Site-to-Site VPN Firepower Threat Defense

Firepower Threat Defense Site-to-Site VPN 정보

Firepower Threat Defense Site-to-Site VPN은 다음 기능을 지원합니다.

- IPsec IKEv1 및 IKEv2 프로토콜이 모두 지원됩니다.
- 인증을 위한 인증서 및 자동 또는 수동 사전 공유 키.
- IPv4 및 IPv6. 내부와 외부의 모든 조합이 지원됩니다.
- IPsec IKEv2 Site-to-Site VPN 토폴로지는 보안 인증을 준수하기 위한 구성 설정을 제공합니다.
- 정적 및 동적 인터페이스.
- Firepower Management Center 및 FTD HA 환경에 대한 지원.
- 터널이 다운될 때 VPN 알림.
- FTD Unified CLI를 통해 사용 가능한 터널 통계.
- Point-to-Point 엑스트라넷 및 허브 앤 스포크 VPN에 대한 IKEv1 및 IKEv2 백업 피어 구성 지원.
- '허브 앤 스포크' 구축에서 허브로 작동하는 엑스트라넷 디바이스 지원.

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

VPN 토폴로지

새로운 Site-to-Site VPN 토폴로지를 생성하려면 고유한 이름을 부여하거나 토폴로지 유형을 지정하거나 IPsec IKEv1 또는 IKEv2에 사용되는 IKE 버전 또는 둘 다를 선택해야 합니다. 또한 . 구성된 후 토폴로지를 Firepower Threat Defense 디바이스에 구축합니다. Firepower Management Center는 FTD 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

Firepower 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

엑스트라넷 디바이스

각 토폴로지 유형에는 Firepower Management Center에서 관리되지 않는 디바이스인 엑스트라넷 디바이스가 포함될 수 있습니다. 예를 들면 다음과 같습니다.

- Firepower 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. Firepower Management Center를 사용하여 타사 디바이스에 구성을 생성하거나 구축할 수 없습니다.

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

Firepower 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.
- Firepower Threat Defense VPN은 Firepower Management 백업을 통해서만 백업됩니다.
- Firepower Threat Defense VPN은 현재 PDF 내보내기 및 정책 비교를 지원하지 않습니다.
- Firepower Threat Defense VPN에는 터널별 또는 디바이스별 편집 옵션이 없으므로 전체 토폴로지만 편집할 수 있습니다.
- FTD VPN은 클러스터링된 환경에서 지원되지 않습니다.
- 터널 상태는 실시간으로 업데이트되지 않지만 Firepower Management Center에서 5분 간격으로 업데이트됩니다.
- 전송 모드는 지원되지 않으며 터널 모드만 지원됩니다. IPsec 터널 모드는 새 IP 패킷에서 페이로드가 되는 원래 IP 데이터그램 전체를 암호화합니다. 방화벽 뒤에 배치되어 있는 호스트와 주고받는 트래픽을 방화벽이 보호하는 경우 터널 모드를 사용합니다. 터널 모드는 인터넷 등의 신뢰할 수 없는 네트워크를 통해 연결하는 두 방화벽 또는 기타 보안 게이트웨이 간에 일반 IPSec이 구현되는 통상적인 방식입니다.
- "(큰 따옴표)는 사전 공유 키로 지원되지 않습니다. 사전 공유 키에서 "를 사용한다면, Firepower Threat Defense 6.30으로 업그레이드한 후에 해당 문자를 변경해야 합니다.

사이트 간 VPN 요구 사항 및 사전 요건

모델 지원

FTD

지원되는 도메인

Leaf

사용자 역할

관리자

Firepower Threat Defense Site-to-Site VPN 관리

프로시저

단계 **1** VPN에 대한 인증서 인증의 경우 Firepower Threat Defense 인증서 기반 인증에서 설명한 대로 신뢰 지점을 할당하여 디바이스를 준비해야 합니다.

단계 **2** **Devices(**디바이스**) > VPN > Site to Site(**사이트 대 사이트**)**를 선택하여 Firepower Threat Defense Site-to-Site VPN 구성 및 구축을 관리하십시오. 다음 중에서 선택합니다.

