관리자 안내서

AWS 클라이언트 VPN

AWS 클라이언트 VPN: 관리자 안내서

Table of Contents

AWS Client VPN이란 무엇인가요?

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

목차

Client VPN의 기능

Client VPN은 다음과 같은 기능을 제공합니다.

- 보안 연결 - OpenVPN 클라이언트를 사용하여 어떤 위치에서든 안전한 TLS 연결을 제공합니다.
- 관리형 서비스 — AWS 관리형 서비스이므로 타사 원격 액세스 VPN 솔루션을 배포하고 관리하는 운영 부담을 없애줍니다.
- 고가용성 및 탄력성 — AWS 리소스 및 온프레미스 리소스에 연결하는 사용자 수에 따라 자동으로 확장됩니다.
- 인증 - Active Directory 인증, 연동 인증 및 인증서 기반 인증을 사용한 클라이언트 인증을 지원합니다.
- 세분화된 제어 - 네트워크 기반 액세스 규칙을 정의하여 사용자 지정 보안 제어를 구현할 수 있습니다. 이러한 규칙은 Active Directory 그룹의 세부 수준에서 구성됩니다. 또한 보안 그룹을 사용하여 액세스 제어를 구현할 수도 있습니다.
- 사용 편의성 — 단일 VPN 터널을 사용하여 AWS 리소스와 온프레미스 리소스에 액세스할 수 있습니다.
- 관리 효율성 - 클라이언트 연결 시도에 대한 세부 정보를 제공하는 연결 로그를 볼 수 있습니다. 또한 활성 클라이언트 연결을 종료하는 기능을 포함하여 활성 클라이언트 연결을 관리할 수도 있습니다.
- 심층 통합 — Amazon VPC를 비롯한 AWS Directory Service 기존 AWS 서비스와 통합됩니다.

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. VPC의 서브넷이 대상 네트워크입니다. 서브넷을 Client VPN 엔드포인트와 연결하면 VPN 세션을 설정할 수 있습니다. 고가용성을 위해 여러 서브넷을 하나의 Client VPN 엔드포인트와 연결할 수 있습니다. 모든 서브넷이 동일한 VPC에 위치해야 합니다. 각 서브넷이 서로 다른 가용 영역에 속해야 합니다.

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. 클라이언트 CIDR 범위(예: `10.2.0.0/16`)를 선택합니다.

Client VPN 포트

AWS 클라이언트 VPN은 TCP와 UDP 모두에 대해 포트 443과 1194를 지원합니다. 기본값은 포트 443입니다.

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. 그런 다음 클라이언트 CIDR 범위의 소스 IP 주소가 Client VPN 네트워크 인터페이스 IP 주소로 변환되는 소스 네트워크 주소 변환(SNAT)이 적용됩니다.

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), (미국 서부) 지역의 서비스 스택으로 뒷받침되는 글로벌 서비스입니다. AWS GovCloud

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. 가입한 경우 Amazon VPC 콘솔에 로그인하고 탐색 창에서 Client VPN을 선택할 수 있습니다. AWS 계정

AWS Command Line Interface (AWS CLI)

는 Client VPN 퍼블릭 API에 대한 직접 액세스를 AWS CLI 제공합니다. 이는 Windows, macOS, Linux에서 지원됩니다. 시작하는 방법에 대한 자세한 내용은 AWS Command Line Interface 사용 설명서를 참조하십시오. AWS CLI Client VPN 명령에 대한 자세한 내용은 AWS CLI 명령 참조를 참조하세요.

AWS Tools for Windows PowerShell

AWS PowerShell 환경에서 스크립트를 작성하는 사용자를 위한 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

클라이언트 VPN HTTPS 쿼리 API를 사용하면 클라이언트 VPN 및 에 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. 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 계정에 CloudWatch 로그 로그 그룹을 생성해야 합니다. 로그 그룹 이용 시 요금이 부과됩니다. 자세한 내용은 Amazon CloudWatch 가격 책정 (유료 티어에서 로그 선택) 을 참조하십시오.

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.

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

의 규칙 및 모범 사례 AWS Client VPN

에 대한 규칙 및 모범 사례는 다음과 같습니다. AWS Client VPN

- 사용자 연결당 최소 10Mbps의 대역폭이 지원됩니다. 사용자 연결당 최대 대역폭은 Client VPN 엔드포인트에 대한 연결 수에 따라 달라집니다.
- 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 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.
- Client VPN은 IPv4 트래픽만 지원합니다. IPv6에 대한 자세한 내용은 AWS Client VPN에 대한 IPv6 고려 사항을 참조하세요.
- Client VPN은 Federal Information Processing Standard(FIPS)를 준수하지 않습니다.
- 상호 인증을 사용하여 인증하는 클라이언트에는 셀프 서비스 포털을 사용할 수 없습니다.
- 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 확인할 수 있습니다. 제공된 DNS 이름을 사용하여 Client VPN 엔드포인트에 연결하는 것이 좋습니다.
- 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 지역에 있어야 합니다.
- Active Directory에 대해 다중 인증(MFA)이 비활성화된 경우 사용자 암호에 다음과 같은 형식을 사용할 수 없습니다.

```
SCRV1:base64_encoded_string:base64_encoded_string
```

- 운영 체제에 로그인한 사용자가 여러 명인 경우 컴퓨터에서 VPN 연결을 설정할 수 없습니다.
- Client VPN 서비스를 사용하려면 클라이언트가 연결된 IP 주소가 클라이언트 VPN 엔드포인트의 DNS 이름이 확인하는 IP와 일치해야 합니다. 즉, Client VPN 엔드포인트에 대한 사용자 지정 DNS 레코드를 설정한 다음 엔드포인트의 DNS 이름이 확인되는 실제 IP 주소로 트래픽을 전달하는 경우 최근에 AWS제공한 클라이언트에서는 이 설정이 작동하지 않습니다. 이 규칙은 다음과 같이 서버 IP 공격을 완화하기 위해 추가되었습니다. TunnelCrack
- Client VPN 서비스를 사용하려면 클라이언트 장치의 LAN (Local Area Network) IP 주소 범위가 다음 표준 사설 IP 주소 범위 (`10.0.0.0/8`, `172.16.0.0/12`192.168.0.0/16, 또는) 내에 있어야 `169.254.0.0/16` 합니다. 클라이언트 LAN 주소 범위가 위 범위를 벗어나는 것으로 감지되면 클라

이언트 VPN 엔드포인트는 OpenVPN 지침 “리디렉션 게이트웨이 블록 로컬”을 자동으로 클라이언트에 푸시하여 모든 LAN 트래픽을 VPN으로 강제 전송합니다. 따라서 VPN 연결 중에 LAN 액세스가 필요한 경우 위에 나열된 일반 LAN 주소 범위를 사용하는 것이 좋습니다. 이 규칙은 다음과 같이 로컬 네트워크 공격의 가능성을 줄이기 위해 적용됩니다. TunnelCrack

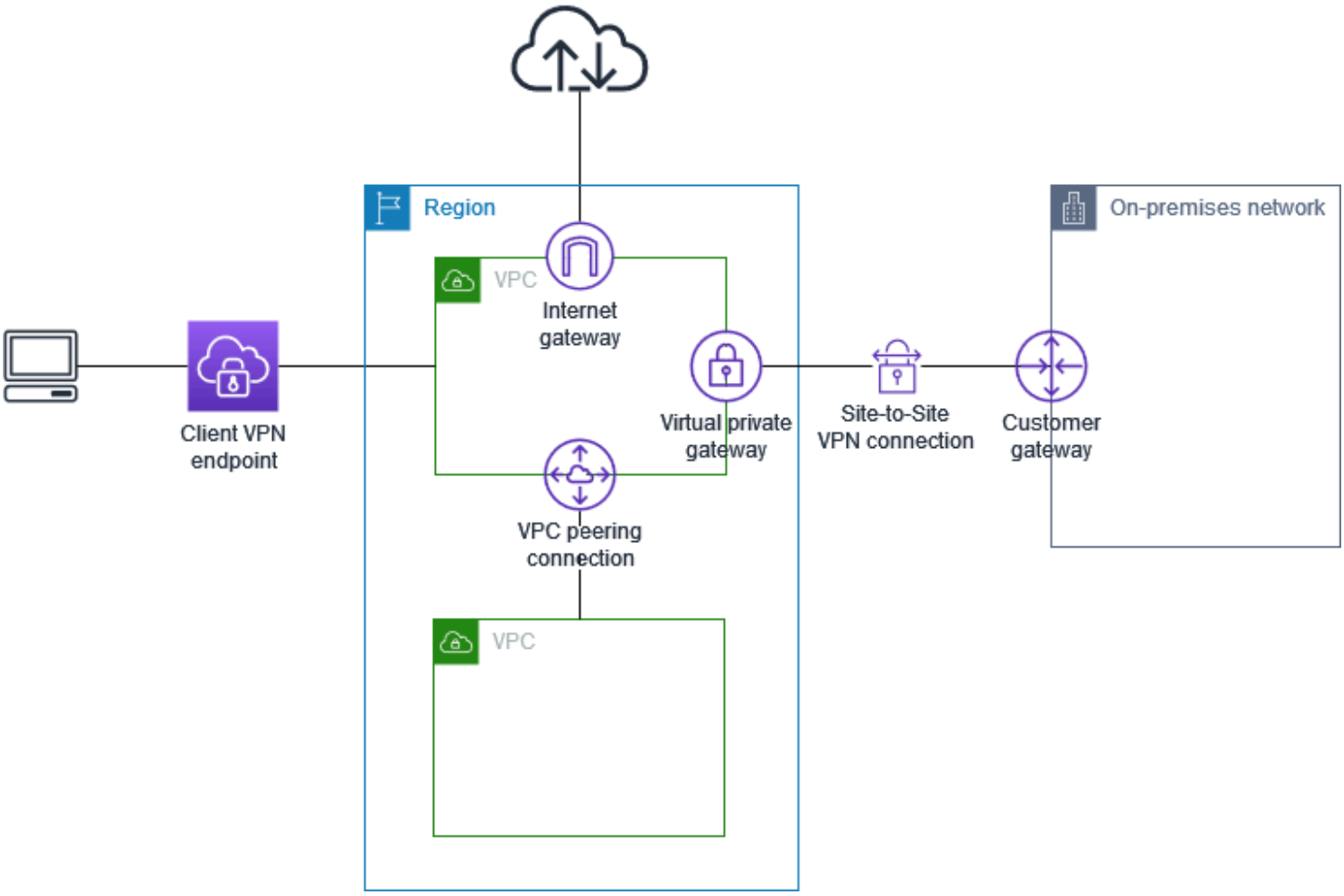
AWS Client VPN의 작동 방식

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

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 AWS Client VPN 시작하기 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.



클라이언트 인증

클라이언트 인증은 AWS 클라우드에 진입하는 첫 번째 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)

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 만들려면 사용하는 인증 유형에 관계없이 에서 AWS Certificate Manager서버 인증서를 프로비저닝해야 합니다. 서버 인증서를 생성하고 프로비저닝하는 방법에 대한 자세한 내용은 상호 인증의 단계를 참조하십시오.

Active Directory 인증

Client VPN은 다음과 통합하여 액티브 디렉터리 지원을 제공합니다. AWS Directory Service Active Directory 인증에서는 클라이언트가 기존 Active Directory 그룹에 의해 인증됩니다. 를 사용하여 AWS Directory Service Client VPN은 온프레미스 네트워크에서 AWS 또는 온프레미스 네트워크에서 프로비전된 기존 Active Directory에 연결할 수 있습니다. 이를 통해 기존 클라이언트 인증 인프라를 사용할 수 있습니다. 온-프레미스 Active Directory를 사용 중이고 기존 AWS 관리형 Microsoft AD가 없는 경우 AD 커넥터 (Active Directory 커넥터) 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.

상호 인증

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.

AWS Certificate Manager (ACM) 에 서버 인증서를 업로드하고 Client VPN 엔드포인트를 생성할 때 이를 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.

> **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. 이 자동화 프로세스에는 최대 24시간이 소요될 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 를 AWS CLI 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.

서버 인증서 갱신

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

서버 인증서 갱신하기

1. 다음 중 하나를 수행하십시오.
   - 이지 RSA 버전 3.1.x
     - 인증서 갱신 명령을 실행합니다.

       ```
       $ ./easyrsa renew server nopass
       ```
   - 이지 RSA 버전 3.2.x
     a. 만료 명령을 실행합니다.

        ```
        $ ./easyrsa expire server
        ```
     b. 새 인증서에 서명하세요.

