01 용어 정리

용어 정리

이 가이드는 Check Point R82을 처음부터 설치하고, 기존 버전에서 업그레이드하고, 여러 배포 형태로 펼치는 일을 다룹니다. 본문에 자주 나오는 핵심 용어를 설치·업그레이드 관점 에서 흐름에 따라 풀어 둡니다.

무엇을 설치하나 — 제품의 두 축

Check Point 환경은 크게 두 축으로 나뉩니다. **Security Gateway** 는 트래픽을 검사하고 보안 정책을 집행하는 전용 서버 이고, **Security Management Server** 는 그 게이트웨이가 따를 객체와 정책을 한 도메인 안에서 관리하는 서버 입니다. 게이트웨이가 길목에서 막아서는 문지기라면, 관리 서버는 그 문지기에게 규칙을 내려보내는 본부인 셈입니다. 관리 서버를 GUI로 다루는 도구가 **SmartConsole** 로, 정책 구성·장비 관리·모니터링·업데이트 설치를 모두 여기서 합니다.

규모가 커지면 **Multi-Domain Server(MDS)** 를 씁니다. 하나의 물리 서버 안에 **Domain Management Server** 라 불리는 가상 관리 서버를 여러 개 호스팅 해, 여러 도메인을 한자리에서 운영하게 합니다. 로그만 따로 모으는 전용 서버는 **Log Server**, Multi-Domain 환경의 로그 서버는 **Multi-Domain Log Server(MDLS)** 입니다.

배포 형태 — Standalone·Distributed

같은 제품을 어떻게 펼치느냐가 배포 시나리오를 가릅니다. **Distributed Deployment** 는 Security Gateway와 Security Management Server를 서로 다른 컴퓨터에 나눠 설치 하는 것이고, **Standalone** 은 둘을 같은 서버에 함께 설치 하는 것입니다. 운영체제는 모두 **Gaia** — SecurePlatform과 IPSO의 장점을 합친 Check Point 보안 운영체제 입니다. Gaia는 웹 인터페이스 **Gaia Portal**, 기본 제한 셸 **Gaia Clish**, 그리고 root 권한의 **Expert Mode** 로 다룹니다.

가용성을 높이는 구성도 있습니다. **Cluster** 는 게이트웨이 둘 이상을 High Availability나 Load Sharing으로 묶은 것 이고, 그 안의 각 멤버가 **Cluster Member** 입니다. **VSX(Virtual System Extension)** 는 한 장비·클러스터 위에 여러 가상 게이트웨이와 네트워크 장치를 올리는 가상 네트워킹 솔루션 이고, 이를 호스팅하는 물리 서버가 **VSX Gateway** 입니다. **Bridge Mode** 는 게이트웨이를 L2 브리지로 동작시켜 기존 토폴로지에 손쉽게 끼워 넣는 방식입니다.

설치·업그레이드의 핵심 작업

가장 처음부터 까는 일을 **Clean Install** — 빈 컴퓨터에 운영체제를 새로 설치 — 라 합니다. 반대로 기존 환경을 옮길 때는 두 가지 개념이 등장합니다. **Migration** 은 한 Check Point 컴퓨터에서 구성 데이터베이스를 내보내(export) 다른 컴퓨터로 들여오는(import) 일 이고, **Database Migration** 은 그중에서도 최신 버전을 별도 컴퓨터에 깔고 기존 관리 데이터베이스를 옮겨 위험을 최소화하는 업그레이드 방식 을 가리킵니다.

업데이트를 떠받치는 엔진이 **CPUSE(Check Point Upgrade Service Engine)** 로, Gaia OS와 그 위의 Check Point 제품을 자동으로 갱신 합니다. 그 위에 작은 수정은 **Hotfix**, 여러 핫픽스를 한 패키지로 묶은 것이 **Jumbo Hotfix Accumulator(JHF)** 입니다. 라이선스·계약을 다루던 옛 GUI 도구가 **SmartUpdate**, 옛 정책 편집 클라이언트가 **SmartDashboard** 입니다.

