사이트 대 사이트 VPN

VPN(Virtual Private Network)은 인터넷과 같은 공개 소스나 기타 네트워크를 통해 원격 피어 간에 보안 터널을 설정하는 네트워크 연결입니다. VPN은 터널을 사용하여 IP 기반 네트워크를 통해 전달할 수 있도록 일반 IP 패킷 내의 데이터 패킷을 캡슐화합니다. VPN은 암호화를 사용해 개인 정보와 인증을 확인함으로써 데이터의 무결성을 보장합니다.

VPN 기본 사항

터널링을 통해 인터넷과 같은 공용 TCP/IP 네트워크를 사용하고 원격 사용자와 사설 기업 네트워크 간의 안전한 연결을 생성할 수 있습니다. 각 보안 연결을 터널이라고 부릅니다.

IPsec 기반 VPN 기술은 ISAKMP/IKE(Internet Security Association and Key Management Protocol) 및 IPsec 터널링 표준을 사용하여 터널을 작성하고 관리합니다. ISAKMP 및 IPsec는 다음 사항을 수행합니다.

- 터널 파라미터 협상
- 터널 설정
- 사용자 및 데이터 인증
- 보안 키 관리
- 데이터 암호화 및 암호 해독
- 터널을 통한 데이터 전송 관리
- 터널 엔드포인트 또는 라우터로 데이터 전송 인바운드 및 아웃바운드 관리

VPN의 디바이스는 양방향 터널 엔드포인트로 작동합니다. 사설 네트워크에서 일반 패킷을 수신하여 캡슐화하고 터널을 생성하며, 캡슐 해제하여 최종 대상에 전송하는 다른 쪽 터널의 끝으로 보낼

수 있습니다. 또한 공용 네트워크에서 캡슐화된 패킷을 수신하여 캡슐을 해제하여 사설 네트워크의 최종 대상에 보낼 수 있습니다.

사이트 대 사이트 VPN 연결이 설정되면 로컬 게이트웨이의 뒤에 있는 호스트는 보안 VPN 터널을 통해 원격 게이트의 뒤에 있는 호스트와 연결할 수 있습니다. 연결은 두 게이트웨이의 IP 주소와 호스트 이름, 그 뒤에 있는 서브넷, 두 게이트웨이가 상호 인증에 사용하는 방법으로 구성됩니다.

IKE(Internet Key Exchange)

IKE(Internet Key Exchange)는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(Security Association, 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 정책은 두 피어가 상호 간의 KIE 협상을 보호하는 데 사용하는 알고리즘 집합입니다. IKE 협상에서는 두 피어가 먼저 공통(공유) IKE 정책을 합의합니다. 이 정책은 후속 IKE 협상을 보호하는 보안 파라미터를 제시합니다. IKEv1(IKE 버전 1)의 경우 IKE 정책에는 단일 알고리즘 집합과 모듈러스 그룹이 포함됩니다. IKEv1과 달리 IKEv2 정책에서는 피어가 1단계 협상 중에 선택할 수 있는 여러 알고리즘 및 모듈러스 그룹을 선택할 수 있습니다. 단일 IKE 정책을 생성할 수도 있지만, 여러 정책을 생성해 가장 적절한 옵션에 더 높은 우선 순위를 지정할 수도 있습니다. 사이트 대 사이트 VPN의 경우에는 단일 IKE 정책을 생성할 수 있습니다.

IKE 정책을 정의하려면 다음 사항을 지정합니다.

- 고유한 우선 순위(1~65,543, 1이 우선 순위가 가장 높음)
- 데이터 및 개인정보를 보호하기 위한 IKE 협상의 암호화 방법
- 보낸 사람의 ID를 확인하고 메시지가 전송 중에 수정되지 않았는지 확인할 HMAC(Hashed Message Authentication Codes, 해시 메시지 인증 코드) 방법(IKEv2에서는 무결성 알고리즘이라고 함)
- IKEv2의 경우 IKEv2 터널 암호화에 필요한 키 요소 및 해싱 작업을 파생시키기 위한 알고리즘으로 사용되는 별도의 PRF(Pseudo Random Function, 의사 난수 함수). 옵션은 해시 알고리즘에 사용되는 것과 동일합니다.
- encryption-key-determination 알고리즘의 수준을 결정하는 Diffie-Hellman 그룹. 디바이스는 이 알고리즘을 사용하여 암호화 및 해시 키를 파생합니다.
- 피어의 ID를 확인할 인증 방법
- 디바이스가 교체 전 암호화 키를 사용하는 시간제한

IKE 협상이 시작되면 협상을 시작한 피어가 활성화된 모든 정책을 원격 피어로 보내고 원격 피어는 우선 순위대로 자신의 정책과 일치하는 정책을 검색합니다. 암호화, 해시(IKEv2의 경우 무결성 및 PRF), 인증 및 Diffie-Hellman 값이 동일하고 SA 수명이 전송된 정책의 수명보다 작거나 같으면 IKE 정책은 서로 일치하는 것으로 간주됩니다. 수명이 동일하지 않은 경우에는 원격 피어에서 가져온 더 짧은 수명이 적용됩니다. 기본적으로는 DES를 사용하는 단순 IKE 정책만 활성화됩니다. 우선 순위가 더 높은 다른 IKE 정책을 활성화하여 더욱 강력한 암호화 표준을 협상할 수도 있지만, DES 정책으로도 협상은 정상적으로 진행됩니다.

VPN 연결의 보안 수준 결정

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.

참고 강력한 암호화에 적합한 경우 평가판 라이선스에서 스마트 라이선스로 업그레이드하기 전에 VPN 구성이 제대로 작동하도록 암호화 알고리즘을 확인하고 업데이트하십시오. AES 기반 알고리즘을 선택합니다. 강력한 암호화를 지원하는 계정을 사용하여 등록한 경우 DES는 지원되지 않습니다. 등록 후에는 모든 DES 사용을 제거할 때까지 변경 사항을 구축할 수 없습니다.

- 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 - 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.
- Null, ESP-Null-사용하지 않습니다. null 암호화 알고리즘은 암호화를 수행하지 않는 인증 기능을 제공합니다. 이는 대부분의 플랫폼에서 지원되지 않습니다.

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(SHA1)에서는 160비트 다이제스트를 생성합니다.

  IKEv2 컨피그레이션에는 다음과 같은 더욱 안전한 SHA-2 옵션을 사용할 수 있습니다. NSA Suite B 암호화 사양을 구현하려는 경우 이러한 옵션 중 하나를 선택합니다.

  - SHA256 - 256비트 다이제스트를 생성하는 Secure Hash Algorithm SHA 2를 지정합니다.
  - SHA384 - 384비트 다이제스트를 생성하는 Secure Hash Algorithm SHA 2를 지정합니다.
  - SHA512 - 512비트 다이제스트를 생성하는 Secure Hash Algorithm SHA 2를 지정합니다.

- null 또는 None(NULL, ESP-NONE) - (IPsec 제안에만 해당됨) null 해시 알고리즘으로, 대개 테스트용으로만 사용됩니다. 그러나 AES-GCM 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.

- 14 - Diffie-Hellman 그룹 14: 2048비트 MODP(모듈식 지수) 그룹. 192비트 키에 적합한 보호를 제공합니다.
- 15 - Diffie-Hellman 그룹 15: 3072비트 MODP 그룹
- 16 - Diffie-Hellman 그룹 16: 4096비트 MODP 그룹
- 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
- 31 - Diffie-Hellman 그룹 31: Curve25519 256비트 EC 그룹

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 Site-to-Site VPN 연결을 컨피그레이션해야 하는 경우, 사전 공유 키 방법 대신 인증서 방법을 사용하십시오.

인증서

디지털 인증서에서는 RSA 키 쌍을 사용하여 IKE 키 관리 메시지에 서명하고 이를 암호화합니다. Site-to-Site VPN 연결의 양쪽 엔드를 컨피그레이션하는 경우, 원격 피어에서 로컬 피어를 인증할 수 있도록 로컬 디바이스의 ID 인증서를 선택하십시오.

인증서 방법을 사용하려면 다음 작업을 수행해야 합니다.

1. CA(Certification Authority)로 로컬 피어를 등록하여 디바이스 ID 인증서를 가져옵니다. 이 인증서를 디바이스에 업로드합니다. 자세한 내용은 내부 및 내부 CA 인증서 업로드를 참고하십시오.

   원격 피어에 대한 책임도 있는 경우, 원격 피어도 등록하십시오. 피어에 대해 동일한 CA를 사용하는 것이 편리하지만 필수 요건은 아닙니다.

   SSC(자가서명 인증서)를 사용해 VPN 연결을 설정할 수는 없습니다. Certificate Authority로 디바이스를 등록해야 합니다.

   Windows CA(Certificate Authority)를 사용하여 Site-to-Site VPN 엔드포인트용 인증서를 생성하는 경우, 애플리케이션 정책 확장을 위해 IP 보안 엔드 시스템을 지정하는 인증서를 사용해야 합니다. Windows CA 서버의 Extensions(확장) 탭에 있는 인증서의 Properties(속성) 대화

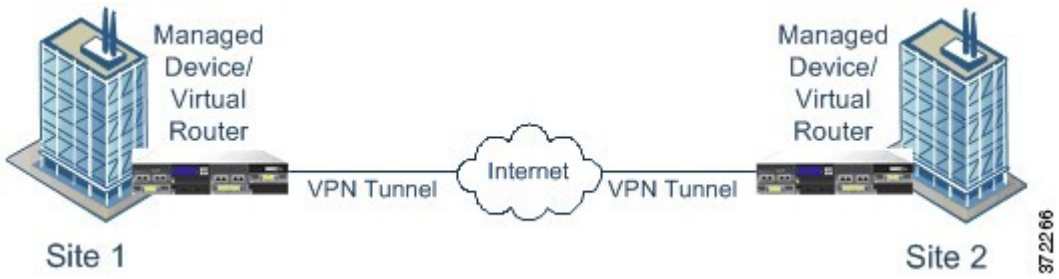
상자에서 이를 확인할 수 있습니다. 이 확장의 기본값은 device manager을 사용하여 구성된 Site-to-Site VPN에 대해 작동하지 않는 IP 보안 IKE 중개입니다.

2. 로컬 피어의 ID 인증서에 서명하는 데 사용된 신뢰할 수 있는 CA 인증서를 업로드합니다. 중간 CA를 사용한 경우, 루트 및 중간 인증서를 포함하여 전체 체인을 업로드합니다. 자세한 내용은 신뢰할 수 있는 CA 인증서 업로드를 참고하십시오.
3. 원격 피어가 다른 CA로 등록된 경우, 원격 피어의 ID 인증서 서명에 사용된 신뢰할 수 있는 CA 인증서도 업로드하십시오. 원격 피어를 제어하는 조직에서 인증서를 가져옵니다. 중간 CA를 사용한 경우, 루트 및 중간 인증서를 포함하여 전체 체인을 업로드합니다.
4. 사이트 대 사이트 VPN 연결을 컨피그레이션하는 경우, 인증서 방법을 선택한 후 로컬 피어의 ID 인증서를 선택합니다. 연결의 양쪽 엔드에서는 연결의 로컬 엔드에 대해 인증서를 지정합니다. 원격 피어에 대해서는 인증서를 지정하지 마십시오.

VPN 토폴로지

device manager를 통해서는 포인트 투 포인트 VPN 연결만 구성할 수 있습니다. 모든 연결은 포인트 투 포인트 방식이지만, 디바이스가 참여하는 각 터널을 정의하여 보다 규모가 큰 허브 앤 스포크(hub and spoke) 또는 메시 VPN에 연결할 수 있습니다.

다음 다이어그램은 일반적인 포인트 투 포인트 VPN 토폴로지를 보여줍니다. 포인트 투 포인트 VPN 토폴로지에서는 2개의 엔드포인트가 서로 직접 통신합니다. 두 엔드포인트를 피어 디바이스로 구성하며, 두 디바이스 중 하나가 보안 연결을 시작할 수 있습니다.



동적 주소 지정 피어로 Site-to-Site VPN 연결 설정

피어의 IP 주소를 알지 못하는 경우에도 피어에 사이트 대 사이트 VPN 연결을 생성할 수 있습니다. 이러한 기능은 다음 상황에서 유용할 수 있습니다.

- 피어에서 DHCP를 사용하여 해당 주소를 가져오는 경우, 특정 정적 IP 주소가 있는 원격 엔드포인트에는 의존할 수 없습니다.
- hub-and-spoke 토폴로지에 허브 역할을 하는 디바이스와 연결을 설정하기 위해 확정되지 않은 수의 원격 피어를 허용하려는 경우

동적 주소 지정 피어 B에 보안 연결을 설정해야 하는 경우, 연결의 엔드인 A에 정적 IP 주소가 있는지 확인해야 합니다. 그런 다음, A에 연결을 생성할 때 피어의 주소가 동적 상태가 되도록 지정합니다.

그러나 피어 B에 연결을 컨피그레이션하는 경우, 반드시 A에 대한 IP 주소를 원격 피어 주소로 입력해야 합니다.

시스템에서 사이트 대 사이트 VPN 연결을 설정하는 경우, 피어에 동적 주소가 있는 모든 연결은 응답 전용입니다. 즉 원격 피어는 연결을 시작하는 것이어야 합니다. 원격 피어에서 연결 설정을 시도하면 장치에서는 사전 공유 키든 인증서든 연결에 정의한 방법을 사용하여 연결을 확인합니다.

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.

Virtual Tunnel Interface 및 경로 기반 VPN

기존에는 VPN 터널을 통해 암호화할 특정 로컬 및 원격 네트워크를 정의하여 사이트 대 사이트 VPN 연결을 구성했습니다. 이는 VPN 연결 프로파일의 일부인 암호화 맵에서 정의됩니다. 이러한 유형의 사이트 대 사이트 VPN을 정책 기반이라고 합니다.

