01 용어 정리

용어 정리

Remote Access VPN은 원격 사용자와 내부망 사이에 암호화 터널 을 만들어, 직원이 어디서든 안전하게 사내 자원에 접근하게 합니다. 이 가이드를 읽는 데 바탕이 되는 핵심 용어를 흐름에 따라 풀어 둡니다.

VPN의 기본

VPN(Virtual Private Network) 은 공용 인프라 위의 안전한 암호화 연결 입니다. **Remote Access VPN** 은 게이트웨이와 원격 클라이언트(노트북·휴대폰 등) 사이의 터널 이고, Site-to-Site VPN은 두 게이트웨이 사이의 터널입니다(이 가이드는 Remote Access를 다룹니다).

터널의 바탕은 키를 관리하는 **IKE**, 암호화하는 **IPsec** 입니다. 신뢰의 바탕은 관리 서버에 내장된 인증 기관 **ICA** 가 발급하는 인증서입니다(소개, 인증).

연결 모드 — Office Mode·Visitor Mode

원격 클라이언트는 IP·프로토콜 문제로 연결이 까다로울 수 있어, **VPN 연결 모드** 로 이를 넘깁니다. **Office Mode** 는 원격 클라이언트에게 내부망의 IP를 캡슐화해 줘, 마치 사무실에 있는 것처럼 트래픽을 보내 게 합니다(Office Mode). **Visitor Mode** 는 모든 프로토콜을 443 포트의 일반 TCP 연결로 터널링 해, HTTP/HTTPS만 허용되는 환경(호텔 등)에서도 접속하게 합니다.

클라이언트의 종류

클라이언트는 크게 나뉩니다 — **Client-Based**(엔드포인트에 설치, 대부분 자원 접근), **Clientless**(웹 브라우저·HTTPS, 주로 웹 자원), **On-demand**(브라우저로 접속 시 클라이언트 자동 설치) 입니다. 또 **Secure Connectivity**(트래픽 암호화, 모든 솔루션 제공) 만 주는 것과 **Endpoint Security**(Desktop Firewall 등으로 단말 보호) 까지 주는 것으로 나뉩니다(솔루션과 클라이언트).

단말 보안 용어

원격 단말을 지키는 기능이 둘 있습니다. **Desktop Security** 는 클라이언트에 Desktop Firewall 정책(Desktop Rule Base)을 적용 해 단말을 방화벽으로 보호하고(Desktop Security), **SCV(Secure Configuration Verification)** 는 원격 단말이 보안 정책에 맞게 구성됐는지 검증 해, 미준수 단말의 접근을 제한합니다(SCV).

고급 기능 용어

운영·확장을 돕는 기능이 여럿입니다 — **Machine Certificate**(기기 인증서), **L2TP**(L2TP 클라이언트 지원), **VPN Routing**(Hub Mode 등 라우팅), **MEP**(여러 진입점 고가용성), **Secondary Connect**(여러 게이트웨이 자동 연결), **SAML**(클라우드 ID 공급자 인증), **Dynamic Split Tunneling**(SaaS 트래픽을 터널에서 제외), **strongSwan**(IKEv2 오픈소스 클라이언트 지원) 이 뒤 장들에서 이어집니다.

02 Check Point VPN 소개

Check Point VPN 소개

Remote Access VPN 은 원격 사용자와 내부망 사이에 암호화 터널을 만들 어, 직원이 다양한 장소·기기에서 민감 정보에 접근할 때 그 접근이 보안 취약점이 되지 않게 합니다. 이 장은 VPN의 토대와 원격 접속의 큰 그림을 잡습니다.

IPsec VPN의 토대

IPsec VPN 솔루션은 게이트웨이가 다른 게이트웨이·클라이언트와 주고받는 트래픽을 암호화·복호화 합니다. 터널은 인증·기밀·무결성 을 보장하며, 키 관리는 **IKE**, 암호화는 **IPsec** 이 맡습니다(Site-to-Site VPN 가이드의 IPsec·IKE에서 자세히). **Mobile Access 블레이드** 는 이 Remote Access 기능을 더 많은 클라이언트·배포 형태 로 넓힙니다.