신뢰와 통신 — SIC·ICA

게이트웨이와 관리 서버가 서로를 믿고 안전하게 대화하려면 신원 확인이 필요합니다. 관리 서버에 내장된 인증 기관 **ICA(Internal Certificate Authority)** 가 인증서를 발급 하고, 그 인증서를 바탕으로 Check Point 컴퓨터끼리 SSL로 서로를 인증하는 메커니즘이 **SIC(Secure Internal Communication)** 입니다. 설치 후 게이트웨이를 관리 서버에 처음 붙일 때 이 SIC를 세우는 일이 핵심 단계입니다.

성능과 가속 — CoreXL·SecureXL

게이트웨이의 처리량을 끌어올리는 두 기술이 자주 언급됩니다. **CoreXL** 은 멀티코어에서 Firewall 커널을 여러 벌 복제해 코어마다 병렬로 돌리는 기술이고(각 복제본이 **CoreXL Firewall Instance**, 들어오는 트래픽을 분배하는 부분이 **CoreXL SND**), **SecureXL** 은 게이트웨이를 지나는 IPv4·IPv6 트래픽을 가속 합니다. 어느 것이든 업그레이드·설치 후 게이트웨이 성능에 직결되는 기반 기술입니다.

Software Blade — 기능의 단위

Check Point의 기능은 **Software Blade** 단위로 켜고 끕니다. 게이트웨이 쪽 Blade는 트래픽의 특정 측면을 검사 하고(IPS·Anti-Virus·Anti-Bot·Application Control·URL Filtering·IPsec VPN·Mobile Access·Threat Emulation 등), 관리 서버 쪽 Blade는 관리 기능 을 더합니다(Network Policy Management·Endpoint Policy Management·Logging & Status·Compliance·Provisioning 등). 어떤 Blade를 켜느냐가 곧 그 장비의 역할이 되므로, 설치 후 첫 구성에서 정합니다.

이 용어들을 손에 쥐었다면, 이제 시작하기 — 배포 시나리오로 넘어가 R82을 어떤 형태로 펼칠지부터 정해 봅시다.

02 시작하기 — 배포 시나리오

시작하기 — 배포 시나리오

R82을 설치하거나 업그레이드하기 전에, 무엇을 어디에 어떻게 펼칠지부터 정하는 것 이 첫걸음입니다. 이 장은 시작 전 점검 사항과, Check Point가 지원하는 네 가지 배포 시나리오를 그림으로 풀어 설명합니다. 이 가이드는 appliance와 open server에 Gaia 운영체제를 올려 R82을 운영하는 관리자 를 위한 것입니다.

시작하기 전에 — 두 가지는 꼭

설치든 업그레이드든, 손대기 전에 반드시 두 가지를 해야 합니다.

> 중 요
>
> R82을 설치·업그레이드하기 전에: 첫째, R82 Release Notes를 읽으세요. 둘째, 현재 시스템을 백업하세요(백업과 복원).

처음 도입하는 고객이라면 **Check Point User Center** 에서 사용자·계정을 관리하고, 제품을 활성화하고, 지원을 받고, 서비스 요청을 열고, 기술 지식 베이스를 검색할 수 있습니다.

설치·업그레이드 마법사는 디스크에 제품을 깔 공간이 충분한지 자동으로 확인 합니다. 공간이 모자라면 필요한 용량·설치 경로·현재 가용 공간을 알려 주는 오류가 뜨므로, 공간을 확보한 뒤 다시 진행하면 됩니다.

네 가지 배포 시나리오

Check Point 제품은 상황에 따라 여러 형태로 펼칠 수 있습니다. 핵심은 관리 서버와 게이트웨이를 "나눌지 합칠지", 그리고 가용성을 어디까지 줄지 입니다.

가장 일반적인 형태는 **Distributed Deployment(분산 배포)** 입니다. Security Management Server와 Security Gateway를 서로 다른 컴퓨터에 설치하고 네트워크로 연결 합니다. 관리와 집행이 분리돼 있어 규모 확장과 운영이 깔끔합니다.