또는 경로 기반의 사이트 대 사이트 VPN을 구성할 수 있습니다. 이 경우 특정 물리적 인터페이스(일반적으로 외부 인터페이스)와 연결된 가상 인터페이스인 VTI(Virtual Tunnel Interface)를 생성합니다. 그 다음 정적 및 동적 경로와 함께 라우팅 테이블을 사용하여 원하는 트래픽을 VTI로 보냅니다. VTI(이그레스(egressing))를 통해 라우팅되는 모든 트래픽은 VTI에 대해 구성한 VPN 터널을 통해 암호화됩니다.

따라서 경로 기반 사이트 대 사이트 VPN을 통해 VPN 연결 프로파일을 전혀 변경하지 않고 간단히 라우팅 테이블을 변경하여 지정된 VPN 연결에서 보호된 네트워크를 관리할 수 있습니다. 이 변경 사항을 고려하여 원격 네트워크를 추적하고 VPN 연결 프로파일을 업데이트할 필요가 없습니다. 이는 클라우드 서비스 제공자 및 대기업에 대한 VPN 관리를 간소화합니다.

또한 터널에서 허용되는 트래픽 유형을 세부적으로 조정하기 위해 VTI에 대한 액세스 제어 규칙을 생성할 수 있습니다. 예를 들어 침입 검사, URL 및 애플리케이션 필터링을 적용할 수 있습니다.

경로 기반 VPN 구성을 위한 개요 프로세스

일반적으로 경로 기반 사이트 대 사이트 VPN을 설정하는 프로세스에는 다음 단계가 포함됩니다.

프로시저

단계 **1** 로컬 엔드포인트에 대한 IKEv1/2 정책 및 IPsec 제안을 생성합니다.

단계 **2** 원격 피어를 향하는 물리적 인터페이스와 연결된 VTI(Virtual Tunnel Interface)를 생성합니다.

단계 **3** VTI, IKE 정책 및 IPsec 제안을 사용하는 사이트 대 사이트 VPN 연결 프로파일을 생성합니다.

단계 **4** 원격 피어, 원격 VTI, 원격 피어 관점에서 이 로컬 VTI를 원격 엔드포인트로 지정하는 사이트 대 사이트 VPN 연결 프로파일에 동일한 IKE 및 IPsec 제안을 생성합니다.

단계 **5** 터널을 통해 적절한 트래픽을 전송하기 위해 두 피어에서 경로 및 액세스 제어 규칙을 생성합니다.

트래픽이 양방향으로 흐를 수 있도록 각 엔드포인트의 경로와 액세스 제어가 서로 미러링되는지 확인합니다.

정적 경로의 일반적인 특성은 다음과 같습니다.

- **Interface(**인터페이스**)** — VTI(Virtual Tunnel Interface) 이름입니다.
- **Networks(**네트워크**)** — 원격 엔드포인트로 보호되는 원격 네트워크를 정의하는 네트워크 개체입니다.
- **Gateway(**게이트웨이**)** — VPN 터널 원격 엔드포인트의 IP 주소를 정의하는 네트워크 개체입니다.

Virtual Tunnel Interface 및 경로 기반 VPN을 위한 지침

IPv6 지침

Virtual tunnel interface는 IPv4 주소만 지원합니다. VTI에서는 IPv6 주소를 구성할 수 없습니다.

추가 지침

- 최대 1,024개의 VTI를 생성할 수 있습니다.
- VTI 경로 기반 VPN에서는 정적이든 동적이든 RRI(reverse route injection) 설정을 구성할 수 없습니다. (threat defense API만 사용하여 RRI(reverse route injection) 설정을 구성할 수 있습니다.)
- VTI를 로컬 인터페이스로 선택할 경우 동적 피어 주소를 구성할 수 없습니다.
- VTI를 로컬 인터페이스로 선택할 경우 원격 백업 피어를 구성할 수 없습니다.
- 맞춤형 가상 라우터에 할당된 소스 인터페이스에는 VTI를 생성할 수 없습니다. 가상 라우터를 사용할 때 전역 가상 라우터의 인터페이스에서만 VTI를 설정할 수 있습니다.
- IKE 및 IPsec 보안 연계는 터널에서 데이터 트래픽에 관계없이 지속적으로 다시 입력됩니다. 이렇게 하면 VTI 터널은 항상 작동합니다.
- IKEv1 및 IKEv2는 모두 경로 기반 연결 프로파일에서 구성할 수 없습니다. 하나의 IKE 버전만 구성해야 합니다.
- VTI에 대한 암호화 맵 및 터널 대상에서 구성된 피어 주소가 서로 다르다면 동일한 물리적 스페이스에서 서로 다른 VTI 및 정책 기반(암호화 맵) 컨피그레이션을 구성할 수 있습니다.
- BTI 라우팅 프로토콜만 VTI를 통해 지원됩니다.
- 시스템에서 IOS IKEv2 VTI 클라이언트를 종료하는 경우 시스템이 IOS VTI 클라이언트에서 시작한 세션의 mode-CFG 특성을 검색할 수 없으므로 IOS에서 config-exchange 요청을 비활성화합니다.
- 경로 기반의 사이트 대 사이트 VPN은 양방향으로 구성됩니다. 즉, VPN 터널의 엔드포인트가 연결을 시작할 수 있습니다. 연결 프로파일을 생성한 후 이 엔드포인트를 유일한 이니시에이터(INITIATE_ONLY) 또는 전적으로 응답자(RESPOND_ONLY)로 변경할 수 있습니다. 보완 연결 유형을 사용하도록 원격 엔드포인트를 수정해야 합니다. 이 변경을 수행하려면 API Explorer로 이동하여 GET / devices/default/s2sconnectionprofiles를 사용하여 연결 프로파일을 찾아야 합니다.

그 다음 본문 콘텐츠를 PUT / devices/default/s2sconnectionprofiles/{objId} 메서드에 복사/붙여 넣기하고 **connectionType**을 업데이트하여 원하는 유형을 지정하고 메서드를 실행할 수 있습니다.

IPsec 플로우 오프로드

IPsec 플로우 오프로드를 사용하도록 지원 디바이스 모델을 구성할 수 있습니다. IPsec 사이트 간 VPN 또는 원격 액세스 VPN 보안 연계(SA)의 초기 설정 후 IPsec 연결은 디바이스의 FTPA(field-programmable gate Array)로 오프로드되므로 디바이스 성능이 향상됩니다.

오프로드된 작업은 특히 인그레스의 사전 암호 해독 및 암호 해독 처리 및 이그레스의 사전 암호화 및 암호화 처리와 관련이 있습니다. 시스템 소프트웨어는 보안 정책을 적용하기 위해 내부 플로우를 처리합니다.

IPsec 플로우 오프로드는 기본적으로 활성화되어 있으며 다음 디바이스 유형에 적용됩니다.

- Secure Firewall 3100

IPsec 플로우 오프로드에 대한 제한 사항

다음 IPsec 흐름은 오프로드되지 않습니다.

- IKEv1 터널. IKEv2 터널만 오프로드됩니다. IKEv2는 더 강력한 암호를 지원합니다.
- 볼륨 기반 키 재설정이 구성된 플로우.
- 압축이 구성된 플로우.
- 전송 모드 플로우. 터널 모드 플로우만 오프로드됩니다.
- AH 형식. ESP/NAT-T 형식만 지원됩니다.
- 사후 조각화가 구성된 플로우.
- 64비트 이외의 재생 방지 창 크기가 있는 플로우 및 재생 방지는 비활성화되지 않습니다.
- 방화벽 필터가 활성화된 플로우.

IPsec 플로우 오프로드 구성

IPsec 플로우 오프로드는 해당 기능을 지원하는 하드웨어 플랫폼에서 기본으로 활성화됩니다. 구성을 변경하려면 FlexConfig를 사용하여 **flow-offload-ipsec** 명령을 구현합니다. 명령에 대한 자세한 내용은 ASA 명령 참조를 확인하십시오.

사이트 대 사이트 VPN 관리

VPN(Virtual Private Network)은 인터넷과 같은 공개 소스나 기타 네트워크를 통해 원격 피어 간에 보안 터널을 설정하는 네트워크 연결입니다. VPN은 터널을 사용하여 IP 기반 네트워크를 통해 전달할 수 있도록 일반 IP 패킷 내의 데이터 패킷을 캡슐화합니다. VPN은 암호화를 사용해 개인 정보와 인증을 확인함으로써 데이터의 무결성을 보장합니다.

피어 디바이스에 대한 VPN 연결을 생성할 수 있습니다. 모든 연결은 포인트 투 포인트 방식이지만, 모든 관련 연결을 구성하여 규모가 더 큰 허브 앤 스포크(hub and spoke) 또는 메시 VPN에 디바이스를 연결할 수 있습니다.

시작하기 전에

다음 사실은 다시 생성할 수 있는 사이트 대 사이트 VPN 연결의 유형과 수를 제어합니다.

- VPN 연결은 암호화를 사용하여 네트워크 개인 정보를 보호합니다. 사용할 수 있는 암호화 알고리즘은 기본 라이선스가 강력한 암호화를 허용하는지에 따라 달라집니다. 강력한 암호화 허용 여부는 Cisco Smart License Manager에 등록할 때 디바이스에서 내보내기 제어 기능을 허용하는 옵션을 선택했는지에 따라 제어됩니다. 평가 라이선스를 사용 중이거나 내보내기 제어 기능을 활성화하지 않은 경우에는 강력한 암호화를 사용할 수 없습니다.
- 최대 20개의 고유한 IPsec 프로파일을 생성할 수 있습니다. 고유성은 IKEv1/v2 제안 및 인증서, 연결 유형, DH 그룹 및 SA 수명의 조합에 따라 결정됩니다. 기존 프로파일을 재사용할 수 있습니다. 따라서 모든 사이트 대 사이트 VPN 연결에 동일한 설정을 사용하는 경우 하나의 고유한 IPsec 프로파일을 갖습니다. 20개의 고유한 IPsec 프로파일 제한에 도달하면 기존 연결 프로파일에 사용한 것과 동일한 특성 조합을 사용하지 않는 한 새 사이트 대 사이트 VPN 연결을 생성할 수 없습니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, 사이트 대 사이트 VPN 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

그러면 구성한 모든 연결이 나열되는 사이트 대 사이트 VPN 페이지가 열립니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 사이트 대 사이트 VPN 연결을 생성하려면 + 버튼을 클릭합니다. 사이트 대 사이트 VPN 연결 구성, 11 페이지의 내용을 참조하십시오.

  아직 연결이 없는 경우에는 **Create Site-to-Site Connection(**사이트 대 사이트 연결 생성**)** 버튼을 클릭할 수도 있습니다.

- 기존 연결을 수정하려면 해당 연결의 수정 아이콘( )을 클릭합니다. 사이트 대 사이트 VPN 연결 구성, 11 페이지의 내용을 참조하십시오.

- 연결 컨피그레이션 요약을 클립보드에 복사하려면 해당 연결의 복사 아이콘( )을 클릭합니다. 이 정보를 문서에 붙여넣은 다음 원격 디바이스 관리자에게 보내면 관리자가 해당 연결 쪽을 쉽게 구성할 수 있습니다.

- 더 이상 필요하지 않은 연결을 삭제하려면 해당 연결의 삭제 아이콘( )을 클릭합니다.

사이트 대 사이트 VPN 연결 구성

원격 디바이스 소유자가 협조하며 권한을 제공한다고 가정할 때 디바이스를 서로 연결하기 위한 포인트 투 포인트 VPN 연결을 생성할 수 있습니다. 모든 연결은 포인트 투 포인트 방식이지만, 디바이스가 참여하는 각 터널을 정의하여 보다 규모가 큰 허브 앤 스포크(hub and spoke) 또는 메시 VPN에 연결할 수 있습니다.

시작하기 전에

로컬 네트워크/원격 네트워크 조합별로 단일 VPN 연결을 생성할 수 있습니다. 그러나 각 연결 프로파일에서 원격 네트워크가 고유한 경우에는 로컬 네트워크에 대해 여러 연결을 생성할 수 있습니다.

원격 네트워크가 중복되는 경우, 더욱 제한적인 연결 프로파일을 먼저 생성해야 합니다. 시스템에서는 표시되는 순서(단순히 영문자 순)가 아니라 연결 프로파일을 생성하는 순서대로 터널을 생성합니다.

예를 들어 192.16.0.0/16에서 10.91.0.0/16까지의 하나의 터널을 원격 엔드포인트 A로 이동하면서 터널 192.16.0.0/24를 원격 엔드포인트 B를 통해 나머지 10.0.0.0/8로 이동하게 하려면 B용 연결 프로파일을 생성하기 전에 A용 연결 프로파일을 생성해야 합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, 사이트 대 사이트 VPN 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 사이트 대 사이트 VPN 연결을 생성하려면 + 버튼을 클릭합니다.

  아직 연결이 없는 경우에는 **Create Site-to-Site Connection(**사이트 대 사이트 연결 생성**)** 버튼을 클릭할 수도 있습니다.

- 기존 연결을 수정하려면 해당 연결의 수정 아이콘( )을 클릭합니다.

더 이상 필요하지 않은 연결을 삭제하려면 해당 연결의 삭제 아이콘( )을 클릭합니다.

단계 **3** 포인트 투 포인트 VPN 연결의 엔드포인트를 정의합니다.

- **Connection Profile Name(**연결 프로파일 이름**)** - 이 연결의 이름을 공백 없이 64자까지 입력합니다. 예를 들면 MainOffice를 입력합니다. IP 주소는 이름으로 사용할 수 없습니다.
- 유형 — VPN 터널을 통해 어떤 트래픽을 전송해야 하는지 식별하는 방법입니다. 다음 중 하나를 선택합니다.
  - **Route Based (VTI)(**경로 기반**(VTI))** — 라우팅 테이블(주로 정적 경로)을 사용하여 터널에 참여해야 하는 로컬 및 원격 네트워크를 정의합니다. 이 옵션을 선택하는 경우 VTI(Virtual Tunnel Interface)를 로컬 VPN 액세스 인터페이스로 선택해야 합니다. 또한 터널의 원격 엔드에 대해 정적 IP 주소를 사용해야 합니다. VPN 연결 프로파일을 생성한 후 VTI에 대한 적절한 정적 경로 및 액세스 제어 규칙을 구성해야 합니다.