- 추가 - 새 VPN 토폴로지를 생성하려면 추가( )**Add VPN(VPN** 추가**) > Firepower Threat Defense Device(Firepower Threat Defense** 디바이스**)**를 클릭하고 Firepower Threat Defense Site-to-Site VPN 구성, 5 페이지의 설명에 따라 계속 진행합니다.

  참고 VPN 토폴로지는 리프 도메인에서만 생성될 수 있습니다.

- 편집 - 기존 VPN 토폴로지의 설정을 수정하려면 수정( )을 클릭합니다. 수정 방법은 구성 방법과 비슷하며, 위의 설명에 따라 계속 진행합니다.

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

  사용자 두 명이 RA VPN 정책을 동시에 수정할 수 없으나, 웹 인터페이스에서는 동시 수정이 차단되지 않습니다.

- 삭제 - VPN 구축을 삭제하려면 삭제( )를 클릭합니다.

- VPN 상태 보기 - 이 상태는 Firepower VPN에만 적용됩니다. 현재 FTD VPN에 대한 상태는 표시되지 않습니다. FTD VPN 상태를 확인하려면 Firepower Threat Defense VPN 모니터링 섹션을 참조하십시오.

- 구축 - **Deploy(**구축**) > Deployment(**구축**)**를 선택합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

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

Firepower Threat Defense Site-to-Site 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. FTD VPN 및 토폴로지 유형을 나타내기 위해 토폴로지의 이름을 지정하는 것이 좋습니다.

단계 **3** 사이트 대 사이트 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.

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

FTD 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. FTD VPN IKE 옵션, 8 페이지

단계 **8** (선택 사항) 설명에 따라 이 구축에 대해 기본값 이외의 IPSec 옵션을 지정합니다. FTD VPN IPsec 옵션, 9 페이지

단계 **9** (선택 사항) FTD 고급 Site-to-site VPN 구축 옵션, 11 페이지FTD 고급 VPN 구축 옵션의 설명에 따라 이 구축에 대해 기본값 이외의 고급 옵션을 지정합니다.

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

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

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 Firepower Threat Defense VPN 모니터링 및 Firepower Threat Defense VPN 문제 해결 섹션을 참고하십시오.

FTD 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.

- Firepower Management Center에서 관리되는 FTD 디바이스.
- Firepower Management Center에서 관리되는 FTD 고가용성 컨테이너.
- 이 Firepower 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

- Firepower 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 주소(이 관리되는 디바이스의 인터페이스에 이미 할당된 주소)를 선택합니다.
- 토폴로지의 모든 엔드포인트는 동일한 IP 주소 체계를 가져야 합니다. IPv4 터널은 IPv6 트래픽을 전달할 수 있으며 그 반대도 마찬가지입니다. 보호되는 네트워크는 터널링된 트래픽이 사용할 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.

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
Originate-Only	Answer-Only
양방향	Answer-Only
양방향	양방향

인증서 맵

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

보호되는 네트워크

이 VPN 엔드포인트가 보호하는 네트워크를 정의합니다. 사용 가능한 네트워크 개체를 선택하거나 네트워크 개체를 인라인으로 추가하려면 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 네트워크 목록에 IPv4 또는 IPv6 항목이 하나 이상 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 네트워

크의 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 역방향 경로 삽입은 **Firepower Management Center**에서 기본적으로 활성화되어 있습니다.

보호되는 네트워크를 *Any(*모두*)*로 선택하고 트래픽 기본 경로 트래픽의 삭제를 확인하면 **VPN**> **Site to Site** > edit a VPN(VPN 편집) > **IPsec** > **Enable Reverse Route Injection(Reverse Route Injection** 비활성화**)**에서 Reverse Route Injection을 비활성화합니다. 구성 변경 사항을 구축합니다. 이렇게 하면 암호화 맵 구성의 set reverse-route(Reverse Route Injection)가 제거되고 역방향 터널 트래픽이 삭제되도록 유도하는 VPN-advertised reverse route가 제거됩니다.

