# VPN 개요

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

이 장은 Secure Firewall Threat Defense 디바이스의 Remote Access 및 Site-to-Site VPN에 적용됩니다. 여기에서는 Site-to-Site 및 Remote Access VPN을 구축하는 데 사용되는 IPsec(Internet Protocol Security) 및 ISAKMP(Internet Security Association and Key Management Protocol) 표준에 대해 설명합니다.



# VPN 유형

management center에서는 다음과 같은 유형의 VPN 연결을 지원합니다.

- threat defense 디바이스의 Remote Access VPN.

  Remote Access VPN은 원격 사용자와 회사의 프라이빗 네트워크 간에 보안, 암호화된 연결 또는 터널입니다. 연결은 VPN 클라이언트 기능이 있는 워크스테이션 또는 모바일 장치인 VPN 엔드포인트 장치 및 회사 프라이빗 네트워크의 에지에 있는 VPN 헤드엔드 장치 또는 보안 게이트웨이로 구성됩니다.

  Secure Firewall Threat Defense 디바이스는 SSL을 통한 Remote Access VPN 또는 management center에 의한 IPsec IKEv2를 지원하도록 구성될 수 있습니다. 이 용량의 보안 게이트웨이로 작동하여 원격 사용자를 인증하고 액세스 권한을 부여하며 데이터를 암호화하여 네트워크에 대한 보안 연결을 제공합니다. management center에 의해 관리되는 다른 유형의 어플라이언스는 Remote Access VPN 연결을 지원하지 않습니다.

Secure Firewall Threat Defense 보안 게이트웨이는 Secure Client 전체 터널 클라이언트를 지원합니다. 이 클라이언트는 원격 사용자에게 안전한 SSL IPsec IKEv2 연결을 제공해야 합니다. 이 클라이언트는 연결 시 클라이언트 플랫폼에 배포할 수 있으므로 네트워크 관리자가 원격 컴퓨터에 클라이언트를 설치하고 구성할 필요 없이 원격 사용자에게 클라이언트의 이점을 제공합니다. 이는 엔드포인트 디바이스에서만 지원되는 클라이언트입니다.

- threat defense 디바이스의 Site-to-Site VPN.

  Site-to-Site VPN은 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 IKEv1 또는 IKEv2를 사용하여 구축됩니다. VPN 연결이 설정되면 로컬 게이트웨이의 뒤에 있는 호스트는 보안 VPN 터널을 통해 원격 게이트의 뒤에 있는 호스트와 연결할 수 있습니다.

# 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 간 VPN의 경우에는 IKE 정책을 생성할 수 있습니다. IKEv1 및 IKEv2는 각각 최대 20개의 IKE 정책을 지원하고 서로 다른 설정 값을 사용합니다. 생성한 각 정책에 고유 우선순위를 지정하십시오. 우선순위 번호가 낮을수록 우선순위가 더 높습니다.

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
- 보낸사람의 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 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 피어 정책의 더 짧은 수명이 적용됩니다. 기본적으로 Secure Firewall Management Center에서는 협상이 정상적으로 진행되도록 모든 VPN 엔드포인트에 대해 가장 낮은 우선 순위의 IKEv1 정책을 구축합니다.

# IPSec

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 공

용 네트워크를 사용하여 전송됩니다. 터널은 두 피어 간의 안전한 논리적 통신 경로입니다. IPsec 터널로 진입하는 트래픽은 보안 프로토콜 및 알고리즘의 조합에 의해 보호됩니다.

IPsec 제안 정책은 IPsec 터널에 필요한 설정을 정의합니다. IPsec 제안은 디바이스의 VPN 인터페이스에 적용되는 하나 이상의 암호화 맵 모음입니다. 암호화 맵은 다음과 같이 IPsec 보안 연결을 설정하는 데 필요한 모든 구성 요소를 결합합니다.

- IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합의 제안(변환 집합). IPsec 보안 연계(SA) 협상 중에 피어는 두 피어에서 동일한 제안을 검색합니다. 검색된 제안은 해당 암호화 맵의 액세스 목록에 있는 데이터 흐름을 보호하는 SA를 생성하여 VPN의 트래픽을 보호하는 데 적용됩니다. IKEv1과 IKEv2에 대한 별도의 IPsec 제안이 있습니다. IKEv1 제안(또는 변환 집합)에서 각 파라미터에 대해 하나의 값을 설정합니다. IKEv2 제안의 경우 단일 제안에 여러 개의 암호화와 인증 유형 및 여러 개의 무결성 알고리즘을 구성할 수 있습니다.
- 암호화 맵은 IPsec SA를 정의하는 데 필요한 IPsec 규칙, 제안, 원격 피어 및 기타 파라미터를 비롯하여 IPsec SA(보안 연결)를 필요한 모든 구성 요소를 결합합니다. 두 피어에서 SA를 설정하려고 시도할 때 최소 1개 이상의 호환 가능한 암호화 맵이 있어야 합니다.

  알 수 없는 원격 피어가 로컬 허브와의 IPsec 보안 연결을 시작하려고 하면 동적 암호화 맵 정책이 Site-to-Site VPN에 사용됩니다. 허브는 보안 연결 협상의 이니시에이터가 될 수 없습니다. 동적 암호화 정책은 허브가 원격 피어의 ID를 알지 못하는 경우에도 원격 피어가 IPsec 트래픽을 로컬 허브와 교환할 수 있게 허용합니다. 동적 암호화 맵 정책은 기본적으로 모든 파라미터가 구성되지 않은 상태의 암호화 맵 항목을 생성합니다. 누락된 파라미터는 나중에 원격 피어의 요구사항과 일치하도록 동적으로 구성됩니다(IPsec 협상의 결과).

  동적 암호화 맵 정책은 허브 및 스포크와 및 지점 간 VPN 토폴로지 모두에 적용됩니다. 동적 암호화 맵 정책을 적용하려면 토폴로지의 피어 중 하나에 동적 IP 주소를 지정하고, 이 토폴로지에서 동적 암호화 맵이 활성화되어 있는지 확인합니다. Full-mesh VPN 토폴로지에서는 정적 암호화 맵 정책만 적용할 수 있습니다.

참고 동시 IKEv2 동적 암호화 맵은 FTD(Firepower Threat Defense)의 사이트 간 VPN 및 원격 액세스 모두에 대해 동일한 인터페이스에 지원되지 않습니다.

# VPN 패킷 플로우

threat defense 디바이스에서 기본적으로 명시적 권한 없이 액세스 컨트롤을 통과하도록 허용되는 트래픽은 없습니다. VPN 터널 트래픽도 Snort를 통과할 때까지 엔드포인트에 릴레이되지 않습니다. 수신 터널 패킷은 Snort 프로세스로 전송되기 전에 암호 해독됩니다. Snort는 암호화되기 전에 발신 패킷을 처리합니다.

VPN 터널의 각 엔드포인트 노드에 대해 보호된 네트워크를 식별하는 액세스 컨트롤은 threat defense 디바이스를 통과해 엔드포인트로 이동할 수 있는 트래픽을 결정합니다. Remote Access VPN 트래픽의 경우 VPN 트래픽 흐름을 허용하도록 그룹 정책 필터 또는 액세스 컨트롤 규칙을 구성해야 합니다.

또한 터널이 다운된 상태에서는 공개 소스에 터널 트래픽을 보내지 않습니다.

# 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
- Secure Firewall 4200

IPsec 플로우 오프로드는 디바이스의 VTI 루프백 인터페이스가 활성화된 경우에도 사용됩니다.

### 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.

# VPN 라이선싱

Secure Firewall Threat Defense VPN 활성화를 위한 특정 라이선싱은 없으므로 기본적으로 제공됩니다.

management center는 Smart Licensing 서버에서 제공하는 속성을 기준으로 하여 threat defense 디바이스에서 강력한 암호화 사용을 허용할지 아니면 차단할지를 결정합니다.

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.

평가 라이선스를 사용하여 VPN 설정을 생성한 후 라이선스를 평가에서 내보내기 제어 기능이 있는 스마트 라이선스로 업그레이드한 경우 더 강력한 암호화와 VPN이 제대로 작동하는지 암호화 알고리즘을 확인하고 업데이트하십시오. DES 기반 암호화는 더 이상 지원되지 않습니다.

