CDO에서 가상 프라이빗 네트워크 관리

VPN(Virtual Private Network)은 인터넷과 같은 공용 네트워크를 통해 엔드포인트 간에 보안 터널을 설정합니다.

이 섹션은 ASA(Adaptive Security Appliance) 디바이스의 원격 액세스 및 사이트 투 사이트 VPN에 적용됩니다. 또한 ASA에서 VPN 연결을 배포하고 원격 액세스하는 데 사용되는 SSL 표준에 대해서도 설명합니다.

CDO에서는 다음과 같은 유형의 VPN 연결을 지원합니다.

사이트 간 가상 프라이빗 네트워크 소개

사이트간 VPN 터널은 다양한 위치에 있는 네트워크를 연결합니다. 관리형 디바이스 및 관리형 디바이스와 모든 관련 표준을 준수하는 다른 Cisco 또는 타사 피어 간에 Site-to-Site IPsec 연결을 만들 수 있습니다. 이러한 피어는 IPv4와 IPv6 주소를 사용하여 내부 주소와 외부 주소를 함께 포함할 수 있습니다 . Site-to-Site 터널은 IPsec(Internet Protocol Security) 프로토콜 제품군 및 인터넷 키 교환 버전 2(IKEv2)를 사용하여 구축됩니다. VPN 연결이 설정되면 로컬 게이트웨이의 뒤에 있는 호스트는 보안 VPN 터널을 통해 원격 게이트의 뒤에 있는 호스트와 연결할 수 있습니다.

VPN 토폴로지

새로운 사이트 간 VPN 토폴로지를 생성하려면 고유한 이름을 부여하거나 토폴로지 유형을 지정하거나 IPsec IKEv1 또는 IKEv2에 사용되는 IKE 버전 또는 둘 다 및 인증 방법을 선택해야 합니다. 구성된 후 토폴로지를 ASA에 구축합니다.

IPsec 및 **IKE** 프로토콜

CDO에서 사이트 간 VPN은 IKE 정책과 VPN 토폴로지에 할당된 IPsec 제안을 기반으로 구성됩니다. 정책 및 제안은 IPsec 터널에서 트래픽을 보호하는 데 사용되는 보안 프로토콜 및 알고리즘과 같은 사이트 간 VPN의 특성을 정의하는 파라미터 집합입니다. VPN 토폴로지에 할당할 수 있는 전체 구성 이미지를 정의하려면 몇 가지 정책 유형이 필요할 수 있습니다.

인증 **VPN** 터널

VPN 연결을 인증하려면 각 디바이스의 토폴로지에서 사전 공유 키를 구성합니다. 사전 공유 키를 사용하면 IKE 인증 단계에서 사용되는 보안 키를 두 피어 간에 공유할 수 있습니다.

VPN 암호화 도메인

VPN의 암호화 도메인은 경로 기반 또는 정책 기반 트래픽 선택기라는 두 가지 방법으로 정의할 수 있습니다.

- 정책 기반: 암호화 도메인은 IPSec 터널에 들어오는 모든 트래픽을 허용하도록 설정됩니다. IPSec 로컬 및 원격 트래픽 선택기는 0.0.0.0으로 설정됩니다. 즉, IPSec 터널로 라우팅되는 모든 트래픽은 소스/대상 서브넷에 관계없이 암호화됩니다. ASA는 암호화 맵을 사용하는 정책 기반 VPN을 지원합니다.
- 경로 기반: 암호화 도메인은 소스와 대상 모두에 대해 특정 IP 범위만 암호화하도록 설정됩니다. 이는 가상 IPsec 인터페이스를 생성하며, 해당 인터페이스에 들어오는 모든 트래픽은 암호화 및 암호 해독됩니다. ASA는 VTI(Virtual Tunnel Interface)를 사용하여 경로 기반 VPN을 지원합니다.

외부 디바이스 정보

비 시스코 또는 관리되지 않는 시스코 디바이스를 정적 또는 동적 IP 주소를 가진 "엑스트라넷" 장치로 VPN 토폴로지에 추가할 수 있습니다.

- 비 시스코 디바이스: CDO를 사용하여 비 시스코 디바이스에 구성을 생성하거나 구축할 수 없습니다.
- 관리되지 않는 시스코 디바이스: 회사 내 다른 조직에서 관리하는 네트워크의 스포크 또는 서비스 제공업체 또는 파트너 네트워크에 대한 연결과 같이 조직에서 관리하지 않는 시스코 디바이스입니다.

관련 정보**:**

- ASA 사이에 사이트 간 VPN 구성, on page 2
- ASA 사이트 간 가상 프라이빗 네트워크 모니터링

ASA 사이에 사이트 간 VPN 구성

CDO는 ASA(Adaptive Security Appliance) 디바이스에서 사이트 간 VPN 기능의 다음 측면을 지원합니다.

- IPsec IKEv1 및 IKEv2 프로토콜이 모두 지원됩니다.
- 인증을 위한 자동 또는 수동 사전 공유 키.
- IPv4 및 IPv6. 내부와 외부의 모든 조합이 지원됩니다.
- IPsec IKEv2 사이트 간 VPN 토폴로지는 보안 인증을 준수하기 위한 구성 설정을 제공합니다.
- 정적 및 동적 인터페이스.

- 엔드포인트로 작동하는 엑스트라넷 디바이스의 정적 또는 동적 IP 주소 지원.

동적 주소 지정 피어로 사이트 간 VPN 연결 구성

CDO를 사용하면 피어의 VPN 인터페이스 IP 주소 중 하나를 알 수 없거나 인터페이스가 DHCP 서버에서 주소를 가져올 때 피어 간에 사이트 간 VPN 연결을 생성할 수 있습니다. 사전 공유 키, IKE 설정 및 IPsec 구성이 다른 피어와 일치하는 모든 동적 피어는 사이트 간 VPN 연결을 설정할 수 있습니다.

피어 A와 B를 고려하십시오. 고정 피어는 VPN 인터페이스의 IP 주소가 고정되어 있는 디바이스이고 동적 피어는 VPN 인터페이스의 IP 주소를 알 수 없거나 임시 IP 주소가 있는 디바이스입니다.

다음 사용 사례에서는 동적으로 주소가 지정된 피어를 사용하여 안전한 사이트 간 VPN 연결을 설정하는 다양한 시나리오를 설명합니다.

- A는 정적 피어이고 B는 동적 피어이거나 그 반대입니다.
- A는 고정 피어이고 B는 DHCP 서버에서 확인된 IP 주소를 사용하거나 그 반대로 하는 동적 피어입니다.
- A는 동적 피어이고, B는 고정 또는 동적 IP 주소를 사용하는 엑스트라넷 디바이스입니다.
- A는 DHCP 서버에서 확인된 IP 주소를 사용하는 동적 피어이고, B는 고정 또는 동적 IP 주소를 사용하는 엑스트라넷 디바이스입니다.

참고 ASDM(Adaptive Security Device Manager)과 같은 로컬 관리자를 사용하여 인터페이스의 IP 주소를 변경하면 CDO에서 해당 피어의 **Configuration Status(**구성 상태**)**에 "Conflict Detected(충돌 탐지됨)"가 표시됩니다. 이 대역 외 변경 사항을 해결하면 다른 피어의 **Configuration Status(**구성 상태**)**가 "Not Synced(동기화되지 않음)" 상태로 변경됩니다. "Not Synced(동기화되지 않음)" 상태인 디바이스에 CDO 구성을 구축해야 합니다.

일반적으로 동적 피어는 연결을 시작하는 피어여야 합니다. 다른 피어는 동적 피어의 IP 주소를 알지 못하기 때문입니다. 원격 피어가 연결을 설정하려고 시도하면 다른 피어가 사전 공유 키, IKE 설정 및 IPsec 구성을 사용하여 연결을 검증합니다.

원격 피어에서 연결을 시작한 후에만 VPN 연결이 설정되므로 VPN 터널에서 트래픽을 허용하는 액세스 제어 규칙과 일치하는 모든 아웃바운드 트래픽은 연결이 설정될 때까지 중단됩니다. 이를 통해 데이터가 적절한 암호화 및 VPN 보호 없이 네트워크를 벗어나지 않게 합니다.

참고 다음 시나리오에서는 사이트 간 VPN 연결을 구성할 수 없습니다.

디바이스에 둘 이상의 동적 피어 연결이 있는 경우

- 3개의 디바이스 A, B 및 C를 고려하십시오.
- A(고정 피어)와 B(동적 피어) 간에 사이트 간 VPN 연결을 구성합니다.
- 엑스트라넷 디바이스를 생성하여 A와 C(동적 피어) 간에 사이트 간 VPN 연결을 구성합니다. A의 고정 VPN 인터페이스 IP 주소를 엑스트라넷 디바이스에 할당하고 C와의 연결을 설정합니다.

ASA 사이트 간 VPN 지침 및 제한 사항

- CDO는 S2S VPN에 대한 흥미로운 트래픽을 설계하기 위해 crypto-acl을 지원하지 않습니다. 이는 보호된 네트워크만 지원합니다.
- IKE 포트 500/4500이 사용 중이거나 활성화된 일부 PAT 변환이 있을 때마다 사이트 간 VPN을 동일한 포트에서 구성할 수 없으므로 해당 포트에서 서비스를 시작하는 데 실패합니다.
- 전송 모드는 지원되지 않으며 터널 모드만 지원됩니다. IPsec 터널 모드는 새 IP 패킷에서 페이로드가 되는 원래 IP 데이터그램 전체를 암호화합니다. 방화벽 뒤에 배치되어 있는 호스트와 주고받는 트래픽을 방화벽이 보호하는 경우 터널 모드를 사용합니다. 터널 모드는 인터넷 등의 신뢰할 수 없는 네트워크를 통해 연결하는 두 방화벽 또는 기타 보안 게이트웨이 간에 일반 IPSec이 구현되는 통상적인 방식입니다.
- 이 릴리스에서는 하나 이상의 VPN 터널을 포함하는 PTP 토폴로지만 지원됩니다. Point-to-Point 구축에서는 두 엔드포인트 간에 VPN 터널을 설정합니다.

Virtual Tunnel Interface에 대한 지침

- VTI는 IPsec 모드에서만 구성할 수 있습니다. ASA에서의 GRE 터널 종료는 지원되지 않습니다.
- 터널 인터페이스를 사용하여 트래픽에 대한 동적 또는 정적 경로를 사용할 수 있습니다.
- 기본 물리적 인터페이스에 따라 VTI에 대한 MTU가 자동으로 설정됩니다. 그러나 VTI가 활성화된 후 물리적 인터페이스 MTU를 변경하는 경우, 새 MTU 설정을 사용하려면 VTI를 비활성화했다가 다시 활성화해야 합니다.
- 네트워크 주소 변환을 적용해야 할 경우, IKE 및 ESP 패킷이 UDP 헤더에서 캡슐화됩니다.
- IKE 및 IPsec 보안 연계는 터널에서 데이터 트래픽에 관계없이 지속적으로 다시 입력됩니다. 이렇게 하면 VTI 터널은 항상 작동합니다.
- 터널 그룹 이름은 피어가 IKEv1 또는 IKEv2 id로 전송하는 항목과 일치해야 합니다.
- LAN-to-LAN 터널 그룹에서 IKEv1의 경우, 터널 인증 방법이 디지털 인증서 및/또는 적극적인 모드를 사용하도록 구성된 피어인 경우, IP 주소가 아닌 이름을 사용할 수 있습니다.

- VTI 및 암호화 맵 구성은 동일한 물리적 인터페이스에서 공존할 수 있으며 암호화 맵에 구성된 피어 주소를 제공하며 VTI에 대한 터널 대상은 서로 다릅니다.
- 기본적으로 VTI를 통과하는 모든 트래픽이 암호화됩니다.
- 기본적으로 VTI 인터페이스의 보안 레벨은 0입니다.
- 액세스 목록은 VTI를 통과하는 트래픽을 제어하기 위해 VTI 인터페이스에 적용될 수 있습니다.
- VTI에서는 BGP만 지원됩니다.
- ASA가 IOS IKEv2 VTI 클라이언트를 종료하는 경우, IOS에서 config-exchange 요청을 비활성화합니다. ASA는 IOS VTI 클라이언트에서 시작한 이 L2L 세션에 대한 mode-CFG 속성을 검색할 수 없기 때문입니다.
- IPv6은 지원되지 않습니다.

관련 정보:

- ASA 사이에 사이트 간 VPN 터널 생성, 8 페이지
- VPN에서 사용되는 암호화 및 해시 알고리즘
- NAT에서 원격 액세스 VPN 트래픽 제외, 70 페이지

VPN에서 사용되는 암호화 및 해시 알고리즘

VPN 터널은 일반적으로 공용 네트워크(대개 인터넷)를 통과하므로 연결을 암호화하여 트래픽을 보호해야 합니다. IKE 정책 및 IPsec 제안을 사용하여 적용할 암호화 및 기타 보안 기술을 정의합니다.

디바이스 라이선스에서 강력한 암호화 적용이 허용되는 경우에는 광범위한 암호화 및 해시 알고리즘과 Diffie-Hellman 그룹 중에서 선택할 수 있습니다. 그러나 일반적으로는 터널에 적용하는 암호화가 강력할수록 시스템 성능은 더 나빠집니다. 따라서 효율성을 저하하지 않으면서 충분한 보호 기능을 제공하는 보안과 성능 간의 적절한 균형 지점을 찾아야 합니다.

Cisco는 선택할 수 있는 옵션에 대한 구체적인 지침을 제공하지는 않습니다. 대규모 기업이나 기타 조직 내에서 보안을 담당하는 경우 충족해야 하는 표준이 이미 정의되어 있을 수 있습니다. 그렇지 않은 경우, 선택할 수 있는 옵션에 대해 조사해야 합니다.

다음 주제에서는 사용 가능한 옵션에 대해 설명합니다.

사용할 암호화 알고리즘 결정

IKE 정책 또는 IPsec 제안에 사용할 암호화 알고리즘을 결정할 때는 VPN의 디바이스가 지원하는 알고리즘으로 선택이 제한됩니다.

IKEv2의 경우 여러 암호화 알고리즘을 구성할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 해당 순서를 사용하여 피어와 협상합니다. IKEv1의 경우 단일 옵션만 선택할 수 있습니다.

IPsec 제안의 경우 알고리즘은 인증, 암호화 및 재생 방지 서비스를 제공하는 ESP(Encapsulating Security Protocol)에서 사용됩니다. ESP는 IP 프로토콜 유형 50입니다. IKEv1 IPsec 제안에서 알고리즘 이름에는 ESP- 접두사가 붙습니다.

디바이스 라이선스에 따라 강력한 암호화를 사용할 수 있는 경우 다음 암호화 알고리즘 중에서 선택할 수 있습니다. 강력한 암호화를 사용할 수 없으면 DES만 선택할 수 있습니다.

- AES-GCM - (IKEv2에만 해당됨) 기밀 유지 및 데이터 원본 인증 기능을 제공하는 블록 암호화 작동 모드인 AES-GCM(Advanced Encryption Standard in Galois/Counter Mode)은 AES보다 보안성이 뛰어납니다. AES-GCM은 세 가지 키 강도(128비트, 192비트 및 256비트 키)를 제공합니다. 키 길이가 길수록 보안성은 더 높지만 성능은 낮습니다. GCM은 NSA Suite B를 지원하는 데 필요한 AES의 모드입니다. NSA Suite B는 암호화 강도에 대한 연방 기준을 충족시키기 위해 디바이스가 지원해야 하는 암호화 알고리즘 세트입니다.
- AES-GMAC - (IKEv2 IPsec 제안에만 해당됨) AES-GMAC(Advanced Encryption Standard Galois Message Authentication Code)는 데이터 원본 인증 기능만 제공하는 블록 암호화 작동 모드입니다. 이 모드는 데이터를 암호화하지 않고 데이터 인증을 허용하는 AES-GCM의 변형입니다. AES-GMAC는 세 가지 키 강도(128비트, 192비트 및 256비트 키)를 제공합니다.
- AES - AES(Advanced Encryption Standard)는 DES보다 보안성이 뛰어나며 3DES보다 계산 효율성이 높은 대칭 암호화 알고리즘입니다. AES는 세 가지 키 강도(128비트, 192비트 및 256비트 키)를 제공합니다. 키 길이가 길수록 보안성은 더 높지만 성능은 낮습니다.
- DES - 56비트 키를 사용하여 암호화를 수행하는 DES(Data Encryption Standard)는 대칭 보안 키 블록 알고리즘입니다. 라이선스 어카운트가 내보내기 제어에 대한 요건을 충족하지 않는 경우에는 이 옵션이 유일한 옵션입니다. 3DES보다 속도가 빠르며 시스템 리소스를 더 적게 사용하지만 보안성은 더 낮습니다. 강력한 데이터 기밀 유지 기능이 필요하지 않으며 시스템 리소스나 속도가 중요한 경우에는 DES를 선택하십시오.
- 3DES - 56비트 키를 사용하여 암호화를 3회 수행하는 3DES(Triple DES)는 서로 다른 키를 사용하여 각 데이터 블록을 3회 처리하므로 DES보다 안전합니다. 그러나 시스템 리소스를 더 많이 사용하며 DES보다 속도가 느립니다.
- NULL - null 암호화 알고리즘은 암호화를 수행하지 않는 인증 기능을 제공합니다. 이 알고리즘은 대개 테스트용으로만 사용됩니다.

사용할 해시 알고리즘 결정

IKE 정책에서 해시 알고리즘은 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성합니다. IKEv2에서 해시 알고리즘은 두 가지 옵션으로 구분됩니다. 그중 하나는 무결성 알고리즘 옵션이고 다른 하나는 PRF(Pseudo-Random Function: 의사 난수 함수) 옵션입니다.

IPsec 제안에서 해시 알고리즘은 인증을 위한 ESP(Encapsulating Security Protocol)에서 사용됩니다. IKEv2 IPsec 제안에서는 이러한 알고리즘을 무결성 해시라고 합니다. IKEv1 IPsec 제안에서는 알고리즘 이름에 ESP- 접두사가 붙으며 -HMAC(Hash Method Authentication Code) 접미사도 붙습니다.

IKEv2의 경우 여러 해시 알고리즘을 구성할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 해당 순서를 사용하여 피어와 협상합니다. IKEv1의 경우 단일 옵션만 선택할 수 있습니다.

다음 해시 알고리즘 중에서 선택할 수 있습니다.

- SHA(Secure Hash Algorithm) - 표준 SHA(SHA-1)에서는 160비트 다이제스트를 생성합니다. SHA는 MD5보다 무차별 암호 대입 공격에 대한 방어력이 뛰어납니다. 그러나 MD5 보다 리소스를 더 많이 사용 합니다. 최고 보안 레벨이 필요한 구현의 경우 SHA 해시 알고리즘을 사용합니다.
- IKEv2 컨피그레이션에는 다음과 같은 더욱 안전한 SHA-2 옵션을 사용할 수 있습니다. NSA Suite B 암호화 사양을 구현하려는 경우 이러한 옵션 중 하나를 선택합니다.
  - SHA-256 - 256비트 다이제스트를 생성하는 Secure Hash Algorithm SHA-2를 지정합니다.
  - SHA-384 - 384비트 다이제스트를 생성하는 Secure Hash Algorithm SHA-2를 지정합니다.
  - SHA-512 - 512비트 다이제스트를 생성하는 Secure Hash Algorithm SHA-2를 지정합니다.
- MD5(Message Digest 5) - 128비트 다이제스트를 생성합니다. MD5는 SHA보다 전반적으로 성능이 우수하여 처리 시간이 짧지만 SHA보다 취약한 것으로 간주됩니다.
- null 또는 None(NULL, ESP-NONE) - (IPsec 제안에만 해당됨) null 해시 알고리즘으로, 대개 테스트용으로만 사용됩니다. 그러나 AES-GCM/GMAC 옵션 중 하나를 암호화 알고리즘으로 선택하는 경우에는 null 무결성 알고리즘을 선택해야 합니다. null 이외의 옵션을 선택하더라도 이러한 암호화 표준에 대해서는 무결성 해시가 무시됩니다.

사용할 **Diffie-Hellman** 모듈러스 그룹 결정

다음 Diffie-Hellman 키 파생 알고리즘을 사용하여 IPsec 보안 연계(SA) 키를 생성할 수 있습니다. 각 그룹의 크기 모듈러스는 서로 다릅니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어에 일치하는 모듈러스 그룹이 있어야 합니다.

AES 암호화를 선택하는 경우 AES에 필요한 큰 키를 지원하려면 DH(Diffie-Hellman) 그룹 5 이상을 사용해야 합니다. IKEv1 정책에서는 아래에 나열된 그룹을 모두 지원하지는 않습니다.

NSA Suite B 암호화 사양을 구현하려면 IKEv2를 사용하고 ECDH(Elliptic Curve Diffie-Hellman) 옵션 19, 20, 21 중 하나를 선택합니다. 2048비트 모듈러스를 사용하는 엘립틱 커브 옵션과 그룹은 Logjam과 같은 공격에 노출될 가능성이 작습니다.

IKEv2의 경우에는 여러 그룹을 구성할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 해당 순서를 사용하여 피어와 협상합니다. IKEv1의 경우 단일 옵션만 선택할 수 있습니다.

- 2 - Diffie-Hellman 그룹 2: 1024비트 MODP(모듈식 지수) 그룹. 이 옵션은 더 이상 좋은 보호 방법으로 간주되지 않습니다.
- 5 - Diffie-Hellman 그룹 5: 1536비트 MODP 그룹. 전에는 이 옵션이 128비트 키에 대해 좋은 보호 방법으로 간주되었지만 이제는 더 이상 좋은 보호 방법으로 간주되지 않습니다.
- 14 - Diffie-Hellman 그룹 14: 2048비트 MODP(모듈식 지수) 그룹. 192비트 키에 적합한 보호를 제공합니다.
- 19 - Diffie-Hellman 그룹 19: NIST(국내 표준 및 기술) 256비트 ECP(elliptic curve modulo a prime) 그룹
- 20 - Diffie-Hellman 그룹 20: NIST 384비트 ECP 그룹

- 21 - Diffie-Hellman 그룹 21: NIST 521비트 ECP 그룹
- 24 - Diffie-Hellman 그룹 24: 2048비트 MODP 그룹 및 256비트 소수 위수 하위 그룹. 이 옵션은 더 이상 권장되지 않습니다.

사용할 인증 방법 결정

다음과 같은 방법을 사용하여 Site-to-Site VPN 연결에서 피어를 인증할 수 있습니다.

사전 공유 키

사전 공유 키는 연결에서 각 피어에 컨피그레이션된 암호 키 문자열입니다. 이 키는 인증 단계 중에 IKE에서 사용합니다. IKEv1의 경우, 각 피어에서 동일한 사전 공유 키를 컨피그레이션해야 합니다. IKEv2의 경우, 각 피어에 고유 키를 컨피그레이션할 수 있습니다.

사전 공유 키는 인증서에 비해 확장성이 떨어집니다. 다수의 사이트 간 VPN 연결을 구성해야 하는 경우, 사전 공유 키 방법 대신 인증서 방법을 사용하십시오.

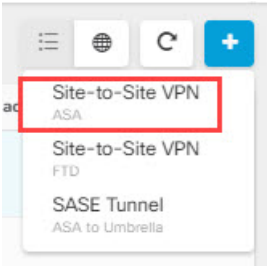
ASA 사이에 사이트 간 VPN 터널 생성

두 ASA 또는 엑스트라넷 디바이스를 사용하는 ASA 간에 사이트 간 VPN 터널을 생성하려면 다음 절차를 수행합니다.

프로시저

단계 **1** 탐색 창에서 **VPN** > **Site-to-Site ASA/FDM (**사이트 간 **ASA/FDM)**을 선택합니다.

단계 **2** 오른쪽 상단 모서리에 있는 파란색 더하기  를 클릭하고 ASA 레이블이 있는 **Site-to-Site VPN(**사이트 간 **VPN)**을 클릭합니다.



단계 **3** **Configuration Name(**구성 이름**)** 필드에 생성한 사이트 간 VPN 구성의 이름을 입력합니다.

단계 **4** 새 정책 기반 또는 경로 기반 사이트 간 VPN을 생성하는 옵션 중 하나를 선택합니다.

단계 **5** **Peer Devices(**피어 디바이스**)** 섹션에서 다음을 수행합니다.

a) 피어 **1**: ASA 디바이스를 선택하고 **Select(**선택**)**를 클릭합니다.

b) 피어 **2**: 다른 ASA 디바이스를 선택한 다음 **Select(**선택**)**를 클릭합니다.

엑스트라넷: 피어 2에서 엑스트라넷 디바이스를 선택하려면 엑스트라넷 슬라이더를 클릭하여 활성화합니다.

Static(고정**)**을 선택하고 IP 주소를 지정하거나, DHCP 할당 IP가 있는 엑스트라넷 디바이스의 경우 **Dynamic(**동적**)**을 선택합니다. **IP Address(IP** 주소**)**는 정적 인터페이스의 IP 주소 또는 동적 인터페이스의 **DHCP Assigned(DHCP** 할당됨**)**를 표시합니다.

c) **Next(**다음**)**를 클릭합니다.

d) 엔드포인트 디바이스에 대한 **VPN** 액세스 인터페이스를 선택합니다.

e) (경로 기반 VPN에 적용 가능) LAN 서브넷을 제어하는 **LAN** 인터페이스를 선택합니다. 여러 인터페이스를 선택할 수 있습니다.

선택한 LAN 인터페이스에 연결된 네트워크가 라우팅 정책 액세스 목록에 추가됩니다. 라우팅 정책 액세스 목록과 일치하는 트래픽은 VPN 터널에 의해 암호화/암호 해독됩니다.

f) 참여하는 디바이스에 대해 **Protected Networks(**보호된 네트워크**)**를 추가하려면 **Add Network(**네트워크 추가**)**를 클릭합니다. 보호된 네트워크는 이 VPN 엔드포인트로 보호되는 네트워크를 정의합니다.

g) (선택 사항이며 정책 기반에 적용 가능) 로컬 VPN 액세스 인터페이스의 NAT 정책에서 VPN 트래픽을 제외하려면 **NAT Exempt(NAT** 면제**)**를 선택합니다. 개별 피어에 대해 수동으로 구성해야 합니다. NAT 규칙을 로컬 네트워크에 적용하지 않으려는 경우 로컬 네트워크를 호스팅하는 인터페이스를 선택합니다. 이 옵션은 로컬 네트워크가 단일 라우팅 인터페이스(브리지 그룹 멤버 아님) 뒤에 있는 경우에만 작동합니다. 로컬 네트워크가 둘 이상의 라우팅 인터페이스 또는 하나 이상의 브리지 그룹 멤버 뒤에 있는 경우에는 NAT 제외 규칙을 수동으로 생성해야 합니다. 필요한 규칙을 수동으로 생성하는 방법에 대한 자세한 내용은 NAT에서 ASA 사이트 간 VPN 트래픽 제외를 참조하십시오.

h) **Next(**다음**)**를 클릭합니다.

단계 **6** (라우트 기반에 적용 가능) 이전 단계에서 피어 디바이스가 구성되면 터널 세부 정보에서 **VTI** 주소 필드가 자동으로 채워집니다. 필요한 경우 새 VTI로 사용할 IP 주소를 수동으로 입력할 수 있습니다.

단계 **7** **IKE Settings(IKE** 설정**)** 섹션에서 IKE(Internet Key Exchange) 협상 중에 사용할 IKE 버전을 선택하고 프라이버시 구성을 지정합니다. IKE 정책에 대한 자세한 내용은 전역 IKE 정책 정보을 참조하십시오.

CDO는 사용자가 수행한 구성에 따라 IKE 설정을 제안합니다. 권장 IKE 구성 설정을 계속 사용하거나 새로 정의할 수 있습니다.

참고
IKE 정책은 디바이스에 전역적이며 연결된 모든 VPN 터널에 적용됩니다. 따라서 정책을 추가하거나 삭제하면 이 디바이스가 참여하는 모든 VPN 터널에 영향을 미칩니다.

a) 적절하게 IKE 버전 중 하나 또는 둘 다를 선택합니다.

기본적으로 **IKEV** 버전 **2**가 활성화되어 있습니다.

참고
경로 기반 VPN에는 두 IKE 버전을 모두 활성화할 수 없습니다.

b) **Add IKEv2 Policy(IKEv2** 정책 추가**)**를 클릭하고 IKEv2 정책을 선택합니다.

참고
Create New IKEv2 Policy(새 **IKEv2** 정책 생성**)**를 클릭하여 새 IKEv2 정책을 생성합니다. 새 IKEv2 정책 생성에 대한 자세한 내용은 IKEv2 정책 관리을 참고하십시오. 기존 IKEv2 정책을 삭제하려면 선택한 정책 위에 마우스를 놓고 x 아이콘을 클릭합니다.

c) 참여 디바이스에 대한 사전 공유 키를 입력합니다. 사전 공유 키는 연결에서 각 피어에 컨피그레이션된 암호 키 문자열입니다. IKE는 인증 단계 중에 이러한 키를 사용합니다.

(IKEv2) 피어 **1** 사전 공유 키, 피어 **2** 사전 공유 키: IKEv2의 경우 각 피어에서 고유한 키를 구성할 수 있습니다. 사전 공유 키를 입력합니다. show(표시) 버튼을 클릭하고 피어에 대해 적절한 사전 공유를 입력할 수 있습니다. 키는 영숫자 1~127자가 될 수 있습니다. 다음 표에서는 두 피어에 대한 사전 공유 키의 용도에 대해 설명합니다.

	로컬 사전 공유 키	원격 피어 사전 공유 키
피어 **1**	피어 1 사전 공유 키	피어 2 사전 공유 키
피어 **2**	피어 2 사전 공유 키	피어 1 사전 공유 키

d) **IKE Version 1(IKE** 버전 **1)**을 클릭하여 활성화합니다.

e) **Add IKEv1 Policy(IKEv1** 정책 추가**)**를 클릭하고 IKEv1 정책을 선택합니다. **Create New IKEv1 Policy(**새 **IKEv1** 정책 생성**)**를 클릭하여 새 IKEv1 정책을 생성합니다. 새 IKEv1 정책 생성에 대한 자세한 내용은 IKEv1 정책 관리을 참고하십시오. 기존 IKEv1 정책을 삭제하려면 선택한 정책 위에 마우스를 올리고 x 아이콘을 클릭합니다.

f) (IKEv1) 사전 공유 키: IKEv1의 경우, 각 피어에서 동일한 사전 공유 키를 컨피그레이션해야 합니다. 키는 영숫자 1~127자가 될 수 있습니다. 이 시나리오에서 피어 1과 피어 2는 동일한 사전 공유 키를 사용하여 데이터를 암호화하고 해독합니다.

g) **Next(**다음**)**를 클릭합니다.

단계 **8** **IPSec Settings(IPSec** 설정**)** 섹션에서 CDO는 사용자가 수행한 구성을 기반으로 IKEv2 제안을 제안합니다. 권장 IKE 구성 설정을 계속 사용하거나 새로 정의할 수 있습니다. IPSec 설정에 대한 자세한 내용은 IPsec 제안 구성을 참고하십시오.

a) **+ IKEv2 Proposals(+ IKEv2** 제안**)**를 클릭하여 IPSec 구성을 선택합니다. **IKE Settings(IKE** 설정**)** 단계에서 선택한 항목에 따라 해당 IKEV 제안을 사용할 수 있습니다. 기존 IKEv2 제안을 삭제하려면 선택한 제안 위에 마우스를 올려 놓고 x 아이콘을 클릭합니다.