-

Advanced Settings(고급 설정**)**

동적 **RRI(Reverse Route Injection)** 활성화 - RRI(Reverse Route Injection)는 원격 터널 엔드포인트로 보호되는 네트워크 및 호스트에 대한 라우팅 프로세스에 경로를 자동으로 삽입할 수 있는 기능입니다. 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.

FTD 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 IKEv1 또는 IKEv2 정책 개체를 선택하거나 사용할 정책 개체를 새로 만듭니다. 자세한 내용은 다음 섹션을 참조하십시오. FTD IKE 정책

키 유형

- **Manual(**수동**)** - 이 VPN에 대해 사용되는 사전 공유 키를 수동으로 할당합니다. **Key(**키**)**를 지정하고 **Confirm Key(**확인 키**)**에 다시 입력합니다.
- **Automatic(**자동**)** - Management Center는 이 VPN에 사용되는 사전 공유 키를 자동으로 정의합니다. **Key Length(**키 길이**)**에 키의 문자 수(1~27)를 지정합니다.

FTD 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. 암호화 맵 항목에 정의된 제안은 IPsec 보안 협상에 사용되어 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. 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.

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 해독하

고 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 허용되지 않습니다. 협상을 지원하지 않는 하나의 엔드포인트로 인해 여러 엔드포인트가 전송 모드를 성공적으로 협상할 수 없는 경우 VPN 연결이 수행되지 않습니다.

제안
: 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.

FTD 고급 Site-to-site VPN 구축 옵션

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

FTD VPN 고급 IKE 옵션

Advanced(고급**) > IKE > ISAKAMP** 설정

IKE Keepalive

IKE Keepalive를 활성화 또는 비활성화합니다. 또는 EnableInfinite로 설정하여 디바이스가 자체적으로 Keepalive 모니터링을 시작하지 않도록 지정합니다.

임계값
IKE keep alive 신뢰 구간을 지정합니다. 이것은 keep alive 모니터링을 시작하기 전에 피어가 유휴 상태에 있도록 허용하는 시간(초)입니다. 기본값 및 최소값은 10초이고, 최대값은 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 Identity(ID)를 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.

적극적인 모드 활성화
: 허브 앤 스포크 VPN 토폴로지에만 사용할 수 있습니다. 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.

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.

- 사용자 지정:
- 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.

FTD 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**)**
SA(Security Association)의 PMTU 값이 원래 값으로 재설정되는 시간(분)을 입력합니다. 유효 범위는 10~30분이며, 기본값은 무제한입니다.

FTD 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 표시되지 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 keepalive는 VPN 연결 허브 및 스포크 사이에 위치한 디바이스(중간 디바이스)가 있는 경우 keepalive 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.

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.

Sysopt Connection Permit-vpn 옵션 활성화

암호 해독된 트래픽 검사를 생략하려면 다음 단계에 따라 *sysopt connection permit-vpn* 옵션을 활성화합니다. 하지만 AAA 서버에서 다운로드한 VPN 필터 ACL 및 인증 ACL이 여전히 VPN 트래픽에 적용됩니다.

프로시저

단계 **1** FMC 웹 인터페이스의 경우 **Objects(**개체**)** > **Object Management(**개체 관리**)** > **FlexConfig** > **Text Object(**텍스트 개체**)** > **Add Text Object(**텍스트 개체 추가**)**를 선택합니다.

단계 **2** **sysopt** 값이 있는 단일 항목인 텍스트 개체 변수(예: **vpnSysVar**)를 생성합니다.

단계 **3** **Objects(**개체**)** > **Object Management(**개체 관리**)** > **FlexConfig** > **FlexConfig Object(FlexConfig** 개체**)** > **Add FlexConfig Object(FlexConfig** 개체 추가**)**로 이동합니다.

단계 **4** **connection permit-vpn** 명령으로 FlexConfig 개체를 생성합니다.

단계 **5** 명령의 시작 부분에 FlexConfig 개체의 텍스트 개체 변수(예: **$vpnSysVar connection permit-vpn**)를 삽입하고 **Save(**저장**)**를 클릭합니다.