# 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.

## 보안 인증 요구 사항 준수

많은 VPN 설정에는 다양한 보안 인증 표준을 준수할 수 있는 옵션이 있습니다. VPN 구성을 계획하려면 인증 요구 사항 및 사용 가능한 옵션을 검토합니다.

## 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. 이 알고리즘은 대개 테스트용으로만 사용됩니다. 그러나 가상 및 Firepower 2100를 비롯한 여러 플랫폼에서 전혀 작동하지 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

사전 공유 키와 디지털 인증서는 VPN에서 사용할 수 있는 인증 방법입니다.

Site-to-Site, IKEv1 및 IKEv2 VPN 연결은 두 가지 옵션을 모두 사용할 수 있습니다.

SSL 및 IPsec IKEv2 만 사용하는 원격 액세스는 디지털 인증서 인증만 지원합니다.

사전 공유 키를 사용하면 보안 키를 두 피어 간에 공유할 수 있으며 인증 단계 수행 시 IKE에서 보안 키를 사용할 수 있습니다. 각 피어에서 동일한 공유 키를 구성해야 하며, 그렇지 않으면 IKE SA를 설정할 수 없습니다.

디지털 인증서에서는 RSA 키 쌍을 사용하여 IKE 키 관리 메시지에 서명하고 이를 암호화합니다. 인증서는 두 피어 간의 통신 부인 방지(non-repudiation)를 제공하며, 이는 실제로 통신이 이루어진 것을 증명할 수 있다는 의미입니다. 이 인증 방법을 사용하는 경우 피어가 CA(Certificate Authority)에서 디지털 인증서를 가져올 수 있는 위치에 PKI(Public Key Infrastructure)가 정의되어 있어야 합니다. CA는 인증서 요청을 관리하고 참여 네트워크 디바이스에 인증서를 발급하여 모든 참여 디바이스에 대한 중앙 집중식 키 관리를 제공합니다.

사전 공유 키는 확장되지 않으며 CA를 사용하면 IPsec 네트워크의 관리 효율성과 확장성이 향상됩니다. CA를 사용하면 모든 암호화 디바이스 간에 키를 구성할 필요가 없습니다. 대신, 참여하는 각 디바이스는 CA에 등록되고 CA의 인증서를 요청합니다. 고유한 인증서와 CA의 공개 키가 있는 각 디바이스는 지정된 CA 도메인 내의 모든 다른 디바이스를 인증할 수 있습니다.

## 사전 공유 키

사전 공유 키를 사용하면 두 피어 간에 비밀 키를 공유할 수 있습니다. IKE는 인증 단계 중에 키를 사용합니다. 각 피어에서 동일한 공유 키를 구성해야 합니다. 그렇지 않으면 IKE SA를 설정할 수 없습니다.

사전 공유 키를 구성하려면 수동 또는 자동으로 생성된 키를 사용할지 여부를 선택한 다음 IKEv1/IKEv2 옵션에서 키를 지정합니다. 그런 다음 구성이 배포되면 키가 토폴로지의 모든 디바이스에 구성됩니다.

## PKI 인프라 및 디지털 인증서

### Public Key Infrastructure

PKI는 참여 네트워크 디바이스에 대한 중앙 집중식 키 관리를 제공합니다. 일반적으로 디지털 인증서로 알려진 공개 키 인증서를 생성, 확인 및 취소하여 공개 키 암호화를 지원하는 정책, 절차 및 역할의 정의된 집합입니다.

공개 키 암호화에서 각 연결 엔드포인트는 공개 키와 개인 키로 구성된 키 쌍을 가지고 있습니다. 키 쌍은 VPN 엔드포인트가 메시지에 서명하고 암호화하는 데 사용됩니다. 키는 상호 보완적 역할을 하는데, 둘 중 하나의 키로 암호화된 것은 다른 하나의 키를 사용하여 해독할 수 있으며 연결을 통한 데이터 흐름을 보호할 수 있습니다.

서명 및 암호화에 모두 사용되는 범용 RSA, ECDSA 또는 EDDSA 키 쌍을 생성하거나, 용도별로 각각 RSA 키 쌍을 생성합니다. 서명용 키와 암호화용 키를 달리하면 키의 노출을 줄일 수 있습니다. SSL은

암호화용 키를 사용하지만 서명용 키는 사용하지 않으며 IKE는 서명용 키를 사용하지만 암호화용 키는 사용하지 않습니다. 각각에 별도의 키를 사용하면 키 노출이 최소화됩니다.

