01 용어 정리

용어 정리

Mobile Access는 원격·모바일 사용자가 웹 브라우저나 가벼운 앱만으로 사내 자원에 안전하게 접속 하게 해 주는 Check Point 솔루션입니다. 이 가이드를 읽는 데 바탕이 되는 핵심 용어를, 백과사전식 나열 대신 이해의 흐름에 따라 풀어 둡니다.

Mobile Access의 두 기둥 — 블레이드와 포털

Mobile Access 는 Security Gateway에서 켜는 Software Blade 로, 관리·비관리 클라이언트 모두에게 Remote Access VPN을 제공합니다(약어 MAB). 이 블레이드를 켜면 게이트웨이마다 **Mobile Access Portal** 이 생기는데, 원격 사용자가 표준 HTTPS로 접속해 로그인하면 그 안에서 허용된 웹 앱·메일·파일 공유를 쓰는 클라이언트리스 관문 입니다. 즉 블레이드는 게이트웨이의 기능, 포털은 사용자가 보는 화면 이라고 보면 됩니다(소개, 포털).

접속 방식을 가르는 말들

클라이언트는 크게 **Client-Based**(엔드포인트에 설치, 대부분 자원 접근), **Clientless**(웹 브라우저·HTTPS, 주로 웹 자원), **On-demand**(브라우저 접속 시 클라이언트 자동 설치) 로 나뉩니다(솔루션). Mobile Access의 핵심은 Clientless·On-demand 쪽이며, 그 보강 장치가 **SSL Network Extender(SNX)** 입니다 — 포털에서 자동으로 내려받아져, 브라우저만으로는 어려운 native application(사내 서버의 IP 기반 응용)까지 암호화 SSL 터널로 이어 주는 온디맨드 클라이언트입니다. 모바일 기기에서는 **Capsule Workspace** 가 기기 안에 격리된 컨테이너를 만들어 사내 웹·파일·Exchange를 안전하게 쓰게 하고, **Capsule Connect/VPN** 은 전체 Layer 3 터널 을 엽니다.

인증과 권한

Authentication(인증) 은 "당신이 누구인지" 확인, **Authorization(권한 부여)** 은 "무엇에 접근할 수 있는지" 결정 입니다. 인증을 통과해야 포털에 들어오고, 권한에 따라 보이는 앱이 달라집니다(인증, 권한). 신뢰의 바탕은 관리 서버에 내장된 인증 기관 **ICA(Internal Certificate Authority)** 가 발급하는 인증서 이며, **DynamicID** 는 이메일·문자로 보내는 일회용 비밀번호(OTP)로 다중 인증 을 더합니다.

단말 상태를 검증하는 말들

Endpoint Compliance(Endpoint Security on Demand) 는 접속하려는 단말이 보안 기준(최신 Anti-Virus·활성 Firewall 등)에 맞는지 스캔 해, 미준수 단말의 접근을 막거나 제한합니다(Endpoint 준수). **Secure Workspace** 는 세션 동안 암호화된 가상 작업 공간을 만들고 종료 시 흔적을 지우는 Check Point 전용 가상 데스크톱입니다(단, R82 기준 단계적 지원 종료 예정). **Protection Level** 은 자원마다 요구하는 보안 수준(어떤 인증·준수 검사를 거쳐야 하는지) 으로, Permissive·Normal·Restrictive 세 가지가 미리 정의돼 있습니다.

정책과 기반 기능

Mobile Access 규칙은 **Unified Access Policy**(권장, Access Control 정책 안에서 Mobile Application 객체로 규칙 작성)와 **Legacy Policy**(SmartDashboard의 별도 Mobile Access 정책) 두 방식으로 운영합니다(권한). 이 모두를 받쳐 주는 게 **Security Gateway·Security Management Server·SmartConsole** 같은 Check Point 공통 구성요소이며, **IPS·Anti-Virus** 같은 다른 Software Blade가 Mobile Access 트래픽도 함께 지킵니다(블레이드 연동). Remote Access VPN·Identity Awareness·Security Gateway 가이드와 함께 보면 전체 그림이 잡힙니다.

02 Mobile Access 소개

Mobile Access 소개

직원은 어디서든 사내 메일·캘린더·업무 시스템에 접속하길 원하지만, 그 통로가 보안의 약점이 되어서는 안 됩니다. **Mobile Access** 는 바로 이 둘을 동시에 푸는 Check Point의 답입니다. 이 장은 Mobile Access가 무엇을 해 주고, 어떻게 관리되며, 서버·클라이언트 양쪽에서 어떤 보안을 제공하는지 큰 그림을 잡습니다.

Mobile Access가 하는 일

Mobile Access는 Check Point의 원격 접속 Software Blade로, 노트북이든 모바일 기기든 인터넷만 있으면 사내 애플리케이션에 안전하게 연결 하게 해 줍니다. Layer 3 VPN과 SSL VPN을 모두 지원하므로 메일·캘린더·연락처는 물론 일반 사내 응용까지 쓸 수 있고, 그 과정에서 네트워크와 단말을 위협으로부터 함께 보호 합니다.

> *Check Point Mobile Remote Access VPN Software Blade is the safe and easy solution to connect to corporate applications over the internet with your mobile device or PC.*
>
> — Mobile Access AdminGuide, "Introduction" (p.19)

사용자가 보는 얼굴은 **Mobile Access Portal** 입니다. 원격 사용자가 표준 HTTPS 요청으로 게이트웨이에 접속하면, 게이트웨이는 사용자 이름·비밀번호·인증서·SecurID 같은 방식으로 인증한 뒤 Mobile Access 정책에 따라 허용된 애플리케이션만 보여 줍니다. 모바일 기기에서는 **Check Point Mobile Apps**(Capsule Workspace 등)가 비관리 스마트폰·태블릿에서도 사내 자원에 암호화 통신을 열어 줍니다.

어떤 애플리케이션을 제공하나

Mobile Access는 여러 종류의 사내 응용을 원격 사용자에게 중계합니다. 가장 흔한 것이 브라우저로 접근하는 **Web application**(예: 재고·인사 관리 시스템처럼 같은 맥락의 URL 묶음) 이고, 네트워크 너머의 파일을 열고 쓰는 **file share**, 사내 XenApp 서버로 잇는 **Citrix** 연결도 지원합니다. 메일은 IMAP·SMTP를 지원하는 어떤 메일 서버든 앞단을 대신하는 내장 Web mail 과, Outlook Web Access(OWA)·IBM iNotes 같은 외부 웹메일 중계 두 갈래가 있습니다. 모바일 기기에는 웹 앱·메일/캘린더/연락처 접근과 다중 인증을 제공하며, 포털과 Capsule Workspace 접속에 대해서는 **IPv6** 인바운드 연결도 지원합니다(단 SNX는 IPv6 미지원). 그리고 브라우저만으로는 어려운 **native application**(사내 서버의 IP 기반 응용)은 Mobile Access가 **SSL Network Extender** 를 자동 실행해, 모든 트래픽을 암호화한 채 native 클라이언트로 잇게 합니다. 애플리케이션별 상세는 애플리케이션 장에서 다룹니다.

어떻게 관리하나

운영 부담을 줄이도록, Mobile Access는 별도 콘솔이 아니라 기존 Check Point 관리 체계 안에 녹아 있습니다. 모든 게이트웨이를 관리하는 Security Management Server가 Mobile Access 게이트웨이도 그대로 관리하고, 구성은 SmartDashboard의 Mobile Access 탭과 Access Control Rule Base에서 하며, Mobile Access 사용자·네트워크 객체는 SmartConsole에 나타납니다. 로그는 SmartConsole의 Logs & Events 뷰(SmartLog)에서 봅니다.

자주 나오는 개념

본문에 반복해서 등장하는 개념을 미리 짚어 둡니다. **Authentication(인증)** 은 사용자가 본인임을 하나 이상의 방식으로 증명하는 단계이고(인증), **Authorization(권한 부여)** 은 인증된 사용자가 실제로 어떤 사내 응용에 닿을 수 있는지를 정책으로 결정합니다(권한). **Endpoint Compliance Scanner**(Endpoint Security on Demand)는 접속 전 단말이 보안 정책에 맞는지 검사 하고(Endpoint 준수), **Secure Workspace** 는 세션 동안 암호화된 가상 데스크톱을 띄워 데이터 유출을 막고 종료 시 흔적을 지웁니다. **Protection Level**(Permissive·Normal·Restrictive)은 자원마다 요구하는 보안 수준이고, **Session** 은 인증 후 로그아웃·타임아웃까지 이어지는 통신 기간이며, 앞서 본 **SSL Network Extender** 가 native 응용 접근을 가능케 합니다.

서버·클라이언트 양쪽의 보안

Mobile Access 게이트웨이는 다른 Security Gateway와 똑같은 보안 기능을 그대로 누리면서, 원격 접속에 특화된 보호를 더 합니다. 서버 쪽에서는 **IPS**(특히 Web Intelligence 구성요소가 Cross-Site Scripting·버퍼 오버플로·SQL 인젝션·디렉터리 탐색 같은 웹 공격을 막음)와 **Anti-Virus** 가 Mobile Access 트래픽에도 적용됩니다(블레이드 연동). 클라이언트 쪽에서는 세밀한 권한 정책으로 누가 어떤 앱에 닿을지를 제한하고, 웹 앱 트래픽을 모두 HTTPS로 암호화 하며, 앞서 본 Endpoint Compliance와 Secure Workspace로 단말을 보호하고, 브라우저 캐싱 제어·쿠키 보관·다중 인증 같은 장치로 공용 PC에서의 정보 노출까지 줄입니다.

03 원격 접속 솔루션과 클라이언트

원격 접속 솔루션과 클라이언트

Check Point의 원격 접속 솔루션은 종류가 많고, Mobile Access는 그중 하나입니다. 이 장은 전체 원격 접속 지형 속에서 Mobile Access가 어디에 놓이는지, 어떤 기준으로 클라이언트를 고르는지를 정리합니다. 모든 솔루션이 기업급 보안 연결·강력한 사용자 인증·세밀한 접근 제어 를 주지만, 기능과 용도가 다릅니다. (원격 접속 전반은 Remote Access VPN 가이드에서 더 깊이 다룹니다.)

고를 때의 두 가지 기준

첫째 축은 **Client-Based vs Clientless** 입니다 — **Client-Based**(엔드포인트에 Check Point 클라이언트 설치, 대부분의 사내 자원 접근), **Clientless**(웹 브라우저·HTTPS만, 주로 웹 자원), **On-demand**(브라우저 접속 시 필요할 때 클라이언트 자동 설치) 로 나뉩니다. Mobile Access의 본령은 Clientless와 On-demand 쪽이며, 모든 Check Point 클라이언트는 IPsec·SSL 암호화를 쓰고 공항·호텔처럼 NAT·핫스팟·프록시가 얽힌 복잡한 토폴로지도 통과 합니다.

둘째 축은 **Secure Connectivity vs Endpoint Security** 입니다. **Secure Connectivity**는 클라이언트와 VPN 게이트웨이 사이 트래픽 암호화 + 강력한 인증(모든 솔루션이 제공, 동시 접속자 수 기준 라이선스) 이 기본이고, 여기에 **Security Verification**(접속 단말이 보안 요건을 충족하는지 검증, 미준수 시 접근 제한), **Desktop Firewall**(중앙 관리 정책으로 단말을 상시 보호 — 원격 단말은 보호망 밖이라 중요), 나아가 anti-malware·디스크 암호화 같은 추가 Endpoint Security까지 얹는 솔루션이 있습니다(설치 클라이언트 수 기준 라이선스).

대표 클라이언트 — 무엇을 언제 쓰나

쓰임새별 대표 클라이언트는 이렇게 정리됩니다.

클라이언트 없이 쓰는 핵심이 **Mobile Access Portal**(Clientless SSL)과, 브라우저로 자동 설치되는 **SSL Network Extender**(On-demand) 입니다. 모바일 기기에서는 **Capsule Workspace**(기기 안 격리 컨테이너에 업무 데이터만 보호, SSL)와 **Capsule Connect/VPN**(전체 Layer 3 터널) 이 iOS·Android용으로 제공됩니다. Capsule Connect/VPN과 모바일 클라이언트는 보통 게이트웨이에 **Mobile Access Software Blade** 라이선스를 필요로 합니다.

