사이트 대 사이트 VPN

사이트 간 VPN 정보

Secure Firewall Threat Defense Site-to-Site VPN은 다음 기능을 지원합니다.

- IPsec IKEv1 및 IKEv2 프로토콜 모두.
- 인증을 위한 인증서 및 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.
- management center 및 threat defense 모두에 대한 HA 환경.
- 터널이 다운될 때 VPN 알림.
- threat defense Unified CLI를 통해 사용 가능한 터널 통계.
- Point-to-Point 엑스트라넷 및 허브 앤 스포크 VPN에 대한 IKEv1 및 IKEv2 백업 피어 구성.
- '허브 앤 스포크' 구축에서 허브로 작동하는 엑스트라넷 디바이스.

- 'Point-to-Point' 구축에서 엑스트라넷 디바이스와 페어링된 관리 대상 엔드포인트의 동적 IP 주소.
- 엔드포인트로 작동하는 엑스트라넷 디바이스의 동적 IP 주소.
- '허브 앤 스포크' 구축에서 엑스트라넷으로 작동하는 허브.

VPN 토폴로지

새로운 사이트 간 VPN 토폴로지를 생성하려면 고유한 이름을 지정하거나 토폴로지 유형을 지정하거나 IPsec IKEv1 또는 IKEv2에 사용되는 IKE 버전 또는 둘 다를 선택해야 합니다. 또한 하여 인증 방법을 결정합니다. 구성된 후 토폴로지를 threat defense 디바이스에 구축합니다. Secure Firewall Management Center는 threat defense 디바이스에서만 Site-to-Site VPN을 구성합니다.

하나 이상의 VPN 터널을 포함하는 3가지 토폴로지 유형 중에서 선택할 수 있습니다.

- Point-to-Point 구축에서는 두 엔드포인트 간에 VPN 터널을 설정합니다.
- 허브 앤 스포크 구축은 허브 엔드포인트를 스포크 노드 그룹에 연결하는 VPN 터널 그룹을 설정합니다.
- 풀 메시 구축은 일련의 엔드포인트 사이에 VPN 터널 그룹을 설정합니다.

IPsec 및 **IKE**

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

인증

VPN 연결을 인증하려면 토폴로지의 사전 공유 키 또는 각 디바이스의 신뢰 지점을 구성합니다. 사전 공유 키를 사용하면 IKE 인증 단계에서 사용되는 보안 키를 두 피어 간에 공유할 수 있습니다. 신뢰 지점에는 CA의 ID, CA별 파라미터, 하나의 등록된 ID 인증서와의 연결 관계가 포함되어 있습니다.

엑스트라넷 디바이스

각 토폴로지 유형에는 management center에서 관리되지 않는 디바이스인 엑스트라넷 디바이스가 포함될 수 있습니다. 예를 들면 다음과 같습니다.

- Secure Firewall Management Center에서 지원하지만 조직에는 책임이 부여되지 않는 Cisco 디바이스. 회사 내의 다른 조직에서 관리하는 네트워크의 스포크 또는 서비스 제공자나 파트너의 네트워크에 대한 연결 등이 포함됩니다.
- 타사 디바이스. Secure Firewall Management Center를 사용하여 타사 디바이스에 구성을 생성하거나 구축할 수 없습니다.

타사 디바이스 또는 Secure Firewall Management Center가 관리하지 않는 Cisco 디바이스를 '엑스트라넷' 디바이스로 VPN 토폴로지에 추가합니다. 또한 각 원격 디바이스의 IP 주소를 지정합니다.

Secure Firewall Threat Defense Site-to-Site VPN 지침 및 제한 사항

- VPN 연결은 현재 도메인에 존재하지 않는 엔드포인트에 대해 엑스트라넷 피어를 사용하여 도메인 전반에서만 수행될 수 있습니다.
- VPN 토폴로지는 도메인 간에 이동할 수 없습니다.
- '범위 '옵션이 있는 네트워크 개체는 VPN에서 지원되지 않습니다.
- IKEv1은 CC/UCAPL 호환 디바이스를 지원하지 않습니다. 이러한 디바이스에는 IKEv2를 사용하는 것이 좋습니다.
- Secure Firewall Threat Defense VPN은 Firepower Management 백업을 통해서만 백업됩니다.
- Secure Firewall Threat Defense VPN은 현재 PDF 내보내기 및 정책 비교를 지원하지 않습니다.
- Secure Firewall Threat Defense VPN에는 터널별 또는 디바이스별 편집 옵션이 없으므로 전체 토폴로지만 편집할 수 있습니다.
- 암호화 ACL을 선택하면 전송 모드에서 디바이스 인터페이스 주소 확인이 수행되지 않습니다.
- 암호화 ACL 또는 보호된 네트워크를 사용하여 토폴로지의 모든 노드를 구성해야 합니다. 한 노드에서는 암호화 ACL을 사용하고 다른 노드에서는 보호된 네트워크를 사용하여 토폴로지를 구성할 수 없습니다.
- 자동 ACE 미러링 생성은 지원되지 않습니다. 피어에 대한 ACE 미러링 생성은 양측에서 모두 수동 프로세스입니다.
- 암호화 ACL을 사용하는 동안에는 VPN 토폴로지의 터널 상태 이벤트가 지원되지 않습니다. 암호화 ACL을 사용하면 허브, 스포크 및 풀 메시 토폴로지는 지원되지 않습니다. Point-to-Point VPN만 지원됩니다.
- 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.
- 터널 상태는 실시간으로 업데이트되지 않지만 management center에서 5분 간격으로 업데이트됩니다.
- "(큰 따옴표)는 사전 공유 키로 지원되지 않습니다. 사전 공유 키에서 "를 사용한다면, Secure Firewall Threat Defense 6.30으로 업그레이드한 후에 해당 문자를 변경해야 합니다.
- ECMP 영역 인터페이스는 사이트 간 VPN에서 지원됩니다.

사이트 간 **VPN** 요구 사항 및 사전 요건

모델 지원

Threat Defense

지원되는 도메인

Leaf

사용자 역할

관리자

사이트 간 VPN 관리

Site to Site VPN(사이트 간 VPN) 페이지는 사이트 간 VPN 터널의 스냅샷을 제공합니다. 터널의 상태를 보고 디바이스, 토폴로지 또는 터널 유형에서 터널 기반을 필터링할 수 있습니다. 이 페이지에는 페이지당 20개의 토폴로지가 나열되며, 페이지 간에 이동하여 더 많은 토폴로지 세부 정보를 볼 수 있습니다. 개별 VPN 토폴로지를 클릭하여 엔드포인트의 세부 정보를 확장하고 볼 수 있습니다.

시작하기 전에

사이트 간 VPN에 대한 인증서 인증의 경우 인증서에서 설명한 대로 신뢰 지점을 할당하여 디바이스를 준비해야 합니다.

프로시저

Devices(디바이스**) > VPN > Site to Site(**사이트 대 사이트**)**를 선택하여 Firepower Threat Defense Site-to-Site VPN 구성 및 구축을 관리하십시오.

이 페이지에는 사이트 간 VPN 토폴로지가 나열되고 색상 코드를 사용하는 터널의 상태가 표시됩니다:

- 활성(녹색) - 활성 IPsec 터널이 있습니다.
- 알 수 없음(주황색) – 디바이스에서 터널 설정 이벤트가 아직 수신되지 않았습니다.
- 다운(빨간색) – 활성 IPsec 터널이 없습니다.
- 구축 보류 중 – 토폴로지가 디바이스에 아직 구축되지 않았습니다.

다음 중에서 선택합니다.

- **Refresh(**새로 고침**)** - VPN의 업데이트된 상태를 확인합니다.
- **Add(**추가**)** - 새 정책 기반 또는 경로 기반 사이트 간 VPN을 생성합니다.
- **Edit(**편집**)**—기존 VPN 토폴로지의 설정을 수정합니다.

  참고 토폴로지 유형을 처음 저장한 후에는 편집할 수 없습니다. 토폴로지 유형을 변경하려면 토폴로지를 삭제하고 새 토폴로지를 생성합니다.

  사용자 두 명이 토폴로지를 동시에 편집할 수 없으나, 웹 인터페이스에서는 동시 편집이 차단되지 않습니다.

- **Delete(**삭제**)**—VPN 구축을 삭제하려면 **Delete(**삭제**)** ( )를 클릭합니다.
- 구축 - **Deploy(**구축**)** > **Deployment(**구축**)**를 선택합니다. 구성 변경 사항 구축의 내용을 참조하십시오.

  참고 일부 VPN 설정은 구축 도중에만 검증됩니다. 구축에 성공했는지 확인하십시오.

정책 기반 사이트 간 VPN 구성

프로시저

단계 **1** **Devices(**장치**)** > **VPN** > **Site To Site(**사이트 대 사이트**)**. 그런 다음 **Add VPN(VPN** 추가**)** > **Firepower Threat Defense Device** 또는 나열된 VPN Topology(VPN 토폴로지)를 수정합니다. 을(를) 선택합니다.

단계 **2** 고유한 토폴로지 이름을 입력합니다. threat defense VPN 및 토폴로지 유형을 나타내기 위해 토폴로지의 이름을 지정하는 것이 좋습니다.

단계 **3** 사이트 간 VPN을 구성하려면 **Policy Based(Crypto Map)(**정책 기반**(**암호화 맵**)**를 클릭합니다.

단계 **4** 이 VPN에 대한 **Network Topology(**네트워크 토폴로지**)**를 선택합니다.

단계 **5** IKE 협상 중에 사용할 IKE 버전을 선택합니다. **IKEv1** 또는 **IKEv2**입니다.

기본값은 IKEv2입니다. 적절한 옵션 중 하나 또는 두 가지를 선택합니다. 토폴로지의 디바이스가 IKEv2를 지원하지 않으면 IKEv1을 선택합니다.

포인트 투 포인트 엑스트라넷 VPN에 대한 백업 피어를 구성할 수도 있습니다. 자세한 내용은 Threat Defense VPN 엔드포인트 옵션, 6 페이지을 참조하십시오.

단계 **6** 필수: 토폴로지의 각 노드에 대한 **Add(**추가**)** ( )을 클릭하여 이 VPN 구축에 대한 엔드포인트를 추가합니다.

Threat Defense VPN 엔드포인트 옵션, 6 페이지의 설명에 따라 각 엔드포인트 필드를 구성합니다.

- Point-to-Point의 경우 노드 **A**와 노드 **B**를 구성합니다.
- 허브 앤 스포크의 경우 허브 노드 및 스포크 노드를 구성합니다.
- 풀 메시의 경우 여러 노드를 구성합니다.

단계 **7** (선택 사항) 설명에 따라 이 구축에 대해 기본값 이외의 IKE 옵션을 지정합니다. Threat Defense VPN IKE 옵션, 10 페이지

단계 **8** (선택 사항) 설명에 따라 이 구축에 대해 기본값 이외의 IPSec 옵션을 지정합니다. Threat Defense VPN IPsec 옵션, 12 페이지

단계 **9** (선택 사항) Threat Defense 고급 Site-to-site VPN 구축 옵션, 15 페이지의 설명에 따라 이 구축에 대해 기본값 이외의 고급 옵션을 지정합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.
엔드포인트가 구성에 추가됩니다.

다음에 수행할 작업

Deploy configuration changes(구성 변경 사항 구축)참조.

참고 일부 VPN 설정은 구축 도중에만 검증됩니다. 구축에 성공했는지 확인하십시오.

VPN 세션이 가동 중일 때도 VPN 터널이 비활성 상태라는 알림이 표시되면 VPN 문제 해결 지침에 따라 VPN이 활성 상태인지 확인합니다. 자세한 내용은 VPN 모니터링 및 문제 해결 및 VPN 문제 해결의 내용을 참조하십시오.

Threat Defense VPN 엔드포인트 옵션

탐색 경로

Devices(디바이스**) > VPN > Site To Site(**사이트 대 사이트**)**. 그런 다음 **ADD VPN(VPN** 추가**) > Firepower Threat Defense Device**, 또는 나열된 VPN Topology(VPN 토폴로지)를 수정합니다. **Endpoint(**엔드포인트**)** 탭을 엽니다.