        ```
        $ ./easyrsa 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
   ```

Single sign-on(SAML 2.0 기반 연동 인증)

AWS Client VPN Client VPN 엔드포인트에 대한 보안 어설션 마크업 언어 2.0 (SAML 2.0) 과의 ID 페더레이션을 지원합니다. SAML 2.0을 지원하는 ID 공급자 (IdPs) 를 사용하여 중앙 집중식 사용자 ID를 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.

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

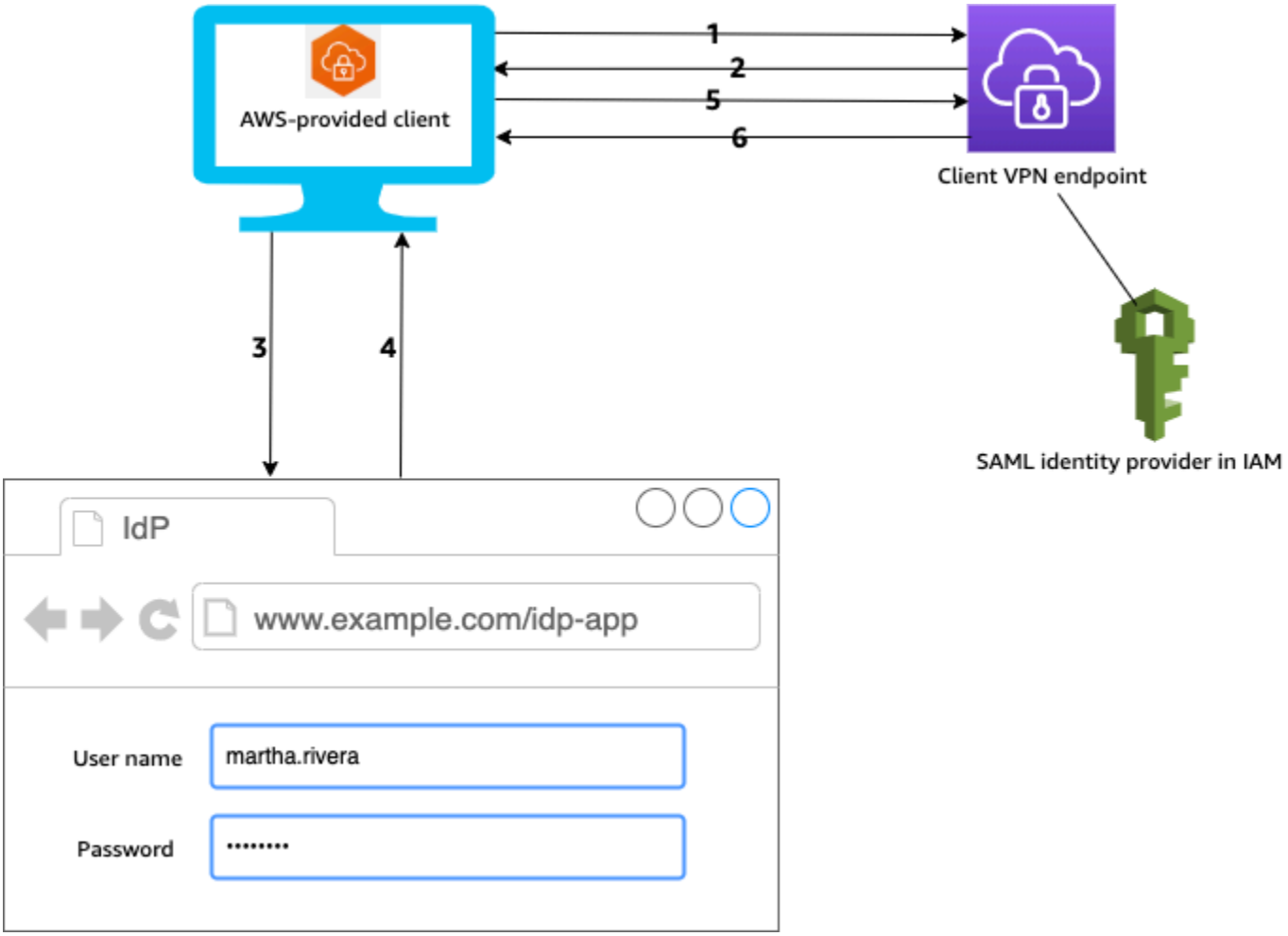
1. 선택한 IdP에서 SAML 기반 앱을 생성하여 함께 AWS Client VPN사용하거나 기존 앱을 사용할 수 있습니다.
2. IdP를 구성하여 와 신뢰 관계를 설정합니다 AWS리소스에 대한 자세한 내용은 SAML 기반 IdP 구성 리소스 단원을 참조하십시오.
3. 사용 중인 IdP에서 조직을 IdP로 설명하는 연동 메타데이터 문서를 생성하고 다운로드합니다. 이 서명된 XML 문서는 IdP AWS 간의 신뢰 관계를 설정하는 데 사용됩니다.
4. Client VPN 엔드포인트와 동일한 AWS 계정에 IAM SAML ID 공급자를 생성합니다. IAM SAML ID 공급자는 IdP에서 생성한 메타데이터 문서를 사용하여 조직의 IdP와AWS 신뢰 관계를 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 Client VPN 엔드포인트를 생성합니다.을 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. 또는 Client VPN 엔드포인트에 대한 셀프 서비스 포털을 활성화한 경우 사용자에게 셀프 서비스 포털로 이동하여 구성 파일과 제공된 클라이언트를 가져오도록 안내하세요. AWS 자세한 정보는 셀프 서비스 포털 액세스을 참조하세요.

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. 사용자가 장치에서 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 클라이언트는 사용자 장치에서 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 클라이언트가 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 SAML 문서에는 서명해야 합니다.
- AWS Client VPN SAML AudienceRestriction 어설션의 "" NotBefore 및 NotOnOrAfter "조건만 지원합니다.
- SAML 응답에 대해 지원되는 최대 크기는 128KB입니다.
- AWS Client VPN 서명된 인증 요청을 제공하지 않습니다.
- SAML 단일 로그아웃은 지원되지 않습니다. 사용자는 AWS 제공된 클라이언트와의 연결을 끊어 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 사용한 Connect를 참조하십시오.
- IdP 인증을 지원하는 브라우저로는 Apple Safari, Google Chrome, Microsoft Edge, Mozilla Firefox 등이 있습니다.
- AWS 제공된 클라이언트는 SAML 응답을 위해 사용자 장치의 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 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.

SAML 기반 IdP 구성 리소스

다음 표에는 사용을 위해 테스트한 SAML 기반 IdPs 및 IdP AWS Client VPN구성에 도움이 되는 리소스가 나열되어 있습니다.

IdP	리소스
Okta	SAML로 사용자 인증하기 AWS Client VPN
Microsoft Azure Active Directory	자세한 내용은 Microsoft 설명서 웹 사이트의 자습서: Azure Active Directory 싱글 사인온 (SSO) 과 AWS ClientVPN의 통합을 참조하십시오.
JumpCloud	싱글 사인온 (SSO) 을 사용하여 AWS Client VPN
AWS IAM Identity Center	인증 및 권한 AWS Client VPN 부여에 IAM ID 센터 사용

앱 생성을 위한 서비스 공급자 정보

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

- 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 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
```

특정 GovCloud 지역에서 Client VPN 엔드포인트를 사용하는 경우 다음 ACS URL을 대신 사용하십시오. 동일한 IDP 앱을 사용하여 표준 및 GovCloud 지역 모두를 인증하는 경우 두 URL을 모두 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 ID 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.

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 대상 네트워크에 보안 그룹 적용을 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.

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 Groups]를 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.

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 AWS 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 정보는 권한 부여 규칙을 참조하십시오.

연결 권한 부여

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 클라이언트 VPN 엔드포인트와 AWS 동일한 지역 및 AWS 동일한 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 정보는 클라이언트 연결 종료을 참조하세요.
- 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 NameID입니다. 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— 클라이언트 버전. AWS
- 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 v3입니다.