데스크톱·노트북에는 Layer 3 IPsec 클라이언트가 줄지어 있습니다. 가장 강력한 것이 **Endpoint Security VPN**(SecureClient 후속)으로, IPsec VPN + Security Verification + 중앙 관리 Desktop Firewall 까지 주는 중·대규모 기업용 Windows/macOS 클라이언트입니다(단 macOS판은 Desktop Firewall은 있지만 Security Verification은 없음). **Check Point Mobile for Windows** 는 Endpoint Security 정책이 필요 없는 환경에 맞는 IPsec 클라이언트(Secure Connectivity + Security Verification)이고, **SecuRemote** 는 무료지만 기능이 제한된 기본 IPsec 클라이언트입니다. 여러 단말 보안을 한 콘솔에서 통합 관리하려면 **Endpoint Security Suite**(Firewall·디스크 암호화·anti-malware 등 + Remote Access VPN 블레이드)를 씁니다. Windows 10·8.1용으로는 OS에 내장되거나 스토어에서 받는 **Capsule VPN·VPN Plugin**(SSL Layer 3) 같은 가벼운 클라이언트도 있습니다.

정리하면

단말 보안까지 필요하면 Endpoint Security VPN, 연결만 필요하면 Check Point Mobile/SecuRemote, 그리고 설치 없이 웹·메일 위주로 쓰려면 Mobile Access Portal·Capsule Workspace 식으로 환경에 맞춰 고르고, 한 조직 안에서 여러 솔루션을 함께 쓸 수도 있습니다. 각 클라이언트의 최신 버전·지원 OS·다운로드 위치·필요 라이선스의 세부는 sk67820에 한데 정리돼 있습니다.

04 시작하기 — 배포·워크플로·마법사

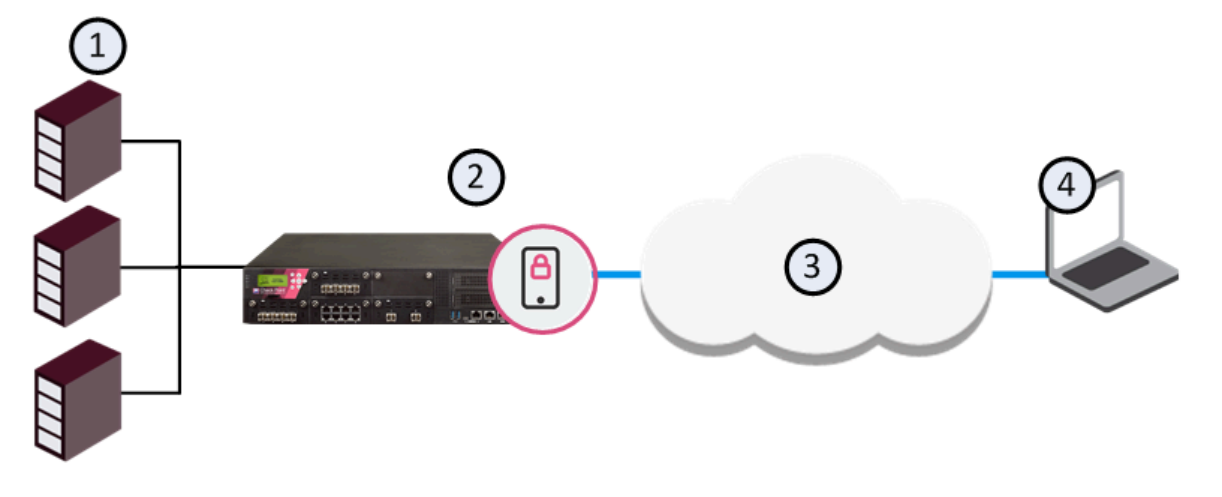
시작하기 — 배포·워크플로·마법사

Mobile Access를 실제로 켜는 과정은 생각보다 단순합니다. 이 장은 어디에 게이트웨이를 놓을지(배포), 어떤 순서로 구성할지(워크플로), 그리고 처음 켤 때 뜨는 마법사가 무엇을 묻는지 를 따라가며, 첫 포털을 띄우기까지의 길을 잡습니다.

어디에 배포하나

배포 방식은 조직 구조와 선호에 따라 여러 가지입니다.

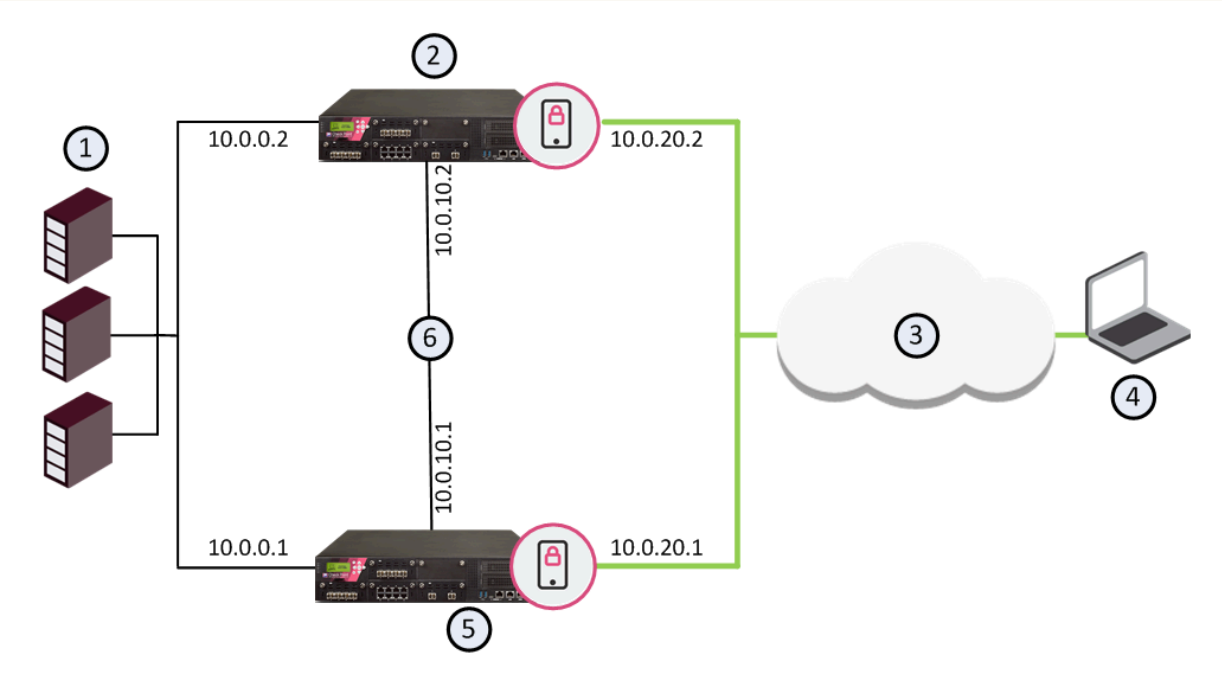
가장 간단하고 권장되는 형태가 **Simple Deployment** 입니다 — Mobile Access를 켠 게이트웨이 한 대가 Mobile Access를 포함한 모든 트래픽을 검사하며, IPS·Anti-Virus도 함께 적용합니다. 게이트웨이 한 대만 있으면 되니 가장 저렴하고 구성하기 쉽습니다.



① 내부 서버 ② Mobile Access를 켠 Security Gateway ③ 인터넷을 지나는 SSL 터널 ④ 원격 사용자 — 게이트웨이 한 대가 모든 트래픽을 검사하는 기본 배포

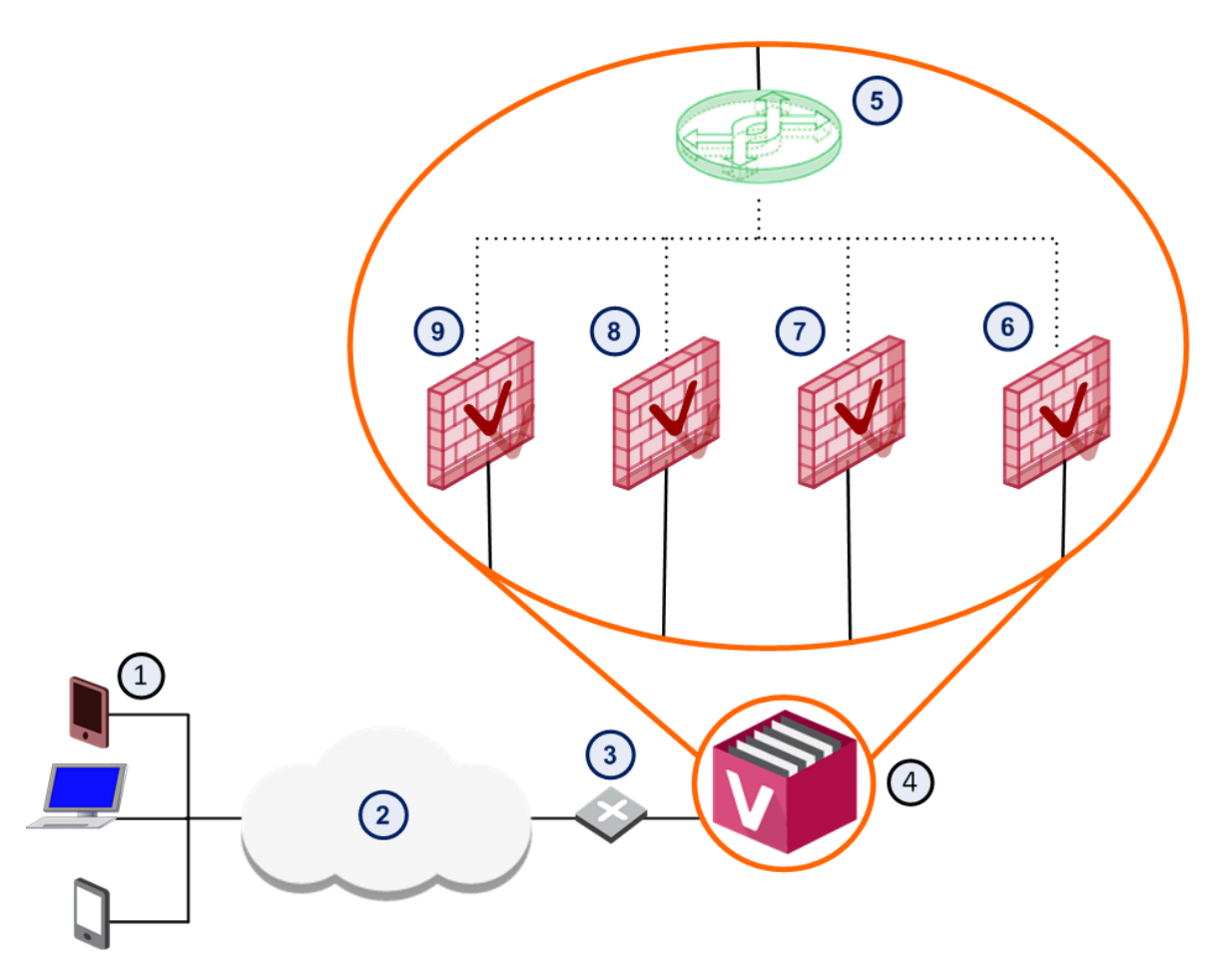
보안을 한층 높이려면 **DMZ 배포** 를 씁니다. Mobile Access 게이트웨이를 DMZ에 두면 인터넷과 LAN 양쪽에서 오는 트래픽이 모두 방화벽 제약을 받아, 인터넷에서 LAN으로의 직접 접근을 열 필요가 없 어집니다. 원격 사용자는 게이트웨이로 SSL 연결을 열고, 거기서 SSL 종료·IPS·Anti-Virus·인증·권한 부여가 이뤄진 뒤 게이트웨이가 내부 서버로 요청을 전달합니다.

동시 접속자가 많고 무중단 접속이 중요하다면 **Cluster 배포** 로 갑니다. ClusterXL로 Load Sharing이나 High Availability를 구성하면 한 멤버가 죽어도 다른 멤버가 세션을 이어받습니다(ClusterXL 가이드 참고).