필드

디바이스

다음과 같이 구축에 대한 엔드포인트 노드를 선택합니다.

- 이 management center에서 관리되는 threat defense 디바이스.
- 이 management center에서 관리되는 threat defense 고가용성 컨테이너.
- 이 management center에서 관리하지 않는 모든 디바이스인 엑스트라넷 디바이스(Cisco 또는 타사).

Device Name(디바이스 이름**)**
엑스트라넷 디바이스의 경우에만 이 디바이스의 이름을 제공합니다. 관리되지 않는 디바이스로 식별할 수 있도록 이름을 지정하는 것이 좋습니다.

인터페이스

매니지드 디바이스를 엔드포인트로 선택한 경우 해당 디바이스에서 인터페이스를 선택합니다.

'Point-to-Point' 구축의 경우 동적 인터페이스로 엔드포인트를 구성할 수도 있습니다. 동적 인터페이스가 있는 엔드포인트는 엑스트라넷 디바이스와 페어링될 수 있으며 매니지드 디바이스가 있는 엔드포인트와는 페어링할 수 없습니다.

Devices(디바이스**) > Device Management(**디바이스 관리**) > Add/Edit device(**디바이스 추가/편집**) > Interfaces(**인터페이스**)**에서 디바이스 인터페이스를 구성할 수 있습니다.

IP 주소

- management center에서 관리하지 않는 엑스트라넷 디바이스를 선택하는 경우 엔드포인트의 IP 주소를 지정합니다.

  엑스트라넷 디바이스에서 동적 엑스트라넷 디바이스를 허용하려면 **Static(**정적**)**을 선택하고 IP 주소를 지정하거나 **Dynamic(**동적**)**을 선택합니다.

- 매니지드 디바이스를 엔드포인트로 선택한 경우 드롭다운 목록에서 단일 IPv4 주소 또는 여러 IPv6 주소를 선택합니다. 이러한 IP 주소는 매니지드 디바이스의 이 인터페이스에 이미 할당되어 있습니다.
- 토폴로지의 모든 엔드포인트는 동일한 IP 주소 체계를 가져야 합니다. IPv4 터널은 IPv6 트래픽을 전달할 수 있으며 그 반대도 마찬가지입니다. 보호되는 네트워크는 터널링된 트래픽이 사용하는 주소 체계를 정의합니다.
- 매니지드 디바이스가 고가용성 컨테이너인 경우 인터페이스 목록에서 선택합니다.

이 **IP**는 비공개입니다

엔드포인트가 네트워크 주소 변환(NAT) 기능을 갖춘 방화벽의 뒤에 상주할 경우 확인란을 선택합니다.

참고 피어가 동일한 management center에 의해 관리되는 경우에만 이 옵션을 사용하고, 피어가 엑스트라넷 디바이스인 경우에는 이 옵션을 사용하지 마십시오.

공용 **IP** 주소

This IP is Private(이 **IP**는 비공개입니다**)** 확인란을 선택한 경우 방화벽의 공용 IP 주소를 지정합니다. 엔드포인트가 responder일 경우 이 값을 지정합니다.

연결 유형

허용되는 협상을 양방향, 응답 전용 또는 시작 전용으로 지정합니다. 연결 유형에 대해 지원되는 조합은 다음과 같습니다.

표 ***1:*** 지원되는 연결 유형 조합

Remote 노드	**Central** 노드
발신 전용	응답 전용
양방향	응답 전용
양방향	양방향

인증서 맵

사전 구성된 인증서 맵 개체를 선택하거나 **Add(**추가**)** (+)을 클릭하여 인증서 맵 개체를 추가합니다. 인증서 맵은 VPN 연결에 유효하도록 수신된 클라이언트 인증서에 필요한 정보를 정의합니다. 자세한 내용은 인증서 맵 개체를 참조하십시오.

보호되는 네트워크

⚠

주의 허브 앤 스포크 토폴로지 - 동적 암호화 맵에 대한 트래픽 삭제를 방지하려면 두 엔드포인트에 대해 보호되는 네트워크 *any*를 선택하지 않아야 합니다.

보호된 네트워크가 *any*로 구성된 경우 두 엔드포인트에서 터널에서 작동하는 암호화 ACL이 생성되지 않습니다.

이 VPN 엔드포인트로 보호되는 네트워크를 정의합니다. 이 엔드포인트로 보호되는 네트워크를 정의하는 서브넷/IP 주소 목록을 선택하여 네트워크를 선택합니다. 사용 가능한 네트워크 개체를 선택하거나 새 네트워크 개체를 추가하려면 **Add(**추가**)** (+)을 클릭합니다. 네트워크 개체 생성의 내용을 참조하십시오. ACL(Access Control Lists)은 여기에서 선택한 항목에서 생성됩니다.

- **Subnet/IP Address (Network)(**서브넷**/IP** 주소**(**네트워크**))** - VPN 엔드포인트는 동일한 IP 주소를 가질 수 없으며 VPN 엔드포인트 쌍의 보호되는 네트워크는 중복될 수 없습니다. 어떤 엔드포인트의 보안 네트워크에 IPv4 또는 IPv6 항목이 포함될 경우 나머지 엔드포인트의 보안 네트워크는 동일한 유형(즉 IPv4 또는 IPv6)의 항목을 하나 이상 가져야 합니다. 그렇지 않으면 나머지 엔드포인트의 IP 주소가 동일한 유형이고 또한 보안 네트워크의 항목과 중복되지 않아야 합니다. (IPv4에는 /32 CIDR 주소 영역을, IPv6에는 /128 CIDR 주소 영역을 사용합니다.) 두 검사 모두 실패할 경우 엔드포인트 쌍은 잘못된 것입니다.

참고 기본적으로 Secure Firewall Management Center에서 역방향 경로 삽입은 활성화되어 있습니다.

Subnet/IP Address (Network)(서브넷**/IP** 주소**(**네트워크**)**는 기본 선택으로 유지됩니다.

보호되는 네트워크를 *Any(*모두*)*로 선택하고 기본 경로 트래픽의 삭제를 확인하면 RRI(reverse route injection) 설정을 비활성화합니다. **VPN**> **Site to Site(**사이트 간**)** > edit a VPN(VPN 편집) > **IPsec** > **Enable Reverse Route Injection(RRI(reverse route injection)** 설정 활성화**)**을 선택합니다. 암호화 맵 구성의 set reverse-route(Reverse Route Injection)를 제거되고 역방향 터널 트래픽이 삭제되도록 유도하는 VPN-advertised reverse route를 제거되도록 구성 변경 사항을 구축합니다.

- **Access List (Extended)(**액세스 목록**(**확장**))** - 확장된 액세스 목록은 GRE 또는 OSPF 트래픽과 같이 이 엔드포인트에서 수락할 트래픽 유형을 제어하는 기능을 제공합니다. 트래픽은 주소 또는 포트로 제한될 수 있습니다. **Add(**추가**)** (+)을 클릭하여 ACL(Access Control List) 개체를 추가합니다.

참고 ACL은 Point-to-Point 토폴로지에서만 지원됩니다.

Advanced Settings(고급 설정**)**

동적 **RRI(Reverse Route Injection)** 활성화 - RRI(Reverse Route Injection)를 사용하면 원격 터널 엔드포인트로 보호되는 네트워크 및 호스트에 대한 라우팅 프로세스에 경로를 자동으로 삽입할 수 있습니다. 동적 RRI 경로는 IPsec SA(Security Associations)를 성공적으로 설정한 경우에만 생성됩니다.

참고
- 동적 RRI는 IKEv2에서만 지원되며 IKEv1 또는 IKEv1 + IKEv2에서는 지원되지 않습니다.
- 동적 RRI는 발신 전용 피어, 풀 메시 토폴로지 및 엑스트라 넷 피어에서 지원되지 않습니다.
- 포인트 투 포인트에서는 한 피어에서만 동적 RRI를 활성화할 수 있습니다.
- 허브와 스포크 간에는 엔드포인트 중 하나만 동적 RRI를 활성화할 수 있습니다.
- 동적 RRI는 동적 암호화 맵과 결합할 수 없습니다.

Send Local Identity to Peers(피어에 로컬 **ID** 전송**)** - 로컬 ID 정보를 피어 디바이스로 전송하려면 이 옵션을 선택합니다. 목록에서 다음 **Local Identity Configuration(**로컬 **ID** 구성**)** 중 하나를 선택하고 로컬 ID를 구성합니다.

- **IP address(IP** 주소**)** — ID에 대한 인터페이스의 IP 주소를 사용합니다.
- **Auto(**자동**)** - 인증서 기반 연결을 위해 사전 공유 키 및 인증서 DN에 IP 주소를 사용합니다.
- **Email ID(**이메일 **ID)** - ID에 사용할 이메일 ID를 지정합니다. 이메일 ID는 최대 127자입니다.
- **Hostname(**호스트 이름**)**—정규화된 호스트 이름을 사용합니다.
- **Key ID(**키 **ID)** - ID에 사용할 키 ID를 지정합니다. 키 ID는 65자 미만이어야 합니다.

로컬 ID는 모든 터널에 대한 전역 ID 대신 IKEv2 터널별로 고유한 ID를 구성하는 데 사용됩니다. 고유 ID를 사용하면 threat defense에서 NAT 뒤에 여러 IPsec 터널을 포함하여 Cisco Umbrella SIG(Secure Internet Gateway)에 연결할 수 있습니다.

Umbrella에서 고유한 터널 ID를 구성하는 방법에 대한 자세한 내용은 **Cisco Umbrella SIG** 사용 설명서를 참조하십시오.

VPN Filter(VPN 필터**)** - 목록에서 확장 액세스 목록을 선택하거나 **Add(**추가**)**를 클릭하여 사이트 간 VPN 트래픽을 필터링할 새 확장 액세스 목록 개체를 만듭니다.

VPN 필터는 추가 보안을 제공하고 확장된 액세스 목록을 사용하여 사이트 간 VPN 데이터를 필터링합니다. VPN 필터에 대해 선택된 확장 액세스 목록 개체를 사용하면 VPN 터널에 들어가기 전에 사전 암호화된 트래픽과 VPN 터널을 나가는 암호 해독된 트래픽을 필터링할 수 있습니다. **sysopt permit-vpn** 옵션이 활성화되면 VPN 터널에서 오는 트래픽에 대한 액세스 제어 정책 규칙

을 우회합니다. **sysopt permit-vpn** 옵션이 활성화된 경우 VPN 필터는 사이트 간 VPN 트래픽을 식별하고 필터링하는 데 도움이 됩니다.

참고 VPN 필터는 포인트 투 포인트 및 허브 앤 스포크 토폴로지에서만 지원됩니다. 메시 토폴로지에서는 지원되지 않습니다.

허브 앤 스포크 토폴로지의 경우 특정 터널에서 다른 VPN 필터를 활성화해야 하는 경우 스포크 엔드포인트에서 허브 VPN 필터를 재정의하도록 선택할 수 있습니다.

Override VPN Filter on the Hub(허브에서 **VPN** 필터 재정의**)** 옵션을 선택하여 스포크에서 허브 VPN 필터를 재정의합니다. **Remote VPN Filter(**원격 **VPN** 필터**)** 확장 액세스 목록 개체를 선택하거나 재정의할 액세스 목록을 생성합니다.

참고 스포크인 엑스트라넷 디바이스의 경우, **Override VPN filter on the Hub(**허브에서 **VPN** 필터 재정의**)** 옵션만 사용할 수 있습니다.

sysopt permit-VPN에 대한 자세한 내용은 Threat Defense 고급 Site-to-site VPN 터널 옵션, 17 페이지의 내용을 참조하십시오.

Threat Defense VPN IKE 옵션

이 토폴로지에 대해 선택한 IKE 버전의 경우 **IKEv1/IKEv2** 설정을 지정합니다.

참고 이 대화 상자의 설정은 전체 토폴로지, 모든 터널 및 모든 매니지드 디바이스에 적용됩니다.