참고
Create New IKEv2 Proposals(새 **IKEv2** 제안 생성**)**를 클릭하여 새 IKEv2 제안을 생성합니다. 새 IKEv2 정책 생성에 대한 자세한 내용은 IPsec 제안 정보을 참고하십시오.

b) **Perfect Forward Secrecy**용 **Diffie-Hellman** 그룹을 선택합니다. 자세한 내용은 VPN에서 사용되는 암호화 및 해시 알고리즘, 5 페이지를 참조하십시오.

c) **Next(**다음**)**를 클릭합니다.

단계 **9** **Finish(**완료**)** 섹션에서 구성을 읽고 구성에 만족하는 경우에만 계속 진행하고 **Submit(**제출**)**을 클릭하십시오.

새로 구성된 사이트 간 VPN 터널을 표시하는 VPN Tunnels(VPN 터널) 페이지로 이동합니다. 변경 사항이 준비되며 수동으로 구축해야 합니다. VTI 터널을 통해 디바이스 간에 VTI 트래픽을 자동으로 라우팅하도록 라우팅 정책이 생성됩니다. 이 정책을 보려면 **Inventory(**인벤토리**)** 페이지에서 디바이스를 선택하고 **Configuration(**구성**)** > **Diff(**차이**)**를 선택하십시오.

새 터널과 연결된 디바이스에 사이트 간 VPN 구성을 구축하려면 구성 변경 사항 구축 섹션을 참조하십시오.

NAT에서 사이트 간 VPN 트래픽 제외

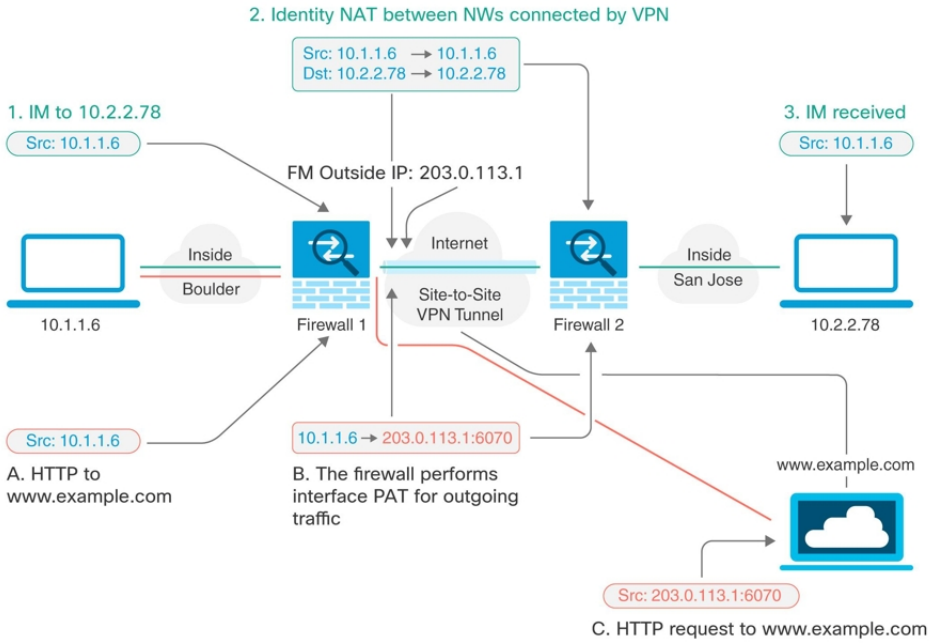
인터페이스에 사이트 간 VPN 연결이 정의되어 있고 해당 인터페이스에 대한 NAT 규칙도 있는 경우 NAT 규칙에서 VPN의 트래픽을 선택적으로 제외할 수 있습니다. VPN 연결의 원격 쪽에서 내부 주소를 처리할 수 있는 경우 이러한 VPN 트래픽을 제외할 수 있습니다.

VPN 연결을 생성할 때 **NAT Exempt(NAT** 제외**)** 옵션을 선택하여 규칙을 자동으로 생성할 수 있습니다. 그러나 브리지 그룹 멤버가 아닌 단일 라우팅 인터페이스를 통해 보호된 로컬 네트워크에 연결하는 경우에만 이 방법을 사용할 수 있습니다. 그렇지 않고 연결의 로컬 네트워크가 둘 이상의 라우팅 인터페이스 또는 하나 이상의 브리지 그룹 멤버에 있는 경우에는 NAT 제외 규칙을 수동으로 구성해야 합니다.

NAT 규칙에서 VPN 트래픽을 제외하려면 대상이 원격 네트워크일 때 로컬 트래픽에 대한 ID 수동 NAT 규칙을 생성합니다. 그런 다음 대상이 인터넷 등의 다른 항목일 때 트래픽에 NAT를 적용합니다. 로컬 네트워크의 인터페이스가 여러 개인 경우 각 인터페이스에 대해 규칙을 생성합니다. 또한 다음과 같은 제안 사항을 고려합니다.

- 연결에 로컬 네트워크가 여러 개 있으면 네트워크를 정의하는 개체를 포함할 네트워크 개체 그룹을 생성합니다.
- VPN에 IPv4 및 IPv6 네트워크를 둘 다 포함하는 경우 각 네트워크에 대해 별도의 ID NAT 규칙을 생성합니다.

볼더 사무실과 산호세 사무실을 연결하는 사이트 간 터널을 보여주는 다음 예를 살펴보십시오. 인터넷으로 이동할 트래픽(예: 볼더의 10.1.1.6에서 www.example.com으로)의 경우 인터넷 액세스를 위해 NAT에서 제공하는 공용 IP 주소가 필요합니다. 아래 예에서는 인터페이스 PAT(Port Address Translation) 규칙을 사용합니다. 그러나 VPN 터널을 지나갈 트래픽(예: 볼더의 10.1.1.6에서 산호세의 10.2.2.78로)에 대해서는 NAT를 수행하지 않으려고 합니다. 그렇게 하려면 ID NAT 규칙을 만들어 해당 트래픽을 제외해야 합니다. ID NAT는 주소를 동일한 주소로 변환합니다.



다음 예에서는 방화벽1(볼더)의 컨피그레이션에 대해 설명합니다. 이 예에서는 내부 인터페이스가 브리지 그룹이라고 가정하므로 각 멤버 인터페이스에 대해 규칙을 작성해야 합니다. 라우팅 내부 인터페이스가 하나이든 여러 개이든 프로세스는 동일합니다.

Note 이 예에서는 IPv4만 사용한다고 가정합니다. VPN에 IPv6 네트워크도 포함되어 있으면 IPv6용 병렬 규칙을 생성합니다. IPv6 인터페이스 PAT를 구현할 수는 없으므로 PAT에 사용할 고유 IPv6 주소가 포함된 호스트 개체를 생성해야 합니다.

Procedure

단계 **1** 여러 네트워크를 정의하기 위한 개체를 생성합니다.

a. 왼쪽 창에서 개체를 클릭합니다.

b. 파란색 더하기 버튼 을 클릭하여 개체를 생성합니다.

c. **ASA** > **Network(ASA** 네트워크**)**를 클릭합니다.

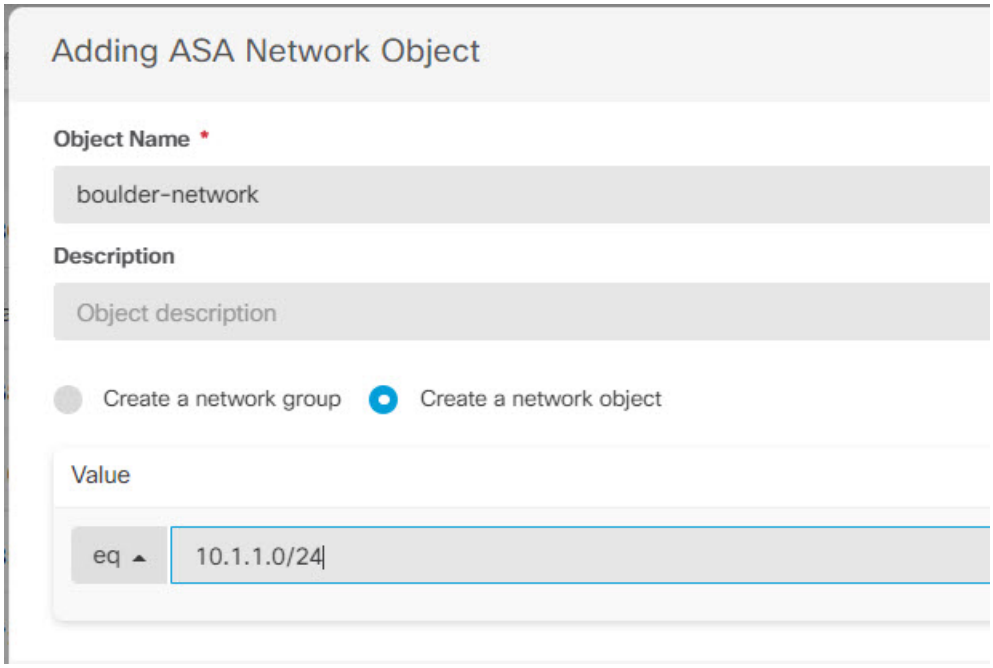
d. 볼더 내부 네트워크를 확인합니다.

e. 개체 이름을 입력합니다(예: boulder-network).

f. **Create a network object(**네트워크 개체 생성**)**를 선택합니다.

g. Value(값) 섹션에서 다음을 수행합니다.

- **eq**를 선택하고 단일 IP 주소 또는 CIDR 표기법으로 표시된 서브넷 주소를 입력합니다.
- 범위를 선택하고 IP 주소 범위를 입력합니다. 예를 들어 네트워크 주소를 10.1.1.0/24로 입력합니다.



h. **Add(**추가**)**를 클릭합니다.

i. 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.

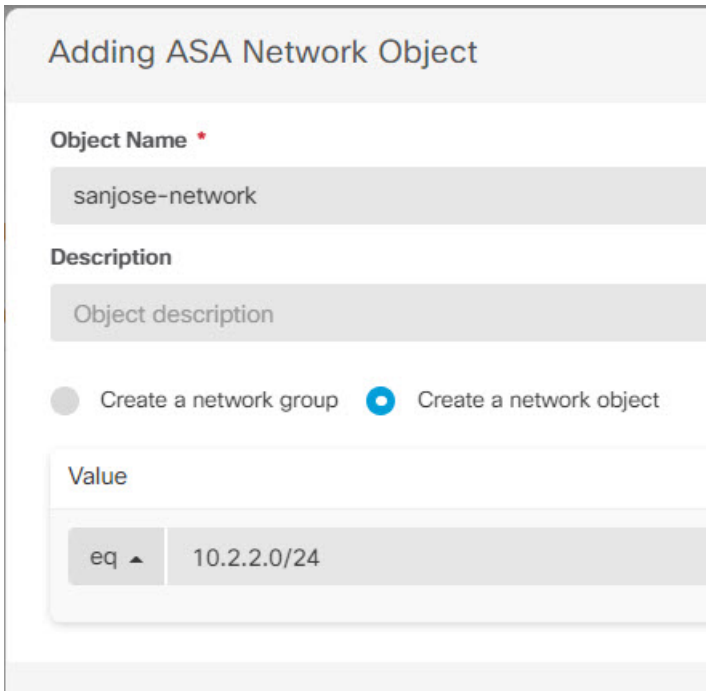
j. 내부 산호세 네트워크를 정의합니다.

k. 개체 이름(예: san-jose)을 입력합니다.

l. **Create a network object(**네트워크 개체 생성**)**를 선택합니다.

m. Value(값) 섹션에서 다음을 수행합니다.

- **eq**를 선택하고 단일 IP 주소 또는 CIDR 표기법으로 표시된 서브넷 주소를 입력합니다.
- 범위를 선택하고 IP 주소 범위를 입력합니다. 예를 들어 네트워크 주소를 10.1.1.0/24로 입력합니다.



n. **Add(**추가**)**를 클릭합니다.

단계 **2** 방화벽1(볼더)에서 VPN을 통해 산호세로 이동할 때 볼더 네트워크용 수동 ID NAT를 구성합니다.

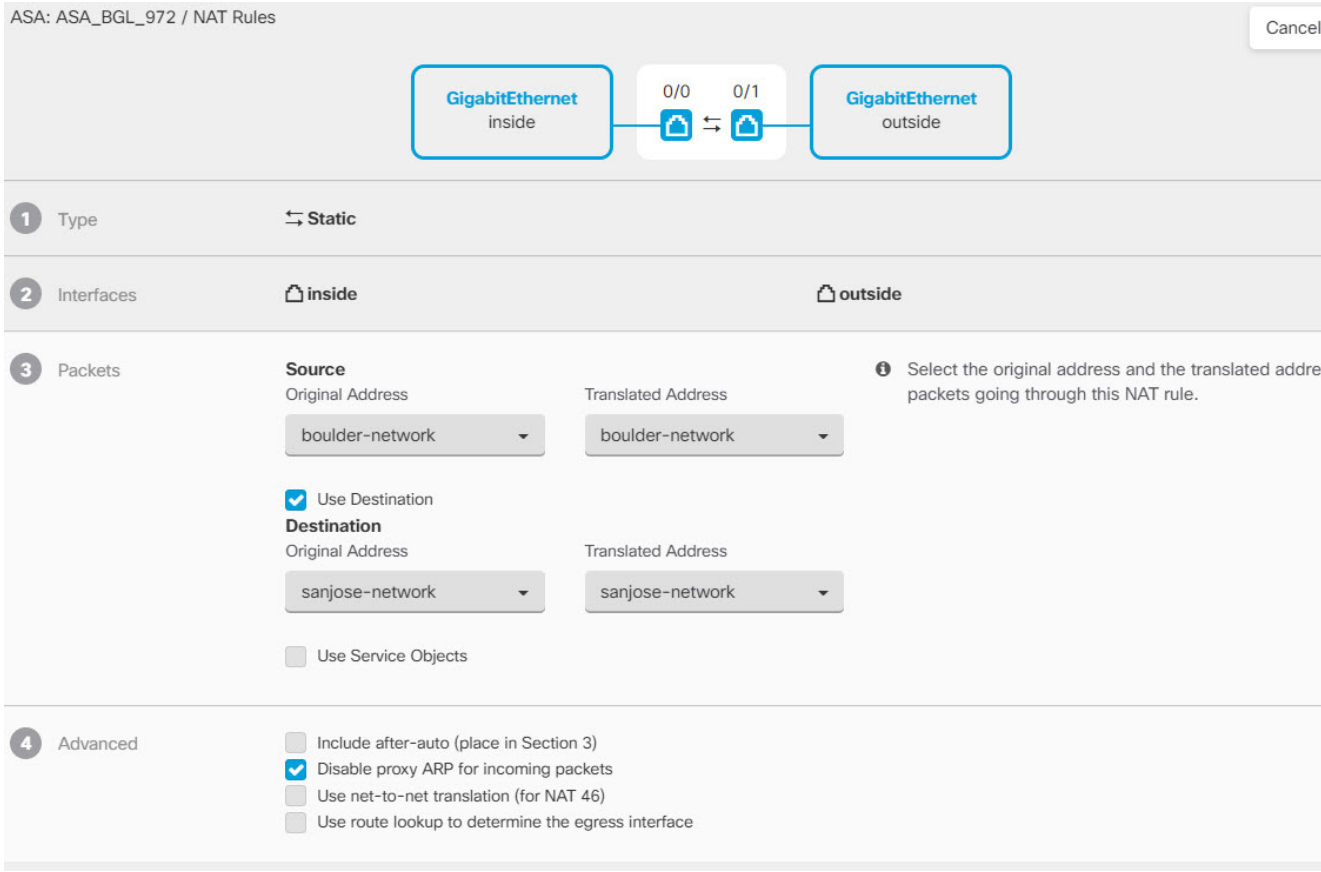
a. 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

b. 필터를 사용하여 NAT 규칙을 생성할 디바이스를 찾습니다.

c. 상세정보 패널의 Management(관리) 영역에서 **NAT** NAT 를 클릭합니다.

d. + > **2**회 **NAT**를 클릭합니다.

- 섹션 1에서 **Static(**정적**)**을 선택합니다. **Continue(**계속**)**를 클릭합니다.
- 섹션 2에서 **Source Interface(**소스 인터페이스**)** = **inside(**내부**)** 및 **Destination Interface(**대상 인터페이스**)** = **outside(**외부**)**를 선택합니다. **Continue(**계속**)**를 클릭합니다.
- 섹션 3에서 **Source Original Address(**소스 원본 주소**)** = 'boulder-network' 및 **Source Translated Address(**소스 변환 주소**)** = 'boulder-network'를 선택합니다.
- **Use Destination(**대상 사용**)**을 선택합니다.
- **Destination Original Address(**대상 원본 주소**)** = 'sanjose-network' 및 **Source Translated Address(**소스 변환 주소**)** = 'sanjose-network'를 선택합니다. 참고: 대상 주소를 변환하지 않을 것이기 때문에 원본 주소 및 변환된 대상 주소에 대해 동일한 주소를 지정하여 대상 주소에 대한 ID NAT를 구성해야 합니다. 포트 필드는 모두 비워 둡니다. 이 규칙은 소스 및 대상 둘 다에 대해 ID NAT를 구성합니다.



- **Disable proxy ARP for Incoming packet(**수신 패킷에 대해 프록시 **ARP** 비활성화**)**을 선택합니다.
- **Save(**저장**)**를 클릭합니다.
- 이 프로세스를 반복하여 각각의 기타 내부 인터페이스에 대해 동일 규칙을 생성합니다.

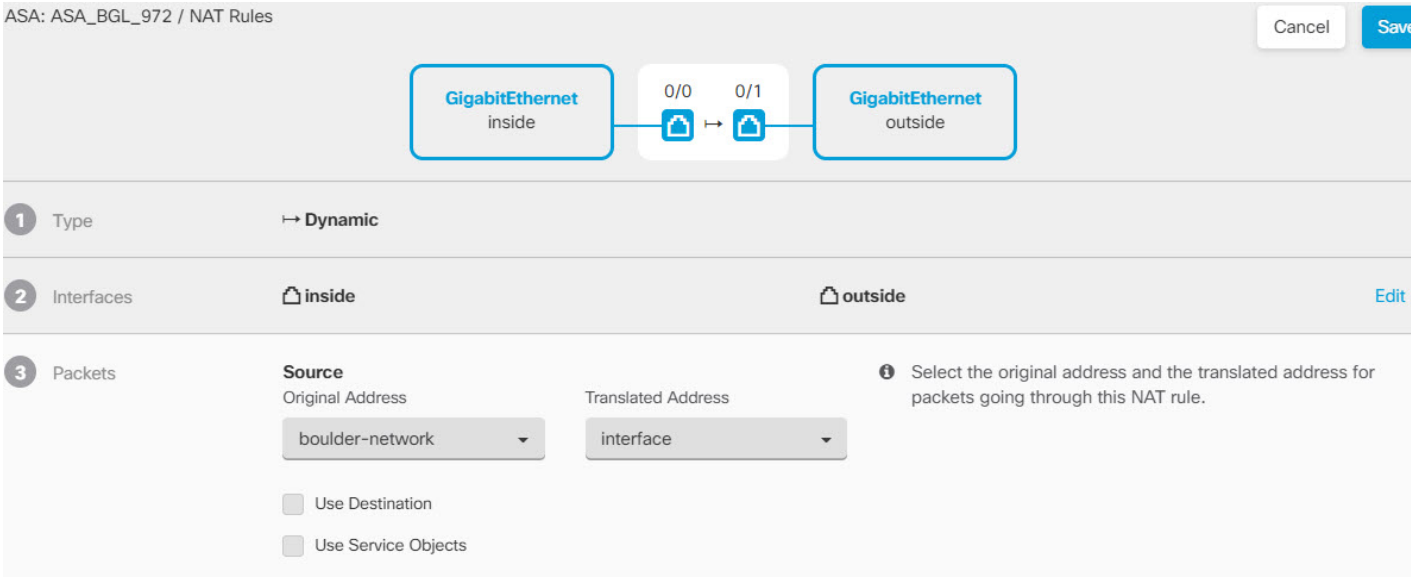
단계 **3** 방화벽1(볼더)에서 내부 볼더 네트워크에 대해 인터넷으로 이동할 때 수동 동적 인터페이스 PAT를 구성합니다. 참고: 모든 IPv4 트래픽에 적용되는 내부 인터페이스용 동적 인터페이스 PAT 규칙은 이미 있을 수 있습니다. 이러한 규칙은 초기 구성 중에 기본적으로 생성되기 때문입니다. 그러나 여기서는 완전한 설명을 위해 컨피그레이션을 제공합니다. 이러한 단계를 완료하기 전에 내부 인터페이스와 네트워크에 적용되는 규칙이 이미 있는지 확인하고 해당 규칙이 있으면 이 단계를 건너뜁니다.

a.  > **2**회 **NAT**를 클릭합니다.

b. 섹션 1에서 **Dynamic(**동적**)**을 선택합니다. **Continue(**계속**)**를 클릭합니다.

c. 섹션 2에서 **Source Interface(**소스 인터페이스**) = inside(**내부**)** 및 **Destination Interface(**대상 인터페이스**) = outside(**외부**)**를 선택합니다. **Continue(**계속**)**를 클릭합니다.

d. 섹션 3에서 **Source Original Address(**소스 원본 주소**)** = 'boulder-network' 및 **Source Translated Address(**소스 변환 주소**)** = 'interface'를 선택합니다.



e. **Save(**저장**)**를 클릭합니다.

f. 이 프로세스를 반복하여 각각의 기타 내부 인터페이스에 대해 동일 규칙을 생성합니다.

단계 **4** CDO에 구성 변경 사항을 구축합니다. 자세한 내용은 CDO GUI를 사용하여 구성 변경 사항 구축를 참고하십시오.

단계 **5** 방화벽2(산호세)도 관리하는 경우 해당 디바이스에 대해 비슷한 규칙을 구성할 수 있습니다.

- 대상이 boulder-network일 때는 sanjose-network용 수동 ID NAT 규칙을 구성합니다. 방화벽2 내부 및 외부 네트워크용으로 새 인터페이스 개체를 생성합니다.
- 대상이 "임의"일 때는 sanjose-network용 수동 동적 인터페이스 PAT 규칙을 생성합니다.

ASA와 멀티 클라우드 방어 게이트웨이 사이에 사이트 간 VPN 구성

모든 관련 표준을 준수하는 ASA와 멀티 클라우드 방어 게이트웨이 사이에 사이트 간 IPsec 연결을 생성할 수 있습니다. VPN 연결이 설정되면 방화벽 뒤에 있는 호스트는 보안 VPN 터널을 통해 게이트웨이 뒤에 있는 호스트에 연결할 수 있습니다.

멀티 클라우드 방어에서는 현재 AWS(Amazon Web Services), Azure, GCP(Google Cloud Platform) 및 Oracle OCI 클라우드 어카운트를 지원합니다.

ASA와 멀티 클라우드 방어 게이트웨이 사이에 사이트 간 VPN 터널 생성

다음 절차를 수행하여 CDO에 의해 관리되는 ASA 디바이스와 CDO 대시보드의 멀티 클라우드 방어 게이트웨이 사이에 VPN 터널을 생성합니다.

시작하기 전에

다음 사전 요건이 충족되는지 확인합니다.

- ASA 디바이스에는 보류 중인 변경 사항이 없어야 합니다.
- VPN 터널을 생성하기 전에 ASA 콘솔에서 BGP 프로파일을 생성합니다. 자세한 내용은 ASA Border 게이트웨이 프로토콜 설정을 참조하십시오.
- 멀티 클라우드 방어 게이트웨이는 **Active(**활성**)** 상태여야 합니다.
- 멀티 클라우드 방어 게이트웨이는 VPN 활성화 상태여야 합니다. 게이트웨이 내에서 VPN 활성화를 참조하십시오.
- 자세한 내용은 ASA 사이트 간 VPN 제한 사항 및 지침을 참조하십시오.
- 자세한 내용은 마이그레이션에 대한 멀티 클라우드 방어 게이트웨이 사전 요건 및 제한 사항을 읽어보십시오.

프로시저

단계 **1** 왼쪽 창에서 **VPN** > 사이트 간 **VPN(**사이트 간 **VPN)**을 선택합니다.

단계 **2** 오른쪽 상단의 터널 생성( ) 버튼을 클릭하고 멀티 클라우드 방어 레이블을 가진 사이트 간 **VPN**을 클릭합니다.

단계 **3** **Configuration Name(**구성 이름**)** 필드에 생성한 사이트 간 VPN 구성의 이름을 입력합니다.

단계 **4** 피어 디바이스 영역에서 다음 정보를 입력합니다.

- 디바이스 **1**: 드롭다운 목록 에서 **ASA** 탭을 클릭하고 원하는 ASA 디바이스를 선택합니다.
- 디바이스 **2**: 드롭다운 목록 에서 멀티 클라우드 방어 탭을 클릭하고 원하는 게이트웨이를 선택합니다.
- **VPN** 액세스 인터페이스: 멀티 클라우드 방어에 연결하는 데 사용할 ASA 인터페이스를 선택합니다.
- **Public IP (**선택 사항**)**: 선택한 ASA의 외부 인터페이스에 매핑되는 네트워크 주소 변환(NAT)의 공용 IP 주소를 지정합니다.
- 라우팅 : **Add Networks(**네트워크 추가**)**를 클릭하고 ASA에서 보호된 네트워크를 하나 이상 선택하여 선택한 네트워크 및 멀티 클라우드 방어 게이트웨이 사이에 사이트 간 터널을 생성합니다.

단계 **5** **Next(**다음**)**를 클릭합니다.

단계 **6** **Tunnel Details(**터널 상세정보**)** 영역에서 다음 정보를 제공합니다.

- **Virtual Tunnel Interface IP(**가상 터널 인터페이스 **IP)**: 피어에서 새 가상 터널 인터페이스의 주소를 지정합니다. CDO는 충돌이 발생하는 경우 변경할 수 있는 ASA에 대한 샘플 주소를 제공합니다. 이 디바이스에서 현재 사용되지 않는 미사용 IP 주소를 할당할 수 있습니다.

- 자동 시스템 번호(피어 1): ASA 디바이스에 자동 시스템 번호가 구성되어 있지 않은 경우 CDO는 디바이스에 대해 자동 시스템 번호를 제안하며, 이 번호는 수정할 수 있습니다. 디바이스에 이미 자동 시스템 번호가 구성된 경우 현재 값이 표시되고 수정할 수 없습니다.
- 자동 시스템 번호(피어 2): BGP 프로파일이 멀티 클라우드 방어 게이트웨이에 할당된 경우 프로파일과 연결된 자동 번호가 표시되며 이는 수정할 수 없습니다. 멀티 클라우드 방어 게이트웨이 추가를 참조하십시오.

단계 **7** **Next(**다음**)**를 클릭합니다.

단계 **8** **IKE** 설정 영역 에서 CDO는 기본 사전 공유 키를 생성합니다. 이것은 피어에 구성된 암호 키 문자열입니다. IKE는 인증 단계 중에 이 키를 사용합니다. 피어 간에 터널을 설정할 때 서로를 확인하는 데 사용됩니다.

단계 **9** **Next(**다음**)**를 클릭합니다.

단계 **10** **Finish(**완료**)** 영역에서 구성을 검토하고 구성에 만족하는 경우에만 계속 진행합니다.

기본적으로 **Deploy changes to ASA immediately(ASA**에 즉시 변경 사항 구축**)** 확인란이 선택되어 **Submit(**제출**)**을 클릭한 후 ASA 디바이스에 즉시 구성을 구축합니다.

나중에 수동으로 설정을 검토하고 구축하려면 이 확인란의 선택을 취소합니다 .

단계 **11** **Submit(**제출**)**를 클릭합니다.

구성은 멀티 클라우드 방어 게이트웨이로 푸시됩니다.

CDO의 VPN 페이지에는 피어 간에 생성된 사이트 간 터널이 표시됩니다. 멀티 클라우드 방어 게이트웨이 포털에서 해당 터널을 확인할 수 있습니다.

전역 IKE 정책 정보

IKE(Internet Key Exchange)는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용되는 키 관리 프로토콜입니다.

IKE 협상은 2단계로 구성됩니다. 1단계에서는 두 IKE 피어 간의 보안 연계를 협상합니다. 그러면 피어가 2단계에서 안전하게 통신할 수 있습니다. 2단계 협상 중에는 IKE가 IPsec 등의 기타 애플리케이션에 대해 SA를 설정합니다. 두 단계에서는 모두 연결을 협상할 때 제안을 사용합니다. IKE 제안은 두 피어가 상호 간의 IKE 협상을 보호하는 데 사용하는 알고리즘 집합입니다. IKE 협상에서는 두 피어가 먼저 공통(공유) IKE 정책을 합의합니다. 이 정책은 후속 IKE 협상을 보호하는 데 사용되는 보안 파라미터를 제시합니다.

IKE 정책 개체는 이러한 협상을 위한 IKE 제안을 정의합니다. 활성화하는 개체는 피어가 VPN 연결을 협상할 때 사용됩니다. 연결당 서로 다른 IKE 정책을 지정할 수는 없습니다. 각 개체의 상대 우선순위에 따라 이러한 정책 중 먼저 사용을 시도할 정책이 결정되며, 숫자가 작을수록 우선 순위는 높습니다. 협상에서 장애가 발생하여 두 피어가 모두 지원할 수 있는 정책을 찾지 못하면 연결이 설정되지 않습니다.

글로벌 IKE 정책을 정의하려면 각 IKE 버전에 대해 활성화할 개체를 선택합니다. 사전 정의된 개체가 요건을 충족하지 않는 경우 새 정책을 생성하여 보안 정책을 적용합니다.

다음 절차에서는 개체 페이지를 통해 글로벌 정책을 구성하는 방법을 설명합니다. IKE 정책 설정에서 Edit(수정)을 클릭하여 VPN 연결을 수정할 때 정책을 활성화, 비활성화 및 생성할 수도 있습니다.

다음 항목에서는 각 버전에 대해 IKE 정책을 구성하는 방법에 대해 설명합니다.

- IKEv1 정책 관리
- IKEv2 정책 관리

IKEv1 정책 관리

IKEv1 정책 정보

IKE(Internet Key Exchange) 버전 1 정책 개체에는 VPN 연결을 정의할 때 IKEv1 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv1 정책이 있습니다. 필요에 맞는 정책이 있으면 State(상태) 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

Related Topics

IKEv1 정책 생성, 19 페이지

IKEv1 정책 생성

IKE(Internet Key Exchange) 버전 1 정책 개체에는 VPN 연결을 정의할 때 IKEv1 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv1 정책이 있습니다. 필요에 맞는 정책이 있으면 State(상태) 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 편집할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKE Policy(**새 **IKE** 정책 생성**)** 링크를 클릭하여 사이트 간 VPN 연결에서 IKE 설정을 편집하면서 IKEv1 정책을 생성할 수도 있습니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 파란색 더하기  버튼을 클릭하고 **FDM** > **IKEv1 Policy(IKEv1** 정책**)**를 선택하여 새 IKEv1 정책을 생성합니다.

- 개체 페이지에서 편집할 IKEv1 정책을 선택하고 오른쪽의 Actions(작업) 창에서 **Edit(편집)**를 클릭합니다.

단계 **3** 개체 이름을 최대 128자로 입력합니다.

단계 **4** IKEv1 속성을 구성합니다.