!① Security Management Server ② 네트워크 연결 ③ Security Gateway — 관리 서버와 게이트웨이를 다른 컴퓨터에 분리한 분산 배포
① Security Management Server ② 네트워크 연결 ③ Security Gateway

이를 한 대로 줄인 것이 **Standalone Deployment** 입니다. Security Management Server와 Security Gateway를 같은 컴퓨터에 함께 설치 해, 소규모 환경에서 장비 수를 줄입니다(Standalone 설치).

!① Security Management Server ③ Security Gateway ② 같은 컴퓨터 — 관리 서버와 게이트웨이를 한 대에 합친 Standalone 배포 *① Security Management Server ③ Security Gateway — ② 같은 컴퓨터에 함께 설치*

가용성을 높이고 싶다면 **Management High Availability** 가 있습니다. Primary 관리 서버와 Secondary 관리 서버를 두고 데이터베이스를 수동 또는 일정에 따라 동기화 해 서로를 백업합니다. 관리자는 한쪽을 Active, 다른 쪽을 Standby로 두며, Active 서버가 죽으면 Standby를 Active로 승격 합니다.

!① Primary Security Management Server ② 직접·간접 연결 ③ Secondary Security Management Server — 두 관리 서버가 데이터베이스를 동기화하는 Management High Availability *① Primary Security Management Server ② 직접·간접 연결 ③ Secondary Security Management Server*

가장 촘촘한 형태가 **Full High Availability** 입니다. 두 Check Point appliance가 각각 ClusterXL Cluster Member이자 Security Management Server로 동시에 동작 하는 High Availability 구성입니다. 한 appliance(①)의 관리 서버가 Primary·ClusterXL이 Active로, 다른 appliance(③)의 관리 서버가 Secondary·ClusterXL이 Standby로 돌고, 둘은 동기화 연결(②)로 트래픽 정보를 주고받습니다. 유지보수 부담을 줄이는 대신, Standalone 구성을 지원하는 Check Point appliance에서만 배포·구성할 수 있 다는 제약이 있습니다(R82 Release Notes 및 Standalone 설치 참고).

!① appliance 1(Primary 관리 서버·Active ClusterXL) ② 동기화 연결 ③ appliance 2(Secondary 관리 서버·Standby ClusterXL) — Full High Availability *① appliance 1(Primary·Active) ② 동기화 연결 ③ appliance 2(Secondary·Standby)*

어떤 시나리오를 고르든 출발점은 같습니다 — 먼저 Gaia 운영체제를 설치하고 첫 구성을 마친 뒤, 역할에 맞는 관리 서버·게이트웨이를 얹는 순서입니다.

03 백업과 복원

백업과 복원

업그레이드는 언제든 어긋날 수 있으므로, 손대기 전에 되돌아갈 수 있는 안전망을 만들어 두는 것 이 무엇보다 중요합니다. 이 장은 무엇을·언제·어떻게 백업해야 하는지, 그리고 장비 종류별로 어떤 방법을 쓰는지를 정리합니다. 핵심은 "스냅샷·백업·CPinfo를 두 번, 그리고 외부 저장소로" 입니다.

언제 백업하나 — 두 번의 시점

좋은 백업 습관은 시점을 둘로 나눕니다. **업그레이드 직전** 에 원본 시스템의 스냅샷을 뜨고, 백업을 받고, CPinfo 파일을 수집 합니다.
스냅샷은 전체 구성을 통째로 백업하고, 백업 파일은 가장 중요한 구성을 쉽게 꺼내 쓰게 하며, CPinfo는 DiagnosticsView 도구(sk125092)로 핵심 구성을 한눈에 보게 해 줍니다(CPinfo 수집은 sk92739).

두 번째 시점은 **Pre-Upgrade Verifier(PUV)** 가 성공적으로 끝나고 더 이상 권고 사항을 내놓지 않은 직후 입니다. 이때 스냅샷·백업·CPinfo를 한 번 더 받습니다. 그런 다음 CPinfo·스냅샷·백업·내보낸 데이터베이스 파일을 모두 외부 저장 장치로 옮기되, 반드시 바이너리 모드로 전송 합니다.