탐색 경로

Devices(디바이스**) > VPN > Site To Site(**사이트 대 사이트**)**. 그런 다음 **ADD VPN(VPN** 추가**) > Firepower Threat Defense Device**, 또는 나열된 VPN Topology(VPN 토폴로지)를 수정합니다. **IKE** 탭을 엽니다.

필드

정책

사전 정의된 목록에서 필요한 IKEv1 또는 IKEv2 정책 개체를 선택하거나 사용할 새 개체를 만듭니다. 여러 IKEv1 및 IKEv2 정책을 선택할 수 있습니다.

자세한 내용은 다음 섹션을 참조하십시오. Threat Defense IKE 정책

인증 유형

사이트 간 VPN은 두 가지 인증 방법, 즉 사전 공유 키와 인증서를 지원합니다. 두 가지 방법에 대한 설명은 사용할 인증 방법 결정에서 확인할 수 있습니다.

참고 IKEv1을 지원하는 VPN 토폴로지에서는 선택한 IKEv1 정책 개체에서 지정된 **Authentication Method(**인증 방법**)**가 IKEv1 **Authentication Type(**인증 유형**)** 설정의 기본값이 됩니다. 이러한 값은 서로 일치해야 하며, 그렇지 않을 경우 컨피그레이션에 오류가 발생합니다.

- **Pre-shared Automatic Key(**사전 공유 자동 키**)**—management center는 이 VPN에 대한 사전 공유 키를 자동으로 정의합니다. **Pre-shared Key Length(**사전 공유 키 길이**)**에 키의 문자 수(1~27)를 지정합니다.

  "(큰 따옴표)는 사전 공유 키로 지원되지 않습니다. 사전 공유 키에서 "를 사용한다면, Secure Firewall Threat Defense 6.30 이상으로 업그레이드한 후에 해당 문자를 변경해야 합니다.

- **Pre-shared Manual Key(**사전 공유 수동 키**)** - 이 VPN에 대한 사전 공유 키를 수동으로 할당합니다. **Key(**키**)**를 지정하고 **Confirm Key(**확인 키**)**에 동일한 내용을 다시 입력합니다.

  IKEv2에 대해 이 옵션을 선택하면 **Enforce hex-based pre-shared key only(16**진수 기반 사전 공유 키만 적용**)** 확인란이 나타나며 원하는 경우 선택합니다. 적용하는 경우 숫자 0~9 또는 A~F를 사용하여 키의 올바른 16진수 값, 짝수 2~256자를 입력해야 합니다.

- 인증서 - VPN 연결 인증 방법으로 인증서를 사용하는 경우 피어는 인증을 위해 PKI 인프라의 CA 서버에서 디지털 인증서를 가져와 거래합니다.

  Certificate(인증서**)** 필드에서 사전 구성된 인증서 등록 개체를 선택합니다. 이 등록 개체는 매니지드 디바이스에서 같은 이름의 신뢰 지점을 생성합니다. 등록 프로세스가 끝나면 인증서 등록 개체를 디바이스에 연결하고 설치해야 하며, 설치가 끝나면 신뢰 지점이 생성됩니다.

  신뢰 지점은 CA 또는 ID 쌍을 나타낸 것입니다. 신뢰 지점에는 CA의 ID, CA별 구성 파라미터, 하나의 등록된 ID 인증서와의 연결 관계가 포함되어 있습니다.

  이 옵션을 선택하기 전에 다음 사항에 유의하십시오.

  - 토폴로지의 모든 엔드포인트에 인증서 등록 개체를 등록했는지 확인하십시오. 인증서 등록 개체에는 CSR(Certificate Signing Requests)을 생성하고 지정된 CA(Certification Authority)에서 ID 인증서를 가져오기 위해 필요한 CA 서버 정보 및 등록 매개변수가 포함되어 있습니다. 인증서 등록 개체는 PKI 인프라에 매니지드 디바이스를 등록하고, VPN 연결을 지원하는 디바이스에 트러스트 포인트(CA 개체)를 생성합니다. 인증서 등록 개체를 생성하는 방법은 인증서 등록 개체 추가을(를) 참조하고, 개체를 엔드포인트에 등록하는 방법은 다음 중 적용되는 항목을 참조하십시오.
    - 자체 서명 등록을 사용한 인증서 설치
    - EST 등록을 사용한 인증서 설치
    - SCEP 등록을 사용한 인증서 설치
    - 수동 등록을 사용한 인증서 설치
    - PKCS12 파일을 사용하여 인증서 설치

참고 사이트 간 VPN 토폴로지의 경우에는 같은 인증서 등록 개체가 토폴로지의 모든 엔드포인트에 등록되어 있는지 확인합니다. 자세한 내용은 아래 표를 참조하십시오.

- 다음 표를 참조해 다양한 시나리오에서의 등록 요구 사항을 확인하십시오. 일부 시나리오에서는 특정 디바이스에 대한 인증서 등록 개체를 재지정해야 합니다. 개체를 재정의하는 방법은 개체 재정의 관리에서 확인할 수 있습니다.

인증서 등록 유형	모든 엔드포인트에 대한 디바이스 **ID** 인증서를 동일한 **CA**에서 얻었습니다.		모든 엔드포인트에 대한 디바이스 **ID** 인증서를 다른 **CA**에서 얻었습니다.
	디바이스별 매개변수가 인증서 등록 개체에 지정되지 않았습니다.	디바이스별 매개변수가 인증서 등록 개체에 지정되었습니다.	
수동	재정의 필요 없음	재정의 필요	재정의 필요
EST	재정의 필요 없음	재정의 필요	재정의 필요
SCEP	재정의 필요 없음	재정의 필요	재정의 필요
PKCS	재정의 필요	재정의 필요	재정의 필요
자체 서명	해당 없음	해당 없음	해당 없음

- Secure Firewall Threat Defense VPN 인증서 가이드라인 및 제한 사항에 언급된 VPN 인증서 제한 사항을 확인합니다.

참고 Windows Certificate Authority(CA)를 사용한다면 기본 애플리케이션 정책 확장은 **IP** 보안 **IKE** 중급입니다. 이 기본 설정을 사용한다면, 선택한 개체의 PKI **Certificate Enrollment(PKI**인증서 등록) 대화상자에 있는 **Key(**키**)** 탭의 Advanced Settings(고급 설정) 섹션에서 **Ignore IPsec Key Usage(IPsec** 키 사용량 무시**)** 옵션을 선택해야 합니다. 그렇지 않으면 엔드포인트에서 사이트 간 VPN 연결을 완료할 수 없습니다.

Threat Defense VPN IPsec 옵션

참고 이 대화 상자의 설정은 전체 토폴로지, 모든 터널 및 모든 매니지드 디바이스에 적용됩니다.

암호화 맵 유형

암호화 맵은 IPsec 보안 연결(SA)을 설정하는 데 필요한 모든 구성 요소를 결합합니다. 두 피어에서 SA를 설정하려고 시도할 때 최소 1개 이상의 호환 가능한 암호화 맵이 있어야 합니다. IPsec 보안 협상은 암호화 맵 항목에 정의된 제안을 사용하여 해당 암호화 맵의 IPsec 규칙에 지정된 데이터 흐름을 보호합니다. 이 구축의 암호화 맵에 대해 정적 또는 동적 여부를 선택합니다.

- **Static(**정적**)** - Point-to-Point 또는 풀 메시 VPN 토폴로지에서 정적 암호화 맵을 사용합니다.
- **Dynamic(**동적**)** -동적 암호화 맵은 기본적으로 모든 파라미터가 구성되지 않은 상태의 암호화 맵 항목을 생성합니다. 누락된 파라미터는 나중에 원격 피어의 요구 사항과 일치하도록 동적으로 구성됩니다(IPsec 협상의 결과).

  동적 암호화 맵 정책은 허브 및 스포크와 및 지점 간 VPN 토폴로지 모두에 적용됩니다. 이러한 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.

IKEv2 모드

IKEv2의 경우 터널에 ESP 암호화 및 인증을 적용하려면 캡슐화 모드를 지정합니다. 이는 원래 IP 패킷의 어느 부분에 ESP가 적용되어 있는지 결정합니다.

- **Tunnel(**터널**)** 모드 - (기본값) 캡슐화 모드가 터널 모드로 설정됩니다. Tunnel(터널) 모드는 전체 원래 IP 패킷(IP 헤드 및 데이터)에 ESP 암호화 및 인증을 적용하여 최종 소스 및 대상 주소를 숨기며 새 IP 패킷에서 페이로드가 됩니다.

  터널 모드의 주요 장점은 IPsec이 보장하는 이점을 위해 최종 시스템을 수정할 필요가 없다는 점입니다. 이 모드에서는 라우터와 같은 네트워크 디바이스가 IPsec 프록시 역할을 합니다. 즉, 라우터는 호스트를 대신하여 암호화를 수행합니다. 소스 라우터는 패킷을 암호화하고 IPsec 터널을 따라 패킷을 전달합니다. 대상 라우터는 원래 IP 데이터그램을 암호 해독하고 대상 시스템으로 전달합니다. 터널 모드는 또한 트래픽 분석으로부터 보호 기능을 제공하므로 터널 모드를 통해 공격자는 터널 엔드포인트만 판단할 수 있으며 터널링된 패킷이 터널 엔드포인트와 동일하더라도 해당 소스 및 대상은 판단할 수 없습니다.

- **Transport preferred(**기본 설정 전송**)** - 피어가 지원하지 않는 경우 캡슐화 모드는 터널 모드에 대한 폴백 옵션을 사용하는 전송 모드로 설정됩니다. Transport(전송) 모드에서는 IP 페이로드만 암호화되며 원래 IP 헤더는 그대로 유지됩니다. 따라서 관리자는 VPN 인터페이스 IP 주소와 일치하는 보호되는 네트워크를 선택해야 합니다.

  이 모드는 적은 바이트만 각각의 패킷에 추가하고 공용 네트워크에서 디바이스가 패킷의 최종 소스 및 대상을 확인할 수 있다는 이점이 있습니다. 전송 모드를 사용하면 IP 헤더의 정보에 기반하여 중간 네트워크에서 특수 처리(예: QoS)를 활성화할 수 있습니다. 그러나 패킷 검사를 제한하는 Layer 4 헤더가 암호화됩니다.

- **Transport required(**전송 필요**)** - 캡슐화 모드가 전송 모드로 설정되며, 터널 모드의 폴백이 허용됩니다. 협상을 지원하지 않는 하나의 엔드포인트로 인해 여러 엔드포인트가 전송 모드를 성공적으로 협상할 수 없는 경우 VPN 연결이 수행되지 않습니다.

제안

Edit(수정**)** ( )을 클릭하여 선택한 IKEv1 또는 IKEv2 방법에 대한 제안을 지정합니다. 사용 가능한 **IKEv1 IPsec** 제안 또는 **IKEv2 IPsec** 제안 개체 중에서 선택하거나 새로 생성한 다음 선택합니다. 자세한 내용은 IKEv1 IPsec 제안 개체 설정 및 IKEv2 IPsec 제안 개체 설정 섹션을 참조하십시오.

SA(Security Association) 강점 시행 활성화

이 옵션을 활성화하면 하위 IPsec SA에서 사용하는 암호화 알고리즘이 상위 IKE SA에 비해 키의 비트 수와 관련하여 더 강점을 보이지 않습니다.

Reverse Route Injection 활성화

Reverse Route Injection(RRI)은 원격 터널 엔드포인트로 보호되는 네트워크 및 호스트에 대한 라우팅 프로세스에 정적 경로를 자동으로 삽입할 수 있도록 활성화합니다.

PFS(Perfect Forward Secrecy) 활성화

PFS(Perfect Forward Secrecy)를 사용하여 암호화된 각 교환에 대해 고유 세션 키를 생성하고 사용할지를 결정합니다. 고유 세션 키는 전체 교환이 기록되었으며 공격자가 엔드포인트 디바이스에서 사용하는 사전 공유 키 또는 개인 키를 확보했더라도 후속 암호 해독에서 교환을 보호합니다. 이 옵션을 선택하는 경우 모듈러스 그룹 목록에서 PFS 세션 키를 생성할 때 사용할 Diffie-Hellman 키 파생 알고리즘도 선택합니다.