단계 **6** FlexConfig 개체 유형으로 **Append(**추가**)**를 적용하고 Deployment(구축)를 **Everytime(**항상**)**으로 선택합니다.

단계 **7** **Devices(**디바이스**)** > **FlexConfig**로 이동하여 및 기존 정책을 수정하거나 새로 생성합니다.

단계 **8** 새로 생성된 FlexConfig 개체를 추가하고 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

Virtual Tunnel Interface 정보

Firepower Management Center는 VTI(Virtual Tunnel Interface)라는 논리적 인터페이스를 지원합니다. 정책 기반 VPN 대신, 구성된 Virtual Tunnel Interface와 피어 간에 VPN 터널을 생성할 수 있습니다. 이는 각 터널 끝에 IPsec 프로파일이 연결된 라우팅 기반 VPN을 지원합니다. 그러면 동적 또는 정적 경로를 사용할 수 있습니다. VTI에서 이그레스(Egress)되는 트래픽은 암호화되어 피어로 전송되고, 연결된 SA가 VTI로 인그레스(Ingress)되는 트래픽의 암호를 해독합니다.

VTI를 사용하면 정적 암호화 맵 액세스 목록을 구성하고 이를 인터페이스에 매핑하기 위한 요구 사항이 없어집니다. 더 이상 모든 원격 서브넷을 추적하고 암호화 맵 액세스 목록에 포함하지 않아도 됩니다. 구축이 더 간편해지고, 동적 라우팅 프로토콜과 라우팅 기반 VPN을 지원하는 정적 VTI가 있

어 가상 프라이빗 클라우드의 많은 요구 사항도 충족합니다. FMC를 사용하면 암호화 맵 기반 VPN 설정에서 VTI 기반 VPN으로 쉽게 마이그레이션할 수 있습니다.

정적 가상 터널 인터페이스를 설정하여 FMC, FTD 디바이스 REST API 및 FDM에서 경로 기반 VPN을 설정할 수 있습니다. FMC는 VTI 또는 경로 기반 VPN을 설정하는 데 기본값을 사용하는 사이트 간 VPN 마법사를 지원합니다. 트래픽은 정적 경로 또는 BGP를 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.

- 두 대의 FTD 디바이스
- FTD 및 퍼블릭 클라우드
- FTD 및 서비스 제공자 리던던시가 있는 또 다른 FTD
- FTD 및 VTI 인터페이스가 설정된 기타 디바이스

Virtual Tunnel Interface에 대한 지침 및 제한 사항

IPv6 지원

- IPv6은 지원되지 않습니다.

제한 사항

- 20개의 고유한 IPSec 프로파일만 지원됩니다.
- 물리적 인터페이스당 100개의 VTI만 지원됩니다.
- 동적 VTI, OSPF 및 QoS는 지원되지 않습니다.
- VTI로 생성된 사이트 간 VPN 터널은 터널이 다운될 때 상태 알림을 생성하지 않습니다. VTI를 사용하는 VPN에서 패킷 손실이 발생하는 경우, VPN 설정을 확인하십시오.

일반 구성 지침

- VTI는 IPsec 모드에서만 구성할 수 있습니다.
- 터널 인터페이스를 사용하여 트래픽에 대한 동적 또는 정적 경로를 사용할 수 있습니다.
- 기본 물리적 인터페이스에 따라 VTI에 대한 MTU가 자동으로 설정됩니다.
- VTI는 IKE 버전 v1, v2를 지원하고 IPsec을 사용하여 터널의 소스와 대상 간에 데이터를 전송 및 수신합니다.
- 네트워크 주소 변환을 적용해야 할 경우, IKE 및 ESP 패킷이 UDP 헤더에서 캡슐화됩니다.