연결의 걸림돌과 연결 모드

원격 클라이언트는 IP·프로토콜 때문에 연결이 까다로울 수 있습니다 — 클라이언트 IP를 미리 알 수 없거나, 호텔 LAN의 사설 IP 뒤에 있거나, 지원되지 않는 프로토콜 을 써야 하는 경우입니다. 이를 **VPN 연결 모드** 로 넘깁니다.

Office Mode 는 라우팅 문제를 풀 어 줍니다 — 원격 사용자에게 내부망의 가용 IP를 캡슐화해 줘, 사무실에 있는 것처럼 트래픽을 보내 게 합니다(Office Mode). **Visitor Mode** 는 HTTP/HTTPS만 허용되는 곳에서, 모든 프로토콜을 443 포트의 일반 TCP로 터널링 해 접속하게 합니다.

구성요소와 연결 수립

VPN은 **엔드포인트**(게이트웨이·클러스터·원격 클라이언트), **신뢰 주체**(ICA 인증 기관), **관리 도구**(관리 서버·SmartConsole) 로 이뤄집니다.

연결은 이렇게 맺어집니다. 원격 사용자가 게이트웨이에 연결을 시작 → IKE 협상에서 서로의 신원을 인증(인증서·사전 공유 비밀·서드파티 PKI 등) → 성공하면 VPN 터널 수립 . 이후 클라이언트와 게이트웨이의 VPN 도메인(뒤 LAN) 사이 모든 연결이 IPsec으로 암호화 되며, 인증을 묻는 순간을 빼면 이 과정은 사용자에게 투명합니다.

!원격 사용자와 게이트웨이의 연결 *① Host 1(VPN Site 1) ② VPN Gateway 1 ③ 인터넷 ④ 원격 클라이언트 ⑤ VPN Gateway 2(Site 2) ⑥ LDAP 서버(Site 2)*

위 예처럼 사용자 관리는 VPN DB가 아닌 LDAP 서버 가 맡을 수 있어, 게이트웨이가 LDAP에 사용자 존재를 질의해 인증합니다. 실제 구성은 시작하기에서 이어집니다.

03 시작하기

시작하기

직원에게 원격 접속을 열어 주는 큰 흐름은 세 걸음 입니다 — IPsec VPN 블레이드 켜고 기본 구성, 게이트웨이를 Remote Access 커뮤니티에 추가, 사용자를 커뮤니티에 포함. 이 장은 그 흐름을 정리합니다.

작업 흐름

전체 흐름은 이렇습니다. ① 게이트웨이에서 IPsec VPN 블레이드를 켜고 기본 구성 → ② 게이트웨이를 **Remote Access VPN Community** 에 추가 → ③ 사용자를 그 커뮤니티에 포함 합니다.

기본 게이트웨이 구성

게이트웨이를 만드는 절차는 Site-to-Site VPN과 같습니다 — 게이트웨이/클러스터 설치·인터페이스 구성 → SmartConsole에서 객체 생성 → **SIC** 신뢰 수립 → 인터페이스·토폴로지 취득 . 그다음 **General Properties** > **Network Security** 에서 **IPsec VPN** 을 선택 합니다.

사용자 포함과 인증

Remote Access는 누가 접속할지(사용자) 가 핵심입니다. 사용자는 SmartConsole의 사용자 DB에 직접 만들거나, **LDAP Account Unit**(Active Directory 등)로 가져 옵니다. 사용자 그룹 객체를 만들어 Remote Access VPN Community의 참여자 로 넣고, 방화벽 규칙에서 이 그룹으로 접근을 통제합니다.

인증 방식은 다양합니다 — 인증서, 사전 공유 비밀, 그 밖의 방법 중에 고르며, 자세한 내용은 사용자·클라이언트 인증에서 다룹니다.

다음 단계

기본을 세운 뒤에는 정책 구성으로 VPN 접근 규칙 을 만들고, 클라이언트 선택(솔루션과 클라이언트), Office Mode로 IP 문제 해결, Desktop Security·SCV로 단말 보호 같은 기능을 더해 갑니다. 이어지는 장들이 이를 하나씩 풀어 씁니다.