① 내부 서버 ② cluster member B ③ 인터넷 ④ SSL로 접속하는 원격 사용자 ⑤ cluster member A ⑥ 동기화 전용 보안 네트워크 — 멤버 간 세션을 동기화하는 클러스터 배포

마지막으로 **VSX 배포** 가 있습니다. 한 VSX Gateway의 여러 Virtual System마다 서로 다른 애플리케이션·접근 정책·인증 요건·모바일 클라이언트를 가진 Mobile Access 포털을 따로 둘 수 있습니다. 예컨대 개발·영업·재무·협력사 팀별로 별도 포털 URL과 정책을 운영하는 식입니다(VSX 가이드 참고).



① 원격 사용자 ② 인터넷 ③ 라우터 ④ VSX Gateway ⑤ Virtual Switch ⑥~⑨ Mobile Access를 켠 Virtual System 4~1(팀별 포털 URL) — 한 장비에 팀별 독립 포털을 올리는 VSX 배포

이 밖에 게이트웨이를 Reverse Proxy로 동작시켜, 포털을 거치지 않고도 내부 서버를 외부에 노출하는 방식도 있습니다.

구성 워크플로

전체 구성은 다음 흐름을 따릅니다. SmartConsole에서 게이트웨이의 Mobile Access 블레이드를 켜면 구성 마법사가 뜨고, 거기서 모바일 클라이언트·포털·애플리케이션(예: OWA)·AD 서버를 정합니다. 그다음 정책 유형을 고르는데, 기본은 SmartDashboard에서 다루는 **Legacy Policy** 이고, 게이트웨이 속성의 Mobile Access에서 **Unified Access Policy** 를 선택하면 통합 정책에 포함됩니다. 정책에 규칙을 추가하고, 게이트웨이 속성 > Mobile Access > Authentication에서 인증을 설정한 뒤, Access Control 정책을 게이트웨이에 설치하면 사용자가 포털로 접속할 수 있습니다. 선택적으로 Capsule Workspace 앱에 인증서 인증으로 안전하게 접속하게 하려면, 인증 설정에서 클라이언트 인증서를 요구하고 인증서 생성·배포 마법사로 인증서를 나눠 줍니다.

Mobile Access 마법사가 묻는 것

블레이드를 켜면 실행되는 **Mobile Access Wizard** 는 선택된 원격 사용자에게 사내 웹·메일 앱 접근을 빠르게 열어 줍니다. 마법사는 먼저 사용자가 어디서 접속할지(Web 브라우저, Capsule Workspace/Capsule Connect 같은 모바일 앱, 또는 데스크톱/노트북 클라이언트)를 묻고, **포털 URL** 을 정하게 합니다(기본은 `https://<게이트웨이 IP>/sslvpn` 이며, 같은 IP의 모든 포털은 같은 인증서를 씁니다). 이어 노출할 **애플리케이션**(데모 웰드클락·사용자 정의 웹 앱·Exchange 메일/캘린더/연락처)을 고르고, **Active Directory** 도메인을 연결하며(쓰지 않으면 건너뜀), 접근을 허용할 **사용자·그룹** 을 선택합니다.

마법사가 끝나면 **What's Next?** 화면이 남은 일을 안내합니다 — Remote Access Community에 규칙 추가, 게이트웨이에 정책 설치(이걸 해야 마법사 변경이 적용됨), 그리고 `https://<IP>/sslvpn` 포털로 로그인 해 확인하는 일입니다. 데스크톱 VPN 클라이언트나 Capsule Connect를 쓰려면 마법사가 해당 게이트웨이를 자동으로 Remote Access VPN 커뮤니티에 넣고, 클라이언트는 방화벽 Rule Base에서 접근 규칙을 받습니다.

포털 설정과 정책의 기본

각 Mobile Access 게이트웨이는 자기만의 포털로 이어지며, 사용자는 그 게이트웨이에 설정된 인증 방식으로 로그인 합니다. HTTP로 들어오면 자동으로 HTTPS 포털로 넘어갑니다. 포털 URL과 모양새는 게이트웨이 속성의 Portal Settings·Portal Customization에서 조정하며, 세부는 포털 장에서 다룹니다.

정책은 **Unified Access Policy**(게이트웨이의 모든 규칙을 통합 정책에서 작성, 권장)와 **Legacy Policy**(SmartDashboard의 공유 Mobile Access 정책) 중 하나로 운영합니다. 어느 쪽이든 규칙에는 **사용자·그룹**(통합 정책에서는 Access Role), 사용자가 접근할 **애플리케이션**, 규칙이 적용될 **게이트웨이** 가 들어가며, 규칙에 VPN·Remote Access 클라이언트를 넣어 어떤 클라이언트로 접근할지도 지정할 수 있습니다. 다만 Mobile Access 정책은 Mobile Access Portal과 Capsule Workspace에만 적용되고, Desktop 클라이언트나 Capsule Connect에는 적용되지 않 습니다. 규칙 작성의 세부는 권한 부여와 접근 제어에서 이어집니다.

Capsule Workspace와 클라이언트 인증서 준비

모바일 기기를 Capsule Workspace로 접속시키려면, 게이트웨이에서 Mobile Access를 켜고 Mobile Devices·Capsule Workspace를 선택한 뒤 인증 방식을 정합니다. 필요하면 기기와 게이트웨이 사이 인증서를 관리하고, 모바일 앱 트래픽(Exchange·앱 서버 접근)을 허용하는 Access Control 규칙을 둡니다. 사용자는 App Store·Google Play에서 Capsule Workspace 앱을 받고, 관리자는 **Site Name** 과 (인증서 인증을 쓰면) **Registration key** 를 안내합니다. 인증서를 쓴다면 이 정보를 인증서 배포 이메일에 함께 담는 것이 좋습니다.

클라이언트 인증서 자체는 SmartConsole의 Security Policies > Access Control > Access Tools > Client Certificates에서 **Certificate Creation and Distribution wizard** 로 만들고 배포합니다. 모바일·태블릿 접속과 인증서 관리의 세부는 스마트폰·태블릿 접속 장에서 다룹니다.

05 Mobile Access Portal

Mobile Access Portal

Mobile Access Portal 은 원격 사용자가 보는 얼굴 입니다. 사용자는 여기에 로그인해 허용된 웹 앱·메일·파일을 쓰고, 관리자는 여기서 URL·인증서·외관·접근 범위를 조정합니다. 이 장은 포털의 일반 설정, R81부터 도입된 New Portal과 구버전 Legacy Portal, 그리고 신뢰받는 서버 인증서를 갖추는 길 을 정리합니다.

포털의 일반 설정

게이트웨이는 HTTPS 위에서 여러 웹 포털을 동시에 돌립니다 — Gaia Portal, Identity Awareness의 Captive Portal, DLP 포털, **Mobile Access Portal**, SSL Network Extender 포털, Reverse Proxy 포털, UserCheck 포털 등입니다. 이들은 모두 443 포트에서 IPv4·IPv6 호스트를 처리하며, TLS 1.1·1.2가 기본 활성 입니다(SSLv3·TLS 1.0도 지원하나 최소·최대 버전은 SmartDashboard의 Global Properties에서 조정 가능).

포털 URL 은 `https://<게이트웨이 IP>/sslvpn` 형태로, IP나 그 IP로 풀리는 FQDN으로 접속하며 HTTP는 자동으로 HTTPS로 넘어갑니다. Hostname Translation 방식의 링크 변환을 쓰면 FQDN이 필수 입니다. URL은 게이트웨이 속성 > Mobile Access > Portal Settings의 Main URL에서 바꾸고, Aliases로 `portal.example.com` 같은 별칭을 메인 URL로 리디렉트 할 수도 있습니다(별칭은 DNS에서 메인 URL로 풀려야 동작).

Portal Accessibility Settings 는 포털에 어디서 접근할 수 있는지를 토폴로지에 따라 정합니다 — 모든 인터페이스, 내부 인터페이스만, DMZ 포함, VPN 암호화 인터페이스 포함, 또는 방화벽 정책에 따라(누가 포털에 접근하는지 규칙으로 통제할 때) 중에서 고릅니다.

New Mobile Access Portal

R81부터 Check Point는 다른 Check Point 제품과 비슷한 인터페이스의 New Mobile Access Portal을 도입 했고, 블레이드를 켜면 이 새 포털이 기본입니다. Legacy 포털은 하위 호환용으로 남아 있습니다.

새 포털은 PHP 파일을 건드릴 필요 없이 **CSS만으로 외관을 커스터마이즈** 합니다. `$CVPNDIR/htdocs/includes/css/custom.css` 파일을 만들어 기본 CSS 값을 덮어쓰면 되고, 변경은 진행 중인 세션에 영향을 주지 않습니다. 로그인 페이지·메인 페이지 배경, 로그인 아이콘 교체, Check Point 로고 숨기기, 주소·경로 입력란 숨기기 같은 흔한 변경은 이 파일에 CSS 규칙을 더해 처리합니다. 자주 쓰는 커스터마이즈를 모은 **Demo Customization Package** 도 있어, `apply_custom_style.sh` 로 적용하고 `revert_custom_style.sh` 로 되돌립니다(패키지 안 이미지를 바꿀 때 파일 이름은 그대로 둘 것).

새 포털과 Legacy 포털 사이 전환은 게이트웨이에서 Expert 모드로 `$CVPNDIR/scripts/sslvpn_portal_toggle_ui.sh` 를 실행합니다.

> 주 의
>
> 포털 버전을 전환하면 활성 Mobile Access 세션이 모두 끊깁니다.

Legacy Portal과 사용자 워크플로

Legacy 포털은 게이트웨이 속성 > Mobile Access > Portal Customization에서 외관을 조정하며, 영어 외에 중국어·프랑스어·독일어·일본어·러시아어 등 여러 언어로 현지화 됩니다. `Main.virtualhost.conf`의 `CVPN_PORTAL_LANGUAGE_AUTO_DETECT` 플래그를 켜면 관리자 기본 언어보다 사용자 브라우저의 언어 설정을 우선 하고, 사용자가 포털에서 직접 고른 언어는 그 무엇보다 우선합니다.

사용자 입장의 흐름은 단순합니다 — 로그인하고 언어를 고른 뒤, 처음 쓰는 경우 native 응용용으로 ActiveX/Java 구성요소를 설치하고, 초기 설정을 거쳐 애플리케이션에 접근 합니다. Endpoint Compliance Scanner·Secure Workspace·SSL Network Extender는 첫 사용 시 ActiveX(Windows + Internet Explorer) 또는 Java 구성요소를 단말에 설치하며, 하나가 설치되면 나머지도 같은 방식으로 깔립니다. 인증 후에는 관리자가 구성하고 사용자가 권한을 가진 사내 애플리케이션이 포털에 펼쳐집니다.

> 참 고
>
> 일부 팝업 차단기가 포털 기능을 방해할 수 있으니, 사용자에게 Mobile Access 팝업을 허용하도록 안내하는 것이 좋습니다.

기본 포털 대신 그룹별로 다른 시작 페이지를 주려면 **Alternative Portal** 을 씁니다 — Mobile Access 정책에서 그 포털을 웹 애플리케이션으로 등록하고 접근할 그룹을 지정하며, 사용자가 여러 그룹에 속하면 정렬된 규칙처럼 첫 일치 그룹의 포털로 안내됩니다.

