링 문제

분할 터널링 구성으로 인해 트래픽 라우팅이 잘못되었습니다. 필요에 따라 분할 터널링 설정을 검토하고 조정합니다.

클라이언트 IP 풀 소진

클라이언트 CIDR 블록에 사용 가능한 IP 주소가 없습니다. 클라이언트 CIDR 범위를 확장하거나 사용하지 않는 클라이언트의 연결을 해제합니다.

MTU 문제

MTU 크기 제한으로 인해 대용량 패킷이 삭제되고 있습니다. MTU를 1436바이트로 설정하거나 클라이언트 디바이스에서 경로 MTU 검색을 활성화해 봅니다.

DNS 확인 문제

클라이언트가 프라이빗 DNS 이름을 확인할 수 없습니다. DNS 서버 구성을 확인하고 보안 그룹을 통해 DNS 트래픽이 허용되는지 확인합니다.

IP 범위 겹침

클라이언트 CIDR 블록이 로컬 네트워크 범위와 충돌합니다. 클라이언트 CIDR과 로컬 네트워크 간에 겹치는 IP 주소 범위를 확인하고 해결합니다.

TLS 핸드셰이크 실패

TLS 협상 중에 연결이 실패합니다. 인증서 유효성을 확인하고, 올바른 암호 제품군을 확인하고, 클라이언트 및 서버 인증서가 올바르게 구성되었는지 확인합니다.

경로 전파 지연

클라이언트가 새 경로를 즉시 사용할 수 없습니다. Client VPN 경로를 변경한 후 경로 전파에 1~2분을 기다립니다.

연결 끊김/불안정

연결이 자주 끊기거나 불안정합니다. 클라이언트 디바이스에서 네트워크 정체, 방화벽 간섭 또는 전원 관리 설정을 확인합니다.

Client VPN 사용 설명서에 대한 문서 기록

다음 표에서는 AWS Client VPN 관리자 안내서 업데이트를 설명합니다.

변경 사항	설명	날짜
IPv6 지원	이제 Client VPN은 Client VPN 엔드포인트에 대한 전체 IPv6 연결을 활성화하여 VPC의 IPv6 리소스 및 IPv6 네트워크의 클라이언트와의 연결을 지원합니다.	2025년 8월 25일
클라이언트 경로 강제 적용 기능	클라이언트 경로 강제 적용 기능 추가.	2025년 4월 20일
Client VPN 할당량 증가	Client VPN 엔드포인트당 권한 부여 규칙 할당량을 50에서 200으로 늘렸습니다.	2025년 3월 13일
세션 시간 초과 시 연결 해제 지원	세션 제한 시간은 이제 세션 최대 지속 시간 도달 시 연결 해제를 지원합니다.	2025년 1월 13일
늘어난 할당량	Client VPN 엔드포인트당 권한 부여 규칙 및 Client VPN 엔드포인트당 경로 할당량이 각각 50 및 10에서 100으로 증가했습니다.	2024년 12월 19일
권한 부여 규칙 예	권한 부여 규칙에 대한 예제 시나리오 추가	2022년 9월 15일
VPN 최대 세션 기간	보안 및 규정 준수 요구 사항을 충족하도록 더 짧은 최대 VPN 세션 기간을 구성할 수 있습니다.	2022년 1월 20일

클라이언트 로그인 배너	규정 및 규정 준수 요구 사항을 충족하기 위해 VPN 세션을 설정할 때 AWS 제공 Client VPN 데스크톱 애플리케이션에 텍스트 배너를 활성화할 수 있습니다.	2022년 1월 20일
클라이언트 연결 핸들러	Client VPN 엔드포인트에 대해 클라이언트 연결 핸들러를 활성화하여 새 연결 권한을 부여하는 사용자 지정 논리를 실행할 수 있습니다.	2020년 11월 4일
셀프 서비스 포털	클라이언트에 대해 Client VPN 엔드포인트에서 셀프 서비스 포털을 활성화할 수 있습니다.	2020년 10월 29일
클라이언트 간 액세스	Client VPN 엔드포인트에 연결하는 클라이언트가 서로 연결되도록 할 수 있습니다.	2020년 9월 29일
SAML 2.0 기반 연동 인증	SAML 2.0 기반 연동 인증을 사용하여 Client VPN 사용자를 인증할 수 있습니다.	2020년 5월 19일
생성 중 보안 그룹 지정	AWS Client VPN 엔드포인트를 생성할 때 VPC 및 보안 그룹을 지정할 수 있습니다.	2020년 3월 5일
구성 가능한 VPN 포트	AWS Client VPN 엔드포인트에 지원되는 VPN 포트 번호를 지정할 수 있습니다.	2020년 1월 16일
멀티 펙터 인증(MFA) 지원	AWS Client VPN 엔드포인트는 Active Directory에 대해 활성화된 경우 MFA를 지원합니다.	2019년 9월 30일

분할 터널 지원	AWS Client VPN 엔드포인트에서 분할 터널을 활성화할 수 있습니다.	2019년 7월 24일
최초 릴리스입니다.	이 릴리스는 AWS Client VPN을 도입했습니다.	2018년 12월 18일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.