- **Priority(우선순위)**—IKE 정책의 상대 우선 순위는 1~65,535입니다. 우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다. 원격 IPsec 피어는 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위에 정의된 파라미터 사용을 시도합니다. 번호가 낮을수록 우선 순위가 높습니다.
- **Encryption(암호화)** - 2단계 협상 보호를 위한 1단계 SA(보안 연계)를 설정하는 데 사용되는 암호화 알고리즘입니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정을 참조하십시오.
- **Diffie-Hellman Group(Diffie-Hellman 그룹)** - 공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 파생하는 데 사용할 Diffie Hellman 그룹입니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. 옵션에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정을 참조하십시오.
- **Lifetime(라이프타임)**—SA(보안 연결)의 라이프타임(초)으로, 120~2147483647의 값이거나 비어 있습니다. 라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 특정 지점까지는 라이프타임이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다. 기본값은 86400입니다. 무제한 라이프타임을 지정하려면 아무 값도 입력하지 않고 필드를 비워 둡니다.
- **Authentication(인증)** - 두 피어 간에 사용할 인증 방법입니다. 자세한 내용은 사용할 인증 방법 결정을 참조하십시오.
  - **Preshared Key(사전 공유 키)** - 각 디바이스에 정의된 사전 공유 키를 사용합니다. 이 키를 사용하면 보안 키를 두 피어 간에 공유할 수 있으며 인증 단계 수행 시 IKE에서 보안 키를 사용할 수 있습니다. 동일한 사전 공유 키를 사용하여 피어를 구성하지 않으면 IKE SA를 설정할 수 없습니다.
  - **Certificate(인증서)** - 서로 식별할 피어에 대해 디바이스 ID 인증서를 사용합니다. Certificate Authority에서 각 피어를 등록하여 이 인증서를 가져와야 합니다. 또한 각 피어에서 ID 인증서 서명에 사용되는 신뢰할 수 있는 CA 루트 및 중간 CA 인증서를 업로드해야 합니다. 피어는 동일한 또는 다른 CA에 등록할 수 있습니다. 어느 피어든 간에 SSC(자가서명 인증서)를 사용할 수 없습니다.
- **Hash(해시)** - 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하기 위한 해시 알고리즘입니다. 옵션에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정을 참조하십시오.

단계 **5** **Add(추가)**를 클릭합니다.

IKEv2 정책 관리

IKEv2 정책 정보

IKE(Internet Key Exchange) 버전 2 정책 개체에는 VPN 연결을 정의할 때 IKEv2 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이

며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv2 정책이 있습니다. 필요에 맞는 정책이 있으면 State(상태) 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

Related Topics

IKEv2 정책 생성, 21 페이지

IKEv2 정책 생성

IKE(Internet Key Exchange) 버전 2 정책 개체에는 VPN 연결을 정의할 때 IKEv2 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv2 정책이 있습니다. 필요에 맞는 정책이 있으면 State(상태) 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 편집할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKEv2 Policy(**새 **IKEv2** 정책 생성**)** 링크를 클릭하여 사이트 간 VPN 연결에서 IKE 설정을 편집하면서 IKEv2 정책을 생성할 수도 있습니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 파란색 더하기  버튼을 클릭하고 **FTD** > **IKEv2 Policy(IKEv2** 정책**)**를 선택하여 새 IKEv2 정책을 생성합니다.
- 개체 페이지에서 편집할 IKEv2 정책을 선택하고 오른쪽의 Actions(작업) 창에서 **Edit(**편집**)**를 클릭합니다.

단계 **3** 개체 이름을 최대 128자로 입력합니다.

단계 **4** IKEv2 속성을 구성합니다.

- **Priority(**우선순위**)**—IKE 정책의 상대 우선 순위는 1~65,535입니다. 우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다. 원격 IPsec 피어는 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위에 정의된 파라미터 사용을 시도합니다. 번호가 낮을수록 우선 순위가 높습니다.
- **State(**상태**)** - IKE 정책이 활성화되어 있는지 여부입니다. 토글을 클릭하여 상태를 변경합니다. IKE 협상 중에는 활성화된 정책만 사용됩니다.
- **Encryption(**암호화**)** - 2단계 협상 보호를 위한 1단계 SA(보안 연계)를 설정하는 데 사용되는 암호화 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 단, 같은 정책에 혼합 모드(AES-GCM) 및 일반 모드 옵션을

둘 다 포함할 수는 없습니다. 일반 모드에서는 무결성 해시를 선택해야 하는 반면 혼합 모드에서는 개별 무결성 해시 선택이 금지됩니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정을 참조하십시오.

- **Diffie-Hellman Group(Diffie-Hellman** 그룹**)** - 공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 파생하는 데 사용할 Diffie Hellman 그룹입니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 그룹에서 가장 취약한 그룹 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 사용할 Diffie-Hellman 모듈러스 그룹 결정을 참조하십시오.

- **Integrity Hash(**무결성 해시**)** - 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하기 위한 해시 알고리즘의 무결성 부분입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. AES-GCM 암호화 옵션에서는 무결성 해시가 사용되지 않습니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정을 참조하십시오.

- **PRF(Pseudo-Random Function)** 해시 - 해시 알고리즘의 PRF(Pseudo Random Function) 부분으로, IKEv2 터널 암호화에 필요한 키 요소 및 해싱 작업을 파생시키기 위해 알고리즘으로 사용됩니다. IKEv1에서는 무결성 및 PRF 알고리즘이 구분되지 않지만 IKEv2에서는 이러한 요소에 대해 서로 다른 알고리즘을 지정할 수 있습니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정을 참조하십시오.

- **Lifetime(**라이프타임**)**—SA(보안 연결)의 라이프타임(초)으로, 120~2147483647의 값이거나 비어 있습니다. 라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 특정 지점까지는 라이프타임이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다. 기본값은 86400입니다. 무제한 라이프타임을 지정하려면 아무 값도 입력하지 않고 필드를 비워 둡니다.

단계 **5** **Add(**추가**)**를 클릭합니다.

IPsec 제안 정보

IPsec는 가장 안전하게 VPN 설정을 하는 방법 중 하나입니다. IPsec는 IP 패킷 레벨에서 데이터 암호화 기능을 제공하는 강력한 표준 기반 솔루션입니다. IPsec를 사용하는 경우 데이터는 터널을 통해 공용 네트워크를 사용하여 전송됩니다. 터널은 두 피어 간의 안전한 논리적 통신 경로입니다. IPsec 터널로 진입하는 트래픽은 보안 프로토콜 및 알고리즘이 조합된 변환 집합에 의해 보호됩니다. IPsec 보안 연계(SA) 협상 중에 피어는 두 피어에서 동일한 변환 집합을 검색합니다.

IKE 버전(IKEv1 또는 IKEv2)에 따라 각기 다른 IPsec 제안 개체가 있습니다.

- IKEv1 IPsec 제안을 생성할 때는 IPsec가 동작하는 모드를 선택하고 필요한 암호화 및 인증 유형을 정의합니다. 알고리즘에 대해서는 단일 옵션을 선택할 수 있습니다. VPN에서 여러 조합을 지원하려면 여러 IKEv1 IPsec 제안 개체를 생성하여 선택합니다.

- IKEv2 IPsec 제안을 생성할 때는 VPN에서 허용되는 모든 암호화 및 해시 알고리즘을 선택할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하

고 일치하는 항목을 찾을 때까지 피어와 협상합니다. 이를 통해 IKEv1과 마찬가지로 허용된 각 조합을 개별적으로 전송하는 대신 모든 허용된 조합을 전달하는 단일 제안서를 보낼 수 있습니다.

IKEv1 및 IKEv2 IPsec 제안에는 모두 ESP(Encapsulating Security Protocol)가 사용됩니다. ESP는 인증, 암호화 및 재생 방지 서비스를 제공합니다. ESP는 IP 프로토콜 유형 50입니다.

Note IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

다음 항목에서는 각 IKE 버전에 대해 IPsec 제안을 구성하는 방법을 설명합니다.

- IKEv1 IPsec 제안 개체 관리
- IKEv2 IPsec 제안 개체 관리

IKEv1 IPsec 제안 개체 관리

IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다. IKEv1과 IKEv2용으로 별도의 개체가 있습니다. 현재 CDO는 IKEv1 IPsec 제안 개체를 지원합니다.

IKEv1 및 IKEv2 IPsec 제안에는 모두 ESP(Encapsulating Security Protocol)가 사용됩니다. ESP는 인증, 암호화 및 재생 방지 서비스를 제공합니다. ESP는 IP 프로토콜 유형 50입니다.

Note IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

Related Topics

IKEv1 IPsec 제안 개체 생성, 23 페이지

IKEv1 IPsec 제안 개체 생성

IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다. IKEv1과 IKEv2용으로 별도의 개체가 있습니다. 현재 CDO는 IKEv1 IPsec 제안 개체를 지원합니다.

IKEv1 및 IKEv2 IPsec 제안에는 모두 ESP(Encapsulating Security Protocol)가 사용됩니다. ESP는 인증, 암호화 및 재생 방지 서비스를 제공합니다. ESP는 IP 프로토콜 유형 50입니다.

Note IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

여러 가지 사전 정의된 IKEv1 IPsec 제안이 있습니다. 새 제안을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 편집할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKEv1 Proposal(**새 **IKEv1** 제안 생성**)** 링크를 클릭하여 사이트 간 VPN 연결에서 IKEv1 IPsec 설정을 편집하면서 IKEv1 IPsec 제안 개체를 생성할 수도 있습니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 파란색 플러스 버튼  을 클릭하고 **FDM** > **IKEv1 IPsec Proposal(IKEv1 IPsec** 제안**)**을 선택하여 새 개체를 생성합니다.
- 개체 페이지에서 편집할 IPsec 제안을 선택하고 오른쪽의 작업 창에서 **Edit(**편집**)**를 클릭합니다.

단계 **3** 새 개체의 개체 이름을 입력합니다.

단계 **4** IKEv1 IPsec 제안 개체가 작동하는 모드를 선택합니다.

- 터널 모드에서는 전체 IP 패킷이 캡슐화됩니다. IPSec 헤더는 원본 IP 헤더와 새 IP 헤더 사이에 추가됩니다. 이는 기본값입니다. 방화벽 뒤에 배치되어 있는 호스트와 주고받는 트래픽을 방화벽이 보호하는 경우 터널 모드를 사용합니다. 터널 모드는 인터넷 등의 신뢰할 수 없는 네트워크를 통해 연결하는 두 방화벽 또는 기타 보안 게이트웨이 간에 일반 IPsec이 구현되는 통상적인 방식입니다.
- 전송 모드에서는 IP 패킷의 상위 레이어 프로토콜만 캡슐화됩니다. IPSec 헤더는 TCP 등의 상위 계층 프로토콜 헤더와 IP 헤더 사이에 삽입됩니다. 전송 모드에서는 소스 호스트와 대상 호스트가 모두 IPsec를 지원해야 합니다. 터널의 대상 피어가 IP 패킷의 최종 대상인 경우에만 전송 모드를 사용할 수 있습니다. 전송 모드는 대개 GRE, L2TP, DLSW 등의 레이어 2 또는 레이어 3 터널링 프로토콜을 보호할 때만 사용됩니다.

단계 **5** 이 제안에 대한 **ESP Encryption(ESP** 암호화**)**(Encapsulating Security Protocol) 알고리즘을 선택합니다. 자세한 내용은 사용할 암호화 알고리즘 결정을 참조하십시요.

단계 **6** 인증에 사용할 **ESP Hash(ESP** 해시**)** 또는 무결성 알고리즘을 선택합니다. 자세한 내용은 사용할 해시 알고리즘 결정을 참조하십시오.

단계 **7** **Add(**추가**)**를 클릭합니다.

IKEv2 IPsec 제안 개체 관리

IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다.

IKEv2 IPsec 제안을 생성할 때는 VPN에서 허용되는 모든 암호화 및 해시 알고리즘을 선택할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 일치하는 항목을 찾을 때까지 피어와 협상합니다. 이를 통해 IKEv1과 마찬가지로 허용된 각 조합을 개별적으로 전송하는 대신 모든 허용된 조합을 전달하는 단일 제안서를 보낼 수 있습니다.

Related Topics

IKEv2 IPsec 제안 개체 생성 또는 편집, 25 페이지

IKEv2 IPsec 제안 개체 생성 또는 편집

여러 가지 사전 정의된 IKEv2 IPsec 제안이 있습니다. 새 제안을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 편집할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 Create New IPsec Proposal(새 IPsec 제안 생성) 링크를 클릭하여 VPN 연결에서 IKEv2 IPsec 설정을 편집하면서 IKEv2 IPsec 제안 개체를 생성할 수도 있습니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 파란색 플러스 버튼  을 클릭하고 **FDM** > **IKEv2 IPsec Proposal(IKEv2 IPsec** 제안**)**을 선택하여 새 개체를 생성합니다.
- 개체 페이지에서 편집할 IPsec 제안을 선택하고 오른쪽의 작업 창에서 **Edit(**편집**)**를 클릭합니다.

단계 **3** 새 개체의 개체 이름을 입력합니다.

단계 **4** IKE2 IPsec 제안 개체 구성:

- **Encryption(**암호화**)** - 이 제안에 대한 ESP(Encapsulating Security Protocol) 암호화 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정을 참조하십시오.
- **Integrity Hash(**무결성 해시**)** - 인증에 사용할 해시 또는 무결성 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정을 참조하십시오.

단계 **5** **Add(**추가**)**를 클릭합니다.

ASA 사이트 간 가상 프라이빗 네트워크 모니터링

CDO를 사용하면 온보딩된 ASA 디바이스에서 이미 존재하는 사이트 간 VPN 구성을 모니터링할 수 있습니다. 사이트 간 구성을 수정하거나 삭제할 수 없습니다.

사이트 투 사이트 VPN 터널 연결 확인

Check Connectivity(연결 확인**)** 버튼을 사용하여 터널에 대한 실시간 연결 확인을 트리거하여 터널이 현재 사이트 간 VPN 터널 검색 및 필터링인지를 식별합니다. 온디맨드 연결 확인 버튼을 클릭하지 않으면 온보딩된 모든 디바이스에서 사용 가능한 모든 터널의 확인이 1시간에 한 번 수행됩니다.

Note

- CDO는 ASA에서 이 연결성 검사 명령을 실행하여 터널이 활성 상태인지 유휴 상태인지를 확인합니다.

  ```
  show vpn-sessiondb l2l sort ipaddress
  ```

- 모델 ASA 디바이스 터널은 항상 유휴로 표시됩니다.

VPN 페이지에서 터널 연결을 확인하려면 다음을 수행합니다.

Procedure

단계 **1** 왼쪽 창에서 VPN > ASA/FDM 사이트 간 VPN(ASA/FDM 사이트 간 VPN)를 클릭합니다.
단계 **2** 사이트 투 사이트 VPN 터널에 대한 터널 목록을 사이트 간 VPN 터널 검색 및 필터링하고 선택합니다.
단계 **3** 오른쪽의 작업 창에서 **Check Connectivity(**연결 확인**)**를 클릭합니다.

사이트 간 VPN 대시보드

CDO에서는 테넌트에서 생성된 사이트 간 VPN 연결에 대한 통합 정보를 제공합니다.

왼쪽 창에서 **Dashboard(**대시보드**)**를 클릭합니다. 사이트 간 **VPN**은 다음 위젯의 정보를 제공합니다.

- **Sessions and Insights(**세션 및 인사이트**)**: 활성 VPN 터널 및 유휴 VPN 터널을 나타내는 막대 그래프를 적절한 색상으로 표시합니다.
- **Issues(**문제**)**: 문제로 탐지된 총 터널 수를 표시합니다.
- **Pending Deploy(**구축 보류**)**: 보류 중인 구축이 있는 총 터널 수를 표시합니다.

원형 차트 또는 위젯의 링크를 클릭하면 선택한 값에 따라 필터가 적용된 사이트 간 VPN 목록 페이지가 표시됩니다. 예를 들어 **VPN** 터널 상태 위젯에서 **Active VPN Tunnels(**활성 **VPN** 터널**)**을 클릭하면 활성 상태 필터가 적용된 사이트 간 VPN 목록 페이지로 이동하며 활성 터널만 표시됩니다.

VPN 문제 식별

CDO는 ASA에서 VPN 문제를 식별할 수 있습니다. (이 기능은 아직 AWS VPC 사이트 투 사이트 VPN 터널에 사용할 수 없습니다.) 이 문서에서는 다음을 설명합니다.

- 누락된 피어가 있는 VPN 터널 찾기
- 암호화 키 문제가 있는 VPN 피어 찾기

- 터널에 대해 정의된 불완전하거나 잘못 구성된 액세스 목록 찾기
- 터널 구성에서 문제 찾기

터널 구성 문제 해결, on page 28

누락된 피어가 있는 VPN 터널 찾기

"Missing IP Peer" 상태는 FDM 관리 디바이스보다 ASA 디바이스에서 발생할 가능성이 높습니다.

Procedure

단계 1 왼쪽 창에서 **VPN** > **ASA/FDM Site-to-Site VPN(ASA/FDM** 사이트 간 **VPN)**를 클릭하여 VPN 페이지를 엽니다.

단계 2 **Table View(**테이블 보기**)**를 선택합니다.

단계 3 필터 아이콘을 클릭하여 필터 패널을 엽니다.

단계 4 감지된 문제를 확인합니다.

단계 5 문제를 보고하는 각 디바이스를 선택하고 오른쪽의 Peers(피어) 창을 확인합니다. 하나의 피어 이름이 나열됩니다. CDO는 다른 피어 이름을 "[Missing peer IP.]"로 보고합니다.

암호화 키 문제가 있는 VPN 피어 찾기

이 접근 방식을 사용하여 다음과 같은 암호화 키 문제가 있는 VPN 피어를 찾습니다.

- IKEv1 또는 IKEv2 키가 잘못되었거나 누락되었거나 일치하지 않습니다.
- 사용되지 않거나 낮은 암호화 터널

Procedure

단계 1 왼쪽 창에서 **VPN** > **ASA/FDM Site-to-Site VPN(ASA/FDM** 사이트 간 **VPN)**를 클릭하여 VPN 페이지를 엽니다.

단계 2 **Table View(**테이블 보기**)**를 선택합니다.

단계 3 필터 아이콘을 클릭하여 필터 패널을 엽니다.

단계 4 문제를 보고하는 각 디바이스를 선택하고 오른쪽의 Peers(피어) 창을 확인합니다. 피어 정보에는 두 피어가 모두 표시됩니다.

단계 5 디바이스 중 하나에 대해 **View Peers(**피어 보기**)**를 클릭합니다.

단계 6 Diagram View(다이어그램 보기)에서 문제를 보고하는 디바이스를 두 번 클릭합니다.

단계 7 하단의 Tunnel Details(터널 세부 정보) 창에서 **Key Exchange(**키 교환**)**를 클릭합니다. 두 디바이스를 모두 보고 해당 지점에서 주요 문제를 진단할 수 있습니다.

터널에 대해 정의된 불완전하거나 잘못 구성된 액세스 목록 찾기

"불완전하거나 잘못 구성된 액세스 목록" 상태는 ASA 디바이스에서만 발생할 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 **VPN** > **ASA/FDM Site-to-Site VPN(ASA/FDM** 사이트 간 **VPN)**를 클릭하여 VPN 페이지를 엽니다.

단계 **2** **Table View(**테이블 보기**)**를 선택합니다.

단계 **3** 필터 아이콘을 클릭하여 필터 패널을 엽니다.

단계 **4** 문제를 보고하는 각 디바이스를 선택하고 오른쪽의 Peers(피어) 창을 확인합니다. 피어 정보에는 두 피어가 모두 표시됩니다.

단계 **5** 디바이스 중 하나에 대해 **View Peers(**피어 보기**)**를 클릭합니다.

단계 **6** Diagram View(다이어그램 보기)에서 문제를 보고하는 디바이스를 두 번 클릭합니다.

단계 **7** 하단의 Tunnel Details(터널 세부 정보) 패널에서 **Tunnel Details(**터널 세부 정보**)**를 클릭합니다. "Network Policy: Incomplete(네트워크 정책: 완료되지 않음)" 메시지가 표시됩니다.

터널 구성에서 문제 찾기

터널 구성 오류는 다음 시나리오에서 발생할 수 있습니다.

- 사이트 투 사이트 VPN 인터페이스의 IP 주소가 변경되면 "피어 IP 주소 값이 변경되었습니다."
- VPN 터널의 IKE 값이 다른 VPN 터널과 일치하지 않으면 "IKE 값 불일치" 메시지가 나타납니다.

Procedure

단계 **1** 왼쪽 창에서 **VPN** > **ASA/FDM** 사이트 간 **VPN(ASA/FDM** 사이트 간 **VPN)**를 클릭하여 VPN 페이지를 엽니다.

단계 **2** **Table View(**테이블 보기**)**를 선택합니다.

단계 **3** 필터 아이콘을 클릭하여 필터 패널을 엽니다.

단계 **4** 터널 문제에서 탐지된 문제를 클릭하여 오류를 보고하는 VPN 구성을 봅니다. 구성 보고 문제를 볼 수 있습니다.

단계 **5** VPN 구성 보고 문제를 선택합니다.

단계 **6** 오른쪽의 피어 창에 문제가 있는 피어에 대한 아이콘이 나타납니다. 아이콘 위로 마우스를 가져가면 문제와 해결 방법을 볼 수 있습니다.

다음 단계: 터널 구성 문제 해결.

터널 구성 문제 해결

이 절차는 다음과 같은 터널 구성 문제를 해결하려고 시도합니다.

- 사이트 투 사이트 VPN 인터페이스의 IP 주소가 변경되면 "피어 IP 주소 값이 변경되었습니다."
- VPN 터널의 IKE 값이 다른 VPN 터널과 일치하지 않으면 "IKE 값 불일치" 메시지가 나타납니다.

자세한 내용은 터널 구성에서 문제 찾기를 참조하십시오.

프로시저

단계 **1** 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.
단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.
단계 **3** 적절한 디바이스 유형 탭을 클릭하고 문제를 보고하는 VPN 구성과 연결된 디바이스를 선택합니다.
단계 **4** 디바이스 변경 사항을 수락합니다.
단계 **5** 왼쪽 창에서, **VPN** > **ASA/FDM** 사이트 간 **VPN(**사이트 간 **VPN)**을 클릭하여 VPN 페이지를 엽니다.
단계 **6** 이 문제를 보고하는 VPN 구성을 선택합니다.
단계 **7** **Actions(**작업**)**창에서 **Edit**(편집) 아이콘을 클릭합니다.
단계 **8** 4단계에서 **Finish(**마침**)** 버튼을 클릭할 때까지 각 단계에서 **Next(**다음**)**를 클릭합니다.
단계 **9** 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.

사이트 간 VPN 터널 검색 및 필터링

필터 사이드바를 검색 필드와 함께 사용하여 VPN 터널 다이어그램에 표시된 VPN 터널 검색에 집중할 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 **VPN** > **ASA/FDM** 사이트 간 **VPN**를 클릭하여 VPN 페이지를 엽니다.
단계 **2** 필터 아이콘을 클릭하여 필터 창을 엽니다.
단계 **3** 다음 필터를 사용하여 검색을 구체화합니다.

- **Filter by Device(**디바이스별 필터링**) - Filter by Device(**디바이스별 필터링**)**를 클릭하고 디바이스 유형 탭을 선택한 후 필터링을 통해 찾으려는 디바이스를 선택합니다.
- **Tunnel Issues(**터널 문제**)** - 터널의 양쪽에 문제가 있음을 탐지했는지 여부입니다. 디바이스에 문제가 있는 몇 가지 예로는 연결된 인터페이스 또는 피어 IP 주소 또는 액세스 목록 누락, IKEv1 제안 불일치 등이 있습니다 (AWS VPC VPN 터널에서는 터널 문제 탐지를 아직 사용할 수 없음).
- **Devices/Services(**디바이스/서비스**)** -디바이스 유형을 기준으로 필터링합니다.
- **Status(**상태**)** – 터널 상태는 활성 또는 유휴 상태일 수 있습니다.

- **Active(활성)** - 네트워크 패킷이 VPN 터널을 통과하는 열린 세션이 있거나 성공적인 세션이 설정되었고 아직 시간 초과되지 않았습니다. Active(활성)는 터널이 활성 상태이고 관련성이 있음을 나타내는 데 도움이 될 수 있습니다.
- 유휴 - CDO는 이 터널에 대해 열려 있는 세션을 검색할 수 없습니다. 터널이 사용 중이 아니거나 이 터널에 문제가 있을 수 있습니다.

- **Onboarded(온보딩됨)** - CDO에서 디바이스를 관리하거나 CDO에서 관리하지 않을 수 있습니다(관리되지 않음).
  - **Managed(관리됨)** - CDO가 관리하는 디바이스별로 필터링합니다.
  - **Unmanaged(관리되지 않음)** - CDO가 관리하지 않는 디바이스로 필터링합니다.

- **Device Types(디바이스 유형)** - 터널의 한쪽이 라이브(연결된 디바이스) 디바이스인지 아니면 모델 디바이스인지 여부입니다.

단계 **4** 검색 창에 디바이스 이름 또는 IP 주소를 입력하여 필터링된 결과를 검색할 수도 있습니다. 검색은 대/소문자를 구분하지 않습니다.

관리되지 않는 사이트 간 VPN 피어 온보딩

CDO는 피어 중 하나가 온보딩될 때 사이트 간 VPN 터널을 검색 합니다. 두 번째 피어가 CDO에서 관리되지 않는 경우 VPN 터널 목록을 필터링하여 관리되지 않는 디바이스를 찾아 온보딩할 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 **VPN** > **ASA/FDM Site-to-Site VPN(ASA/FDM 사이트 간 VPN)**를 클릭하여 VPN 페이지를 엽니다.

단계 **2** **Table View(테이블 보기)**를 선택합니다.

단계 **3** 를 클릭하여 필터 패널을 엽니다.

단계 **4** **Unmanaged(관리되지 않음)**를 선택합니다.

단계 **5** 결과의 테이블에서 터널을 선택합니다.

단계 **6** 오른쪽의 **Peers(피어)** 창에서 **Onboard Device(온보드 디바이스)**를 클릭하고 화면의 지침을 따릅니다.

관련 정보**:**

- 디바이스 및 서비스 온보딩
- CDO에 ASA 디바이스 온보딩

사이트 투 사이트 VPN 터널의 IKE 개체 세부 정보 보기

선택한 터널의 피어/디바이스에 구성된 IKE 개체의 세부 정보를 볼 수 있습니다. 이러한 세부 정보는 IKE 정책 개체의 우선 순위에 따라 계층 구조의 트리 구조로 나타납니다.

Note 엑스트라넷 디바이스는 IKE 개체 세부 정보를 표시하지 않습니다.

Procedure

단계 **1** 왼쪽 창에서 **VPN** > **ASA/FDM Site-to-Site VPN(ASA/FDM** 사이트 간 **VPN)**를 클릭하여 VPN 페이지를 엽니다.

단계 **2** **VPN Tunnels(VPN** 터널**)** 페이지에서 피어를 연결하는 VPN 터널의 이름을 클릭합니다.

단계 **3** 오른쪽의 **Relationships(**관계**)** 아래에 세부 정보를 보려는 개체를 확장합니다.

마지막으로 성공한 사이트 투 사이트 VPN 터널 설정 날짜 보기

Procedure

단계 **1** 사이트 간 VPN 터널 정보 보기.

단계 **2** **Tunnel Details(**터널 세부 정보**)** 창를 클릭합니다.

단계 **3** **Last Seen Active(**마지막 확인한 활성**)** 필드를 확인합니다.

사이트 간 VPN 터널 정보 보기

사이트 간 VPN 테이블 보기는 CDO에 온보딩된 모든 디바이스에서 사용 가능한 모든 사이트 간 VPN 터널의 전체 목록입니다. 터널은 이 목록에 한 번만 존재합니다. 테이블에 나열된 터널을 클릭하면 추가 조사를 위해 터널의 피어로 직접 이동할 수 있는 옵션이 오른쪽 사이드바에 제공됩니다.

CDO가 터널의 양쪽을 모두 관리하지 않는 경우 관리되지 않는 사이트 간 VPN 피어 온보딩를 클릭하여 언매니지드 피어의 온보드 기본 온보딩 페이지를 열 수 있습니다. CDO가 터널의 양쪽을 모두 관리하는 경우 Peer 2(피어 2) 열에 매니지드 디바이스의 이름이 포함됩니다. 그러나 AWS VPC의 경우 Peer 2 열에 VPN 게이트웨이의 IP 주소가 포함됩니다.

테이블 보기에서 사이트 간 VPN 연결을 보려면 다음을 수행합니다.

Procedure

단계 **1** 왼쪽 창에서 **VPN** > **ASA/FDM Site-to-Site VPN(ASA/FDM** 사이트 간 **VPN)**를 클릭하여 VPN 페이지를 엽니다.

단계 2 **Table view(**테이블 보기**)** 버튼을 클릭합니다.

단계 3 사이트 간 VPN 터널 검색 및 필터링를 사용하여 특정 터널을 찾거나 전역 보기 그래픽을 확대하여 원하는 VPN 게이트웨이 및 해당 피어를 찾습니다.

사이트 투 사이트 **VPN** 전역 보기

Procedure

단계 1 왼쪽 창에서 다음을 클릭합니다. **VPN > ASA/FDM** 사이트 간 **VPN(**사이트 간 **VPN).**

단계 2 **Global view(**전역 보기**)** 버튼을 클릭합니다.

단계 3 사이트 간 VPN 터널 검색 및 필터링를 사용하여 특정 터널을 찾거나 전역 보기 그래픽을 확대하여 원하는 VPN 게이트웨이 및 해당 피어를 찾습니다.

단계 4 전역 보기에 표시된 피어 중 하나를 선택합니다.

단계 5 **View Details(**세부사항 보기**)**를 클릭합니다.

단계 6 VPN 터널의 다른 쪽 끝을 클릭하면 CDO에 해당 연결에 대한 Tunnel Details(터널 세부 정보), NAT Information(NAT 정보) 및 Key Exchange(키 교환) 정보가 표시됩니다.

- **Tunnel Details(**터널 세부 정보**)** - 터널에 대한 이름 및 연결 정보를 표시합니다. Refresh(새로 고침) 아이콘을 클릭하면 터널에 대한 연결 정보가 업데이트됩니다.
- **Tunnel Details specific to AWS connections(AWS** 연결 관련 터널 세부 정보**)** -AWS 사이트 투 사이트 연결에 대한 터널 세부 정보는 다른 연결과 약간 다릅니다. AWS VPC에서 VPN 게이트웨이로의 각 연결에 대해 AWS는 2개의 VPN 터널을 생성합니다. 이는 고가용성을 위한 것입니다.
  - 터널의 이름은 VPN 게이트웨이가 연결된 VPC의 이름을 나타냅니다. 터널에 이름이 지정된 IP 주소는 VPN 게이트웨이가 VPC로 인식하는 IP 주소입니다.
  - CDO 연결 상태가 **active(**활성**)**로 표시되면 AWS 터널 상태가 **Up(**가동 중**)**입니다. CDO 연결 상태가 **inactive(**비활성**)**인 경우 AWS 터널 상태는 **Down(**중단**)**입니다.
- **NAT Information(NAT** 정보**)** - 사용 중인 NAT 규칙의 유형, 원래 및 변환된 패킷 정보를 표시하고, 해당 터널에 대한 NAT 규칙을 볼 수 있는 NAT 테이블에 대한 링크를 제공합니다. (AWS VPC 사이트 투 사이트 VPN에는 아직 사용할 수 없습니다.)
- **Key Exchange(**키 교환**)** - 터널 및 키 교환 문제에서 사용 중인 암호화 키를 표시합니다. (AWS VPC 사이트 투 사이트 VPN에는 아직 사용할 수 없습니다.)