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: 조절로 인해) 다음과 같은 기본 메시지가 클라이언트에게 반환됩니다.

```
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 처리기를 사용하여 최소 AWS Client VPN 응용 프로그램 버전을 적용할 수 있지만 연결 처리기의 필드는 `aws-client-version` AWS Client VPN 응용 프로그램에만 적용할 수 있으며 사용자 장치의 환경 변수로 채워집니다.

클라이언트 연결 핸들러 활성화

클라이언트 연결 핸들러를 활성화하려면 Client VPN 엔드포인트을 생성하거나 수정하고 Lambda 함수의 Amazon 리소스 이름(ARN)을 지정합니다. 자세한 내용은 Client VPN 엔드포인트를 생성합니다. 및 Client VPN 엔드포인트를 수정합니다. 단원을 참조하십시오.

서비스 연결 역할

AWS Client VPN 라는 계정에 서비스 연결 역할을 자동으로 생성합니다. AWSServiceRoleForClientVPNConnections 역할에는 Client VPN 엔드포인트에 연결할 때 Lambda 함수를 호출할 수 있는 권한이 있습니다. 자세한 정보는 Client VPN에 서비스 연결 역할 사용을 참조하십시오.

연결 권한 부여 실패 모니터링

Client VPN 엔드포인트 연결의 연결 권한 부여 상태를 볼 수 있습니다. 자세한 정보는 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 연결 로깅을 참조하십시오.

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

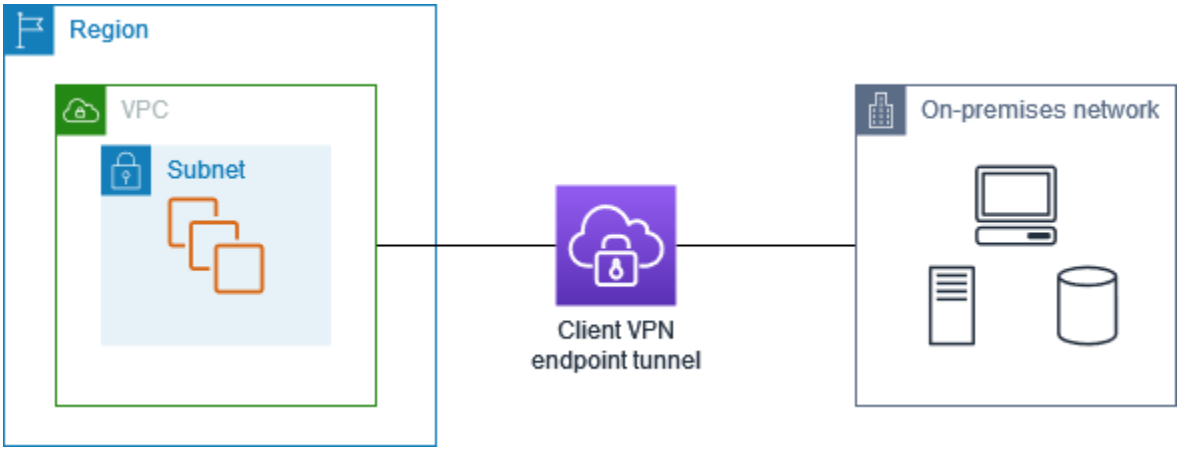
- `client-connect-failed` - Lambda 함수로 인해 연결을 설정할 수 없습니다.
- `client-connect-handler-timed-out` - Lambda 함수가 시간 초과되었습니다.
- `client-connect-handler-other-execution-error` - Lambda 함수에서 예기치 않은 오류가 발생했습니다.
- `client-connect-handler-throttled` - Lambda 함수가 조절되었습니다.
- `client-connect-handler-invalid-response` - 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 경로 테이블에 `0.0.0.0/0` 경로를 추가하지 않는 것이 좋습니다.

- 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.

- Client VPN 엔드포인트를 생성합니다.
- Client VPN 엔드포인트를 수정합니다.

연결 로깅

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

연결 로그에는 연결 로그 항목이 포함되어 있습니다. 각 연결 로그 항목에는 클라이언트(최종 사용자)가 Client VPN 엔드포인트에서 연결하거나 연결을 시도하거나 연결을 해제할 때의 연결 이벤트에 대한 정보가 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 연결 로그 작업 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 부응할 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 의 규칙 및 모범 사례 AWS Client VPN을(를) 참조하세요.

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

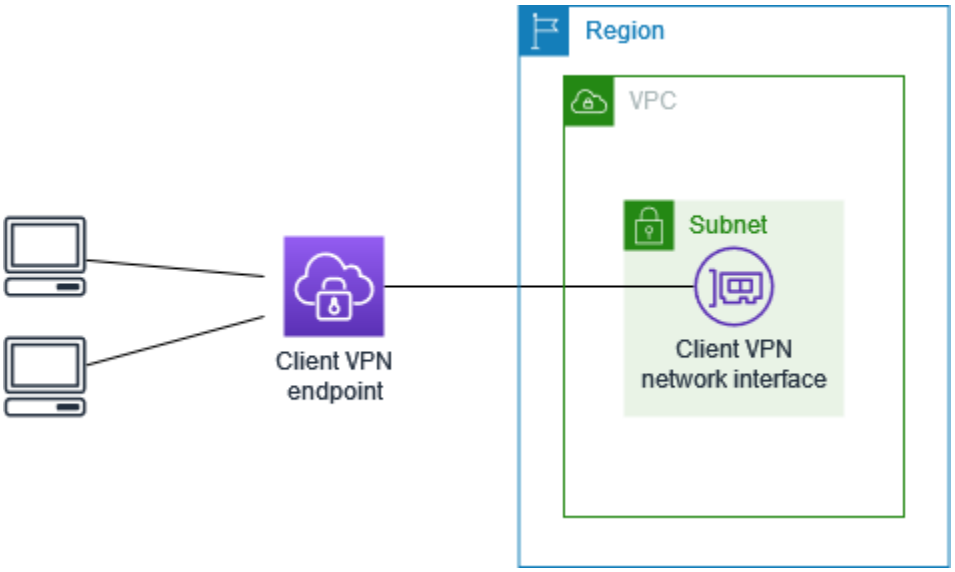
AWS Client VPN의 시나리오 및 예제

이 단원에서는 클라이언트에 대한 Client VPN 액세스 권한을 생성하고 구성하는 예를 제공합니다.

내용

AWS Client VPN을 사용하여 VPC 액세스

이 시나리오의 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.

- 의 규칙 및 모범 사례 AWS Client VPN에서 Client VPN 엔드포인트에 대한 규칙과 제한 사항을 검토합니다.

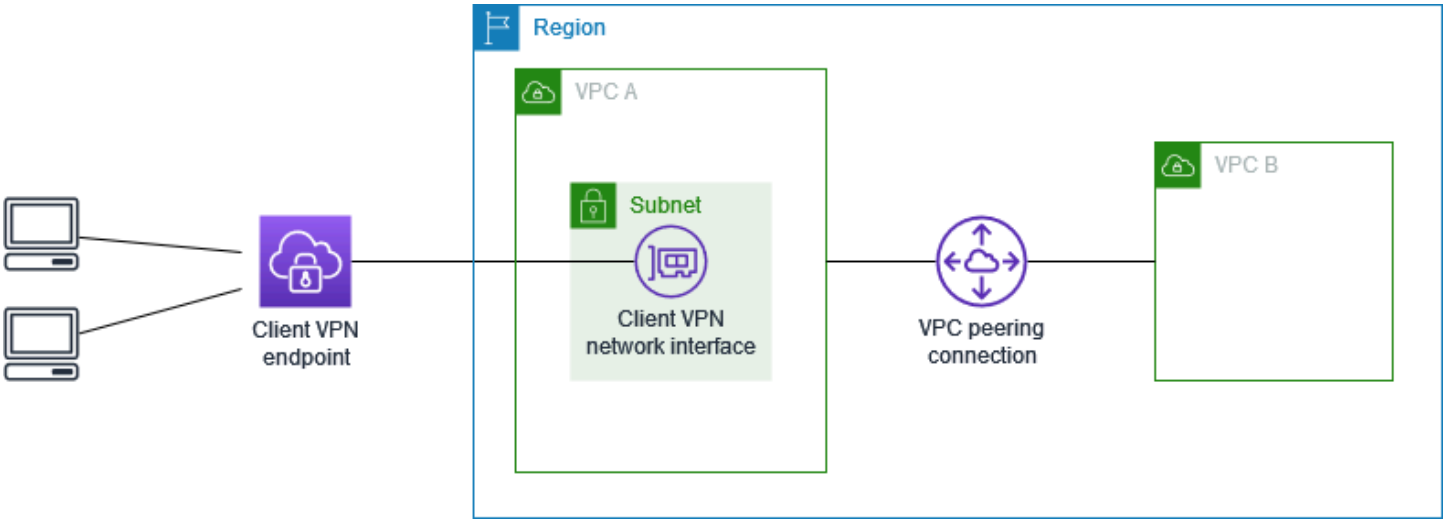
이 구성을 구현하는 방법

1. VPC와 동일한 리전에서 Client VPN 엔드포인트를 생성합니다. 이렇게 하려면 Client VPN 엔드포인트를 생성합니다.에 설명된 단계를 수행합니다.
2. 서브넷을 Client VPN 엔드포인트와 연결합니다. 이렇게 하려면 대상 네트워크를 Client VPN 엔드포인트와 연결합니다.에 설명된 단계를 수행하고 앞에서 식별한 서브넷 및 VPC를 선택합니다.
3. 권한 부여 규칙을 추가하여 클라이언트에 VPC에 대한 액세스 권한을 부여합니다. 이렇게 하려면 Client VPN 엔드포인트에 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 설명은 보안 그룹 섹션을 참조하세요.

AWS Client VPN을 사용하여 피어링된 VPC 액세스

이 시나리오의 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**
>
> 아래에 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.
- 의 규칙 및 모범 사례 AWS Client VPN에서 Client VPN 엔드포인트에 대한 규칙과 제한 사항을 검토합니다.

이 구성을 구현하는 방법

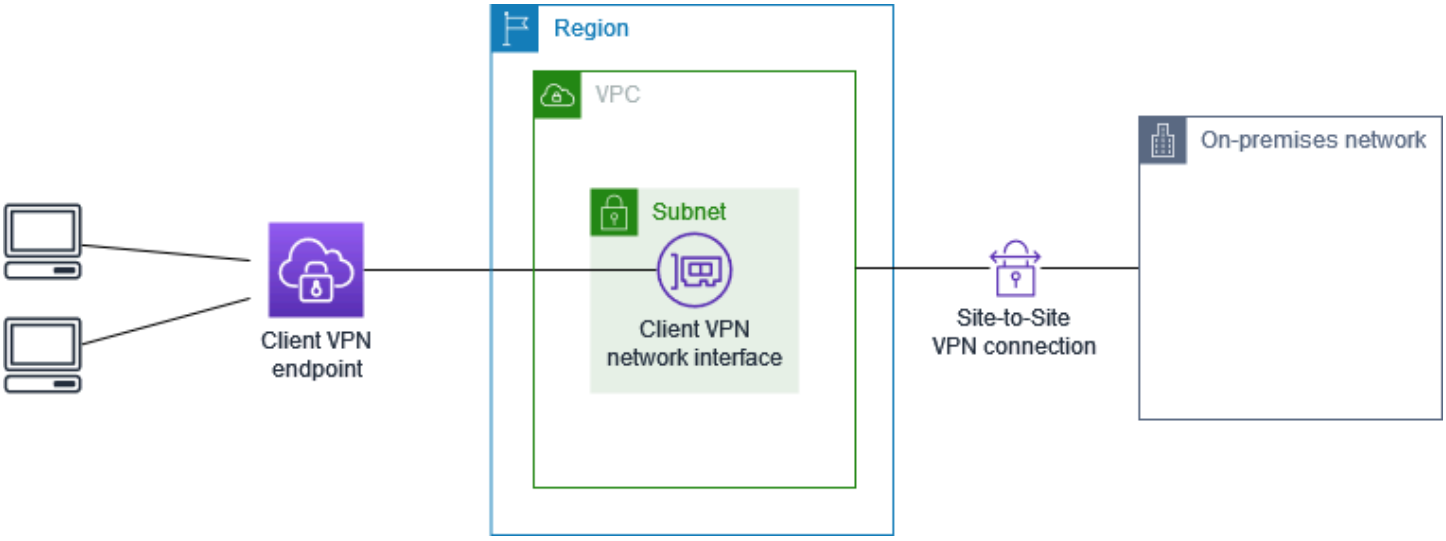
1. VPC 사이에 VPC 피어링 연결을 설정합니다. Amazon VPC 피어링 가이드의 VPC 피어링 연결 생성 및 수락에 있는 단계를 따릅니다. VPC A의 인스턴스에서 피어링 연결을 사용하여 VPC B의 인스턴스와 통신할 수 있는지 확인합니다.
2. 대상 VPC와 동일한 리전에서 Client VPN 엔드포인트를 생성합니다. 다이어그램에서 이것은 VPC A입니다. Client VPN 엔드포인트를 생성합니다.에 설명된 단계를 수행합니다.
3. 식별한 서브넷을 생성한 Client VPN 엔드포인트와 연결합니다. 이렇게 하려면 대상 네트워크를 Client VPN 엔드포인트와 연결합니다.에 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 Client VPN 엔드포인트에 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 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 Client VPN 엔드포인트에 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 설명은 보안 그룹 섹션을 참조하세요.

AWS Client VPN을 사용하여 온프레미스 네트워크 액세스

이 시나리오의 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.
- 의 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.

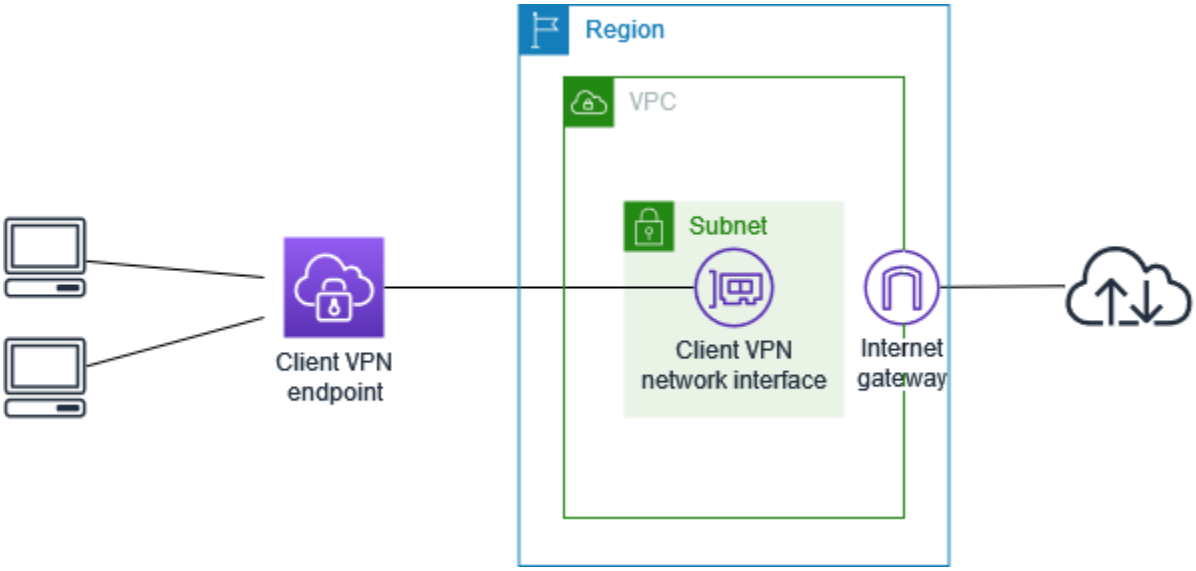
   > **Note**
   >
   > 또는 VPC와 온프레미스 네트워크 간의 AWS Direct Connect 연결을 사용하여 이 시나리오를 구현할 수 있습니다. 자세한 내용은 AWS Direct Connect 사용 설명서를 참조하세요.

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 Client VPN 엔드포인트를 생성합니다.에 설명된 단계를 수행합니다.
4. 앞에서 식별한 서브넷을 Client VPN 엔드포인트와 연결합니다. 이렇게 하려면 대상 네트워크를 Client VPN 엔드포인트와 연결합니다.에 설명된 단계를 수행하고 VPC 및 서브넷을 선택합니다.
5. AWS Site-to-Site VPN 연결에 대한 액세스를 허용하는 경로를 추가합니다. 이렇게 하려면 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 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.

AWS Client VPN을 사용하여 인터넷 액세스

이 시나리오의 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.

AWS Client VPN 시작하기 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.
- 의 규칙 및 모범 사례 AWS Client VPN에서 Client VPN 엔드포인트에 대한 규칙과 제한 사항을 검토합니다.

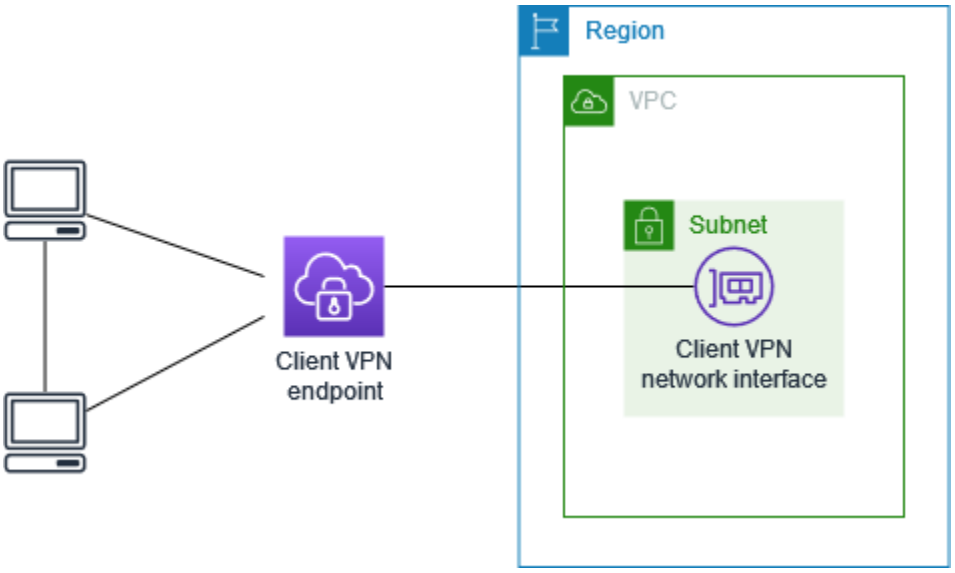
이 구성을 구현하는 방법

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 Client VPN 엔드포인트를 생성합니다.에 설명된 단계를 수행합니다.

5. 앞에서 식별한 서브넷을 Client VPN 엔드포인트와 연결합니다. 이렇게 하려면 대상 네트워크를 Client VPN 엔드포인트와 연결합니다.에 설명된 단계를 수행하고 VPC 및 서브넷을 선택합니다.
6. 권한 부여 규칙을 추가하여 클라이언트에 VPC에 대한 액세스 권한을 부여합니다. 이렇게 하려면 Client VPN 엔드포인트에 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 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 Client VPN 엔드포인트에 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.

AWSClient VPN을 사용한 C lient-to-client 액세스

이 시나리오의 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.
- 의 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 Client VPN 엔드포인트를 생성합니다.에 설명된 단계를 수행합니다.
2. 앞에서 식별한 서브넷을 Client VPN 엔드포인트와 연결합니다. 이렇게 하려면 대상 네트워크를 Client VPN 엔드포인트와 연결합니다.에 설명된 단계를 수행하고 VPC 및 서브넷을 선택합니다.
3. 라우팅 테이블의 로컬 네트워크에 대한 경로를 추가합니다. 이렇게 하려면 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 Client VPN 엔드포인트에 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 Client VPN 엔드포인트에 권한 부여 규칙 추가에 설명된 단계를 수행합니다. 활성화할 대상 네트워크(Destination network to enable)에 클라이언트 CIDR 범위를 입력합니다.

AWS Client VPN을 사용한 네트워크 액세스 제한

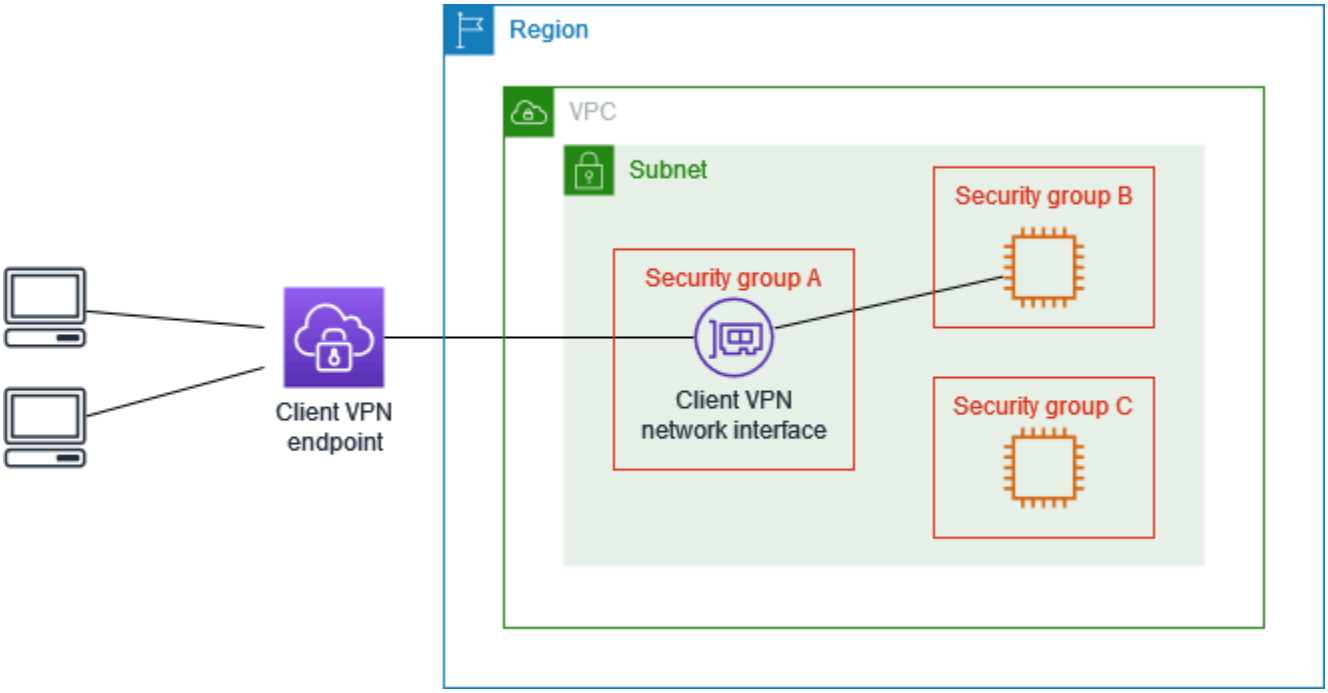
VPC의 특정 리소스에 대한 액세스를 제한하도록 Client VPN 엔드포인트를 구성할 수 있습니다. 사용자 기반 인증의 경우 Client VPN 엔드포인트에 액세스하는 사용자 그룹을 기반으로 네트워크 일부에 대한 액세스를 제한할 수도 있습니다.

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 AWS 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 보안 그룹(Security Groups)을 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 보안 그룹(Security Groups)을 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. AWS Directory Service 또는 IdP에서 사용자 및 그룹을 구성합니다. 자세한 정보는 다음 주제를 참조하세요.