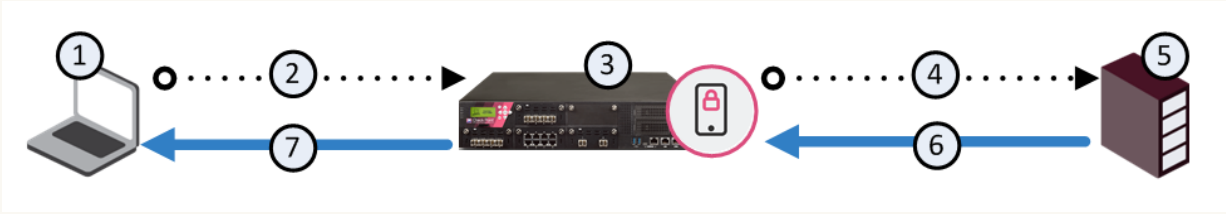
서버 인증서 — 브라우저 경고 없애기

게이트웨이는 기본적으로 관리 서버의 ICA가 만든 인증서를 쓰는데, 브라우저는 이를 신뢰하지 않아 경고가 뜹니다. 경고를 없애려면 Entrust·VeriSign·Thawte 같은 알려진 CA가 서명한 서버 인증서를 설치 해야 합니다(같은 IP의 모든 포털은 같은 인증서 공유). 절차는 크게 세 단계입니다 — 첫째 게이트웨이에서 `cpopenssl req` 로 **CSR(인증서 서명 요청)** 과 개인 키를 만들어 CA에 보내고(Common Name에 FQDN 필수), 둘째 서명받은 인증서와 개인 키를 `cpopenssl pkcs12 -export` 로 **P12 파일** 로 묶으며(전체 인증서 체인이 루트 CA까지 이어지도록), 셋째 SmartConsole의 Portal Settings에서 그 인증서를 Import합니다.

Hostname Translation을 쓴다면 사내 웹 앱이 서브도메인마다 다른 호스트명으로 번역되므로, 한 장 인증서로는 경고가 나 **와일드카드 인증서** 가 필요합니다. CSR의 Alternate Name에 FQDN과 `*.도메인` 을 함께 넣거나, `openssl.cnf` 의 `subjectAltName` 에 와일드카드를 추가해 생성합니다.

데이터 압축과 클러스터 동작

Mobile Access는 웹 콘텐츠를 압축해 더 빠른 사이트와 더 적은 대역폭 을 줄 수 있습니다 (다만 CPU 사용은 늘어남). gzip·deflate·compress 방식을 지원하며, GuiDBEdit 도구에서 게이트웨이별로 `enable_web_compression` · `compression_level` (1~9, 기본 5) 등을 설정합니다.



① 웹 브라우저 ② 압축된 요청 ③ Mobile Access 게이트웨이 ④ 압축 해제된 요청 ⑤ 웹 서버 ⑥ 응답 ⑦ 압축된 응답 — 게이트웨이가 서버 응답을 압축해 클라이언트로 보내는 흐름

클러스터로 운영하면 멤버 간 세션·상태를 보안 동기화 네트워크로 공유해, 한 멤버가 죽어도 무중단 페일오버 를 제공합니다. **SSL Network Extender를 쓴다면 Sticky Decision Function을 반드시 켜야** 하는데, 이는 한 클라이언트 IP의 연결이 항상 같은 멤버를 거치게 묶어 줍니다. 페일오버 시 사용자 체감은 응용마다 다릅니다 — 웹 브라우징·파일 공유·Secure Workspace는 대체로 끊김을 모르고(링크 클릭 중이면 새로고침 필요할 수 있음), Citrix는 세션이 끊겨 재접속해야 하며, SNX Network Mode는 잠깐 멈췄다 이어지지만 Application Mode는 터널 위 응용 연결이 끊깁니다.

06 Mobile Access 애플리케이션

Mobile Access 애플리케이션

Mobile Access의 가치는 결국 사용자가 포털 안에서 어떤 사내 응용을 쓸 수 있느냐 에 있습니다. 이 장은 클라이언트리스로 제공되는 응용의 종류(웹 앱·파일 공유·Citrix·웹메일), 인터넷용 링크로 바꿔 주는 Link Translation, 그리고 한 번 로그인으로 여러 응용을 쓰게 하는 Single Sign-On 을 정리합니다. (스마트폰·태블릿 전용 메일 응용은 스마트폰·태블릿 장에서 따로 다룹니다.)

클라이언트리스 응용을 정의한다는 것

원격 사용자에게 내부망을 여는 것은 곧 외부 위협에 노출시키는 일이라, 연결성과 보안 사이의 균형 이 핵심입니다. 그래서 응용을 정의한다는 것은 곧 어떤 사내 응용을, 어떤 종류의 원격 사용자에게 노출할지를 결정 하는 일입니다. Mobile Access는 웹 애플리케이션·파일 공유·Citrix 서비스·웹메일·native 응용을 제공합니다.

가장 흔한 것이 **Web application** 으로, 같은 맥락에서 브라우저로 접근하는 URL 묶음(재고·인사 관리 등)입니다. HTML·JavaScript 사이트는 그대로 지원하지만, VBScript·Java·Flash로 임베디드 링크를 다루는 사이트나 기본 브라우저로만 동작하는 사이트는 native application으로 정의해 SSL Network Extender로 처리 해야 합니다. 웹 앱은 특정 유형으로도 지정할 수 있는데, **iNotes**(IBM Domino Web Access)와 **Outlook Web Access(OWA)** 가 그것입니다. 이들은 클라이언트 측 캐싱이 필요해 일부 Web Intelligence 보호(XSS·command/SQL injection)가 해제되며, OWA는 `/exchange/` · `/owa/` · `/public/` 같은 디렉터리가 허용 경로로 설정됩니다.

응용 객체는 SmartConsole의 Object Explorer에서 New > Custom Application/Site > Mobile Application으로 만듭니다. 웹 앱 정의는 이름, 접근을 허용할 위치(호스트·디렉터리·서비스), 포털에 보일 링크, 그리고 Protection Level 로 이뤄집니다. URL·링크·툴팁에는 `$$user` 매크로를 넣을 수 있어, `http://host/$$user` 처럼 정의하면 사용자 aa에게는 `http://host/aa` 로, bb에게는 `http://host/bb` 로 개인화 됩니다(인증서 인증이면 인증서에서 추출된 이름으로 풀림).

응용마다 **Protection Level** 로 보안 요건을 더할 수 있습니다 — 기본은 게이트웨이 요건을 그대로 따르지만, 응용에 별도 Protection Level을 묶으면 포털 요건에 더해 그 응용만의 요건까지 충족해야 접근됩니다(Endpoint 준수). 또 **브라우저 캐싱** 도 여기서 제어합니다 — 공용 PC에서의 정보 노출을 막으려면 모든 콘텐츠 캐싱을 차단 할 수 있는데(단, 그러면 Word·PDF 같은 외부 뷰어용 파일은 못 열 수 있어 로컬 저장이 필요), Hostname Translation을 쓰면 모든 콘텐츠 캐싱 허용이 권장됩니다.

Link Translation — 내부 링크를 인터넷용으로

클라이언트리스 접속의 핵심 기술이 **Link Translation** 입니다. 사내 웹 서버가 돌려주는 내부 URL을, 인터넷에서 게이트웨이를 거쳐 닿을 수 있는 유효한 링크로 바꿔 줘야 하기 때문입니다. 방식은 세 가지로, **Path Translation**(신규 설치 기본), **URL Translation**(추가 구성 없이 지원), **Hostname Translation(HT)** 입니다. HT를 쓰면 클라이언트 브라우저에 `https://<가려진 호스트명>.<Mobile Access FQDN>/path` 형태의 난수 같은 호스트명이 보이고, 각 부분은 RFC 1034에 따라 63자로 제한됩니다. HT는 OWA 2013/2016에 최적이지만 '엔드포인트 쿠키 저장'을 켜야 하며, 와일드카드 서버 인증서가 필요합니다(포털).

성능을 위해 **Link Translation Domain** 을 직접 지정하는 것이 좋습니다 — 번역할 내부 도메인만 목록에 두면, 메일 속 외부 사이트 링크가 깨지지 않고 게이트웨이 부하도 줄어듭니다(기본은 모든 도메인 번역). 모바일 기기에서는 Check Point Mobile App이 보안 컨테이너에 감싼 **wrapped application** 의 링크 번역을 클라이언트가 맡으며, 이런 응용은 포털에 보이지 않습니다.

이 밖에 웹 앱에는 효율·보안을 위한 기능이 여럿 있습니다 — 3-way handshake를 줄여 성능을 높이는 **Reuse TCP Connections**(기본 활성), 표준 HTTP 인증을 못 쓰는 사내 응용에 사용자명·IP를 헤더로 전달하는 **CvpnAddHeader**, 응용별 HTTP/HTTPS 프록시 지정, 그리고 사전 설치 클라이언트 없이 브라우저로 RDP/VDI를 쓰게 하는 **WebSocket**(RFC 6455) 지원 등입니다(WebSocket 관련 웹 앱은 Path Translation을 써야 함).

파일 공유·Citrix

File share 는 네트워크 너머의 파일을 열고 읽고 쓰고 지우게 해 주는 응용 으로, 웹 앱과 비슷하게 허용 위치·경로를 정해 만듭니다. 경로에 `$$user` 를 넣어 사용자 홈 디렉터리를 가리키게 할 수 있습니다.

Citrix 는 사내 XenApp 서버로의 클라이언트 연결을 중계 합니다. 클라이언트리스로 Citrix 세션을 열어 주며, 페일오버 시에는 세션이 끊겨 사용자가 다시 연결해야 합니다.

Single Sign-On — 한 번 로그인으로

Single Sign-On(SSO) 은 사용자가 응용마다 다시 자격 증명을 입력하지 않도록, 포털 로그인 자격을 응용에 자동 전달 하는 기능으로, 응용 보안과 사용자 편의를 함께 높입니다. 사용자가 어떤 응용에 처음 자격을 입력하면 Mobile Access가 이를 안전하게 저장해 두었다가, 같은 응용에 다시 접근할 때 대신 채워 줍니다. 다만 일부 조건에서는 SSO가 지원되지 않으니, 적용 전 대상 응용의 동작을 확인하는 것이 좋습니다.

웹 애플리케이션 구성을 마치려면 정의한 응용을 정책 규칙에 넣고 정책을 설치합니다 — Unified Access Policy 또는 Legacy 정책 방식 중 환경에 맞는 쪽을 따르며, 응용별 캐싱·헤더·프록시 같은 세부는 원문 해당 절과 관련 sk(예: 프록시 sk34810, WebSocket sk95311)를 참고합니다.

07 사용자 인증과 세션 관리

사용자 인증과 세션 관리

포털에 들어와 응용을 쓰려면 먼저 사용자가 본인임을 증명 해야 합니다. 이 장은 Mobile Access가 지원하는 인증 방식, 한 게이트웨이에 여러 로그인 옵션을 두는 Multiple Login Options, 클라우드 ID 공급자와 잇는 SAML, 일회용 비밀번호 DynamicID로 더하는 다중 인증, 그리고 로그인 이후의 세션 관리 까지를 정리합니다.

어떤 방식으로 인증하나

인증(Authentication)은 사용자가 자신이 주장하는 그 사람인지 확인 하는 단계입니다. SmartDashboard에 정의된 사용자는 다음 중 하나 이상으로 게이트웨이에 인증합니다 — 사용자 이름·비밀번호, 클라이언트 인증서(ICA 또는 제3자 OPSEC CA 발급), RADIUS 서버, SecurID(RSA의 토큰 기반), 그리고 1차 인증 뒤에 더하는 **DynamicID 일회용 비밀번호 (OTP)** 입니다. 이 밖에 사용자 레코드에 인증 방식을 박아 두는 Legacy Authentication도 있습니다. 게이트웨이에 설정되지 않은 방식으로 인증을 시도한 사용자는 접근이 거부 됩니다.

Multiple Login Options — 여러 로그인 옵션

한 게이트웨이에 여러 로그인 옵션을 두어, 사용자가 그중 하나를 골라 로그인 하게 할 수 있습니다(Mobile Access·IPsec VPN 모두, 게이트웨이·블레이드·클라이언트별로 다르게). 각 옵션은 여러 게이트웨이에서 재사용하는 전역 객체 라, 한 번 만들면 여러 곳에 적용됩니다. 기본 옵션으로 Personal_Certificate(인증서), Username_Password(이름·비밀번호), Cert_Username_Password(둘 다)가 있습니다.

옵션 하나는 하나 이상의 인증 요소(Factor)와 그 설정의 묶음 입니다 — 예컨대 SecurID를 고르면 SecurID 서버와 토큰 카드 유형을, Personal Certificate를 고르면 어느 인증서 필드에서 사용자명을 뽑을지(**Certificate Parsing**, 기본 DN, 이메일·일련번호도 가능)를 정합니다. 옵션의 순서도 정하는데, Personal Certificate를 포함하면 반드시 첫 번째여야 하고, DynamicID는 첫 번째일 수 없 습니다. 각 옵션은 Mobile Access Portal·Capsule Workspace 중 어디서 보일지도 지정하며, **Customize Display** 로 로그인 화면의 제목·입력란 설명을 사용자가 이해하기 쉬운 말(예: "AD 사용자명", "이메일 주소")로 바꿀 수 있습니다.