모듈러스 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 자세한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정를 참조하십시오.

라이프타임

만료되기 전에 보안 연결이 있는 시간(초)입니다. 기본값은 28,800초입니다.

수명 크기

만료되기 전에 지정된 보안 연결을 사용하여 IPsec 피어 간에 전달할 수 있는 트래픽 볼륨(KB)입니다. 기본값은 4,608,000킬로바이트입니다. 무한 데이터는 허용되지 않습니다.

ESPv3 설정

수신 **ICMP** 오류 메시지 확인

IPsec 터널을 통해 수신되고 비공개 네트워크의 내부 호스트로 전달되는 이러한 ICMP 오류 메시지를 검증할지 여부를 선택합니다.

'Do Not Fragment(조각화 금지**)'** 정책 활성화

IPsec 하위 시스템에서 IP 헤더에 DF(Do Not Fragment) 비트가 설정된 대용량 패킷을 처리하는 방법을 정의합니다.

정책

- Copy DF bit(DF 비트 복사) - DF 비트를 유지합니다.
- Clear DF bit(DF 비트 지우기) - DF 비트를 무시합니다.
- Set DF bit(DF 비트 설정) - DF 비트를 설정하고 사용합니다.

TFC(Traffic Flow Confidentiality) 패킷 활성화
터널을 우회하는 트래픽 프로파일을 마스킹하는 더미 TFC 패킷을 활성화합니다. **Burst(**버스트**)**, **Payload Size(**페이로드 크기**)** 및 **Timeout(**시간 초과**)** 파라미터를 사용하여 지정된 SA에서 무작위 간격으로 임의 길이의 패킷을 생성할 수 있습니다.

참고 사용자가 IPsec 보안 연계(SA)에서 임의의 길이 및 간격으로 더미 TFC(Traffic Flow Confidentiality: 트래픽 흐름 기밀성)를 활성화할 수 있습니다. TFC를 활성화하기 전에 IKEv2 IPsec 제안서가 있어야 합니다.

TFC 패킷을 활성화하면 VPN 터널이 유휴 상태가 되지 않습니다. 따라서 TFC 패킷을 활성화하면 그룹 정책에 구성된 VPN 유휴 시간 제한이 예상대로 작동하지 않습니다.

Threat Defense 고급 Site-to-site VPN 구축 옵션

다음 섹션에서는 사이트 간 VPN 구축에서 지정할 수 있는 고급 옵션에 대해 설명합니다. 이 설정은 전체 토폴로지, 모든 터널 및 모든 매니지드 디바이스에 적용됩니다.

Threat Defense VPN 고급 IKE 옵션

Advanced(고급**) > IKE > ISAKAMP** 설정

IKE Keepalive

IKE Keepalive를 활성화 또는 비활성화합니다. 장치가 Keepalive 모니터링 자체를 시작하지 않도록 이 옵션을 EnableInfinite로 설정할 수 있습니다.

임계값
IKE keep alive 신뢰 구간을 지정합니다. 이 간격은 keepalive 모니터링을 시작하기 전에 피어가 유휴 상태에 있도록 허용하는 시간(초)입니다. 기본값 및 최소 간격은 10초이고, 최대 간격은 3600초입니다.

다시 시도 간격
IKE keep alive 재시도 간에 대기할 시간(초)을 지정합니다. 기본값은 2초, 최대값은 10초입니다.

Identity Sent to Peer(피어로 전송되는 **ID)**
IKE 협상 중에 피어가 자신을 식별하는 데 사용할 ID를 선택합니다.

- **autoOrDN**(기본값) — 연결 유형에 따라 IKE 협상을 결정합니다. 예: 사전 공유 키의 IP 주소 또는 인증서 인증의 Cert DN(지원하지 않음)
- **ipAddress** - ISAKMP ID 정보를 교환하는 호스트의 IP 주소를 사용합니다.
- **hostname**—ISAKMP ID 정보를 교환하는 호스트의 정규화된 도메인 이름을 사용합니다. 이 이름은 호스트 이름 및 도메인 이름으로 구성됩니다.

참고 모든 VPN 연결에 대한 이 옵션을 활성화하거나 비활성화합니다.

적극적인 모드 활성화
IP 주소를 알 수 없고 DNS 확인을 디바이스에서 사용할 수 없는 경우, 키 정보 교환을 위해 이 협상 방법을 선택합니다. 협상은 호스트 이름 및 도메인 이름을 기반으로 합니다.

Enable Notification on Tunnel Disconnect(터널 연결 해제 알림 활성화**)**
SA에서 수신한 인바운드 패킷이 해당 SA의 트래픽 선택기와 일치하지 않는 경우, 관리자가IKE 알림 피어 전송을 활성화 또는 비활성화할 수 있습니다. 이 알림은 기본적으로 비활성화되어 있습니다.

Advanced(고급**) > IKE > IVEv2 Security Association (SA) Settings (IVEv2** 보안 연결**(SA)** 설정**)**

IKE v2에서는 열려 있는 SA 수를 제한하는 세션 제어를 추가로 사용할 수 있습니다. 기본적으로 열려 있는 SA 수에는 제한이 없습니다.

쿠키 챌린지
SA에 대한 응답으로 쿠키 챌린지를 피어 디바이스로 전송할지 여부에 따라 Dos(서비스 거부)공격을 차단할 수 있는 패킷이 시작됩니다. 기본적으로 사용 가능한 SA의 50%가 협상중인 경우 쿠키 챌린지를 사용합니다. 다음 옵션 중 하나를 선택합니다.

- 맞춤형
- Never(기본값)
- Always

수신 쿠키 챌린지 임계값
총 협상 허용 SA의 비율 이렇게 하면 이후의 모든 SA 협상에 대해 쿠키 챌린지가 트리거됩니다. 범위는 0~100%이고,

협상이 허용된 **SA** 수
언제든지 협상에 참여할 수 있는 최대 SA 수를 제한합니다. Cookie Challenge(쿠키 챌린지)와 함께 사용하는 경우 효과적인 교차 확인을 위해 쿠키 챌린지 임계값을 이 한도보다 낮은 값으로 구성합니다.

허용된 최대 **SA** 수
허용되는 IKEv2 연결 수를 제한합니다. 기본값은 무제한입니다.

Enable Notification on Tunnel Disconnect(터널 연결 해제 알림 활성화**)**
SA에서 수신한 인바운드 패킷이 해당 SA의 트래픽 선택기와 일치하지 않는 경우, 관리자가IKE 알림 피어 전송을 활성화 또는 비활성화할 수 있습니다. 이 알림의 전송은 기본적으로 비활성화되어 있습니다.

Threat Defense VPN 고급 IPsec 옵션

Advanced(고급) > IPsec > IPsec Settings(IPsec 설정)

Enable Fragmentation Before Encryption(암호화 이전 단편화 활성화)
이 옵션을 사용하면 트래픽이 IP 단편화를 지원하지 않는 NAT 디바이스를 통과할 수 있습니다. IP 단편화를 지원하는 NAT 디바이스의 작동을 방해하지 않습니다.

Path Maximum Transmission Unit Aging(경로 최대 전송 단위 에이징)
SA(Security Association)의 PMTU(Path Maximum Transmission Unit) 재설정 간격인 PMTU Aging 활성화를 선택합니다.

Value Reset Interval(값 재설정 간격)
SA의 PMTU 값이 원래 값으로 재설정되는 시간(분)을 입력합니다. 유효 범위는 10~30분이며, 기본값은 무제한입니다.

Threat Defense 고급 Site-to-site VPN 터널 옵션

탐색 경로

Devices(디바이스) > VPN > Site To Site(사이트 대 사이트), 그런 다음 **Add VPN(VPN 추가) > Firepower Threat Defense Device** 또는 나열된 VPN Topology를 수정합니다. **Advanced(고급)** 탭을 열고 탐색창에서 **Tunnel(터널)**을 선택합니다.

터널 옵션

허브 앤 스포크, 풀 메시 토폴로지만 사용할 수 있습니다. 이 섹션은 Point-to-Point 구성에 대해서는 나타나지 않습니다.

- **Enable Spoke to Spoke Connectivity through Hub(허브를 통한 스포크 투 스포크 연결 활성화)** - 기본적으로 비활성화되어 있습니다. 이 필드를 선택하면 스포크 양쪽 끝에 있는 디바이스가 허브 노드를 통해 다른 디바이스로 연결을 확장할 수 있습니다.

NAT 설정

- **Keepalive Messages Traversal(Keepalive 메시지 순회)** - NAT keepalive 메시지 순회 활성화 여부를 선택합니다. NAT 순회 킵얼라이브는 VPN 연결 허브 및 스포크 사이에 위치한 디바이스(중간 디바이스)가 있는 경우 킵얼라이브 메시지 전송에 사용되며, 해당 디바이스는 IPsec flow에서 NAT를 수행합니다.

  이 옵션을 선택하는 경우, 스포크와 중간 디바이스 간에 전송된 keepalive 신호 간격을 초 단위로 구성하고 해당 세션이 활성임을 표시합니다. 이 값의 범위는 5~3600초입니다. 기본값은 20초입니다.

VPN 트래픽에 대한 액세스 제어

- **Bypass Access Control policy for decrypted traffic(암호 해독된 트래픽에 대해 액세스 제어 정책 우회)(sysopt permit-vpn)**: 기본적으로 threat defense은 암호 해독된 트래픽에 액세스 제어 정책

검사를 적용합니다. ACL 검사를 우회하려면 이 옵션을 활성화합니다. threat defense는 여전히 AAA 서버에서 다운로드한 VPN 필터 ACL 및 권한 부여 ACL을 VPN 트래픽에 적용합니다.

모든 VPN 연결에 대한 옵션을 활성화하거나 비활성화합니다. 이 옵션을 비활성화하는 경우, 액세스 제어 정책 또는 사전 필터 정책에서 트래픽을 허용해야 합니다.

인증서 맵 설정

- **Use the certificate map configured in the Endpoints to determine the tunnel(**엔드포인트에서 구성된 인증서 맵을 사용하여 터널 결정**)** - 이 옵션을 활성화(선택)하면 수신한 인증서의 내용을 엔드포인트 노드에 구성된 인증서 맵 개체와 연결하여 터널을 결정합니다.
- **Use the certificate OU field to determine the tunnel(**인증서 **OU** 필드를 사용하여 터널 결정**)** - 구성된 매핑(위의 옵션)을 기반으로 노드가 결정되지 않으면 수신된 인증서의 주체 DN(고유 이름)에 OU(조직 구성 단위) 값을 사용하여 터널을 결정합니다.
- **Use the IKE identity to determine the tunnel(IKE ID**를 사용하여 터널 결정**)** - 노드가 OU와 일치하는 규칙 또는 OU에서 가져온 옵션(위의 옵션)을 기반으로 결정되지 않으면 인증서 기반 IKE 세션이 phase1 IKE ID의 내용을 기반으로 터널에 매핑됩니다.
- **Use the peer IP address to determine the tunnel(**피어 **IP** 주소를 사용하여 터널 결정**)** - 터널이 OU 또는 IKE ID 방법과 일치하는 규칙이나 OU 또는 IKE ID 방법에서 가져온 옵션(위의 옵션)을 기반으로 결정되지 않으면 설정된 피어 IP 주소를 사용합니다.

Virtual Tunnel Interface 정보

Management Center는 VTI(Virtual Tunnel Interface)라는 라우팅 가능한 논리적 인터페이스를 지원합니다. VTI에서는 IPsec 세션을 물리적 인터페이스에 정적으로 매핑할 필요가 없습니다. IPsec 터널 엔드포인트는 가상 인터페이스와 연결 됩니다. 이러한 인터페이스를 다른 인터페이스처럼 사용하고 정적 및 동적 라우팅 정책을 적용할 수 있습니다. VTI를 사용할 때는 정적 크립토 맵 액세스 목록을 구성하고 인터페이스에 매핑할 필요가 없습니다. 더 이상 모든 원격 서브넷을 추적하고 암호화 맵 액세스 목록에 포함하지 않아도 됩니다.