04 Remote Access 솔루션과 클라이언트

Remote Access 솔루션과 클라이언트

Check Point의 원격 접속 솔루션은 종류가 많습니다. 이 장은 어떤 기준으로 클라이언트를 고르고, 어떤 클라이언트가 무엇에 맞는지 를 정리합니다. 모두 기업급 보안 연결·강력한 사용자 인증·세밀한 접근 제어 를 제공하지만, 기능과 용도가 다릅니다.

고를 때의 두 가지 기준

첫째는 **Client-Based vs Clientless** 입니다 — **Client-Based**(엔드포인트에 Check Point 클라이언트 설치, 대부분 자원 접근), **Clientless**(웹 브라우저만, 주로 웹 자원), **On-demand**(브라우저 접속 시 클라이언트 자동 설치) 로 나뉩니다. 모든 클라이언트는 NAT·핫스팟·프록시(공항·호텔 같은 복잡한 토폴로지)를 통과 할 수 있습니다.

둘째는 **Secure Connectivity vs Endpoint Security** 입니다. **Secure Connectivity** 는 트래픽 암호화와 강력한 인증(모든 솔루션 제공, 동시 접속 사용자 수 기준 라이선스) 이고, 여기에 더해 **Security Verification**(단말이 보안 요건을 충족하는지 검증, SCV) , **Desktop Firewall**(중앙 관리 정책으로 단말을 상시 보호, Desktop Security) , 그리고 anti-malware·디스크 암호화 같은 추가 Endpoint Security 를 주는 솔루션도 있습니다(설치 클라이언트 수 기준 라이선스).

대표 클라이언트

쓰임새별 대표 클라이언트는 이렇습니다.

가장 강력한 것이 **Endpoint Security VPN**(SecureClient 후속)입니다 — IPsec VPN + Security Verification + 통합 Desktop Firewall(중앙 관리) 을 주는, 중·대규모 기업용 Windows/macOS 클라이언트입니다. **Check Point Mobile for Windows** 는 Endpoint Security 정책이 필요 없는 환경 에 맞는 IPsec 클라이언트(Secure Connectivity + Security Verification)이고, **SecuRemote** 는 무료지만 기능이 제한된 기본 IPsec 클라이언트입니다.

클라이언트 없이 쓰는 **Mobile Access Web Portal**(Clientless SSL)과, 브라우저로 자동 설치되는 **SSL Network Extender**(On-demand, Network Mode는 관리자 권한 필요 ·Application Mode는 불필요)도 있습니다. 모바일용으로는 **Capsule Workspace**(앱 안 업무 데이터만 보호, SSL), **Capsule Connect/VPN**(전체 L3 터널) 등 iOS·Android 클라이언트가 있고, **Endpoint Security Suite** 는 방화벽·디스크 암호화·anti-malware를 한 콘솔에서 통합 관리하면서 Remote Access VPN을 함께 제공합니다.

대부분 클라이언트는 게이트웨이에 **Mobile Access** 또는 **IPsec VPN** 블레이드 라이선스 가 필요하며, 최신 버전·세부는 sk67820에 정리되어 있습니다. 정리하면, 단말 보안까지 필요하면 Endpoint Security VPN, 연결만 필요하면 Mobile/SecuRemote, 웹 자원 위주면 Clientless 포털 식으로 환경에 맞춰 고르고, 여러 솔루션을 함께 쓸 수도 있습니다.

05 정책 구성

정책 구성

게이트웨이와 사용자를 준비했다면, 원격 접속을 허용하는 정책 을 구성합니다. 이 장은 그 큰 줄기를 정리합니다.

Step 1 — 게이트웨이/클러스터 객체

먼저 시작하기에서 본 대로 게이트웨이를 준비합니다 — 게이트웨이/클러스터 설치·인터페이스 구성 → SmartConsole에서 객체 생성 → **SIC** 신뢰 수립 → 인터페이스·토폴로지 취득 . 이 객체에서 IPsec VPN 블레이드를 켜 둡니다.

Remote Access 커뮤니티와 규칙

원격 사용자가 접근하려면 게이트웨이가 **Remote Access VPN Community** 에 속하고, 사용자(그룹)가 그 커뮤니티의 참여자 여야 합니다(시작하기).