Management High Availability 환경이라면 일관성이 관건입니다. 모든 Security Management Server 또는 Multi-Domain Server의 백업·스냅샷을 같은 시점에 함께 수집·복원 해야 하며(Multi-Domain Log Server는 예외), 백업이 끝날 때까지 다른 관리자가 SmartConsole에서 변경하지 못하게 막아야 합니다.

장비 종류별 백업 방법

무엇을 백업하느냐에 따라 도구가 달라집니다.

Security Management Server 는 Gaia에서라면 먼저 Gaia 스냅샷을 뜨고, `migrate_server export` 명령으로 백업을 받은 뒤, Log Exporter 구성(sk127653)까지 챙깁니다. Linux에서는 스냅샷 단계만 빠지고 나머지는 같습니다.

Multi-Domain Server 는 스냅샷 뒤에 `mds_backup` 명령으로 전체 백업 을 받고 Log Exporter 구성을 수집합니다(Linux는 스냅샷 생략).

Security Gateway·Cluster Member 는 단순합니다 — Gaia 스냅샷만 뜨면 됩니다. **VSX 환경** 은 별도 절차가 필요해 sk100395(VSX Gateway 백업·복원)를 따르고, 가상 머신 환경은 해당 가상 플랫폼 벤더 문서를 봅니다.

> 팁
>
> 더 깊은 내용은 sk108902(Gaia OS 백업 모범 사례), Gaia Administration Guide, Multi-Domain Security Management Administration Guide의 `mds_backup` 절, Command Line Interface Reference Guide의 `migrate_server` 명령을 참고하세요.

백업이라는 안전망을 갖췄다면, 이제 실제 설치로 들어갑니다 — 모든 것의 바탕인 Gaia 운영체제 설치와 첫 구성부터 시작합니다.

04 Gaia 운영체제 설치와 첫 구성

Gaia 운영체제 설치와 첫 구성

모든 Check Point 제품은 **Gaia** 운영체제 위에서 돕니다. 그래서 어떤 배포 시나리오를 고르든 출발점은 같습니다 — Gaia를 깨끗하게(Clean Install) 깐 뒤, **First Time Configuration Wizard** 로 첫 구성을 마치는 일입니다. 이 장은 appliance와 open server에 Gaia를 설치하는 여러 방법, 빠른 배포 도구 **Blink**, 그리고 첫 구성 마법사가 무엇을 묻는지를 개념·선택지 위주로 풀어 설명합니다. 세부 절차는 원문 "The Gaia Operating System" 절을 참고하세요.

Gaia를 어디에 까나 — appliance vs open server

설치 대상이 Check Point **appliance** 인지 **open server** 인지에 따라 방법이 갈립니다.

Check Point appliance 에는 세 갈래가 있습니다. 가장 간단한 것은 **factory defaults로 초기화** — 직렬 콘솔로 접속해 재부팅하고, 부팅 중 Boot menu에서 "Reset to factory defaults"를 골라 마지막 Clean Install 버전으로 되돌리는 방법입니다. 또는 **Bootable USB** 로 Clean Install ISO를 부팅 하거나(USB는 sk65205의 **ISOmorphic Tool** 로 제작), Gaia가 이미 깔려 있다면 CPUSE로 로컬 설치할 수 있습니다.

> 중요
>
> ISOmorphic Tool은 항상 최신 빌드를 쓰세요. 오래된 빌드를 쓰면 설치가 실패할 수 있습니다.

Open Server 도 비슷하되 미디어 선택이 더 넓습니다. **DVD-ROM** 으로 ISO를 구워 BIOS에서 부팅 순서를 잡아 설치 하거나, **Bootable USB** 또는 CPUSE 로 깝니다. DVD 설치는 설치가 끝난 뒤 재부팅 전에 DVD를 빼고, BIOS에서 부팅 순서를 다시 Hard Disk로 돌려놓는 점만 유의하면 됩니다. 어느 경로든 마지막은 First Time Configuration Wizard 실행으로 끝납니다.