   - 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 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 특

정 부분에 액세스할 수 있도록 하려면 여러 Client VPN 엔드포인트를 생성할 수 있습니다. 예를 들어, 네트워크에 액세스하는 각 사용자 그룹에 대해 다음을 수행합니다.

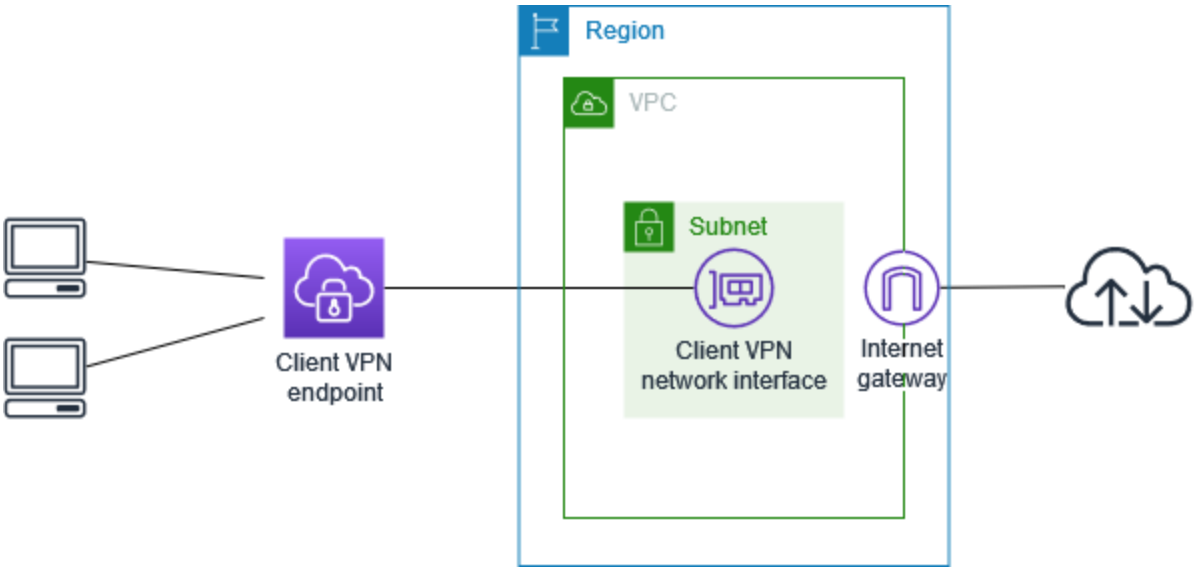
1. 해당 사용자 그룹에 대한 서버 및 클라이언트 인증서 및 키 집합을 생성합니다. 자세한 내용은 상호 인증 단원을 참조하세요.
2. Client VPN 엔드포인트를 생성합니다. 자세한 내용은 Client VPN 엔드포인트를 생성합니다. 단원을 참조하세요.
3. 네트워크의 전체 또는 일부에 대한 액세스 권한을 부여하는 권한 부여 규칙을 생성합니다. 예를 들어, 관리자가 사용하는 Client VPN 엔드포인트의 경우 전체 네트워크에 대한 액세스 권한을 부여하는 권한 부여 규칙을 생성할 수 있습니다. 자세한 내용은 Client VPN 엔드포인트에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

AWS Client VPN 시작하기

이 자습서에서는 다음을 수행하는 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

- 사전 조건
- 1단계: 서버와 클라이언트 인증서 및 키 생성
- 2단계: 클라이언트 VPN 엔드포인트 생성
- 3단계: 대상 네트워크 연결
- 4단계: VPC에 대한 권한 부여 규칙 추가
- 5단계: 인터넷 액세스 제공
- 6단계: 보안 그룹 요구 사항 확인
- 7단계: Client VPN 엔드포인트 구성 파일 다운로드
- 8단계: 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: 서버와 클라이언트 인증서 및 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 상호 인증 단원을 참조하세요.

> **Note**
>
> 서버 인증서는 Client VPN 엔드포인트를 생성할 AWS 리전에서 프로비저닝하거나 AWS Certificate Manager(ACM)로 가져와야 합니다.

2단계: 클라이언트 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 여세요.
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 ARN(Server certificate ARN)에서 1단계에서 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. 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 Client VPN 엔드포인트를 생성합니다. 섹션을 참조하세요.

3단계: 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 여세요.

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.

4단계: 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 여세요.
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.

5단계: 인터넷 액세스 제공

AWS 서비스, 피어링된 VPC, 온프레미스 네트워크, 인터넷 등 VPC에 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 여세요.
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.

6단계: 보안 그룹 요구 사항 확인

이 자습서에서는 2단계에서 Client VPN 엔드포인트를 생성하는 동안 보안 그룹을 지정하지 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 설명은 보안 그룹 섹션을 참조하세요.

7단계: 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 여세요.
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. 1단계에서 생성된 클라이언트 인증서 및 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 클라이언트 구성 파일 내보내기 및 구성 단원을 참조하십시오.

8단계: Client VPN 엔드포인트에 연결

AWS 제공 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 참조하세요.

AWS Client VPN 작업

다음 항목에서는 Client VPN을 사용하는 방법을 설명합니다.

목차

셀프 서비스 포털 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 AWS CLI를 사용하여 내보내는 구성 파일과 동일합니다. 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

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 Active Directory 그룹에 대한 권한 부여 규칙이 예상대로 작동하지 않습니다. 및 경로 우선 순위를 참조하십시오.

목차

Client VPN 엔드포인트에 권한 부여 규칙 추가

AWS Management Console을 사용하여 Client VPN 엔드포인트에 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 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.

Client VPN 엔드포인트에서 권한 부여 규칙 제거

권한 부여 규칙을 제거하여 지정된 네트워크에 에 대한 액세스 권한을 제거합니다.

콘솔 또는 AWS CLI를 사용하여 Client VPN 엔드포인트에서 권한 부여 규칙을 제거할 수 있습니다.

Client VPN 엔드포인트에서 권한 부여 규칙을 제거하는 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 규칙이 추가된 Client VPN 엔드포인트를 선택하고 권한 부여 규칙(Authorization rules)을 선택합니다.
4. 삭제할 권한 부여 규칙을 선택한 다음 권한 부여 규칙 제거(Remove authorization rule), 권한 부여 규칙 제거((Remove authorization rule)를 차례로 선택합니다.

Client VPN 엔드포인트에서 권한 부여 규칙을 제거하려면(AWS CLI)

revoke-client-vpn-ingress 명령을 사용합니다.

권한 부여 규칙 보기

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

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.

권한 부여 규칙에 대한 예제 시나리오

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

목차

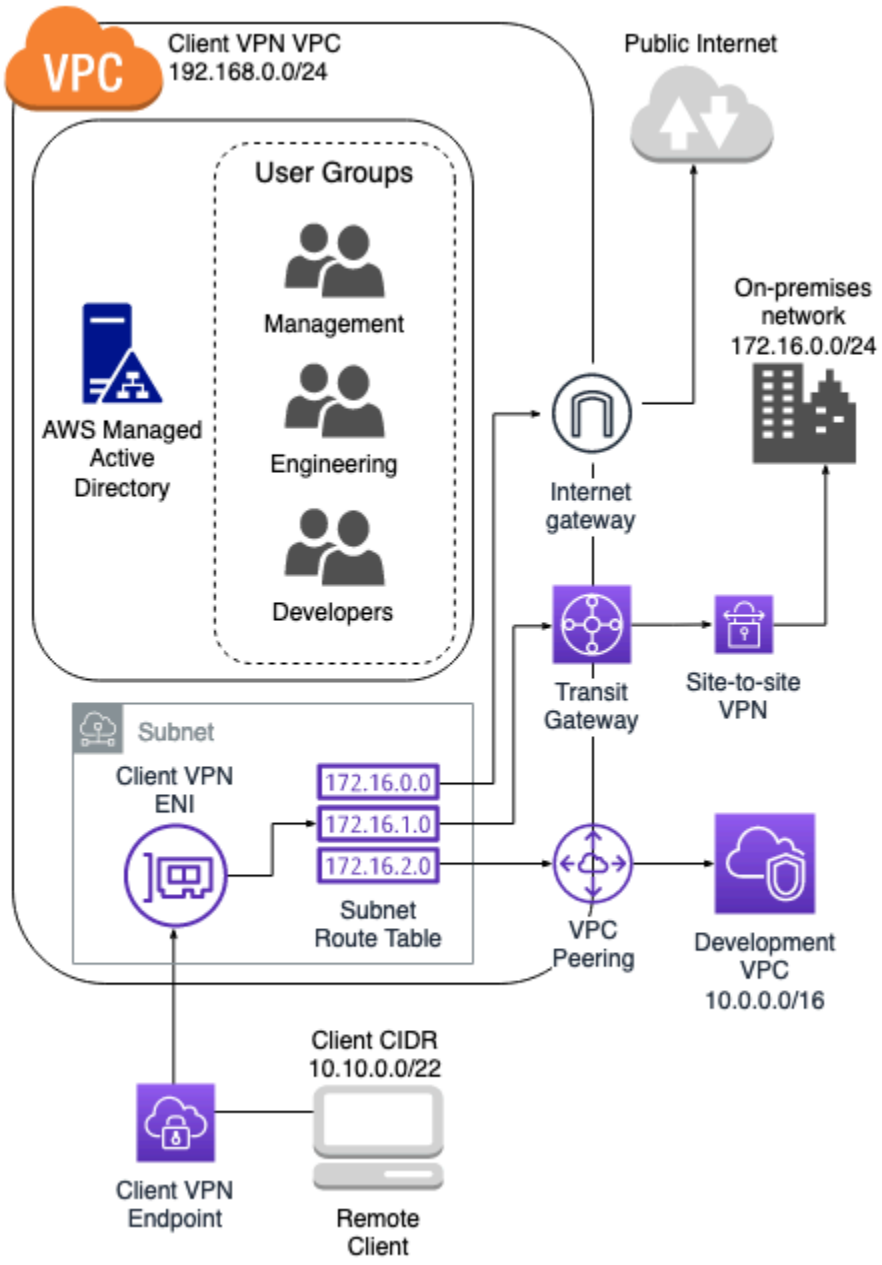
권한 부여 규칙을 이해하기 위한 중요 사항

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.

권한 부여 규칙 시나리오의 아키텍처 예

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



시나리오 1: 단일 대상에 대한 액세스

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

규칙 설명	그룹 ID입니다.	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 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.

시나리오 2: 모든 대상(0.0.0.0/0) CIDR 사용

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

규칙 설명	그룹 ID입니다.	모든 사용자에게 액세스 허용	대상 CIDR
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

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.

시나리오 3: 더 긴 IP 접두사 일치

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

규칙 설명	그룹 ID입니다.	모든 사용자에게 액세스 허용	대상 CIDR
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	10.0.1.66/32

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.

시나리오 4: 겹치는 CIDR(동일한 그룹)

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

규칙 설명	그룹 ID입니다.	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	10.0.1.66/32
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.

시나리오 5: 추가 0.0.0.0/0 규칙

규칙 설명	그룹 ID입니다.	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	10.0.1.66/32
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 `10.0.2.119/32`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 172.16.0.128/25를 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.

시나리오 6: 192.168.0.0/24에 대한 규칙 추가

규칙 설명	그룹 ID입니다.	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	10.0.1.66/32
엔지니어링 그룹에 온프레미스 네트워크의	S-xxxxx14	False	172.16.0.128/25

규칙 설명	그룹 ID입니다.	모든 사용자에게 액세스 허용	대상 CIDR
서브넷에 대한 액세스 제공			
엔지니어링 그룹에 모든 대상에 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

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.

시나리오 7: 모든 사용자 그룹의 액세스

규칙 설명	그룹 ID입니다.	모든 사용자에게 액세스 허용	대상 CIDR

규칙 설명	그룹 ID입니다.	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	10.0.1.66/32
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 10.0.2.119/32를 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 퍼블릭 인터넷, 172.16.0.0/24 및 172.16.0.128/25에 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.

클라이언트 인증서 해지 목록

클라이언트 인증서 해지 목록을 사용하여 특정 클라이언트 인증서의 Client VPN 엔드포인트에 대한 액세스를 취소할 수 있습니다.

> **Note**
>
> 서버와 클라이언트 인증서 및 키 생성에 대한 자세한 내용은 상호 인증 단원을 참조하십시오.

클라이언트 인증서 해지 목록에 추가할 수 있는 항목 수에 대한 자세한 내용은 Client VPN 할당량 단원을 참조하십시오.

목차

클라이언트 인증서 해지 목록 생성

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
```