### 디지털 인증서 또는 ID 식별

VPN 연결의 인증 방법으로 디지털 인증서를 사용하면 피어가 CA(Certificate Authority)에서 디지털 인증서를 받도록 구성됩니다. CA는 인증서에 "서명"하여 그 진위를 확인함으로써 해당 디바이스 또는 사용자의 ID를 보장하는 신뢰받는 기관입니다.

CA 서버는 공개 CA 인증서 요청을 관리하고 PKI(Public Key Infrastructure)의 일부로 참여 네트워크 디바이스에 인증서를 발급합니다. 이 활동을 인증서 등록이라고 합니다. ID 인증서라고도 하는 이러한 디지털 인증서에는 다음이 포함됩니다.

- 이름, 일련 번호, 회사, 부서 또는 IP 주소와 같은 인증 소유자의 디지털 ID.
- 암호화된 데이터를 인증서 소유자와 주고받는 데 필요한 공개 키.
- CA의 보안 디지털 서명.

또한 인증서는 두 피어 간의 통신 부인 방지(non-repudiation)를 제공하며, 이는 실제로 통신이 이루어진 것을 증명한다는 의미입니다.

### 인증서 등록

PKI를 사용하면 모든 암호화 디바이스 간에 사전 공유 키를 구성할 필요가 없기 때문에 VPN의 관리성과 확장성이 개선됩니다. 대신, ID를 확인하고 디바이스의 ID 인증서를 생성하기 위해 명시적으로 신뢰할 수 있는 CA 서버로 각 참여 디바이스를 개별적으로 등록합니다. 이 작업이 완료되면 참여한 각 피어가 다른 피어에 ID 인증서를 전송하여 IDFMF 확인하고 인증서에 포함된 공개 키로 암호화된 세션을 설정합니다. threat defense 디바이스 등록에 대한 상세 정보는 인증서 등록 개체의 내용을 참조하십시오.

### 인증 기관 인증서

피어의 인증서를 확인하려면 각 참여 디바이스는 서버에서 CA의 인증서를 검색해야 합니다. CA 인증서는 다른 인증서에 서명하는 데 사용되며 자체 서명되며 루트 인증서라고도 합니다. 이 인증서에는 CA의 공개 키가 포함되어 있으며 CA의 디지털 서명과 수신된 피어 인증서의 내용을 암호 해독하고 확인하는 데 사용됩니다. CA 인증서는 다음과 같은 방법으로 얻을 수 있습니다.

- SCEP(Simple Certificate Enrollment Protocol) 또는 EST(Enrollment over Secure Transport)를 사용하여 CA 서버에서 CA 인증서 검색
- 다른 참여 디바이스에서 CA 인증서를 수동으로 복사

### 신뢰 지점

등록이 완료되면 관리형 디바이스에 신뢰 지점이 생성됩니다. 이는 CA 및 관련 인증서의 개체 표현입니다. 신뢰 지점에는 CA의 ID, CA별 파라미터, 하나의 등록된 ID 인증서와의 연결 관계가 포함되어 있습니다.

**PKCS #12** 파일

PKCS# 12 또는 PFX 파일은 서버 인증서, 중간 인증서 및 개인 키를 하나의 암호화된 파일에 보관합니다. 이 유형의 파일을 디바이스에 직접 가져와서 신뢰 지점을 생성할 수 있습니다.

해지 검사

CA는 더 이상 네트워크에 참여하지 않는 피어의 인증서를 폐기할 수도 있습니다. 폐기된 인증서는 OCSP(Online Certificate Status Protocol) 서버에서 관리하거나 LDAP 서버에 저장된 CRL(인증서 해치 목록)에 나열됩니다. 피어는 다른 피어에서 인증서를 수락하기 전에 이를 확인할 수 있습니다.

# 제거되었거나 사용되지 않는 해시 알고리즘, 암호화 알고리즘 및 **Diffie-Hellman** 모듈러스 그룹

보안 수준이 낮은 암호에 대한 지원이 제거되었습니다. VPN이 올바르게 작동하도록 threat defense 6.70을 지원되는 DH 및 암호화 알고리즘으로 업그레이드하기 전에 VPN 설정을 업데이트하는 것이 좋습니다.

threat defense 6.70에서 지원되는 것과 일치하도록 IKE 제안 및 IPSec 정책을 업데이트한 다음 설정 변경 사항을 구축합니다.