사이트 간 **VPN** 터널 창

Tunnels(터널) 창에는 특정 VPN 게이트웨이와 연결된 모든 터널의 목록이 표시됩니다. VPN 게이트웨이와 AWS VPC 간의 사이트 간 VPN 연결의 경우, tunnels(터널) 창에는 VPN 게이트웨이에서 VPC

로의 모든 터널이 표시됩니다. VPN 게이트웨이와 AWS VPC 간의 각 사이트 간 VPN 연결에는 2개의 터널이 있으므로 다른 디바이스에 대해 일반적으로 표시되는 터널 수가 두 배입니다.

VPN 게이트웨이 세부 정보

VPN 게이트웨이에 연결된 피어의 수 및 VPN 게이트웨이의 IP 주소를 표시합니다. 이는 VPN Tunnels(VPN 터널) 페이지에만 표시됩니다.

피어 보기

사이트 간 VPN 피어 쌍을 선택하면 Peers(피어) 창에 쌍의 두 디바이스가 나열되며 디바이스 중 하나에 대해 **View Peers(**피어 보기**)**를 클릭할 수 있습니다. **View Peers(**피어 보기**)**를 클릭하면 디바이스가 연결된 다른 사이트 간 피어가 표시됩니다. 이는 Table(테이블) 보기 및 Global(전역) 보기에 표시됩니다.

CDO 사이트 간 VPN 터널 삭제

Procedure

단계 **1** 탐색 창에서 **VPN** > 사이트 간 **VPN(**사이트 간 **VPN)**을 선택합니다.
단계 **2** 삭제할 원하는 사이트 투 사이트 VPN 터널을 선택합니다.
단계 **3** 오른쪽의 **Actions(**작업**)** 창에서 **Delete(**삭제**)**를 클릭합니다.

선택한 사이트 투 사이트 VPN 터널이 삭제됩니다.

원격 액세스 가상 프라이빗 네트워크 소개

사용자는 원격 액세스 VPN(원격 액세스 가상 프라이빗 네트워크) 기능을 통해 물리적 사무실 건물 외부의 위치에서 기업 네트워크에 연결할 수 있습니다. 즉, 사용자는 인터넷에 연결되어 있는 지원되는 iOS/ Android 디바이스 또는 컴퓨터를 사용하여 네트워크 리소스에 안전하게 액세스 수 있습니다. 이 기능은 데이터를 안전하게 보호하면서 홈 네트워크 또는 공용 Wifi 네트워크 에서 연결해야 하는 모바일 근무자에게 특히 유용합니다.

관련 정보**:**

- ASA에 대한 원격 액세스 가상 프라이빗 네트워크 구성, on page 33

ASA에 대한 원격 액세스 가상 프라이빗 네트워크 구성

ASA에서는 사용자에게 프라이빗 연결로 표시되는 TCP/IP 네트워크(예를 들어 인터넷)를 통해 보안 연결을 생성하여 원격 액세스 VPN(Virtual Private Network)을 생성합니다. 단일 사용자 -LAN(single-user-to-LAN) 연결 및 LAN-to-LAN 연결을 만들 수 있습니다.

보안 연결을 터널이라고 하며, ASA에서는 터널링 프로토콜을 사용하여 보안 파라미터를 협상하고, 터널을 생성하고 관리하며, 패킷을 캡슐화하고, 터널을 통해 패킷을 전송하거나 수신하고, 패킷의 캡슐화를 해제합니다. ASA에서는 양방향 터널 엔드포인트로서의 기능을 수행합니다. 플레인 패킷을 수신하고, 이를 캡슐화한 다음, 해당 패킷의 캡슐화가 해제되고 최종 대상으로 전송되는 터널의 다른 쪽 끝에 패킷을 전송합니다. ASA에서는 캡슐화된 패킷을 수신하고 해당 패킷의 캡슐화를 해제한 후 이를 최종 대상으로 전송할 수도 있습니다.

CDO는 새로운 원격 액세스 VPN을 구성하기 위한 직관적인 사용자 인터페이스를 제공합니다. 또한 CDO에 온보딩된 여러 ASA(Adaptive Security Appliance) 디바이스에 대한 원격 액세스 VPN 연결을 쉽고 빠르게 구성할 수 있습니다.

CDO를 사용하면 ASA 디바이스에서 원격 액세스 VPN 구성을 처음부터 구성할 수 있습니다. 또한 ASDM(Adaptive Security Defense Manager) 또는 CSM(Cisco Security Manager)과 같은 다른 ASA 관리 도구를 사용하여 이미 구성된 원격 액세스 VPN 설정을 관리할 수 있습니다. 이미 원격 액세스 VPN 설정이 있는 ASA 디바이스를 온보딩하는 경우 CDO는 자동으로 "기본 원격 액세스 VPN 구성"을 생성하고 ASA 디바이스를 이 구성과 연결합니다. 이 기본 구성은 디바이스에 정의된 모든 연결 프로파일 개체를 포함할 수 있습니다. CDO로 읽히는 원격 액세스 VPN 속성을 이해하려면 기존 ASA Remote Access VPN 설정 관리 및 구축 섹션을 참조하십시오. 그렇지 않으면 "ASA에 대한 엔드 투 엔드 원격 액세스 VPN 구성 프로세스" 섹션에 설명된 단계를 수행할 수 있습니다.

관련 정보:

- ASA에 대한 엔드 투 엔드 원격 액세스 VPN 구성 프로세스
  - ASA에 대한 ID 소스 구성
    - ASA Active Directory 영역 개체 생성
    - ASA RADIUS 서버 개체 또는 그룹 생성
  - ASA 원격 액세스 VPN 그룹 정책 생성, on page 41
  - ASA 원격 액세스 VPN 구성 생성, on page 49
  - ASA 원격 액세스 VPN 연결 프로파일 구성, on page 53
- 기존 ASA Remote Access VPN 설정 관리 및 구축
- IP 주소 풀 생성
- NAT에서 원격 액세스 VPN 트래픽 제외, on page 70
- ASA 원격 액세스 VPN 구성 검증
- ASA 원격 액세스 VPN 구성 세부 정보 보기

ASA에 대한 엔드 투 엔드 원격 액세스 VPN 구성 프로세스

이 섹션에서는 CDO에 온보딩된 ASA 디바이스에서 원격 액세스 VPN을 구성하는 엔드 투 엔드 절차를 제공합니다.

클라이언트에 대한 원격 액세스 VPN을 활성화하려면 여러 개의 개별 항목을 구성해야 합니다. 다음 절차에서는 이러한 엔드 투 엔드 프로세스를 제공합니다.

Procedure

단계 **1** 원격 사용자 인증에 사용되는 ID 소스를 구성합니다. 자세한 내용은 ASA에 대한 ID 소스 구성을 참조하십시오.

다음 소스를 사용하여 원격 액세스 VPN을 사용하여 네트워크에 연결을 시도하는 사용자를 인증할 수 있습니다. 또한 인증을 위해 클라이언트 인증서를 단독으로 또는 ID 소스와 함께 사용할 수 있습니다.

- AD(Active Directory) ID 영역: 기본 인증 소스로 사용됩니다. AD(Active Directory) 서버에서 사용자 어카운트가 정의됩니다. AD ID 영역 구성을 참조하십시오. ASA Active Directory 영역 개체 생성을 참조하십시오.
- RADIUS 서버 그룹: 기본 또는 보조 인증 소스로서, 권한 부여 및 계정 관리를 위한 것입니다. ASA RADIUS 서버 개체 또는 그룹 생성을 참조하십시오.
- Local Identity Source(로컬 사용자 데이터베이스): 기본 또는 대체 소스로 사용됩니다. 외부 서버를 사용하지 않고 디바이스에서 직접 사용자를 정의할 수 있습니다. 로컬 데이터베이스를 대체 소스로 사용하는 경우 외부 서버에 설명한 것과 같은 사용자 이름/비밀번호를 정의해야 합니다. 참고: ASDM(Adaptive Security Device Manager)에서만 ASA 디바이스에서 직접 사용자 계정을 생성할 수 있습니다. Cisco ASA Series Firewall ASDM 구성 가이드, XY의 개체 액세스 제어" 장에서 "로컬 사용자 그룹 구성" 섹션을 참조하십시오.

단계 **2** (선택 사항) ASA 원격 액세스 VPN 그룹 정책 생성, on page 41. 그룹 정책에서는 사용자와 관련된 속성을 정의합니다. 그룹 멤버십에 근거하여 리소스에 차등 액세스를 제공하도록 그룹 정책을 구성할 수 있습니다. 또는 모든 연결에 기본 정책을 사용합니다.

단계 **3** ASA 원격 액세스 VPN 구성 생성, on page 49.

단계 **4** ASA 원격 액세스 VPN 연결 프로파일 구성, on page 53.

단계 **5** (선택 사항) NAT에서 원격 액세스 VPN 트래픽 제외, on page 70.

단계 **6** 디바이스에 대한 구성 변경 사항 미리보고 구축합니다.

Important
ASDM(Adaptive Security Device Manager)과 같은 로컬 관리자를 사용하여 원격 액세스 VPN 구성을 변경하면 CDO에서 해당 디바이스의 구성 상태가 "Conflict Detected(충돌 탐지됨)"로 표시됩니다. ASA 디바이스의 대역외 변경 사항을 참조하십시오. 이 ASA에서 구성 충돌을 해결할 수 있습니다.

What to do next

다음 단계

원격 액세스 VPN 구성이 ASA 디바이스에 다운로드되면 사용자는 인터넷에 연결된 컴퓨터 또는 기타 지원되는 iOS 또는 Android 디바이스를 사용하여 원격 위치에서 네트워크에 연결할 수 있습니다. 테넌트의 모든 온보딩된 ASA 원격 액세스 VPN 헤드엔드에서 라이브 AnyConnect 원격 액세스 VPN 세션을 모니터링할 수 있습니다. 원격 액세스 가상 프라이빗 네트워크 세션을 참조하십시오.

ASA에 대한 ID 소스 구성

Microsoft Active Directory(AD) 영역 및 RADIUS 서버와 같은 ID 소스는 조직 내 사용자의 사용자 계정을 정의하는 AAA 서버 및 데이터베이스입니다. 이 정보는 IP 주소와 연결된 사용자 ID를 제공하거나, 원격 액세스 VPN 연결 또는 CDO 액세스를 인증하는 등 다양한 방식으로 사용할 수 있습니다.

개체를 클릭한 다음 (+)>**Identity Source(ID** 소스**)**를클릭하여 소스를 생성합니다. 그런 다음, ID 소스가 필요한 서비스를 구성할 때 이러한 개체를 사용할 수 있습니다. 적절한 필터를 적용하여 기존 소스를 검색하고 관리할 수 있습니다.

디렉터리 기본 *DN* 결정

디렉터리 속성을 구성할 때는 사용자와 그룹에 대한 공통 기본 DN(고유 이름)을 지정해야 합니다. 이 기준은 디렉터리 서버에서 정의되며 네트워크마다 다릅니다. 올바른 기준을 입력해야 ID 정책이 실행됩니다. 기준이 잘못된 경우 시스템이 사용자 또는 그룹 이름을 확인할 수 없으므로 ID 기반 정책이 실행될 수 없습니다.

Note 올바른 기준을 가져오려면 디렉터리 서버 담당 관리자에게 문의하십시오.

Active Directory의 경우 도메인 관리자로 Active Directory 서버에 로그인하여 다음과 같이 명령 프롬프트에 **dsquery** 명령을 사용해 기준을 확인하여 올바른 기준을 확인할 수 있습니다.

사용자 검색 기준

알려진 사용자 이름(부분 또는 전체)을 포함한 **dsquery user** 명령을 입력하여 기본 고유 이름을 확인합니다. 예를 들어 다음 명령은 부분 이름 "John*"를 사용하여 "John"으로 시작되는 모든 사용자에 대한 정보를 반환합니다.

C:\Users\Administrator>dsquery user -name "John*"

"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"

이 경우 기본 DN은 "DC=csc-lab,DC=example,DC=com"이 됩니다.

그룹 검색 기준

알려진 그룹 이름을 포함한 **dsquery group** 명령을 입력하여 기본 고유 이름을 확인합니다. 예를 들어 다음 명령은 그룹 이름 Employees를 사용하여 고유 이름을 반환합니다.

C:\>dsquery group -name "Employees"

"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"

이 경우 그룹 기본 DN은 “DC=csc-lab,DC=example,DC=com”이 됩니다.

ADSI 편집 프로그램을 사용하여 Active Directory 구조를 찾을 수도 있습니다(**Start(**시작**)** > **Run(**실행**)** > **adsiedit.msc**). ADSI 편집에서 조직 단위(OU), 그룹, 사용자 등의 개체를 마우스 오른쪽 단추로 클릭하고 **Properties(**속성**)**를 선택하여 고유 이름을 확인합니다. 그러면 DC 값 문자열을 기준으로 복사할 수 있습니다.

기준이 올바른지를 확인하려면 다음 단계를 수행합니다.

Procedure

단계 **1** 디렉터리 속성의 Test Connection(연결 테스트) 버튼을 클릭하여 연결을 확인합니다. 모든 문제를 해결하고 디렉터리 속성을 저장합니다.

단계 **2** 디바이스에 변경 사항을 커밋합니다.

단계 **3** 액세스 규칙을 생성하고 **Users(**사용자**)** 탭을 선택한 다음 디렉터리에서 알려진 사용자 및 그룹 이름을 추가해 봅니다. 디렉터리가 포함된 영역에서 일치하는 사용자 및 그룹을 입력하면 자동 완성 제안 사항이 표시됩니다. 이러한 제안 사항이 드롭다운 목록에 표시되는 경우 시스템이 디렉터리를 정상적으로 쿼리한 것입니다. 입력한 문자열이 사용자 또는 그룹 이름에 포함되어 있는데 제안 사항이 표시되지 않으면 해당하는 검색 기준을 편집해야 합니다.

What to do next

자세한 내용은 ASA Active Directory 영역 개체 생성을 참조하십시오.

RADIUS 서버 및 그룹

RADIUS 서버를 사용하여 관리 사용자를 인증하고 권한을 부여할 수 있습니다. RADIUS 서버를 사용하도록 기능을 구성할 때는 개별 서버 대신 RADIUS 그룹을 선택합니다. RADIUS 그룹은 서로의 복사본인 RADIUS 서버가 모인 컬렉션입니다. 그룹에 서버가 여러 개 포함된 경우 이러한 서버는 백업 서버 체인을 형성하여 한 서버를 사용할 수 없는 경우 이중화를 제공합니다. 하지만 서버가 하나뿐이더라도 멤버가 하나인 그룹을 생성하여 기능에 대한 RADIUS 지원을 구성해야 합니다.

이 소스는 다음과 같은 목적으로 사용할 수 있습니다.

- 인증용 ID 소스이자 권한 부여 및 과금 용도의 원격 액세스 VPN. AD를 RADIUS 서버와 함께 사용할 수 있습니다.
- ID 정책(원격 액세스 VPN 로그인에서 사용자 ID를 수집하기 위한 패시브 ID 소스로 사용)

자세한 내용은 ASA RADIUS 서버 개체 또는 그룹 생성을 참조하십시오.

ASA Active Directory 영역 개체 생성

AD 영역 개체와 같은 ID 소스 개체를 생성하거나 편집할 때 CDO는 SDC를 통해 ASA 디바이스에 구성 요청을 보냅니다. 그런 다음 ASA는 구성된 AD 영역과 통신합니다.

개체를 생성하려면 다음 절차를 따르십시오.

프로시저

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** **Create Object(**개체 생성**)** (+) **RA VPN Objects(**개체**) (ASA & FDM)** > **Identity Source(ID** 소스**)**를 클릭합니다.

단계 **3** 개체의 **Object name(**개체 이름**)**을 입력합니다.

단계 **4** **Device Type(**장치 유형**)**을 **ASA**로 선택합니다.

단계 **5** 마법사의 첫 번째 부분에서 **ID** 소스 유형으로 **Active Directory** 영역을 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **6** 기본 영역 속성을 구성합니다.

- 디렉터리 사용자 이름**,** 디렉터리 암호- 검색하려는 사용자 정보에 대한 적절한 권한이 있는 사용자의 고유한 사용자 이름과 암호입니다. Active Directory의 경우에는 사용자에게 상승된 권한이 필요하지 않습니다. 도메인에 어떤 사용자라도 지정할 수 있습니다. 사용자 이름은 정규화되어야 합니다. 예를 들어 Administrator@example.com(단순히 Administrator가 아님)입니다.

  참고
  시스템은 이 정보에서 ldap-login-dn 및 ldap-login-password를 생성합니다. 예를 들어 Administrator@example.com은 cn=administrator,cn=users,dc=example,dc=com으로 변환됩니다. cn=users는 항상 이 변환의 일부이므로 여기에서 일반 이름 "users" 폴더 아래에 지정하는 사용자를 구성해야 합니다.

- **Base Distinguished Name(**기본 고유 이름**)** - 사용자 및 그룹 정보를 검색하거나 조회하기 위한 디렉토리 트리, 즉 사용자 및 그룹의 공통 상위. cn=users,dc=example,dc=com을 예로 들 수 있습니다.

단계 **7** 디렉터리 서버 속성을 구성합니다.

- **Hostname/IP Address(**호스트 이름**/IP** 주소**)** - 디렉터리 서버의 호스트 이름 또는 IP 주소입니다. 서버에 대한 암호화된 연결을 사용하는 경우에는 IP 주소가 아닌 FQDN(Fully-Qualified Domain Name)을 입력해야 합니다.
- **Port(**포트**)** - 서버와의 통신에 사용되는 포트 번호입니다. 기본값은 389입니다. 암호화 방법으로 LDAPS를 선택하는 경우에는 포트 636을 사용합니다.
- 암호화- 사용자 및 그룹 정보를 다운로드하기 위해 암호화된 연결을 사용하려면 **LDAPS**를 선택하여 SSL을 사용하여 ASA와 LDAP 서버 간의 통신을 보호합니다. SSL을 통한 LDAP가 필요합니다. 이 옵션은 포트 636을 사용합니다.

  기본값은 **None(**없음**)**입니다. 이 옵션은 사용자 및 그룹 정보를 일반 텍스트로 다운로드함을 의미합니다.

단계 **8** (선택 사항) **Test(**테스트**)** 버튼을 사용하여 구성을 확인합니다.

단계 **9** (선택 사항) AD(Active Directory) 영역에 여러 AD 서버를 추가하려면 **Add another configuration(**다른 구성 추가**)**를 클릭합니다. 이 AD 서버들은 서로의 중복이어야 하고 동일한 AD 도메인을 지원해야 합니다. 따라서 디렉터리 이름, 디렉터리 암호 및 기본 고유 이름과 같은 기본 영역 속성은 해당 AD 영역과 연결된 모든 AD 서버에서 동일해야 합니다.

단계 **10** **Add(**추가**)**를 클릭합니다.

ASA Active Directory 영역 개체 편집

ID 소스 개체를 편집할 때는 ID 소스 유형을 변경할 수 없습니다. 올바른 유형으로 새 개체를 생성해야 합니다.

프로시저

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.

단계 **3** 편집할 개체를 선택합니다.

단계 **4** 세부정보 패널의 **Actions(**작업**)** 창에서 편집 아이콘 를 클릭합니다.

단계 **5** 위의 절차에서 만든 것과 같은 방식으로 대화 상자에서 값을 편집합니다. 아래 나열된 구성 표시줄을 확장하여 호스트 이름/IP 주소 또는 암호화 정보를 편집하거나 테스트합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

단계 **7** CDO에 변경의 영향을 받을 정책이 표시됩니다. **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

단계 **8** 지금 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

ASA RADIUS 서버 개체 또는 그룹 생성

When you create or edit an identity source object such as a RADIUS server object or a group of RADIUS server objects, CDO sends the configuration request to ASA devices through the SDC.

ASA RADIUS 서버 개체 생성

RADIUS 서버는 AAA(인증, 권한 부여 및 계정 관리) 서비스를 제공합니다.

개체를 생성하려면 다음 절차를 따르십시오.

Procedure

단계 **1** 왼쪽 CDO 탐색 모음에서 개체를 클릭합니다.

단계 **2** **Create Object(**개체 생성**)** ( )**> RA VPN Objects(**개체**) (ASA & FDM)** > **Identity Source(ID** 소스**)**를 클릭합니다.

단계 **3** 개체의 **Object name(**개체 이름**)**을 입력합니다.

단계 **4** **Device Type(**장치 유형**)**을 **ASA**로 선택합니다.

단계 **5** **ID** 소스 유형으로 **RADIUS Server Group(RADIUS** 서버 그룹**)** 을 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **6** 다음 속성을 사용하여 ID 소스 구성을 편집합니다.

- **Server Name or IP Address(**서버 이름 또는 **IP** 주소**)** - 서버의 정규화된 호스트 이름(FQDN) 또는 IP 주소입니다.
- **Authentication Port(**인증 포트**)**(선택 사항) - RADIUS 인증 및 권한 부여가 수행되는 포트입니다. 기본값은 1,812입니다.

- **Timeout(**시간 제한**)** - 시스템이 다음 서버로 요청을 보내기 전까지 서버의 응답을 기다리는 시간(1~300초)입니다. 기본값은 10초입니다.
- **Server Secret Key(**서버 비밀 키**)**입력(선택 사항) - ASA 디바이스와 RADIUS 서버 간에 데이터를 암호화하는 데 사용되는 공유 비밀입니다. 이 키는 대/소문자를 구분하며 공백은 포함하지 않는 영숫자 문자열(최대 64자)입니다. 또한 영숫자 문자 또는 밑줄로 시작해야 하며 특수 문자 $ & - _ . + @는 포함할 수 없습니다. 문자열은 RADIUS 서버에 구성된 것과 일치해야 합니다. 비밀 키를 구성하지 않으면 연결이 암호화되지 않습니다.

단계 **7** **Add(**추가**)**를 클릭합니다.

단계 **8** 지금 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

ASA RADIUS 서버 그룹 생성

RADIUS 서버 그룹은 하나 이상의 RADIUS 서버 개체를 포함합니다. 그룹 내의 서버는 서로의 복사본이어야 합니다. 이러한 서버는 백업 서버 체인을 형성하므로 첫 번째 서버를 사용할 수 없는 경우 시스템이 목록의 다음 서버 사용을 시도할 수 있습니다.

개체 그룹을 생성하려면 다음 절차를 따르십시오.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** **Create Object(**개체 생성**)** (+) **RA VPN Objects(**개체**) (ASA & FDM)Identity Source(ID** 소스**)**를 클릭합니다.

단계 **3** 개체의 **Object name(**개체 이름**)**을 입력합니다.

단계 **4** **Device Type(**장치 유형**)**을 **ASA**로 선택합니다.

단계 **5** ID 소스 유형으로 **RADIUS Server (RADIUS** 서버**) Group(**그룹**)**을 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **6** 다음 속성을 사용하여 ID 소스 구성을 편집합니다.

- 데드 타임 - 실패한 서버는 모든 서버가 실패한 후에만 재활성화됩니다. 데드 시간은 모든 서버를 다시 활성화하기 전에 마지막 서버가 실패한 후 대기하는 시간입니다.
- **Maximum Failed Attempts(**최대 실패 시도 횟수**)** - 다음 서버 사용을 시도하기 전에 그룹의 RADIUS 서버로 전송되었으나 실패한 요청(즉, 응답을 받지 못한 요청)의 수입니다. 최대 실패 시도 횟수가 초과되면 시스템에서 해당 서버를 Failed(장애 발생)로 표시합니다. 특정 기능에 대해 로컬 데이터베이스를 사용하여 대체 방법을 구성했는데 그룹의 모든 서버가 응답하지 않으면 해당 그룹은 응답이 없는 것으로 간주되고 대체 방법을 시도합니다. 서버 그룹은 데드 타임 동안 응답하지 않는 것으로 표시된 상태를 유지하므로 해당 기간 내의 추가 AAA 요청은 서버 그룹에 연결을 시도하지 않으며 폴백 방법이 즉시 사용됩니다.
- **Dynamic Authorization/Port(**동적 인증/포트**) (**선택사항**)** - RADIUS 동적 인증 또는 이 RADIUS 서버 그룹에 대한 CoA(Change of Authorization) 서비스를 활성화할 경우, 해당 그룹은 CoA 알림이 등록되며 Cisco ISE(Identity Services Engine)의 CoA 정책 업데이트를 위해 지정된 포트를 수신합니다. ISE와 함께 원격 액세스 VPN에서 이 서버 그룹을 사용하는 경우에만 동적 인증을 활성화합니다.

단계 **7** 드롭다운 메뉴에서 RADIUS 서버를 지원하는 AD 영역을 선택합니다. AD 영역을 아직 생성하지 않은 경우 드롭다운 메뉴에서 **Create(**생성**)**를 클릭합니다.

단계 **8** 기존 RADIUS 서버 개체를 추가하려면 **RADIUS SERVER Add(RADIUS** 서버 추가**)**  버튼을 클릭합니다. 선택 사항으로 이 창에서 새 RADIUS 서버 개체를 만들 수 있습니다.

Note
목록의 첫 번째 서버가 응답하지 않을 때까지 사용되므로 이러한 개체를 우선 순위에 추가하십시오. 그런 다음 ASA는 목록의 다음 서버로 기본 설정됩니다.

단계 **9** 지금 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

ASA Radius 서버 개체 또는 그룹 편집

Radius 서버 개체 또는 Radius 서버 그룹을 편집하려면 다음 절차를 따르십시오.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.

단계 **3** 편집할 개체를 선택합니다.

단계 **4** 세부정보 패널의 **Actions(**작업**)** 창에서 편집 아이콘  를 클릭합니다.

단계 **5** 위의 절차에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 편집합니다. 호스트 이름/IP 주소 또는 암호화 정보를 편집하거나 테스트하려면 구성 표시줄을 확장합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

단계 **7** CDO에 변경의 영향을 받을 정책이 표시됩니다. **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

단계 **8** 지금 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

ASA 원격 액세스 **VPN** 그룹 정책 생성

그룹 정책은 원격 액세스 VPN 연결을 위한 사용자 중심 속성/값 쌍의 집합입니다. 연결 프로파일은 터널이 설정된 이후에 사용자 연결을 위한 조건을 설정하는 그룹 정책을 사용합니다. 그룹 정책을 사용하면 각 사용자에 대해 개별적으로 각 특성을 지정할 필요 없이 사용자 또는 사용자 그룹에 전체 특성 집합을 적용할 수 있습니다.

시스템에는 "DfltGrpPolicy"라는 이름의 기본 그룹 정책이 포함되어 있습니다. 필요한 서비스를 제공하는 추가 그룹 정책을 만들 수 있습니다.

참고 일치하지 않는 그룹 정책 개체를 원격 액세스 VPN 구성에 추가할 수 없습니다. 원격 액세스 VPN 구성 그룹 정책을 추가하기 전에 모든 불일치를 해결하십시오.

프로시저

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 파란색 더하기 버튼을 클릭합니다.

단계 **3** **RA VPN Objects (ASA & FTD)(RA VPN** 개체 **(ASA** 및 **FDM))** > **RA VPN Group Policy(RA VPN** 그룹 정책**)**를 클릭합니다.

단계 **4** 그룹 정책의 이름을 입력합니다. 이름은 최대 64자까지 입력할 수 있고 공백이 허용됩니다.

단계 **5** **Device Type(**디바이스 유형**)** 드롭다운에서 **ASA**를 선택합니다.

단계 **6** 다음 중 하나를 수행합니다.

- 필요한 탭을 클릭하고 페이지에서 속성을 구성합니다.
  - ASA 원격 액세스 VPN 그룹 정책 속성
  - AnyConnect 클라이언트 프로파일, 43 페이지
  - 세션 설정 속성, 44 페이지
  - 주소 할당 속성, 44 페이지
  - 스플릿 터널링 속성, 45 페이지
  - AnyConnect 속성, 46 페이지
  - 트래픽 필터 속성, 48 페이지
  - Windows 브라우저 프록시 속성, 48 페이지

단계 **7** **Save(**저장**)**를 클릭하여 그룹 정책을 생성합니다.

ASA 원격 액세스 *VPN* 그룹 정책 속성

이 섹션에서는 ASA 원격 액세스 VPN 그룹 정책과 관련된 속성에 대해 설명합니다.

일반 속성

그룹 정책의 일반 속성에서는 그룹의 이름 및 기타 기본 설정을 정의합니다.

- **DNS Server(DNS** 서버**)**: VPN에 연결된 경우 도메인 이름 확인을 위한 DNS 서버의 IP 주소를 입력합니다. 쉼표를 사용하여 주소를 구분할 수 있습니다.

- **Banner(**배너**)**: 로그인 시 사용자에게 표시할 배너 텍스트 또는 환영 메시지입니다. 기본값은 배너 없음입니다. 길이는 최대 496자까지 가능합니다. AnyConnect 클라이언트에서는 부분 HTML을 지원합니다. 원격 사용자에게 배너가 적절히 표시되게 하려면
 태그를 사용하여 줄 바꿈을 나타냅니다.
- **Default Domain(**기본 도메인**)**: 원격 액세스 VPN의 사용자에 대한 기본 도메인 이름입니다. example.com 등을 예로 들 수 있습니다. 이 도메인은 정규화되지 않은 호스트 이름(예: serverA.example.com이 아닌 serverA)에 추가됩니다.

AnyConnect 클라이언트 프로파일

이 기능은 소프트웨어 버전 6.7 이상을 실행하는 FTD에서 지원됩니다.

Cisco AnyConnect VPN 클라이언트는 다양한 내장 모듈을 통해 향상된 보안을 제공합니다. 이러한 모듈은 웹 보안, 엔드 포인트 플로우에 대한 네트워크 가시성, 네트워크 외부 로밍 보호와 같은 서비스를 제공합니다. 각 클라이언트 모듈에는 요구 사항에 따라 사용자 지정 구성 그룹이 포함된 클라이언트 프로파일이 포함되어 있습니다.

VPN 사용자가 VPN AnyConnect 클라이언트 소프트웨어를 다운로드할 때 클라이언트에 다운로드할 AnyConnect VPN 프로파일 개체 및 AnyConnect 모듈을 선택할 수 있습니다.

1. AnyConnect VPN 프로파일 개체를 선택하거나 생성합니다. RA VPN AnyConnect 클라이언트 프로파일 업로드, on page 73의 내용을 참조하십시오. DART 및 Start Before Login(로그인 전 시작) 모듈을 제외하고 AnyConnect VPN 프로파일 개체를 선택해야 합니다.
2. **Add Any Connect Client Module(**모든 연결 클라이언트 모듈 추가**)**을 클릭합니다.

   다음 AnyConnect 모듈은 선택 사항이며 이러한 모듈을 VPN AnyConnect 클라이언트 소프트웨어와 함께 다운로드하도록 구성할 수 있습니다.