프롬프트가 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 셸을 시작합니다.

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

3. EasyRSA 셸에서 클라이언트 인증서를 해지합니다.

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

4. 프롬프트가 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
```

클라이언트 인증서 해지 목록 가져오기

가져올 클라이언트 인증서 해지 목록 파일이 있어야 합니다. 클라이언트 인증서 해지 목록 생성에 대한 자세한 내용은 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
```

클라이언트 인증서 해지 목록 내보내기

콘솔 및 AWS CLI를 사용하여 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.

클라이언트 연결

연결은 클라이언트에 의해 설정된 VPN 세션입니다. 클라이언트가 성공적으로 Client VPN 엔드포인트에 연결하면 연결이 설정됩니다.

목차

클라이언트 연결 보기

콘솔 및 AWS CLI를 사용하여 클라이언트 연결을 볼 수 있습니다. 연결 정보에는 클라이언트 CIDR 범위에서 할당된 IP 주소가 포함됩니다.

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.

클라이언트 연결을 보려면(AWS CLI)

describe-client-vpn-connections 명령을 사용합니다.

클라이언트 연결 종료

클라이언트 연결을 종료하면 VPN 세션이 끝납니다.

콘솔 및 AWS CLI를 사용하여 클라이언트 연결을 종료할 수 있습니다.

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 연결(Connections)을 선택합니다.
4. 종료할 연결을 선택하고 Terminate Connection(연결 종료), Terminate Connection(연결 종료)을 선택합니다.

클라이언트 연결을 종료하려면(AWS CLI)

terminate-client-vpn-connections 명령을 사용합니다.

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.

클라이언트 데스크톱 애플리케이션에 대한 자세한 내용은 AWS Client VPN사용 설명서의 AWS 제공 클라이언트에 대한 릴리스 정보를 참조하세요.

목차

Client VPN 엔드포인트 생성 중 클라이언트 로그인 배너 구성

Client VPN 엔드포인트 생성 중에 클라이언트 로그인 배너를 활성화하는 자세한 단계는 Client VPN 엔드포인트를 생성합니다. 단원을 참조하세요.

기존 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 텍스트(Client login banner text)에 VPN 세션이 설정될 때 AWS 제공 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 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.

Client VPN 엔드포인트의 기존 배너 텍스트 수정

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 텍스트(Client login banner text)에서 기존 텍스트를 VPN 세션이 설정될 때 AWS 제공 클라이언트의 배너에 표시될 새 텍스트로 대체합니다. 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 로그인 배너 보기

현재 구성된 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.

Client VPN 엔드포인트

모든 클라이언트 VPN 세션은 Client VPN 엔드포인트에서 종료됩니다. Client VPN 엔드포인트를 구성하여 모든 클라이언트 VPN 세션을 관리하고 제어합니다.

내용

- Client VPN 엔드포인트를 생성합니다.
- Client VPN 엔드포인트를 수정합니다.
- Client VPN Endpoint 보기
- Client VPN 엔드포인트를 삭제합니다.

Client VPN 엔드포인트를 생성합니다.

클라이언트가 VPN 세션을 설정할 수 있도록 하려면 Client VPN 엔드포인트를 생성합니다.

Client VPN은 의도한 대상 네트워크가 프로비저닝되는 AWS 계정과 동일한 계정에서 생성되어야 합니다.

사전 조건

시작하기 전에 다음이 있는지 확인하십시오.

- 의 규칙 및 모범 사례 AWS Client VPN에서 규칙 및 제한 사항을 검토합니다.
- 서버 인증서를 생성하고, 필요한 경우 클라이언트 인증서를 생성합니다. 자세한 설명은 클라이언트 인증 섹션을 참조하세요.

Client VPN 엔드포인트를 생성하려면(콘솔)

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 여세요.
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) Client VPN 엔드포인트의 이름 태그와 설명을 입력합니다.
4. 클라이언트 IPv4 CIDR에서 클라이언트 IP 주소를 할당할 IP 주소 범위(CIDR 표기법)를 지정합니다. 예: `10.0.0.0/22`.

   > **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. 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.

6. 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 사용(Use mutual authentication)]을 선택한 다음, [클라이언트 인증서 ARN(Client certificate ARN)]에 AWS Certificate Manager(ACM)에서 프로비저닝되는 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.

7. (선택 사항) 연결 로깅의 경우 Amazon Logs를 사용하여 클라이언트 연결에 대한 데이터를 CloudWatch 기록할지 여부를 지정합니다. 클라이언트 연결에 대한 로그 세부 정보 활성화(Enable log details on client connections)를 켭니다. CloudWatch 로그 로그 그룹 이름에는 사용할 로그 그룹 이름을 입력합니다. 로그 CloudWatch 로그 스트림 이름에는 사용할 로그 스트림의 이름을 입력하거나 이 옵션을 비워 두면 로그 스트림을 자동으로 생성할 수 있습니다.
8. (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 처리

기 ARN)에서 연결을 허용하거나 거부하는 논리가 포함된 Lambda 함수의 Amazon 리소스 이름(ARN)을 지정합니다.

9. (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.

10. (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.

11. (선택 사항) 엔드포인트를 분할 터널 Client VPN 엔드포인트로 사용하려면 분할 터널 활성화(Enable split-tunnel)를 켭니다. 기본적으로 Client VPN 엔드포인트의 분할 터널은 비활성화됩니다.
12. (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.
13. (선택 사항) VPN 포트의 경우 VPN 포트 번호를 선택합니다. 기본값은 443입니다.
14. (선택 사항) 클라이언트에 대한 셀프 서비스 포털 URL을 생성하려면 셀프 서비스 포털 활성화(Enable self-service portal)를 켭니다.
15. (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.
16. (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.
17. 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.
- AWS 제공 클라이언트 또는 다른 OpenVPN 기반 클라이언트 애플리케이션을 사용하여 Client VPN 엔드포인트에 연결하도록 클라이언트에 지시합니다. 자세한 내용은 AWS Client VPN 사용 설명서를 참조하세요.

Client VPN 엔드포인트(AWS CLI)를 생성하려면

create-client-vpn-endpoint 명령을 사용합니다.

Client VPN 엔드포인트를 수정합니다.