다음과 같이 안전성이 상대적으로 낮은 암호는 threat defense 6.70 이상에서 제거되었거나 더 이상 사용되지 않습니다.

- **Diffie-Hellman GROUP 5**는 IKEv1 및 IKEv2에서 더 이상 사용되지 않습니다.
- Diffie-Hellman GROUP 2 및 24가 제거되었습니다.
- 암호화 알고리즘: 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256이 제거되었습니다.

참고 **DES**는 평가 모드에서 또는 강력한 암호화를 위한 내보내기 제어 항목을 충족하지 않는 사용자를 대상으로 계속 지원됩니다.

**NULL**은 IKEv2 정책에서 제거되지만, IKEv1 및 IKEv2 IPsec 변형 집합에서 모두 지원됩니다.

# **VPN** 토폴로지 옵션

새 VPN 토폴로지를 생성할 때 고유한 이름을 부여하고 토폴로지 유형을 지정하고 IKE 버전을 선택해야 합니다. 각각 VPN 터널의 그룹을 포함하는 3가지 토폴로지 유형 중에서 선택할 수 있습니다.

- Point-to-Point 토폴로지에서는 두 엔드포인트 간에 VPN 터널을 설정합니다.
- 허브 앤 스포크 토폴로지는 허브 엔드포인트를 스포크 엔드포인트 그룹에 연결하는 VPN 터널 그룹을 설정합니다.

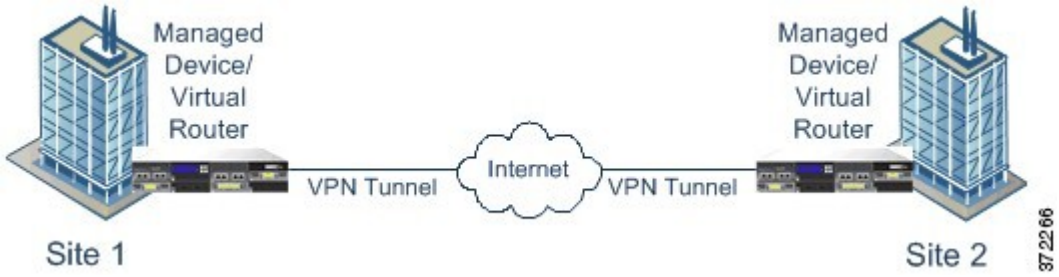
- 풀 메시 토폴로지는 일련의 엔드포인트 사이에 VPN 터널 그룹을 설정합니다.

VPN 인증을 위한 사전 공유 키를 수동 또는 자동으로 정의합니다. 기본 키는 없습니다. 자동을 선택하면 Secure Firewall Management Center에서 사전 공유 키를 생성하고 토폴로지의 모든 노드에 할당합니다.

# Point-to-Point VPN 토폴로지

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

다음 다이어그램은 일반적인 포인트 투 포인트 VPN 토폴로지를 보여줍니다.