   - **AMP Enabler** — 엔드포인트용 AMP(Advanced Malware Protection)를 구축합니다.
   - **DART** — 시스템 로그 및 기타 진단 정보를 캡처하여 데스크톱에 .zip 파일을 만듭니다. 따라서 편리하게 Cisco TAC로 문제 해결 정보를 보낼 수 있습니다.
   - **Feedback(**피드백**)** - 고객이 활성화하고 사용한 기능 및 모듈에 대한 정보를 제공합니다.
   - **ISE Posture**: OPSWAT v3 라이브러리를 사용하여 엔드포인트의 컴플라이언스를 평가하기 위한 상태 확인을 수행합니다.
   - **Network Access Manager** - 802.1X(계층 2)와 유선 및 무선 네트워크에 액세스하기 위한 디바이스 인증을 제공합니다.
   - **Network Visibility(**네트워크 가시성**)** — 용량 및 서비스 계획, 감사, 컴플라이언스 및 보안 분석을 수행하기 위한 엔터프라이즈 관리자의 역량을 개선합니다.
   - **Start Before Login(**로그인 전 시작**)** - Windows 로그인 대화 상자가 나타나기 전에 AnyConnect를 시작하여 Windows에 로그온하기 전에 VPN 연결을 통하여 사용자를 엔터프라이즈 인프라에 연결시킵니다.
   - **Umbrella** 로밍 보안 — 활성 VPN이 없을 때 DNS 레이어 보안을 제공합니다.

- 웹 보안 - 정의된 보안 정책에 따라 웹 페이지의 요소를 분석하고 허용되는 콘텐츠를 허용하며 악성 또는 허용되지 않는 콘텐츠를 차단합니다.

3. 클라이언트 모듈 목록에서 **AnyConnect** 모듈을 선택합니다.
4. **Profile(**프로파일**)** 목록에서 AnyConnect 클라이언트 프로파일을 포함하는 프로파일 개체를 선택하거나 생성합니다.
5. 프로파일과 함께 클라이언트 모듈을 다운로드하려면 **Enable Module Download(**모듈 다운로드 활성화**)**를 선택하여 엔드포인트를 활성화합니다. 선택하지 않으면 엔드포인트는 클라이언트 프로파일만 다운로드할 수 있습니다.

세션 설정 속성

그룹 정책의 세션 설정에서는 사용자가 VPN을 통해 연결할 수 있는 시간과 설정할 수 있는 별도 연결의 개수를 제어합니다.

- **Maximum Connection Time(**최대 연결 시간**)**: 사용자가 로그아웃했다가 다시 연결하지 않고 VPN에 연결된 상태를 유지할 수 있는 최대 시간을 1~4473924(분)로 입력하거나 비워 둡니다. 기본값은 무제한(비워 둠)이지만 유휴 시간 제한은 계속 적용됩니다.
- **Connection Time Alert Interval(**연결 시간 알림 간격**)**: 최대 연결 시간을 지정하는 경우, 알림 간격에서는 사용자에게 앞으로 다가올 자동 연결 해제에 관해 경고를 표시하기까지 지나야 할 최대 시간을 정의합니다. 사용자는 연결 종료를 선택하고 다시 접속해 타이머를 다시 시작할 수 있습니다. 기본값은 1분입니다. 1분에서 30분까지 지정할 수 있습니다.
- **Idle Time(**유휴 시간**)**: VPN 연결이 자동으로 종료될 때까지 유휴 상태일 수 있는 시간을 1~35791394(분) 범위 내로 입력합니다. 이 연속되는 분 단위 시간 동안 연결에서 통신 활동이 없는 경우, 시스템에서는 연결을 중지합니다. 기본값은 30분입니다.
- **Idle Time Alert Interval(**유휴 시간 알림 간격**)**: 유휴 세션으로 인해 사용자에게 앞으로 다가올 자동 연결 해제에 관해 경고를 표시하기까지 지나야 할 유휴 시간입니다. 어떤 활동에서도 타이머를 재설정할 수 있습니다. 기본값은 1분입니다. 1분에서 30분까지 지정할 수 있습니다.
- **Simultaneous Login Per User(**사용자당 동시 로그인 수**)**: 한 사용자에게 허용되는 동시 연결의 최대 개수입니다. 기본값은 3입니다. 1~2147483647개의 연결을 지정할 수 있습니다. 다수의 동시 연결을 허용하면 보안이 취약해지고 성능이 저하될 수 있습니다.

주소 할당 속성

그룹 정책의 주소 할당 속성에서는 그룹에 대해 IP 주소 풀을 정의합니다. 여기에 정의된 풀은 이 그룹을 사용하는 모든 연결 프로파일에 정의된 풀을 재정의합니다. 연결 프로파일에 정의된 풀을 사용하려면 이러한 설정을 비워둡니다.

- **IPv4 Address Pool(IPv4** 주소 풀**), IPv6 Address Pool(IPv6** 주소 풀**)**: 이 옵션에서는 원격 엔드포인트의 주소 풀을 정의합니다. 클라이언트가 VPN 연결을 설정하는 데 사용하는 IP 버전에 따라 이러한 풀의 주소가 클라이언트에 할당됩니다. 지원하려는 각 IP 유형에 대한 서브넷을 정의하는 IP 주소 풀을 선택합니다. 해당 IP 버전을 지원하고 싶지 않은 경우, 목록을 비워두십시오. 예를 들어 IPv4 풀을 10.100.10.0/24로 정의할 수 있습니다. 주소 풀은 외부 인터페이스의 IP 주소와

동일한 서브넷에 있을 수 없습니다. 새 IP 주소 풀 생성을 생성합니다. 로컬 주소 할당에 사용할 최대 6개의 주소 풀로 구성된 목록을 지정할 수 있습니다. 풀을 지정하는 순서는 중요합니다. 시스템에서는 풀이 표시되는 순서에 따라 이 풀에서 주소를 할당합니다. 참고: 동일한 그룹 정책에 대해 IPv4 주소 풀과 IPv6 주소 풀을 둘 다 구성할 수 있습니다. 동일한 그룹 정책에 두 버전의 IP 주소가 모두 구성된 경우 IPv4에 대해 구성된 클라이언트는 IPv4 주소를 가져오고 IPv6에 대해 구성된 클라이언트는 IPv6 주소를 가져오며 IPv4 주소와 IPv6 주소 둘 다에 대해 구성된 클라이언트는 IPv4 주소와 IPv6 주소를 둘 다 가져옵니다.

- **DHCP Scope(DHCP 범위)**: 연결 프로파일에서 주소 풀에 대한 DHCP 서버를 컨피그레이션하는 경우, DHCP 범위에서는 이 그룹에 대한 풀에 사용할 서브넷을 식별합니다. 또한 DHCP 서버 주소에는 해당 범위에서 식별하는 동일한 풀에 주소가 있어야 합니다. 이 범위를 통해 사용자는 DHCP 서버에 정의된 주소 풀의 하위 집합을 선택하여 이 특정 그룹에 사용할 수 있습니다. 네트워크 범위를 정의하지 않으면 DHCP 서버에서 구성된 주소 풀 순으로 IP 주소를 할당합니다. 할당되지 않은 주소를 식별할 때까지 풀을 검색합니다. 범위를 지정하려면 네트워크 번호 호스트 주소를 포함하는 네트워크 개체를 입력합니다. 예를 들어 192.168.5.0/24 서브넷 풀에서 주소를 사용하도록 DHCP 서버에 지시하려면 192.168.5.0을 호스트 주소로 지정하는 네트워크 개체를 입력하십시오. IPv4 주소 지정에만 DHCP를 사용할 수 있습니다.

스플릿 터널링 속성

그룹 정책의 스플릿 터널링 속성에서는 내부 네트워크로 가는 트래픽과 외부로 가는 트래픽을 시스템에서 각각 분별하여 처리하는 방식을 정의합니다. 스플릿 터널링은 일부 네트워크 트래픽이 VPN 터널(암호화됨)을 통과하도록 유도하고 나머지 네트워크 트래픽은 VPN 터널 외부(암호화되지 않음 또는 일반 텍스트 형식)로 보냅니다.

일반적으로 원격 액세스 VPN에서는 VPN 사용자가 디바이스를 통해 인터넷에 액세스하도록 할 수 있습니다. 그러나 VPN 사용자가 원격 액세스 VPN에 연결되어 있는 동안 외부 네트워크에 액세스하도록 허용할 수 있습니다. 이 기술을 스플릿 터널링 또는 헤어피닝이라고도 합니다. 스플릿 터널을 이용하면 보안 터널을 통한 원격 네트워크 VPN 연결이 가능하며, VPN 터널 외부의 네트워크에도 연결할 수 있습니다. 스플릿 터널링은 FTD 디바이스의 네트워크 부하를 줄이고 외부 인터페이스의 대역폭을 늘립니다.

시작하기 전에

IPv4 네트워크에 대해 스플릿 터널 정책을 생성하고 IPv6 네트워크에 대해 다른 스플릿 터널 정책을 생성하는 경우, 지정한 액세스 목록이 두 가지 프로토콜 모두에 사용됩니다. 따라서 액세스 목록은 IPv4 및 IPv6 트래픽에 대한 ACE(Access Control Entries: 액세스 제어 항목)를 포함해야 합니다.

ASA 디바이스가 CDO에 온보딩되면 디바이스와 연결된 확장 ACL을 읽습니다. 자세한 내용은 그룹 정책 을 참조하십시오. 새 ACL을 생성하려면 ASA Lists(ASA 목록)을 참조하십시오.

Note 생성 중인 ACL에서 스플릿 터널링을 위한 네트워크를 소스 네트워크로 지정해야 합니다.

- **IPv4 Split Tunneling(IPv4 스플릿 터널링)**, **IPv6 Split Tunneling(IPv6 스플릿 터널링)**: 트래픽에서 IPv4와 IPv6 중 어떤 주소 지정을 사용하는지에 따라 다른 옵션을 지정할 수 있지만, 각각의

경우 옵션은 동일합니다. 스플릿 터널링을 활성화하려는 경우, 네트워크 개체를 선택해야 하는 옵션 중 하나를 지정합니다.

- **Allow all traffic over tunnel(**터널을 지나는 모든 트래픽 허용**)**: 스플릿 터널링은 실행하지 마십시오. 사용자가 원격 액세스 VPN 연결을 하면 사용자의 모든 트래픽은 보호된 터널을 통과합니다. 이는 기본값입니다. 또한 이 기본값은 가장 안전한 옵션으로 간주됩니다.
- **Allow specified traffic over the tunnel(**터널을 통해 지정된 트래픽 허용**)**: 소스 네트워크를 정의하는 확장 액세스 목록을 선택합니다. 이러한 소스의 모든 트래픽은 보호된 터널을 통과합니다. 클라이언트는 다른 소스의 트래픽을 터널 외부의 연결(예: 로컬 Wi-Fi 또는 네트워크 연결)로 라우팅합니다.
- **Exclude networks specified below(**아래에 지정된 네트워크 제외**)**: 소스 네트워크를 정의하는 네트워크 개체를 선택합니다. 클라이언트는 이러한 소스의 모든 트래픽을 터널 외부의 연결로 라우팅합니다. 다른 소스의 트래픽은 터널을 통과합니다.
- **Network List(**네트워크 목록**)**: IPv4 및 IPv6 네트워크를 모두 포함할 수 있는 확장 ACL 네트워크를 선택합니다.

- **Split DNS(**스플릿 **DNS)**: 보안 연결을 통해 일부 DNS 요청을 전송하도록 시스템을 구성함과 동시에 클라이언트가 클라이언트에 구성된 DNS 서버로 다른 DNS 요청을 전송하도록 허용할 수 있습니다. 다음 DNS 동작을 컨피그레이션할 수 있습니다.
  - **Send DNS Request as per split tunnel policy(**스플릿 터널 정책에 따라 **DNS** 요청 전송**)**: 이 옵션을 사용하면 스플릿 터널 옵션을 정의하는 것과 동일한 방식으로 DNS 요청이 처리됩니다. 스플릿 터널링을 활성화하는 경우, DNS 요청은 대상 주소에 근거하여 전송됩니다. 스플릿 터널링을 활성화하지 않는 경우, 모든 DNS 요청은 보호된 연결을 경유해 전송됩니다.
  - **Always send DNS requests over tunnel(**항상 터널을 통해 **DNS** 요청 전송**)**: 스플릿 터널링을 활성화하되 모든 DNS 요청을 보호된 연결을 경유해 그룹에 정의된 DNS 서버로 전송하려는 경우, 이 옵션을 선택합니다.
  - **Send only specified domains over tunnel(**지정된 도메인만 터널을 통해 전송**)**: 보호된 DNS 서버에서 특정 도메인에 대해서만 주소를 확인하게 하고 싶은 경우, 이 옵션을 선택합니다. 그런 다음, 도메인 이름을 쉼표로 구분하여 해당 도메인을 지정합니다. example.com, example1.com을 예로 들 수 있습니다. 내부 DNS 서버에서는 내부 도메인의 이름을 확인하고 외부 DNS 서버에서는 다른 모든 인터넷 트래픽을 처리하게 하려는 경우, 이 옵션을 사용합니다.

AnyConnect 속성

그룹 정책의 AnyConnect 속성에서는 원격 액세스 VPN 연결에 대해 AnyConnect 클라이언트에서 사용하는 일부 SSL 및 연결 설정을 정의합니다.

- **SSL** 설정
  - **Enable Datagram Transport Layer Security (DTLS)(DTLS(Datagram Transport Layer Security)** 활성화**)**: AnyConnect 클라이언트에서 2개의 터널(SSL 터널 및 DTLS 터널)을 동시에 사용하도록 허용할지 여부를 선택합니다. DTLS를 사용하면 일부 SSL 연결에서 발생하

는 레이턴시 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능을 개선할 수 있습니다. DTLS를 활성화하지 않은 경우에는 SSL VPN 연결을 설정하는 AnyConnect 클라이언트 사용자가 SSL 터널만 사용하여 연결합니다.

- **DTLS Compression(DTLS** 압축**)**: LZS를 사용하여 이 그룹에 대한 DTLS(Datagram Transport Layer Security) 연결을 압축할지 여부를 선택합니다. DTLS 압축은 기본적으로 비활성화되어 있습니다.
- **SSL** 압축: 데이터 압축 활성화 여부를 선택하고, 활성화하는 경우 압축 해제 또는 **LZS** 중 사용할 데이터 압축 방법을 선택합니다. SSL 압축은 기본적으로 **Disabled(**비활성화**)** 상태입니다. 데이터를 압축하면 전송 속도가 빨라지지만 각 사용자 세션에 대한 메모리 요건 및 CPU 사용량이 증가합니다. 따라서 SSL 압축으로 인해 디바이스의 전체 처리량은 줄어듭니다.
- **SSL Rekey Method(SSL** 키 재입력 방법**)**, **SSL Rekey Interval(SSL** 키 재입력 간격**)**: 클라이언트는 VPN 연결에 키를 재입력하여 암호화 키 및 초기화 벡터를 재협상할 수 있어 연결 보안이 강화됩니다. **None(**없음**)**을 선택하여 키 재입력을 비활성화합니다. 키 재입력을 활성화하려면 **New Tunnel(**새 터널**)**을 선택하여 매번 새 터널을 생성합니다. (**Existing Tunnel(**기존 터널**)** 옵션을 선택하면 **New Tunnle(**새 터널**)**과 동일한 조치가 수행됩니다.) 키 재입력을 활성화하는 경우, 키 재입력 간격도 설정하십시오. 기본값은 4분입니다. 4~10080분(일주일) 범위 내에서 간격을 설정할 수 있습니다.

- 연결 설정
  - **Ignore the DF (Don't Fragment) bit(DF(Don't Fragment)** 비트 무시**)**: 단편화해야 하는 패킷에서 DF(Don't Fragment) 비트를 무시할지 여부를 선택합니다. 이 옵션을 선택하면 DF 비트가 설정된 패킷의 강제 단편화가 허용되므로 이 패킷이 터널을 통과할 수 있습니다.
  - **Client Bypass Protocol(**클라이언트 우회 프로토콜**)**: 이 옵션을 선택하면 보안 게이트웨이에서 IPv6 트래픽만 예상할 때 IPv4 트래픽을 관리하는 방법 또는 IPv4 트래픽만 예상할 때 IPv6 트래픽을 관리하는 방법을 구성할 수 있습니다.

    AnyConnect 클라이언트에서 헤드엔드와의 VPN 연결을 수행할 때 헤드엔드에서는 IPv4 주소나 IPv6 주소 또는 IPv4 및 IPv6 주소 모두를 지정합니다. 헤드엔드에서 AnyConnect 연결에 IPv4 주소만 또는 IPv6 주소만 지정할 경우, 헤드엔드에서 IP 주소를 지정하지 않은 네트워크 트래픽을 삭제하거나 이 트래픽이 헤드엔드를 우회하여 암호화되지 않은 또는 "일반 텍스트" 형태(활성화 및 확인된 상태)로 클라이언트에서 전송되는 것을 허용하도록 Client Bypass Protocol(클라이언트 우회 프로토콜)을 컨피그레이션할 수 있습니다.

    예를 들어 보안 게이트웨이에서 AnyConnect 연결에 IPv4 주소만 지정하고 엔드포인트는 이중 스택이라고 가정합시다. 엔드포인트가 IPv6 주소에 연결하려고 시도할 때 클라이언트 우회 프로토콜이 비활성화된 경우 IPv6 트래픽이 끊기지만 클라이언트 우회 프로토콜이 활성화된 경우, IPv6 트래픽은 클라이언트에서 암호화되지 않은 상태로 전송됩니다.
  - **MTU**: Cisco AnyConnect VPN 클라이언트에서 설정한 SSL VPN 연결의 MTU(Maximum Transmission Unit)입니다. 기본값은 1406바이트입니다. 범위는 576~1462바이트입니다.
    - **Keepalive Messages Between AnyConnect and VPN Gateway(AnyConnect**와 **VPN** 게이트웨이 간의 연결 유지 메시지**)**: 피어 간에 연결 유지 메시지를 교환하여 터널에서 데이터를 송수신하는 데 사용할 수 있다는 것을 시연할지 여부를 선택합니다. 연결 유지 메

시지는 설정된 간격에 따라 전송됩니다. 기본 간격은 20초, 유효 범위는 15~600초입니다.

- **DPD on Gateway Side Interval(**게이트웨이 측 간격의 **DPD)**, **DPD on Client Side Interval(**클라이언트 측 간격의 **DPD)**: DPD(Dead Peer Detection)를 활성화하면 피어가 더 이상 응답하지 않을 경우 VPN 게이트웨이 또는 VPN 클라이언트를 신속하게 탐지할 수 있습니다. 게이트웨이 또는 클라이언트 DPD를 별도로 활성화할 수 있습니다. DPD 메시지 전송의 기본 간격은 30초입니다. 간격은 5-3600초 사이일 수 있습니다.

트래픽 필터 속성

그룹 정책의 트래픽 필터 속성에서는 그룹에 할당된 사용자에게 부과하고 싶은 제한 사항을 정의합니다. 액세스 제어 정책 규칙을 생성하는 대신 이 속성을 사용해 원격 액세스 VPN 사용자를 호스트 또는 서브넷 주소 및 프로토콜, VLAN에 따라 특정 리소스로 제한할 수 있습니다. 기본적으로 그룹 정책에 따라 원격 액세스 VPN 사용자는 보호된 네트워크의 어떤 대상에 액세스하는 것도 제한되지 않습니다.

- **Access List Filter(**액세스 목록 필터**)**: 확장된 ACL(액세스 제어 목록)을 사용하여 액세스를 제한합니다. Smart CLI 확장 ACL 개체를 선택합니다. 확장 ACL을 통해 소스 주소, 대상 주소 및 프로토콜(예: IP 또는 TCP)을 기준으로 필터링할 수 있습니다. ACL은 하향식, 최초 일치 방식에 따라 평가되므로 특정 규칙이 다수의 일반 규칙보다 먼저 배치되도록 보장합니다. ACL의 끝에는 암묵적 "deny any(모두 거부)"가 있으므로 서브넷 몇 개에 대한 액세스만 거부하고 다른 모든 액세스는 허용하려면 ACL의 끝에 "permit any(모두 허용)" 규칙을 포함하십시오. 확장 ACL 스마트 CLI 개체를 수정하는 중에는 네트워크 개체를 생성할 수 없으므로 그룹 정책을 수정하기 전에 ACL을 생성해야 합니다. 그러지 않는 경우, 개체만 생성할 수 있습니다. 그런 다음 다시 돌아가 네트워크 개체를 생성한 후 필요한 모든 액세스 제어 항목을 생성하면 됩니다. ACL을 생성하려면 FDM에 로그인하고 **Device(**디바이스**)** > **Advanced Configuration(**고급 구성**)** > **Smart CLI(**스마트 **CLI)** > **Objects(**개체**)**로 이동하여 개체를 생성하고 **Extended Access List(**확장 액세스 목록**)**를 개체 유형으로 선택합니다.
- **Restrict VPN to VLAN(VPN**을 **VLAN**으로 제한**)**: “VLAN 매핑”이라고도 하는 이 속성에서는 이 그룹 정책이 적용되는 세션에 이그레스(egress) VLAN 인터페이스를 지정합니다. 시스템에서는 이 그룹에서 나오는 모든 트래픽을 선택한 VLAN으로 전달합니다. 이 특성을 사용하여 그룹 정책에 VLAN을 할당하면 액세스 제어를 간소화할 수 있습니다. ACL을 사용하여 세션의 트래픽을 필터링하는 방법 대신 이 속성에 값을 할당하는 방법도 가능합니다. 디바이스에서 하위 인터페이스에 정의된 VLAN 번호를 반드시 지정하십시오. 값의 범위는 1에서 4094까지입니다.

Windows 브라우저 프록시 속성

그룹 정책의 Windows 브라우저 프록시 속성에서는 사용자의 브라우저에 정의된 프록시의 작동 방식과 작동 여부를 결정합니다.

Browser Proxy During VPN Session(VPN 세션 중 브라우저 프록시**)**에 대해 다음 값 중 하나를 선택할 수 있습니다.

- **No change in endpoint settings(**엔드포인트 설정에 변경 사항 없음**)**: 이 옵션을 통해 사용자는 HTTP에 대해 브라우저 프록시를 컨피그레이션하거나 컨피그레이션하지 않을 수 있으며 컨피그레이션되어 있는 경우 프록시를 사용할 수 있습니다.
- **Disable browser proxy(**브라우저 프록시 비활성화**)**: 브라우저에 대해 정의된 프록시(있는 경우)를 사용하지 않습니다. 이 경우 프록시를 통해 브라우저 연결이 설정되지 않습니다.
- **Auto detect settings(**설정 자동 탐지**)**: 클라이언트 디바이스에 대해 브라우저에서 자동 프록시 서버 감지를 사용하도록 활성화합니다.
- **Use custom settings(**사용자 정의 설정 사용**)**: HTTP 트래픽에 대해 모든 클라이언트 디바이스에서 사용해야 하는 프록시를 정의합니다. 다음 설정을 구성합니다.
  - **Proxy Server IP or Hostname(**프록시 서버 **IP** 또는 호스트네임**), Port(**포트**)**: 프록시 서버의 IP 주소 또는 호스트네임, 프록시 서버에서 프록시 연결에 사용하는 포트입니다. 호스트와 포트를 합해 100자를 초과할 수 없습니다.
  - **Browser Exemption List(**브라우저 면제 목록**)**: 면제 목록의 호스트/포트에 대한 연결은 프록시를 통과하지 않습니다. 프록시를 사용해서는 안 되는 대상에 대해 모든 호스트/포트 값을 추가합니다. www.example.com port 80을 예로 들 수 있습니다. 목록에 항목을 추가하려면 **Add Proxy Exemption(**프록시 예외 추가**)**을 클릭합니다. 항목을 삭제하려면 휴지통 아이콘을 클릭합니다. 모든 주소와 포트를 합한 전체 프록시 예외 목록은 255자를 초과할 수 없습니다.

ASA 원격 액세스 VPN 구성 생성

CDO를 사용하면 하나 이상의 ASA(Adaptive Security Appliance) 디바이스를 원격 액세스 VPN 구성 마법사에 추가하고 디바이스와 연결된 VPN 인터페이스, 액세스 제어 및 NAT 면제 설정을 구성할 수 있습니다. 따라서 각 원격 액세스 VPN 구성에는 원격 액세스 VPN 구성과 연결된 여러 ASA 디바이스에서 공유되는 연결 프로파일 및 그룹 정책이 있을 수 있습니다. 또한 연결 프로파일 및 그룹 정책을 생성하여 구성을 개선할 수 있습니다.

이미 원격 액세스 VPN 설정으로 구성된 ASA 디바이스 또는 원격 액세스 VPN 설정이 없는 새 디바이스를 온보딩할 수 있습니다. CDO에 ASA 디바이스 온보딩를 참고하십시오. 이미 원격 액세스 VPN 설정이 있는 ASA 디바이스를 온보딩하는 경우 CDO는 자동으로 "기본 원격 액세스 VPN 구성"을 생성하고 ASA 디바이스를 이 구성과 연결합니다. 또한 이 기본 구성은 디바이스에 정의된 모든 연결 프로파일 개체를 포함할 수 있습니다. 기존 ASA Remote Access VPN 설정 관리 및 구축를 참조하십시오. CDO에서 기본 구성을 삭제할 수 있습니다.

중요

- 동일한 원격 액세스 VPN 구성에서 ASA 및 FTD 를 추가할 수 없습니다.
- ASA 디바이스에는 둘 이상의 원격 액세스 VPN 설정이 있을 수 없습니다.

시작하기 전에

원격 액세스 VPN 구성에 ASA 디바이스를 추가하려면 먼저 다음 사전 요건을 충족해야 합니다.

- 라이선스 요구 사항

  수출 통제 기능을 사용하려면 디바이스를 활성화해야 합니다.

  ASA 디바이스의 라이선스 요약을 보려면 ASA 명령줄 인터페이스에서 show license summary 명령을 실행합니다. CDO ASA CLI 인터페이스를 사용하려면 CDO인터페이스에서 ASA CLI 사용을 참조하십시오.

  - 라이선스 요약에서 활성화된 수출 통제 기능의 예:

```
등록: 상태: REGISTERED 스마트 어카운트: Cisco SVS temp-request access licensing@cisco.com
내보내기 제어 기능: ALLOWED

마지막 갱신 시도: 없음

다음 갱신 시도: 2021년 6월 8일 09:46:22 UTC
```

  VPN 구성을 생성하거나 편집하려면 '내보내기 제어 기능' 속성이 '허용됨' 상태여야 합니다.

  이 속성이 '허용되지 않음' 상태인 경우 CDO는 VPN 구성을 생성하거나 편집하고 디바이스에서 원격 액세스 VPN 구성을 허용하지 않을 때 오류 메시지('원격 액세스 VPN은 수출 규격이 아닌 디바이스에 대해 구성할 수 없습니다.')를 표시합니다.

- 디바이스 ID 인증서

  클라이언트와 ASA 디바이스 간의 SSL 연결을 인증하려면 인증서가 필요합니다. VPN 구성을 시작하려면 먼저 ASA 디바이스에 ID 인증서가 이미 있는지 확인합니다.

  디바이스에 인증서가 있는지 여부를 확인하려면 ASA 명령줄 인터페이스에서 **show crypto CA Certificates** 명령을 실행합니다. CDO ASA CLI 인터페이스를 사용하려면 CDO인터페이스에서 ASA CLI 사용을 참조하십시오.

  ID 인증서가 없거나 새 인증서를 등록하려는 경우 CDO를 사용하여 ASA에 설치합니다. ASA 인증서 관리를 참조하십시오.

  원격 액세스 VPN 컨텍스트에서 디지털 인증서의 사용은 원격 액세스 VPN 인증서 기반 인증, 69 페이지에 설명되어 있습니다.

- 외부 인터페이스.

  외부 인터페이스는 ASA 디바이스에 이미 구성되어 있어야 합니다. 인터페이스를 구성하려면 **ASDM** 또는 **ASA CLI**를 사용해야 합니다. ASDM을 사용한 인터페이스 구성에 대해 알아보려면 Cisco ASA Series General Operations CLI Configuration Guide, X.Y의 "Interfaces" 책을 참조하십시오.

- AnyConnect 패키지를 다운로드하고 원격 서버에 업로드하십시오. 나중에 원격 액세스 VPN 마법사 또는 ASA 파일 관리 마법사를 사용하여 서버에서 ASA로 AnyConnect 소프트웨어 패키지를 업로드하십시오. ASA 디바이스에서 AnyConnect 소프트웨어 패키지 관리를 참조하십시오.

- 보류 중인 구성 배포이 없습니다.

- 인증에 로컬 데이터베이스를 사용하는 경우 ASDM 또는 ASA CLI를 사용하여 로컬 데이터베이스에 사용자 계정을 추가합니다.

ASDM을 사용하여 사용자 계정을 추가하려면 Cisco ASA Series VPN CLI 구성 가이드, X.Y의 "AAA 서버 및 로컬 데이터베이스" 책에서 "로컬 데이터베이스에 사용자 계정 추가" 섹션을 참조하십시오.

ASA CLI를 사용하여 사용자 계정을 추가하려면, **username[***username***] password [***password***] privilege [***priv_level]*** command.usernamepasswordpriv_level] 명령을 실행합니다.

- ASA 변경 사항은 CDO에 동기화됩니다.
  1. 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭하고 동기화할 하나 이상의 ASA 디바이스를 검색합니다.
  2. 디바이스를 하나 이상 선택 다음 **Check for changes(**변경 사항 확인)를 클릭합니다. CDO는 하나 이상의 FTD 디바이스와 통신하여 변경 사항을 동기화 합니다.
- 원격 액세스 VPN 구성 그룹 정책 개체가 일치합니다.
  - 일치하지 않는 모든 그룹 정책 개체는 원격 액세스 VPN 구성에 추가할 수 없으므로 확인해야 합니다. 문제를 해결하거나 **Objects(**개체**)** 페이지에서 일치하지 않는 그룹 정책 개체를 제거합니다. 자세한 내용은 중복 개체 문제 해결 및 불일치 개체 문제 해결을 참조하십시오.

프로시저

단계 **1** CDO에 ASA 디바이스 온보딩.

단계 **2** 왼쪽 창에서 **VPN** > **ASA/FDM Remote Access VPN Configuration(**원격 액세스 **VPN** 구성**)**을 클릭합니다.

단계 **3** 파란색 더하기  버튼을 클릭하여새 원격 액세스 VPN 구성을 생성합니다.

단계 **4** 원격 액세스 VPN 구성의 이름을 입력합니다.

단계 **5** 파란색 더하기  버튼을 클릭하여 ASA 디바이스를 구성에 추가합니다.

디바이스 세부 정보를 추가하고 디바이스와 연결된 네트워크 트래픽 관련 권한을 구성할 수 있습니다.

1. 다음 디바이스 세부 사항을 입력합니다.
   - 디바이스: 추가할 ASA 디바이스를 선택하고 **Select(**선택**)**를 클릭합니다. 중효동일한 원격 액세스 VPN 구성에서 ASA 및 FTD를 추가할 수 없습니다.
   - **Certificate of Device Identity(**디바이스 **ID**의 인증서**)**: 디바이스의 ID를 설정하는 데 사용되는 내부 인증서를 선택합니다. 그러면 AnyConnect 클라이언트가 디바이스에 연결할 때 디바이스 ID를 설정합니다. 보안 VPN 연결을 완료하려면 클라이언트가 이 인증서를 허용해야 합니다.
   - **Outside Interface(**외부 인터페이스**)**: 원격 액세스 VPN 연결 시 사용자가 연결할 인터페이스를 선택합니다. 이 인터페이스는 대개 외부(인터넷 연결) 인터페이스이지만, 이 연결 프로파일을 사용하여 지원하려는 디바이스와 엔드 유저 간의 인터페이스를 선택하면 됩니다.