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
- 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

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

Client VPN 엔드포인트를 수정하려면(콘솔)

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

6. Amazon Logs를 사용하여 클라이언트 연결에 대한 데이터를 CloudWatch 기록할지 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. CloudWatch로그 로그 그룹 이름에서 사용할 로그 그룹 이름을 선택합니다. 로그 CloudWatch 로그 스트림 이름에서 사용할 로그 스트림의 이름을 선택하거나 이 옵션을 비워 두면 로그 스트림을 자동으로 생성할 수 있습니다.
   - 클라이언트 연결 로깅을 비활성화하려면 클라이언트 연결에 대한 로그 세부 정보 활성화(Enable log details on client connections)를 끕니다.

7. 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.

8. DNS 서버 활성화(Enable DNS servers)를 켜거나 끕니다. 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.

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

10. 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.

11. VPN 포트의 경우 VPN 포트 번호를 선택합니다. 기본값은 443입니다.

12. 클라이언트에 대한 셀프 서비스 포털 URL을 생성하려면 셀프 서비스 포털 활성화(Enable self-service portal)를 켭니다.

13. 세션 제한 시간(Session timeout hours)에서 사용 가능한 옵션에서 원하는 최대 VPN 세션 기간(시간)을 선택하거나 기본값 24시간으로 설정된 상태로 둡니다.

14. 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.

15. 클라이언트 VPN 엔드포인트 수정(Modify Client VPN endpoint)을 선택합니다.

Client VPN 엔드포인트를 수정하려면(AWS CLI)

modify-client-vpn-endpoint 명령을 사용합니다.

Client VPN Endpoint 보기

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 여세요.
2. 탐색 창에서 Client VPN 엔드포인트(Client VPN Endpoints)를 선택합니다.
3. 보려는 Client VPN 엔드포인트를 선택합니다.
4. 세부 정보(Details), 대상 네트워크 연결(Target network associations), 보안 그룹(Security groups), 권한 부여 규칙(Authorization rules), 라우팅 테이블(Route table), 연결(Connections) 및 태그(Tags) 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.

Client VPN 엔드포인트를 삭제합니다.

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 AWS CLI를 사용하여 Client VPN 엔드포인트를 삭제할 수 있습니다.

Client VPN 엔드포인트를 삭제하려면(콘솔)

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

연결 로그 작업

새 Client VPN 엔드포인트 또는 기존 Client VPN 엔드포인트에 연결 로깅을 활성화하고 연결 로그 캡처를 시작할 수 있습니다.

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

연결 로깅을 활성화하면 로그 그룹에서 로그 스트림의 이름을 지정할 수 있습니다. 로그 스트림을 지정하지 않으면 Client VPN 서비스에서 자동으로 로그 스트림을 생성합니다.

새 Client VPN 엔드포인트에 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 Client VPN 엔드포인트를 생성합니다. 섹션을 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.

AWS CLI를 사용하여 새 Client VPN 엔드포인트에 연결 로깅을 활성화하려면

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 Client VPN 엔드포인트에 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.

AWS CLI를 사용하여 기존 Client VPN 엔드포인트에 연결 로깅을 활성화하려면

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"
```

```
}
```

연결 로그 보기

CloudWatch Logs 콘솔을 사용하여 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.

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.

클라이언트 구성 파일 내보내기 및 구성

Client VPN 엔드포인트 구성 파일은 클라이언트(사용자)가 Client VPN 엔드포인트와 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 설명은 셀프 서비스 포털 액세스 섹션을 참조하세요.

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 와일드카드 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.

클라이언트 구성 파일 내보내기

콘솔 또는 AWS CLI를 사용하여 클라이언트 구성을 내보낼 수 있습니다.

클라이언트 구성을 내보내는 방법(콘솔)

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

클라이언트 인증서 및 키 정보 추가(상호 인증)

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
```

경로

각 Client VPN 엔드포인트에는 사용 가능한 대상 네트워크 라우팅을 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 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.

목차

Client VPN 엔드포인트의 분할 터널 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.

엔드포인트 라우팅 생성

라우팅을 생성할 때 대상 네트워크의 트래픽이 어떻게 전달될지 지정합니다.

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

콘솔과 AWS CLI를 사용하여 Client VPN 엔드포인트에 경로를 추가할 수 있습니다.

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.

엔드포인트 라우팅 보기

콘솔 또는 AWS CLI를 사용하여 특정 Client VPN 엔드포인트의 경로를 볼 수 있습니다.

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.

엔드포인트 라우팅 삭제

수동으로 추가한 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 AWS CLI를 사용하여 Client VPN 엔드포인트에서 경로를 삭제할 수 있습니다.

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.

대상 네트워크

대상 네트워크는 VPC 안의 서브넷입니다. 클라이언트가 연결하여 VPN 연결을 설정할 수 있도록 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 AWS Client VPN의 시나리오 및 예제 단원을 참조하십시오.

목차

대상 네트워크를 Client VPN 엔드포인트와 연결합니다.

하나 이상의 대상 네트워크(서브넷)를 Client VPN 엔드포인트와 연결할 수 있습니다.

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 Client VPN 엔드포인트를 수정합니다. 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.

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.

대상 네트워크에 보안 그룹 적용

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 섹션을 참조하세요.

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

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.

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.

대상 네트워크 보기

콘솔 또는 AWS CLI를 사용하여 Client VPN 엔드포인트에 연결된 대상을 볼 수 있습니다.

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.

AWS CLI를 사용하여 대상 네트워크를 보려면

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

VPN 세션 최대 기간

AWS Client VPN에서는 최대 VPN 세션 기간에 대한 몇 가지 옵션을 제공합니다. 보안 및 규정 준수 요구 사항을 충족하도록 더 짧은 최대 VPN 세션 기간을 구성할 수 있습니다. 기본적으로 최대 VPN 세션 기간은 24시간입니다.

> **Note**
>
> 최대 VPN 세션 기간 값이 감소하면 새 제한 시간 값보다 오래된 활성 VPN 세션의 연결이 끊어집니다.

클라이언트 데스크톱 애플리케이션에 대한 자세한 내용은 AWS Client VPN사용 설명서의 AWS 제공 클라이언트에 대한 릴리스 정보를 참조하세요.

목차

Client VPN 엔드포인트 생성 중 최대 VPN 세션 구성

Client VPN 엔드포인트 생성 중에 최대 VPN 세션을 구성하는 자세한 단계는 Client VPN 엔드포인트를 생성합니다. 단원을 참조하세요.

현재 최대 VPN 세션 기간 보기

현재 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(Session timeout hours) 옆에 있는 현재 최대 VPN 세션 기간을 봅니다.

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

describe-client-vpn-endpoints 명령을 사용합니다.

최대 VPN 세션 기간 수정

현재 최대 VPN 세션 기간을 수정하려면 다음 단계를 사용합니다.

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. 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.

AWS Client VPN의 보안

AWS에서 클라우드 보안을 가장 중요하게 생각합니다. AWS 고객은 보안에 가장 보안에 민감한 조직의 요구 사항에 부합하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

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

- 클라우드의 보안 - AWS는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호합니다. AWS는 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 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 서비스 를 참조하세요.
- 클라우드 내 보안 – 귀하의 책임은 귀하가 사용하는 AWS 서비스에 의해 결정됩니다. 또한 귀하는 데이터의 민감도, 회사 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.

목차

AWS Client VPN의 데이터 보호

AWS Shared Responsibility Model은 AWS Client VPN의 데이터 보호에 적용됩니다. 이 모델에서 설명하는 것처럼 AWS은(는) 모든 AWS 클라우드를 실행하는 글로벌 인프라를 보호할 책임이 있습니다.

이 인프라에서 호스팅되는 콘텐츠에 대한 제어를 유지하는 것은 사용자의 책임입니다. 또한 사용하는 AWS 서비스의 보안 구성과 관리 작업은 사용자의 책임입니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하십시오. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하십시오.

데이터를 보호하려면 AWS 계정보안 인증 정보를 보호하고 AWS IAM Identity Center또는 AWS Identity and Access Management(IAM)를 통해 개별 사용자 계정을 설정하는 것이 좋습니다. 이러한 방식에는 각 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- AWS CloudTrail(으)로 API 및 사용자 활동 로깅을 설정합니다.
- AWS 암호화 솔루션을 AWS 서비스내의 모든 기본 보안 컨트롤과 함께 사용합니다.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용합니다.
- 명령줄 인터페이스 또는 API를 통해 AWS에 액세스할 때 FIPS 140-2 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 FIPS(Federal Information Processing Standard) 140-2를 참조하십시오.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 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 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 보안 인증 정보를 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 보호

인터네트워크 액세스 활성화

클라이언트가 Client VPN 엔드포인트를 통해 VPC 및 기타 네트워크에 연결하도록 할 수 있습니다. 자세한 정보와 지침은 AWS 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 AWS 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)

AWS Client VPN의 ID 및 액세스 관리

AWS Identity and Access Management (IAM) 은 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 도와줍니다. IAM 관리자는 누가 Client VPN 리소스를 사용하도록 인증되고(로그인됨) 권한이 부여되는지(권한 있음)를 제어합니다. IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

주제

- 고객
- ID를 통한 인증
- 정책을 사용한 액세스 관리
- AWS 클라이언트 VPN이 IAM과 작동하는 방식
- Client VPN의 ID 기반 정책 예제 AWS
- AWS Client VPN ID 및 액세스 문제 해결
- Client VPN에 서비스 연결 역할 사용

고객

사용 방법 AWS Identity and Access Management (IAM) 은 Client VPN에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 - Client VPN 서비스를 사용하여 작업을 수행하는 경우 필요한 보안 인증 정보와 권한을 관리자가 제공합니다. 더 많은 Client VPN 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. Client VPN의 기능에 액세스할 수 없는 경우 AWS Client VPN ID 및 액세스 문제 해결 섹션을 참조하세요.

서비스 관리자 - 회사에서 Client VPN 리소스를 책임지고 있는 경우 Client VPN에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 Client VPN 기능과 리소스를 결정합니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하십시오. 회사가 Client VPN에서 IAM을 사용하는 방법에 대해 자세히 알아보려면 AWS 클라이언트 VPN이 IAM과 작동하는 방식 섹션을 참조하세요.

IAM 관리자 - IAM 관리자라면 Client VPN에 대한 액세스 권한 관리 정책 작성 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 Client VPN 자격 증명 기반 정책 예제를 보려면 Client VPN의 ID 기반 정책 예제 AWS 섹션을 참조하세요.

ID를 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자로 인증 (로그인 AWS) 하거나 IAM 역할을 맡아 인증 (로그인) 해야 합니다. AWS 계정 루트 사용자

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 페더레이션 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트 (SDK) 와 명령줄 인터페이스 (CLI) 를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하십시오.

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 태스크를 수행하는 데 사용하세요. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하십시오.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 AWS 서비스 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 액세스하도록 하는 것입니다.

페더레이션 ID는 기업 사용자 디렉토리, 웹 ID 공급자, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 액세스하는 AWS 서비스 모든 사용자를 말합니다. AWS Directory Service페더레이션 ID에 AWS 계정액세스하면 이들이 역할을 맡고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center(을)를 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여 모든 사용자 및 애플리케이션에서 사용할 수 있습니다. AWS 계정 IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇입니까?를 참조하십시오.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한을 AWS 계정 가진 사용자 내 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 보안 인증이 있는 IAM 사용자를 생성하는 대신 임시 보안 인증을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 보안 인증이 필요한 특정 사용 사례가 있는 경우, 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우 정기적으로 액세스 키 교체를 참조하십시오.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용

자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님)를 참조하십시오.

IAM 역할

IAM 역할은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM 역할 사용을 참조하십시오.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 서드 파티 ID 공급자의 역할 생성 단원을 참조하십시오. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관짓습니다. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하십시오.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 태스크에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 계정 간 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하십시오.
- 서비스 간 액세스 — 일부는 다른 기능을 사용합니다. AWS 서비스 AWS 서비스예를 들어 서비스에서 직접적 호출을 수행하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 태스크를 수행할 수 있습니다.
  - 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을

수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

- 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하십시오.
- 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

- Amazon EC2에서 실행되는 애플리케이션 — IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 API 요청을 AWS CLI 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하십시오.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조하십시오.

정책을 사용한 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요를 참조하십시오.

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.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

보안 인증 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하십시오.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 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 태스크를 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

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

액세스 제어 목록(ACL)

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

ACL을 지원하는 서비스의 예로는 아마존 S3와 아마존 VPC가 있습니다. AWS WAF ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 가이드의 ACL(액세스 제어 목록) 개요를 참조하십시오.