Blink — 5~7분 만에 게이트웨이 배포

Blink 는 Gaia를 빠르게 배포하는 절차 로, 아직 첫 구성 마법사를 돌리지 않은 appliance에 깨끗한 Security Gateway를 5~7분 안에 깔아 줍니다. Clean Gateway·Hotfix·최신 Software Blade 시그니처까지 한 번에 설치 되고, 수동 마법사 실행을 대신합니다. Blink 이미지는 USB로 굽거나 appliance로 내려받아 쓰며, USB를 첫 구성 마법사가 뜨기 전에 꽂아 두면 과정이 자동으로 시작 됩니다.

여기에 더해 Blink는 특별한 XML 파일로 무인(unattended) 설치 도 지원합니다. 호스트 이름, Gaia 관리자 암호, 네트워크 옵션(IP·서브넷·기본 게이트웨이), **SIC** 키, 클러스터 멤버십, 업로드·다운로드 승인 같은 값을 미리 정의해 둘 수 있습니다(자세히는 sk120193).

비슷한 무인 설치는 ISOmorphic Tool로도 가능합니다 — 숙련된 관리자가 특정 인터페이스의 IP·넷마스크·기본 게이트웨이를 미리 설정한 USB를 만들어 보내면, 받은 사람은 그저 꽂고 재부팅만 하면 됩니다(단 open server는 무인 설치 미지원).

디스크 파티션 — 미리 정해진 크기 조정

appliance에서는 디스크 파티션 크기가 미리 정해져 있습니다. 일부 Smart-1 모델(525·5050·5150, 50·150·3050·3150)에서는 설치 시작 후 첫 20초 안 에만 기본 파티션을 바꿀 수 있고, 이 창을 놓치면 비대화식 설치가 그대로 진행됩니다. Open Server 설치 시에는 System-swap·System-root·Logs·Backup and upgrade 파티션이 기본 크기로 잡히며, system-root와 logs 파티션 크기를 바꾸면 backup·upgrade 파티션 용량이 자동으로 따라 조정 됩니다(상세는 sk95566). 설치를 마친 뒤에는 Expert 모드에서 `df -h` 로 파티션 크기를 보고, Gaia Portal의 Maintenance > Snapshot Management에서 백업 이미지용 공간을 확인합니다.

First Time Configuration Wizard — 첫 구성 마법사

Gaia를 처음 깔고 나면 **First Time Configuration Wizard** 로 시스템과 그 위의 Check Point 제품을 구성합니다. **Gaia Portal**(웹) 또는 **CLI Expert 모드** 둘 중 하나 로 돌릴 수 있습니다.

Gaia Portal 방식은 직관적입니다 — 컴퓨터를 Gaia 장비에 연결하고, 같은 서브넷의 정적 IPv4를 잡은 뒤, 브라우저로 `https://<Gaia 관리 인터페이스 IP>` 에 접속해 기본 계정 `admin` / `admin` 으로 로그인 하면 마법사가 열립니다. 마법사 창들은 제품·하드웨어에 따라 다르게 나타나며, 큰 흐름은 다음을 차례로 묻습니다.

먼저 **Deployment Options** 에서 이 Gaia를 그대로 구성할지(Continue), Check Point Cloud나 USB에서 다른 버전을 새로 깔지, 기존 스냅샷을 가져올지 를 정합니다. 이어 **Authentication Details** 에서 Expert 모드 암호와 Maintenance Mode(GRUB) 암호를 잡는데, 보안상 둘을 서로 다르게 두는 것이 권장 됩니다. **Management Connection** 에서는 Gaia Portal·CLI 접속에 쓸 주 관리 인터페이스와 그 IP를 정합니다.

> 중요
>
> R82은 Gaia 관리 인터페이스에 IPv6 주소를 지원하지 않습니다(알려진 제한 PMTR-47313).