     주의

수출 규격이 아닌 디바이스에 대한 원격 액세스 VPN 구성을 생성하거나 편집할 수 없습니다. 수출 통제 기능이 활성화된 ASA 디바이스에 라이선스를 부여하고 다시 시도해야 합니다.

2. **Continue(**계속**)**를 클릭하여 트래픽 권한을 구성합니다.

   - **Bypass Access Control policy for decrypted traffic(**암호 해독된 트래픽에 대해 액세스 제어 정책 우회**)(sysopt permit-vpn)**: 암호 해독된 트래픽은 기본적으로 액세스 제어 정책 검사를 받습니다. 이 옵션을 활성화하면 암호 해독된 트래픽 옵션이 액세스 제어 정책 검사를 무시하지만, VPN 필터 ACL과 AAA 서버에서 다운로드한 인증 ACL이 VPN 트래픽에 계속 적용됩니다.

     이 옵션을 선택하는 경우, 시스템에서는 전역 설정인 sysopt connection permit-vpn 명령을 구성한다는 점에 유의하십시오. 이로 인해 Site-to-Site VPN 연결의 동작도 영향을 받습니다.

     이 옵션을 선택하지 않는 경우, 외부 사용자가 원격 액세스 VPN 주소 풀의 IP 주소를 스푸핑할 수 있고, 따라서 네트워크에 액세스할 수 있습니다. 이것이 가능한 이유는 주소 풀에서 내부 리소스에 액세스할 수 있게 허용하는 액세스 제어 규칙을 생성해야 하기 때문입니다. 액세스 제어 규칙을 사용하는 경우, 소스 IP 주소만 사용하기보다 사용자 사양을 이용해 액세스를 제어하는 것이 좋습니다.

     이 옵션을 선택할 경우의 단점은 VPN 트래픽이 검사되지 않는다는 것입니다. 즉 침입 및 파일 보호, URL 필터링 또는 기타 고급 기능이 트래픽에 적용되지 않습니다. 즉 트래픽에 대해 연결 이벤트가 생성되지 않고, 따라서 통계 대시보드에 VPN 연결이 반영되지 않는다는 의미이기도 합니다.

   - **NAT** 제외**(Exempt)**: NAT NAT 제외는 주소 변환을 제외하고 변환된 호스트와 원격 호스트가 모두 보호되는 호스트와의 연결을 시작할 수 있도록 허용합니다. NAT 제외를 구성하여 NAT 변환에서 원격 액세스 VPN 엔드포인트로 오가는 트래픽을 제외합니다. NAT에서 원격 액세스 VPN 트래픽 제외, 70 페이지의 내용을 참조하십시오.

3. **OK(**확인**)**를 클릭합니다.

   AnyConnect Packages Detected(감지된 **AnyConnect** 패키지**)**는 디바이스에서 이미 사용 가능한 AnyConnect 패키지를 표시합니다.

   원격 액세스 VPN 마법사에서 AnyConnect 패키지를 ASA에 업로드하는 두 가지 옵션이 있습니다.

   - (방법 1): CDO 저장소에서 패키지를 선택합니다. ASA는 인터넷에 액세스할 수 있어야 합니다.
   - (방법 2): AnyConnect 패키지가 사전 로드된 ftp/http/https/scp/smb/tftp URL 위치를 지정합니다.

   지침은 ASA 디바이스에서 AnyConnect 소프트웨어 패키지 관리를 참조하십시오.

   참고
   참고: 기존 패키지를 교체하려면 ASA 디바이스에서 AnyConnect 소프트웨어 패키지 관리를 참조하십시오.

단계 **6** **OK(**확인**)**를 클릭합니다.

ASA VPN 구성이 생성됩니다.

ASA 원격 액세스 *VPN* 구성 수정

기존 원격 액세스 VPN 구성의 이름 및 디바이스 세부 정보를 수정할 수 있습니다.

Procedure

단계 **1** 수정할 구성을 선택하고 **Actions(**작업**)** 아래에서 **Edit(**편집**)**를 클릭합니다.

- 필요한 경우 이름을 수정합니다.
- 디바이스를 추가하려면 파란색 더하기 버튼  을 클릭합니다.
-  을 클릭하여 ASA 디바이스에서 다음을 수행합니다.
  - **Edit(**편집**)**를 클릭하여 기존 원격 액세스 VPN 구성을 수정합니다.
  - **Remove(**제거**)**를 클릭하여 원격 액세스 VPN 구성에서 ASA 디바이스를 제거합니다. 그룹 정책을 제외하고 해당 디바이스와 연결된 모든 연결 프로파일 및 원격 액세스 VPN 설정이 삭제됩니다. 개체 페이지에서 그룹 정책을 명시적으로 제거할 수 있습니다.

    Note
    ASA가 구성을 사용하는 유일한 디바이스인 경우 ASA를 제거할 수 없습니다. 또는 원격 액세스 VPN 구성을 제거할 수 있습니다.

단계 **2** 구성 변경 사항 구축.

What to do next

구성 또는 디바이스의 이름을 입력하여 Remote Access VPN 구성을 검색할 수도 있습니다.
관련 정보**:**

- ASA 원격 액세스 VPN 연결 프로파일 구성, on page 53.

ASA 원격 액세스 **VPN** 연결 프로파일 구성

원격 액세스 VPN 연결 프로파일에서는 외부 사용자가 AnyConnect 클라이언트를 사용하여 시스템에 VPN 연결을 할 수 있게 허용하는 특성을 정의합니다. 각 프로파일에서 정의하는 것은 사용자를 인증하는 데 사용되는 AAA 서버 및 인증서, 사용자에게 IP 주소를 할당하기 위한 주소 풀, 다양한 사용자 중심 속성을 정의하는 그룹 정책입니다.

여러 사용자 그룹에 가변적인 서비스를 제공해야 하는 경우 또는 다양한 인증 소스가 있는 경우, 원격 액세스 VPN구성 내에 프로파일을 여러 개 생성합니다. 예를 들어 조직이 다른 인증 서버를 사용하는 다른 조직과 병합하는 경우, 해당 인증 서버를 사용하는 새 그룹에 대해 프로파일을 만들 수 있습니다.

원격 액세스 VPN 연결 프로파일을 사용하면 홈 네트워크 등의 외부 네트워크에 있는 사용자가 내부 네트워크에 연결할 수 있습니다. 다른 인증 방법을 수용하기 위해 별도 프로파일을 생성합니다.

시작하기 전에

ASA 원격 액세스 VPN 구성 생성, 49 페이지.

프로시저

단계 **1** 왼쪽 창에서 **VPN** > **ASA/FDM Remote Access VPN Configuration(**원격 액세스 **VPN** 구성**)**을 클릭합니다. VPN 구성을 클릭하여 현재 얼마나 많은 연결 프로파일 및 그룹 정책이 구성되어 있는지에 대한 요약 정보를 볼 수 있습니다.

참고
디바이스에 할당된 그룹 정책을 확인하려면 **Actions(**작업**)**에서 **Group Policies(**그룹 정책**)**를 클릭합니다. 연결 프로파일에 할당된 그룹 정책은 목록에 자동으로 추가되며 제거할 수 없습니다.

필요한 그룹 정책이 아직 없는 경우  을 클릭하고 목록에서 선택합니다. 필요한 서비스를 제공하는 추가 그룹 정책을 만들 수 있습니다. ASA 원격 액세스 VPN 그룹 정책 생성, 41 페이지을 참조하십시오.

단계 **2** 연결 프로파일을 클릭하고 오른쪽 사이드바의 **Actions(**작업**)** 아래에서 **Add Connection Profile(**연결 프로파일 추가**)**를 클릭합니다.

단계 **3** 기본 연결 속성을 구성합니다.

- **Connection Profile Name(**연결 프로파일 이름**)**: 이 연결의 이름을 공백 없이 50자까지 입력합니다. 예를 들면 MainOffice를 입력합니다.

  참고
  여기서 입력하는 이름이 AnyConnect 클라이언트에서 사용자에게 표시되는 연결 목록에 나타납니다. 따라서 사용자가 쉽게 이해할 수 있는 이름을 선택해야 합니다.

- **Group Alias(**그룹 별칭**), Group URL(**그룹 **URL)**: 별칭에는 특정 연결 프로파일에 대한 대체 이름 또는 URL이 포함되어 있습니다. ASA 디바이스에 연결하는 경우, VPN 사용자는 연결 목록의 AnyConnect 클라이언트에서 별칭 이름을 선택할 수 있습니다. 연결 프로파일 이름이 그룹 별칭으로 자동 추가됩니다. 또한 원격 액세스 VPN 연결을 시작하는 동안 엔드포인트에서 선택할 수 있는 그룹 URL의 목록을 구성할 수 있습니다. 사용자가 그룹 URL을 사용하여 연결하는 경우, 시스템에서는 URL과 일치하는 연결 프로파일을 자동으로 사용합니다. 이 URL은 설치된 AnyConnect 클라이언트가 아직 없는 클라이언트에서 사용됩니다. 그룹 별칭 및 URL을 필요한 만큼 추가하십시오. 이러한 별칭 및 URL은 디바이스에 정의된 모든 연결 프로파일 전반에 걸쳐 고유한 것이어야 합니다. 그룹 URL은 **https://**로 시작해야 합니다.

- 예를 들어 별칭 계약자 및 그룹 URL https://ravpn.example.com/contractor가 있을 수 있습니다. AnyConnect 클라이언트가 설치된 후 사용자는 연결의 AnyConnect VPN 드롭다운 목록에서 그룹 별칭을 선택하기만 하면 됩니다.

단계 **4** 기본 ID 소스를 구성하고, 선택적으로 보조 ID 소스를 구성합니다. 이 옵션을 통해 원격 사용자가 원격 액세스 VPN 연결을 활성화하기 위해 디바이스에 인증하는 방식을 결정합니다. 가장 간단한 방식은 AAA만 사용하여 AD

영역을 선택하거나 LocalIdentitySource를 사용하는 것입니다. **Authentication Type(**인증 유형**)**에는 다음과 같은 방식을 사용할 수 있습니다.

- **AAA Only(AAA**만**)**: 사용자 이름 및 암호에 근거하여 사용자를 인증하고 사용자에게 권한을 부여합니다. 자세한 내용은 연결 프로파일에 대해 AAA 구성 , 55 페이지 섹션을 참조하십시오.
- **Client Certificate Only(**클라이언트 인증서만**)**: 클라이언트 디바이스 ID 인증서에 근거하여 사용자를 인증합니다. 자세한 내용은 연결 프로파일에 대한 인증서 인증 구성을 참조하십시오.
- **AAA and ClientCertificate(AAA** 및 **ClientCertificate)**: 사용자 이름/암호와 클라이언트 디바이스 ID 인증서를 모두 사용합니다.

단계 **5** 클라이언트에 대해 주소 풀을 구성합니다. 주소 풀에서는 원격 클라이언트가 VPN 연결을 설정할 때 시스템에서 원격 클라이언트에 할당할 수 있는 IP 주소를 정의합니다. 자세한 내용은 클라이언트 주소 풀 할당 구성을 참조하십시오.

단계 **6** **Continue(**계속**)**를 클릭합니다.

단계 **7** 목록에서 이 프로파일에 사용할 **Group Policy(**그룹 정책**)**를 선택하고 **Select(**선택**)**를 클릭합니다.

그룹 정책에서는 터널이 설정된 후에 사용자 연결에 대한 조건을 설정합니다. 시스템에는 'DfltGrpPolicy'라는 이름의 기본 그룹 정책이 포함되어 있습니다. 필요한 서비스를 제공하는 추가 그룹 정책을 만들 수 있습니다. ASA 원격 액세스 VPN 그룹 정책 생성, 41 페이지을 참조하십시오.

단계 **8** **Continue(**계속**)**를 클릭합니다.

단계 **9** 요약을 검토합니다. 먼저 요약이 정확한지 확인합니다. AnyConnect 소프트웨어를 처음으로 설치하고 VPN 연결을 완료할 수 있는지를 테스트하기 위해 엔드 유저가 수행해야 하는 작업을 파악할 수 있습니다.  를 클릭하여 지침을 클립보드에 복사한 다음 사용자에게 배포합니다.

단계 **10** **Done(**완료**)**를 클릭합니다.

단계 **11** ASA에 대한 엔드 투 엔드 원격 액세스 VPN 구성 프로세스의 5단계를 수행합니다.

연결 프로파일에 대해 *AAA* 구성

인증, 권한 부여, 계정 관리 (AAA) 서버에서는 사용자 이름과 암호를 사용하여 사용자에게 원격 액세스 VPN에 대한 액세스가 허용되어 있는지 확인합니다. RADIUS 서버를 사용하는 경우, 인증된 사용자들 사이에서 권한 부여 수준을 구별하여 보호받는 리소스에 대한 차등 액세스를 제공할 수 있습니다. 또한 RADIUS 계정 관리 서비스를 사용하여 사용량을 추적할 수 있습니다.

AAA를 구성하는 경우, 기본 ID 소스를 구성해야 합니다. 보조 및 대체 소스는 선택 사항입니다. 2단계 인증을 구현하려면 RSA 토큰 또는 듀오와 같은 보조 소스를 사용합니다.

기본 **ID** 소스 옵션

- 사용자 인증을 위한 기본 **ID** 소스: 인증은 일반적으로 액세스 권한이 부여되기 전에 사용자가 유효한 사용자 이름과 유효한 암호를 입력하도록 하여 사용자를 식별하는 방법을 제공합니다. 원격 사용자를 인증하는 데 사용되는 기본 ID 소스입니다. VPN 연결을 완료하려면 이 소스 또는 대체 소스(선택 사항)에서 최종 사용자를 정의해야 합니다. 다음 중 하나를 선택합니다.
  - AD(Active Directory) ID 영역.

- Radius 서버 그룹.
- LocalIdentitySource(로컬 사용자 데이터베이스): 외부 서버를 사용하지 않고 디바이스에서 직접 사용자를 정의할 수 있습니다.

  ASA에 대한 ID 소스 구성를 클릭하여 새 ID 소스를 생성할 수 있습니다.

- **Fallback Local Identity Source(**대체 로컬 **ID** 소스**)**: 기본 소스가 외부 서버인데 기본 서버를 사용할 수 없는 경우, 대체 소스로 LocalIdentitySource를 선택할 수 있습니다. 로컬 데이터베이스를 대체 소스로 사용하는 경우 외부 서버에 정의한 것과 같은 로컬 사용자 이름/비밀번호를 정의해야 합니다.
- **Strip options(**제거 옵션**)**: 영역은 관리 도메인입니다. 다음 옵션을 활성화하면 사용자 이름에만 근거하여 인증할 수 있습니다. 이러한 옵션의 조합을 활성화할 수 있습니다. 그러나 서버에서 구분 기호를 구문 분석할 수 없는 경우, 두 확인란을 모두 선택해야 합니다.
  - **Strip Identity Source Server from Username(**사용자 이름에서 **ID** 소스 서버 제거**)**: AAA 서버로 사용자 이름을 전달하기 전에 사용자 이름에서 ID 소스 이름을 제거할지 여부. 예를 들어 이 옵션을 선택하고 사용자가 사용자 이름으로 domain\username을 입력하면 도메인이 사용자 이름에서 제거되고 인증을 위해 AAA 서버로 전송됩니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.
  - **Strip Group from Username(**사용자 이름에서 그룹 제거**)**: AAA 서버로 사용자 이름을 전달하기 전에 사용자 이름에서 그룹 이름을 제거할지 여부. 이 옵션은 username@domain 형식에서 지정된 이름에 적용되며, 도메인 및 @ 기호를 제거합니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.

보조 **ID** 소스

- **Secondary Identity Source for User Authorization(**사용자 권한 부여를 위한 보조 **ID** 소스**)**: 두 번째 ID 소스로서 선택 사항입니다. 사용자가 기본 소스로 인증에 성공하는 경우, 사용자에게 보조 소스를 사용해 인증하라는 메시지가 표시됩니다. AD 영역, RADIUS 서버 그룹 또는 로컬 ID 소스를 선택할 수 있습니다.
- **Advanced options(**고급 옵션**)**: **Advanced(**고급**)** 링크를 클릭하고 다음 옵션을 구성합니다.
  - **Fallback Local Identity Source for Secondary(**보조용 대체 시스템 로컬 **ID** 소스**)**: 보조 소스가 외부 서버인데 보조 서버를 사용할 수 없는 경우, LocalIdentitySource를 대체 소스로 선택할 수 있습니다. 로컬 데이터베이스를 대체 소스로 사용하는 경우, 보조 외부 서버에 정의한 것과 같은 로컬 사용자 이름/암호를 정의해야 합니다.
  - **Use Primary Username for Secondary Login(**보조 로그인에 기본 사용자 이름 사용**)**: 보조 ID 소스를 사용하는 경우, 시스템에서는 기본적으로 보조 소스에 대한 사용자 이름 및 암호를 모두 입력하라는 메시지를 표시합니다. 이 옵션을 선택하는 경우, 시스템에서는 보조 암호만 입력하라는 메시지를 표시하고 기본 ID 소스에 대해 인증된 보조 소스에 동일한 사용자 이름을 사용합니다. 기본 및 보조 ID 소스 모두에서 동일한 사용자 이름을 구성하는 경우, 이 옵션을 선택합니다.

- **Username for Session Server(**세션 서버의 사용자 이름**)**: 인증에 성공하면 사용자 이름이 이벤트 및 통계 대시보드에 표시되고, 이 이름은 사용자 또는 그룹 기반 SSL 암호 해독 및 액세스 제어 규칙에 대한 일치 여부를 확인하고 계정을 관리하는 데 사용됩니다. 두 가지 인증 소스를 사용하고 있기 때문에 기본 또는 보조 사용자 이름을 사용자 ID로 사용할지 여부를 시스템에 알려주어야 합니다. 기본적으로 기본 이름을 사용합니다.
- **Password Type(**암호 유형**)**: 보조 서버의 암호를 가져오는 방법. 기본값은 **Prompt(**프롬프트**)**입니다. 이는 사용자에게 암호를 입력하라는 메시지가 표시됨을 뜻합니다. 사용자가 기본 서버에 인증할 때 입력한 암호를 자동으로 사용하려면 **Primary Identity Source Password(**기본 **ID** 소스 암호**)**를 선택합니다. 모든 사용자에 대해 동일한 암호를 사용하려면 **Common Password(**공통 암호**)**를 선택한 다음, **Common Password(**공통 암호**)** 필드에 해당 암호를 입력합니다.

- **Authorization Server(**권한 부여 서버**)**: 원격 액세스 VPN 사용자를 인증하도록 구성된 RADIUS 서버 그룹. 인증이 완료되면 권한 부여 기능에서 인증된 각 사용자에게 사용할 수 있는 서비스 및 명령을 제어합니다. 권한 부여 기능은 사용자가 수행할 수 있도록 인가를 받은 것이 무엇인지, 즉 사용자의 실제 능력 및 제한 사항을 설명하는 일련의 속성을 결합함으로써 작동합니다. 권한 부여 기능을 사용하지 않는 경우, 인증 기능에서만 인증된 모든 사용자에게 동일한 액세스 권한을 제공합니다.

  시스템이 그룹 정책에 정의된 것과 중복되는 권한 부여 속성을 RADIUS 서버에서 가져오는 경우, RADIUS 속성은 그룹 정책 속성을 오버라이드한다는 점에 유의하십시오.

  ASA RADIUS 서버 개체 또는 그룹 생성을 클릭하여 새 서버 그룹을 생성할 수 있습니다.

- **Accounting Server(**과금 서버**)**: (선택 사항) 원격 액세스 VPN 세션에 대한 계정 관리에 사용할 RADIUS 서버 그룹입니다. 계정 관리 기능에서는 사용자가 액세스 중인 서비스뿐 아니라 사용 중인 네트워크 리소스의 수까지도 추적합니다. ASA 디바이스에서는 RADIUS 서버에 사용자 활동을 보고합니다. 계정 관리 정보에는 세션 시작 및 중지 시각, 사용자 이름, 각 세션의 디바이스를 통과한 바이트 수, 사용한 서비스, 각 세션의 지속시간이 포함됩니다. 네트워크 관리, 클라이언트 요금 청구 또는 감사에 대한 데이터를 분석할 수 있습니다. 관리 계정 기능을 단독으로 사용하거나 인증 및 권한 부여 기능과 함께 사용할 수 있습니다.

  ASA RADIUS 서버 개체 또는 그룹 생성을 클릭하여 새 서버 그룹을 생성할 수 있습니다.

연결 프로파일에 대한 인증서 인증 구성

Note 이 섹션은 **Authentication Type(**인증 유형**)**이 **AAA Only(AAA**만**)**인 경우에는 적용되지 않습니다.

클라이언트 디바이스에 설치된 인증서를 사용해 원격 액세스 VPN 연결을 인증할 수 있습니다.

클라이언트 인증서를 사용하는 경우에도 보조 ID 소스, 대체 소스, 권한 부여 및 과금 서버를 구성할 수 있습니다. 이 옵션은 AAA 옵션입니다. 자세한 내용은 ASA 원격 액세스 VPN 연결 프로파일 구성, on page 53을 참조하십시오.

다음은 인증서별 속성입니다. 기본 및 보조 ID 소스에 대해 개별적으로 이러한 속성을 구성할 수 있습니다. 보조 소스 구성은 선택 사항입니다.

- **Username from Certificate(**인증서의 사용자 이름**)**: 다음 중 하나를 선택합니다.
  - **Map Specific Field(**특정 필드 매핑**)**: **Primary Field(**기본 필드**)** 및 **Secondary Field(**보조 필드**)**의 순서대로 인증서 요소를 사용합니다. 기본값은 CN(Common Name) 및 OU(Organizational Unit)입니다. 조직에 대해 작동하는 옵션을 선택합니다. 필드는 서로 결합하여 사용자 이름을 제공하고, 이 이름은 이벤트, 대시보드에서 사용되며 SSL 암호 해독 및 액세스 제어 규칙에서 일치 목적으로 사용됩니다.
  - **Use entire DN (distinguished name) as username(**전체 **DN(**고유 이름**)**을 사용자 이름으로 사용**)**: 시스템은 DN 필드에서 사용자 이름을 자동으로 파생합니다.
- 고급 옵션(**Authentication Type(**인증 유형**)**이 **Client Certificate Only(**클라이언트 인증서 전용**)**인 경우에는 해당되지 않음): **Advanced(**고급**)** 링크를 클릭하고 다음 옵션을 구성합니다.
  - **Prefill username from certificate on user login window(**인증서의 사용자 이름을 사용자 로그인 창에 미리 채우기**)**: 사용자에게 인증하라는 메시지를 표시할 때 사용자 이름 필드에 검색된 사용자 이름을 입력할지 여부.
  - **Hide username in login window(**로그인 창에서 사용자 이름 숨기기**)**: **Prefill(**미리 채우기**)** 옵션을 선택하면 사용자 이름을 숨길 수 있습니다. 따라서 사용자는 암호 프롬프트에서 사용자 이름을 편집할 수 없습니다.

클라이언트 주소 풀 할당 구성

원격 액세스 VPN에 연결하는 엔드포인트에 대한 IP 주소를 시스템에서 제공할 방법이 있어야 합니다. AAA 서버는 이러한 주소, DHCP 서버, 그룹 정책에 구성된 IP 주소 풀 또는 연결 프로파일에 구성된 IP 주소 풀을 제공할 수 있습니다. 시스템은 순서대로 이 리소스를 시도하고 사용 가능한 주소를 가져올 때 중지했다가 이 주소를 클라이언트에 할당합니다. 따라서 동시 연결 수가 비정상적인 경우에 페일세이프를 생성할 수 있는 여러 가지 옵션을 구성할 수 있습니다.

연결 프로파일에 대한 주소 풀을 구성하려면 다음 방법 중 한 가지 이상을 사용합니다.

- **IPv4 Address Pool(IPv4** 주소 풀**)** 및 **IPv4 Address Pool(IPv4** 주소 풀**)**: 먼저 서브넷을 지정하는 최대 6개의 네트워크 개체를 생성합니다. IPv4 및 IPv6에 대해 별도 풀을 구성할 수 있습니다. 그런 다음, 그룹 정책 또는 연결 프로파일의 **IPv4 Address Pool(IPv4** 주소 풀**)** 및 **IPv6 Address Pool(IPv6** 주소 풀**)** 옵션에서 이러한 개체를 선택합니다. IPv4 및 IPv6 모두 구성할 필요는 없고 지원하려는 주소 체계를 구성하면 됩니다. 또한 그룹 정책 및 연결 프로파일 모두에서 풀을 구성할 필요는 없습니다. 그룹 정책에서는 연결 프로파일 설정을 오버라이드하므로 그룹 정책에서 풀을 구성하는 경우, 연결 프로파일에서 옵션을 비워두십시오. 풀은 나열한 순서대로 사용된다는 점에 유의하십시오. 새 IPv4 또는 IPv6 주소 풀을 생성하려면, IP 주소 풀 생성을 참조하십시오.
- **DHCP Servers(DHCP** 서버**)**: 먼저 원격 액세스 VPN에 대한 IPv4 주소 범위를 하나 이상 사용하여 DHCP 서버를 구성합니다(DHCP를 사용하여 IPv6 풀을 구성할 수는 없음). 그런 다음, DHCP 서버의 IP 주소로 호스트 네트워크 개체를 생성합니다. 그러면 연결 프로파일의 **DHCP Servers(DHCP** 서버**)** 속성에서 이 개체를 선택할 수 있습니다. 두 개 이상의 DHCP 서버를 구성

할 수 있습니다. DHCP 서버에 주소 풀이 여러 개인 경우, 연결 프로파일에 연결하는 ASA 원격 액세스 VPN 그룹 정책 생성에서 **DHCP Scope(DHCP** 범위**)** 속성을 사용해 어떤 풀을 사용할지 선택할 수 있습니다. 풀의 네트워크 주소로 호스트 네트워크 개체를 생성합니다. 예를 들어 DHCP 풀에 192.168.15.0/24 및 192.168.16.0/24가 포함된 경우, DHCP 범위를 192.168.16.0으로 설정하면 192.168.16.0/24 서브넷에서 주소가 선택됩니다.

관련 정보**:**

ASA에 대한 엔드 투 엔드 원격 액세스 VPN 구성 프로세스

ASA 디바이스에서 AnyConnect 소프트웨어 패키지 관리

원격 액세스 VPN 마법사를 사용하여 AnyConnect 패키지를 업로드하려면 다음 단계 중 하나를 수행할 수 있습니다.

- CDO 저장소에서 패키지를 업로드합니다.
- HTTP, HTTPS, TFTP, FTP, SMB 또는 SCP 프로토콜을 사용하여 서버에서 패키지를 업로드합니다.

CDO 저장소에서 *AnyConnect* 패키지 업로드

원격 액세스 VPN 구성 마법사는 CDO 저장소에서 운영 체제별로 AnyConnect 패키지를 제공하며, 이러한 패키지를 선택하여 디바이스에 업로드할 수 있습니다. 디바이스가 인터넷 및 적절한 DNS 구성에 액세스할 수 있는지 확인합니다.

참고 표시된 목록에서 원하는 패키지를 사용할 수 없거나 디바이스에서 인터넷에 액세스할 수 없는 경우 AnyConnect 패키지가 미리 로드된 서버를 사용하여 패키지를 업로드할 수 있습니다.

프로시저

단계 **1** 운영 체제에 해당하는 필드를 클릭하고 AnyConnect 패키지를 선택합니다.

단계 **2** 를 클릭하여 패키지를 업로드합니다. 체크섬이 일치하지 않으면 AnyConnect 패키지 업로드가 실패합니다. 장애에 대한 자세한 내용은 디바이스의 워크플로우 탭을 참조하십시오.

서버에서 *ASA*로 *AnyConnect* 패키지 업로드

AnyConnect 클라이언트 소프트웨어 패키지를 컴퓨터에 다운로드하고 ASA에서 액세스할 수 있는 원격 서버에 업로드합니다. 나중에 RA VPN 마법사 또는 ASA 파일 관리 마법사를 사용하여 서버에서 ASA로 AnyConnect 소프트웨어 패키지를 업로드하십시오. 도메인 이름을 사용하는 URL의 경우 디바이스에서 DNS를 올바르게 구성해야 합니다.

ASA RA VPN 마법사는 HTTP, HTTPS, TFTP, FTP, SMB 또는 SCP 프로토콜을 사용한 패키지 업로드를 지원합니다.

파일 업로드에 지원되는 프로토콜의 syntax(명령문):

프로토콜	구문	예
HTTP	http://[[path/]filename]	http://www.geonames.org/data-sources.html
HTTPS	https://[[path/]filename]	https://docs.aws.amazon.com/amazov/tagging.html
TFTP	tftp://[[path/]filename]	tftp://10.10.16.6/ftd/components.html
FTP	ftp://[[user[:password]@]server[:port]/[path/]filename]	[illegible]
SMB	smb://[[path/]filename]	smb://10.10.32.145//sambashare/hello.txt
SCP	scp://[[user[:password]@]server[/path]/ filename]	scp://rootcisco123@10.10.166//root/events_send.py

Before you begin

원하는 운영 체제에 대한 "AnyConnect 헤드엔드 배포 패키지"를 다운로드했는지 확인하십시오. 항상 최신 AnyConnect 버전을 다운로드하여 최신 기능, 버그 수정 및 보안 패치가 있는지 확인하십시오. 디바이스에서 패키지를 정기적으로 업데이트합니다.

Important ASA 파일 관리 마법사를 사용하여 패키지를 업로드하려는 경우, 다운로드한 후 패키지의 이름을 수정하지 마십시오.

Note 운영 체제(Windows, Mac, Linux)별로 AnyConnect 패키지를 하나씩 업로드할 수 있습니다. 지정된 OS 유형의 여러 버전을 업로드할 수는 없습니다.

Procedure

단계 **1** https://software.cisco.com/download/home/283000185에서 AnyConnect 패키지를 다운로드합니다.

- EULA에 동의하고 K9(암호화된 이미지) 권한이 있는지 확인합니다.
- 운영 체제에 맞는 "AnyConnect Headend Deployment Package" 패키지를 선택합니다. 패키지 이름은 "anyconnect-win-4.7.04056-webdeploy-k9.pkg"와 유사합니다. Windows, macOS 및 Linux용 별도의 헤드엔드 패키지가 있습니다.

단계 **2** AnyConnect 패키지를 원격 서버에 업로드합니다. ASA 디바이스 및 서버에서 네트워크 경로가 있는지 확인합니다.

ASA RA VPN 마법사는 HTTP, HTTPS, TFTP, FTP, SMB 또는 SCP 프로토콜로 패키지 업로드를 지원합니다.

Important
AnyConnect 패키지를 HTTPS 서버에 업로드하는 경우 다음 단계를 수행해야 합니다.

- ASA 디바이스에서 해당 서버의 신뢰할 수 있는 CA 인증서를 업로드합니다.
- HTTPS 서버에 신뢰할 수 있는 CA 인증서를 설치합니다.

단계 **3** 원격 서버의 URL은 인증 프롬프트가 표시되지 않는 직접 링크여야 합니다. URL이 사전 인증된 경우 RA VPN 마법사의 URL을 지정하여 파일을 다운로드할 수 있습니다.

단계 **4** 원격 서버 IP 주소가 NAT된 경우 원격 서버 위치의 NAT된 공용 IP 주소를 제공해야 합니다.