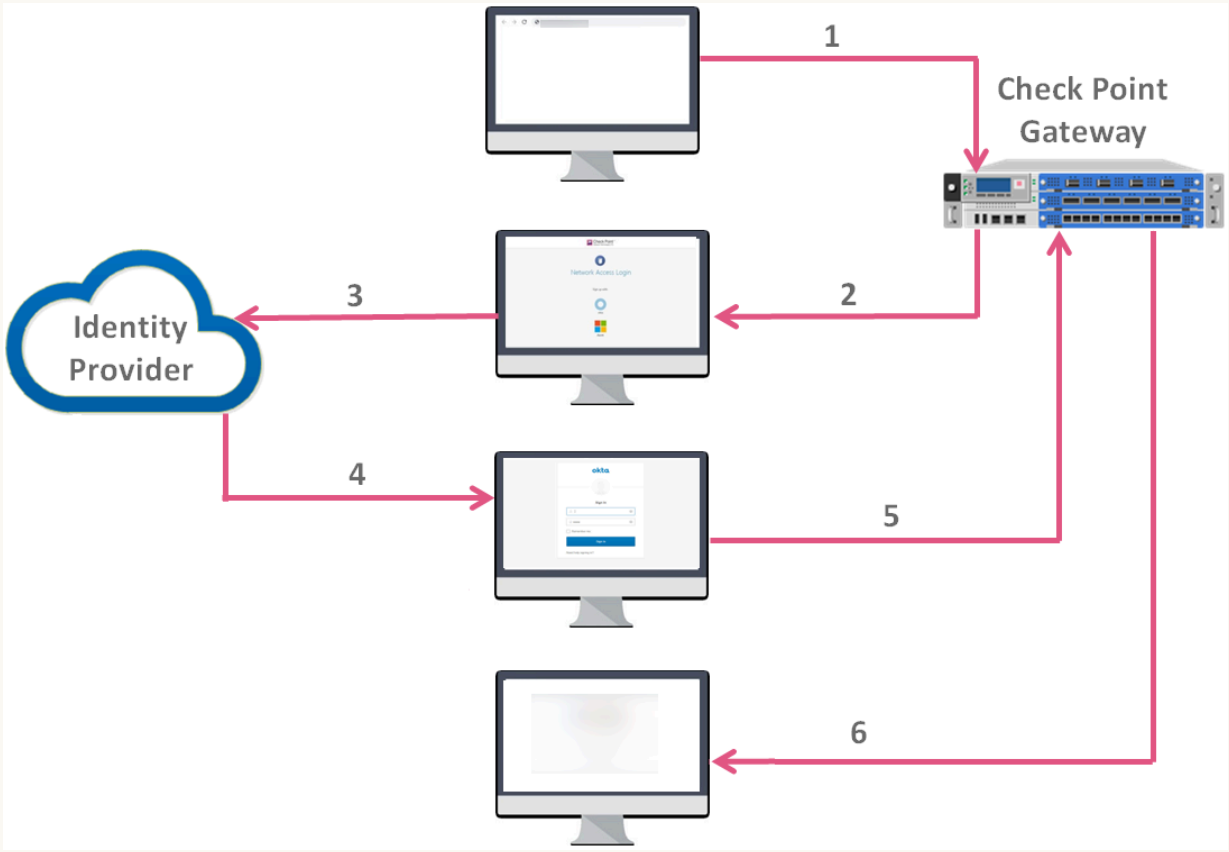
> 팁
>
> 사용자 이름·비밀번호만 쓰기보다, 인증서나 OTP 같은 또 다른 인증 방식을 함께 두는 것이 보안상 권장됩니다.

구버전 클라이언트와의 호환도 고려해야 합니다. 기본적으로 구버전 클라이언트의 접속이 허용 되지만, 대부분을 다중 로그인 옵션 지원 버전으로 올렸다면 구버전을 차단해 더 안전하게 운영할 수 있고, 반대로 신버전 클라이언트가 구버전용 설정으로 접속하게 할지도 선택할 수 있습니다.

SAML — 클라우드 ID 공급자와 잇기

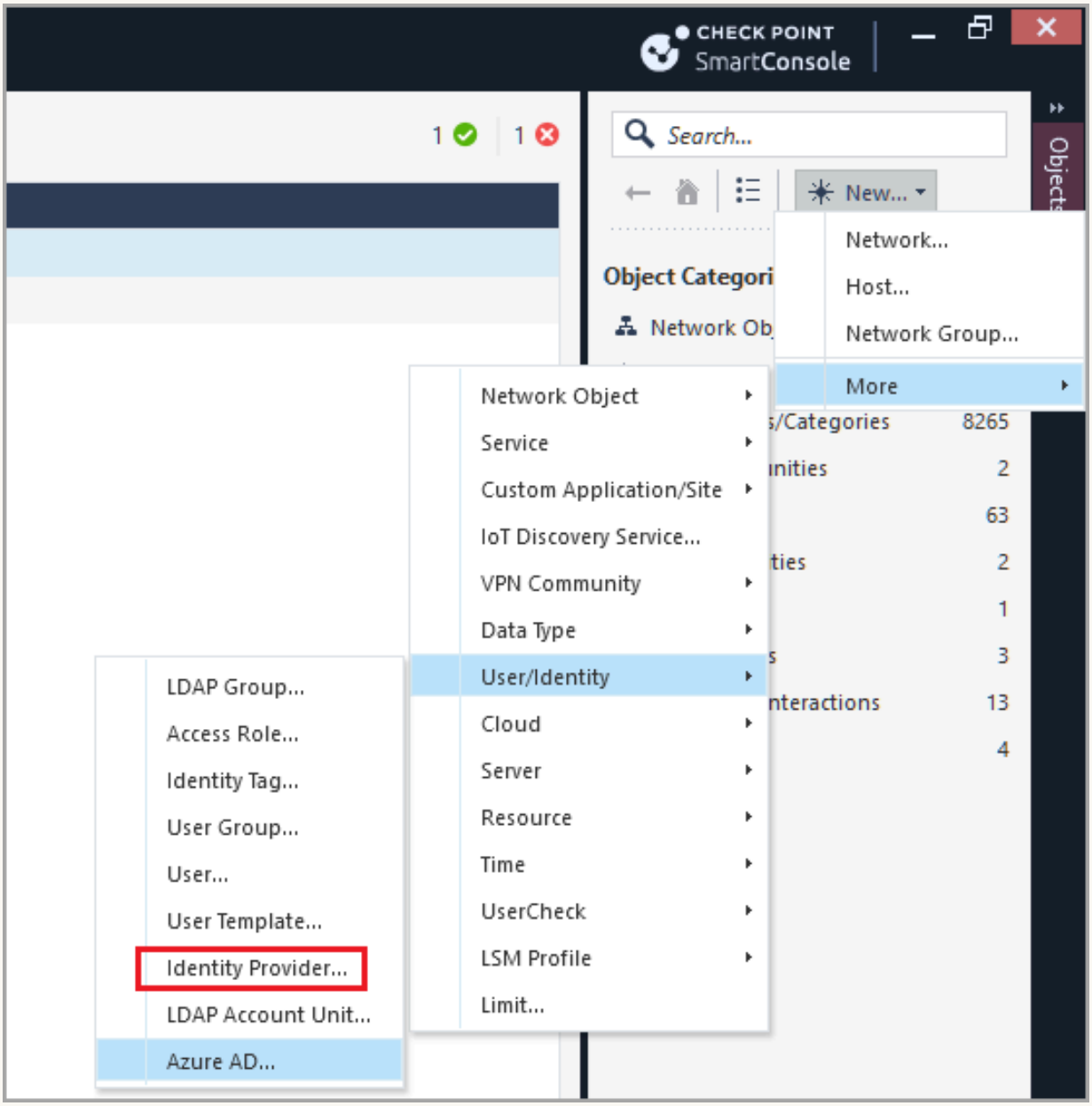
SAML 을 쓰면 제3자 Identity Provider(예: Okta)를 인증 수단으로 삼아, Mobile Access 게이트웨이·포털이 Service Provider 역할 을 합니다. Identity Provider는 신원을 만들고 관리하며 인증 서비스를 제공하고, Service Provider는 그렇게 인증된 사용자에게 서비스를 제공 합니다.

흐름은 이렇습니다 — 사용자가 게이트웨이 URL로 접속(①)하면 게이트웨이가 로그인 페이지를 열고(②), 사용자 브라우저를 Identity Provider 포털로 보내(③) 거기서 인증하게 합니다(④). Identity Provider는 디지털 서명된 SAML assertion을 만들어 브라우저로 돌려보내고(④), 브라우저는 이를 게이트웨이로 전달(⑤)하며, 게이트웨이가 assertion을 검증한 뒤 사용자를 포털로 보내 사내 자원에 접근하게 합니다(⑥).

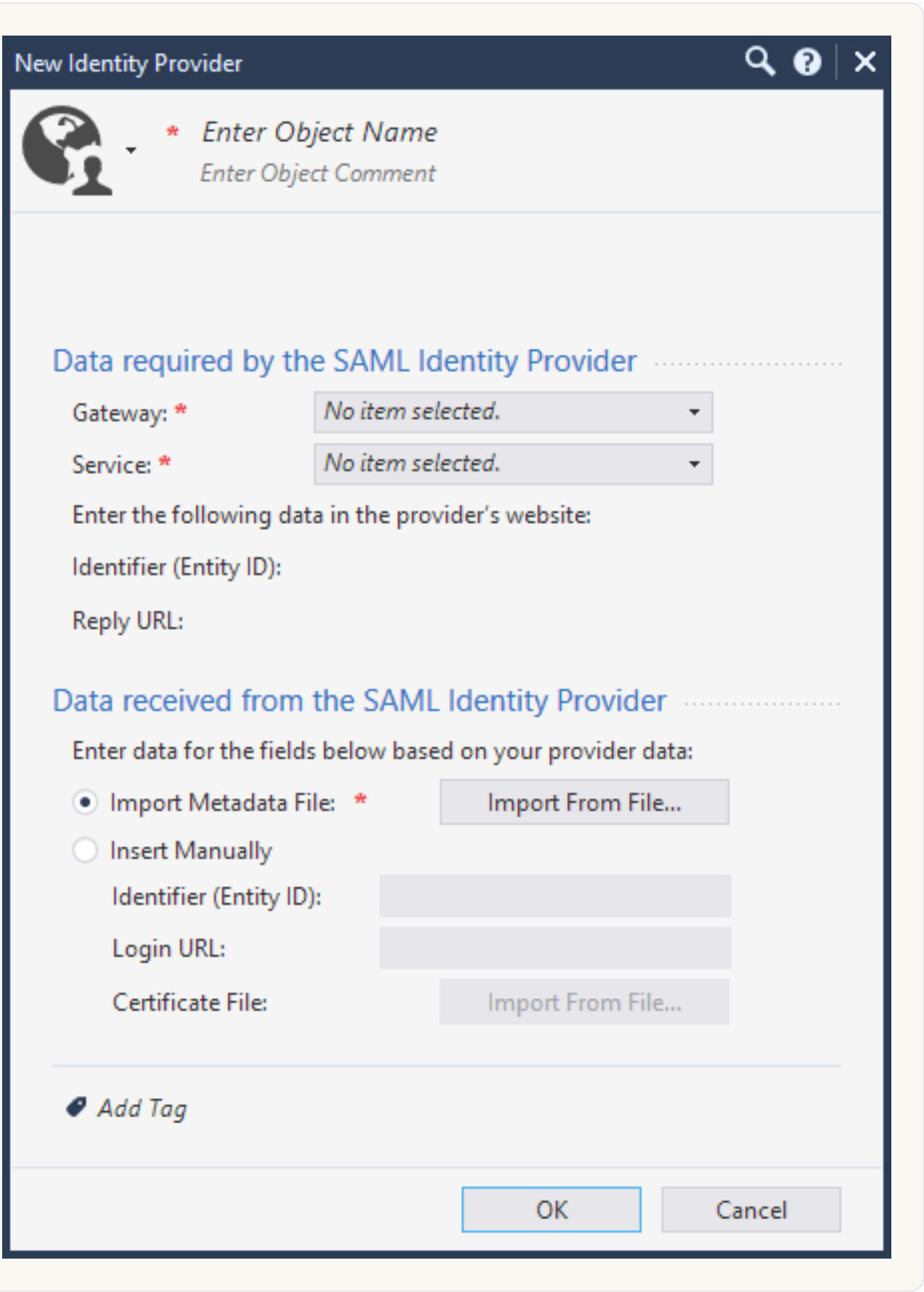


① 게이트웨이 접속 ② 로그인 페이지 ③ Identity Provider(Okta)로 리디렉트 ④ 사용자 인증·SAML assertion 발급 ⑤ assertion을 게이트웨이로 전달 ⑥ 검증 후 포털 접근 — Mobile Access를 Service Provider로, Okta를 Identity Provider로 두는 SAML 인증 흐름

구성은 크게 블레이드·포털 설정 → Legacy SmartDashboard에 모든 IdP 인증 사용자를 대표하는 generic External User Profile 만들기 → SmartConsole에서 Identity Provider 객체 생성 순으로 진행합니다.