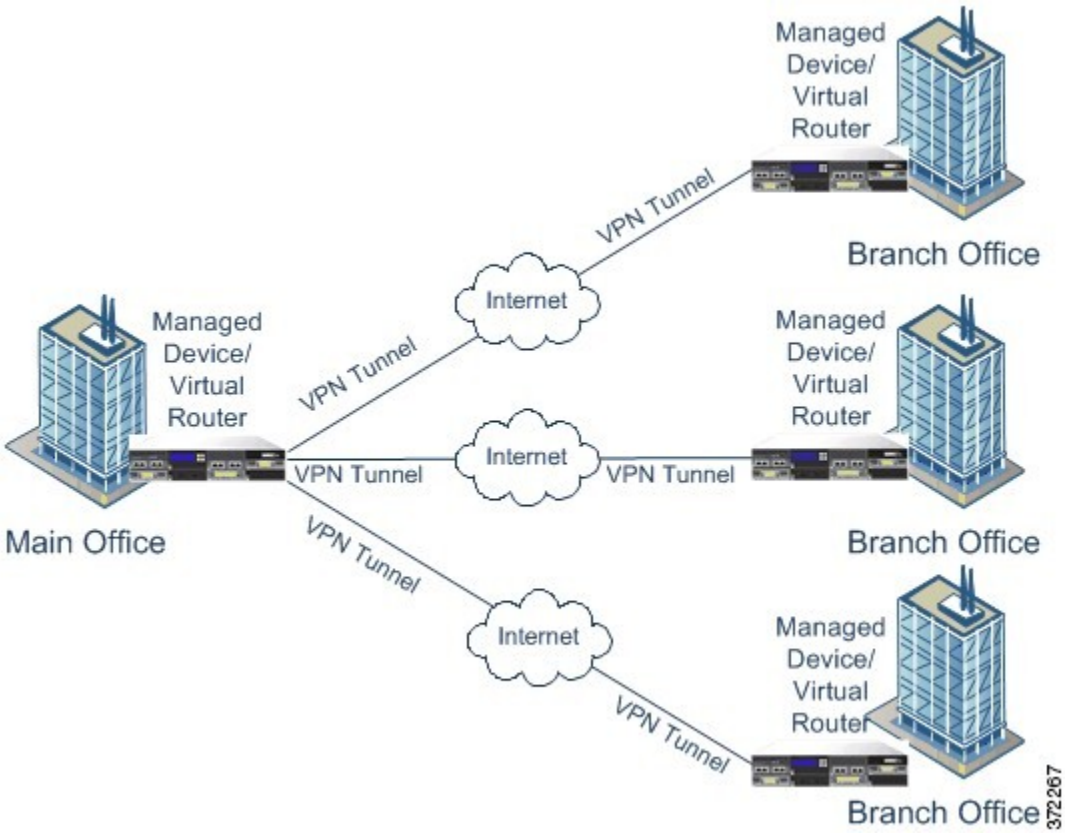



# 허브 앤 스포크 VPN 토폴로지

허브 앤 스포크 VPN 토폴로지에서 중앙 엔드포인트(허브 노드)는 여러 원격 엔드포인트(스포크 노드)와 연결됩니다. 허브 노드와 개별 스포크 엔드포인트 사이의 각 연결은 별도의 VPN 터널입니다. 스포크 노드 뒤에 있는 호스트는 허브 노드를 통해 서로 통신할 수 있습니다.

허브 앤 스포크 토폴로지는 주로 인터넷이나 기타 서드파티 네트워크를 통한 보안 연결을 사용하여 조직의 본사 및 지사 위치와 연결하는 VPN을 나타냅니다. 이러한 구축에서는 모든 직원이 조직의 네트워크에 대해 통제된 액세스 권한을 갖습니다. 일반적으로 허브 노드는 본사에 있습니다. 스포크 노드는 지사에 있으며 대부분의 트래픽을 시작합니다.