정책 기반 VPN 대신 VTI를 사용하여 피어 간에 VPN 터널을 생성할 수 있습니다. VTI는 각 터널 끝에 IPsec 프로파일이 연결된 라우팅 기반 VPN을 지원합니다. VTI는 정적 또는 동적 경로를 사용합니다. 디바이스는 터널 인터페이스에서 들어오고 나가는 트래픽을 암호화하거나 암호 해독하고 라우팅 테이블에 따라 전달합니다. 구축이 더 간편해지고, 동적 라우팅 프로토콜과 라우팅 기반 VPN을 지원하는 VTI가 있어 가상 프라이빗 클라우드의 많은 요구 사항도 충족합니다. Management Center를 사용하면 암호화 맵 기반 VPN 설정에서 VTI 기반 VPN으로 쉽게 마이그레이션할 수 있습니다.

management center, threat defense, 디바이스 REST AP 및 device managerI에서 정적 VTI를 구성하여 경로 기반 VPN을 구성할 수 있습니다. management center는 VTI 또는 경로 기반 VPN을 설정하는 데 기본값을 사용하는 사이트 간 VPN 마법사를 지원합니다. 트래픽이 고정 경로 또는 BGP,를 사용하여 암호화됩니다.

라우팅된 보안 영역을 생성하고 여기에 VTI 인터페이스를 추가하며 VTI 터널을 통해 해독된 트래픽 제어를 위한 액세스 제어 규칙을 정의할 수 있습니다.

VTI 기반 VPN은 다음 간에 생성할 수 있습니다.

- threat defense 디바이스 2개.
- threat defense 및 퍼블릭 클라우드.
- threat defense 및 서비스 제공자 리던던시가 있는 또 다른 threat defense
- threat defense 및 VTI 인터페이스가 있는 기타 디바이스.

자세한 내용은 정적 VTI, 19 페이지 의 내용을 참조하십시오.

위협 방어 기능 기록

정적 VTI

두 사이트 간에 터널이 상시 연결 상태인 사이트 간 연결에 정적 VTI 구성을 사용할 수 있습니다. 정적 VTI 인터페이스의 경우 물리적 인터페이스를 터널 소스로 정의해야 합니다. 디바이스당 최대 1024개의 VTI를 연결할 수 있습니다. 관리 센터에서 고정 VTI 인터페이스를 생성하려면 VTI 인터페이스 추가, 21 페이지의 내용을 참조하십시오.

Virtual Tunnel Interface에 대한 지침 및 제한 사항

IPv6 지원

- VTI는 IPv6를 지원합니다.
- 터널 소스 인터페이스에 IPv6 주소를 사용하고 터널 엔드포인트와 동일한 주소를 사용할 수 있습니다.
- management center는 공용 IP 버전을 통해 다음과 같은 VTI IP(또는 내부 네트워크 IP 버전) 조합을 지원합니다:
  - IPv6를 통한 IPv6
  - IPv6를 통한 IPv4
  - IPv4를 통한 IPv4
  - IPv4를 통한 IPv6
- VTI는 정적 및 동적 IPv6 주소를 터널 소스 및 대상으로 지원합니다.
- 터널 소스 인터페이스에는 IPv6 주소가 있을 수 있으며 터널 엔드포인트 주소를 지정할 수 있습니다. 주소를 지정하지 않으면 기본적으로 threat defense은 목록의 첫 번째 IPv6 글로벌 주소를 터널 엔드포인트로 사용합니다.

BGP IPv6 지원

VTI는 IPv6 BGP를 지원합니다.

다중 인스턴스 및 클러스터링

- VTI는 다중 인스턴스에서 지원됩니다.
- VTI에서는 클러스터링이 지원되지 않습니다.

방화벽 모드

VTI는 라우팅 모드에서만 지원됩니다.

정적 VTI에 대한 제한 사항

- 20개의 고유한 IPSec 프로파일만 지원됩니다.
- 동적 VTI, OSPF 및 QoS는 지원되지 않습니다.
- 정책 기반 라우팅에서는 VTI를 이그레스 인터페이스로만 구성할 수 있습니다.

정적 VTI에 대한 일반 구성 지침

- VTI는 IPsec 모드에서만 구성할 수 있습니다.
- 터널 인터페이스를 사용하여 트래픽에 대한 BGP 또는 정적 경로를 사용할 수 있습니다.
- 디바이스에서 최대 1024개의 정적 VTI를 설정할 수 있습니다. VTI 수를 계산할 때 다음 사항을 고려하십시오.
  - 디바이스에 설정할 수 있는 총 VTI 수를 확인하려면 nameif 하위 인터페이스를 포함합니다.
  - 포트 채널의 멤버 인터페이스에서는 nameif를 설정할 수 없습니다. 따라서 터널 수는 멤버 인터페이스가 아닌 실제 기본 포트 채널 인터페이스의 수만으로 감소합니다.
  - 플랫폼의 VTI 수는 해당 플랫폼에서 설정 가능한 VLAN 수로 제한됩니다. 예를 들어, Firepower 1120은 512개의 VLAN을 지원하며, 터널 수는 설정된 물리적 인터페이스 수에서 512를 뺀 값입니다.
- 고가용성 설정의 디바이스에서 400개 이상의 VTI를 구성하는 경우 threat defense-HA의 유닛 보류 시간으로 45초를 구성해야 합니다.
- 기본 물리적 인터페이스에 따라 VTI에 대한 MTU가 자동으로 설정됩니다.
- 정적 VTI는 IKE 버전 v1, v2를 지원하고 IPsec을 사용하여 터널의 소스와 대상 간에 데이터를 전송 및 수신합니다.
- NAT를 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.
- 암호화 맵에 피어 주소가 구성되고 VTI에 대한 터널 대상이 서로 다른 경우 VTI 및 암호화 맵 구성은 동일한 물리적 인터페이스에서 공존할 수 있습니다.
- 기본적으로 VTI를 통해 전송되는 모든 트래픽이 암호화됩니다.
- 액세스 규칙은 VTI를 통과하는 트래픽을 제어하기 위해 VTI 인터페이스에 적용될 수 있습니다.
- VTI 인터페이스를 ECMP 영역과 연결하고 ECMP 고정 경로를 구성하여 다음을 수행할 수 있습니다.
  - 로드 밸런싱(액티브/액티브 VTI) - 병렬 VTI 터널 중 하나를 통해 연결이 흐를 수 있습니다.
  - 원활한 연결 마이그레이션 - VTI 터널에 연결할 수 없는 경우 플로우가 동일한 영역에 구성된 다른 VTI 인터페이스로 원활하게 마이그레이션됩니다.
  - 비대칭 라우팅 - 하나의 VTI 인터페이스를 통해 트래픽 흐름을 전달하고 다른 VTI 인터페이스를 통해 역방향 트래픽 흐름을 구성합니다.

ECMP 구성에 대한 자세한 내용은 동일 비용 정적 경로 구성의 내용을 참조하십시오.

백업 **VTI** 지침 및 제한 사항

- 터널 페일오버 전반의 플로우 복원력은 지원되지 않습니다. 예를 들어, 터널 페일오버 후 평문 TCP 연결이 손실되므로 페일오버 중에 발생한 FTP 전송을 다시 시작해야 합니다.
- 인증서 인증은 백업 VTI에서 지원되지 않습니다.

관련 항목

루프백 인터페이스에 대한 지침 및 제한 사항
라우트 기반 사이트 간 VPN 생성, 24 페이지

VTI 인터페이스 추가

경로 기반 사이트 간 VPN을 설정하려면 VTI 터널의 두 노드에 있는 디바이스에서 VTI 인터페이스를 생성해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**) > Device Management(**디바이스 관리**)**를 선택합니다.
단계 **2** VTI 인터페이스를 생성하려는 디바이스 옆의 **Edit(**편집**)** 아이콘을 클릭합니다.
단계 **3** **Add Interfaces(**인터페이스 추가**) > Virtual Tunnel Interface(**가상 터널 인터페이스**)**를 선택합니다.
단계 **4** 인터페이스 이름 및 설명을 입력합니다. 기본적으로 인터페이스는 활성화되어 있습니다.

28자 이하의 이름을 지정해야 합니다.

단계 **5** (선택사항) **Security Zone(**보안 영역**)** 드롭다운 목록에서 보안 영역을 선택하여 정적 VTI 인터페이스를 해당 영역에 추가합니다.

보안 영역을 기준으로 트래픽 검사를 수행하려는 경우, 보안 영역에 VTI 인터페이스를 추가하고 액세스 제어(AC) 규칙을 설정할 수 있습니다. 터널을 통한 VPN 트래픽을 허용하려면 이 보안 영역이 있는 AC 규칙을 소스 영역으로 추가해야 합니다.

단계 **6** **Priority(**우선순위**)** 필드에 여러 VTI 간에 트래픽을 로드 밸런싱할 우선순위를 입력합니다.

범위는 0~65535입니다. 가장 낮은 숫자가 가장 높은 우선 순위를 가집니다. 이 옵션은 동적 VTI에 적용되지 않습니다.

단계 **7** 정적 VTI의 경우 **Tunnel ID(**터널 **ID)** 필드에 0 - 10413 범위의 고유한 터널 ID를 입력합니다.

단계 **8** **Tunnel Source(**터널 소스**)** 드롭다운 목록에서 터널 소스 인터페이스를 선택합니다.

VPN 터널은 물리적 인터페이스인 이 인터페이스에서 종료됩니다. 드롭다운 목록에서 인터페이스의 IP 주소를 선택합니다. IPsec 터널 모드와 상관없이 IP 주소를 선택할 수 있습니다. IPv6 주소가 여러 개인 경우, 터널 엔드포인트로 사용할 주소를 선택합니다.

단계 **9** **IPSec Tunnel Mode(IPSec** 터널 모드**)**에서 **IPv4** 또는 **IPv6** 라디오 버튼을 클릭하여 IPsec 터널에 대한 트래픽 유형을 지정합니다.

단계 **10** **IP Address(IP** 주소**)** 필드에 터널 엔트포인트에 사용할 IP 주소와 서브넷을 입력합니다. 경로 기반 VPN의 두 엔드포인트 모두에 대한 VTI IP 주소는 동일한 서브넷에 있어야 합니다.

참고 threat defense 예약된 범위(169.254.1.x/24)를 제외한 169.254.x.x/16 범위의 IP를 사용하는 것이 좋습니다. 또한 VTI 터널의 양 끝에 두 개의 주소만 최적으로 사용하려면 /30을 넷마스크로 사용하는 것이 좋습니다. 예: 169.254.100.1/30

단계 **11** **OK(**확인**)**를 클릭합니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

백업 **VTI** 터널을 통해 트래픽을 라우팅하는 방법

Secure Firewall Threat Defense은 경로 기반(VTI) VPN에 대한 백업 터널의 구성을 지원합니다. 기본 VTI가 트래픽을 라우팅할 수 없는 경우 VPN의 트래픽은 백업 VTI를 통해 터널링됩니다.

다음 시나리오에서 백업 VTI 터널을 구축할 수 있습니다.

- 두 피어 모두 서비스 제공자 이중화 백업을 보유하고 있습니다.

  이 경우에는 피어의 두 VTI에 대한 터널 소스 역할을 하는 두 개의 물리적 인터페이스가 있습니다.

- 피어 중 하나만 서비스 제공자 이중화 백업을 가지고 있습니다.

