01 용어 정리

용어 정리

Site-to-Site VPN은 두 사이트의 게이트웨이를 암호화 터널로 이어 안전하게 통신하게 합니다. 이 가이드를 읽는 데 바탕이 되는 핵심 용어를 흐름에 따라 풀어 둡니다.

VPN의 기본

VPN(Virtual Private Network) 은 공용 인프라 위에 만드는 안전한 암호화 연결 입니다. **Site-to-Site VPN** 은 보통 지리적으로 다른 두 사이트의 Security Gateway 사이를 잇는 암호화 터널 이고, **Remote Access VPN** 은 게이트웨이와 원격 클라이언트(노트북·휴대폰 등) 사이의 터널 입니다(이 가이드는 Site-to-Site를 다룹니다).

VPN 터널은 세 가지를 보장합니다 — **Authenticity**(인증), **Privacy**(모든 데이터 암호화), **Integrity**(무결성) (소개).

VPN을 이루는 객체

VPN Domain(VPN 도메인) 은 한 게이트웨이가 보호하는, 터널에 연결된 내부 네트워크·IP의 묶음 입니다(Encryption Domain이라고도 함). **VPN Community(VPN 커뮤니티)** 는 여러 VPN 도메인을 묶은 명명된 집합 으로, 터널과 그 속성을 정의합니다. **VPN Peer** 는 터널로 연결되는 상대 게이트웨이 입니다.

커뮤니티는 두 가지 **토폴로지** 로 짭니다 — **Star(성형)** 는 위성(satellite) 게이트웨이가 중앙(central) 게이트웨이하고만 터널을 맺는 hub-and-spoke 이고, **Mesh(망형)** 는 모든 게이트웨이 쌍이 서로 터널 을 맺습니다.

트래픽을 라우팅하는 두 방식

VPN 트래픽을 보내는 방법이 둘입니다. **Domain-Based VPN** 은 SmartConsole에 정의된 VPN 도메인에 따라 라우팅 하고, **Route-Based VPN** 은 OS의 라우팅 설정(정적·동적)에 따라 **VTI(VPN Tunnel Interface)** 라는 가상 인터페이스로 라우팅 합니다(VPN 토폴로지).

암호화의 핵심 — IKE와 IPsec

터널의 바탕은 두 프로토콜입니다. **IKE(Internet Key Exchange)** 는 암호화 키를 관리하고 터널을 만드는 키 관리 프로토콜 이고, **IPsec** 은 인증·암호화된 안전한 IP 통신을 지원하는 프로토콜 입니다. IKE 협상의 결과물이 **SA(Security Association)** — 키와 방법에 대한 합의 — 입니다(IPsec와 IKE).

신뢰의 바탕은 인증서입니다. **ICA(Internal Certificate Authority)** 는 관리 서버에 내장된 인증 기관 으로 게이트웨이에 VPN 인증서를 발급하며, 외부 CA 연동은 **PKI** 로 다룹니다(PKI).

고급 기능 용어

운영·확장을 돕는 기능이 여럿입니다. **Link Selection**(VPN 트래픽에 쓸 인터페이스·경로 선택), **MEP(Multiple Entry Point)**(VPN 고가용성·부하분산), **Permanent Tunnel**(상시 유지 터널), **RIM(Route Injection Mechanism)**(VPN 피어 도메인을 내부망에 동적 라우팅으로 전파), **Wire Mode**(신뢰 VPN 트래픽의 방화벽 우회), **Directional VPN**(트래픽 방향 강제), **LSV(Large Scale VPN)**(대규모 피어를 설정 없이 배포) 가 뒤 장들에서 이어집니다.

02 Site-to-Site VPN 소개

Site-to-Site VPN 소개

Site-to-Site VPN 은 두 사이트의 Security Gateway가 협상해 암호화 터널을 만들고, 그 터널로 안전하게 통신 하게 합니다. 이 장은 VPN의 구성요소와 토폴로지, 라우팅 방식의 큰 그림을 잡습니다.

IPsec VPN과 구성요소

IPsec VPN 솔루션은 게이트웨이가 다른 게이트웨이·클라이언트와 주고받는 트래픽을 암호화·복호화 합니다. SmartConsole로 연결을 구성하며, 터널은 인증(Authenticity)·기밀(Privacy)·무결성(Integrity) 을 보장합니다.

핵심 구성요소는 셋입니다 — **VPN 엔드포인트**(게이트웨이·클러스터·원격 클라이언트), **VPN 신뢰 주체**(ICA 같은 인증 기관), **VPN 관리 도구**(관리 서버·SmartConsole) 입니다. 키 관리는 IKE, 암호화는 IPsec이 맡습니다.