SmartConsole에서 New > More > User/Identity > Identity Provider로 새 IdP 객체를 만드는 화면



게이트웨이를 고르고 SAML Identity Provider가 요구하는 데이터를 채우는 New Identity Provider 창

> 주 의
>
> Check Point 서비스 포털에서 로그아웃해도 Identity Provider 쪽 세션은 자동으로 끝나지 않습니다.

다중 인증과 그 변형들 — DynamicID 등

DynamicID 는 1차 인증을 통과한 사용자에게 이메일·문자로 보낸 일회용 비밀번호(OTP)를 추가로 요구 하는 다중 인증입니다. 이 밖에도 게이트웨이마다 다른 인증을 쓰는 구성, Image-Based RADIUS 인증, MS-CHAPv2와 UPN을 쓰는 RADIUS 인증, 그리고 자동화 봇을 거르는 **Google reCAPTCHA Challenge** 같은 변형이 지원됩니다. 인증 과정에서 게이트웨이가 디렉터리 서버에서 사용자를 어떻게 찾는지(검색 순서) 도 구성할 수 있으며, 이런 시나리오별 세부 절차는 원문 해당 절을 참고합니다.

로그인 이후 — 세션 관리

인증을 마치면 사용자에게 **세션** 이 부여되며, 로그아웃하거나 연결이 타임아웃될 때까지 이어지는 통신 기간 입니다. **Session Settings** 에서 세션 타임아웃·동시 세션 같은 정책을 정하고, **Advanced Password Management** 로 비밀번호 만료·변경 흐름을 다룹니다. 운영 중에는 **Session Visibility and Management Utility** 로 현재 활성 세션을 보고 필요하면 강제 종료 할 수 있습니다. 한 게이트웨이의 모든 인증 설정을 한눈에 보려면 SmartDashboard의 Mobile Access 탭 > Gateways에서 각 게이트웨이를 펼쳐 확인합니다. 세부 설정값은 원문 Session Settings·Advanced Password Management 절을 참고하세요.

08 권한 부여와 접근 제어

권한 부여와 접근 제어

인증이 "당신이 누구인지"라면, **권한 부여(Authorization)** 는 인증된 사용자가 실제로 어떤 사내 응용에 닿을 수 있는지를 정책으로 결정 하는 일입니다. 이 장은 Mobile Access를 Unified Access Policy에 녹여 규칙을 짜는 방법, 규칙 순서·레이어의 모범 사례, 자원별 보안 수준인 Protection Level, 그리고 모바일 기기 상태를 MDM과 연동해 강제하는 방법 을 정리합니다.

두 가지 정책 방식

Mobile Access 규칙은 **Unified Access Policy**(권장)와 **Legacy Policy** 중 하나 로 운영합니다(시작하기). 통합 정책을 쓰면 Mobile Access Portal·Capsule Workspace·온디맨드 클라이언트 관련 규칙을 모두 Access Control 정책 한곳에서 다루며, Protection Level·Secure Workspace·Endpoint Compliance 같은 기능도 그대로 적용됩니다(단 일부 설정은 여전히 SmartDashboard의 Mobile Access 탭에서 함).

게이트웨이를 통합 정책으로 돌리려면 게이트웨이 객체 > Mobile Access > Policy Source에서 Unified Access Policy를 고르고, Mobile Access 응용이 든 레이어마다 Mobile Access를 활성화 해야 합니다(Ordered Layer·Inline Layer 모두).

Unified Policy에서 규칙 짜기

통합 정책에서 규칙을 만들 때 지켜야 할 핵심이 몇 가지 있습니다. 응용이 포털이나 Capsule Workspace에 보이게 하려면 반드시 **Mobile Application 객체** 를 Services & Applications 열에 넣어야 합니다 — 거기에 `Any` 를 두면 허용은 되지만 포털에 보이지 않고(URL 직접 입력 시에만 열림, Capsule Workspace에선 불가), `HTTPS` 같은 서비스 객체를 두면 Mobile Access의 https 응용과 매칭되지 않습니다. 또 URL Filtering 같은 다른 용도의 응용 객체는 Mobile Access 규칙에서 동작하지 않 으므로, 예컨대 Facebook을 허용하려면 URL Filtering의 Facebook이 아니라 그 URL로 새 Web Application을 만들어야 합니다.

규칙의 구성요소는 이렇게 정리됩니다 — **Source** 에는 사용자·그룹이나 Mobile/Remote Access 클라이언트를 담은 **Access Role**, **Services & Applications** 에는 Mobile Application 객체, **VPN** 열에는 `Any` 또는 게이트웨이를 담은 Remote Access Community, **Action** 은 Accept/Drop(Reject은 Drop처럼 동작), **Install On** 에는 Mobile Access와 Identity Awareness가 켜지고 Unified Access Policy를 쓰는 게이트웨이 가 들어갑니다. Mobile Access나 IPsec 블레이드를 켜면 게이트웨이는 자동으로 RemoteAccess VPN Community에 들어갑니다.

규칙 순서와 레이어 — 함정 피하기

통합 정책에서 가장 흔한 실수가 규칙 순서입니다. 응용을 허용하는 Mobile Access 규칙은, 그 응용이 쓰는 서비스(HTTP/HTTPS)를 다루는 규칙보다 **위에** 와야 합니다. 예컨대 OWA(웹 기반 Mobile Access 응용)를 허용하는 규칙을 일반 HTTPS 허용 규칙보다 아래에 두면, 사용자는 포털·Capsule Workspace에서 OWA를 아예 못 보고 접근도 못 합니다. HTTPS 규칙이 먼저 트래픽을 채 가기 때문입니다.

복잡한 정책에서는 **Mobile Access Inline Layer** 로 깔끔하게 묶는 것이 좋습니다 — 부모 규칙의 Source에 모든 Mobile Access 클라이언트(Capsule Workspace·포털·ActiveSync·SNX 등)를 담은 Access Role을 두고, Action을 Inline Layer로 하여 그 안에서 응용 규칙을 짭니다(끝에는 Action이 Drop인 Cleanup 규칙). Ordered Layer를 여러 개 쓴다면, Mobile Access 레이어보다 앞선 모든 레이어에 Mobile Access 트래픽을 통과시키는 **bypass 규칙**(Source는 Mobile Access 사용자 Access Role, Action은 Accept) 을 두어야 트래픽이 Mobile Access 레이어까지 흘러갑니다.

Protection Level — 자원별 보안 수준

Protection Level 은 연결성과 보안의 균형을 맞춘, 미리 정의된 보안 설정 묶음 입니다. 비슷한 요건의 응용들에 같은 수준의 보호를 한 번에 적용할 수 있어, 응용마다 일일이 설정하지 않아도 됩니다. 기본으로 **Normal·Restrictive·Permissive** 세 가지가 제공 되며, 새로 만들거나 기존 것을 고칠 수 있습니다.

응용을 정의할 때 기본값은 "게이트웨이의 보안 요건을 그대로 따름"(포털에 인증된 사용자는 이 응용에도 인증됨) 이지만, 여기에 별도 Protection Level을 묶으면 포털 요건에 더해 그 응용만의 요건까지 충족해야 합니다. Protection Level 안에서는 허용할 **인증 방식**(이 중 하나로 인증해야 접근), SMS 인증 강제, 그리고 **Endpoint Security**(선택한 Endpoint Compliance 정책을 통과해야, 또는 Secure Workspace 안에서만 접근) 를 정합니다 (Endpoint 준수).

MDM Cooperative Enforcement — 모바일 기기 상태 강제

MDM Cooperative Enforcement 는 제3자 Mobile Device Management 서버와 연동해, 조직 보안 정책을 따르는 관리 기기만 사내 자원에 접속 하게 합니다. Check Point 앱(Capsule Connect·Capsule Workspace)이 게이트웨이로 VPN을 열면, 게이트웨이가 MDM 서버에 기기의 준수 수준을 조회하고, 그 결과와 사용자 권한을 종합해 접근을 허용하거나 차단 합니다. 즉 단말 자체의 관리 상태를 외부 MDM의 판단에 맡겨 강제하는 방식입니다. 지원 벤더와 iOS 버전별 구성은 sk98201·sk98447에 정리돼 있으며, MDM 계정·라이선스 같은 전제 조건과 게이트웨이 설정 절차의 세부는 원문 해당 절을 참고하세요.

09 스마트폰·태블릿 접속

스마트폰·태블릿 접속

데스크톱과 달리 비관리 스마트폰·태블릿은 통제하기 까다롭 습니다. Mobile Access는 Check Point 모바일 앱(특히 Capsule Workspace)과 인증서·프로파일을 묶어 이 문제를 풉니다. 이 장은 모바일 사용자에게 무엇을 준비시키는지, 인증서를 어떻게 만들어 배포하는지, 사용자 경험을 좌우하는 Mobile Profile, 분실 기기를 지우는 Remote Wipe 를 정리합니다. (모바일 메일/캘린더 응용은 애플리케이션 장의 Exchange 부분과 이어집니다.)

모바일 접속 준비의 큰 그림

모바일 사용자를 붙이려면 몇 가지를 갖춰야 합니다 — 메일·캘린더·연락처용으로 Mobile Mail이나 ActiveSync 응용을 구성(마법사로 자동 가능)하고, 필요하면 웹 앱을 더하며, 사용자가 게이트웨이에 인증할 자격 증명(인증서 인증이면 인증서 생성·배포 마법사)을 마련하고, **Mobile Profile** 이 조직 요건에 맞는지 확인하며, 어떤 앱을 깔지 안내하고, 스마트폰·태블릿 사용자를 Mobile Access 정책에 포함시키는 일입니다.

인증서 인증과 클라이언트 인증서

핸드헬드 기기가 게이트웨이에 붙으려면 인증서가 제대로 설정돼야 합니다. Personal Certificate를 인증 방식으로 쓰면 사용자마다 클라이언트 인증서를 생성 해야 하고, 서버 쪽은 제3자 신뢰 CA(예: Entrust) 서명 인증서가 강력히 권장 됩니다(없으면 ICA 자가 서명 인증서가 이미 설정돼 있으나 브라우저·기기 경고가 날 수 있음).

Check Point 모바일 앱은 인증서만으로, 또는 인증서 + 사용자명/비밀번호의 2요소 로 인증하며, 인증서는 게이트웨이를 관리하는 관리 서버의 ICA가 서명합니다. 인증서는 SmartConsole의 Security Policies > Access Control > Access Tools > Client Certificates 에서 관리합니다 — Client Certificates 창에서 인증서를 만들고·수정하고·폐기하며 상태·만료일·등록 키를 보고, **Certificate Creation and Distribution wizard** 로 생성·배포합니다. 함께 있는 Email Templates 창에서는 배포용 이메일 템플릿을 만들어 미리 보고 , 비슷한 템플릿은 Clone으로 복제합니다. 사용자가 메일 속 QR 코드나 링크를 열면 사이트가 만들어지고 인증서가 등록되며, 메일에는 Link URL·QR Code·HTML Link 같은 요소를 골라 담을 수 있습니다.