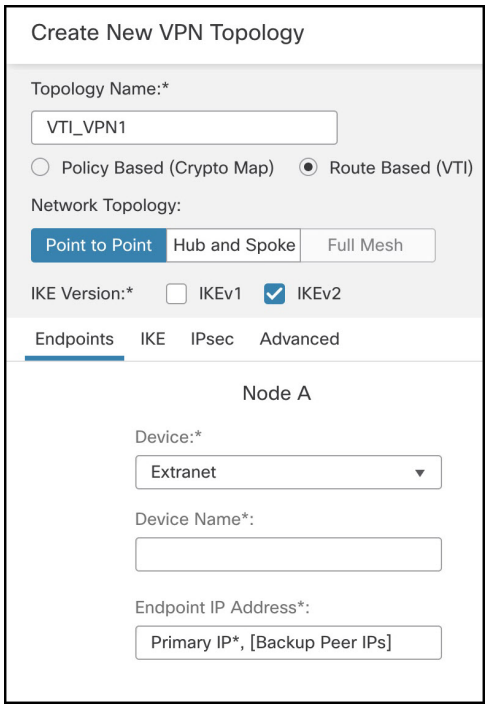
이 경우에는 피어의 한쪽에만 인터페이스 백업이 있고 다른쪽에는 터널 소스 인터페이스가 하나뿐입니다.

단계	수행해야 할 작업	추가 정보
1	지침 및 제한 사항을 검토합니다.	Virtual Tunnel Interface에 대한 지침 및 제한 사항, 19 페이지
2	VTI 인터페이스를 생성합니다.	VTI 인터페이스 추가, 21 페이지
3	**Create New VPN Topology(**새 **VPN** 토폴로지 생성**)** 마법사의 **Add Endpoint(**엔드포인트 추가**)** 대화 상자에서 **Add Backup VTI(**백업 **VTI** 추가**)**를 클릭하여 각 피어에 대한 백업 인터페이스를 구성합니다.	• 포인트 투 포인트 토폴로지에 대한 엔드포인트 구성, 25 페이지 • 허브 앤 스포크 토폴로지에 대한 엔드포인트 구성, 28 페이지
4	라우팅 정책을 구성합니다.	• **Devices(**디바이스**) > Device Management(**디바이스 관리**)**를 선택하고 위협 방어 디바이스를 편집합니다. • **Routing(**라우팅**)**을 클릭합니다.
5	액세스 제어 정책을 구성합니다.	• **Policies(**정책**) > Access Control(**액세스 제어**)**을 선택합니다.

백업 **VTI** 터널 구성 지침

- 엑스트라넷 피어의 경우 백업 인터페이스의 터널 소스 IP 주소를 지정하고 관리되는 피어에서 터널 대상 IP를 구성할 수 있습니다.

  Create New VPN Topology(새 **VPN** 토폴로지 생성**)** 마법사의 **Endpoint IP Address(**엔드포인트 **IP** 주소**)** 필드에서 백업 피어 IP 주소를 지정할 수 있습니다.



- 백업 인터페이스를 구성한 후 라우팅 트래픽에 대한 라우팅 정책 및 액세스 제어 정책을 구성합니다.

  기본 및 백업 VTI는 항상 사용 가능하지만 트래픽은 라우팅 정책에 구성된 터널을 통해서만 흐릅니다. 자세한 내용은 VTI에 대한 추가 구성, 30 페이지를 참조하십시오.

라우트 기반 사이트 간 VPN 생성

포인트 투 포인트 토폴로지 네트워크의 경우 두 노드 간에 경로 기반 사이트 간 VPN을 구성하거나 허브 및 스포크 토폴로지의 경우 허브와 스포크 간에 경로 기반 VPN을 구성할 수 있습니다. 포인트 투 포인트 토폴로지의 경우 VTI 기반 VPN을 구성하려면 터널의 두 노드 모두에 가상 터널 인터페이스가 필요합니다. 허브 및 스포크 토폴로지의 경우 정적 또는 VTI를 사용하여 관리되는 스포크에서 가상 터널 인터페이스를 구성해야 합니다.

엑스트라넷 디바이스를 허브로 구성하고 매니지드 디바이스를 스포크로 구성할 수 있습니다. 여러 허브 및 스포크를 구성할 수 있으며, 백업 허브 및 스포크도 구성할 수 있습니다.

- 엑스트라넷 허브 및 스포크의 경우 여러 IP를 백업으로 구성할 수 있습니다.
- 매니지드 스포크의 경우 기본 VTI 인터페이스와 함께 백업 정적 VTI 인터페이스를 구성할 수 있습니다.

VTI에 대한 자세한 내용은 Virtual Tunnel Interface 정보, 18 페이지의 내용을 참조하십시오.

프로시저

단계 1 **Devices(**디바이스**) > Site To Site(**사이트 간**)**를 선택합니다.

단계 2 **Add VPN(VPN** 추가**)** 드롭다운 메뉴에서 **Firepower Threat Defense Device(Firepower Threat Defense** 디바이스**)**를 선택합니다.

단계 3 **Add(**추가**)**를 선택합니다.

단계 4 **Topology Name(**토폴로지 이름**)** 필드에 VPN 토폴로지의 이름을 입력합니다.

단계 5 **Route Based (VTI)(**경로 기반**(VTI))**를 선택하고 다음 중 하나를 수행합니다.

- 네트워크 토폴로지로 **Point to Point(**포인트 투 포인트**)**를 선택합니다. 경로 기반 **Point-to-Point** 토폴로지에 대한 엔드포인트를 구성하려면 포인트 투 포인트 토폴로지에 대한 엔드포인트 구성, 25 페이지 섹션을 참조하십시오.
- 네트워크 토폴로지로 **Hub and Spoke(**허브 앤 스포크**)**를 선택합니다. 경로 기반 **Hub and Spoke(**허브 앤 스포크**)** 토폴로지에 대한 엔드포인트를 구성하려면 허브 앤 스포크 토폴로지에 대한 엔드포인트 구성, 28 페이지 섹션을 참조하십시오.

단계 6 (선택 사항) Threat Defense VPN IKE 옵션, 10 페이지에 설명된 대로 구축에 대한 **IKE** 옵션을 지정합니다.

단계 7 (선택 사항) Threat Defense VPN IPsec 옵션, 12 페이지에 설명된 대로 구축에 대한 **IPsec** 옵션을 지정합니다.

단계 8 (선택 사항) Threat Defense 고급 Site-to-site VPN 구축 옵션, 15 페이지에 설명된 대로 구축에 대한 **Advanced(**고급**)** 옵션을 지정합니다.

단계 9 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

두 디바이스에서 VTI 인터페이스 및 VTI 터널을 구성한 후에는 다음을 구성해야 합니다.

- VTI 터널을 통해 디바이스 간에 VTI 트래픽을 라우팅하는 라우팅 정책입니다. 자세한 내용은 VTI에 대한 추가 구성, 30 페이지을 참고하십시오.
- 암호화된 트래픽을 허용하는 액세스 제어 규칙입니다. **Policies(**정책**) > Access Control(**액세스 제어**)**을 선택합니다.

포인트 투 포인트 토폴로지에 대한 엔드포인트 구성

Point-to-Point 토폴로지 노드에 대해 경로 기반 사이트 간 VPN에 대한 엔드포인트를 구성하려면 다음 매개변수를 구성합니다.

시작하기 전에

라우트 기반 사이트 간 VPN 생성, 24 페이지에 설명된 대로 경로 기반 VPN에서 Point-to-Point 토폴로지에 대한 기본 매개변수를 구성하고 **Endpoints(**엔드포인트**)**탭을 클릭합니다.

프로시저

단계 **1** 노드 **A**의 **Device(**디바이스**)** 드롭다운 메뉴에서 등록된 디바이스(threat defense) 또는 엑스트라넷의 이름을 VTI 터널의 첫 번째 엔드포인트로 선택합니다.

엑스트라넷 피어의 경우 다음 매개변수를 지정합니다.

1. 디바이스의 이름을 지정합니다.
2. **Endpoint IP address(**엔드포인트 **IP** 주소**)** 필드에 기본 IP 주소를 입력합니다. 백업 VTI를 구성하는 경우 쉼표를 추가하고 백업 IP 주소를 지정합니다.
3. **OK(**확인**)**를 클릭합니다.

엑스트라넷 허브에 대해 위의 매개변수를 구성한 후 **IKE** 탭에서 엑스트라넷에 대한 사전 공유 키를 지정합니다.

참고 AWS VPC에는 기본 정책으로 **AES-SHA-SHA-LATEST**가 있습니다. 원격 피어가 AWS VPC에 연결하는 경우 **Policy(**정책**)** 드롭다운 목록에서 **AES-GCM-NULL-SHA-LATEST**를 선택하여 AWS의 기본값을 변경하지 않고 VPN 연결을 설정합니다.

단계 **2** 등록된 디바이스의 경우 **Virtual Tunnel Interface(Virtual Tunnel Interface)** 드롭다운 목록에서 노드 A에 대한 VTI 인터페이스를 지정할 수 있습니다.

선택한 터널 인터페이스는 노드 A의 소스 인터페이스이며 노드 B의 터널 대상이 됩니다.

노드 A에서 새 인터페이스를 생성하려면 **+** 아이콘을 클릭하고 VTI 인터페이스 추가, 21 페이지에 설명된 대로 필드를 구성합니다.

기존 VTI의 구성을 편집하려면 **Virtual Tunnel Interface(**가상 터널 인터페이스**)** 드롭다운 필드에서 VTI를 선택하고 **Edit VTI(VTI** 편집**)**를 클릭합니다.

단계 **3** 노드 A 디바이스가 NAT 디바이스 뒤에 있는 경우 **Tunnel Source IP is Private(**터널 소스 **IP**는 전용**)** 확인란을 선택합니다. **Tunnel Source Public IP Address(**터널 소스 공용 **IP** 주소**)** 필드에 터널 소스 공용 IP 주소를 입력합니다.

단계 **4** **Send Local Identity to Peers(**피어에 로컬 **ID** 전송**)** - 로컬 ID 정보를 피어 디바이스로 전송하려면 이 옵션을 선택합니다. 목록에서 다음 **Local Identity Configuration(**로컬 **ID** 구성**)** 중 하나를 선택하고 로컬 ID를 구성합니다.

- **IP address(IP** 주소**)** — ID에 대한 인터페이스의 IP 주소를 사용합니다.
- **Auto(**자동**)** - 인증서 기반 연결을 위해 사전 공유 키 및 인증서 DN에 IP 주소를 사용합니다.
- **Email ID(**이메일 **ID)** - ID에 사용할 이메일 ID를 지정합니다. 이메일 ID는 최대 127자입니다.
- **Hostname(**호스트 이름**)**—정규화된 호스트 이름을 사용합니다.
- **Key ID(**키 **ID)** - ID에 사용할 키 ID를 지정합니다. 키 ID는 65자 미만이어야 합니다.

로컬 ID는 모든 터널에 대한 전역 ID 대신 IKEv2 터널별로 고유한 ID를 구성하는 데 사용됩니다. 고유 ID를 사용하면 threat defense에서 NAT 뒤에 여러 IPsec 터널을 포함하여 Cisco Umbrella SIG(Secure Internet Gateway)에 연결할 수 있습니다.

Umbrella에서 고유한 터널 ID를 구성하는 방법에 대한 자세한 내용은 **Cisco Umbrella SIG** 사용 설명서를 참조하십시오.

단계 **5** (선택사항) **Add Backup VTI(**백업 **VTI** 추가**)**를 클릭하여 백업 인터페이스로 추가 VTI를 지정하고 매개 변수를 구성합니다.

참고 두 토폴로지 피어 모두 백업 VTI에 대해 동일한 터널 소스가 없는지 확인합니다. 디바이스에는 터널 소스 및 터널 대상이 동일한 2개의 VTI가 있을 수 없습니다. 따라서 고유한 터널 소스 및 터널 대상 조합을 구성합니다.

가상 터널 인터페이스가 백업 VTI에 지정되어 있지만 라우팅 구성에 따라 기본 또는 백업으로 사용할 터널이 결정됩니다.

단계 **6** **Connection Type(**연결 유형**)** 드롭다운 메뉴에서 **Answer Only(**응답 전용**)** 또는 **Bidirectional(**양방향**)**을 선택합니다. IKE 프로토콜 버전을 IKEv1로 선택한 경우 노드 중 하나가 **Answer Only(**응답 전용**)**이어야 합니다.

Answer Only(응답 전용**)**: 피어 디바이스가 연결을 시작하는 경우에만 디바이스가 응답할 수 있으며 어떤 연결도 시작할 수 없습니다.