- **Policy Based(**정책 기반**)** — 사이트 대 사이트 VPN 연결 프로파일에서 로컬 및 원격 네트워크를 직접 지정합니다. 이는 VPN 터널로 보호해야 하는 트래픽을 정의하는 기존의 접근 방식입니다.

- 로컬 사이트 - 이러한 옵션은 로컬 엔드포인트를 정의합니다.
  - 로컬 **VPN** 액세스 인터페이스 - 원격 피어가 연결할 수 있는 인터페이스를 선택합니다. 이 인터페이스는 대개 외부 인터페이스이며, 브리지 그룹의 멤버일 수는 없습니다. 정책 기반 연결을 위해 백업 피어를 구성하는 경우, 피어가 연결할 수 있는 모든 인터페이스를 선택해야 합니다. 경로 기반 연결의 경우 하나의 인터페이스만 선택할 수 있습니다.
  - **Local Network(**로컬 네트워크**)** — (정책-기반 전용) **+**를 클릭하고 VPN 연결에 참여해야 하는 로컬 네트워크를 식별하는 네트워크 개체를 선택합니다. 이러한 네트워크의 사용자는 해당 연결을 통해 원격 네트워크에 접속할 수 있습니다.

    참고 이러한 네트워크에는 IPv4 또는 IPv6 주소를 사용할 수 있지만, 연결 양쪽의 주소 유형이 일치해야 합니다. 예를 들어 로컬 IPv4 네트워크에 대한 VPN 연결에는 원격 IPv4 네트워크가 하나 이상 있어야 합니다. 단일 연결의 양쪽에서 IPv4 및 IPv6를 함께 사용할 수 있습니다. 엔드포인트에 대한 보호된 네트워크는 겹칠 수 없습니다.

- 원격 사이트 - 이러한 옵션은 원격 엔드포인트를 정의합니다.
  - **Static(**정적**)**/**Dynamic(**동적**)** - 원격 피어의 IP 주소가 정적으로 정의되는지, 아니면 동적으로 정의되는지 여부(예: DHCP를 통한 정의). **Static(**정적**)**을 선택하는 경우, 원격 피어의 IP 주소도 입력합니다. **Dynamic(**동적**)**을 선택하는 경우, 원격 피어에서만 이 VPN 연결을 시작할 수 있습니다.

    경로-기반 VPN의 경우 **Static(**정적**)**만 선택할 수 있습니다.
  - **Remote IP Address(**원격 **IP** 주소**)**(정적 주소 지정에만 해당) - VPN 연결을 호스팅할 원격 VPN 피어 인터페이스의 IP 주소를 입력합니다.
  - **Remote Backup Peers(**원격 백업 피어**)** - (선택 사항, 정책 기반 연결에만 해당.) 원격 피어의 백업을 추가하려면 **Add Peer(**피어 추가**)**를 클릭합니다. 기본 엔드포인트를 사용할 수 없는 경우 시스템은 백업 피어 중 하나를 사용하여 VPN 연결 재설정을 시도합니다. 여러 백업을 추가할 수 있습니다.

    각 백업 피어를 구성할 때 해당 피어와 함께 사용할 사전 공유 키 및 인증서를 구성할 수 있습니다. 기본 원격 피어에 대해 구성한 것과 동일한 기술을 사용합니다. 연결 프로파일에 대해 설정된 동일한 값을 사용하려면 이 설정을 비워둡니다.

    첫 번째 백업 피어를 구성한 후에는 **Add Another Peer(**다른 피어 추가**)**를 클릭하여 피어를 추가 또는 삭제하거나 **Edit(**편집**)**를 클릭하여 피어의 설정을 변경할 수 있습니다.

    기본 피어가 아닌 다른 인터페이스를 통해 백업 피어에 연결할 수 있는 경우 **Local VPN Access Interface(**로컬 **VPN** 액세스 인터페이스**)**에서 필요한 인터페이스를 선택해야 합니다.
  - **Remote Network(**원격 네트워크**)** — (정책 기반 전용) **+**를 클릭하고 VPN 연결에 참여해야 하는 원격 네트워크를 식별하는 네트워크 개체를 선택합니다. 이러한 네트워크의 사용자는 해당 연결을 통해 로컬 네트워크에 접속할 수 있습니다.

단계 **4** **Next(**다음**)**를 클릭합니다.

단계 **5** VPN에 대한 프라이버시 컨피그레이션을 정의합니다.

참고 라이선스에 따라 선택 가능한 암호화 프로토콜이 결정됩니다. 가장 기본적인 옵션 외의 옵션을 선택하려면 강력한 암호화를 사용할 수 있어야 합니다(내보내기 제어를 충족해야 함).

- **IKE** 버전 **2**, **IKE** 버전 **1** - IKE(Internet Key Exchange) 협상 중에 사용할 IKE 버전을 선택합니다. 정책 기반 연결의 경우 둘 중 하나 또는 두 개 모두를 선택할 수 있습니다. 경로 기반의 경우 하나만 선택할 수 있습니다. 디바이스는 다른 피어와의 연결 협상을 시도할 때 사용자가 허용하며 다른 피어가 수락하는 버전을 사용합니다. 두 버전을 모두 허용하는 경우 디바이스는 처음 선택한 버전을 통한 협상이 실패하면 다른 버전으로 자동 대체합니다. IKEv2가 구성되어 있으면 IKEv2 사용을 항상 먼저 시도합니다. IKEv2를 협상에서 사용하려면 두 피어가 모두 IKEv2를 지원해야 합니다.
- **IKE** 정책 - 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. IKE는 글로벌 정책이므로 활성화하는 개체가 모든 VPN에 적용됩니다. **Edit(**수정**)**을 클릭하여 IKE 버전별로 현재 전체적으로 활성화된 정책을 점검하고 새 정책을 활성화 및 생성합니다. 자세한 내용은 글로벌 IKE 정책 구성, 16 페이지의 내용을 참고하십시오.
- **IPsec** 제안 - IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다. **Edit(**수정**)**을 클릭하고 각 IKE 버전에 대한 제안을 선택합니다. 허용하려는 모든 제안을 선택합니다. 시스템 기본값만 선택하려면 **Set Default(**기본값 설정**)**를 클릭합니다. 이러한 기본값은 내보내기 컴플라이언스에 따라 다릅니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 제안에서 가장 취약한 제안 순서대로 피어와 협상을 합니다. 자세한 내용은 IPsec 제안 구성, 21 페이지의 내용을 참고하십시오.
- 인증 유형 - VPN 연결에서 피어를 인증하고 싶은 방법으로 사전 공유 수동 키 또는 인증서를 선택합니다. 선택에 따라 다음 필드도 입력해야 합니다. IKEv1의 경우, 선택한 방법은 연결에 대해 컨피그레이션된 IKEv1 정책 개체에서 선택한 인증 방법과 일치해야 합니다. 이 옵션에 대한 세부 정보는 사용할 인증 방법 결정, 5 페이지의 내용을 참조하십시오.
  - (IKEv2) 로컬 사전 공유 키, 원격 피어 사전 공유 키 - VPN 연결을 위한 원격 디바이스와 이 디바이스에 정의된 키입니다. IKEv2에서는 이러한 키가 다를 수 있습니다. 키는 영숫자 1~127자가 될 수 있습니다.
  - (IKEv1) 사전 공유 키 - 로컬 디바이스와 원격 디바이스에 모두 정의된 키입니다. 키는 영숫자 1~127자가 될 수 있습니다.
  - 인증서 - 로컬 피어에 대한 디바이스 ID 인증서입니다. 이 인증서는 CA(Certification Authority)에서 가져온 것이어야 하며 SSC(자가서명 인증서)는 사용할 수 없습니다. 인증서를 업로드하지 않은 경우, **Create New Object(**새 개체 생성**)** 링크를 클릭합니다. ID 인증서 서명에 사용되는 신뢰할 수 있는 루트 및 중간 CA 인증서를 업로드해야 합니다. **IPsec** 클라이언트를 포함하도록 업로드된 인증서의 검증 사용을 설정해야 합니다. 인증서를 아직 업로드하지 않은 경우, 이 마법사를 완료한 후 업로드하면 됩니다.

- **IPsec Settings(IPsec** 설정**)** - 보안 연결의 수명입니다. 수명에 도달하면 시스템은 보안 연결을 다시 협상합니다. 시스템이 피어로부터 협상 요청을 받을 때, 피어에서 제안한 수명 값과 새 보안 연결의 수명으로 로컬에 설정된 수명 값 중 더 작은 값을 사용합니다. 수명에는 "timed" 수명과 "traffic-volume" 수명의 2가지가 있습니다. 이 수명 중 더 짧은 것에 도달하면 보안 연결이 만료됩니다.
  - **Lifetime Duration(**수명 기간**)** - 보안 연결이 만료되기 전에 유지할 수 있는 시간(초)입니다. 범위는 120~214,783,647초입니다. 전역 기본값은 28,800초(8시간)입니다.
  - **Lifetime Size(**수명 크기**)** - 보안 연결이 만료되기 전에 지정된 보안 연결을 사용하여 피어 간에 전달할 수 있는 트래픽 볼륨(KB)입니다. 범위는 10~2,147,483,647킬로바이트 또는 공백입니다. 전역 기본값은 4,608,000킬로바이트입니다. 크기 기반 제한을 제거하고 기간을 유일한 제한으로 사용하려면 필드를 비워 두십시오.
- **NAT Exempt(NAT** 제외**)** — (정책 기반 전용) 로컬 VPN 액세스 인터페이스의 NAT 정책에서 VPN 트래픽을 제외할지 여부를 선택합니다. 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 사이트 대 사이트 VPN 트래픽 제외, 27 페이지를 참조하십시오.
- **PFS(Perfect Forward Secrecy)**에 대한 **Diffie-Helman** 그룹 - PFS(Perfect Forward Secrecy)를 사용하여 암호화된 각 교환에 대해 고유 세션 키를 생성하고 사용할지 여부를 선택합니다. 고유 세션 키는 전체 교환이 기록되었으며 공격자가 엔드포인트 디바이스에서 사용하는 사전 공유 키 또는 개인 키를 확보했더라도 후속 암호 해독에서 교환을 보호합니다. PFS(Perfect Forward Secrecy)를 활성화하려면 모듈러스 그룹 목록에서 PFS 세션 키를 생성할 때 사용할 Diffie-Hellman 키 파생 알고리즘을 선택합니다. IKEv1 및 IKEv2를 모두 활성화하면 IKEv1에서 지원하는 옵션만 선택할 수 있습니다. 옵션에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정, 4 페이지를 참조하십시오.

단계 **6** **Next(**다음**)**를 클릭합니다.

단계 **7** 요약을 검토하고 **Finish(**종료**)**를 클릭합니다.

요약 정보가 클립보드에 복사됩니다. 해당 정보를 문서에 붙여넣은 다음 원격 피어를 구성하는 데 사용하거나 피어 구성 담당자에게 보낼 수 있습니다.

사이트 대 사이트 VPN을 통한 트래픽 허용, 16 페이지의 설명대로 추가 단계를 수행하여 VPN 터널 내의 트래픽을 허용해야 합니다.

컨피그레이션을 구축한 후 디바이스 CLI에 로그인하고 **show ipsec sa** 명령을 사용하여 엔드포인트에서 보안 연결을 설정하는지 확인합니다. 사이트 대 사이트 VPN 연결 확인, 23 페이지의 내용을 참조하십시오.

Virtual Tunnel Interface 구성

경로 기반 사이트 대 사이트 VPN 연결 프로파일에서만 VTI(Virtual Tunnel Interface)를 사용할 수 있습니다. VTI는 물리적 인터페이스와 연결되며 이를 통해 원격 피어에 VPN 연결이 설정됩니다. 가상 인터페이스를 사용하면 연결 프로파일에서 VPN에 대한 로컬 및 원격 네트워크를 지정하는 대신 정적 및 동적 경로를 사용하여 사이트 대 사이트 VPN 연결을 간소화하고 트래픽을 제어할 수 있습니다.

프로시저

단계 **1** 디바이스를 클릭하고 인터페이스 요약의 링크를 클릭한 다음, **Virtual Tunnel Interfaces(Virtual Tunnel Interface)**를 클릭합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **+** 또는 **Create Virtual Tunnel Interface(Virtual Tunnel Interface** 생성**)**를 클릭하여 새 인터페이스를 생성합니다.
- 기존 인터페이스에 대해 수정 아이콘( )을 클릭합니다.

인터페이스가 더 이상 필요하지 않은 경우 해당 인터페이스에 대해 삭제 아이콘( )을 클릭합니다. 먼저 인터페이스를 사용하는사이트 대 사이트 연결 프로파일을 삭제해야 이를 삭제할 수 있습니다.

단계 **3** 다음 옵션을 구성합니다.