그다음 **Internet Connection**(선택), **Device Information**(호스트 이름·DNS·프록시), **Date and Time**(수동 또는 NTP)을 채웁니다. 여기까지는 어떤 제품이든 공통입니다.

무엇을 설치할지 정하기 — Installation Type·Products

마법사의 핵심 분기점은 **Installation Type** 과 **Products** 창입니다. 여기서 이 Gaia가 어떤 역할이 될지 가 결정됩니다.

크게 두 갈래입니다. **Security Gateway and/or Security Management** 를 고르면 단일 Security Gateway·Cluster Member·Security Management Server(Management High Availability 포함)·Endpoint Security Management Server·Endpoint Policy Server·CloudGuard Controller·전용 Log Server·전용 SmartEvent Server·Standalone 중 하나를 깔 수 있고, **Multi-Domain Server** 를 고르면 Multi-Domain Server(HA 포함)나 전용 Multi-Domain Log Server를 깝니다. Scalable Platform(ElasticXL·Maestro·Chassis)은 단일 Security Gateway 옵션만 지원 한다는 점을 기억하세요.

게이트웨이를 고른 경우 **Unit is a part of a cluster** 를 켜면 클러스터 멤버가 되며, 클러스터 종류로 **ElasticXL**(HyperScale 기반)·**ClusterXL**·**VRRP Cluster** 중 하나를 고릅니다. 관리 서버 쪽이면 **Define Security Management as** 에서 Primary·Secondary·Log Server/SmartEvent only를 정합니다.

뒤이어 나오는 창들은 앞 선택에 따라 달라집니다. 게이트웨이라면 **Dynamically Assigned IP** 로 DAIP 여부 를, **Secure Communication to Management Server** 에서 일회용 Activation Key 를 정합니다(이 키는 나중에 SmartConsole에서 객체를 만들고 **SIC** 를 초기화할 때 다시 입력). 관리 서버라면 SmartConsole 로그인용 **Security Management Administrator** 와, 접속을 허용할 **GUI Clients**(모든 IP·이 컴퓨터·특정 네트워크·IP 범위)를 정합니다. Multi-Domain Server라면 Leading VIP Interface와 GUI Clients를 추가로 묻습니다.

마지막 **Summary** 창에서는 EULA와 함께 Software Blade 계약·보안 업데이트·기능 업데이트 자동 다운로드, 익명 정보·core dump 공유 여부를 정합니다(보안·비보안 데이터 다운로드는 모두 강력 권장).

> 주의
>
> core dump 파일은 메모리 스냅샷이라 개인·민감 정보를 담을 수 있으므로, 공유 여부는 신중히 정하세요.

마법사가 끝나면 Gaia가 재부팅하고 초기화가 몇 분간 백그라운드로 진행됩니다. 관리 서버·Multi-Domain Server는 이 시간 동안 SmartConsole에서 읽기 전용으로만 접근됩니다. 구성이 끝났는지는 `/var/log/ftw_install.log` 파일에 `installation succeeded` 또는 `FTW: Complete` 가 찍혔는지 로 확인합니다.

CLI로 자동화하기 — config_system

마법사를 손으로 클릭하는 대신, Expert 모드의 `config_system` 유틸리티로 첫 구성을 자동화할 수 있습니다. 대화식 도구가 아니라, 미리 적어 둔 값으로 첫 구성을 한 번에 적용 하는 비대화식 자동화 도구입니다(Scalable Platform에서는 해당 Security Group의 Expert 모드에서 실행).