Bidirectional(양방향**)**: 디바이스가 연결을 시작하거나 연결에 응답할 수 있습니다. 이것이 기본 옵션입니다.

단계 **7** **Additional Configuration(**추가 구성**)**에서 다음을 수행합니다.

- VTI로 트래픽을 라우팅하려면 **Routing Policy(**라우팅 정책**)**를 클릭합니다. Management Center는 **Devices(**디바이스**)** > **Routing(**라우팅**)** 페이지를 표시합니다.

  VPN 트래픽에 대해 고정 또는 BGP 라우팅을 구성할 수 있습니다.

- VPN 트래픽을 허용하려면 **AC Policy(AC** 정책**)**를 클릭합니다. Management Center는 디바이스의 액세스 제어 정책 페이지를 표시합니다. 계속해서 VTI의 보안 영역을 지정하는 허용/차단 규칙을 추가합니다. 백업 VTI가 구성된 경우 기본 VTI와 동일한 보안 영역에 백업 터널을 포함해야 합니다. AC 정책 페이지에는 백업 VTI에 대한 특정 설정이 필요하지 않습니다.

단계 **8** 노드 B에 대해 위의 절차를 반복합니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- (선택 사항) Threat Defense VPN IKE 옵션, 10 페이지에 설명된 대로 구축에 대한 **IKE** 옵션을 지정합니다.
- (선택 사항) Threat Defense VPN IPsec 옵션, 12 페이지에 설명된 대로 구축에 대한 **IPsec**옵션을 지정합니다.

- (선택 사항) Threat Defense 고급 Site-to-site VPN 구축 옵션, 15 페이지에 설명된 대로 구축에 대한 **Advanced(**고급**)** 옵션을 지정합니다.
- **Save(**저장**)**를 클릭합니다.
- VTI로 트래픽을 라우팅하려면 **Devices(**디바이스**) > Device Management(**디바이스 관리**)**를 선택하고 위협 방어 디바이스를 편집한 다음 **Routing(**라우팅**)** 탭을 클릭합니다.

  정적 경로를 구성하거나 BGP를 사용하여 VPN 트래픽을 라우팅할 수 있습니다.
- VPN 트래픽을 허용하려면 **Policies(**정책**) > Access Control(**액세스 제어**)**을 선택합니다. . VTI의 보안 영역을 지정하는 규칙을 추가합니다. 백업 VTI의 경우 기본 VTI와 동일한 보안 영역에 백업 VTI를 포함해야 합니다.

허브 앤 스포크 토폴로지에 대한 엔드포인트 구성

Hub and Spoke(허브 및 스포크**)** 토폴로지 노드에 대해 경로 기반 사이트 간 VPN에 대한 엔드포인트를 구성하려면 다음 매개변수를 구성합니다.

시작하기 전에

라우트 기반 사이트 간 VPN 생성, 24 페이지에 설명된 대로 경로 기반 VPN에서 허브 및 스포크 토폴로지에 대한 기본 매개변수를 구성하고 **Endpoints(**엔드포인트**)** 탭을 클릭합니다.

프로시저

단계 **1** 허브 노드를 추가합니다.

a) **Hub Nodes(**허브 노드**)**에서 **Add (+)(**추가**)**를 클릭합니다.
b) **Device Name(**디바이스 이름**)**에 디바이스 이름을 입력합니다.
c) **Endpoint IP address(**엔드포인트 **IP** 주소**)**에 기본 IP 주소를 입력합니다. 백업 허브를 구성하는 경우 쉼표를 입력한 다음 백업 IP 주소를 지정합니다.
d) **IKE** 탭을 클릭하고 엑스트라넷에 제공된 사전 공유 키를 지정합니다.
e) **OK(**확인**)**를 클릭합니다.

스포크 노드를 추가합니다.

- 엑스트라넷 스포크의 경우 구성 매개 변수는 허브와 유사합니다.
- 관리되는 스포크 노드의 경우 포인트 투 포인트 노드와 유사한 매개 변수를 구성합니다.

a) **Spoke Nodes(**스포크 노드**)**에서 **Add (+)(**추가**)**를 클릭합니다.
b) **Device(**디바이스**)** 드롭다운 메뉴에서 등록된 디바이스의 이름을 선택합니다(threat defense).
c) 인터페이스 설정을 지정합니다.

- **Static Virtual Tunnel Interface(**고정 가상 터널 인터페이스**)** 드롭다운 메뉴에서 VTI 엔드포인트로 선택한 threat defense 디바이스에서 생성한 VTI 인터페이스를 선택합니다.

- 새 인터페이스를 생성하려면 + 아이콘을 클릭하고 VTI 인터페이스 추가, 21 페이지에 설명된 대로 필드를 채웁니다.
- 기존 VTI의 구성을 편집하려면 **Static Virtual Tunnel Interface(**고정 가상 터널 인터페이스**)** 드롭다운 필드에서 VTI를 선택하고 **Edit VTI(VTI** 편집**)**를 클릭합니다.

단계 **2** 엔드포인트 디바이스가 NAT 디바이스 뒤에 있는 경우 **Tunnel Source IP is Private(**터널 소스 **IP**는 전용**)** 확인란을 선택합니다. **Tunnel Source Public IP Address(**터널 소스 공용 **IP** 주소**)** 필드에 터널 소스 공용 IP 주소를 입력합니다.

단계 **3** **Send Local Identity to Peers(**피어에 로컬 **ID** 전송**)** - 로컬 ID 정보를 피어 디바이스로 전송하려면 이 옵션을 선택합니다. 목록에서 다음 **Local Identity Configuration(**로컬 **ID** 구성**)** 중 하나를 선택하고 로컬 ID를 구성합니다.

- **IP address(IP** 주소**)** — ID에 대한 인터페이스의 IP 주소를 사용합니다.
- **Auto(**자동**)** - 인증서 기반 연결을 위해 사전 공유 키 및 인증서 DN에 IP 주소를 사용합니다.
- **Email ID(**이메일 **ID)** - ID에 사용할 이메일 ID를 지정합니다. 이메일 ID는 최대 127자입니다.
- **Hostname(**호스트 이름**)**—정규화된 호스트 이름을 사용합니다.
- **Key ID(**키 **ID)** - ID에 사용할 키 ID를 지정합니다. 키 ID는 65자 미만이어야 합니다.

로컬 ID는 모든 터널에 대한 전역 ID 대신 IKEv2 터널별로 고유한 ID를 구성하는 데 사용됩니다. 고유 ID를 사용하면 threat defense에서 NAT 뒤에 여러 IPsec 터널을 포함하여 Cisco Umbrella SIG(Secure Internet Gateway)에 연결할 수 있습니다.

Umbrella에서 고유한 터널 ID를 구성하는 방법에 대한 자세한 내용은 **Cisco Umbrella SIG** 사용 설명서를 참조하십시오.

단계 **4** (선택 사항) 백업 인터페이스로 추가 VTI를 지정하려면 **Add Backup VTI(**백업 **VTI** 추가**)**를 클릭합니다.

참고 토폴로지의 두 피어가 동일한 터널 소스에 백업 VTI를 구성하지 않았는지 확인합니다. 예를 들어 피어 A에 단일 터널 소스 인터페이스로 구성된 2개의 VTI(기본 및 백업)가 있는 경우(예: 10.10.10.1/30), 피어 B에는 단일 터널 소스 IP(예: 20.20.20.1/30)를 사용하는 2개의 VTI도 포함할 수 없습니다.

참고 가상 터널 인터페이스가 백업 VTI에 지정되어 있지만 라우팅 구성에 따라 기본 또는 백업으로 사용할 터널이 결정됩니다.

다음을 수행할 수 있습니다.

- 새 백업 인터페이스를 생성하려면 + 아이콘을 사용합니다.
- 기존 백업 VTI의 구성을 편집하려면 **Edit VTI(VTI** 편집**)**를 사용합니다.

참고 디바이스가 NAT 디바이스 뒤에 있는 경우 **Tunnel Source IP is Private(**터널 소스 **IP**는 전용**)** 확인란을 선택합니다. **Tunnel Source Public IP Address(**터널 소스 공용 **IP** 주소**)** 필드에 터널 소스 공용 IP 주소를 입력합니다.

단계 **5** **Advance Settings(**고급 설정**)**를 확장하고 **Connection Type(**연결 유형**)** 드롭다운 메뉴에서 **Answer Only(**응답 전용**)** 또는 **Bidirectional(**양방향**)**을 선택합니다. IKE 프로토콜 버전을 IKEv1로 선택한 경우 노드 중 하나가 **Answer Only(**응답 전용**)**이어야 합니다.

단계 **6** 엑스트라넷 스포크의 경우 다음 매개변수를 지정합니다.

1. **Device Name(**디바이스 이름**)**에 디바이스 이름을 입력합니다.
2. **Endpoint IP address(**엔드포인트 **IP** 주소**)**에 기본 IP 주소를 입력합니다. 백업 VTI를 구성하는 경우 쉼표를 입력한 다음 백업 IP 주소를 지정합니다.
3. **IKE** 탭을 클릭하고 엑스트라넷에 제공된 사전 공유 키를 지정합니다.

참고 AWS VPC에는 기본 정책으로 **AES-SHA-SHA-LATEST**가 있습니다. 따라서 원격 피어가 AWS VPC에 연결되면 **Policy(**정책**)** 드롭다운 목록에서 **AES-SHA-SHA-LATEST**를 선택하여 AWS에서 기본값을 변경할 필요 없이 VPN 연결을 설정합니다.

단계 **7** 추가 스포크 노드를 구성하려면 이전 절차를 반복합니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- (선택 사항) Threat Defense VPN IKE 옵션, 10 페이지에 설명된 대로 구축에 대한 **IKE** 옵션을 지정합니다.
- (선택 사항) Threat Defense VPN IPsec 옵션, 12 페이지에 설명된 대로 구축에 대한 **IPsec**옵션을 지정합니다.
- (선택 사항) Threat Defense 고급 Site-to-site VPN 구축 옵션, 15 페이지에 설명된 대로 구축에 대한 **Advanced(**고급**)** 옵션을 지정합니다.
- **Save(**저장**)**를 클릭합니다.

VTI에 대한 추가 구성

두 디바이스에서 VTI 인터페이스 및 VTI 터널을 구성한 후에는 VTI 터널을 통해 디바이스간에 VTI 트래픽을 라우팅하도록 라우팅 정책을 구성해야 합니다. 암호화된 트래픽을 허용하도록 액세스 제어 규칙을 구성해야 합니다.

VTI를 위한 라우팅 구성

고정 경로

VTI 터널을 통해 디바이스 간의 트래픽 흐름을 라우팅하도록 두 디바이스(두 종단 모두)에서 고정 라우팅을 구성합니다.

VPN에 대해 백업 터널이 구성된 경우 백업 터널을 통한 트래픽 흐름의 페일오버를 처리할 수 있도록 다른 메트릭으로 고정 경로를 구성합니다.

고정 경로를 구성할 때 다음을 구성해야 합니다.

- **Interface(**인터페이스**)**-VPN에서 사용되는 VTI 인터페이스를 선택합니다. 백업 터널의 경우 VPN에서 사용되는 백업 VTI 인터페이스를 선택합니다.
- **Selected Network(**선택한 네트워크**)**-원격 피어의 보호된 네트워크(네트워크 개체로 추가됨)를 선택합니다.
- **Gateway(**게이트웨이**)**-원격 피어의 터널 인터페이스 IP 주소를 게이트웨이로 선택합니다. 백업 터널의 경우 원격 피어의 백업 터널 인터페이스 IP 주소를 게이트웨이로 선택합니다.

고정 라우팅에 대한 자세한 내용은 고정 경로 추가을 참조하십시오.

BGP(Border Gateway Protocol)

다음 설정을 사용하여 라우팅 정보를 공유하고 터널을 통해 디바이스간에 트래픽 흐름을 라우팅하도록 두 디바이스 모두에서 BGP를 구성합니다.