- **Name(**이름**)** - 인터페이스의 이름(최대 48자)입니다. 기존 인터페이스의 이름을 변경하면 해당 인터페이스가 포함된 모든 정책 및 개체에서 자동으로 변경됩니다. 이름에 대문자를 사용할 수 없습니다.
- **Status(**상태**)** — Enabled(활성화됨) 위치로 슬라이더를 클릭합니다( ).
- **Description(**설명**)** — (선택 사항). 설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.
- **Tunnel ID(**터널 **ID)** — 0~10413 사이의 숫자. 이 번호는 Tunnel이라는 단어에 추가되어 인터페이스의 하드웨어 이름을 구성합니다. 다른 VTI에는 아직 사용하지 않은 번호를 선택해야 합니다. 예를 들어, 인터페이스 Tunnel1을 생성하려면 1을 입력합니다.
- **Tunnel Source(**터널 소스**)** — 이 VTI와 연결된 인터페이스를 선택합니다. 터널 소스는 가상 터널 인터페이스에 정의된 사이트 대 사이트 VPN이 원격 엔드포인트에 연결하는 데 사용하는 인터페이스입니다. 외부 인터페이스와 같이 원격 엔드포인트에 연결할 수 있는 인터페이스를 선택합니다. 소스 인터페이스는 물리적 인터페이스, 하위 인터페이스 또는 Etherchannel일 수 있으며, 이름이 있어야 합니다. BVI(Bridge Virtual Interface)의 멤버일 수는 없습니다.
- **IP Address and Subnet Mask(IP** 주소 및 서브넷 마스크**)** — IPv4 주소 및 관련 서브넷 마스크입니다. 예를 들어 192.168.1.1/24 또는 /255.255.255.0입니다. 이 주소는 터널 소스 인터페이스의 주소와 동일한 서브넷에 있을 필요는 없습니다. 하지만 소스 인터페이스에서 RA(원격 액세스) VPN을 설정하는 경우 VTI IP 주소는 RA VPN에 대해 설정된 주소 풀 내에 있을 수 없습니다.

단계 4 **OK(**확인**)**를 클릭합니다.

사이트 대 사이트 VPN을 통한 트래픽 허용

다음 기법 중 하나를 사용해 Site-to-Site VPN 터널의 트래픽 흐름을 활성화할 수 있습니다.

- **sysopt connection permit-vpn** 명령을 컨피그레이션합니다. 이 명령에서는 VPN 연결과 일치하는 트래픽을 액세스 제어 정책에서 제외합니다. 이 명령의 기본값은 **no sysopt connection permit-vpn** 입니다. 이는 액세스 제어 정책에서도 VPN 트래픽을 허용해야 한다는 의미입니다.

  이 방법은 외부 사용자가 보호되는 원격 네트워크에서 IP 주소를 스푸핑할 수 없기 때문에 VPN에서 트래픽을 더 안전하게 허용할 수 있습니다. 하지만 VPN 트래픽이 검사되지 않는다는 단점이 있습니다. 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.

  이 명령을 컨피그레이션하는 더 나은 방법은 원격 액세스 VPN 연결 프로파일을 만들어 여기에서 **Bypass Access Control policy for decrypted traffic(**암호 해독된 트래픽에 대해 액세스 제어 정책 우회**)** 옵션을 선택하는 것입니다. RA VPN을 컨피그레이션하고 싶지 않거나 RA VPN을 컨피그레이션할 수 없는 경우, FlexConfig를 사용해 명령을 컨피그레이션할 수 있습니다.

참고 이 방법은 VTI(Virtual Tunnel Interface)에 구성된 경로 기반 VPN 연결에는 적용되지 않습니다. 항상 경로 기반 VPN에 대한 액세스 제어 규칙을 구성해야 합니다.

- 원격 네트워크에서 연결을 허용하는 액세스 제어 규칙을 생성합니다. 이 방법을 사용하는 경우 VPN 트래픽이 검사되며, 연결에 고급 서비스를 적용할 수 있습니다. 하지만 외부 사용자가 IP 주소를 스푸핑하여 내부 네트워크에 액세스할 가능성이 있다는 단점이 있습니다.

글로벌 IKE 정책 구성

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 높

습니다. 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.

참고 최대 20개의 IKE 정책을 활성화할 수 있습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **IKE Policies(IKE** 정책**)**를 차례로 선택합니다.

IKEv1과 IKEv2에 대한 정책이 개별 목록에 표시됩니다.

단계 **2** 각 IKE 버전에 대해 허용할 IKE 정책을 활성화합니다.

a) 개체 테이블 위의 **IKEv1** 또는 **IKEv2**를 선택하여 해당 버전의 정책을 표시합니다.

b) **State(**상태**)** 토글을 클릭하여 적절한 개체를 활성화하고 요건을 충족하지 않는 개체를 비활성화합니다.

보안 요건 중 일부가 기존 개체에 반영되어 있지 않은 경우에는 새 개체를 정의하여 요건을 구현합니다. 자세한 내용은 다음 항목을 참조하십시오.

• IKEv1 정책 구성, 17 페이지
• IKEv2 정책 구성, 19 페이지

c) 상대 우선 순위가 요건과 일치하는지 확인합니다.

정책 우선 순위를 변경해야 하는 경우 정책을 수정합니다. 사전 정의된 시스템 정책의 경우에는 정책의 고유 버전을 생성하여 우선 순위를 변경해야 합니다.

우선 순위는 절대값이 아닌 상대값입니다. 예를 들어 우선 순위 80이 160보다 높습니다. 최고 우선 순위 개체로 80을 활성화하면 해당 정책이 첫 번째로 선택됩니다. 그런 후에 우선 순위가 25인 정책을 활성화하면 해당 정책이 최우선으로 선택됩니다.

d) 두 IKE 버전을 모두 사용하는 경우에는 다른 버전에 대해 프로세스를 반복합니다.

IKEv1 정책 구성

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 VPN 연결에서 IKEv1 설정을 수정하면서 IKEv1 정책 개체를 생성할 수도 있습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **IKE Policies(IKE** 정책**)**를 차례로 선택합니다.

단계 **2** 개체 테이블 위의 **IKEv1**을 선택하여 IKEv1 정책을 표시합니다.

단계 **3** 요구사항에 맞는 시스템 정의 정책이 있으면 **State(**상태**)** 토글을 클릭하여 활성화합니다.

원치 않는 정책을 비활성화할 때도 **State(**상태**)** 토글을 사용합니다. 상대 우선 순위에 따라 이러한 정책 중 먼저 사용을 시도할 정책이 결정되며, 숫자가 작을수록 우선 순위가 높습니다.

단계 **4** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **5** 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.
- **Name(**이름**)** - 개체의 이름(최대 128자)입니다.
- **State(**상태**)** - IKE 정책이 활성화되어 있는지 여부입니다. 토글을 클릭하여 상태를 변경합니다. IKE 협상 중에는 활성화된 정책만 사용됩니다.
- **Authentication(**인증**)** - 두 피어 간에 사용할 인증 방법입니다. 자세한 내용은 사용할 인증 방법 결정, 5 페이지의 내용을 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. 피어

는 동일한 또는 다른 CA에 등록할 수 있습니다. 어느 피어든 간에 SSC(자가서명 인증서)를 사용할 수 없습니다.

- **Encryption(암호화)** - 2단계 협상 보호를 위한 1단계 SA(보안 연계)를 설정하는 데 사용되는 암호화 알고리즘입니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정, 3 페이지를 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 결정, 4 페이지를 참조하십시오.
- **Hash(해시)** - 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하기 위한 해시 알고리즘입니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정, 4 페이지를 참조하십시오.
- **Lifetime(수명 주기)** - 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 **6** **OK(확인)**를 클릭하여 변경 사항을 저장합니다.

IKEv2 정책 구성

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 IKE Policy(새 IKE 정책 생성)** 링크를 클릭하여 VPN 연결에서 IKEv2 설정을 수정하면서 IKEv2 정책 개체를 생성할 수도 있습니다.

프로시저

단계 **1** 목차에서 **Objects(개체)**와 **IKE Policies(IKE 정책)**를 차례로 선택합니다.

단계 **2** 개체 테이블 위의 **IKEv2**를 선택하여 IKEv2 정책을 표시합니다.

단계 **3** 요구사항에 맞는 시스템 정의 정책이 있으면 **State(상태)** 토글을 클릭하여 활성화합니다.

원치 않는 정책을 비활성화할 때도 **State(**상태**)** 토글을 사용합니다. 상대 우선 순위에 따라 이러한 정책 중 먼저 사용을 시도할 정책이 결정되며, 숫자가 작을수록 우선 순위가 높습니다.

단계 **4** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **5** 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.
- **Name(**이름**)** - 개체의 이름(최대 128자)입니다.
- **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 결정, 3 페이지를 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 Diffie-Hellman 모듈러스 그룹 결정, 4 페이지를 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 결정, 4 페이지를 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 결정, 4 페이지를 참조하십시오.

- **Lifetime(**수명 주기**)** - 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 **6** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

IPsec 제안 구성

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 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.

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.

참고 IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

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

IKEv1용 **IPsec** 제안 구성

IKEv1 IPsec 제안 개체를 사용하여 IKE 2단계 협상 시 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다.

여러 가지 사전 정의된 IKEv1 IPsec 제안이 있습니다. 새 제안을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 편집하거나 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 IKEv1 IPsec 설정을 수정하면서 IKEv1 IPsec 제안 개체를 생성할 수도 있습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **IPsec Proposals(IPsec** 제안**)**를 차례로 선택합니다.

단계 **2** 개체 테이블 위의 **IKEv1**을 선택하여 IKEv1 IPsec 제안을 표시합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **4** IKEv1 IPsec 제안 속성을 구성합니다.

- **Name(**이름**)** - 개체의 이름(최대 128자)입니다.
- **Mode(**모드**)** - IPSec 터널이 작동하는 모드입니다.
  - 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.
- **ESP Encryption(ESP** 암호화**)** - 이 제안에 대한 ESP(Encapsulating Security Protocol) 암호화 알고리즘입니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정, 3 페이지를 참조하십시오.
- **ESP Hash(ESP** 해시**)** - 인증에 사용할 해시 또는 무결성 알고리즘입니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정, 4 페이지를 참조하십시오.

단계 **5** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

IKEv2용 IPsec 제안 구성

IKEv2 IPsec 제안 개체를 사용하여 IKE 2단계 협상 시 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다.

여러 가지 사전 정의된 IKEv2 IPsec 제안이 있습니다. 새 제안을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 편집하거나 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 수정하면서 IKEv2 IPsec 제안 개체를 생성할 수도 있습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **IPsec Proposals(IPsec** 제안**)**를 차례로 선택합니다.

단계 **2** 개체 테이블 위의 **IKEv2**를 선택하여 IKEv2 IPsec 제안을 표시합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **4** IKEv2 IPsec 제안 속성을 구성합니다.

- **Name(**이름**)** - 개체의 이름(최대 128자)입니다.
- **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 결정, 3 페이지를 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 결정, 4 페이지를 참조하십시오.

  참고 암호화 알고리즘으로 AES-GCM/GMAC 옵션 중 하나를 선택하는 경우에는 null 무결성 알고리즘을 선택해야 합니다. null이 아닌 옵션을 선택하더라도 이러한 암호화 표준은 무결성 해시를 사용하지 않습니다.

단계 **5** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

사이트 대 사이트 VPN 연결 확인

사이트 대 사이트 VPN 연결을 구성하고 디바이스에 컨피그레이션을 구축한 후에는 시스템이 원격 디바이스와 보안 연결을 설정했는지 확인합니다.

연결을 설정할 수 없는 경우, 디바이스 CLI에서 **ping interface***interface_name remote_ip_address* 명령을 사용하여 VPN 인터페이스를 경유해 원격 디바이스에 이르는 경로가 있는지 확인합니다. 컨피그

레이션된 인터페이스를 경유하는 연결이 없는 경우, **interface** *interface_name* 키워드를 중단하고 연결이 다른 인터페이스를 경유하는지 확인합니다. 연결에 잘못된 인터페이스를 연결했을 가능성이 있습니다. 보호되는 네트워크를 향한 네트워크가 아닌, 원격 디바이스를 향하는 인터페이스를 선택해야 합니다.

네트워크 경로가 있을 경우, 두 엔드포인트에서 지원하는 IKE 버전 및 키를 확인하고 필요한 경우 VPN 연결을 조정합니다. 액세스 제어 또는 NAT 규칙이 연결을 차단하고 있지 않은지 확인합니다.

프로시저

단계 **1** CLI(Command Line Interface) 로그인에 설명된 대로 디바이스 CLI에 로그인합니다.

단계 **2** **show ipsec sa** 명령을 사용해 IPsec 보안 연결이 설정되어 있는지 확인합니다.

디바이스(**local addr**)와 원격 피어(**current_peer**) 사이에 VPN 연결이 설정되었는지 확인해야 합니다. 연결을 통해 트래픽을 전송할 때 패킷(pkts) 수가 증가해야 합니다. 액세스 목록에는 연결의 로컬 및 원격 네트워크가 표시되어야 합니다.

예를 들어 다음 출력은 IKEv2 연결을 표시합니다.

```
> show ipsec sa
interface: site-a-outside
    Crypto map tag: s2sCryptoMap, seq num: 1, local addr: 192.168.2.15

      access-list |s2sAcl|0730e31c-1e5f-11e7-899f-27f6e1030344
extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      current_peer: 192.168.4.6


      #pkts encaps: 69, #pkts encrypt: 69, #pkts digest: 69
      #pkts decaps: 69, #pkts decrypt: 69, #pkts verify: 69
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 69, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.2.15/500, remote crypto endpt.: 192.168.4.6/500
      path mtu 1500, ipsec overhead 55(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: CD22739C
      current inbound spi : 52D2F1E4

    inbound esp sas:
      spi: 0x52D2F1E4 (1389556196)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 19, IKEv2, }
         slot: 0, conn_id: 62738432, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (4285434/28730)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
```

```
        0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xCD22739C (3441587100)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 19, IKEv2, }
         slot: 0, conn_id: 62738432, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (4055034/28730)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

다음 출력은 IKEv1 연결을 표시합니다.

```
> show ipsec sa
interface: site-a-outside
    Crypto map tag: s2sCryptoMap, seq num: 1, local addr: 192.168.2.15

      access-list |s2sAcl|0730e31c-1e5f-11e7-899f-27f6e1030344
extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      current_peer: 192.168.4.6


      #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
      #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 10, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.2.15/0, remote crypto endpt.: 192.168.4.6/0
      path mtu 1500, ipsec overhead 74(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 077D72C9
      current inbound spi : AC146DEC

    inbound esp sas:
      spi: 0xAC146DEC (2887020012)
         SA State: active
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, }
         slot: 0, conn_id: 143065088, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (3914999/28567)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x000007FF
    outbound esp sas:
      spi: 0x077D72C9 (125661897)
         SA State: active
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, }
         slot: 0, conn_id: 143065088, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (3914999/28567)
         IV size: 16 bytes
         replay detection support: Y
```

```
        Anti replay bitmap:
         0x00000000 0x00000001
```

단계 **3** **show isakmp sa** 명령을 사용해 IKE 보안 연결을 확인합니다.

sa 키워드 없이 명령을 사용하거나 **stats** 키워드를 대신 사용하여 IKE 통계를 볼 수 있습니다.

예를 들어 다음 출력은 IKEv2 보안 연결을 표시합니다.