*ASA*에 새 *AnyConnect* 패키지 업로드

원격 액세스 VPN 마법사 또는 ASA 파일 관리 마법사를 사용하여 AnyConnect 소프트웨어 패키지를 ASA에 업로드할 수 있습니다.

다음 절차를 사용하여 HTTP 또는 HTTPS 서버에서 ASA 디바이스에 새 AnyConnect 패키지를 업로드합니다.

Procedure

단계 **1** **AnyConnect Package Detected(AnyConnect** 패키지 감지됨**)**에서 Windows, Mac 및 Linux 엔드포인트용 개별 패키지를 업로드할 수 있습니다.

단계 **2** 해당하는 Platform(플랫폼) 필드에서 Windows, Mac 및 Linux와 호환되는 AnyConnect 패키지가 사전 업로드되는 서버의 경로를 지정합니다. 서버 경로의 예:
'http://<ip_address>:port_number/<folder_name>/anyconnect-win-4.8.01090-webdeploy-k9.pkg',
'https://<ip_address>:port_number/<folder_name>/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg'.

단계 **3** 을 클릭하여 패키지를 업로드합니다. CDO는 경로에 연결할 수 있고 지정된 파일 이름이 유효한 패키지인지 확인합니다. 검증에 성공하면 AnyConnect 패키지의 이름이 나타납니다. 원격 액세스 VPN 구성에 ASA 디바이스를 추가하면 AnyConnect 패키지를 여기에 업로드할 수 있습니다.

단계 **4** **OK(**확인**)**를 클릭합니다. AnyConnect 패키지가 원격 액세스 VPN 구성에 추가됩니다.

단계 **5** 5단계부터 ASA 원격 액세스 VPN 구성 생성을 계속 진행합니다.

What to do next

VPN 연결을 완료하려면 사용자가 해당 워크스테이션에 AnyConnect 클라이언트 소프트웨어를 설치해야 합니다. 자세한 내용은 ASA에서 사용자가 AnyConnect 클라이언트 소프트웨어 설치 을 참조하십시오.

파일 관리 마법사를 사용하여 *AnyConnect* 패키지 업로드

HTTP, HTTPS, TFTP, FTP, SMB 또는 SCP 서버에서 단일 또는 여러 ASA 디바이스로 AnyConnect 패키지를 업로드하려면 파일 관리 마법사를 사용합니다. AnyConnect 패키지를 여러 ASA 디바이스에 동시에 푸시하려는 경우 대량 업로드가 유용합니다. 자세한 내용은 ASA 파일 관리를 참조하십시오.

Important ASA 파일 관리 마법사를 사용하여 패키지를 업로드하려는 경우, 다운로드한 후 패키지의 이름을 수정하지 마십시오.

업로드가 완료되면 ASA RA VPN 구성 마법사를 열고 패키지가 자동으로 탐지되는지 확인합니다. OS 버전에 대해 여러 패키지를 업로드하는 경우 마법사의 드롭다운 목록에 해당 패키지가 나열되어 그중 하나를 선택할 수 있습니다. 그런 다음 RA VPN 구성을 생성하여 디바이스에 구축할 수 있습니다.

AnyConnect 패키지 교체

AnyConnect 패키지가 디바이스에 이미 있는 경우 원격 액세스 VPN 마법사에서 확인할 수 있습니다. 드롭다운 목록에서 운영 체제에 대해 사용 가능한 모든 AnyConnect 패키지를 볼 수 있습니다. 목록에서 기존 패키지를 선택하고 새 패키지로 교체할 수 있지만 새 패키지를 목록에 추가할 수는 없습니다.

Note 기존 패키지를 새 패키지로 교체하려면 ASA 디바이스가 연결할 수 있는 네트워크의 서버에 새 AnyConnect 패키지가 이미 업로드되어 있는지 확인합니다.

Procedure

단계 **1** 왼쪽 창에서 **VPN** > **ASA/FDM Remote Access VPN (**원격 액세스 **VPN)**을 클릭합니다.

단계 **2** 수정할 원격 액세스 VPN 구성을 선택하고 **Actions(**작업**)** 아래에서 **Edit(**편집**)**를 클릭합니다.

단계 **3** **AnyConnect Packages Detected(AnyConnect** 패키지 탐지됨**)**에서 기존 AnyConnect 패키지 옆에 나타나는 아이콘을 클릭합니다. 운영 체제에 여러 버전의 AnyConnect 패키지가 있는 경우 목록에서 교체할 패키지를 선택하고 **Edit(**편집**)**를 클릭합니다. 해당 필드에서 기존 패키지가 사라집니다.

단계 **4** 새 AnyConnect 패키지가 사전 로드되는 서버의 경로를 지정하고 을 클릭하여 패키지를 업로드합니다.

단계 **5** **OK(**확인**)**를 클릭합니다. 새 AnyConnect 패키지가 원격 액세스 VPN 구성에 추가됩니다.

단계 **6** 6단계부터 ASA 원격 액세스 VPN 구성 생성, on page 49로 계속 진행합니다.

AnyConnect 패키지 삭제

Procedure

단계 **1** 왼쪽 창에서 **VPN** > **ASA/FDM Remote Access VPN (**원격 액세스 **VPN)**을 클릭합니다.

단계 **2** 수정할 원격 액세스 VPN 구성을 선택하고 **Actions(**작업**)** 아래에서 **Edit(**편집**)**를 클릭합니다.

단계 **3** **AnyConnect Packages Detected(**탐지된 **AnyConnect** 패키지**)**에서 삭제할 AnyConnect 패키지 옆에 표시되는 아이콘을 클릭합니다. 운영 체제에 여러 버전의 AnyConnect 패키지가 있는 경우 목록에서 삭제할 패키지를 선택합니다. 해당 필드에서 기존 패키지가 사라집니다.

Note
삭제 작업을 중지하고 기존 패키지를 유지하려면 **Cancel(**취소**)**을 클릭합니다.

단계 **4** **OK(**확인**)**를 클릭합니다. 디바이스의 구성 상태가 '동기화되지 않음' 상태입니다.

Note
이 단계에서 삭제 작업을 실행 취소하려면 보안 디바이스 페이지로 이동하여 **Discard Changes(**변경 사항 취소**)**를 클릭하여 기존 AnyConnect 패키지를 유지합니다.

단계 **5** 디바이스에 대한 구성 변경 사항 미리보고 구축합니다.

기존 **ASA Remote Access VPN** 설정 관리 및 구축

이미 원격 액세스 VPN 설정이 있는 ASDM 매니지드 ASA 디바이스를 온보딩하는 경우, 기존 원격 액세스 VPN 구성을 검색하여 표시합니다. CDO에서는 자동으로 "기본 원격 액세스 VPN 구성"을 생성하고 ASA 디바이스를 이 구성과 연결합니다. CDO에서 읽히지 않거나 지원되지 않지만 CDO 명령줄 인터페이스에서 구성할 수 있는 일부 원격 액세스 VPN 구성이 있습니다.

Note 이 섹션에서는 CDO에서 지원되거나 지원되지 않는 모든 구성을 다루지는 않습니다. 대신 가장 일반적으로 사용되는 항목만 설명합니다.

온보딩된 ASA에서 원격 액세스 VPN 구성을 보려면, 다음 단계를 수행합니다.

Procedure

단계 **1** 왼쪽 창에서 **VPN** > **ASA/FDM Remote Access VPN Configuration(**원격 액세스 **VPN** 구성**)**을 클릭합니다.

단계 **2** 온보드된 ASA 디바이스에 해당하는 원격 액세스 VPN 구성을 클릭합니다. CDO는 자동으로 **"Default_RA_VPN_Configuration"**을 생성하고 ASA 디바이스가 이 구성에 연결됩니다. 기본 구성을 삭제할 수 있습니다. CDO에서 읽는 ASA 원격 액세스 VPN 구성은 다음과 같이 분류됩니다.

- 디바이스 설정

- 연결 프로파일
- 그룹 정책

디바이스 설정

온보딩된 ASA 디바이스와 연결된 RA VPN 구성이 **Default_RA_VPN_Configuration**에 나타납니다. 해당 구성과 연결된 ASA 디바이스(오른쪽의 **Devices(**디바이스**)** 창에서)의 이름을 보려면 이 구성을 클릭해야 합니다. 편집 버튼을 클릭하여 ASA 디바이스에 있는 AnyConnect 패키지를 확인할 수도 있습니다.

연결 프로파일

CDO는 ASA 디바이스의 "AnyConnect 클라이언트 VPN 액세스"에 정의된 연결 프로파일을 지원하고 읽습니다. "클라이언트리스 SSL VPN 액세스" 구성은 지원되지 않습니다.

연결 프로파일 속성을 보려면 다음을 수행합니다.

Procedure

단계 **1** **Default_RA_VPN_Configuration**을 확장합니다.

단계 **2** 원하는 연결 프로파일 중 하나를 클릭하고 **Edit(**편집**)**를 클릭합니다.

모든 기본 및 고급 ASA 원격 액세스 VPN 속성은 CDO 원격 액세스 VPN 구성 페이지의 연결 프로파일 이름 및 세부 정보에서 확인할 수 있습니다.

Note 기본 구성을 삭제할 수 있습니다(기본 RA VPN 구성을 선택하고 오른쪽의 **Actions(**작업**)** 창에서 **Remove(**제거**)** 클릭).

기본 **ID** 소스

- CDO는 **Connection Aliases(**연결 별칭**)** 및 **Group URLs(**그룹 **URL)** 속성을 **Group Alias(**그룹 별칭**)** 및 **Group URL(**그룹 **URL)**로 읽습니다.

Note

- SAML, 다중 인증서 및 AAA, 다중 인증서로 구성된 연결 프로파일은 읽을 수 없습니다.
- 인터페이스 및 서버 그룹이 있는 인증 서버 그룹은 지원되지 않습니다.

- CDO는 기본 **ID** 소스에서 "AAA", "AAA 및 인증서" 및 "인증서 전용" 인증 방법으로 구성된 AnyConnect 연결 프로파일을 지원합니다.
- **AAA** 서버 그룹은 CDO에서 기본 **ID** 소스의 사용자 인증을 위한 기본 **ID** 소스로 읽힙니다(인증 유형으로 **AAA** 또는 **AAA** 및 클라이언트 인증서를 선택하여 이 속성을 확인할 수 있음).
  - **AAA** 서버 그룹이 로컬이 아닌 다른 항목으로 구성된 경우 CDO는 이 특성을 읽고 **Primary Identity Source(**기본 **ID** 소스**)** 아래의 **Fallback Local Identity Source(**대체 로컬 **ID** 소스**)** 필드에 이 속성을 표시합니다. (인증 유형으로 **AAA**를 선택하여 이 속성을 확인할 수 있습니다.)

    CDO에서 읽은 서버 그룹 특성에 대한 자세한 내용은 AAA 서버 그룹을 참조하십시오.

보조 ID 소스

Secondary Identity Source(보조 **ID** 소스**)**에는 ASA 디바이스의 보조 인증 속성이 표시됩니다. 이러한 속성을 보려면 인증 유형으로 **AAA** 또는 **AAA and Client Certificate(**클라이언트 인증서**)**를 선택하고 **View Secondary Identity Source(**보조 **ID** 소스 보기**)**를 클릭합니다.

- **Secondary Identity Source for User Authentication(**사용자 인증을 위한 보조 **ID** 소스**)**에 보조 인증 **Server Group(**서버 그룹**)** 속성이 표시됩니다.
  - 서버 그룹이 LOCAL(로컬) 이외의 항목으로 구성된 경우 CDO는 이 특성을 읽고 **Secondary Identity Source(**보조 **ID** 소스**)** 아래의 **Fallback Local Identity Source for Secondary(**보조 **ID** 소스에 대한 대체 로컬 **ID** 소스**)** 필드에 이 속성을 표시합니다.
- CDO는 **Attribute Server(**속성 서버**)** 및 **Interface-Specific Authorization Server Groups(**인터페이스별 권한 부여 서버 그룹**)** 속성을 지원하지 않습니다.

CDO에서 읽은 서버 그룹 특성에 대한 자세한 내용은 AAA 서버 그룹을 참조하십시오.

권한 부여 서버

- **Authorization Server(**권한 부여 서버**)**에 권한 부여 **Server Group(**서버 그룹**)** 속성이 표시됩니다.
- CDO는 인터페이스 및 서버 그룹이 있는 권한 부여 서버 그룹을 지원하지 않습니다.

CDO에서 읽은 RADIUS 서버 그룹 특성에 대한 자세한 내용은 RADIUS 서버 그룹을 참조하십시오.

계정 관리 서버

Accounting Server(과금 서버**)**에 과금 서버 그룹 속성이 표시됩니다. CDO에서 읽은 서버 그룹 특성에 대한 자세한 내용은 RADIUS 서버 그룹을 참조하십시오.

클라이언트 주소 풀 할당

CDO는 **Client Address Assignment(**클라이언트 주소 할당**)** 속성(**DHCP** 서버, 클라이언트 주소 풀 및 클라이언트 **IPv6** 주소 풀)을 개체로 읽습니다. (이러한 속성은 **Client Address Pool Assignment(**클라이언트 주소 풀 할당**)**에서 확인할 수 있습니다.) DHCP 서버 세부 정보는 리터럴로 읽힙니다.

Note CDO는 특정 인터페이스에 할당된 IP 주소 풀을 지원하지 않습니다. 그러나 이러한 속성은 ASA CLI(명령줄 인터페이스)에서 확인할 수 있습니다.

AAA 서버 그룹

CDO는 LDAP 서버 그룹 및 연결된 LDAP 서버를 **Active Directory** 영역 개체로 나타냅니다. AD(Active Directory)의 경우 영역은 Active Directory 도메인과 동일합니다. CDO는 이미 존재하는 AD 영역 개체의 AD 비밀번호를 읽습니다.

Procedure

단계 **1** 왼쪽 CDO 탐색 모음에서 개체를 클릭합니다.

단계 **2** 이 개체를 보려면 **Active Directory Realms(Active Directory** 영역**)** 필터를 적용합니다.

단계 **3** 원하는 Active Directory 영역 개체를 선택하고 **Edit(**편집**)**를 클릭하여 세부 정보를 확인합니다.

What to do next

AD 영역에 연결된 AD 서버 및 해당 구성이 포함되어 있음을 확인할 수 있습니다. AD 영역에 대해 여러 AD(Active Directory) 서버가 있는 경우 AD 서버는 서로 중복되어야 하며 동일한 AD 도메인을 지원해야 합니다. 따라서 디렉터리 이름, 디렉터리 암호 및 기본 고유 이름과 같은 기본 영역 속성은 해당 AD 영역과 연결된 모든 AD 서버에서 동일해야 합니다. 이러한 속성이 동일하지 않으면 CDO는 Active Directory 영역 개체에 경고 메시지를 표시합니다. AD 서버 전체에서 일관성을 유지하려면 이러한 속성을 수정해야 합니다. 이 경고를 해결하지 않고 계속 진행하면 CDO는 AD 서버 속성 중 하나를 사용하여 해당 영역 개체의 다른 서버에 적용합니다.

RADIUS 서버 그룹

ASA 디바이스의 AAA RADIUS 서버 그룹 속성은 CDO에서 RADIUS 서버 그룹 개체로 읽힙니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 이 개체를 보려면 **RADIUS** 서버 그룹필터를 적용합니다.

단계 **3** 원하는 개체를 선택한 다음 **Edit(**편집**)**를 클릭하여 세부 정보를 확인합니다.

- ASA에서 **Enable dynamic authorization(**동적 권한 부여 활성화**)**는 CDO에서 **Dynamic Authorization(**동적 권한 부여**)(**원격 액세스 **VPN**에만 해당**)**으로 읽힙니다.
- **Reactivation Mode(**재활성화 모드**)**의 **Depletion(**감소**)** 옵션은 CDO에서 읽히므로, 감소 시간과 관련된 **Dead Time(**데드 타임**)** 값은 CDO에서 읽힙니다. 그러나 **Timed(**시간 제한**)** 속성은 CDO에서 읽히지 않습니다.

- CDO **Accounting Mode(**계정 관리 모드**)**, **Timed(**시간 제한**)**, **Enable interim accounting update(**임시 계정 업데이트 활성화**)**, **Enable interim accounting update(**임시 계정 업데이트 활성화**)** 및 **Use authorization only mode(**권한 부여 전용 모드 사용**)**을 지원하지 않습니다.

RADIUS 서버

CDO는 ASA에서 Radius 서버를 읽을 때 이름을 "Radius 서버 group_server 이름 또는 IP 주소의 이름"으로 지정하는 Radius 서버 개체를 생성합니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 이 개체를 보려면 **RADIUS Server(RADIUS** 서버**)** 필터를 적용합니다.

단계 **3** 원하는 개체를 선택한 다음 **Edit(**편집**)**를 클릭하여 세부 정보를 확인합니다.

그룹 정책

Group Policy(그룹 정책**)** 섹션에서 드롭다운을 클릭하여 디바이스와 연결된 그룹 정책을 확인합니다.

Attention CDO는 터널링 프로토콜로 구성된 그룹 정책을 **SSL VPN** 클라이언트로 읽습니다.

CDO는 ASA에 구성된 대부분의 그룹 정책 속성을 읽습니다. 이 정보는 RA VPN 그룹 정책 마법사의 여러 탭에 표시됩니다. ASA 디바이스에서 읽은 그룹 정책의 세부 정보를 보려면 다음을 수행해야 합니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** **RA VPN Group Policy(RA VPN** 그룹 정책**)**를 기준으로 필터링합니다.

단계 **3** 해당 디바이스와 연결된 그룹 정책을 선택하고 **Edit(**편집**)**를 클릭합니다.

What to do next

Note CDO는 ASA 디바이스의 스플릿 터널링에 정의된 표준 ACL(Access Control List)을 지원하지 않습니다. ACL(Extended Access Control List)을 지원하며 ASA 정책에서 ACL로 읽습니다. 자세한 내용은 ASA 원격 액세스 VPN 그룹 정책 속성을 참조하십시오. 정책을 보려면 내비게이션 바에서 **Policies(**정책**)** > **ASA Access Policies(ASA** 액세스 정책**)**를 클릭합니다.

확장 ACL을 선택하려면 다음을 수행합니다.

- **Split Tunneling(**스플릿 터널링**)** 탭을 클릭합니다.
- ASA의 트래픽이 IPv4 주소를 사용하는지 IPv6 주소를 사용하는지에 따라 해당 드롭다운 목록에서 "Allow specified traffic over tunnel(터널을 통한 지정된 트래픽 허용)" 또는 "Exclude networks specified below(아래에 지정된 네트워크 제외)"를 선택합니다. ASA에서 가져온 확장 ACL을 선택합니다.

IP 주소 풀 생성

VPN 연결을 사용하여 네트워크에 원격으로 연결하는 클라이언트에 할당하도록 ASA에 대한 IPv4 및 IPv6 IP 주소 풀을 구성할 수 있습니다. 풀을 지정하는 순서는 중요합니다. 연결 프로파일 또는 그룹 정책에 대해 둘 이상의 주소 풀을 구성한 경우 ASA에서는 ASA에 추가된 순서대로 주소 풀을 사용합니다.

IPv4 주소 풀을 정의하려면 IP 주소 범위를 제공합니다. IPv4 주소 풀의 예는 10.10.147.100 - 10.10.147.177입니다.

IPv6 주소 풀을 정의하려면 시작 IP 주소 범위, 주소 접두사 및 풀에 구성할 수 있는 주소 수를 지정합니다. IPv6 주소 풀의 예는 2001:DB8:1::1입니다.

로컬이 아닌 서브넷에서 주소를 할당할 경우 이러한 네트워크에 대한 경로를 보다 쉽게 추가할 수 있도록 서브넷 경계에 속하는 풀을 추가하는 것이 좋습니다.

IP 주소 풀을 생성하려면 다음을 수행합니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 파란색 더하기 버튼  을 클릭하고 **ASA** > **Address Pool(ASA** 주소 풀**)**을 선택합니다.

단계 **3** **Create IP Address Pool(IP** 주소 풀 생성**)** 대화 상자에서 다음 정보를 입력합니다.

- **Object Name(**개체 이름**)** - 주소 풀의 이름을 입력합니다. 최대 64자까지 입력할 수 있습니다.
- **IPv4 address pool(IPv4** 주소 풀**)**: IPv4 주소 풀을 구성하려면 이 라디오 버튼을 선택합니다.
  - **IPv4 Address Range(IPv4** 주소 범위**)**: 구성된 각 풀에서 사용 가능한 첫 번째 IP 주소와 마지막 IP 주소를 입력합니다. 예: 10.10.147.100 - 10.10.147.177.

- **Mask(**마스크**)** - 이 IP 주소 풀이 있는 서브넷을 식별합니다.

- **IPv6 address pool(IPv6** 주소 풀**)**: IPv6 주소 풀을 구성하려면 이 라디오 버튼을 선택합니다.
  - **IPv6** 주소: 구성된 풀에서 사용한 첫 번째 IP 주소 및 접두어 길이를 비트로 입력합니다. <address>/<prefix> 형식. 예: 2001:DB8:1::1/3.
  - **Number of Addresses(**주소 수**)** - 풀에 있는 IP 주소부터 시작하여 IPv6 주소의 수를 식별합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

원격 액세스 VPN 인증서 기반 인증

원격 액세스 VPN은 다음 시나리오에서 보안 게이트웨이 및 AnyConnect 클라이언트(종단)를 인증하기 위해 디지털 인증서를 사용합니다.

중요 CDO는 VPN 헤드엔드(ASA)에서 디지털 인증서 설치를 처리합니다. AnyConnect 클라이언트 디바이스에 대한 인증서 설치는 처리하지 않습니다. 조직의 관리자가 이를 처리해야 합니다.

- VPN 헤드엔드 디바이스(ASA) 식별 및 인증:

  VPN 헤드엔드는 AnyConnect 클라이언트가 VPN 연결을 요청할 때 자신을 식별하고 인증하기 위해 ID 인증서가 필요합니다. CDO를 사용하여 디바이스에 ID 인증서를 설치해야 합니다. PKCS12 또는 인증서 및 키를 사용하여 ID 인증서 설치를 참조하십시오. AnyConnect 클라이언트에 발급자의 CA 인증서를 반드시 설치해야 하는 것은 아닙니다.

  CDO에서 원격 액세스 VPN 구성을 생성하는 동안 등록된 ID 인증서를 디바이스의 외부 인터페이스에 할당하고 구성을 디바이스로 다운로드합니다. ID 인증서는 디바이스의 외부 인터페이스에서 완전히 작동합니다.

  AnyConnect 클라이언트가 VPN에 연결을 시도하면 디바이스는 AnyConnect 클라이언트에 ID 인증서를 제공하여 자체적으로 인증합니다. AnyConnect 클라이언트는 신뢰할 수 있는 CA 인증서로 이 ID 인증서를 확인하고 인증서와 디바이스를 신뢰합니다. CA 인증서가 AnyConnect 클라이언트에 설치되어 있지 않은 경우 메시지가 표시되면 사용자는 디바이스를 수동으로 신뢰해야 합니다.

- AnyConnect 클라이언트 식별 및 인증:

참고 이는 원격 액세스 VPN 구성의 연결 프로파일에서 인증 방법으로 "클라이언트 인증서 전용" 또는 "AAA 및 클라이언트 인증서"를 사용하는 경우에 적용됩니다. "AAA 전용"에는 적용되지 않습니다.

디바이스가 신뢰되면 AnyConnect 클라이언트는 VPN 연결을 완료하기 위해 스스로를 인증해야 합니다. AnyConnect 클라이언트에 ID 인증서를 설치하고 CDO를 사용하여 디바이스에 신뢰할

수 있는 CA 인증서를 설치해야 합니다. 동일한 인증 기관이 이러한 인증서를 발급해야 합니다. ASA에서 신뢰할 수 있는 CA 인증서 설치를 참조하십시오.

AnyConnect 클라이언트는 ID 인증서를 제시하고 디바이스는 신뢰할 수 있는 CA 인증서로 이 인증서를 확인하고 VPN 연결을 설정합니다.

NAT에서 원격 액세스 VPN 트래픽 제외

NAT 제외를 구성하여 NAT 변환에서 원격 액세스 VPN 엔드포인트로 오가는 트래픽을 제외합니다. NAT에서 VPN 트래픽을 제외하지 않는 경우 내부 인터페이스와 외부 인터페이스에 대한 기존 NAT 규칙이 주소의 원격 액세스 VPN 풀에 적용되지 않는지 확인합니다. NAT 제외 규칙은 지정된 소스/대상 인터페이스 및 네트워크 조합에 대한 수동 고정 ID NAT 규칙이며 NAT 정책에서는 반영되지 않고 숨겨집니다. NAT 제외를 활성화하는 경우에는 다음 항목도 구성해야 합니다.

- 내부 인터페이스: 원격 사용자가 액세스할 내부 네트워크의 인터페이스를 선택합니다. NAT 규칙은 이러한 인터페이스에 대해 생성됩니다.
- 내부 네트워크: 원격 사용자가 액세스할 내부 네트워크를 나타내는 네트워크 개체를 선택합니다. 네트워크 목록에는 지원할 주소 풀과 동일한 IP 유형이 포함되어 있어야 합니다.

시작하기 전에

해당 디바이스의 연결 프로파일 및 그룹 정책에서 사용되는 로컬 IP 주소 풀의 구성과 일치하는 ASA 네트워크 개체를 생성합니다. 이러한 네트워크 개체는 NAT 규칙을 구성할 때 대상 주소 및 변환된 주소로 할당되어야 합니다. ASA 네트워크 개체 생성의 내용을 참조하십시오.

프로시저

단계 **1** 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

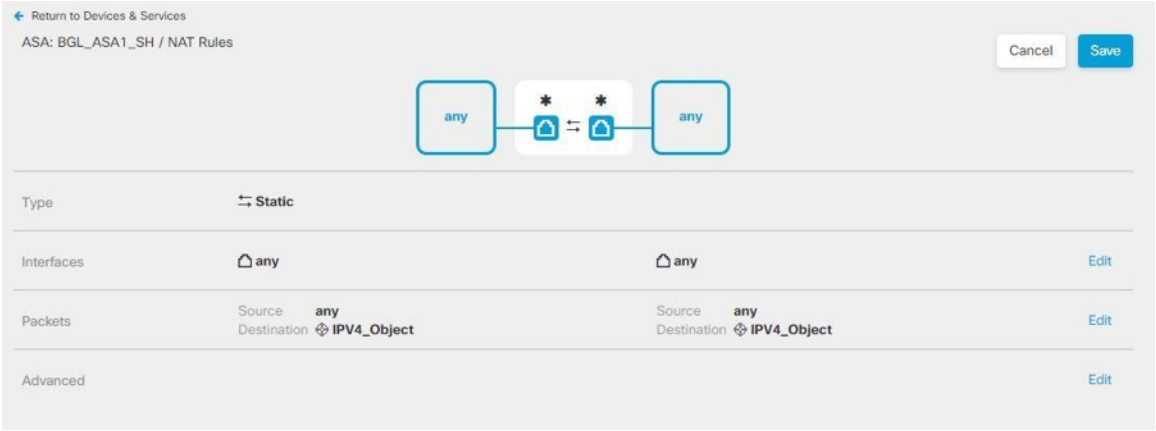
단계 **2** **Inventory(**재고 목록**)** 필터 및 검색 필드를 사용하여 NAT 규칙을 생성하려는 ASA 디바이스를 찾습니다.

단계 **3** 상세정보 패널의 **Management(**관리**)** 영역에서 **NAT** NAT를 클릭합니다.

단계 **4** + > **Twice NAT(2**회 **NAT)**를 클릭합니다.

1. 섹션 1에서 **Static(**정적**)**을 선택합니다. **Continue(**계속**)**를 클릭합니다.
2. 섹션 2에서 **Source Interface(**소스 인터페이스**)** = 'any' 및 **Destination Interface(**대상 인터페이스**)** = 'any'를 선택합니다. **Continue(**계속**)**를 클릭합니다.
3. 섹션 3에서 **Source Original Address(**소스 원본 주소**)** = 'any' 및 **Source Translated Address(**소스 변환 주소**)** = 'any'를 선택합니다.
4. **Use Destination(**대상 사용**)**을 선택합니다.
    1. **Destination Original Address(**대상 원본 주소**)** 및 **Source Translated Address(**소스 변환 주소**)**: 드롭다운에서 **Choose(**선택**)**를 클릭하고 로컬 IP 주소 풀의 구성과 일치하는 네트워크 개체를 선택합니다. 아래 예에서 'IPV4_Object'는 ASA(BGL_ASA1_SH) 디바이스의 연결 프로파일 및 그룹 정책 설정에서 사용되는 IPv4 주

소 풀 개체와 동일한 구성을 가진 네트워크 개체입니다.



2. **Disable proxy ARP for Incoming packet(**수신 패킷에 대해 프록시 **ARP** 비활성화**)**을 선택합니다.
3. **Save(**저장**)**를 클릭합니다.
4. 4단계부터 프로세스를 반복하여 IP 주소 풀에 해당하는 다른 각 네트워크 개체에 대해 동일한 규칙을 생성합니다.

단계 **5** 디바이스에 대한 구성 변경 사항 미리보고 구축합니다.

ASA에서 사용자가 AnyConnect 클라이언트 소프트웨어 설치

VPN 연결을 완료하려면 사용자가 AnyConnect 클라이언트 소프트웨어를 설치해야 합니다. 기존 소프트웨어 배포 방법을 사용하여 소프트웨어를 직접 설치할 수 있습니다. 또는 사용자가 ASA 디바이스에서 AnyConnect 클라이언트를 직접 설치하게 할 수도 있습니다.

Note 소프트웨어를 설치하려면 사용자에게 워크스테이션에 대한 관리자 권한이 있어야 합니다.

사용자가 ASA 디바이스에서 소프트웨어를 처음 설치하도록 하려면 사용자에게 다음 단계를 수행하도록 하십시오.

Note Android 및 iOS 사용자는 해당 앱 스토어에서 AnyConnect를 다운로드해야 합니다.

Procedure

단계 **1** 웹 브라우저를 사용하여 **https://** *ravpn-address*를 엽니다. 여기서 *ravpn-address*는 VPN 연결을 허용할 외부 인터페이스의 IP 주소 또는 호스트 이름입니다. 원격 액세스 VPN을 구성할 때 이 인터페이스를 식별합니다. 시스템에서 사용자에게 로그인하라는 메시지를 표시합니다.

단계 **2** 사이트에 로그인합니다. 사용자는 원격 액세스 VPN용으로 구성된 디렉터리 서버를 사용하여 인증을 합니다. 로그인이 성공해야 설치를 계속할 수 있습니다. 로그인이 성공하면 시스템은 사용자에게 필요한 AnyConnect 클라이언트 버전이 이미 있는지를 확인합니다. 사용자 컴퓨터에 AnyConnect 클라이언트가 없거나 클라이언트가 하위 레벨인 경우에는 시스템에서 AnyConnect 소프트웨어 설치를 자동으로 시작합니다. 설치가 완료되면, AnyConnect에서 원격 액세스 VPN 연결을 완료합니다.

ASA 원격 액세스 VPN 구성 수정

ASA 디바이스가 CDO에 온보딩되면 온보딩된 ASA 디바이스에서 기존 원격 액세스 VPN 구성을 검색하고 표시합니다. 자세한 내용은 기존 ASA Remote Access VPN 설정 관리 및 구축을 참조하십시오.

이러한 구성을 수정하고 새 구성을 디바이스에 다운로드할 수 있습니다.

