사이트 간 VPN 터널 연결

사이트 간 VPN 터널은 다양한 위치에 있는 네트워크를 연결합니다. 서로 다른 두 멀티 클라우드 방어 게이트웨이사이에 또는 멀티 클라우드 방어 게이트웨이와 모든 관련 표준을 준수하는 클라우드 서비스 제공자 간에 사이트 간 IPsec 연결을 생성할 수 있습니다. VPN 연결이 설정되면 로컬 게이트웨이의 뒤에 있는 호스트는 보안 VPN 터널을 통해 원격 게이트의 뒤에 있는 호스트와 연결할 수 있습니다.

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

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

현재 멀티 클라우드 방어는 다음 플랫폼 또는 제품과의 사이트 간 VPN 터널 연결을 지원합니다.

- AWS
- Azure
- GCP

사이트 간 VPN 터널에 대한 사전 요건 및 제한 사항

멀티 클라우드 방어 게이트웨이 사전 요건 및 제한 사항

연결의 대상에 관계없이 VPN 터널을 생성하기 전에 다음 사전 요건을 완료해야 합니다.

- 멀티 클라우드 방어 게이트웨이 버전 24.04 또는 버전 24.04-01을 실행 중 이어야 합니다. 여기에는 Terraform 버전이 포함됩니다.
- 게이트웨이에서 **VPN** 이 활성화되어 있어야 합니다.
- 하나 이상의 클라우드 서비스 제공자 또는 서드파티 디바이스가 이미 멀티 클라우드 방어에 연결되었습니다.
- VPN 터널 연결을 허용하고 생성하도록 클라우드 서비스 제공자 또는 서드파티 디바이스를 구성해야 합니다. 자세한 내용은 서비스 또는 플랫폼 설명서를 참조하십시오.
- 하나 이상의 IPSec 프로파일이 있어야 합니다. 이 프로파일은 VPN 터널 연결에 연결해야 합니다.
- VPC 및 VNET은 양쪽에 N Address Translation 게이트웨이 없이 구축해야 합니다.
- (선택 사항) 하나 이상의 BGP 프로파일을 생성하는 것이 좋습니다. 이 프로파일은 VPN 터널 연결과 연결된 게이트웨이 인스턴스에 연결되어야 합니다.

VPN 터널 연결을 생성할 때는 다음 제한 사항에 유의합니다.

- 선택한 멀티 클라우드 방어 게이트웨이는 이그레스/이스트-웨스트 게이트웨이 여야 합니다.
- AWS 및 Azure 게이트웨이는 **8** 코어 인스턴스 유형이어야 합니다. 현재 2코어 및 4코어는 지원되지 않습니다.
- 사이트 간 VPN 연결은 최대 10개의 VPN 피어만 지원합니다.
- AWS 또는 Azure 환경용 VPC 및 VNET은 단일 가용성 영역을 사용하여 생성해야 합니다. 다중 가용성 영역은 현재 지원되지 않습니다.
- 사이트 간 VPN 터널은 현재 정방향 프록시 방화벽 규칙을 지원하지 않습니다.
- 대역폭은 800Mbps 이상이어야 합니다.

참고 게이트웨이를 활성화하거나 비활성화하는 경우에는 게이트웨이와 연결된 사이트 대 사이트 연결을 삭제하고 VPN 연결을 다시 생성해야 합니다.

게이트웨이 내에서 **VPN** 활성화

멀티 클라우드 방어 컨트롤러 대시보드에서 게이트웨이용 VPN을 활성화 하려면 다음 절차를 따릅니다.

시작하기 전에

멀티 클라우드 방어을(를) 사용하여 두 디바이스 간 VPN 연결을 설정하려면 먼저 게이트웨이가 IPSec 프로파일과 BGP 프로파일을 모두 활용할 수 있도록 활성화해야 합니다. IPSec 프로파일은 필수이며 BGP 프로파일은 선택 사항입니다.

참고 BGP 프로파일을 사용하는 경우 BGP 프로파일은 원격 피어와 함께 IPSEC 터널을 통해 실행됩니다.

단계 1 **Manage(**관리**)** > **Gateways(**게이트웨이**)**로 이동합니다.

단계 2 **Add Gateway(**게이트웨이 추가**)**를 클릭하여 새 게이트웨이를 생성하거나 기존 게이트웨이를 선택하고 Actions(작업) 드롭다운 메뉴에서 **Edit(**편집**)**를 선택합니다.

단계 3 게이트웨이를 생성하거나 편집할 때 창의 하단으로 스크롤한 다음, 프롬프트가 표시되면 드롭다운 메뉴에서 **BGP profile(BGP** 프로파일**)**을 선택합니다.

단계 4 **Advanced Settings(**고급 설정**)**에서 **VPN Connection(VPN** 연결**)** 옵션을 찾습니다. VPN 터널 연결을 옵트인하려면 **Enable VPN(VPN** 활성화**)** 옵션을 선택합니다.

단계 5 **BGP Profile(BGP** 프로파일**)** 드롭다운 메뉴를 확장하고 이미 생성된 프로파일을 선택합니다.

다음에 수행할 작업

사이트 간 터널 연결 생성.

사이트 간 터널 연결 생성

이 절차를 수행하면 게이트웨이와 Azure, AWS 및 GCP 클라우드 서비스 제공자 간에 사이트 간 VPN 터널 연결을 생성할 수 있습니다.

참고 가상 인터페이스 **IP** 주소를 입력할 때는 Threat Defense 예약 범위 169.254.1.x/24를 제외하고 169.254.xx/16 범위의 IP를 사용하는 것이 좋습니다.