쓰는 방식은 세 가지입니다 — `config_system --config-string` 으로 `parameter=value` 쌍을 `&` 로 이어 한 줄로 넘기거나, `config_system -f <파일>` 로 구성 파일을 읽거나, 먼저 `config_system -t <경로>` 로 템플릿을 만든 뒤 값을 채워 쓰는 방법입니다. 적용 전에는 `config_system --config-file <파일> --dry-run` 으로 파일이 유효한지 검증하고, 끝나면 시스템을 재부팅합니다. 쓸 수 있는 파라미터 전체는 `config_system --list-params` 로 보며(버전마다 달라질 수 있음), 예시 문자열은 다음과 같습니다.

```
config_system --config-string "hostname=myhost&domainname=somedomain.com&install_security_gw=true&gateway_daip=false&
```

주요 파라미터를 흐름으로 보면, 설치 역할은 `install_security_gw` · `install_security_managment` · `install_security_vsx` · `install_mds_primary` · `install_mds_secondary` · `instal` 로 정하고, 네트워크는 `ipaddr_v4` · `masklen_v4` · `default_gw_v4` · `iface` , 관리자 계정은 `mgmt_admin_radio` · `mgmt_admin_name` · `mgmt_admin_passwd` , 게이트웨이가 관리 서버에 붙을 키는 `ftw_sic_key` 로 줍니다. 클러스터 멤버는 `gateway_cluster_member=true` (이때 `gateway_daip` 은 반드시 false), DNS·NTP·프록시·시간대·업데이트 다운로드 (`download_info` 등)도 모두 파라미터로 지정합니다.

설치 후 관리 인터페이스와 IPv6

Gaia 관리 인터페이스는 처음에 **192.168.1.1** 로 잡혀 있습니다. 이 IP는 첫 구성 마법사 중에 또는 나중에 바꿀 수 있는데, 마법사 중에 바꾸면 브라우저 연결을 유지하려고 기존 IP가 보조 IP로 남습니다. 설치 후에는 Gaia Portal의 Network Management > Network Interfaces에서 관리 인터페이스를 지정·편집하거나, Gaia Clish에서 `show management interface` → `set management interface <이름>` → `set interface <이름> ipv4-address <IP> subnet-mask <마스크>` → `save config` 로 바꿉니다.

IPv6 는 마법사에서 IPv6 주소를 넣었다면 자동으로 켜 지고, 그러지 않았다면 나중에 수동으로 켭니다 — Gaia Portal의 System Management > System Configuration에서 IPv6 Support를 On으로 하거나, Gaia Clish에서 `set ipv6-state on` → `save config` → `reboot` 합니다(Scalable Platform은 gClish에서). 어느 쪽이든 재부팅 전에는 IPv6 지원이 활성화되지 않 습니다.

Gaia 바탕을 깔았으니, 이제 역할별 제품을 얹을 차례입니다 — 관리 서버 설치로 이어집니다.

05 관리 서버 설치

관리 서버 설치

게이트웨이에게 규칙을 내려보내는 본부가 관리 서버입니다. 이 장은 Security Management Server부터 Multi-Domain Server·Log Server·SmartEvent Server·Endpoint 서버·CloudGuard Controller까지, 여러 종류의 관리 서버를 설치하는 공통 흐름 을 한자리에 모았습니다. 종류는 달라도 뼈대는 똑같습니다 — Gaia를 깔고, 첫 구성 마법사에서 역할을 고르고, 라이선스를 넣은 뒤, SmartConsole에서 객체를 만들어 마무리 합니다. 세부 절차는 원문 각 절을 참고하세요.

공통 설치 패턴

어떤 관리 서버든 두 단계로 나뉩니다. 먼저 장비에서 Gaia를 설치하고 첫 구성 마법사를 돌려 역할을 정한 뒤 유효한 라이선스를 넣고(라이선스 관리), 그다음 SmartConsole에서 그 서버를 나타내는 객체를 만들어 Software Blade를 켜고 데이터베이스를 설치 합니다. 두 번째 서버나 전용 서버라면 여기에 **SIC**(Secure Internal Communication) 초기화 한 단계가 더 붙습니다.

마법사에서 무엇을 고르느냐가 곧 서버의 정체가 됩니다. 단일 도메인 관리 서버 계열은 Installation Type에서 **Security Gateway and/or Security Management** 를 고른 뒤 Products에서 **Security Management only** 를 선택하고, Multi-Domain 계열은 Installation Type에서 바로 **Multi-Domain Server** 를 고릅니다.