그다음 Access Control 정책에 VPN 접근 규칙 을 만듭니다. Site-to-Site VPN과 마찬가지로, 규칙이 Remote Access 커뮤니티에 적용되게 하려면 Rule Base의 **VPN 열** 에 Remote Access 커뮤니티(또는 Any)를 넣 고, 출발지에 사용자 그룹(Access Role)을, 목적지에 내부망을, Action에 Accept를 둡니다. Identity Awareness를 함께 쓰면 사용자·그룹 단위로 더 세밀하게 제어할 수 있습니다.

규칙을 짠 뒤 정책을 설치하면, 인증된 원격 사용자가 허용된 내부 자원에 암호화 터널로 접근하게 됩니다. 인증 방식의 세부는 사용자·클라이언트 인증에서, IP·라우팅 문제 해결은 Office Mode·VPN Routing에서 다룹니다.

06 사용자·클라이언트 인증

사용자·클라이언트 인증

원격 접속에서 인증은 안전한 통신 채널의 핵심 입니다. 이 장은 게이트웨이와 원격 클라이언트가 서로를 인증하는 방식을 정리합니다.

인증 방식

게이트웨이와 클라이언트 사이의 인증에는 여러 방식이 있습니다 — 디지털 인증서, 사전 공유 비밀(pre-shared secret), 그 밖의 방법 입니다. Mobile Access·IPsec VPN 게이트웨이에서는 여러 로그인 옵션을 구성 할 수 있고, 옵션은 게이트웨이마다·Software Blade마다 다르게 둘 수 있습니다. 사용자는 가용 옵션 중 하나를 골라 지원되는 클라이언트로 로그인합니다(어떤 인증 방식을 지원하는지는 클라이언트별 문서 참고).

디지털 인증서

가장 강력한 방식이 **디지털 사용자 인증서** 입니다. Site-to-Site VPN의 PKI에서 본 것처럼, 관리 서버의 **ICA(Internal Certificate Authority)** 가 발급한 인증서 로 사용자를 인증하거나, 외부 PKI 솔루션의 인증서 를 쓸 수 있습니다. IKE 협상 중 클라이언트가 게이트웨이의 신원을, 게이트웨이가 사용자의 신원을 검증 합니다(소개).

기기 단위 인증서는 Machine Certificate에서, 클라우드 ID 공급자 기반 인증은 SAML에서 다룹니다.

여러 로그인 옵션

R82에서는 한 게이트웨이에 여러 로그인 옵션을 정의 해, 사용자가 상황에 맞는 방식(인증서·사용자명/암호·SAML 등)을 고르게 할 수 있습니다. 이렇게 유연한 인증 으로 다양한 클라이언트·사용자 환경을 아우릅니다.

정리하면, Remote Access 인증의 토대는 ICA·외부 PKI 기반 인증서와 사전 공유 비밀 이며, 거기에 SAML 같은 현대적 방식과 여러 로그인 옵션 을 더해 환경에 맞게 구성합니다.

07 Office Mode

Office Mode

원격 클라이언트가 사무실에 있는 것처럼 내부망에 녹아들게 하는 기능이 **Office Mode** 입니다. 원격 접속의 고질적인 IP 문제를 푸는 핵심 기능입니다.

왜 필요한가

원격 클라이언트는 보통 ISP가 준 로컬 IP(때로 NAT 뒤의 사설 IP) 로 접속합니다. 이 때문에 여러 문제가 생깁니다.

일부 프로토콜·자원이 내부 IP를 요구 합니다 — 라우터 ACL이 특정·내부 IP만 허용하도록 설정돼 있으면, 원격 클라이언트의 IP를 미리 알 수 없어 맞추기 어렵습니다. 또 사설 IP가 사내 LAN의 IP와 충돌 하거나, 두 원격 사용자가 같은 IP를 받아 충돌할 수 있습니다. 예를 들어 클라이언트가 `10.0.0.1` 을 받았는데 사내에 같은 IP의 호스트가 있으면, 복호화 후 패킷이 (Anti-Spoofing에 걸려) 드롭될 수 있습니다.