Mobile Profile — 모바일 사용자 경험

Capsule Workspace에서 사용자 경험을 좌우하는 많은 설정이 **Mobile Profile** 에서 옵니다. 각 Mobile Access 사용자 그룹에 하나의 Mobile Profile이 배정 되며 기본은 Default Profile입니다. 프로파일에는 **Passcode 설정**, 메일·캘린더·연락처 사용 가능 여부, 오프라인 콘텐츠 설정, 연락처 출처 같은 항목이 들어갑니다. 관리는 Mobile Access 탭 > Capsule Workspace Settings에서 하며, Mobile Profiles 창에서 프로파일을 만들고·고치고·복제하고, Mobile Profile Policy 창에서 어떤 그룹에 어떤 프로파일을 줄지 규칙 으로 정합니다.

Remote Wipe — 분실 기기 지우기

Remote Wipe 는 사용자 모바일 기기에 캐시된 오프라인 데이터를 원격으로 지웁니다. 관리자가 내부 CA 인증서를 폐기하면, 클라이언트의 Remote Wipe 설정이 푸시 알림 방식이면 Remote Wipe 푸시 알림이 발송 되고, 기기가 알림을 받으면 삭제가 실행됩니다. 다만 푸시 알림은 best effort라 전달이 보장되지 않 으며, 알림을 못 받았더라도 그 기기가 폐기된 CA 인증서로 게이트웨이에 연결을 시도하는 순간 Remote Wipe가 발동됩니다. 푸시 발송 시점과 삭제 성공 시점에는 로그가 남습니다.

ESOD 우회와 기타 구성

핸드헬드 기기는 Endpoint Security on Demand(ESOD) 구성요소를 돌릴 수 없어, 기본적으로 스마트폰·태블릿에는 ESOD가 비활성 입니다(Endpoint 준수). 조직이 ESOD를 켜 두었다면 모바일 앱은 ESOD가 강제되는 응용에 닿지 못하므로, 게이트웨이에서 `cvpnd_settings` 로 `MobileAppBypassESODforApps` 를 `true` (기본, 우회)/ `false` 로 조정합니다(모바일 앱은 HTTP User-Agent 헤더로 식별되지 않음). 이 밖에 OS별 시스템 설정, 최종 사용자 안내, 핸드헬드용 고급 게이트웨이 구성 같은 세부는 원문 해당 절을 참고하세요.

10 Endpoint 준수 검사와 Secure Workspace

Endpoint 준수 검사와 Secure Workspace

원격 접속의 큰 위험은 보호가 허술한 단말이 사내망의 통로가 되는 것 입니다. Mobile Access는 두 장치로 이를 막습니다 — 접속 전에 단말 상태를 검사하는 **Endpoint Security on Demand(ESOD)** 와, 세션 동안 격리된 가상 데스크톱을 띄우는 **Secure Workspace** 입니다. 이 장은 둘을 함께 정리합니다.

Endpoint Compliance — 접속 전 단말 검사

Endpoint Security on Demand(Endpoint 준수 스캐너)는 접속하려는 단말이 미리 정의된 준수 정책에 맞는지 스캔 합니다. 예컨대 최신 Anti-Virus가 깔려 있고 Firewall이 켜져 있는지를 확인해, 준수하면 포털 접근을 허용 합니다. 이렇게 함으로써 보호되지 않은 단말에서 비롯되는 데이터 유출·과도한 대역폭 소비 같은 위협 으로부터 기업을 지킵니다.

준수 정책은 규칙들로 이뤄지며, 적용 단위가 세밀합니다. 정책을 게이트웨이에 배정하면 단말이 준수해야 포털 로그인이 가능 하고, Protection Level에 배정해 응용에 묶으면 그 응용에 한해 더 강한 검사를 강제 할 수 있습니다(권한). 응용에 Protection Level이 걸려 있으면 단말은 게이트웨이 정책과 그 Protection Level 정책을 모두 통과해야 하며, 스캔은 포털 로그인 전에 단 한 번 이뤄지고 그 결과로 모든 정책 준수 여부가 판정됩니다. 비준수 단말에는 Secure Workspace 사용을 강제할 수도 있습니다.

준수 정책의 규칙 유형

정책에는 보안 응용 종류별로 여러 규칙 유형이 있고, 같은 유형을 설정만 달리해 여러 개 둘 수 있습니다. **Windows Security Rule** 은 Windows 특화 점검(최신 Service Pack, 자동 업데이트 상태, Hotfix·패치) 을 하고, **Anti-Spyware·Anti-Virus·Firewall Application Rule** 은 각각 해당 종류의 보안 소프트웨어가 단말에서 실행 중이고 버전·시그니처가 최신인지를 확인합니다(규칙 안의 응용 중 최소 하나가 활성이면 준수로 판정, 지원 공급자는 미리 구성돼 있고 미지원 공급자는 Custom Check로). **Custom Check Rule** 은 다른 규칙으로 못 잡는 것(독자 응용·특정 파일·레지스트리 키·실행 프로세스, 비영어 이름 등) 을 점검하고, **OR Group of Rules** 는 여러 규칙 중 하나만 만족해도 통과시키며, **Spyware Scan Rule** 은 Dialer·Worm·Keystroke Logger·Trojan·Adware·Tracking Cookie 같은 스파이웨어 유형별로 취할 동작 을 정합니다. 모든 규칙은 비준수 시 취할 동작과 사용자에게 보일 안내 메시지(보완 방법 등)를 함께 지정합니다.

운영은 정책을 계획하고(어떤 응용·게이트웨이에 어떤 검사를?), **ICSInfo 도구** 로 정보를 수집하며, 정책을 만들어 응용·게이트웨이에 배정하는 흐름입니다. 스캔 결과는 **Endpoint Compliance Logs** 로 남아 누가 준수·비준수였는지 추적 할 수 있고, 매 로그인마다 스캔하지 않게 하거나 특정 스파이웨어 시그니처를 스캔에서 제외하는 조정도 가능합니다. 지원되지 않는 브라우저용 대안과 정책 마무리 절차의 세부는 원문 해당 절을 참고합니다.

Secure Workspace — 세션 격리 가상 데스크톱

> 주 의
>
> 2024년 2월 1일부로 Check Point는 Mobile Access의 Secure Workspace 기능에 대해 단계적 지원 종료(Feature Deprecation·End-of-Support)를 안내했습니다. 신규 설계 시 sk181968을 확인하세요.

Secure Workspace 는 단말 위에 "실제" 작업 공간과 분리된 안전한 가상 작업 공간을 만들어, 그 안에서만 사내 자원을 다루게 합니다. 이 격리 공간 밖으로는 Mobile Access Portal을 통하는 것 말고는 어떤 데이터도 나가지 못하 며, Secure Workspace 정책이 명시적으로 허용하지 않은 응용·파일·시스템 도구·자원에는 접근할 수 없습니다. 세션 중 임시 파일은 가상 데스크톱의 암호화 폴더(My Secured Documents)에 담기고, 세션이 끝나면 이 폴더와 모든 세션 데이터가 삭제 되어 공용 PC에 흔적이 남지 않습니다.

쓰려면 단말에 Check Point Portal Agent(ActiveX)와 SSL Network Extender가 설치돼 있어야 합니다. 게이트웨이를 켤 때 모든 사용자에게 Secure Workspace 경유를 **강제** 할지, 아니면 단말에서 직접 접속할지 **선택** 하게 할지 를 정합니다. SSL Network Extender를 Secure Workspace 안에서 쓰면 안팎 트래픽이 모두 암호화됩니다.

Secure Workspace 정책은 게이트웨이마다 따로 두며, 사용자가 어떤 응용을 실행할지, 어떤 파일·디렉터리에 저장할지, 포털 보호·사용자 경험을 어떻게 할지 를 통제합니다. 기본 구성은 제한된 응용군만 허용하지만(목록은 sk114454), 대부분의 포털 작업에는 충분합니다. 특정 Protection Level을 Secure Workspace에서 우회(Bypassed)시키거나 완화 모드로 두는 조정은 CLI에서 `cvpnd_settings` 로 하며, 변경 후에는 `cvpnrestart` 로 서비스를 재시작하고 (클러스터라면 모든 멤버에) 정책을 설치합니다. 정책 구성과 최종 사용자 경험, 준수 데이터 업데이트의 세부는 원문 해당 절을 참고하세요.

11 Reverse Proxy

Reverse Proxy

대부분의 Mobile Access 접근은 포털을 거치지만, 포털 없이 곧장 내부 웹 서버를 외부에 노출 하고 싶을 때가 있습니다. 이때 게이트웨이를 **Reverse Proxy** 로 동작시킵니다. 이 장은 Reverse Proxy가 무엇을 하는지, CLI로 어떻게 구성·문제 해결하는지, 그리고 어떤 한계가 있는지 를 정리합니다.

Reverse Proxy가 하는 일

Reverse Proxy 는 외부 사용자가 게이트웨이 IP로 풀리는 URL에 접속하면, 게이트웨이가 Reverse Proxy 규칙에 따라 그 요청을 내부 서버로 대신 전달 하는 방식입니다. 덕분에 외부 클라이언트가 내부 서버 자원에 닿으면서도, 서버의 실제 내부 주소는 감춰 집니다. 규칙으로는 내부 서버의 외부 주소를 실제 네트워크 주소로 매핑하고, 외부 클라이언트가 어떤 자원에 접근할지 허용하며, 사용자–자원 사이 연결을 HTTP로 할지 HTTPS로 할지 를 정합니다.
기본적으로 Reverse Proxy는 비활성이며, CLI에서 켜고 구성합니다.

CLI로 구성하기

Reverse Proxy는 GUI 없이 `ReverseProxyCLI` 명령으로만 다룹니다. 이 명령으로 Reverse Proxy를 켜고/끄고(on/off), 규칙·애플리케이션을 보고(show), 규칙·애플리케이션을 추가하고(add, 대화형), 규칙을 수정·삭제(edit/remove) 합니다. `add application` 은 지원되는 내부 응용(Outlook Anywhere·Capsule Docs)에 대한 규칙 묶음 을 한 번에 더해 줍니다.

```
ReverseProxyCLI {on | off | show {rules | applications} |
  add {rule <rule_name> | application <app_name> {capsule_docs |
  outlook_anywhere} <ext_hostname> <int_hostname>} |
  edit rule <rule_name> | remove rule <rule_name> | apply config}
```

> 주 의
>
> CLI로 규칙을 바꿀 때마다 마지막에 반드시 ReverseProxyCLI apply config를 실행해야 변경이 적용됩니다.

몇 가지 주의할 점이 있습니다. Reverse Proxy로 허용되는 외부 포트는 80과 443뿐 이고(내부 포트는 모두 허용), 게이트웨이의 Gaia Portal이 `https://<IP>/` 처럼 끝에 `/` 만 있는 URL이면 Reverse Proxy와 충돌 하므로 Gaia Portal URL을 `/gaia` 로 바꾸거나 포트를 4434로 옮겨야 합니다(안 그러면 Gaia Portal이 접근 불가). 자세한 예시와 고급 CLI·XML 구성은 sk110348에 있습니다.

문제 해결

Reverse Proxy는 SmartLog 같은 표준 모니터링 도구로 진단합니다. 로그를 남기려면 SmartDashboard > Mobile Access 탭 > Additional Settings > Logging에서 웹 응용 접근 로깅을 켜 고, 로그는 SmartLog의 Mobile Access 로그에서 Category=Mobile Access, Application=Reverse Proxy로 식별합니다(목적지는 로그에 표시되지 않음).

로그의 Access 항목은 세 가지로 나뉩니다 — **Allowed**(허용된 URL), **Denied**(차단된 URL — 오인이면 `ReverseProxyCLI show rules` 로 규칙의 Paths를 확인해 막힌 경로를 추가), **Failed**(내부 서버로 전달 실패) 입니다. Failed에는 Internal Server Error, Proxy not found, Can't resolve host name(해당 호스트를 `nslookup` 으로 게이트웨이가 풀 수 있는지 확인), SSL handshake failed, Server response was too slow 같은 구체적 원인이 함께 나옵니다.