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 타입에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 자격 증명 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 개체의 보안 인증 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 IAM 사용 설명서의 IAM 엔터티에 대한 권한 경계를 참조하십시오.
- 서비스 제어 정책 (SCP) - SCP는 조직 또는 조직 단위 (OU) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations AWS Organizations 사업체가 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각 항목을 포함하여 구성원 계정의 엔티티에 대한 권한을 제한합니다. AWS 계정 루트 사용자조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서의 SCP 작동 방식을 참조하십시오.
- 세션 정책 - 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 보안 인증 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하십시오.

여러 정책 타입

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

AWS 클라이언트 VPN이 IAM과 작동하는 방식

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
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	예
ACLs	아니요
ABAC(정책 내 태그)	아니요
임시 보안 인증	예
보안 주체 권한	예
서비스 역할	예
서비스 연결 역할	예

Client VPN 및 기타 AWS 서비스가 대부분의 IAM 기능과 어떻게 작동하는지 자세히 알아보려면 IAM 사용 설명서의 IAM과 함께 작동하는AWS 서비스를 참조하십시오.

Client VPN에 대한 자격 증명 기반 정책

보안 인증 기반 정책 지원	예

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 보안 인증 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하십시오.

Client VPN 자격 증명 기반 정책 예제

Client VPN 자격 증명 기반 정책의 예를 보려면 Client VPN의 ID 기반 정책 예제 AWS 섹션을 참조하세요.

Client VPN 내 리소스 기반 정책

리소스 기반 정책 지원	아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예는 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 태스크를 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 보안 주체와 리소스가 다른 AWS 계정경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 개체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하십시오.

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 태스크를 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

클라이언트 VPN 작업 목록을 보려면 서비스 권한 부여 참조의 AWS Client VPN에서 정의한 작업을 참조하십시오.

Client VPN의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
ec2
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

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

Client VPN 자격 증명 기반 정책의 예를 보려면 Client VPN의 ID 기반 정책 예제 AWS 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 개체를 지정합니다. 문장에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 태스크를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

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

클라이언트 VPN 리소스 유형 및 해당 ARN 목록을 보려면 서비스 권한 부여 참조의 AWS Client VPN에서 정의한 리소스를 참조하십시오. 각 리소스의 ARN을 지정할 수 있는 작업에 대해 알아보려면 AWS Client VPN에서 정의한 작업을 참조하십시오.

Client VPN 자격 증명 기반 정책의 예를 보려면 Client VPN의 ID 기반 정책 예제 AWS 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` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 `AND` 태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 `OR` 연산을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예컨대, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하십시오.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

클라이언트 VPN 조건 키 목록을 보려면 서비스 권한 부여 참조의 AWS 클라이언트 VPN의 조건 키를 참조하십시오. 조건 키를 사용할 수 있는 작업 및 리소스를 알아보려면 AWS Client VPN에서 정의한 작업을 참조하십시오.

Client VPN 자격 증명 기반 정책의 예를 보려면 Client VPN의 ID 기반 정책 예제 AWS 섹션을 참조하세요.

Client VPN의 ACL

ACL 지원	아니요

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

Client VPN의 ABAC

ABAC 지원(정책의 태그)	아니요

ABAC(속성 기반 액세스 통제)는 속성에 근거하여 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 개체 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

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 정보는 IAM 사용 설명서의 ABAC란 무엇입니까?를 참조하십시오. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하십시오.

Client VPN에서 임시 보안 인증 정보 사용

임시 보안 인증 지원	예

임시 자격 증명을 사용하여 로그인하면 작동하지 AWS 서비스 않는 것도 있습니다. 임시 자격 증명을 사용하는 방법을 AWS 서비스 비롯한 추가 정보는 IAM 사용 설명서의 IAM과AWS 서비스 연동되는 내용을 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하십시오.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 자격 증명 섹션을 참조하십시오.

Client VPN의 서비스 간 보안 주체 권한

전달 액세스 세션(FAS) 지원	예

IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하라는 요청과 결합하여 사용합니다. AWS 서비스 FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. 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 서비스에 대한 권한을 위임할 역할 생성을 참조하십시오.

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 Client VPN 기능이 중단될 수 있습니다. Client VPN에서 관련 지침을 제공하는 경우에만 서비스 역할을 편집하세요.

Client VPN의 서비스 연결 역할

서비스 링크 역할 지원	예

서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하십시오. 서비스 연결 역할 열에서 Yes(이)가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 Yes(네) 링크를 선택합니다.

Client VPN의 ID 기반 정책 예제 AWS

기본적으로 사용자 및 역할은 Client VPN 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS API를 사용하여 작업을 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

각 리소스 유형의 ARN 형식을 포함하여 Client VPN에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 AWS Client VPN의 작업, 리소스 및 조건 키를 참조하십시오.

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 따릅니다.

- AWS 관리형 정책으로 시작하고 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 해당 내용은 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책 또는 직무에 대한AWS 관리형 정책을 참조하십시오.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 태스크를 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 설명서의 IAM의 정책 및 권한을 참조하십시오.
- 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. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하십시오.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 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 Analyzer 정책 검증을 참조하십시오.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA 보호 API 액세스 구성을 참조하십시오.