VPN 커뮤니티와 토폴로지

VPN Domain 은 한 게이트웨이가 보호하는 내부 네트워크 묶음 이고, 이 도메인들을 묶은 것이 **VPN Community** 입니다. 커뮤니티는 두 토폴로지로 짭니다.

!Mesh와 Star 토폴로지 *① Security Gateway ② 위성(Satellite) 게이트웨이 ③ 중앙(Central) 게이트웨이*

Star(성형) 는 각 위성 게이트웨이가 중앙하고만 터널을 맺 고(서로는 안 맺음), **Mesh(망형)** 는 모든 게이트웨이 쌍이 서로 터널 을 맺습니다. 둘을 섞을 수도 있습니다 — 예를 들어 London·New York 본사는 Mesh로 내부망을 공유 하고, 협력사는 Star로 자기가 일하는 사이트의 내부망에만 접근하게 합니다.

VPN 트래픽 라우팅

트래픽을 보내는 방법은 두 갈래입니다. **Domain-Based VPN** 은 SmartConsole에 정의된 VPN 도메인에 따라 라우팅 하고(Star에서 위성끼리 중앙을 거쳐 통신할 때 유용), **Route-Based VPN** 은 OS 라우팅(정적·동적)에 따라 **VTI** 가상 인터페이스로 라우팅 합니다(VPN 토폴로지). 더 정교한 제어는 최적 경로·인터페이스·IP를 고르는 Link Selection 이 맡습니다.

> 참 고
>
> R82는 IPv6를 Site-to-Site VPN(Main IP↔Main IP)에 한해 제한적으로 지원합니다. IPv6는 IKEv2만, IPv4 터널엔 IPv4·IPv6 터널엔 IPv6만 지원하며, Remote Access·MEP·Route-Based(VTI)·Wire Mode·Link Selection 등 상당수 기능은 IPv6 미지원 입니다.

실제 구성은 시작하기에서 단계별로 이어집니다.

03 시작하기

시작하기

Site-to-Site VPN을 처음 세우는 일은 네 걸음 으로 흐릅니다 — IPsec VPN 블레이드 켜기, VPN 커뮤니티 만들기, Access Control 규칙 구성, 터널 확인. 이 장은 그 흐름을 정리합니다.

Step 1 — IPsec VPN 블레이드 켜고 VPN 도메인 정의

Site-to-Site VPN에는 IPsec VPN 블레이드를 켠 게이트웨이가 둘 이상 필요합니다. 각 게이트웨이를 설치·SIC 신뢰 수립·토폴로지 취득한 뒤, **General Properties** > **Network Security** 에서 **IPsec VPN** 을 선택 합니다.

그다음 **Network Management** > **VPN Domain** 에서 VPN 도메인(암호화 도메인) 을 정의합니다 — **토폴로지 기반 자동**(게이트웨이 뒤 모든 IP, 기본값) 또는 **사용자 정의**(특정 네트워크·그룹·범위) 중에 고릅니다. 관리 서버가 ICA에서 이 게이트웨이용 인증서를 자동 발급 하며, 외부 CA 인증서를 올리려면 PKI를 봅니다.

Step 2 — VPN 커뮤니티 만들기

VPN Community 객체가 멤버 게이트웨이 간 암호화·터널 설정 을 정합니다. Object Explorer의 **VPN Communities** 에서 만듭니다.

Star Community 는 Center 게이트웨이와 Satellite 게이트웨이를 지정 하고 (VSX·Maestro Security Group·Quantum Spark는 Center에 못 넣음), VPN Routing을 "To center only" 등으로 정합니다. **Meshed Community** 는 멤버 게이트웨이들을 더하 면 서로 터널을 맺습니다. 양쪽 모두 **Encrypted Traffic** 에서 **Accept all encrypted traffic**(게이트웨이 간 모든 트래픽 암호화) 을 켤지 정하며, 암호화·Shared Secret·고급 설정은 IPsec와 IKE에서 다룹니다.

Step 3 — Access Control 규칙

Accept all encrypted traffic 를 켜지 않았다면, 커뮤니티 내 트래픽을 허용하는 Access Control 규칙 을 만들어야 합니다. 규칙이 VPN 커뮤니티에 적용되게 하려면 Rule Base의 **VPN 열** 에 `Any` (모든 커뮤니티+비VPN) 또는 특정 커뮤니티(예: MyCommunity) 를 넣습니다. 예를 들어 출발지·목적지 Any, VPN=MyCommunity, Action=Accept 면 그 커뮤니티 멤버 도메인 간 암호화 트래픽을 허용합니다. 규칙을 짠 뒤 정책을 설치합니다 (Security Management 가이드의 Access Control).