Office Mode가 푸는 방법

Office Mode 는 IP 패킷을 내부망의 가용 IP로 캡슐화 합니다. 즉 원격 클라이언트에게 내부망에서 라우팅 가능한 IP를 하나 배정 해, 사무실에 있는 것처럼 트래픽을 보내 게 합니다. 그러면 충돌·라우팅 문제 없이 내부 자원에 접근할 수 있습니다.

이 배정된 IP 덕분에 라우터 ACL·내부 서버가 클라이언트를 정상적인 내부 호스트로 인식 하고, 서버의 응답도 올바른 주소로 돌아옵니다. Office Mode는 VPN Routing·MEP 같은 고급 기능의 토대가 되며, IP 배정 방식(풀·DHCP·사용자별 등)과 세부 구성은 원문 해당 절을 참고하세요. 정리하면, Office Mode는 원격 클라이언트에게 내부 IP를 줘 "사무실 안 단말"처럼 만드는 원격 접속의 핵심 기능입니다.

08 Desktop Security

Desktop Security

원격 클라이언트는 보호된 네트워크 밖에 있어 게이트웨이의 검사를 받지 못하므로 공격에 취약 합니다. 게다가 공격자가 취약한 원격 클라이언트를 통해 VPN 터널로 내부망에 침투 할 수도 있습니다. **Desktop Security** 는 이를 막습니다.

Desktop Security 솔루션

Endpoint Security VPN처럼 Desktop Security를 포함하는 클라이언트는 클라이언트 자체에 Desktop Security Policy를 적용해 방화벽 보호 를 합니다. 관리자가 SmartDashboard의 **Desktop Rule Base** 에 정책을 정의 하고, 특정 사용자 그룹이나 전체 사용자에게 규칙을 배정합니다.

동작 흐름은 이렇습니다 — 관리 서버가 Desktop Security Policy를 **Policy Server**(원격 접속 게이트웨이에서 켜는 기능)로 내려보내 고, 원격 클라이언트가 게이트웨이에 연결할 때 Policy Server에서 자기 정책을 내려받 습니다. 클라이언트는 이 정책으로 출발지·목적지·서비스에 따라 연결을 accept·encrypt·drop 합니다.

> 참 고
>
> Endpoint Security VPN을 Endpoint Security Suite의 일부로 쓰면, 클라이언트 방화벽을 SmartDashboard의 Desktop Security에서 가져올지, SmartEndpoint에서 가져올지 정할 수 있습니다.

사용자가 방화벽을 끄게 허용하기

경우에 따라 사용자가 Desktop Firewall을 직접 끌 수 있게 허용할 수도 있습니다 (Letting Users Disable the Desktop Firewall). 다만 이는 단말 보호를 약화 시키므로 신중히 적용합니다.

정리하면, Desktop Security는 보호망 밖의 원격 단말에 중앙 관리 방화벽 정책을 입혀, 단말 자신과 그 단말을 통한 내부망 침투를 함께 막는 기능입니다. 단말이 정책에 맞게 구성됐는지까지 검증하려면 SCV를 함께 씁니다.

09 Secure Configuration Verification(SCV)

Secure Configuration Verification(SCV)

Desktop Security가 단말의 트래픽을 통제한다면, **SCV(Secure Configuration Verification)** 는 단말이 보안 정책에 맞게 "구성"됐는지 검증 합니다. 둘은 다른 종류의 위협을 막습니다.

왜 필요한가

사내 컴퓨터는 관리자가 Java·ActiveX 비활성, Anti-Virus 설치 같은 통제를 직접 할 수 있습니다. 하지만 LAN 밖의 원격 단말은 같은 도구로 통제할 수 없 습니다.

문제는 이렇습니다 — 원격 사용자가 ActiveX를 켜 둔 채 악성 ActiveX가 있는 사이트에 접속해 감염되면, 그 단말이 사내 LAN에 연결될 때 LAN까지 취약 해집니다. 이런 공격은 접근 제어의 허점이 아니라 단말 앱의 취약한 "구성"을 노리 므로, Desktop Security Policy로는 막을 수 없습니다.