- IKE 및 IPsec 보안 연계는 터널에서 데이터 트래픽에 관계없이 지속적으로 다시 입력됩니다. 이렇게 하면 VTI 터널은 항상 작동합니다.
- 터널 그룹 이름은 피어가 IKEv1 또는 IKEv2 id로 전송하는 항목과 일치해야 합니다.
- LAN-to-LAN 터널 그룹에서 IKEv1의 경우, 터널 인증 방법이 디지털 인증서 및/또는 적극적인 모드를 사용하도록 구성된 피어인 경우, IP 주소가 아닌 이름을 사용할 수 있습니다.
- VTI 및 암호화 맵 구성은 동일한 물리적 인터페이스에서 공존할 수 있으며 암호화 맵에 구성된 피어 주소를 제공하며 VTI에 대한 터널 대상은 서로 다릅니다.
- 기본적으로 VTI를 통해 전송되는 모든 트래픽이 암호화됩니다.
- VTI 인터페이스에 대한 보안 레벨 구성이 없습니다.
- 액세스 목록은 VTI를 통과하는 트래픽을 제어하기 위해 VTI 인터페이스에 적용될 수 있습니다.

다중 인스턴스

VTI는 단일 인스턴스에서만 지원됩니다.

방화벽 모드

VTI는 라우팅 모드에서만 지원됩니다.

VTI 인터페이스 추가

경로 기반 사이트 간 VPN을 설정하려면 VTI 터널의 두 노드에 있는 디바이스에서 가상 터널 인터페이스를 생성해야 합니다. 새 VTI 인터페이스를 생성하려면 다음 단계를 수행합니다.

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**)** 드롭다운 메뉴에서 **Virtual Tunnel Interface(**가상 터널 인터페이스**)**를 선택합니다.

단계 **4** **Name(**이름**)** 필드에 새 VTI의 이름을 입력합니다.

단계 **5** 인터페이스를 생성한 후 활성화하려면 **Enabled(**활성화됨**)** 확인란을 선택한 상태(기본값)로 유지합니다.

단계 **6** (선택 사항) 새 VTI의 설명을 입력합니다.

단계 **7** (선택 사항) **Security Zone(**보안 영역**)** 드롭다운 메뉴에서 해당 영역에 VTI 인터페이스를 추가할 보안 영역을 선택합니다. 보안 영역을 기준으로 트래픽 검사를 수행하려는 경우, 보안 영역에 VTI를 추가하고 액세스 제어 규칙을 설정할 수 있습니다. 터널을 통한 VPN 트래픽을 허용하려면 이 보안 영역이 있는 AC 규칙을 소스 영역으로 추가해야 합니다.

단계 **8** **Tunnel ID(**터널 **ID)** 필드에 0~10413 범위의 고유한 터널 ID를 입력합니다.

단계 **9** **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 Cisco는 FTD 예약 범위(169.254.1.x/24)를 제외하고 169.254.x.x/16 범위의 IP를 사용하기를 권장합니다. 또한 VTI 터널의 양 끝에 두 개의 주소만 최적으로 사용하려면 /30을 넷마스크로 사용하는 것이 좋습니다. 예: 169.254.100.1/30

단계 **10** **Tunnel Source(**터널 소스**)** 드롭다운 메뉴에서 터널 소스 인터페이스를 선택합니다.

단계 **11** **OK(**확인**)**를 클릭합니다.

라우트 기반 사이트 대 사이트 **VPN** 생성

두 노드간에 라우트 기반 사이트 대 사이트 VPN을 구성할 수 있습니다. VTI 기반 VPN을 구성하려면 터널의 두 노드에서 모두 가상 터널 인터페이스가 필요합니다.

VTI에 대한 자세한 내용은 Virtual Tunnel Interface 정보, 14 페이지의 내용을 참조하십시오.

프로시저

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

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

단계 **3** Topology Name(토폴로지 이름) 필드에 생성 중인 VPN 토폴로지의 이름을 입력합니다.

단계 **4** 토폴로지 유형으로 VTI(Route Based)를 선택합니다. 네트워크 토폴로지는 포인트 투 포인트로 선택되며 IKE 프로토콜 버전은 사이트 대 사이트 구성에 기본적으로 IKEv2로 선택됩니다.

단계 **5** **Endpoints(**엔드포인트**)** 탭의 노드 **A** 아래에 있는 **Device(**디바이스**)** 드롭다운 메뉴에서 VTI 터널의 첫 번째 엔드포인트로 사용할 등록된 디바이스(FTD) 또는 엑스트라넷의 이름을 선택합니다.