Step 4 — 터널 확인

터널이 동작하는지 확인하려면, 해당 규칙의 Track을 Log로 두고 트래픽을 일으킨 뒤, **Logs & Events** > **Logs** > **Tunnel and User Monitoring** 으로 SmartView Monitor를 열어 IPsec 트래픽·열린 터널 을 봅니다. 성공하면 encrypt·decrypt·key install 로그 가 보입니다 (또는 Logs 탭에서 `VPN` 검색).

고급 설정은 어디에

기본을 세운 뒤의 고급 설정은 게이트웨이 객체와 커뮤니티 객체에 흩어져 있습니다 — 게이트웨이엔 Link Selection·VPN Tunnel Sharing·Wire Mode·NAT Traversal, 커뮤니티엔 Encryption·Tunnel Management·VPN Routing·MEP·Shared Secret 등이 있어, 이어지는 장들에서 하나씩 풀어 씁니다.

04 IPsec와 IKE

IPsec와 IKE

VPN 터널의 심장은 두 프로토콜입니다 — 키를 안전하게 만드는 **IKE** 와 그 키로 데이터를 암호화하는 **IPsec** 입니다. 이 장은 둘이 어떻게 맞물려 터널을 세우는지 정리합니다.

왜 IKE가 필요한가

대칭 암호화에서는 양쪽이 같은 키로 암·복호화 합니다. 그런데 그 키를 안전하게 나눠 갖는 것이 문제입니다. **IKE(Internet Key Exchange)** 의 목표는 양쪽이 키를 직접 주고받지 않고도 똑같은 대칭 키를 독립적으로 만들어 내는 것입니다.

비결이 **Diffie-Hellman(DH)** 입니다. 한쪽의 개인 키와 다른 쪽의 공개 키로 "공유 비밀(shared secret)"을 만들 어, IPsec 대칭 키를 이로부터 파생합니다 — 그래서 대칭 키가 실제로 전송되는 일이 전혀 없 습니다. IKE는 이렇게 양쪽을 인증하고 암호화·무결성 방법에 합의해 터널을 세우며, 그 결과물이 **SA(Security Association)** 입니다.

두 단계로 나뉜 협상

IKE는 두 phase 로 이뤄지고, 첫 단계가 둘째 단계의 토대를 놓습니다.

IKE Phase I 에서는 피어가 인증(인증서 또는 사전 공유 비밀)하고, Diffie-Hellman 키를 만들 며, Phase II를 위한 방법에 합의합니다. DH 키 생성은 느리고 무겁지만, 그 결과물인 **IKE SA** 가 Phase II의 키·방법 합의가 됩니다.

IKE Phase II(Quick Mode)는 Phase I에서 합의한 키·방법으로 암호화 된 채 진행되어, IPsec 키를 만드는 자재를 교환 합니다. 그 결과물이 **IPsec SA** 이고, 이 키·방법에 따라 실제 대량 데이터가 암호화되어 터널을 흐릅 니다.

IKEv1과 IKEv2

IKEv2 는 Simplified 모드 VPN 커뮤니티에서 지원 되며, VPN Community 객체의 **Encryption** 에서 설정합니다(기본은 IKEv1). IPv6 트래픽에는 항상 IKEv2가 자동으로 쓰이고, 암호화 방법 설정은 IPv4에만 적용됩니다.

암호화·무결성 방법

협상에서 두 파라미터가 정해집니다 — **암호화 알고리즘**(AES-128·AES-256 등) 과 **해시(무결성) 알고리즘** 입니다. Phase 1(IKE SA)과 Phase 2(IPsec SA) 각각에 대해 정하며, VPN Community 객체의 Encryption 설정에서 조정합니다. 더 강력한 양자 내성 키 교환은 Quantum Safe Key Exchange에서, 인증서 기반 인증은 PKI에서 다룹니다.

05 Quantum Safe Key Exchange

Quantum Safe Key Exchange

양자 컴퓨터가 현재 암호를 깰 수 있다는 우려가 커지면서, 키 교환을 양자 공격에도 견디게 만드는 것이 중요해졌습니다. **Quantum Safe Key Exchange**(R82 이상)는 IKEv2를 강화해 그 회복력을 높 입니다.