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

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 API를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함됩니다. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
```

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

AWS Client VPN ID 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
- 저는 IAM을 수행할 권한이 없습니다. PassRole
- 외부 사용자가 내 Client VPN AWS 계정 리소스에 액세스할 수 있도록 허용하고 싶습니다.

Client VPN에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 수신되면, 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예제 오류는 mateojacksonIAM 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 mateojackson사용자 정책을 업데이트해야 합니다.

도움이 필요하면 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

저는 IAM을 수행할 권한이 없습니다. PassRole

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

일부 AWS 서비스 서비스에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 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 수 있는 권한을 가지고 있지 않습니다.

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

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

도움이 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 자격 증명을 제공한 사람입니다.

외부 사용자가 내 Client VPN AWS 계정 리소스에 액세스할 수 있도록 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.

자세히 알아보려면 다음을 참조하십시오.

- Client VPN에서 이러한 기능을 지원하는지 여부를 알아보려면 AWS 클라이언트 VPN이 IAM과 작동하는 방식 섹션을 참조하세요.
- 소유한 리소스에 대한 액세스를 제공하는 방법을 알아보려면 IAM 사용 설명서의 다른 AWS 계정 IAM 사용자에게 액세스 권한 제공을 참조하십시오. AWS 계정
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정AWS 계정 소유에 대한 액세스 제공을 참조하십시오.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(자격 증명 페더레이션)을 참조하십시오.
- 교차 계정 액세스에 대한 역할 사용과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하십시오.

Client VPN에 서비스 연결 역할 사용

AWS Client VPN은 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 서비스에서 사용자 대신 다른 AWS 서비스를 호출하기 위해 필요한 모든 권한을 포함합니다.

주제

- Client VPN의 역할 사용
- 연결 권한 부여를 위한 역할 사용

Client VPN의 역할 사용

AWS Client VPN은 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 서비스에서 사용자 대신 다른 AWS 서비스를 호출하기 위해 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.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는 AWS 서비스를 참조하고 서비스 연결 역할(Service-linked roles) 열에 예(Yes)가 있는 서비스를 찾으세요. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예(Yes) 링크를 선택합니다.

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`

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

- 작업: `Resource: "*"`에 대한 `ec2:CreateNetworkInterface`
- 작업: `Resource: "*"`에 대한 `ec2:CreateNetworkInterfacePermission`
- 작업: `Resource: "*"`에 대한 `ec2:DescribeSecurityGroups`
- 작업: `Resource: "*"`에 대한 `ec2:DescribeVpcs`
- 작업: `Resource: "*"`에 대한 `ec2:DescribeSubnets`
- 작업: `Resource: "*"`에 대한 `ec2:DescribeInternetGateways`
- 작업: `Resource: "*"`에 대한 `ec2:ModifyNetworkInterfaceAttribute`
- 작업: `Resource: "*"`에 대한 `ec2:DeleteNetworkInterface`
- 작업: `Resource: "*"`에 대한 `ec2:DescribeAccountAttributes`
- 작업: `Resource: "*"`에 대한 `ds:AuthorizeApplication`
- 작업: `Resource: "*"`에 대한 `ds:DescribeDirectories`
- 작업: `Resource: "*"`에 대한 `ds:GetDirectoryLimits`
- 작업: `Resource: "*"`에 대한 `ds:UnauthorizeApplication`

- 작업: `Resource: "*"`에 대한 `logs:DescribeLogStreams`
- 작업: `Resource: "*"`에 대한 `logs:CreateLogStream`
- 작업: `Resource: "*"`에 대한 `logs:PutLogEvents`
- 작업: `Resource: "*"`에 대한 `logs:DescribeLogGroups`
- 작업: `Resource: "*"`에 대한 `acm:GetCertificate`
- 작업: `Resource: "*"`에 대한 `acm:DescribeCertificate`
- 작업: `Resource: "*"`에 대한 `iam:GetSAMLProvider`
- 작업: `Resource: "*"`에 대한 `lambda:GetFunctionConfiguration`

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

Client VPN의 서비스 연결 역할 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. AWS Management Console, AWS CLI 또는 AWS API를 사용하여 계정에서 첫 번째 Client VPN 엔드포인트를 만들 때 Client VPN은 자동으로 서비스 연결 역할을 생성합니다.

이 서비스 연결 역할을 삭제한 다음 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 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 삭제 섹션을 참조하세요.

Client VPN 서비스 연결 역할이 지원되는 리전

Client VPN에서는 서비스를 사용할 수 있는 모든 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용을 알아보려면 AWS service endpoints(서비스 엔드포인트)를 참조하세요.

연결 권한 부여를 위한 역할 사용

AWS Client VPN은 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 서비스에서 사용자 대신 다른 AWS 서비스를 호출하기 위해 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.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는 AWS 서비스를 참조하고 서비스 연결 역할(Service-linked roles) 열에 예(Yes)가 있는 서비스를 찾으세요. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예(Yes) 링크를 선택합니다.

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 연결 역할을 작성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

Client VPN의 서비스 연결 역할 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. AWS Management Console, AWS CLI 또는 AWS API를 사용하여 계정에서 첫 번째 Client VPN 엔드포인트를 만들 때 Client VPN은 자동으로 서비스 연결 역할을 생성합니다.

이 서비스 연결 역할을 삭제한 다음 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 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 삭제 섹션을 참조하세요.

Client VPN 서비스 연결 역할이 지원되는 리전

Client VPN에서는 서비스를 사용할 수 있는 모든 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용을 알아보려면 AWS service endpoints(서비스 엔드포인트)를 참조하세요.

AWS Client VPN의 복원성

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. AWS 리전에서는 물리적으로 분리되고 격리된 다수의 가용 영역을 제공하며 이러한 가용 영역은 짧은 지연 시간, 높은 처리량 및 높은 중복성을 갖춘 네트워크에 연결되어 있습니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로

장애 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.

AWS Client VPN의 인프라 보안

관리형 서비스인 AWS Client VPN은 AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스와 AWS의 인프라 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안에 대한 모범 사례를 사용하여 AWS 환경을 설계하려면 보안 원칙 AWS Well-Architected Framework의 인프라 보호를 참조하세요.

AWS에서 게시한 API 호출을 사용하여 네트워크를 통해 Client VPN에 액세스합니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(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.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 보안 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 자격 증명을 생성하여 요청에 서명할 수 있습니다.

AWS Client VPN의 보안 모범 사례

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.

모니터링 도구

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

ID 및 액세스 관리

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

AWS Client VPN에 대한 IPv6 고려 사항

현재 Client VPN 서비스는 VPN 터널을 통한 IPv6 트래픽 라우팅을 지원하지 않습니다. 그러나 IPv6 유출을 방지하기 위해 IPv6 트래픽을 VPN 터널로 라우팅해야 하는 경우가 있습니다. IPv6 유출은 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.

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 연

결되었을 때 퍼블릭 사이트에 액세스할 수 있는 경우 문제 해결을 추가로 수행해야 할 수도 있습니다. ipleak.org 같이 공개적으로 사용 가능한 도구를 사용하여 테스트할 수도 있습니다.

AWS Client VPN 모니터링

모니터링은 AWS Client VPN 및 기타 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 중요한 부분입니다. 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 임계값에 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. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

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 연결 로깅 및 Amazon CloudWatch Logs 사용 설명서를 참조하십시오.

AWS Client VPN의 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: 개수

지표	설명
AuthenticationFailures	Client VPN 엔드포인트에 대한 인증 실패 수입니다. 단위: 개수
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: 개수
IngressBytes	Client VPN 엔드포인트에서 수신된 바이트 수입니다. 단위: 바이트
IngressPackets	Client VPN 엔드포인트에서 수신된 패킷 수입니다. 단위: 개수
SelfServicePortalClientConfigurationDownloads	셀프 서비스 포털에서 Client VPN 엔드포인트 구성 파일의 다운로드 수입니다. 단위: 수

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

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 정보는 Amazon CloudWatch 사용 설명서를 참조하세요.

CloudWatch 지표 보기

Client VPN 엔드포인트에 대한 지표를 다음과 같이 볼 수 있습니다.

CloudWatch 콘솔을 사용하여 지표를 보려면

측정치는 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 지표(Metrics)를 선택합니다.
3. 전체 지표(All metrics)에서 Client VPN 지표 네임스페이스를 선택합니다.
4. 지표를 보려면 엔드포인트 기준 지표 측정 기준을 선택합니다.

AWS CLI를 사용하여 지표 보기

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

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

Client VPN에 대한 AWS CloudTrail 로그

AWS Client VPN는 Client VPN에서 사용자, 역할, AWS 서비스가 수행한 작업의 레코드를 제공하는 서비스인 AWS CloudTrail과 통합됩니다. CloudTrail은 Client VPN에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처된 호출에는 Client VPN 콘솔에서 수행된 호출과 Client VPN API 작업에 대한 코드 호출이 포함됩니다. 추적을 생성하면, Client VPN 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 전달할 수 있습니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기

록에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 Client VPN에 수행된 요청, 요청하는 IP 주소, 요청자, 요청 시기 및 추가 세부 정보를 확인합니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

CloudTrail의 Client VPN 정보

CloudTrail은 계정 생성 시 AWS 계정에서 사용되도록 설정됩니다. Client VPN에서 활동이 발생하면, 해당 활동은 이벤트 기록(Event history)에 있는 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

Client VPN의 이벤트를 포함하여 AWS 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 또는 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 받기 및 여러 계정에서 CloudTrail 로그 파일 받기

모든 Client VPN 작업은 CloudTrail에서 기록되며 Amazon EC2 API 참조에 설명되어 있습니다. 예를 들어 `CreateClientVpnEndpoint`, `AssociateClientVpnTargetNetwork` 및 `AuthorizeClientVpnIngress` 작업을 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 자격 증명 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트로 했는지 아니면 AWS Identity and Access Management(IAM) 사용자 자격 증명으로 했는지.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.

Client VPN 로그 파일 항목 이해

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 퍼블릭 API 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

자세한 내용은 Amazon EC2 API 참조의 AWS CloudTrail을 사용하여 Amazon EC2, Amazon EBS 및 Amazon VPC API 호출 로깅을 참조하세요.

AWS Client VPN 할당량

AWS 계정에는 Client VPN 엔드포인트와 관련된 다음과 같은 할당량 (이전에는 한도라고 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 참조하십시오.

Client VPN 할당량

이름	기본값	조정 가능
Client VPN 엔드포인트당 권한 부여 규칙	50	예
리전당 Client VPN 엔드포인트	5	예
Client VPN 엔드포인트당 클라이언트 동시 연결	이 값은 엔드포인트당 서브넷 연결 수에 따라 다릅니다. • 1 - 20,000명 • 2~36,500 • 3~66,500 • 4~96,500 • 5~126,000	예
Client VPN 엔드포인트당 동시 작업 †	10	아니요
Client VPN 엔드포인트용 클라이언트 인증서 해지 목록의 항목	20,000건	아니요
Client VPN 엔드포인트당 경로	10	예

† 작업에는 다음이 포함됩니다.

- 서브넷 연결 또는 연결 해제

- 루트 생성 또는 삭제
- 인바운드 및 아웃바운드 규칙 생성 또는 삭제
- 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 클라이언트 VPN 엔드포인트는 Active Directory 인증에 사용되는 AWS Directory Service 리소스와 동일한 계정에 속해야 합니다.
- SAML 기반 연동 인증을 사용하여 사용자를 인증하는 경우 Client VPN 엔드포인트는 IdP와 신뢰 관계를 정의하기 위해 생성한 IAM SAML ID 공급자와 동일한 계정에 속해야 합니다.AWS IAM SAML ID 공급자는 동일한 계정의 여러 Client VPN 엔드포인트에서 공유할 수 있습니다. AWS

AWS 클라이언트 VPN 문제 해결

다음 주제는 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

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 붙

이도록 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`

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)
- 경로

- 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.

Active Directory 그룹에 대한 권한 부여 규칙이 예상대로 작동하지 않습니다.

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: `10.1.0.0/16`에 액세스하는 그룹 1
- 규칙 2: `0.0.0.0/0`에 액세스하는 그룹 1
- 규칙 3: `0.0.0.0/0`에 액세스하는 그룹 2
- 규칙 4: `0.0.0.0/0`에 액세스하는 그룹 3
- 규칙 5: `172.131.0.0/16`에 액세스하는 그룹 2

이 예시에서는 규칙 2, 규칙 3과 규칙 4를 마지막으로 평가합니다. 그룹 1은 `10.1.0.0/16`에 대한 액세스 권한만 있고 그룹 2는 `172.131.0.0/16`에 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.

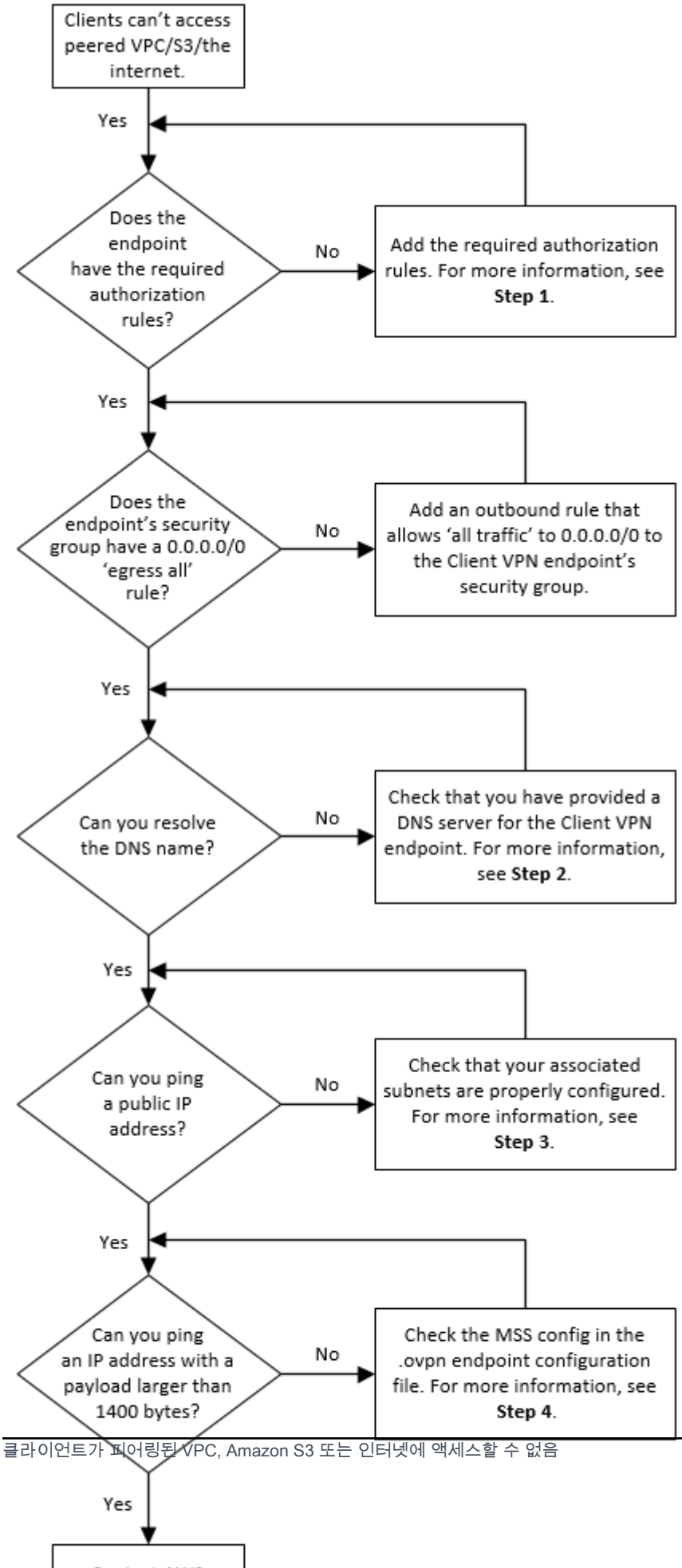
클라이언트가 피어링된 VPC, Amazon S3 또는 인터넷에 액세스할 수 없음

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
```

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`

클라이언트 소프트웨어가 TLS 오류를 반환함

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 설명은 클라이언트 인증서 해지 목록 섹션을 참조하세요.

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 상호 인증 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.

클라이언트 소프트웨어가 사용자 이름 및 암호 오류(Active Directory 인증)를 반환함

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 설명은 클라이언트 구성 파일 내보내기 및 구성 섹션을 참조하세요. Client VPN 엔드포인트를 사용하지 않고 Active Directory의 MFA 구성을 테스트하여 MFA가 예상대로 작동하는지 확인합니다.

클라이언트 소프트웨어에서 사용자 이름 및 암호 오류 (페더레이션 인증) 를 반환합니다.

문제

페더레이션 인증을 사용하여 사용자 이름과 암호로 로그인하려고 시도하면 “받은 자격 증명이 올바르지 않습니다.” 라는 오류 메시지가 나타납니다. IT 관리자에게 문의하십시오.”

원인

이 오류는 IdP의 SAML 응답에 속성이 하나 이상 포함되어 있지 않기 때문에 발생할 수 있습니다.

Solution

IdP의 SAML 응답에 속성이 하나 이상 포함되어 있는지 확인하십시오. 자세한 정보는 SAML 기반 IdP 구성 리소스을 참조하세요

클라이언트를 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 설명은 클라이언트 구성 파일 내보내기 및 구성 섹션을 참조하세요.

클라이언트에서 자격 증명이 최대 크기를 초과한다는 오류를 반환함(연동 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 설명은 SAML 기반 연동 인증에 대한 요구 사항 및 고려 사항 섹션을 참조하세요.

Solution

IdP에서 사용자가 속한 그룹 수를 줄이고 다시 연결해 보십시오.

클라이언트에서 브라우저가 열리지 않음(연동 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 연결해 보십시오.

클라이언트에서 사용 가능한 포트가 없다는 오류를 반환함(연동 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 설명은 SAML 기반 연동 인증에 대한 요구 사항 및 고려 사항 섹션을 참조하세요.

Solution

클라이언트의 디바이스가 TCP 포트 35001을 차단하거나 다른 프로세스에서 사용하고 있지 않은지 확인하십시오.

IP 불일치로 인해 VPN 연결이 종료되었습니다.

문제

VPN 연결이 종료되고 클라이언트 소프트웨어에서 다음 오류가 반환됩니다. `"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 설명은 의 규칙 및 모범 사례 AWS Client VPN 섹션을 참조하세요.

Solution

AWS 제공된 클라이언트와 Client VPN 엔드포인트 사이에 DNS 프록시가 없는지 확인합니다.

LAN으로의 트래픽 라우팅이 예상대로 작동하지 않음

문제

LAN IP 주소 범위가 다음 표준 사설 IP 주소 범위 (`10.0.0.0/8`, `172.16.0.0/12`192.168.0.0/16, 또는) 에 속하지 않는 경우 트래픽을 LAN (Local Area Network) 으로 라우팅하려고 시도하면 예상대로 작동하지 않습니다`169.254.0.0/16`.

원인

클라이언트 LAN 주소 범위가 위의 표준 범위를 벗어나는 것으로 감지되면 Client VPN 엔드포인트는 OpenVPN 지침 “리디렉션 게이트웨이 블록 로컬”을 자동으로 클라이언트에 푸시하여 모든 LAN 트래픽을 VPN으로 강제 전송합니다. 자세한 설명은 의 규칙 및 모범 사례 AWS Client VPN 섹션을 참조하세요.

Solution

VPN 연결 중에 LAN 액세스가 필요한 경우 위에 나열된 일반 LAN 주소 범위를 사용하는 것이 좋습니다.

Client VPN 엔드포인트에 대한 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. 또한 사용자 연결당 10Mbps 대역폭 제한이 있습니다.

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
```

Client VPN 사용 설명서에 대한 문서 기록

다음 표에서는 AWS Client VPN 관리자 안내서 업데이트를 설명합니다.

변경 사항	설명	날짜
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 릴리스	이 릴리스에서는 AWS Client VPN를 소개합니다.	2018년 12월 18일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.