더 깊은 디버깅이 필요하면 `httpd_common.conf` 의 `ReverseProxyHandlerTraceLog` 를 On으로, HTTPS/HTTP는 각각 `httpd_ssl.conf` · `httpd_clear.conf` 의 `LogLevel` 을 debug로 바꿔 trace 로그를 봅니다. `cvpnd_admin debug set TDERROR_ALL_ALL=5` 로 cvpnd 로그를, `ps -ef | grep httpd` 로 Reverse Proxy 프로세스(SSL·Clear) 동작 여부를 확인합니다.

알려진 한계

Reverse Proxy에는 분명한 제약이 있습니다. GUI(SmartDashboard)가 없고, 사용자 단위 접근 제어가 없으며, 네트워크·인터페이스 단위 세분화도, 반환 사이트의 링크 번역도 없습니다. Mobile Access 정책에 Host Translation을 쓰는 응용이 있다면 그 호스트명은 Reverse Proxy 통신의 호스트명과 달라야 하고, Reverse Proxy는 SSL 종료에 인증서를 하나만 쓰므로, 여러 웹 서버를 HTTPS로 받으려면 와일드카드 인증서나 SAN 인증서 가 필요합니다. Lync(Skype for Business)는 지원되지 않습니다. 클러스터에서는 규칙이 멤버 간 자동 동기화되지 않 으므로, 한 멤버에 모든 규칙을 넣은 뒤 `ReverseProxyConf.xml` 을 다른 멤버로 복사하고 각 멤버에서 `apply config` 를 실행해 맞춰 줍니다.

12 블레이드 구성과 다른 블레이드 연동

블레이드 구성과 다른 블레이드 연동

Mobile Access는 홀로 동작하지 않습니다. 같은 게이트웨이의 다른 Software Blade와 맞물려 트래픽을 지키고 자원을 정의합니다. 이 장은 Mobile Access가 IPS·Anti-Virus·IPsec VPN과 어떻게 연동되는지, 대규모 환경에서 동시 연결 한도를 어떻게 조정하는지, 그리고 DNS Name 객체를 어떻게 활용하는지 를 정리합니다.

다른 블레이드와의 통합

Firewall 블레이드를 켠 어떤 Gaia 게이트웨이든 Mobile Access 블레이드도 함께 켤 수 있고, 둘은 완전히 통합됩니다. SmartDashboard에서 만든 대부분의 네트워크 객체·리소스·사용자가 Mobile Access에도 그대로 쓰이고, 반대로 Mobile Access에서 만든 객체·사용자도 SmartDashboard 전반에 나타납니다. 즉 별도 객체 체계를 따로 관리할 필요가 없습니다.

IPS — Mobile Access를 지키는 웹 보호

Mobile Access를 켜면 특정 IPS Web Intelligence 보호가 자동으로 활성 됩니다. 이 보호들은 IPS 프로파일이 아니라 로컬 파일에서 설정값을 가져오며, 게이트웨이에 IPS 블레이드가 없어도 항상 Mobile Access 트래픽에만 적용 됩니다(소개). 여기에는 HTTP Format Sizes·HTTP Methods·Directory Traversal·Cross-Site Scripting·Command Injection·Malicious Code Protector 같은 웹 공격 차단의 핵심 보호 가 포함됩니다.

게이트웨이의 IPS 프로파일을 대신 쓰고 싶다면 그 프로파일에 위 핵심 보호들이 모두 들어 있는지 확인한 뒤, `cvpnd_settings set use_ws_local_configuration false` 로 전환 하고 Check Point 프로세스를 재시작합니다(`cvpnstop ; cvpnstart`). 다시 로컬 자동 설정으로 돌아가려면 같은 플래그를 `true` 로 둡니다.

> 주 의
>
> IPS가 비활성이면, 이 플래그 값과 무관하게 Mobile Access는 로컬 IPS 설정을 써서 게이트웨이를 보호합니다. 고급 문제 해결 목적이 아니라면 이 Web Intelligence 보호를 끄지 않는 것이 좋습니다.

Anti-Virus와 IPsec VPN

Threat Prevention 탭의 Traditional Anti-Virus > HTTP 설정 중 일부는 Mobile Access 트래픽에도 적용 됩니다 — By File Direction으로 스캔하면 사용자가 올리는(Incoming) 트래픽과 내려받는(Outgoing) 트래픽을 검사하고, By IPs로 스캔하면 메일·FTP·HTTP 설정에 따라 포털 트래픽을 검사합니다. Mobile Access의 Anti-Virus는 어떤 옵션을 골라도 항상 proactive 모드 로 동작하며, SSL Network Extender 트래픽은 게이트웨이로 재라우팅된 뒤 일반 비암호화 트래픽처럼 검사됩니다(같은 게이트웨이에 Anti-Virus 블레이드와 Traditional Anti-Virus를 동시에 켤 수는 없음).

IPsec VPN 블레이드와 Mobile Access 블레이드는 같은 게이트웨이에서 함께 켜 서, Site-to-Site와 Remote Access를 동시에 최적으로 제공할 수 있습니다(Site-to-Site VPN, Remote Access VPN). 다만 주의할 점이 있습니다 — Endpoint Connect·SecureClient Mobile 같은 일부 구버전 VPN 클라이언트는 Mobile Access 블레이드와는 동작하지 않고 IPsec VPN 블레이드와만 동작하며, SSL Network Extender는 Mobile Access가 켜진 게이트웨이에서는 반드시 Mobile Access 탭에서 구성 해야 합니다(이전에 IPsec VPN 쪽에 설정했다면 다시 구성해야 함). Office Mode는 둘 중 어느 쪽에서든 구성할 수 있습니다.

동시 연결 한도

Mobile Access는 사용자가 사내 자원에 접속할 때 여러 연결을 만듭니다 — 사용자에서 게이트웨이로, 게이트웨이에서 내부 서버로 각각. 그래서 원격 사용자가 1,000명을 넘는 환경이라면 Gateway Properties > Optimization > Capacity Optimization에서 최대 동시 연결 수를 늘리는 것이 권장 됩니다(예: 기본 25,000에 사용자 2,000명이면 그 두 배인 4,000을 더해 29,000으로).

DNS Name 객체

DNS Name 객체 를 Mobile Access 응용 정의에 쓰면, 서버 IP가 바뀌어도 응용 정의를 고칠 필요가 없 습니다 — 게이트웨이가 접근을 허가할 때 그 이름의 IP를 실시간으로 풀기 때문입니다. 한 응용이 여러 복제 서버에 호스팅되면, 각 호스트를 일일이 정의하는 대신 DNS Name 객체 하나 로 가리킬 수 있습니다. 하나의 DNS 이름에는 여러 별칭(alias)을 둘 수 있고 (예: `www.example.com` · `www.example.co.uk`), 와일드카드는 도메인 앞쪽에만 쓸 수 있습니다(`*.example.com` 은 유효하나 `www.example.*` 는 무효).

DNS Name 객체는 웹 응용·파일 공유·Citrix·웹메일 호스트를 정의할 때와 Hostname Translation 지원에 쓰이며, Security Rule Base에서는 쓸 수 없 습니다. 이름을 풀어 줄 DNS 서버는 SmartDashboard의 Name Resolution 페이지나 게이트웨이 자체에 지정하며, 객체는 Mobile Access 탭 > Additional Settings > DNS Names에서 만듭니다.

13 문제 해결·FAQ·CLI 참조

문제 해결·FAQ·CLI 참조

마지막 장은 운영에서 마주치는 실무를 모았습니다 — Mobile Access가 잘 안 될 때의 점검 순서, 자주 묻는 질문이 가리키는 곳, 그리고 게이트웨이에서 직접 쓰는 명령줄(CLI) 도구 입니다.

문제 해결 — 어디부터 보나

웹 연결 문제는 HTTP 쿠키와 얽혀 자주 생깁니다. Internet Explorer가 평소 웹 서버로 보내던 일부 쿠키를 Mobile Access는 같은 상황에서 전달하지 않기 때문인데, 해결책은 sk31636에 정리돼 있습니다.

가장 흔한 골칫거리가 **Outlook Web Access(OWA)** 입니다(SNX 없이 Mobile Access로 OWA를 쓸 때). 점검은 순서대로 — 첫째 트래픽 로그에서 오류를 찾고, 둘째 Mobile Access 없이 같은 시나리오를 재현해 문제가 사라지는지 확인 하며, 셋째 연결성을 검증(게이트웨이가 Exchange 서버로 가는 경로와 80/443 포트가 열려 있는지, 사용자가 게이트웨이로 가는 경로가 있는지)하고, 넷째 OWA 버전이 지원되는지, 설정이 유효한지 를 확인합니다. 그래도 안 되면 "Common OWA problems" 절에서 증상에 맞는 항목과 인증 관련 문제를 찾습니다.

이 밖에 Citrix(원문 Troubleshooting Citrix 절), File Shares, Push Notifications 도 각각의 점검 절이 있으니, 해당 기능이 말썽이면 그 절을 따릅니다.

자주 묻는 질문(FAQ)

운영 중 자주 나오는 질문은 대개 이 가이드의 다른 장이나 sk로 이어집니다. 지원 브라우저·OS는 R82 Release Notes, 자격 증명 저장은 애플리케이션의 Single Sign-On, 다중 인증과 게이트웨이별 인증 차등은 인증, Mobile Access 프록시 설정은 용도별로(Exchange는 모바일 메일, DynamicID SMS는 인증, 웹 응용은 sk34810), 포털 없이 내부 자원에 접근하는 길은 Reverse Proxy, 웹 응용의 WebSocket 지원은 애플리케이션, 그리고 SNX가 무엇인지는 SSL Network Extender(SNX) Administration Guide 를 가리킵니다.

CLI 참조 — 게이트웨이에서 직접 다루는 도구

대부분의 구성은 SmartConsole에서 하지만, Mobile Access 게이트웨이에는 직접 쓰는 명령줄 도구 가 여럿 있습니다. 전체 구문은 R82 CLI Reference Guide에 있고, 여기서는 자주 쓰는 것을 추려 그 쓰임을 설명합니다. (Maestro·Chassis 같은 Scalable Platform에서는 해당 Security Group의 Expert 모드에서 실행해야 합니다.)

서비스를 다루는 명령이 가장 기본입니다 — `cvpnstart` · `cvpnstop` · `cvpnrestart` 로 Mobile Access(cvpnd) 서비스를 시작·중지·재시작 하며(`cvpnrestart --with-pinger` 로 Pinger까지), 설정을 바꾼 뒤 적용할 때 자주 씁니다. `cvpn_ver` 는 설치된 버전을 보여 줍니다.

설정과 진단에는 `cvpnd_settings` (구성 파일의 플래그를 get/set/add/listAdd/listRemove — 앞 장들에서 ESOD 우회·IPS 로컬 설정·Secure Workspace 완화 모드를 켤 때 등장)와 `cvpnd_admin` (디버그 등 관리 동작) 을 씁니다.

마법사와 사용자 관리도 있습니다 — `admin_wizard` 는 CLI에서 구성 마법사를 돌려 웹사이트·LDAP·Exchange 응용을 빠르게 설정 하고(estimation으로 예상 시간, cancel로 취소), `listusers` 는 사용자 목록을, `deleteUserSettings` 는 특정 사용자(들)의 저장된 설정을, `UserSettingsUtil` 은 사용자 설정 유틸리티를 다룹니다. 이 밖에 모바일 푸시 알림을 관리하는 `fwpush` , ICS(Endpoint 준수) 업데이트를 내려받는 `ics_updates_script` , CA 번들을 다시 해시하는 `rehash_ca_bundle` 같은 특수 목적 명령이 있습니다. 각 명령의 정확한 매개변수와 예시는 원문 Command Line Reference 절과 CLI Reference Guide를 참고하세요.

이로써 Mobile Access의 소개부터 솔루션 선택, 포털·애플리케이션·인증·권한, 모바일 기기와 단말 검사, Reverse Proxy와 블레이드 연동, 그리고 운영 문제 해결까지 한 바퀴를 돌았습니다. 원격 접속 전반을 더 깊이 보려면 Remote Access VPN 가이드와 함께 읽기를 권합니다.