두 가지 IKEv2 강화

이 기능은 IKEv2에 두 가지 보강을 더합니다.

IKEv2 Intermediate Exchange(RFC-9242) 는 기존 IKE 단편화(fragmentation) 메커니즘을 활용하는 추가 교환 을 도입해, 큰 IKE 메시지의 IP 단편화를 방지 합니다. 키 교환 방식이 길어질 때 특히 유용한데, 초기 IKEv2 교환에서는 쓸 수 없는 자리를 메웁니다.

IKEv2 Multiple Key Exchanges(RFC-9370) 는 서로 다른 암호 알고리즘으로 여러 번 키를 교환 하게 해 줍니다 — Post-Quantum(양자 내성) 알고리즘을 포함 할 수 있죠. 핵심은 전체 교환의 보안이 가장 강한 알고리즘만큼은 보장 된다는 점입니다. 즉 한 방법이 뚫려도 전체 키 교환은 안전 하게 유지됩니다.

왜 중요한가

이 강화들은 큰 키 교환과 PQC(Post-Quantum Cryptography)를 도입하는 환경에서 IKEv2의 성능·보안을 끌어올 립니다. 설정은 SmartConsole의 **Object Explorer** > **VPN Communities** 에서 해당 커뮤니티에 적용합니다.

정리하면, Quantum Safe Key Exchange는 여러 알고리즘을 겹쳐 양자 시대에도 터널 키가 안전하도록 IKEv2를 미래 대비시키는 R82의 새 기능입니다.

06 Link Selection

Link Selection

게이트웨이에 인터페이스·회선이 여럿이면, VPN 트래픽을 어느 IP·인터페이스로 보낼지 정해야 합니다. **Link Selection** 은 들어오고 나가는 VPN 트래픽에 쓸 인터페이스와 최적 경로를 정하는 메커니즘입니다.

무엇을 할 수 있나

Link Selection으로 관리자는 각 게이트웨이에서 VPN 트래픽에 쓸 IP 주소를 직접 고 를 수 있습니다. 주요 옵션은 다음과 같습니다.

Probing(탐침) 으로 링크의 가용성에 따라 링크를 선택 하고, **VPN Load Sharing** 으로 가용 링크에 VPN 트래픽을 분산 하며, **Service Based Link Selection** 으로 서비스별 대역폭 사용을 제어 합니다. Remote Access VPN 클라이언트용 설정은 Site-to-Site와 함께 또는 따로 구성할 수 있습니다.

R82의 두 가지 메커니즘

R82부터 Link Selection 메커니즘이 둘입니다. **Enhanced Link Selection**(R82 새 기능) 과 기존 방식이 있어, 환경에 맞게 고릅니다. Enhanced 방식은 링크 선택을 더 정교하고 유연하게 다룹니다.

Link Selection은 ISP 이중화와도 맞물립니다 — ISP Redundancy를 켜면 그 설정이 Link Selection을 덮어쓰며, VPN 연결도 ISP 링크 장애를 넘겨 살아남습니다. 정리하면, Link Selection은 회선이 여럿인 환경에서 VPN 트래픽의 경로·가용성·부하를 세밀하게 통제 하는 손잡이입니다(세부 옵션은 분량이 커서 원문 해당 절 참고).

07 공개 키 기반구조(PKI)

공개 키 기반구조(PKI)

VPN 피어가 서로를 믿는 가장 강력한 방법은 인증서 입니다. **PKI(Public Key Infrastructure)**는 공통으로 신뢰하는 인증 기관(CA)을 통해 신뢰 관계를 맺는 토대입니다.

인증서로 신뢰를 맺는 원리

X.509 기반 PKI는 신뢰하는 CA가 엔티티에 인증서를 발급 하고, 그 인증서에 엔티티의 공개 키 가 담깁니다. CA를 믿는 피어는 CA의 서명을 검증해 인증서를 신뢰 하고, 거기 담긴 "엔티티↔공개 키" 연결을 받아들입니다. IKE 표준도 강력한 인증이 필요한 VPN에 PKI 사용을 권장 합니다.

VPN 터널을 맺는 게이트웨이는 RSA 키 쌍과 신뢰 CA가 발급한 인증서 를 가져야 합니다. 인증서에는 신원, 공개 키, CRL 조회 정보 가 담기고 CA가 서명합니다. 터널을 맺을 때 각자 자기 개인 키로 서명한 정보와 공개 키가 든 인증서를 상대에게 제시 하고, 상대 공개 키로 서명 출처를, CA 공개 키로 인증서 진위를 검증 해 피어를 인증합니다.