단계 **6** 등록된 디바이스의 경우 노드 A에 대한 인터페이스를 지정할 수 있습니다.

- **Virtual Tunnel Interface(**가상 터널 인터페이스**)** 드롭다운 메뉴에서 노드 A로 선택한 FTD 디바이스에서 생성한 VTI 인터페이스를 선택합니다.
- 노드 A에서 새 인터페이스를 생성하려면 + 아이콘을 클릭하고 VTI 인터페이스 추가, 16 페이지에 설명된 대로 필드를 채웁니다.
- 기존 VTI의 구성을 편집하려면 **Virtual Tunnel Interface(**가상 터널 인터페이스**)** 드롭다운 필드에서 VTI를 선택하고 **Edit VTI(VTI** 편집**)**를 클릭합니다.

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

단계 **7** 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 **8** **Connection Type(**연결 유형**)** 드롭다운 메뉴에서 **Answer Only(**응답 전용**)** 또는 **Birectional(**양방향**)**을 선택합니다. IKE 프로토콜 버전을 IKEv1로 선택한 경우 노드 중 하나가 **Answer Only(**응답 전용**)**이어야 합니다.

단계 **9** **Additional Configuration(**추가 구성**)**에서 다음을 수행합니다.

- VTI로 트래픽을 라우팅하려면 **Routing Policy(**라우팅 정책**)**를 클릭합니다. FMC는 **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. FMC는 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 **10** 엑스트라넷 피어의 경우 다음 매개변수를 지정합니다.

a) **Device Name(**디바이스 이름**)**에 디바이스 이름을 입력합니다.
b) **Endpoint IP address(**엔드포인트 **IP** 주소**)**에 기본 IP 주소를 입력합니다.
c) **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 **11** 노드 B에 대해 위의 절차를 반복합니다.

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.
- **Selected Network(**선택한 네트워크**)**-원격 피어의 보호된 네트워크(네트워크 개체로 추가됨)를 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.

- **General Settings(**일반 설정**)**> **BGP**에서 BGP를 활성화하고 로컬 디바이스의 AS 번호를 제공하고 라우터 ID를 추가합니다(수동을 선택한 경우).
- **BGP** 아래의 IPv4를 활성화하고 Neighbor(인접 항목) 탭에서 인접 항목을 구성합니다.
  - **IP Address(IP** 주소**)**-원격 피어의 VTI 인터페이스 IP 주소를 인접 항목의 IP 주소로 지정합니다.
  - **Remote AS(**원격 **AS)**-원격 피어의 AS 번호를 지정합니다.

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.

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

기능	버전	세부 사항
약한 암호 제거 및 사용 중단	6.7	

기능	버전	세부 사항
		보안 수준이 낮은 암호에 대한 지원이 제거되었습니다. VPN이 올바르게 작동하도록 FTD 6.70을 지원되는 DH 및 암호화 알고리즘으로 업그레이드하기 전에 VPN 설정을 업데이트하는 것이 좋습니다. FTD 6.70에서 지원되는 것과 일치하도록 IKE 제안 및 IPSec 정책을 업데이트한 다음 설정 변경 사항을 구축합니다. 다음과 같이 안전성이 상대적으로 낮은 암호는 FTD 6.70 이상에서 제거되었거나 더 이상 사용되지 않습니다. • **Diffie-Hellman GROUP 5**는 IKEv1에서 더 이상 사용되지 않으며 IKEv2에서 제거됩니다. • 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.

기능	버전	세부 사항
동적 RRI 지원	6.7	동적 Reverse Route Injection은 IKEv2 기반 정적 암호화 맵에서 지원됩니다.
사이트 간 VPN을 위한 백업 피어	6.6	FMC를 사용하여 사이트 간 VPN 연결에 백업 피어를 추가할 수 있습니다. 예를 들어 ISP가 2개 있을 경우, 첫 번째 ISP에 대한 연결을 사용할 수 없게 되면 VPN 연결을 백업 ISP로 페일오버하도록 구성할 수 있습니다.