```
> show isakmp sa

There are no IKEv1 SAs

IKEv2 SAs:

Session-id:15317, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local             Remote            Status   Role
592216161 192.168.2.15/500  192.168.4.6/500   READY    INITIATOR
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/12 sec
Child sa: local selector  192.168.1.0/0 - 192.168.1.255/65535
          remote selector 192.168.3.0/0 - 192.168.3.255/65535
          ESP spi in/out: 0x52d2f1e4/0xcd22739c
```

다음 출력은 IKEv1 보안 연결을 표시합니다.

```
> show isakmp sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 192.168.4.6
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs
```

사이트 대 사이트 VPN 모니터링

사이트 대 사이트 VPN 연결을 모니터링하고 트러블슈팅하려면 CLI 콘솔을 열거나 디바이스 CLI에 로그인하여 다음 명령을 사용합니다.

- **show ipsec sa** VPN 세션(보안 연결)을 표시합니다. **clear ipsec sa counters** 명령을 사용하여 이 통계를 재설정할 수 있습니다.
- **show ipsec** *keyword* IPsec 운영 데이터 및 통계가 표시됩니다. 사용 가능한 키워드를 보려면 **show ipsec ?**를 입력합니다.

- **show isakmp** ISAKMP 운영 데이터 및 통계를 표시합니다.

사이트 대 사이트 VPN의 예시

다음에는 사이트 대 사이트 VPN을 구성하는 예시가 나와 있습니다.

NAT에서 사이트 대 사이트 VPN 트래픽 제외

인터페이스에 사이트 대 사이트 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.

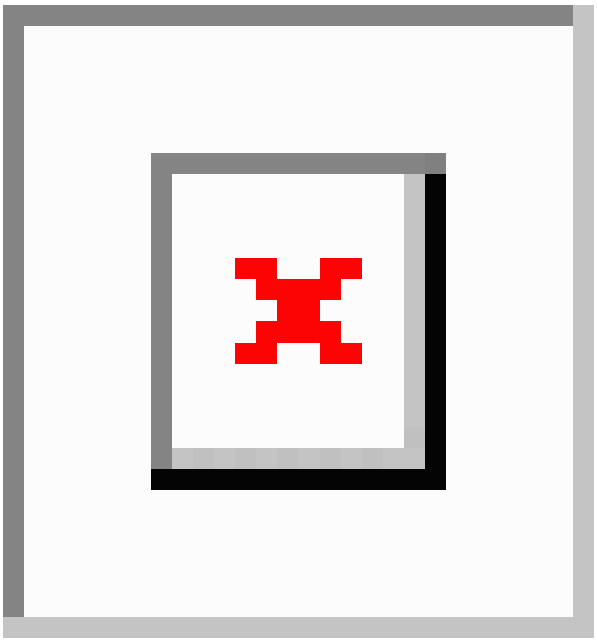
VPN 연결을 생성할 때 **NAT Exempt(NAT** 제외**)** 옵션을 선택하여 규칙을 자동으로 생성할 수 있습니다. 그러나 브리지 그룹 멤버가 아닌 단일 라우팅 인터페이스를 통해 보호된 로컬 네트워크에 연결하는 경우에만 이 방법을 사용할 수 있습니다. 그렇지 않고 연결의 로컬 네트워크가 둘 이상의 라우팅 인터페이스 또는 하나 이상의 브리지 그룹 멤버에 있는 경우에는 NAT 제외 규칙을 수동으로 구성해야 합니다.

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 대 사이트 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. 아래의 예에서는 인터페이스 PAT 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 단순히 주소를 동일한 주소로 변환합니다.

그림 1: 사이트 대 사이트 VPN을 위한 인터페이스 PAT 및 ID NAT



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.

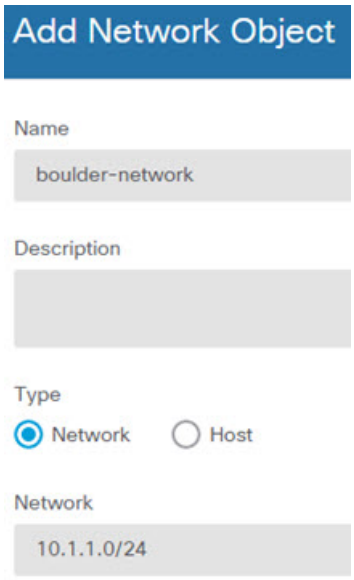
참고 이 예에서는 IPv4만 사용한다고 가정합니다. VPN에 IPv6 네트워크도 포함되어 있으면 IPv6용 병렬 규칙을 생성합니다. IPv6 인터페이스 PAT를 구현할 수는 없으므로 PAT에 사용할 고유 IPv6 주소가 포함된 호스트 개체를 생성해야 합니다.

프로시저

단계 1 여러 네트워크를 정의하기 위한 개체를 생성합니다.

a) **Objects(**개체**)**를 선택합니다.
b) 목차에서 **Network(**네트워크**)**를 선택하고 +를 클릭합니다.
c) 볼더 내부 네트워크를 확인합니다.

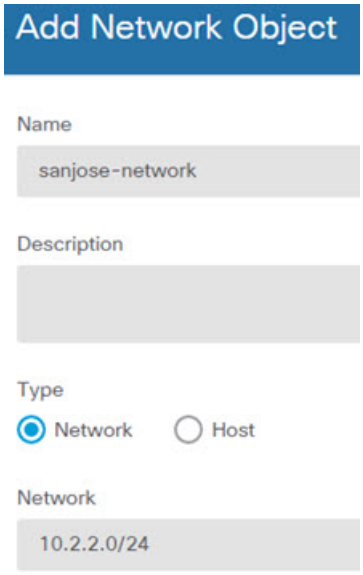
네트워크 개체의 이름을 boulder-network와 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 네트워크 주소 10.1.1.0/24를 입력합니다.



d) **OK(**확인**)**를 클릭합니다.

e) **+**를 클릭하여 내부 산호세 네트워크를 정의합니다.

네트워크 개체의 이름을 sanjose-network와 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 네트워크 주소 10.2.2.0/24를 입력합니다.



f) **OK(**확인**)**를 클릭합니다.

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

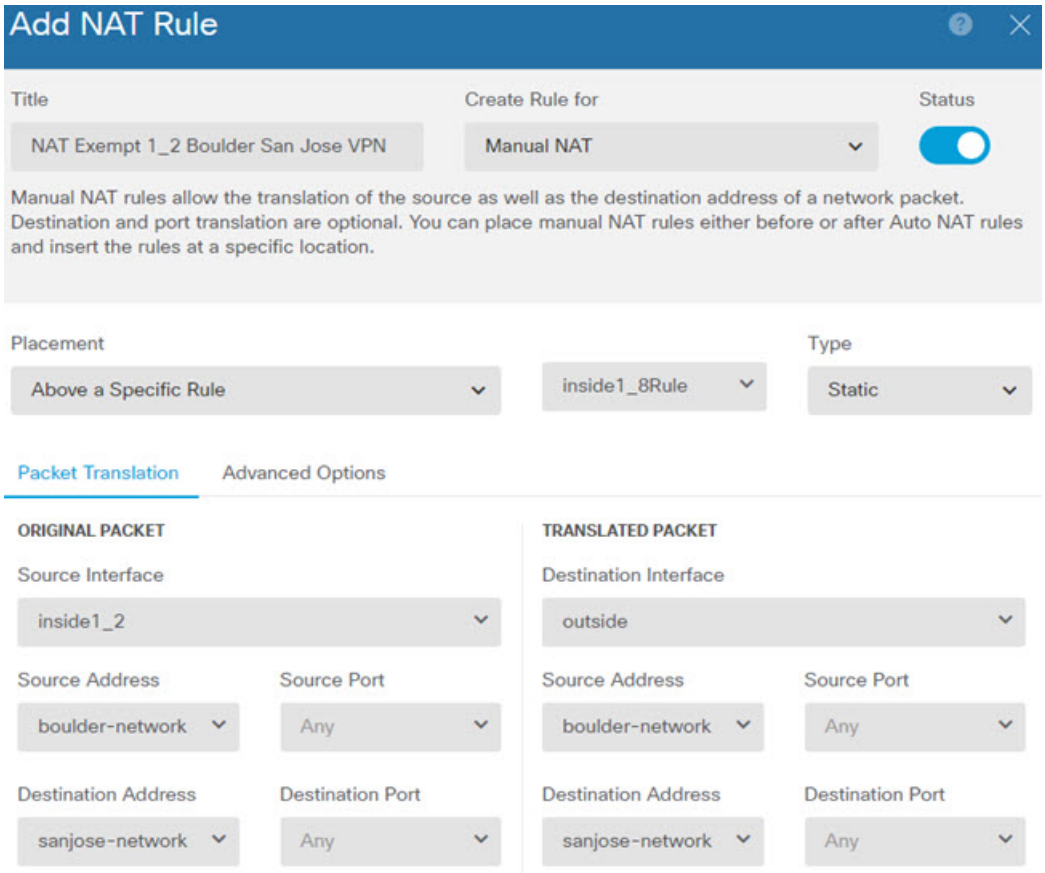
a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) **+** 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- **Title(**제목**)** = NAT Exempt 1_2 Boulder San Jose VPN 또는 원하는 다른 이름
- **Create Rule For(**규칙 생성**)** = 수동 NAT
- **Placement(**배치**)** = 특정 규칙 위를 선택하고 자동 NAT 앞의 수동 NAT 섹션에서 첫 번째 규칙을 선택합니다. 대상 인터페이스의 모든 일반 인터페이스 PAT 규칙 앞에 이 규칙을 배치해야 합니다. 그렇지 않으면 규칙이 적절한 트래픽에 적용되지 않을 수 있습니다.
- **Type(**유형**)** = 고정
- **Source Interface(**소스 인터페이스**)** = inside1_2
- **Destination Interface(**대상 인터페이스**)** = outside
- **Original Source Address(**원본 소스 주소**)** = boulder-network 네트워크 개체
- **Translated Source Address(**변환된 소스 주소**)** = boulder-network 네트워크 개체
- **Original Destination Address(**원본 대상 주소**)** = sanjose-network 네트워크 개체
- **Translated Destination Address(**변환된 대상 주소**)** = sanjose-network 네트워크 개체

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.



d) **Advanced(**고급**)** 탭에서 **Do not proxy ARP on Destination interface(**대상 인터페이스에서 **ARP** 프록시 설정 안 함**)**를 선택합니다.

e) **OK(**확인**)**를 클릭합니다.

f) 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 컨피그레이션 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.

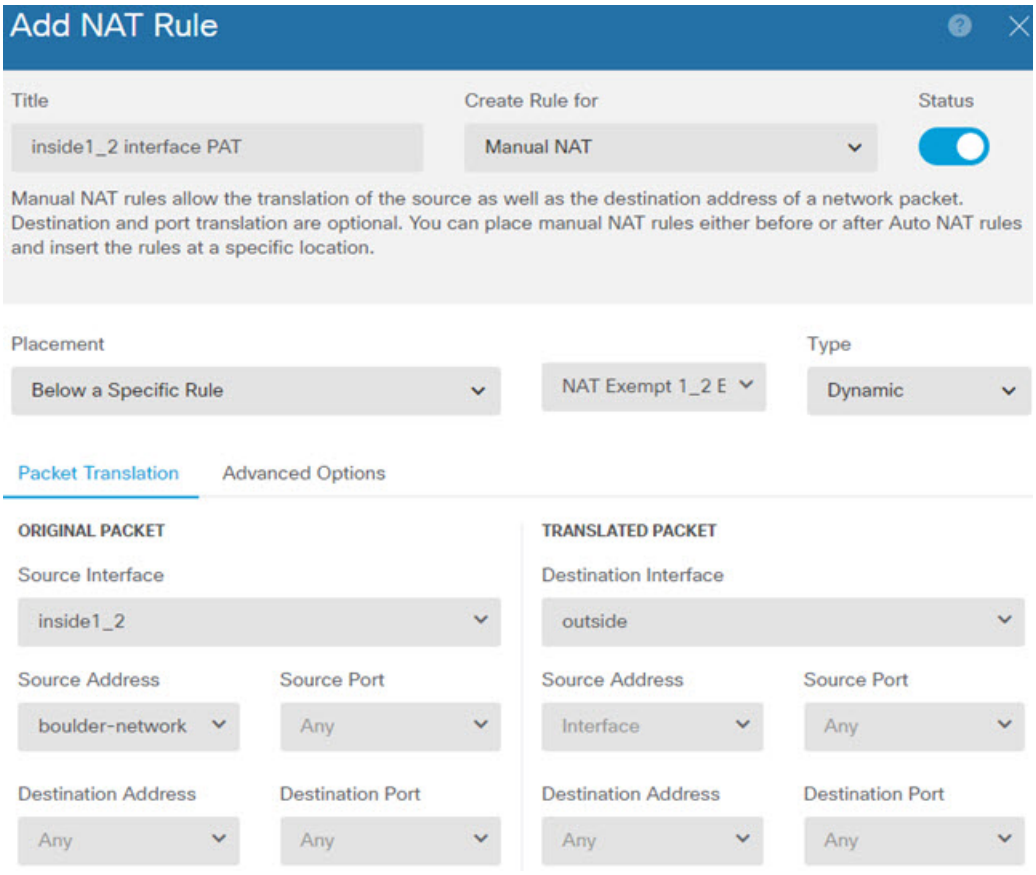
a) + 버튼을 클릭합니다.

b) 다음 속성을 구성합니다.

- **Title(**제목**)** = inside1_2 interface PAT 또는 원하는 다른 이름
- **Create Rule For(**규칙 생성**)** = 수동 NAT
- **Placement(**배치**)** = 특정 규칙 아래를 선택하고 자동 NAT 앞의 수동 NAT 섹션에서 이 인터페이스용으로 생성한 규칙을 선택합니다. 이 규칙은 모든 대상 주소에 적용되므로 sanjose-network

를 대상으로 사용하는 규칙이 이 규칙 앞에 와야 합니다. 그렇지 않으면 sanjose-network 규칙은 어떤 주소와도 일치하지 않게 됩니다. 기본적으로는 "자동 NAT 앞의 NAT 규칙" 섹션 끝에 새 수동 NAT 규칙을 배치합니다. 이 기본 배치를 사용해도 충분합니다.