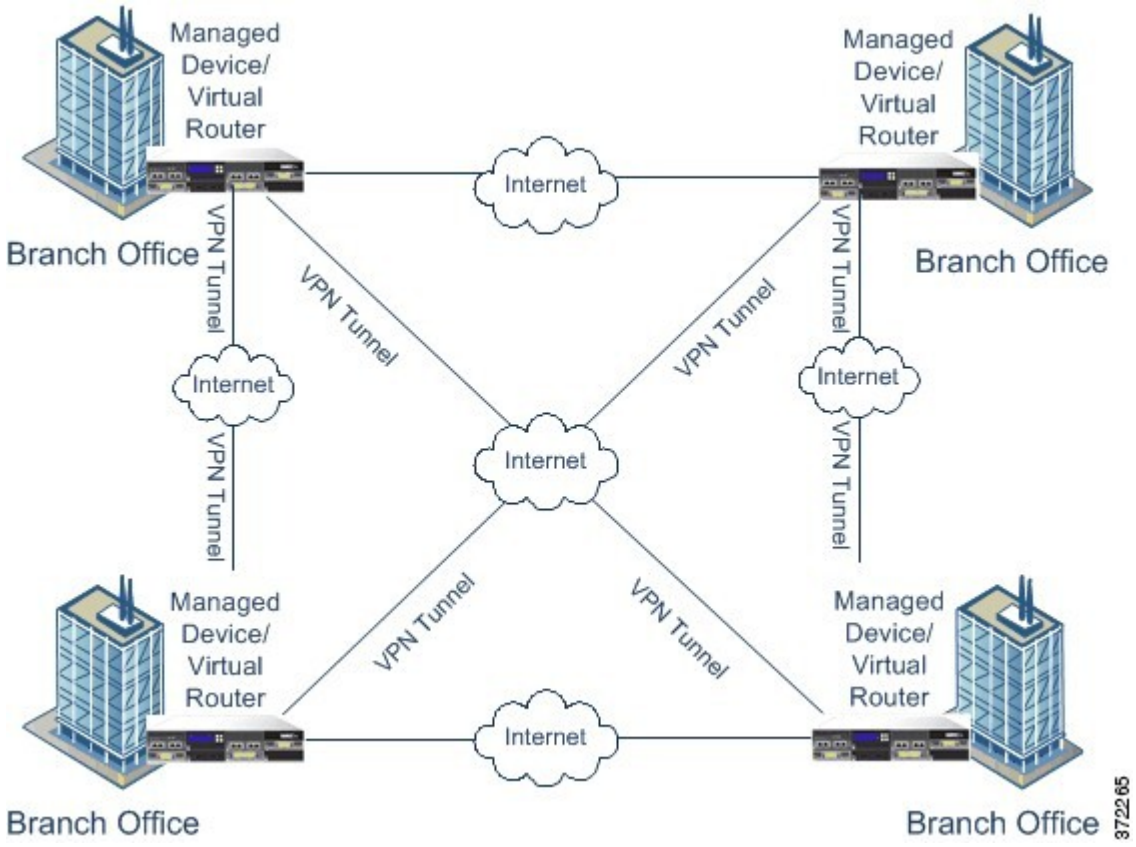
다음 다이어그램은 일반적인 허브 앤 스포크 VPN 토폴로지를 보여줍니다.




# 풀 메시 VPN 토폴로지

풀 메시 VPN 토폴로지에서는 모든 엔드포인트가 개별 VPN 터널을 통해 다른 모든 엔드포인트와 통신할 수 있습니다. 이 토폴로지에서는 한 엔드포인트에 장애가 발생할 경우에도 나머지 엔드포인트는 여전히 서로 통신할 수 있다는 점에서 이중화를 제공합니다. 이는 대개 분산된 지사의 위치를 연결하는 VPN에 사용됩니다. 이러한 구성으로 구축하는 VPN을 지원하는 관리 대상 디바이스의 수는 필요한 이중화 레벨에 따라 달라집니다.

다음 다이어그램은 일반적인 풀 메시 VPN 토폴로지를 보여줍니다.




# 암시적 토폴로지

세 가지 주요 VPN 토폴로지 외에도 이 토폴로지의 조합으로 더욱 복잡한 다른 토폴로지를 생성할 수 있습니다. 그 기능은 다음과 같습니다.

- 부분 메시 - 일부 디바이스가 풀 메시 토폴로지로 구성되고 다른 디바이스는 허브 앤 스포크 또는 일부 메시 디바이스에 대한 Point-to-Point 연결을 구성하는 네트워크입니다. 부분 메시는 전체 메시 토폴로지의 이중화 레벨을 제공하지는 않지만 구현하는 데 비용이 적게 듭니다. 부분 메시 토폴로지는 완전한 메시 백본에 연결되는 주변 장치 네트워크에 사용됩니다.
- 계층화된 허브 앤 스포크 - 디바이스가 하나 이상의 토폴로지에서 허브로 작동하고 다른 토폴로지에서 스포크로 작동할 수 있는 허브 앤 스포크 토폴로지의 네트워크입니다. 트래픽은 스포크 그룹에서 가장 즉각적인 허브까지 허용됩니다.
- 조인된 허브 앤 스포크 - Point-to-Point 터널을 형성하기 위해 연결되는 두 개의 토폴로지(허브 앤 스포크, 포인트 투 포인트 또는 풀 메시)의 조합입니다. 예를 들어 조인된 허브 앤 스포크 토폴로지는 Point-to-Point 토폴로지의 피어 디바이스로 작동하는 허브가 있는 두 개의 허브 앤 스포크 토폴로지로 구성될 수 있습니다.