SCV가 하는 일

SCV 는 원격 접속 클라이언트가 기업 보안 정책에 맞게 구성됐는지 확인 합니다. 원격 클라이언트의 구성 리포트를 받 고, 정책 준수 여부를 검증 해, 준수하지 않는 단말은 사내 자원 접근을 제한하거나 차단 합니다. 예를 들어 "Anti-Virus가 켜져 있는지, 위험한 브라우저 구성이 없는지"를 검사하는 식입니다.

기본과 고급

SCV는 기본 검증과 고급 검증(Secure Configuration Verification - Advanced)으로 나뉩니다. 기본은 흔한 보안 요건을 검사 하고, 고급은 더 정교한 검증 규칙(SCV 정책 파일·맞춤 검사) 을 구성합니다. 세부 검사 항목과 정책 파일 작성은 분량이 커서 원문 해당 절을 참고하세요.

정리하면, Desktop Security가 "단말의 트래픽을 어떻게 다룰지"라면, SCV는 "단말이 안전하게 구성됐는지"를 검증 해, 취약하게 구성된 단말이 VPN으로 사내망을 위협하는 것을 막습니다.

10 Machine Certificate·L2TP

Machine Certificate·L2TP

이 장은 기기 단위 인증(Machine Certificate) 과 L2TP 클라이언트 지원 을 묶어 다룹니다.

Machine Certificate — 기기 단위 인증

사용자 인증이 "누구냐"를 확인한다면, **Machine Certificate** 는 "어떤 기기냐"를 인증서로 확인 합니다. 기기에 발급한 인증서 로, 사용자 자격 증명과 별개로 승인된 기기에서만 접속 하게 하거나, 사용자 로그인 전에 기기 수준의 신뢰를 먼저 확인 하는 데 씁니다.

이를 활용하면 회사가 발급·관리하는 기기에서만 VPN 접속 을 허용하는 식으로 보안을 한 겹 더할 수 있습니다. 인증서의 바탕은 PKI/ICA와 같으며, 발급·배포 절차는 원문 해당 절을 참고하세요.

L2TP 클라이언트

L2TP(Layer 2 Tunneling Protocol) 클라이언트 지원으로, 운영체제에 내장된 L2TP/IPsec 클라이언트 로도 게이트웨이에 접속할 수 있습니다. Check Point 전용 클라이언트를 설치하기 어려운 환경에서, OS 기본 VPN 클라이언트(Windows·macOS 등)로 IPsec 터널 을 맺는 길을 열어 줍니다.

L2TP는 별도 클라이언트 설치 없이 표준 프로토콜로 접속한다는 장점이 있지만, Check Point 전용 클라이언트만큼의 Desktop Security·SCV 기능은 제공하지 않습니다. 구성(인증·IP 배정·정책)의 세부는 원문 해당 절을 참고하세요.

정리하면, Machine Certificate는 기기 신뢰를 더하고, L2TP는 OS 기본 클라이언트로 접속하는 길 을 여는, 인증·클라이언트의 두 보조 수단입니다.

11 VPN Routing·고급 구성

VPN Routing·고급 구성

이 장은 원격 접속의 VPN 라우팅(Hub Mode 등) 과 그 밖의 고급 구성 을 묶어 다룹니다.

VPN Routing의 필요

원격 클라이언트나 게이트웨이가 서로 직접 연결하지 못하는 상황이 있습니다. 예를 들어 두 DAIP 게이트웨이(동적 IP)는 상대 IP를 미리 몰라 직접 터널을 못 맺 고, 원격 클라이언트끼리(VoIP·NetMeeting 등)는 서로 직접 연결하지 못하고 게이트웨이를 거쳐야만 합니다.

Check Point의 해법 — Hub Mode

이를 푸는 것이 **VPN Routing** 입니다. 핵심은 **Hub Mode** — 모든 트래픽을 중앙 게이트웨이(hub)로 보내 거기서 라우팅 하는 방식입니다. 그러면 클라이언트끼리도 hub를 거쳐 통신 하고, 클라이언트의 인터넷 트래픽까지 hub를 거치게 해 검사·통제할 수 있습니다.

Hub Mode는 Office Mode와 맞물려 동작하며, 모든 트래픽을 사내 게이트웨이로 모아 보안 정책을 일괄 적용 한다는 점이 강점입니다. 다만 모든 트래픽이 hub를 거치므로 부하가 늘 수 있어, SaaS 트래픽은 Dynamic Split Tunneling으로 터널에서 빼 부하를 줄입니다.