ICA와 외부 PKI 연동

모든 Check Point 관리 서버에는 **ICA(Internal Certificate Authority)** 가 있어 자신이 관리하는 게이트웨이에 VPN 인증서를 발급 합니다. 같은 관리 서버가 관리하는 게이트웨이끼리는 이 ICA 덕에 VPN 정의가 간단합니다.

하지만 외부 PKI 연동이 필요할 때가 있습니다 — 상대 게이트웨이가 **다른 조직의 관리 서버**(다른 ICA가 서명)에 속하거나, 상대가 **비-Check Point VPN 장비** 인 경우입니다. 이때는 외부 CA가 발급한 인증서를 게이트웨이에 올려 신뢰를 맺습니다(시작하기에서 본 인증서 업로드).

정리하면, 사내 게이트웨이끼리는 ICA로 자동, 외부 조직·서드파티와는 외부 PKI 연동 으로 인증서 기반 신뢰를 세우는 것이 VPN 인증의 핵심입니다. 외부 게이트웨이와의 구체적 구성은 클라우드·외부 게이트웨이 VPN에서 다룹니다.

08 VPN 토폴로지 — Domain-Based·Route-Based

VPN 토폴로지 — Domain-Based·Route-Based

VPN 트래픽을 어떤 방식으로 라우팅하느냐 가 토폴로지를 가릅니다. 두 갈래 — **Domain-Based** 와 **Route-Based** — 가 있고, 환경과 목적에 따라 고릅니다.

Domain-Based VPN

Domain-Based VPN 은 SmartConsole에 정의된 VPN 도메인에 따라 트래픽을 라우팅 합니다. 호스트로 트래픽을 보내려면 먼저 그 게이트웨이의 VPN 도메인을 정의 해야 하고, 라우팅 구성은 SmartConsole이나 게이트웨이의 VPN 라우팅 설정 파일(`vpn_route.conf`)에서 합니다.

핵심 쓰임새는 **VPN Routing** 입니다 — 예를 들어 게이트웨이 A와 B가 기술·정책상 직접 터널을 못 맺을 때, 둘 다와 터널을 맺은 게이트웨이 C를 거쳐 통신하게 합니다. Star 토폴로지에서 위성 게이트웨이끼리 중앙을 거쳐 통신 하는 것이 대표적입니다(중앙이 각 위성에 터널을 맺고 올바른 도메인으로 라우팅).

Route-Based VPN

Route-Based VPN 은 OS의 라우팅 설정(정적·동적)에 따라 라우팅 합니다. 핵심은 **VTI(VPN Tunnel Interface)** — VPN 터널과 연결된 가상 인터페이스 입니다. 두 피어에 서로 대응하는 VTI를 만들면, 마치 직접 연결된 것처럼 동작해, OS의 IP 라우팅이 다른 인터페이스처럼 트래픽을 터널로 보냅니다.

가장 큰 장점은 동적 라우팅 프로토콜을 쓸 수 있 다는 것입니다 — 터널 양 끝의 라우팅 데몬이 한 홉 거리처럼 라우팅 정보를 교환 합니다. 단, Route-Based VPN은 같은 VPN 커뮤니티 안의 게이트웨이끼리만 구현되며, Rule Base에 Directional Rule을 구성 해야 합니다. 또 동적 라우팅이 stateful inspection을 통과하도록 보통 Wire Mode와 함께 씁니다.

어느 쪽을 쓸까

정리하면, 정적인 사이트 간 연결·Star 라우팅에는 Domain-Based, 동적 라우팅이 필요하거나 터널을 물리 인터페이스처럼 다루고 싶으면 Route-Based(VTI) 가 맞습니다. VTI는 RIM(Route Injection)·MEP 같은 고급 기능과도 맞물립니다(단, Route-Based는 IPv6 미지원).

09 Large Scale VPN(LSV)

Large Scale VPN(LSV)

지점·협력사·원격 클라이언트를 잇는 VPN이 수백~수천 피어 에 이르면 새로운 문제가 생깁니다 — 피어가 하나 늘 때마다 참여하는 모든 게이트웨이에 설정·정책 설치 가 필요해지죠. **Large Scale VPN(LSV)** 은 이를 해결합니다.

LSV가 푸는 문제

LSV는 피어별 설정과 정책 설치 없이 대규모 VPN을 배포 하게 해 줍니다. 새 피어가 늘어도 중앙에서 일일이 구성하지 않아도 되므로, 대규모 환경의 관리 부담을 크게 덜어 줍니다.