- **Type(**유형**)** = 동적
- **Source Interface(**소스 인터페이스**)** = inside1_2
- **Destination Interface(**대상 인터페이스**)** = outside
- **Original Source Address(**원본 소스 주소**)** = boulder-network 네트워크 개체
- **Translated Source Address(**변환된 소스 주소**)** = **Interface** 이 옵션은 대상 인터페이스를 사용하여 인터페이스 PAT를 구성합니다.
- **Original Destination Address(**원본 대상 주소**)** = 임의
- **Translated Destination Address(**변환된 대상 주소**)** = 임의



c) **OK(**확인**)**를 클릭합니다.

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

단계 **4** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

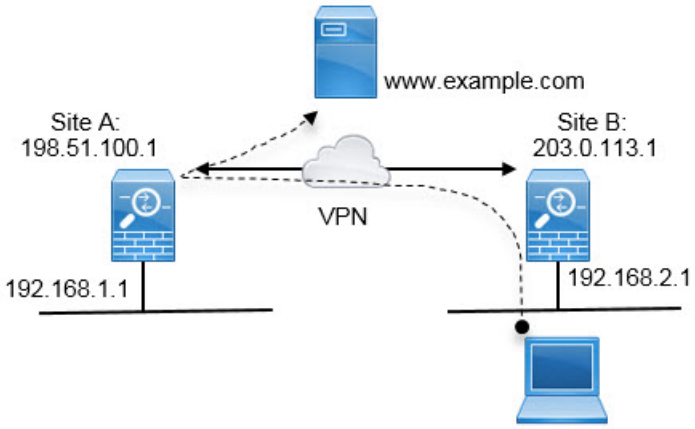
단계 **5** 방화벽2(산호세)도 관리하는 경우 해당 디바이스에 대해 비슷한 규칙을 구성할 수 있습니다.

- 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.

외부 사이트 대 사이트 **VPN** 사용자에게 외부 인터페이스를 통해 인터넷 액세스를 제공하는 방법(헤어피닝)

사이트 대 사이트 VPN에서는 원격 네트워크의 사용자가 디바이스를 통해 인터넷에 액세스하도록 할 수 있습니다. 그러나 원격 사용자는 인터넷에 연결되는 것과 동일한 인터페이스(외부 인터페이스)를 통해 디바이스에 진입하므로 인터넷 트래픽이 외부 인터페이스로 다시 나가도록 바운스해야 합니다. 이 기술을 헤어피닝이라고도 합니다.

다음 그림에 예시가 나와 있습니다. 기본 사이트인 사이트 A의 198.51.100.1과 원격 사이트인 사이트 B의 203.0.113.1 사이에 사이트 대 사이트 VPN 터널이 구성되어 있습니다. 원격 사이트 내부 네트워크인 192.168.2.0/24의 모든 사용자 트래픽은 VPN을 통과합니다. 따라서 해당 네트워크의 사용자가 www.example.com 등의 인터넷 서버로 이동하려는 경우 해당 연결은 먼저 VPN을 통과한 다음 198.51.100.1 인터페이스에서 인터넷으로 다시 라우팅됩니다.



다음 절차에서는 이 서비스를 구성하는 방법을 설명합니다. VPN 터널의 두 엔드포인트를 모두 구성해야 합니다.

시작하기 전에

이 절차에서는 VPN 트래픽을 허용하기 위해 기본 설정을 사용 중이며 이를 통해 VPN 트래픽을 액세스 제어 정책에 종속시킨다고 가정합니다. 이것은 실행 중인 컨피그레이션에서 **no sysopt connection permit-vpn** 명령으로 표시됩니다. 대신에 **sysopt connection permit-vpn** FlexConfig를 통해 또는 RA VPN 연결 프로파일에서 **Bypass Access Control policy for decrypted traffic(**암호 해독된 트래픽에 대해 액세스 제어 정책 우회**)** 옵션을 선택하여 활성화한 경우, 액세스 제어 규칙을 컨피그레이션하는 단계는 필요하지 않습니다.

프로시저

단계 **1** (사이트 A, 기본 사이트.) 원격 사이트 B로의 사이트 대 사이트 VPN 연결을 구성합니다.

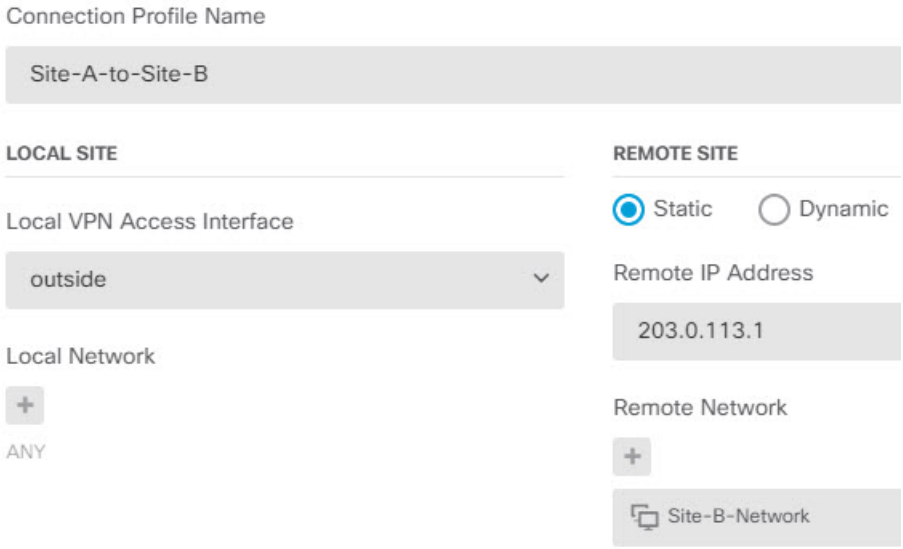
a) 디바이스를 클릭한 다음 사이트 대 사이트 VPN 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

b) **+**를 클릭하여 새 연결을 추가합니다.

c) 다음과 같이 엔드포인트를 정의하고 **Next(**다음**)**를 클릭합니다.

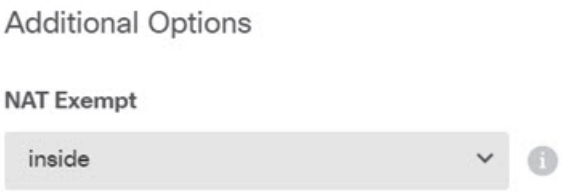
- **Connection Profile Name(**연결 프로파일 이름**)** - Site-A-to-Site-B와 같이 의미 있는 이름을 연결에 지정합니다.
- **Local VPN Access Interface(**로컬 **VPN** 액세스 인터페이스**)** - 외부 인터페이스를 선택합니다.
- **Local Network(**로컬 네트워크**)** - 기본값인 Any(모두)를 유지합니다.
- **Remote IP Address(**원격 **IP** 주소**)** - 원격 피어 외부 인터페이스의 IP 주소를 입력합니다. 이 예시에서는 203.0.113.1입니다.
- **Remote Network(**원격 네트워크**)** - **+**를 클릭하고 원격 피어의 보호된 네트워크를 정의하는 네트워크 개체를 선택합니다. 이 예시에서는 192.168.2.0/24입니다. **Create New Network(**새 네트워크 생성**)**를 클릭하면 바로 개체를 생성할 수 있습니다.

다음 그림은 어떻게 첫 단계가 표시되는지를 보여줍니다.



d) 프라이버시 컨피그레이션을 정의하고 **Next(**다음**)**를 클릭합니다.

- **IKE Policy(IKE** 정책**)** - IKE 설정은 헤어피닝에 영향을 주지 않습니다. 보안 요구 사항에 맞는 IKE 버전, 정책 및 제안만 선택하면 됩니다. 입력하는 로컬 및 원격 사전 공유 키를 적어 두십시오. 원격 피어를 구성할 때 해당 키가 필요합니다.
- **NAT Exempt(NAT** 면제**)** - 내부 인터페이스를 선택합니다.



- **Diffie Helman Group for Perfect Forward Secrecy(PFS(Perfect Forward Secrecy)**를 위한 **Diffie Hellman** 그룹**)** - 이 설정은 헤어피닝에 영향을 주지 않습니다. 따라서 적합하게 구성하면 됩니다.

e) **Finish(**마침**)**를 클릭합니다.

연결 요약이 클립보드에 복사됩니다. 해당 요약을 텍스트 파일 또는 다른 문서에 붙여넣어 원격 피어를 구성하는 데 사용할 수 있습니다.

단계 **2** (사이트 A, 기본 사이트.) 외부 인터페이스에서 외부 IP 주소의 포트로 나가는 모든 연결을 변환하는 NAT 규칙(인터페이스 PAT)을 구성합니다.

초기 디바이스 컨피그레이션을 완료하면 InsideOutsideNatRule이라는 NAT 규칙이 생성됩니다. 이 규칙은 외부 인터페이스를 통해 디바이스에서 나가는 모든 인터페이스의 IPv4 트래픽에 인터페이스 PAT를 적용합니다. 외부 인터페이스는 "Any" 소스 인터페이스에 포함되므로 필요한 규칙을 수정하거나 삭제한 경우가 아니면 규칙이 이미 존재합니다.

다음 절차에서는 필요한 규칙을 생성하는 방법을 설명합니다.

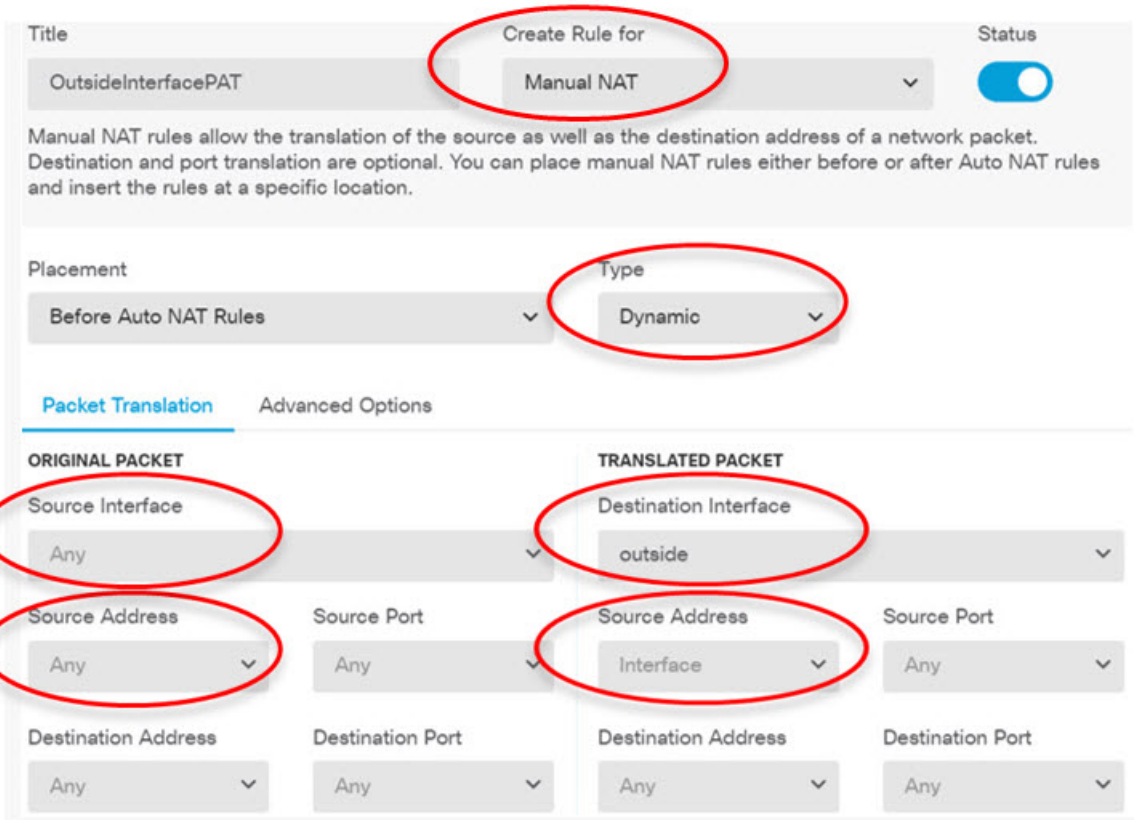
a) **Policies(**정책**)** > **NAT**를 클릭합니다.
b) 다음 중 하나를 수행합니다.

- InsideOutsideNatRule을 수정하려면 **Action(**작업**)** 열 위에 마우스를 놓고 수정 아이콘( )을 클릭합니다.
- 새 규칙을 생성하려면 **+**를 클릭합니다.

c) 다음 속성을 사용하여 규칙을 구성합니다.

- **Title(**제목**)** - 새 규칙의 경우 의미 있는 이름을 공백 없이 입력합니다. 예를 들어 OutsideInterfacePAT를 입력합니다.
- **Create Rule For(**규칙 생성 대상**)** - **Manual NAT(**수동 **NAT)**.
- **Placement(**배치**)** - **Before Auto NAT Rules(**자동 **NAT** 규칙 앞**)**(기본값).
- **Type(**유형**)** - **Dynamic(**동적**)**.