고급 구성

Remote Access Advanced Configuration 에는 세밀한 동작을 조정하는 여러 항목 이 있습니다 — 연결 유지, 재인증 주기, 클라이언트 동작 제어, 백업 게이트웨이 등입니다. 대부분 게이트웨이 객체와 Global Properties의 Remote Access 설정 에 흩어져 있으며, 환경에 맞게 조정합니다(세부는 원문 해당 절 참고).

정리하면, VPN Routing(특히 Hub Mode)은 직접 연결이 안 되는 클라이언트·게이트웨이를 중앙을 거쳐 잇고 트래픽을 일괄 통제 하며, 고급 구성으로 세부 동작을 다듬습니다.

12 MEP·Secondary Connect

MEP·Secondary Connect

원격 접속의 가용성과 여러 게이트웨이 활용 을 위한 두 기능 — **MEP** 와 **Secondary Connect** — 를 묶었습니다.

MEP for Remote Access

MEP(Multiple Entry Point) 는 원격 접속 VPN에 고가용성·부하 분산 을 줍니다. Site-to-Site VPN의 MEP와 같은 개념으로, 같은 내부망에 접근할 수 있는 진입점 게이트웨이를 여럿 두어, 하나가 죽어도 다른 게이트웨이로 원격 사용자가 접속을 유지하게 합니다.

원격 접속에서는 특히 클라이언트가 여러 진입점 중 어느 게이트웨이로 연결할지 선택 하는 방식이 중요합니다 — 가장 가깝거나 응답이 빠른 게이트웨이를 고르거나, 우선순위에 따라 정합니다. 지리적으로 분산된 진입점 으로 가용성과 성능을 함께 높입니다.

Secondary Connect

Secondary Connect 는 사용자가 여러 게이트웨이의 자원에 매끄럽게 접근 하게 해 줍니다. 보통 클라이언트는 한 게이트웨이에 연결되는데, 다른 게이트웨이 뒤의 자원에 접근하려 하면 Secondary Connect가 자동으로 그 게이트웨이에도 연결 해 줍니다. 사용자는 여러 터널을 의식하지 않고 필요한 자원에 접근합니다.

정리하면, MEP는 진입점을 이중화해 가용성을, Secondary Connect는 여러 게이트웨이 자원에 자동 연결로 편의를 더하는 기능입니다. 둘 다 여러 게이트웨이 환경에서 원격 접속을 매끄럽게 만듭니다(세부 구성은 원문 해당 절 참고).

13 SAML·Dynamic Split Tunneling

SAML·Dynamic Split Tunneling

이 장은 현대적 원격 접속의 두 기능 — 클라우드 ID 공급자 인증(SAML) 과 SaaS 트래픽을 터널에서 빼는 Dynamic Split Tunneling 을 묶어 다룹니다.

SAML 인증

SAML Support for Remote Access VPN 으로, 클라우드 기반 SAML Identity Provider(IdP)의 신원을 인식 해 원격 접속을 인증할 수 있습니다. 사용자는 조직의 IdP(Azure AD·Okta 등)에서 인증 하고, 그 결과로 VPN에 접속합니다.

Identity Awareness의 SAML과 같은 흐름으로, 클라우드·온프레미스를 아우르는 SSO 를 원격 접속에 가져옵니다. R82 관리 서버에서 쓰려면 SmartConsole·게이트웨이가 R82(또는 R81.20 Titan 이상) 여야 합니다. 사용자 인증의 여러 로그인 옵션 중 하나로 SAML을 더해, 비밀번호 없이 IdP 인증으로 접속 하게 할 수 있습니다.

Dynamic Split Tunneling

Hub Mode에서는 모든 트래픽이 VPN 터널을 거쳐 게이트웨이로 가므로, Microsoft 365 같은 SaaS 트래픽까지 게이트웨이를 거쳐 부하 가 늘 수 있습니다. **Dynamic Split Tunneling** 은 SaaS 트래픽을 VPN 터널에서 제외 해 이를 덜어 줍니다.