구성 흐름

LSV 구성의 큰 줄기는 다섯 걸음입니다 — ① 인증 기관(CA) 구성 → ② Center VPN 게이트웨이 구성 → ③ VPN 커뮤니티 구성 → ④ **LSV 프로파일** 구성 → ⑤ 정책 설치 입니다.

핵심은 **LSV 프로파일** 입니다. 개별 피어를 일일이 객체로 만들고 커뮤니티에 넣는 대신, 프로파일로 다수의 위성 피어를 한꺼번에 다루 어 PKI 인증서 기반으로 자동 합류 하게 합니다. Star 토폴로지에서 중앙은 고정이고 위성이 대량으로 붙는 형태에 잘 맞습니다.

정리하면, LSV는 "피어가 늘 때마다 손대야 하는" 대규모 VPN의 확장 문제를, CA·프로파일 기반 자동 합류로 해결하는 기능입니다(세부 절차는 원문 해당 절 참고).

10 터널 관리·Route Injection

터널 관리·Route Injection

VPN 터널을 상시 살려 두고, 그 상태를 라우팅에 반영 하는 기능들을 모았습니다 — Permanent Tunnel·VPN Tunnel Sharing(Tunnel Management)과 RIM(Route Injection Mechanism)입니다.

Tunnel Management

Tunnel Management 로 터널의 종류와 개수를 다룹니다.

Permanent Tunnel(상시 터널) 은 VPN 터널을 늘 활성 상태로 유지 합니다. VPN 의존도가 높아지면서 끊김 없는 연결 이 중요해졌는데, 상시 터널은 tunnel test 패킷으로 터널을 살려 두어 장애·연결 문제를 즉시 알아챌 수 있게 합니다. 양쪽을 모니터링해 문제를 지체 없이 식별합니다.

VPN Tunnel Sharing 은 피어 게이트웨이 간 만드는 터널 수를 제어 해 상호운용성과 확장성을 높입니다. 모든 터널 상태는 SmartView Monitor에서 봅니다(Logging and Monitoring 가이드).

Route Injection Mechanism(RIM)

RIM 은 동적 라우팅 프로토콜로 VPN 피어의 암호화 도메인을 내부망에 전파 합니다. 터널이 생기면 RIM이 게이트웨이의 로컬 라우팅 테이블에 피어의 암호화 도메인을 추가 하고, 이를 동적 라우팅으로 내부망에 알립니다.

핵심은 장애 대응 입니다. RIM은 Permanent Tunnel이 구성되어 있어야 켤 수 있는데, tunnel test 패킷에 응답이 없어 터널이 "down"으로 판정되면, RIM이 그 경로를 라우팅 테이블에서 지워 이웃 동적 라우팅 장비들이 정보를 갱신하게 합니다. 그 결과 터널로 가던 트래픽이 미리 정한 대체 경로로 우회 됩니다.

구성은 두 방식입니다 — **Automatic RIM**(피어 암호화 도메인 경로를 자동 주입) 과 **Custom Script**(필요에 맞춘 작업 지정) 입니다. RIM은 MEP와 통합되어 반환 패킷을 같은 MEP 게이트웨이로 돌려보내 기도 합니다(단, RIM은 IPv6 미지원).

정리하면, Permanent Tunnel로 터널을 살려 두고, RIM으로 그 생사를 내부 라우팅에 반영해 장애 시 자동 우회하는 것이 이 장의 요지입니다.

11 Wire Mode·Directional VPN

Wire Mode·Directional VPN

VPN 트래픽의 검사를 건너뛰거나 방향을 강제 하는 두 기능을 묶었습니다 — **Wire Mode** 와 **Directional VPN Enforcement** 입니다.

Wire Mode — 신뢰 트래픽의 방화벽 우회

VPN 커뮤니티 안의 트래픽은 이미 사설이고 안전 하므로, 거기에 방화벽 규칙을 또 적용하는 것이 불필요할 때가 많습니다. **Wire Mode** 는 내부 인터페이스와 커뮤니티를 "신뢰(trusted)"로 지정해 VPN 연결의 방화벽을 우회 합니다.

동작 원리는 두 질문입니다 — 이 정보가 "신뢰" 출발지에서 왔는가? "신뢰" 목적지로 가는가? 둘 다 yes이고 양쪽 게이트웨이가 속한 커뮤니티가 Wire Mode면, stateful inspection을 적용하지 않고 신뢰 인터페이스 간 트래픽이 방화벽을 우회 합니다.