넷 마스크의 경우 /30을 사용하는 것이 좋습니다. 이를 통해 가상 터널 인터페이스 연결의 엔드포인트에 대해 2개의 IP 주소만 사용할 수 있습니다. 예: 169.254.100.1/30

다음 절차에 따라 멀티 클라우드 방어 컨트롤러를 사용하여 사이트 간 VPN 터널을 생성합니다.

단계 1 **Manage(**관리**)** > **Networking(**네트워킹**)** > **Site-2-Site Connections(**사이트간 연결**)**로 이동합니다.

단계 2 **Create VPN Connection(VPN** 연결 생성**)**을 클릭합니다.

단계 3 연결의 이름을 입력합니다.

단계 4 **Device 1(**디바이스 **1)** 드롭다운 메뉴를 확장하여 멀티 클라우드 방어 게이트웨이를 선택하거나 원격 엔드포인트의 공용 IP 주소를 수동으로 입력합니다.

단계 5 **Device 1 Virtual Interface IP(**디바이스 **1** 가상 인터페이스**)** 주소를 입력합니다. 이 필드를 최적화하는 방법에 대한 지침은 이 절차의 시작 부분에 있는 참고 사항를 참조하십시오.

단계 **6** **Device 2(**디바이스 **2)** 드롭다운 메뉴를 확장하여 멀티 클라우드 방어 게이트웨이를 선택하거나 원격 엔드포인트의 공용 IP 주소를 수동으로 입력합니다. 디바이스 1과 디바이스 2에 동일한 디바이스 또는 게이트웨이를 사용하지 마십시오.

단계 **7** **Device 2 Virtual Interface IP(**디바이스 **2** 가상 인터페이스**)** 주소를 입력합니다. 이 필드를 최적화하는 방법에 대한 지침은 이 절차의 시작 부분에 있는 참고 사항를 참조하십시오.

단계 **8** 터널의 **Authentication Value(**인증 값**)**를 입력합니다. 현재 PreShared Key(사전 공유 키)가 기본 인증 방법입니다.

단계 **9** **IPSec Profile(IPSec** 프로파일**)** 드롭다운 메뉴를 확장하여 이미 생성된 프로파일을 선택합니다.

단계 **10** (선택 사항) **BGP Profile(BGP** 프로파일**)** 드롭다운 메뉴를 확장해 이미 생성된 프로파일을 선택합니다. 이 옵션을 활성화하면 IPsec 프로파일이 계속 사용되는 기본 프로파일로 유지되며 BGP 프로파일은 원격 피어를 사용하여 IPSEC 터널을 통해 실행됩니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

연결 상태를 보고 연결 양쪽의 수신 및 발신 바이트 통계를 검토합니다.

사이트 간 VPN 터널 편집

다음 절차에 따라 멀티 클라우드 방어 컨트롤러 대시보드를 사용하여 기존 사이트 간 VPN 연결을 편집합니다.

단계 **1** **Manage(**관리**)** > **Networking(**네트워킹**)** > **Site-2-Site Connections(**사이트간 연결**)**로 이동합니다.

단계 **2** VPN 연결을 선택하여 강조 표시합니다.

단계 **3** **Actions(**작업**)** 드롭다운 메뉴에서 **Edit(**편집**)**을 선택합니다.

단계 **4** 복제된 다음 정보를 수정합니다.

- Name(이름)입니다.
- 디바이스 1.
- 디바이스 1 가상 인터페이스 IP.
- 디바이스 2.
- 디바이스 1 가상 인터페이스 IP.
- 인증 값.
- IPSec 프로파일 선택.

단계 **5** **Save(**저장**)**를 클릭합니다. 언제든지 취소할 수 있습니다.

사이트 간 VPN 터널 연결 복제

다음 절차에 따라 멀티 클라우드 방어 컨트롤러 대시보드에서 VPN 터널 연결을 복제합니다.

단계 1 **Manage(**관리**)** > **Networking(**네트워킹**)** > **Site-2-Site Connections(**사이트간 연결**)**로 이동합니다.
단계 2 VPN 연결을 선택하여 강조 표시합니다.
단계 3 **Actions(**작업**)** 드롭다운 메뉴에서 **Clone(**복제**)**을 선택합니다.
단계 4 연결의 이름을 입력합니다. 복제 중인 연결과 달라야 합니다.
단계 5 복제된 다음 정보를 수정합니다.

- 디바이스 1.
- 디바이스 1 가상 인터페이스 IP.
- 디바이스 2.
- 디바이스 1 가상 인터페이스 IP.
- IPSec 프로파일 선택.

단계 6 인증 유형이 복제되었지만 해당 키 값은 복제되지 않습니다. 터널의 **Authentication Value(**인증 값**)**를 입력합니다.
단계 7 **Save(**저장**)**를 클릭합니다.

VPN 터널 연결 삭제

다음 절차에 따라 멀티 클라우드 방어 컨트롤러 대시보드에서 VPN 터널 연결을 삭제합니다.

단계 1 **Manage(**관리**)** > **Networking(**네트워킹**)** > **Site-2-Site Connections(**사이트간 연결**)**로 이동합니다.
단계 2 VPN 연결을 선택하여 강조 표시합니다.
단계 3 **Actions(**작업**)** 드롭다운 메뉴에서 **Delete(**복제**)**를 선택합니다.
단계 4 삭제 작업을 확인하고 **Delete(**삭제**)**를 클릭합니다.

다음에 수행할 작업

방금 삭제한 VPN 터널에 대해 생성한 모든 BGP 프로파일을 삭제하는 것이 좋습니다.