1. **General Settings(**일반 설정**)**> **BGP**에서 BGP를 활성화하고 로컬 디바이스의 AS 번호를 제공하고 라우터 ID를 추가합니다(수동을 선택한 경우).
2. **BGP**아래의 IPv4/IPv6을 활성화하고 **Neighbor**(인접 항목) 탭에서 인접 항목을 구성합니다.
   - **IP Address(IP** 주소**)**-원격 피어의 VTI 인터페이스 IP 주소를 인접 항목의 IP 주소로 지정합니다. VPN에 대해 백업 터널이 구성된 경우 원격 피어의 백업 VTI 인터페이스 IP 주소가 있는 인접 항목도 추가합니다.
   - **Remote AS(**원격 **AS)**-원격 피어의 AS 번호를 지정합니다.
3. **Redistribution(**재분배**)** 탭에서 Source Protocol(소스 프로토콜)을 Connected(연결됨)로 선택하여 연결된 경로 재분배를 활성화합니다.

BGP 구성에 대한 자세한 내용은 BGP 구성를 확인하십시오.

AC 정책 규칙

디바이스의 액세스 제어 정책에 액세스 제어 규칙을 추가하여 다음 설정으로 VTI 터널 간 암호화된 트래픽을 허용합니다.

1. Allow(허용) 작업으로 규칙을 생성합니다.
2. 로컬 디바이스의 VTI 보안 영역을 소스 영역으로 선택하고 원격 피어의 VTI 보안 영역을 대상 영역으로 선택합니다.
3. 원격 피어의 VTI 보안 영역을 소스 영역으로 선택하고 로컬 디바이스의 VTI 보안 영역을 대상 영역으로 선택합니다.

액세스 제어 규칙 구성에 대한 자세한 내용은 액세스 제어 규칙 생성 및 수정을 참고하십시오.

참고 백업 VTI가 구성된 경우 기본 VTI와 동일한 보안 영역에 백업 터널을 포함해야 합니다. AC 정책 페이지에는 백업 VTI에 대한 특정 설정이 필요하지 않습니다.

사이트 간 VPN 모니터링

Secure Firewall Management Center는 사이트 간 VPN 터널의 상태를 확인하기 위해 사이트 간 VPN 터널의 스냅샷을 제공합니다. 피어 디바이스 간의 터널 목록과 각 터널의 상태(Active(활성), Inactive(비활성) 또는 No Active Data(활성 데이터 없음))를 볼 수 있습니다. 토폴로지, 디바이스 및 상태에 따라 테이블의 데이터를 필터링할 수 있습니다. 모니터링 대시보드의 표에는 라이브 데이터가 표시되며, 지정된 간격으로 데이터를 새로 고치도록 구성할 수 있습니다. 이 표에는 암호화 맵 기반 VPN에 대한 피어 투 피어, 허브 및 스포크 및 전체 메시 토폴로지가 나와 있습니다. 터널 정보에는 경로 기반 VPN 또는 VTI(Virtual Tunnel Interface)에 대한 데이터도 포함됩니다.

이 데이터를 사용하여 다음을 수행할 수 있습니다.

- 문제가 있는 VPN 터널을 식별하고 문제 해결합니다.
- 사이트 간 VPN 피어 디바이스 간의 연결을 확인합니다.
- VPN 터널의 상태를 모니터링하여 사이트 간에 중단 없는 VPN 연결을 제공합니다.

암호화 맵 기반 사이트 간 VPN 구성에 대한 자세한 내용은 정책 기반 사이트 간 VPN 구성, 5 페이지의 내용을 참조하십시오.

VTI에 대한 자세한 내용은 Virtual Tunnel Interface 정보, 18 페이지의 내용을 참조하십시오.

threat defense VPN 모니터링 및 문제 해결에 대한 자세한 내용은 VPN 모니터링 및 문제 해결의 내용을 참조하십시오.

지침 및 제한 사항

- 다음 표에는 구축된 사이트 간 목록이 나와 있습니다. 생성되고 구축되지 않은 터널은 표시되지 않습니다.
- 정책 기반 VPN 및 백업 VTI의 백업 터널에 대한 정보는 표에 표시되지 않습니다.
- 클러스터 구축의 경우 실시간 데이터의 관리자 변경 사항이 표에 표시되지 않습니다. VPN이 구축되었을 때 존재했던 관리자 정보만 표시됩니다. 관리자 변경 사항은 변경 후 터널 AM이 재구축된 후에만 표에 반영됩니다.

사이트 간 VPN 모니터링 대시보드

사이트 간 VPN 모니터링 대시보드에는 사이트 간 VPN 터널에 대한 다음 위젯이 표시됩니다.

- 터널 상태 표—management center를 사용하여 구성된 사이트 간 VPN을 나열하는 표입니다.
- 터널 상태 분포도 - 도넛 그래프로 표시되는 터널의 집계된 상태입니다.
- 토폴로지 요약 목록 - 토폴로지별로 요약된 터널의 상태입니다.

VPN 터널의 상태

사이트 간 모니터링 대시보드에는 다음과 같은 상태의 VPN 터널이 나열됩니다:

- **Inactive(**비활성**)** — 모든 IPSec 터널이 중단된 경우 정책 기반(암호화 맵 기반) VPN 터널이 비활성 상태입니다. 터널에 구성 또는 연결 문제가 발생하면 VTI 또는 터널이 다운된 것입니다.
- **Active(**활성**)** - management center에서 정책 기반 사이트 간 VPN은 IKE 정책과 VPN 토폴로지에 할당된 IPsec 제안을 기반으로 구성됩니다. management center가 구축 후 터널을 통해 대상 트래픽을 식별하는 경우 정책 기반 VPN 터널은 활성 상태입니다. IKE 터널은 하나 이상의 IPsec 터널이 가동 중인 경우에만 작동합니다.

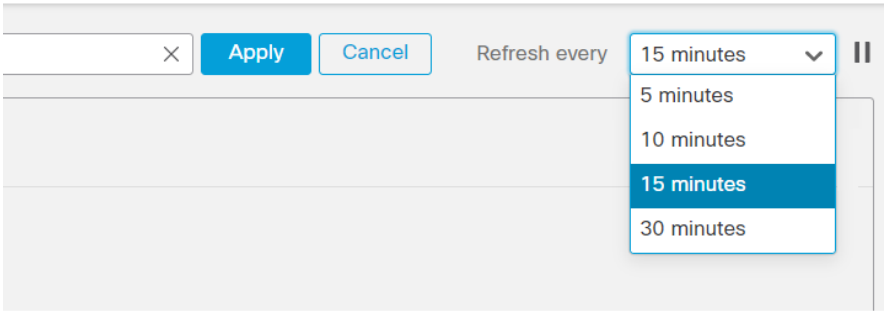
  경로 기반 VPN(VTI) 터널은 활성 상태에 관심 있는 트래픽이 필요 하지 않습니다. 오류 없이 구성 및 구축된 경우 Active(활성) 상태입니다.
- **No Active Data(**활성 데이터 없음**)** — 정책 기반 터널은 처음으로 터널을 통과하는 트래픽 플로우 이벤트가 발생할 때까지 No Active Data(활성 데이터 없음) 상태로 유지됩니다. No Active Data(활성 데이터 없음) 상태에는 오류와 함께 구축된 정책 기반 및 경로 기반 VPN도 나열됩니다.

자동 데이터 새로 고침

테이블의 사이트 간 VPN 데이터는 주기적으로 새로 고쳐집니다. VPN 모니터링 데이터를 특정 간격으로 새로 고치도록 구성하거나 자동 데이터 새로 고침을 끌 수 있습니다.

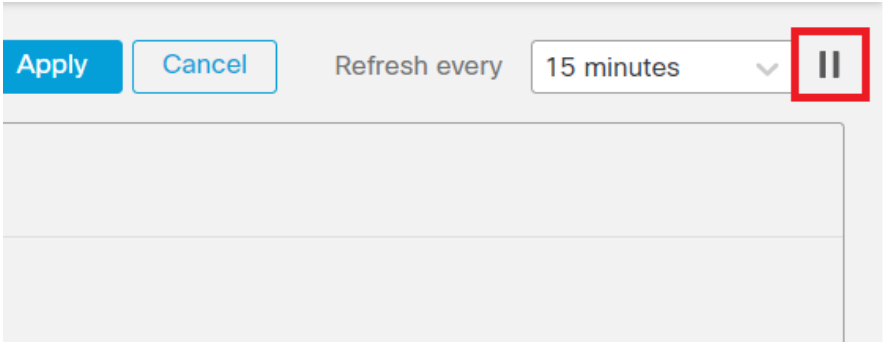
Refresh(새로 고침**)** 간격 드롭다운을 클릭하여 사용 가능한 간격 중에서 선택하여 테이블의 데이터를 새로 고칩니다.

그림 *1:* 터널 데이터 새로 고침



원하는 시간 동안 자동 데이터 새로 고침을 중지하려면 **Pause(**일시 중지**)**를 클릭합니다. 동일한 버튼을 클릭하여 터널 데이터 새로 고침을 재개할 수 있습니다.

그림 *2:* 주기적인 데이터 새로 고침 일시 중지



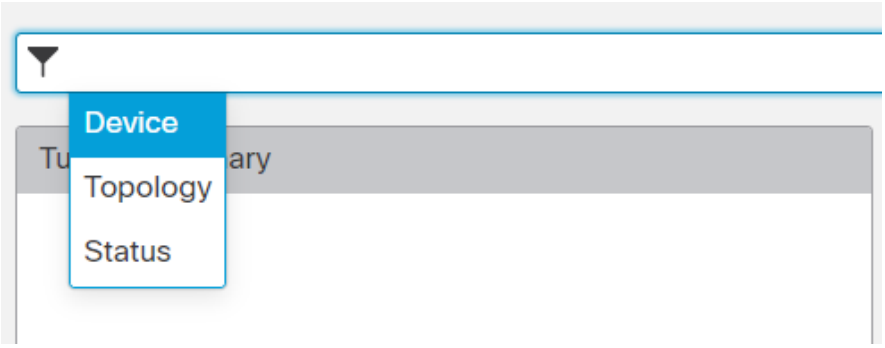
사이트 간 **VPN** 모니터링 데이터 필터링 및 정렬

VPN 모니터링 테이블의 데이터를 토폴로지, 디바이스 및 상태별로 필터링하고 볼 수 있습니다.

예를 들어 특정 토폴로지에서 Down(중단) 상태인 터널을 볼 수 있습니다.

필터 상자 내부를 클릭하여 필터 기준을 선택한 다음 필터링할 값을 지정합니다.

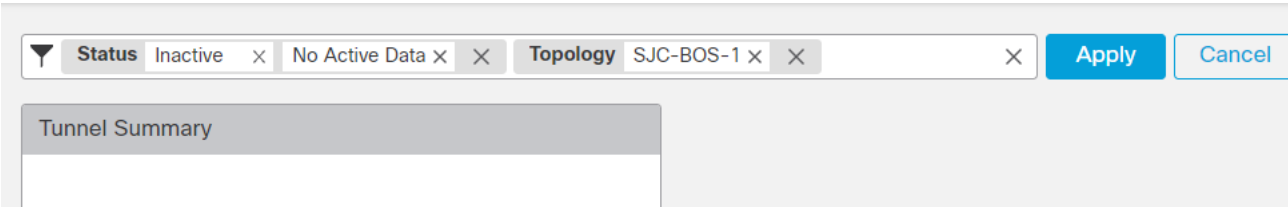
그림 *3:* 터널 데이터 필터링



여러 필터링 기준을 사용하여 요구 사항에 따라 데이터를 볼 수 있습니다.

예를 들어 Up(작동) 및 Down(다운) 상태의 터널만 표시하고 Unknown(알 수 없음) 상태의 터널은 무시하도록 선택할 수 있습니다.

그림 *4:* 예*:* 터널 데이터 필터링



데이터 정렬 - 열을 기준으로 데이터를 정렬하려면 열 제목을 클릭합니다.

관련 항목

사이트 간 VPN 정보, 1 페이지

Virtual Tunnel Interface 정보, 18 페이지