핵심 이점이 둘입니다. 검사가 없으니 패킷이 버려지지 않아 기존 연결의 페일오버가 매끄럽 고, state 검증을 통과 못 하던 동적 라우팅 프로토콜을 쓸 수 있 게 됩니다. 그래서 Wire Mode는 Route-Based VPN을 가능하게 하고, MEP 구성의 연결성·성능을 높이는 데 쓰입니다.

Directional VPN Enforcement — 방향 강제

VPN 커뮤니티를 규칙의 VPN 열에 넣으면, 출발지·목적지가 커뮤니티의 어느 게이트웨이든 될 수 있 어 트래픽이 양방향(bidirectional)입니다. 하지만 보안 정책상 한 방향만 허용하거나, 커뮤니티 밖 게이트웨이를 오가는 암호화 트래픽 을 다뤄야 할 때가 있습니다.

Directional VPN 은 출발지가 어디여야 하고 목적지가 어디여야 하는지를 명시 합니다. 그래서 한 커뮤니티 안에서, 또는 커뮤니티 사이에서 방향을 강제할 수 있습니다. 특히 Route-Based VPN을 배포하려면 Rule Base에 Directional Rule을 구성 해야 합니다.

정리하면, Wire Mode는 신뢰 VPN 트래픽의 검사를 생략해 동적 라우팅·페일오버를 돕 고, Directional VPN은 양방향이 기본인 VPN 트래픽에 방향 제약을 더하는 기능입니다.

12 Multiple Entry Point(MEP) VPN

Multiple Entry Point(MEP) VPN

MEP(Multiple Entry Point) 는 VPN 연결에 고가용성과 부하 분산을 주는 기능입니다. 내부망으로 들어가는 진입점을 여러 게이트웨이로 만들어, 하나가 죽어도 다른 게이트웨이로 접근이 유지되게 합니다.

MEP란

평소 VPN은 한 게이트웨이가 내부망의 단일 진입점 이라, 그 게이트웨이가 죽으면 피어가 내부망에 접근할 수 없습니다. **MEP 환경** 은 같은 VPN 도메인에 접근할 수 있는 게이트웨이를 둘 이상 두어, 피어 게이트웨이들이 중단 없는 접근을 위한 이중화 를 제공합니다.

MEP vs Clustering

MEP와 Clustering(ClusterXL)은 둘 다 고가용성·부하 분산을 이루지만 차이가 큽니다.

Cluster 멤버는 같은 위치에 sync 인터페이스로 직접 연결 되어야 하지만, MEP 게이트웨이는 물리적 위치 제약이 없어 지리적으로 떨어진 장비도 될 수 있습니다. 즉 같은 사이트의 하드웨어 이중화는 Cluster, 지리적으로 분산된 진입점 이중화는 MEP 가 맞습니다.

MEP는 RIM(Route Injection)·Wire Mode와 맞물려 반환 패킷을 들어온 같은 진입점으로 돌려보내 는 등 정교하게 동작합니다. 진입점 선택 방식(어느 MEP 게이트웨이를 쓸지)과 세부 구성은 분량이 커서 원문 해당 절을 참고하세요. 정리하면, MEP는 지리적으로 흩어진 여러 진입점으로 VPN의 가용성과 부하 분산을 이루는 기능입니다(단, IPv6 미지원).

13 클라우드·외부 게이트웨이 VPN

클라우드·외부 게이트웨이 VPN

사내 게이트웨이끼리만이 아니라, 클라우드의 가상 게이트웨이나 외부 조직·서드파티 게이트웨이 와도 VPN을 맺어야 할 때가 있습니다. 이 장은 그 두 시나리오를 정리합니다.

클라우드의 Virtual Gateway와 VPN

클라우드(AWS·Azure 등)에 배포한 가상 Security Gateway와 VPN 을 맺을 수 있습니다. 온프레미스 게이트웨이와 클라우드 가상 게이트웨이 사이에 터널을 세워, 사내망과 클라우드 자원을 안전하게 연결 합니다. CloudGuard 환경과 맞물리며, 구체적 배포는 해당 클라우드용 가이드를 참고합니다.

외부 VPN 게이트웨이와 VPN

External VPN Gateway 는 우리 관리 서버가 관리하지 않는 게이트웨이 입니다. 두 경우로 나뉩니다 — **외부에서 관리되는 Check Point 게이트웨이**(다른 조직의 관리 서버·ICA가 관리) 와 **비-Check Point 게이트웨이** 입니다.