- **Original Packet(**원본 패킷**)** - **Source Address(**소스 주소**)**의 경우 Any(모두) 또는 any-ipv4를 선택합니다. **Source Interface(**소스 인터페이스**)**의 경우 기본값인 Any(모두)를 선택해야 합니다. 기타 모든 Original Packet(원본 패킷) 옵션의 경우 기본값인 Any(모두)를 유지합니다.
- **Translated Packet(**변환된 패킷**)** - **Destination Interface(**대상 인터페이스**)**의 경우 outside(외부)를 선택합니다. **Translated Address(**변환된 주소**)**의 경우 **Interface(**인터페이스**)**를 선택합니다. 기타 모든 Translated Packet(변환된 패킷) 옵션의 경우 기본값인 Any(모두)를 유지합니다.

다음 그림에는 소스 주소로 Any(모두)를 선택하는 간단한 사례가 나와 있습니다.



d) **OK(**확인**)**를 클릭합니다.

단계 **3** (사이트 A, 기본 사이트.) 사이트 B에서 보호된 네트워크에 대한 액세스를 허용하는 액세스 제어 규칙을 구성합니다.

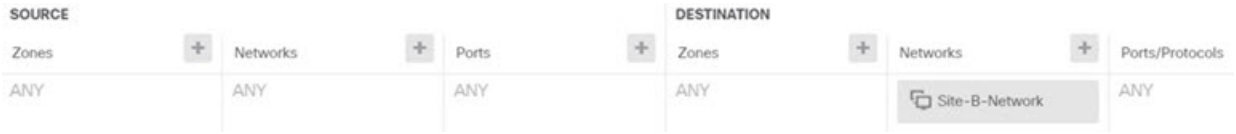
단순히 VPN 연결을 생성한다고 해서 VPN에서 트래픽을 자동으로 허용하지 않습니다. 액세스 제어 정책이 원격 네트워크로의 트래픽을 허용하는지를 확인해야 합니다.

다음 절차는 원격 네트워크에 대해 구체적으로 규칙을 추가하는 방법을 보여줍니다. 추가 규칙이 필요한지 여부는 기존 규칙에 따라 달라집니다.

a) **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 클릭합니다.
b) +를 클릭하여 새 규칙을 생성합니다.
c) 다음 속성을 사용하여 규칙을 구성합니다.

- **Order(**순서**)** - 연결을 찾아 차단하는 다른 규칙 앞에 해당 규칙을 넣도록 정책 내의 위치를 선택합니다. 기본적으로는 규칙이 정책의 끝에 추가됩니다. 나중에 규칙을 재배치해야 하는 경우 이 옵션을 수정하거나, 규칙을 끌어서 표의 원하는 슬롯에 놓을 수 있습니다.
- **Title(**제목**)** - 의미 있는 이름을 공백 없이 입력합니다. 예를 들어 Site-B-Network를 입력합니다.
- **Action(**작업**)** - **Allow(**허용**)**. 이 트래픽의 프로토콜 위반 또는 침입을 검사하지 않으려는 경우 Trust(신뢰)를 선택할 수 있습니다.

- **Source/Destination(**소스/대상**)** 탭 - **Destination(**대상**)** > **Network(**네트워크**)**의 경우 원격 네트워크의 VPN 연결 프로파일에서 사용한 것과 같은 개체를 선택합니다. 기타 모든 Source(소스) 및 Destination(대상) 옵션의 경우 기본값인 Any(모두)를 유지합니다.



- **Application(**애플리케이션**)**, **URL** 및 **Users(**사용자**)** 탭 - 이러한 탭에서는 기본 설정, 즉 아무 설정도 선택하지 않은 상태를 유지합니다.
- **Intrusion(**침입**)**, **File(**파일**)** 탭 - 선택적으로 위협이나 악성코드를 검사하기 위한 침입 또는 파일 정책을 선택할 수 있습니다.
- **Logging(**로깅**)** 탭 - 선택적으로 연결 로깅을 활성화할 수 있습니다.

d) **OK(**확인**)**를 클릭합니다.

단계 **4** (사이트 A, 기본 사이트.) 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다. 창을 활성화한 상태로 유지하면 구축에 성공한 후에 보류 중인 변경 사항이 없다는 메시지가 표시됩니다.

단계 **5** (사이트 B, 원격 사이트.) 원격 사이트의 디바이스에 로그인하여 사이트 A로의 사이트 대 사이트 VPN 연결을 구성합니다.

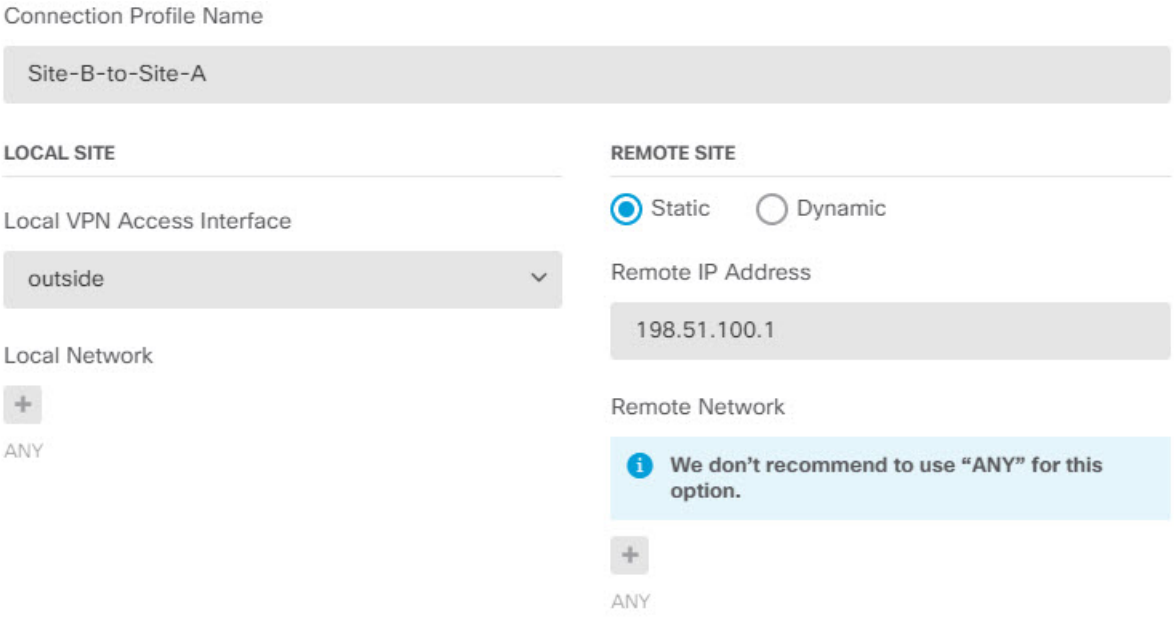
사이트 A 디바이스 컨피그레이션에서 가져온 연결 요약을 사용하여 연결의 사이트 B 측을 구성할 수 있습니다.

a) 디바이스를 클릭한 다음 사이트 대 사이트 VPN 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.
b) +를 클릭하여 새 연결을 추가합니다.
c) 다음과 같이 엔드포인트를 정의하고 **Next(**다음**)**를 클릭합니다.

- **Connection Profile Name(**연결 프로파일 이름**)** - Site-B-to-Site-A와 같이 의미 있는 이름을 연결에 지정합니다.
- **Local VPN Access Interface(**로컬 **VPN** 액세스 인터페이스**)** - 외부 인터페이스를 선택합니다.
- **Local Network(**로컬 네트워크**)** - +를 클릭하고 보호된 로컬 네트워크를 정의하는 네트워크 개체를 선택합니다. 이 예시에서는 192.168.2.0/24입니다. **Create New Network(**새 네트워크 생성**)**를 클릭하면 바로 개체를 생성할 수 있습니다.

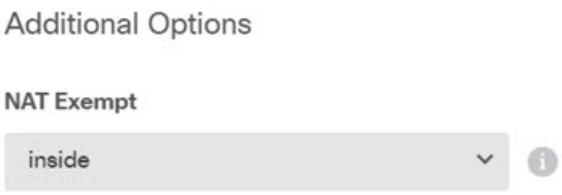
- **Remote IP Address(**원격 **IP** 주소**)** - 기본 사이트 외부 인터페이스의 IP 주소를 입력합니다. 이 예시에서는 198.51.100.1입니다.
- **Remote Network(**원격 네트워크**)** - 기본값인 Any(모두)를 유지합니다. 경고는 이 사용 사례와 관련이 없으므로 무시하십시오.

다음 그림은 어떻게 첫 단계가 표시되는지를 보여줍니다.



d) 프라이버시 컨피그레이션을 정의하고 **Next(**다음**)**를 클릭합니다.

- **IKE Policy(IKE** 정책**)** - IKE 설정은 헤어피닝에 영향을 주지 않습니다. 사이트 A의 VPN 연결 끝과 같거나 호환되는 옵션을 구성합니다. 사전 공유 키를 올바르게 구성해야 합니다. 사이트 A 디바이스에 구성된 로컬 및 원격 키(IKEv2용)를 전환합니다. IKEv1의 경우에는 키가 하나뿐이며 두 피어에서 동일해야 합니다.
- **NAT Exempt(NAT** 면제**)** - 내부 인터페이스를 선택합니다.



- **Diffie Helman Group for Perfect Forward Secrecy(PFS(Perfect Forward Secrecy)**를 위한 **Diffie Hellman** 그룹**)** - 이 설정은 헤어피닝에 영향을 주지 않습니다. 사이트 A의 VPN 연결 끝에서 사용한 설정과 일치시킵니다.

e) **Finish(**마침**)**를 클릭합니다.

단계 **6** (사이트 B, 원격 사이트.) 사이트에서 나가는 모든 트래픽이 VPN 터널을 통과하도록 보호된 네트워크의 모든 NAT 규칙을 삭제합니다.

사이트 A 디바이스가 주소 변환을 수행하므로 이 디바이스에서는 NAT를 수행할 필요가 없습니다. 하지만 구체적인 상황을 점검해야 합니다. 내부 네트워크가 여러 개인데 그중 일부가 이 VPN 연결에 포함되지 않는 경우 해당 네트워크에 필요한 NAT 규칙은 삭제하지 마십시오.

a) **Policies(**정책**)** > **NAT**를 클릭합니다.
b) 다음 중 하나를 수행합니다.

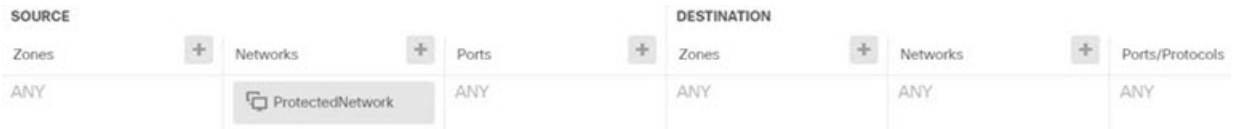
- 규칙을 삭제하려면 Action(작업) 열 위에 마우스를 놓고 삭제 아이콘( )을 클릭합니다.
- 보호된 네트워크에 더 이상 적용되지 않도록 규칙을 수정하려면 Action(작업) 열 위에 마우스를 놓고 수정 아이콘( )을 클릭합니다.

단계 **7** (사이트 B, 원격 사이트.) 보호된 네트워크에서 인터넷에 대한 액세스를 허용하는 액세스 제어 규칙을 구성합니다.

다음 예시에서는 보호된 네트워크에서 특정 대상으로의 트래픽을 허용합니다. 구체적인 요구 사항에 맞게 이 예시를 조정할 수 있습니다. 또한 이 규칙 앞에 원치 않는 트래픽을 필터링하여 제거하는 차단 규칙을 배치할 수도 있습니다. 사이트 A 디바이스에서 차단 규칙을 구성하는 옵션도 있습니다.

a) **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 클릭합니다.
b) +를 클릭하여 새 규칙을 생성합니다.