동작은 Updatable Object를 활용합니다 — 관리자가 제외할 서비스를 지정 → 게이트웨이가 그 서비스의 IP를 인터넷에서 동적으로 가져와 클라이언트에 전달 → 클라이언트가 그 트래픽을 터널에서 제외 합니다. SaaS의 IP는 자주 바뀌므로 동적으로(Updatable Object) 최신 IP를 받아 정확히 제외하는 것이 핵심입니다.

정리하면, SAML은 클라우드 ID로 인증을 현대화하고, Dynamic Split Tunneling은 SaaS 트래픽을 터널에서 빼 게이트웨이 부하를 줄 이는, 요즘 환경에 맞춘 두 기능입니다.

14 strongSwan 클라이언트

strongSwan 클라이언트

strongSwan 은 널리 쓰이는 오픈소스 IPsec 클라이언트 입니다. Check Point는 IKEv2 기반 Remote Access에서 strongSwan 클라이언트를 지원 해, Check Point 전용 클라이언트 대신 표준 오픈소스 클라이언트로도 접속하게 합니다.

무엇을 지원하나

IKEv2를 쓰는 Remote Access 클라이언트는 strongSwan 클라이언트를 사용 할 수 있습니다. 이는 Linux 등에서 표준 오픈소스 IPsec 클라이언트로 Check Point 게이트웨이에 접속 하려는 환경에 유용합니다.

설치와 구성

설치는 strongSwan 공식 문서 의 안내를 따릅니다. 구성은 여러 부분으로 나뉘는데, 핵심은 인증서 설정 입니다 — `ipsec.conf` 파일에 인증서·연결 정보 를 적어 게이트웨이와 IKEv2 터널을 맺도록 구성합니다. 그 밖에 인증 방식·연결 파라미터를 strongSwan 설정 형식에 맞게 지정합니다(세부는 원문 해당 절과 strongSwan 문서 참고).

정리하면, strongSwan 지원은 Check Point 전용 클라이언트가 아닌 표준 IKEv2 오픈소스 클라이언트로도 원격 접속할 수 있게 열어 주어, 클라이언트 선택의 폭을 넓힙니다. 다만 전용 클라이언트가 주는 Desktop Security·SCV 같은 단말 보안 기능은 별도로 고려해야 합니다.

15 연결 문제 해결·CLI

연결 문제 해결·CLI

원격 접속 VPN이 안 될 때의 흔한 원인과 진단 , 그리고 명령줄 참조를 모았습니다.

연결 문제 해결

원격 접속 VPN의 연결 문제는 원인이 다양합니다.

가장 흔한 것이 **NAT** 입니다 — 클라이언트가 NAT·핫스팟·프록시 뒤에 있을 때 입니다. Check Point 클라이언트는 Visitor Mode(443 포트 TCP 터널링)로 HTTP/HTTPS만 허용되는 환경 을 넘고, **NAT Traversal(NAT-T)** 로 IPsec을 UDP 캡슐화 해 NAT를 통과합니다. Office Mode는 IP 충돌·라우팅 문제 를 풉니다.

그 밖에 인증서/인증 방식 불일치, 암호화 방법 불일치, SCV 미준수로 인한 접근 제한, 방화벽이 VPN 포트 차단 등이 원인이 됩니다. 진단은 클라이언트의 연결 로그, SmartConsole의 Logs & Events에서 VPN 로그(encrypt/decrypt 실패), 터널 모니터링 으로 합니다.

명령줄(CLI Commands)

원격 접속 VPN 운영 명령은 **R82 CLI Reference Guide** 에 정리되어 있습니다. Site-to-Site VPN과 마찬가지로 `vpn` 명령 으로 터널 상태·SA를 점검·진단하며, 클러스터에서는 모든 멤버를 똑같이 설정, Scalable Platforms에서는 Expert 모드에서 해당 Security Group 위에서 실행합니다.

정리하면, 연결이 안 되면 NAT(Office/Visitor Mode·NAT-T)·인증·암호화·SCV·방화벽 차단을 순서대로 점검 하고, 깊은 진단은 `vpn` 명령과 클라이언트 로그를 활용합니다. 전체 명령 구문은 R82 CLI Reference Guide가 담당합니다.