인증 방법이 갈립니다. Check Point 외부 게이트웨이끼리는 PKI 인증서 로 신뢰를 맺을 수 있고, 서드파티나 인증서가 어려운 경우엔 **Pre-Shared Secret(사전 공유 비밀)** 으로 맺습니다. 시작하기에서 본 VPN 커뮤니티에 외부 게이트웨이 객체를 멤버로 넣고 암호화·Shared Secret을 구성합니다.

정리하면, 클라우드 가상 게이트웨이는 사내망↔클라우드 연결, 외부 게이트웨이는 인증서(Check Point) 또는 사전 공유 비밀(서드파티) 로 VPN을 확장하는 시나리오입니다. 외부 게이트웨이와 연동할 때 흔한 연결 문제는 제어 연결·연결 문제 해결에서 다룹니다.

14 제어 연결·연결 문제 해결

제어 연결·연결 문제 해결

VPN 커뮤니티가 제대로 동작하려면 게이트웨이·관리 서버 사이의 제어 연결 이 열려 있어야 하고, NAT·MTU 같은 흔한 걸림돌 을 풀어야 합니다. 이 장은 그 둘을 정리합니다.

VPN 커뮤니티의 방화벽 제어 연결

VPN이 동작하려면 멤버들 사이에 여러 제어 연결(control connection) 이 필요합니다 — 키 교환, 터널 테스트, 정책 설치, 신원·상태 공유 등입니다. Check Point 게이트웨이에는 이 제어 연결을 허용하는 implied rule 이 있어 보통은 따로 열 필요가 없습니다.

다만 경로에 서드파티 방화벽이 있거나 implied rule을 끈 경우 에는, 이 제어 연결이 막혀 VPN이 동작하지 않을 수 있습니다. 그래서 어떤 제어 연결이 필요한지 를 알아 두고, 막히면 명시적으로 허용해야 합니다(Identity Sharing에서도 비슷한 implied rule 의존을 봤습니다).

연결 문제 해결

VPN 연결이 안 될 때 흔한 원인과 해법입니다.

가장 흔한 것이 **NAT** 입니다. VPN 트래픽이 중간의 NAT 장비를 지나면 IPsec이 깨질 수 있는데, **NAT Traversal(NAT-T)** 로 IPsec 패킷을 UDP로 캡슐화해 NAT를 통과 시킵니다 (게이트웨이 객체에서 설정 — 시작하기의 고급 설정).

그 밖에 MTU·단편화 문제, 인증서/사전 공유 비밀 불일치, 암호화 방법 불일치, 제어 연결 차단 등이 원인이 됩니다. 진단은 SmartView Monitor의 터널 모니터링으로 터널 상태를 보고, 로그에서 encrypt/decrypt 실패를 확인하며, 깊은 분석은 명령줄·참조의 `vpn` 명령과 커널 디버그를 활용합니다.

정리하면, 제어 연결이 열려 있는지 확인하고(특히 서드파티 방화벽 경로), NAT-T로 NAT를 넘기며, 불일치 설정을 점검 하는 것이 VPN 문제 해결의 출발점입니다.

15 명령줄·참조

명령줄·참조

Site-to-Site VPN을 명령줄로 제어·진단 하는 도구와 참조 자료를 모았습니다. 방대한 명령 사전은 전용 문서로 넘기고, 여기서는 무엇이 있고 어디서 찾는지 를 짚습니다.

VPN 명령줄

VPN 운영 명령 전체는 **R82 CLI Reference Guide** 에 정리되어 있습니다. 핵심은 `vpn` 명령으로, 터널 상태 확인·SA 조회·터널 재협상·디버그 등을 합니다(예: `vpn tu` 로 터널 유틸리티, `vpn debug` 로 디버그). 연결 문제 해결에서 본 진단도 이 명령들로 합니다.

> 참 고
>
> 클러스터에서는 모든 멤버를 똑같이 설정 하고, Scalable Platforms(Maestro·Chassis)에서는 Expert 모드에서 해당 Security Group 위에서 실행합니다.

그 밖의 참조

원문 끝에는 다른 가이드와 마찬가지로 **Working with Kernel Parameters·Kernel Debug** 가 있는데, 이는 Security Gateway 가이드의 명령줄·커널 참조와 같은 공통 주제이니 그쪽을 참고하세요. **Appendix** 에는 VPN 구성 파일(`vpn_route.conf` 등)과 보조 설정 정보가 담겨 있습니다.

정리하면, 일상 구성은 SmartConsole로 하되 터널 상태·SA 진단은 `vpn` 명령 으로 내려가며, 그 전체 구문은 R82 CLI Reference Guide 가 담당합니다.