프로시저

단계 **1** 왼쪽 창에서 **VPN** > **Remote Access VPN Configuration(**원격 액세스 **VPN** 구성**)**을 클릭합니다.

단계 **2** VPN 구성에 그룹 정책을 추가하거나 제거하려면 온보딩된 ASA 디바이스와 연결된 VPN 구성을 클릭합니다. 왼쪽의 Actions(작업) 창에서 **Group Policies(**그룹 정책**)**를 클릭합니다.

a) 파란색 + 아이콘을 클릭하고 선택 항목을 구성한 다음 Select(선택)를 클릭합니다.

b) Save(저장)를 클릭합니다. ASA 원격 액세스 VPN 그룹 정책 생성할 수도 있습니다.

단계 **3** VPN 구성을 클릭하고 **Actions(**작업**)** 창에서 **Edit(**편집**)**를 클릭합니다.

마법사는 구성과 연결된 ASA 디바이스를 나열합니다.

a) 생성된 것과 동일한 방식으로 다음 세부 정보를 수정할 수 있습니다.

- 원격 액세스 VPN 구성의 이름을 변경합니다.
- 디바이스 세부 정보를 표시하는 행에 나타나는 점 3개를 클릭하고 **Edit(**편집**)**를 클릭합니다.

자세한 내용은 ASA 원격 액세스 VPN 구성 생성, 49 페이지 항목을 참조하십시오.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축

ASA 연결 프로파일 수정

프로시저

단계 1 왼쪽 창에서 **VPN** > **Remote Access VPN Configuration(**원격 액세스 **VPN** 구성**)**을 클릭합니다.

단계 2 온보딩된 ASA 디바이스와 연결된 VPN 구성을 확장하고 연결 프로파일을 선택합니다.

단계 3 **Actions(**작업**)** 아래에서 **Edit(**편집**)**를 클릭합니다.

단계 4 생성된 것과 동일한 방식으로 값을 편집하고 **Done(**완료**)**을 클릭합니다.

자세한 내용은 ASA 원격 액세스 VPN 연결 프로파일 구성, 53 페이지을 참조하십시오.

단계 5 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축

RA VPN AnyConnect 클라이언트 프로파일 업로드

원격 액세스 VPN AnyConnect 클라이언트 프로파일은 파일에 저장된 구성 매개변수의 그룹입니다. 핵심 클라이언트 VPN 기능과 선택적 클라이언트 모듈인 Network Access Manager, AMP Enabler, ISE Posture, 네트워크 가시성, 고객 피드백 경험 프로파일, Umbrella 로밍 보안 및 웹 보안에 대한 구성 설정을 포함하는 다양한 AnyConnect 클라이언트 프로파일이 있습니다.

CDO는 이러한 프로파일을 나중에 그룹 정책에서 사용할 수 있는 개체로 업로드할 수 있습니다.

- **AnyConnect VPN** 프로파일 — AnyConnect 클라이언트 프로파일은 AnyConnect 클라이언트 소프트웨어와 함께 클라이언트에 다운로드됩니다. 이러한 프로파일은 시작 시의 자동 연결 및 자동 다시 연결, 그리고 엔드 유저가 AnyConnect 클라이언트 환경 설정 및 고급 설정에서 옵션을 변경할 수 있는지 여부와 같은 여러 클라이언트 관련 옵션을 정의합니다. CDO은 XML 파일 형식을 지원합니다.
- **AMP Enabler** 서비스 프로파일 - 이 프로파일은 AnyConnect AMP Enabler에 사용됩니다. 원격 액세스 VPN 사용자가 VPN에 연결하면 AMP Enabler 및 이 프로파일이 FDM 관리 디바이스에서 엔드포인트로 푸시됩니다. CDO는 XML 및 ASP 파일 형식을 지원합니다.
- 피드백 프로파일 - 고객 경험 피드백 프로파일을 추가하고 이 유형을 선택하여 고객이 활성화하고 사용하는 기능 및 모듈에 대한 정보를 수신할 수 있습니다. CDO는 FSP 파일 형식을 지원합니다.
- **ISE Posture** 프로파일 - AnyConnect ISE Posture 모듈용 프로파일 파일을 추가하는 경우 이 옵션을 선택합니다. CDO는 XML 및 ISP 파일 형식을 지원합니다.
- **Network Access Manager** 서비스 프로파일 - Network Access Manager 프로파일 편집기를 사용하여 NAM 프로파일 파일을 설정하고 추가합니다. CDO는 NSP 파일 형식을 지원합니다.
- 네트워크 가시성 서비스 프로파일 - AnyConnect 네트워크 가시성 모듈의 프로파일 파일입니다. NVM 프로파일 편집기를 사용하여 프로파일을 생성할 수 있습니다. CDO는 XML 및 NVMSP 파일 형식을 지원합니다.

- **Umbrella** 로밍 보안 프로파일 - Umbrella 로밍 보안 모듈을 구축하는 경우 이 파일 유형을 선택해야 합니다. CDO는 XML 및 JSON 파일 형식을 지원합니다.
- 웹 보안 서비스 프로파일 - 웹 보안 모듈용 프로파일 파일을 추가할 때 이 파일 유형을 선택합니다. CDO는 XML, WSO 및 WSP 파일 형식을 지원합니다.

Before you begin

적합한 GUI 기반 AnyConnect 프로필 편집기를 사용하여 필요한 프로파일을 생성합니다. AnyConnect Secure Mobility Client 범주의 Cisco 소프트웨어 다운로드 센터에서 프로파일 편집기를 다운로드하고 AnyConnect "프로파일 편집기 - Windows/독립형 설치 프로그램(MSI)"을 설치할 수 있습니다. 프로파일 편집기 설치 프로그램에는 독립형 버전의 프로파일 편집기가 포함되어 있습니다. 설치 파일은 Windows 전용이며 파일 이름은 anyconnect-profileeditor-win-<version>-k9.msi입니다. 여기서 <version>은 AnyConnect 버전입니다. 예를 들면 anyconnect-profileeditor-win-4.3.04027-k9.msi와 같습니다. 또한 프로파일 편집기를 설치하기 전에 Java JRE 1.6 이상도 설치해야 합니다.

Umbrella 로밍 보안 프로파일 편집기를 제외하고 이 패키지에는 모듈을 생성하는 데 필요한 모든 프로파일 편집기가 포함되어 있습니다. 자세한 내용은 Cisco AnyConnect Secure Mobility Client 관리자 가이드에서 해당 릴리스의 *AnyConnect* 프로파일 편집기 장을 참조하십시오. Umbrella 대시보드와 별도로 Umbrella 로밍 보안 프로파일을 다운로드합니다. 자세한 내용은 Cisco Umbrella 사용 가이드의 "Umbrella 로밍 보안" 장에서 "Umbrella 대시보드에서 AnyConnect 로밍 보안 프로필 다운로드" 섹션을 참고하십시오.

Procedure

단계 **1** 왼쪽 창에서 개체를 선택합니다.

단계 **2** 파란색 더하기  버튼을 클릭합니다.

단계 **3** **RA VPN Objects (ASA & FDM)(RA VPN** 개체**(ASA** 및 **FDM))** > **AnyConnect Client Profile(AnyConnect** 클라이언트 프로파일**)**를 클릭합니다.

단계 **4** **Object Name(**개체 이름**)** 필드에 AnyConnect 클라이언트 프로파일의 이름을 입력합니다.

단계 **5** **Browse(**찾아보기**)**를 클릭하고 프로파일 편집기를 사용하여 생성한 파일을 선택합니다.

단계 **6** **Open(**열기**)**을 클릭하여 프로파일을 업로드합니다.

단계 **7** **Add(**추가**)**를 클릭하여 개체를 추가합니다.

관련 정보**:**

- RA VPN 그룹 정책 창에서 클라이언트 모듈을 AnyConnect VPN 프로파일과 연결합니다. ASA 원격 액세스 VPN 그룹 정책 생성 을 참조하십시오.

Note 클라이언트 모듈 연결은 소프트웨어 버전 6.7 이상을 실행하는 모든 ASA 버전 및 FDM에서 지원됩니다.

ASA 원격 액세스 VPN 구성 검증

원격 액세스 VPN을 구성하고 디바이스에 구성을 배포한 후에는 원격 연결을 수행할 수 있는지 확인합니다.

Procedure

단계 **1** 외부 네트워크에서 AnyConnect 클라이언트를 사용하여 VPN 연결을 설정합니다. 웹 브라우저를 사용하여 **https://** *ravpn-address*를 엽니다. 여기서 *ravpn-address*는 VPN 연결을 허용할 외부 인터페이스의 IP 주소 또는 호스트 이름입니다. 필요한 경우, 클라이언트 소프트웨어를 설치하여 연결을 완료합니다. ASA에서 사용자가 AnyConnect 클라이언트 소프트웨어 설치 을 참조하십시오. 그룹 URL을 구성한 경우, 그룹 URL도 시도해 보십시오.

단계 **2** **Inventory(**재고 목록**)** 페이지에서 확인하려는 디바이스(FTD 또는 ASA)를 선택하고 **Device Actions(**디바이스 작업**)**에서 **Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **3** **show vpn-sessiondb** 명령을 사용하여 현재 VPN 세션에 대한 요약 정보를 봅니다.

단계 **4** 통계에는 활성 AnyConnect 클라이언트 세션, 누적 세션에 대한 정보, 최대 동시 세션 수, 비활성 세션이 표시되어야 합니다. 다음은 명령의 샘플 출력입니다.

```
> show vpn-sessiondb
----------------------------------------------------------------------------
VPN Session Summary
----------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ----------------------------------------------
AnyConnect Client          :      1 :         49 :           3 :        0
  SSL/TLS/DTLS             :      1 :         49 :           3 :        0
Clientless VPN             :      0 :          1 :           1
  Browser                  :      0 :          1 :           1
----------------------------------------------------------------------------


  Total Active and Inactive    :      1             Total Cumulative :     50
  Device Total VPN Capacity    :  10000
  Device Load                  :     0%
  ----------------------------------------------------------------------------

  ----------------------------------------------------------------------------
  Tunnels Summary
  ----------------------------------------------------------------------------
                               Active : Cumulative : Peak Concurrent
                              ----------------------------------------
  Clientless                  :      0 :          1 :               1
  AnyConnect-Parent           :      1 :         49 :               3
  SSL-Tunnel                  :      1 :         46 :               3
  DTLS-Tunnel                 :      1 :         46 :               3
  ----------------------------------------------------------------------------
  Totals                      :      3 :        142
  ----------------------------------------------------------------------------

  ----------------------------------------------------------------------------
  IPv6 Usage Summary
  ----------------------------------------------------------------------------
                               Active : Cumulative : Peak Concurrent
                              ----------------------------------------
  AnyConnect SSL/TLS/DTLS     :      :            :
    Tunneled IPv6             :      1 :         20 :               2
  ----------------------------------------------------------------------------
```

단계 **5** **show vpn-sessiondb anyconnect** 명령을 사용하여 현재 AnyConnect VPN 세션에 대한 세부 정보를 봅니다. 세부 정보에는 사용된 암호화, 전송 및 수신한 바이트 수, 기타 통계 정보가 포함됩니다. VPN 연결을 사용하면 이 명령을 다시 호출할 경우 전송/수신한 바이트 수 변경 사항이 표시되어야 합니다.

단계 **6** **show vpn-sessiondb anyconnect** 명령을 사용하여 현재 AnyConnect VPN 세션에 대한 세부 정보를 봅니다. 세부 정보에는 사용된 암호화, 전송 및 수신한 바이트 수, 기타 통계 정보가 포함됩니다. VPN 연결을 사용하면 이 명령을 다시 호출할 경우 전송/수신한 바이트 수 변경 사항이 표시되어야 합니다.

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : User1                  Index        : 4820
Assigned IP  : 172.18.0.1             Public IP    : 192.168.2.20
Assigned IPv6: 2009::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 27731                  Bytes Rx     : 14427
Group Policy : MyRaVpn|Policy         Tunnel Group : MyRaVpn
Login Time   : 21:58:10 UTC Mon Apr 10 2017
Duration     : 0h:51m:13s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a800fd012d400058ebfff2
Security Grp : none                   Tunnel Zone : 0
```

ASA 원격 액세스 VPN 구성 세부 정보 보기

Procedure

단계 **1** 왼쪽 창에서 **VPN** > **ASA/FDM Remote Access VPN Configuration(**원격 액세스 **VPN** 구성**)**을 클릭합니다.

단계 **2** 존재하는 VPN 구성 개체를 클릭합니다. 현재 얼마나 많은 연결 프로파일 및 그룹 정책이 구성되어 있는지 나타내는 요약 정보를 그룹에서 표시합니다.

- 원격 액세스 VPN 구성을 확장하여 연결된 모든 연결 프로파일을 확인합니다.
  - 추가 + 버튼을 클릭하여 새 연결 프로파일을 추가합니다.
  - 보기 버튼( )을 클릭하여 연결 프로파일 및 연결 지침에 관한 요약 정보를 엽니다. **Actions(**작업**)** 아래에서 **Edit(**편집**)**를 클릭하여 변경 사항을 편집할 수 있습니다.
- **Actions(**작업**)** 아래의 다음 옵션 중 하나를 클릭하여 추가 작업을 수행할 수 있습니다.
  - 그룹 정책을 할당/추가하려면 **Group Policies(**그룹 정책**)**를 클릭합니다.
  - 더 이상 필요하지 않은 구성 개체 또는 연결 프로파일을 클릭하고 **Remove(**제거**)**를 클릭하여 삭제합니다.

원격 액세스 가상 프라이빗 네트워크 세션

원격 액세스 가상 프라이빗 네트워크는 모바일 사용자 또는 재택 근무자와 같은 원격 사용자에게 보안 연결을 제공합니다. 이러한 연결을 모니터링하면 연결 및 사용자 세션 성능에 대한 중요한 지표를 한눈에 확인할 수 있습니다. CDO 원격 액세스 VPN 모니터링 기능을 사용하면 원격 액세스 VPN 문

제의 존재 여부와 그 위치를 신속하게 파악할 수 있습니다. 그런 다음 이 정보를 적용하고 네트워크 관리 도구를 사용하여 네트워크 및 사용자의 문제를 줄이거나 없앨 수 있습니다. 필요에 따라 원격 액세스 VPN 세션의 연결을 끊을 수도 있습니다.

Remote Access Virtual Private Monitoring(원격 액세스 가상 프라이빗 모니터링) 페이지는 다음 정보를 제공합니다.

- 최대 1년 동안의 활성 및 기록 세션 목록입니다.
- CDO에서 관리하는 모든 활성 VPN 헤드엔드의 보기를 한눈에 볼 수 있도록 직관적인 그래픽 시각적 개체를 표시합니다.
- 라이브 세션 화면에는 CDO 테넌트에서 가장 많이 사용되는 운영 체제 및 VPN 연결 프로파일이 표시됩니다. 또한 평균 세션 기간과 업로드 및 다운로드한 데이터도 표시됩니다.
- 디바이스 유형, 디바이스 이름, 세션 길이, 전송 및 수신된 데이터의 양과 같은 기준을 기반으로 검색 범위를 좁힐 수 있는 필터링 기능입니다.

관련 정보:

- 라이브 AnyConnect 원격 액세스 VPN 세션 모니터링, on page 77
- 기록 AnyConnect 원격 액세스 VPN 세션 모니터링, on page 79
- 원격 액세스 VPN 세션 검색 및 필터링
- 원격 액세스 VPN 모니터링 보기 사용자 지정
- 원격 액세스 VPN 세션을 CSV 파일로 내보내기
- 사용자의 모든 활성 RA VPN 세션 연결 끊기

라이브 AnyConnect 원격 액세스 VPN 세션 모니터링

디바이스의 활성 AnyConnect 원격 액세스 VPN 세션에서 실시간 데이터를 모니터링할 수 있습니다. 이 데이터는 10분마다 자동으로 새로 고쳐집니다. 언제든지 최신 세션 목록을 검색하려면 화면 오른쪽 모서리에 나타나는 다시 로드 아이콘 을 클릭하십시오.

시작하기 전에

- 원격 액세스 VPN 헤드 엔드를 CDO에 온보딩합니다.
- 라이브 데이터를 모니터링하려는 디바이스의 연결 상태는 **Security Devices(**보안 디바이스**)** 페이지에서 "Online(온라인)"인지 확인합니다.

프로시저

단계 **1** 왼쪽 창에서 **VPN** > **Remote Access VPN Monitoring(**원격 액세스 **VPN** 모니터링**)**을 클릭합니다.

단계 **2** **RA VPN**을 클릭합니다.

단계 3 **Live(**라이브**)**를 클릭합니다.

원격 액세스 VPN 세션 검색 및 필터링하여 디바이스 유형, 세션 길이, 업로드 및 다운로드 데이터 범위와 같은 기준에 따라 검색 범위를 좁힐 수 있습니다.

참고
데이터 **TX** 및 데이터 **RX** 정보는 FTD에서 사용할 수 없습니다.

라이브 원격 액세스 VPN 데이터 보기

라이브 데이터는 대시보드 및 테이블 형식으로 표시됩니다.

Dashboard(대시보드) 보기

대시보드를 보려면 화면의 오른쪽 상단 모서리에 나타나는 **Show Charts View(**차트 보기 표시**)** 아이콘을 클릭해야 합니다.

대시보드는 CDO에서 관리하는 모든 활성 VPN 헤드엔드의 보기를 한눈에 확인할 수 있도록 제공합니다.

- **Breakdown (All Devices)(**애널리틱스 데이터**(**모든 디바이스**))**: 총 라이브 세션 수를 표시합니다. 4개의 호 길이로 구분된 원도표도 표시됩니다. 세션 수가 가장 많은 상위 3개 디바이스의 VPN 세션 비율을 보여줍니다. 나머지 호 길이는 다른 디바이스의 어그리게이션를 나타냅니다.
- CDO 테넌트에서 가장 많이 사용되는 운영 체제 및 연결 프로파일이 표시됩니다.
- 평균 세션 기간과 업로드 및 다운로드한 데이터도 표시됩니다.
- **Active Sessions by Country(**국가별 활성 세션**)**: RA VPN 헤드엔드에 연결된 사용자 위치의 인터랙티브 히트맵을 표시합니다.
  - 사용자가 연결한 국가는 해당 국가에서 설정된 세션의 상대적 비율에 따라 점점 더 짙은 파란색 음영으로 표시됩니다. 파란색이 어두울수록 해당 국가에서 더 많은 세션이 설정되었음을 의미합니다.
  - 맵의 맨 아래에 있는 범례는 국가의 세션 수와 국가를 표시하는 데 사용되는 파란색 음영 간의 상관관계를 나타내는 척도를 제공합니다.
  - 맵에 마우스 포인터를 올려놓으면 해당 국가의 이름 및 해당 국가에서 설정된 총 활성 사용자 세션 수를 확인할 수 있습니다.
  - 테이블 위에 마우스 포인터를 올려놓으면 해당 국가의 위치와 맵의 총 활성 사용자 세션 수를 확인할 수 있습니다.

테이블 형식 보기

데이터를 테이블 형식으로 보려면 화면의 오른쪽 상단 모서리에 있는 **Show Tabular View(**테이블 형식 보기 표시**)** 아이콘을 클릭합니다.

테이블 형식은 현재 연결된 VPN 사용자의 전체 목록을 제공합니다.

- **Location(위치)** 열에는 공용 IP 주소를 지리위치 지정하여 VPN 헤드엔드에 연결된 모든 사용자의 위치가 표시됩니다. 사용자 상세정보를 보려면 행을 클릭합니다. 왼쪽 창의 위치 링크를 클릭하면 사용자의 위치가 Google 맵에 표시됩니다.

중요 CDO는 라이브 데이터에 표준 필터를 적용하고 대시보드에 표시합니다. 사용자 지정 필터는 시각적 대시보드 보기에서 지원되지 않으므로, 테이블 형식 데이터가 표시되는 경우에만 새 필터를 적용할 수 있습니다. 적용한 모든 필터를 제거하려면 **Clear(지우기)**를 클릭합니다. 표준 필터는 제거할 수 없습니다.

원격 액세스 VPN 세션 검색 및 필터링 기능을 사용하여 디바이스 유형, 세션 길이, 업로드 및 다운로드 데이터 범위와 같은 기준에 따라 검색 범위를 좁힐 수 있습니다. 한 번에 최대 10,000개의 결과를 표시할 수 있습니다.

Status(상태) 열에 **Active(활성)** 레이블이 있는 녹색 점은 활성 VPN 사용자의 세션을 나타냅니다.

기록 AnyConnect 원격 액세스 VPN 세션 모니터링

지난 3개월 동안 기록된 AnyConnect 원격 액세스 VPN 세션의 기록 데이터를 모니터링할 수 있습니다.

시작하기 전에

- RA VPN 헤드 엔드를 CDO에 온보딩합니다.

프로시저

단계 **1** 왼쪽 창에서 **VPN** > **Remote Access VPN Monitoring(원격 액세스 VPN 모니터링)**을 클릭합니다.

단계 **2** **RA VPN**을 클릭합니다.

단계 **3** **Historical(기록)**을 클릭합니다.

- 원격 액세스 VPN 세션 데이터는 저장되며 1년간 조회할 수 있습니다.
- 원격 액세스 VPN 세션 검색 및 필터링 기능을 사용하여 디바이스 유형, 세션 길이, 업로드 및 다운로드 데이터 범위와 같은 기준에 따라 검색 범위를 좁힐 수 있습니다.
- 데이터 **TX** 및 데이터 **RX** 정보는 Secure Firewall Threat Defense에서 사용할 수 없습니다.

원격 액세스 **VPN** 데이터 기록 보기

이력 데이터는 대시보드 및 표 형식으로 표시됩니다.

Dashboard(대시보드**)** 보기

대시보드를 보려면 화면의 오른쪽 상단에 나타나는 **Show Charts View(**차트 보기 표시**)** 아이콘을 클릭해야 합니다. 테이블 보기와 함께 대시보드 보기가 표시됩니다.

대시보드는 CDO에서 관리하는 모든 활성 VPN 헤드엔드의 보기를 한눈에 확인할 수 있도록 제공합니다. 지난 24시간, 7일 및 30일 동안 모든 디바이스에 대해 기록된 VPN 세션을 보여주는 막대 그래프를 제공합니다. 드롭다운에서 기간을 선택할 수 있습니다. 개별 막대에 마우스 커서를 대면 해당 날짜의 총 세션 수와 날짜를 확인할 수 있습니다.

테이블 형식 보기

대시보드를 보려면 화면의 오른쪽 상단에 나타나는 **Show Tabular View(**테이블 형식 보기 표시**)** 아이콘을 클릭하여 테이블 형식 보기만 표시해야 합니다. 테이블 형식은 지난 1년 동안 연결된 VPN 사용자의 전체 목록을 제공합니다.

Location(위치**)** 열에는 공용 IP 주소를 지리위치 지정하여 VPN 헤드엔드에 연결된 모든 사용자의 위치가 표시됩니다. 사용자 상세정보를 보려면 행을 클릭합니다. 왼쪽 창의 위치 링크를 클릭하면 사용자의 위치가 Google 맵에 표시됩니다.

중요 CDO는 기록 데이터에 표준 필터를 적용하고 대시보드에 표시합니다. 대시보드는 맞춤형 필터를 지원하지 않으므로 테이블 형식 데이터가 표시되는 경우에만 새 필터를 적용할 수 있습니다. 새로 적용된 필터를 지우면 대시보드가 다시 실행됩니다. 화면에서 **Clear(**지우기**)**를 클릭하여 수동으로 적용된 필터를 제거합니다. 표준 필터는 제거할 수 없습니다.

원격 액세스 VPN 세션 검색 및 필터링 기능을 사용하여 세션 날짜와 시간 범위, 세션 길이, 업로드 및 다운로드 데이터 범위와 같은 기준에 따라 검색 범위를 좁힐 수 있습니다. 한 번에 최대 10,000개의 결과를 표시할 수 있습니다.

Status(상태) 열에 **Active(**활성**)** 레이블이 있는 녹색 점은 활성 VPN 사용자의 세션을 나타냅니다.

원격 액세스 VPN 세션 검색 및 필터링

검색

검색 창 기능을 사용하여 원격 액세스 VPN 세션을 찾습니다. 검색 창에 디바이스 이름, IP 주소 또는 일련 번호를 입력하기 시작합니다. 그러면 검색 기준에 맞는 원격 액세스 VPN 세션이 표시됩니다. 검색은 대/소문자를 구분하지 않습니다.

필터

필터 사이드바를 사용하여 세션 시간 범위, 세션 길이, 업로드 및 다운로드 데이터 범위 등의 기준에 따라 원격 액세스 VPN 세션을 찾습니다. 필터 기능은 라이브 보기와 기록 보기 모두에서 사용할 수 있습니다.

- **Filter by Devices(**디바이스별 필터링**)**: **All Types(**모든 유형**)** 탭에서 하나 또는 모든 디바이스를 선택하여 선택한 디바이스의 세션을 봅니다. 창은 또한 유형에 따라 디바이스를 분류하고 해당 탭 아래에 표시합니다.

- **Sessions Time Range(**세션 시간 범위**)**(기록 데이터에만 적용 가능): 지정된 날짜 및 시간 범위의 기록 세션을 표시합니다. 지난 3개월 동안 기록된 데이터를 볼 수 있습니다.
- **Sessions Length(**세션 길이**)**: 지정된 세션의 기간 길이를 기준으로 세션을 표시합니다. 시간 단위(시간, 분 또는 초)를 설정하고 슬라이더를 이동하여 최소 및 최대 기간 길이를 지정합니다. 제공된 필드에 길이를 지정할 수도 있습니다.
- **Upload (TX)(**업로드**(TX))**: 보안 네트워크에 업로드되거나 전송된 데이터의 지정된 양을 기준으로 세션을 표시합니다. 단위(GB, MB 또는 KB)를 설정하고 그에 따라 슬라이더를 이동하여 범위를 선택합니다. 사용 가능한 필드에 값을 지정할 수도 있습니다.
- **Download (RX)(**다운로드**(RX))**: 보안 네트워크에서 다운로드하거나 수신한 지정된 데이터 양을 기준으로 세션을 표시합니다. 단위(GB, MB 또는 KB)를 설정하고 그에 따라 슬라이더를 이동하여 범위를 선택합니다. 사용 가능한 필드에 값을 지정할 수도 있습니다.

원격 액세스 VPN 모니터링 보기 사용자 지정

원하는 보기에 적용되는 열 헤더만 포함하도록 라이브 및 기록 모드에서 원격 액세스 VPN 모니터링 보기를 편집할 수 있습니다. 열 오른쪽에 있는 열 필터 아이콘 을 클릭하고 원하는 열을 선택하거나 선택 취소합니다.

CDO는 다음에 CDO에 로그인할 때 선택 항목을 기억합니다.

원격 액세스 VPN 세션을 CSV 파일로 내보내기

하나 이상의 디바이스의 원격 엑세스 VPN 세션을 쉼표로 구분된 값(.csv) 파일로 내보낼 수 있습니다. Microsoft Excel과 같은 스프레드시트 애플리케이션에서 .csv 파일을 열어 목록의 항목을 정렬하고 필터링할 수 있습니다. 이 정보는 원격 액세스 VPN 세션을 분석하는 데 도움이 됩니다. 세션을 내보낼 때마다 CDO는 새 .csv 파일을 생성합니다. 생성된 파일에는 이름에 날짜와 시간이 포함되어 있습니다.

CDO는 최대 100,000개의 활성 세션을 CSV 파일로 내보낼 수 있습니다. 모든 디바이스의 총 세션 수가 최대 제한을 초과하는 경우 **View By Device(**디바이스별 보기**)** 필터를 사용하여 개별 디바이스에 대한 보고서를 생성할 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 **VPN** > **Remote Access VPN Monitoring(**원격 액세스 **VPN** 모니터링**)**을 클릭합니다.

단계 **2** **View By Devices(**디바이스별 보기**)** 영역에서 다음 중 하나를 선택합니다.

- **All Devices(**모든 디바이스**)** - 그 아래에 나열된 모든 디바이스에서 활성 세션을 내보냅니다.
- 해당 디바이스의 세션을 내보낼 디바이스를 클릭합니다.

단계 **3** 오른쪽 상단에 있는 아이콘을 클릭하면 CDO는 화면에 표시되는 규칙을 .csv 파일로 내보냅니다.

단계 4 스프레드시트 애플리케이션에서 .csv 파일을 열어 결과를 정렬하고 필터링합니다.

원격 액세스 VPN 대시보드

CDO는 ASA , 클라우드 제공 Firewall Management Center 매니지드 Threat Defense및 FDM 관리 디바이스의 원격 액세스 VPN 연결에 대한 통합 정보를 제공합니다.

왼쪽 창에서 **Dashboard(**대시보드**)**를 클릭합니다. 원격 액세스 **VPN** 세션 은 다음 위젯의 정보를 제공합니다.

- **VPN Tunnel Status(VPN** 터널 상태**)**: 활성 및 유휴 VPN 터널을 각각 적절한 색상으로 나타내는 원형 차트가 표시됩니다. 이 차트는 헤드엔드별 상위 10개의 원격 액세스 VPN 세션 수를 보여줍니다.
- **Statistics(**통계**)**: 평균 세션 기간과 업로드 및 다운로드한 데이터를 표시합니다.

View All 원격 액세스 **VPN Sessions(**모든 원격 액세스 **VPN** 세션 보기**)**를 클릭하면 모든 라이브 세션 및 기록 세션을 나열하는 원격 액세스 모니터링 페이지로 이동합니다.

ASA 사용자의 원격 액세스 VPN 세션 연결 끊기

ASA 디바이스에서 모든 사용자의 모든 활성 원격 액세스 VPN 세션을 종료할 수 있습니다. 라이브 모드와 기록 모드 모두에서 이 작업을 수행할 수 있습니다.

CDO는 사용자가 VPN 세션을 보고 종료할 수 있도록 VPN 세션 관리자 사용자 역할을 제공합니다. 자세한 내용은 사용자 역할을 참조하십시오.

Procedure

단계 1 왼쪽 창에서 **VPN** > **Remote Access VPN Monitoring(**원격 액세스 **VPN** 모니터링**)**을 클릭합니다.
단계 2 디바이스별 보기 영역에서 해당 디바이스의 모든 활성 세션을 종료하려는 ASA 디바이스를 클릭합니다.
단계 3 오른쪽 상단에 나타나는 **Terminate All Sessions(**모든 세션 종료**)**를 클릭합니다.
단계 4 **Yes, Terminate All Sessions(**예**,** 모든 세션을 종료합니다**)**를 클릭하여 선택을 확인합니다.

사용자의 모든 활성 RA VPN 세션 연결 끊기

사용자의 연결을 끊으면 CDO는 해당 ASA 디바이스에서 사용자의 모든 활성 RA VPN 세션을 종료합니다. 라이브 모드와 기록 모드 모두에서 이 작업을 수행할 수 있습니다.

Procedure

단계 1 왼쪽 창에서 **VPN** > **Remote Access VPN Monitoring(**원격 액세스 **VPN** 모니터링**)**을 클릭합니다.
단계 2 세션의 연결을 끊을 사용자를 검색합니다. **Search(**검색**)** 막대에 검색 기준을 입력할 수 있습니다.

단계 **3** 활성 세션을 클릭하고 오른쪽의 **Actions(**작업**)** 창에서 **Terminate all RA VPN sessions for this user(**이 사용자에 대한 모든 **RA VPN** 세션 종료**)** 링크를 클릭합니다.