c) 다음 속성을 사용하여 규칙을 구성합니다.

- **Order(**순서**)** - 연결을 찾아 차단하는 다른 규칙 앞에 해당 규칙을 넣도록 정책 내의 위치를 선택합니다. 기본적으로는 규칙이 정책의 끝에 추가됩니다. 나중에 규칙을 재배치해야 하는 경우 이 옵션을 수정하거나, 규칙을 끌어서 표의 원하는 슬롯에 놓을 수 있습니다.
- **Title(**제목**)** - 의미 있는 이름을 공백 없이 입력합니다. 예를 들어 Protected-Network-to-Any를 입력합니다.
- **Action(**작업**)** - **Allow(**허용**)**. 이 트래픽의 프로토콜 위반 또는 침입을 검사하지 않으려는 경우 Trust(신뢰)를 선택할 수 있습니다.
- **Source/Destination(**소스/대상**)** 탭 - **Source(**소스**)** > **Network(**네트워크**)**의 경우 로컬 네트워크의 VPN 연결 프로파일에서 사용한 것과 같은 개체를 선택합니다. 기타 모든 Source(소스) 및 Destination(대상) 옵션의 경우 기본값인 Any(모두)를 유지합니다.



- **Application(**애플리케이션**)**, **URL** 및 **Users(**사용자**)** 탭 - 이러한 탭에서는 기본 설정, 즉 아무 설정도 선택하지 않은 상태를 유지합니다.
- **Intrusion(**침입**)**, **File(**파일**)** 탭 - 선택적으로 위협이나 악성코드를 검사하기 위한 침입 또는 파일 정책을 선택할 수 있습니다.

• **Logging(**로깅**)** 탭 - 선택적으로 연결 로깅을 활성화할 수 있습니다.

d) **OK(**확인**)**를 클릭합니다.

단계 **8** (사이트 B, 원격 사이트.) 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭하고 구축이 완료될 때까지 기다립니다.

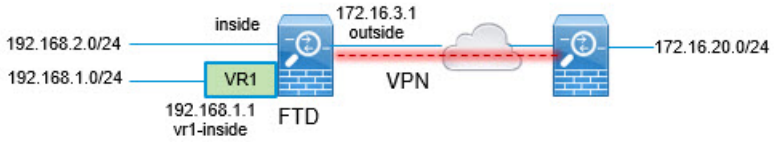
구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다. 창을 활성화한 상태로 유지하면 구축에 성공한 후에 보류 중인 변경 사항이 없다는 메시지가 표시됩니다.

사이트 간 VPN을 통해 여러 가상 라우터의 네트워크에서 트래픽을 보호하는 방법

디바이스에서 여러 가상 라우터를 구성하는 경우에는 전역 가상 라우터에서 사이트 간 VPN을 구성해야 합니다. 사용자 지정 가상 라우터에 할당된 인터페이스에는 사이트 간 VPN을 구성할 수 없습니다.

가상 라우터의 라우팅 테이블은 별도이기 때문에, 사이트 간 VPN을 통해 맞춤형 가상 라우터에서 호스팅되는 네트워크에서 연결을 보호해야 하는 경우 정적 경로를 생성해야 합니다. 또한 이러한 추가 네트워크를 포함하도록 사이트 간 VPN 연결을 업데이트해야 합니다.

다음과 같은 사례를 가정해보십시오. 이 경우 사이트 간 VPN은 172.16.3.1의 외부 인터페이스에 정의됩니다. 내부 인터페이스는 전역 가상 라우터의 일부이므로 이 VPN에는 추가 구성없이 내부 네트워크 192.168.2.0/24를 포함할 수 있습니다. 그러나 VR1 가상 라우터의 일부인 192.168.1.0/24 네트워크에 사이트 간 VPN 서비스를 제공해야 하는 경우에는 정적 경로를 두 가지 방식으로 모두 구성하고 사이트 간 VPN 구성에 네트워크를 추가해야 합니다.



시작하기 전에

이 예에서는 192.168.2.0/24 로컬 네트워크와 172.16.20.0/24 외부 네트워트 간의 사이트 간 VPN을 이미 구성하고 가상 라우터를 정의했으며 적절한 가상 라우터에 인터페이스를 구성 및 할당한 것으로 가정합니다.

프로시저

단계 **1** 전역 가상 라우터에서 VR1으로의 경로 유출을 구성합니다.

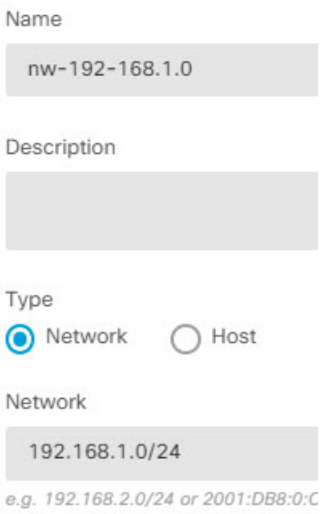
이 경로는 사이트 간 VPN의 외부(원격) 끝에서 보호하는 엔드포인트를 VR1 가상 라우터의 192.168.1.0/24 네트워크에 액세스하는 데 사용할 수 있습니다.

a) **Device(**디바이스**)** > **Routing(**라우팅**)** > **View Configuration(**구성 보기**)**을 선택합니다.

b) 전역 가상 라우터의 View Icon(아이콘 보기)을 클릭합니다.

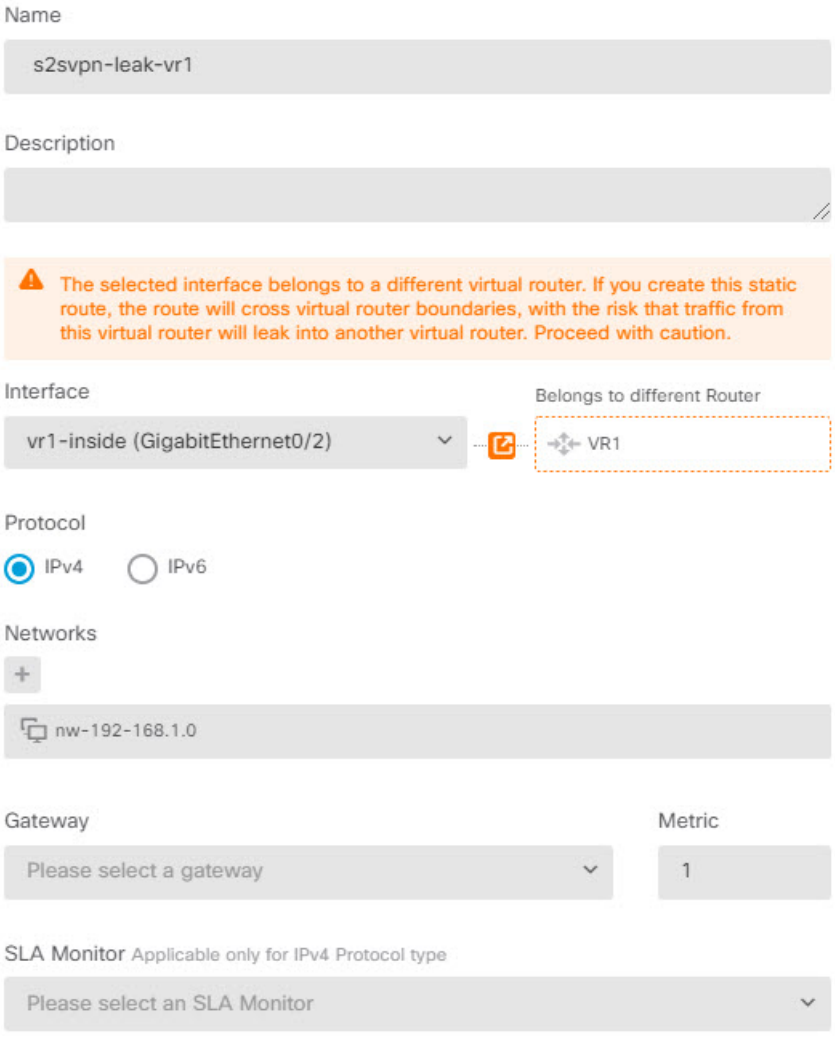
c) 전역 라우터에 대한 **Static Routing(**정적 라우팅**)** 탭에서 **+**를 클릭하고 다음과 같이 경로를 구성합니다.

- **Name(**이름**)**—모든 이름(예: **s2svpn-leak-vr1**)이 수행됩니다.
- **Interface(**인터페이스**)** — **vr1-inside**를 선택합니다.
- **Protocol(**프로토콜**)** — **IPv4**를 선택합니다.
- **Network(**네트워크**)**—192.168.1.0/24 네트워크를 정의하는 개체를 선택합니다. 필요한 경우 **Create New Network(**새 네트워크 생성**)**를 클릭하면 바로 개체를 생성할 수 있습니다.



- **Gateway(**게이트웨이**)** — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이 주소를 선택하지 않습니다.

대화 상자가 다음과 비슷하게 표시됩니다.



d) **OK(**확인**)**를 클릭합니다.

단계 **2** VR1에서 전역 가상 라우터로의 경로 유출을 구성합니다.

이 경로를 사용하면 192.168.1.0/24 네트워크의 엔드포인트에서 사이트 간 VPN 터널을 통과하는 연결을 시작할 수 있습니다. 이 예에서는 원격 엔드포인트에서 172.16.20.0/24 네트워크를 보호하고 있습니다.

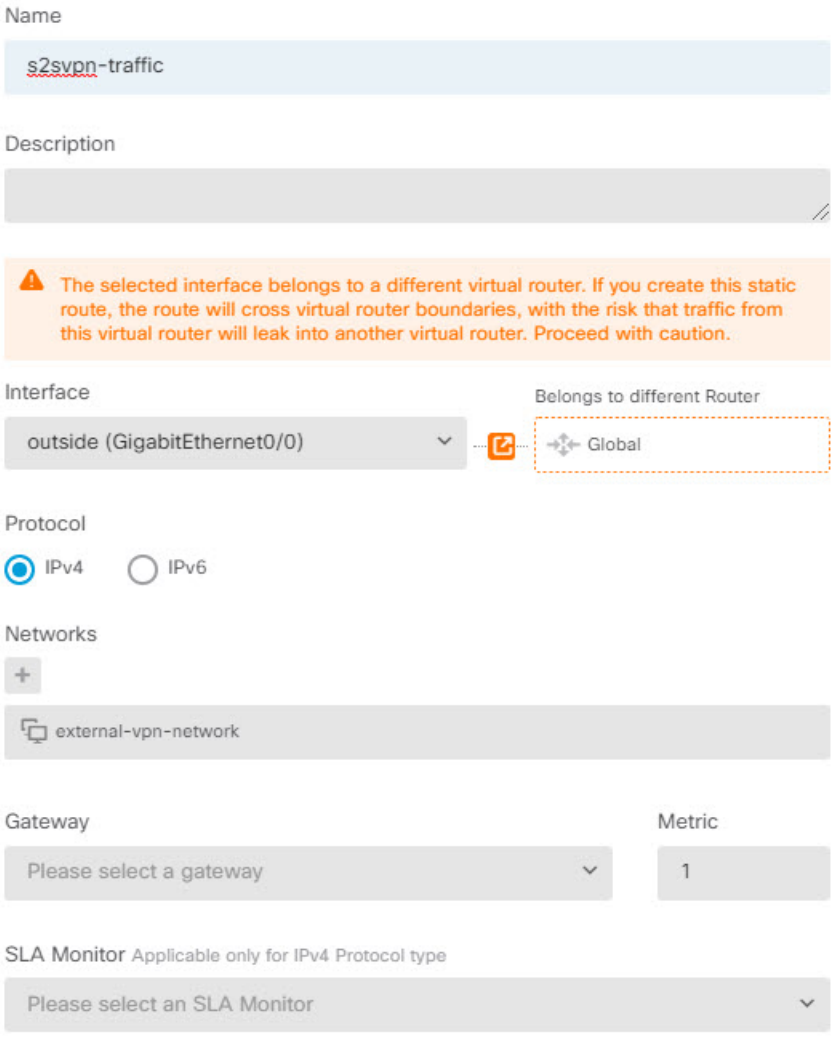
a) 가상 라우터 드롭다운 목록에서 **VR1**을 선택하여 VR1 구성으로 전환합니다.

b) VR1 가상 라우터에 대한 **Static Routing(**정적 라우팅**)** 탭에서 +를 클릭하고 다음과 같이 경로를 구성합니다.

- **Name(**이름**)** — 모든 이름(예: **s2svpn-traffic**)이 수행됩니다.
- **Interface(**인터페이스**)** — **outside**를 선택합니다.
- **Protocol(**프로토콜**)** — **IPv4**를 선택합니다.

- **Network(**네트워크**)** —원격 엔드포인트의 보호된 네트워크(예: 외부 **VPN** 네트워크)에 대해 생성한 개체를 선택합니다.
- **Gateway(**게이트웨이**)** — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이 주소를 선택하지 않습니다.

대화 상자가 다음과 비슷하게 표시됩니다.



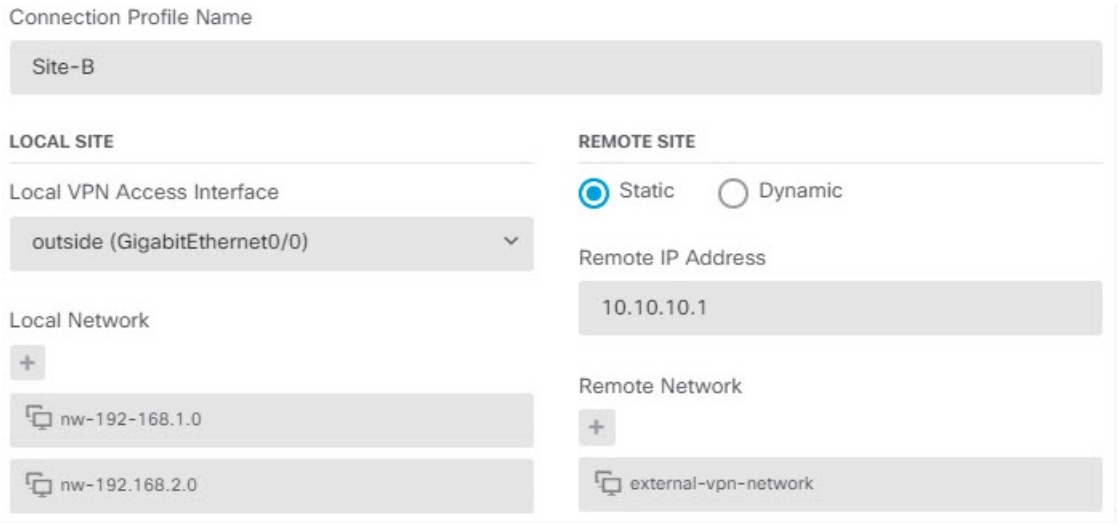
c) **OK(**확인**)**를 클릭합니다.

단계 **3** 사이트 간 VPN 연결 프로파일에 192.168.1.0/24 네트워크를 추가합니다.

a) **Device(**디바이스**)** > **Site-to-Site VPN(**사이트 간 **VPN)** > **View Configuration(**구성 보기**)**을 선택합니다.

b) 연결 프로파일에 대한 edit icon(수정 아이콘)()을(를) 클릭합니다.

c) 마법사의 첫 번째 페이지에서 로컬 네트워크 아래의 +을(를) 클릭하고 192.168.1.0/24 네트워크에 대한 개체를 추가합니다.


Connection Profile Name
Site-B
LOCAL SITE
Local VPN Access Interface
outside (GigabitEthernet0/0)
Local Network
nw-192-168.1.0
nw-192.168.2.0
REMOTE SITE
Static
Dynamic
Remote IP Address
10.10.10.1
Remote Network
external-vpn-network

d) 마법사를 완료합니다.

사이트 간 **VPN**을 통해 여러 가상 라우터의 네트워크에서 트래픽을 보호하는 방법