Security Management Server — Primary와 Secondary

가장 기본인 **Security Management Server** 는, 첫 구성 마법사에서 Security Management only를 고른 뒤 Define Security Management as 에서 **Primary** 를 선택하고, GUI Clients 창에서 SmartConsole로 접속을 허용할 컴퓨터(모든 IP·이 컴퓨터·특정 네트워크·IP 범위) 를 정합니다. 설치 후 SmartConsole에서 서버 객체를 열어 Management 탭에서 필요한 Software Blade를 켜면 끝입니다.

가용성을 위해 두 번째 서버를 둘 때는 Management High Availability가 됩니다. Secondary는 반드시 Primary와 같은 Gaia 설치 버전을 써야 하고, 마법사에서 Define Security Management as 를 **Secondary** 로 고른 뒤 Secure Internal Communication 창에서 일회용 Activation Key(4~127자) 를 입력합니다. 그다음 SmartConsole로 Primary에 접속해 Secondary를 나타내는 **Check Point Host** 객체를 만들고 — 이름·IP·플랫폼(Hardware/Version R82/OS Gaia)을 채우고 Management 탭에서 Network Policy Management를 켠 뒤 — Communication에서 같은 Activation Key를 넣어 SIC를 Initialize(Trust state가 Established가 되어야 함) 합니다. 마지막으로 Install database로 모든 객체에 데이터베이스를 설치하고, Management High Availability 화면에서 두 서버가 동기화되는지 확인합니다.

> 참 고
>
> Management High Availability 환경에서 SmartEvent Software Blade는 Active 관리 서버에서만 지원됩니다(sk25164).

설치 후에는 로그 인덱스용 디스크 공간도 챙겨야 합니다. Log Indexing을 켜면 `$RTDIR/log_indexes/` 에 인덱스 파일이 쌓이는데, 가용 공간이 정해진 최소값(기본 5000 MB 또는 가용 공간의 15%) 아래로 떨어지면 오래된 인덱스부터 지웁니다. 이 최소값은 SmartConsole에서 서버 객체의 Logs > Storage에서 조정합니다.

전용 Log Server·SmartEvent Server

로그만 따로 받는 **전용 Log Server** 나 이벤트 분석용 **SmartEvent Server** 도 같은 패턴입니다. 마법사에서 Define Security Management as 를 **Log Server / SmartEvent only** 로 고르고 Activation Key를 잡은 뒤, SmartConsole에서 Check Point Host 객체를 만들어 SIC를 세웁니다. Software Blade는 역할에 따라 — Log Server라면 Logging & Status(Identity Awareness를 쓰면 Identity Logging까지), SmartEvent Server라면 SmartEvent Server와 SmartEvent Correlation Unit — 를 켭니다. 전용 SmartEvent Server와 전용 Correlation Unit을 따로 설치할 수도 있습니다.

Multi-Domain 환경이라면 한 단계 더 나아간 **Domain Dedicated Log Server** 가 있습니다. R81부터 특정 Domain의 로그만 받는 전용 Log Server를 별도 컴퓨터에 둘 수 있어, 규제 요건에 맞춰 로그를 Multi-Domain 환경과 분리된 네트워크에 둘 수 있습니다. 이 Log Server는 연결된 Domain Server하고만 통신하며 다른 Domain은 그 로그에 접근하지 못 합니다(다만 Domain Dedicated Log Server에 SmartConsole로 붙어 정책을 보는 것은 미지원). 구성은 R82 Multi-Domain Server를 깐 뒤 일반 전용 Log Server를 설치하고, SmartConsole로 해당 Domain에 접속해 그 Log Server 객체를 추가하는 순서입니다. R82로 업그레이드한 환경에서는 마지막에 각 Multi-Domain Server에서 `$MDS_FWDIR/scripts/cpm.sh -tm -op reset -d all -sd` 를 한 번 돌려 주어야 합니다.

> 참 고
>
> Multi-Domain 환경에서는 로그·인덱스 디스크 공간을 Multi-Domain Server 객체에서 정하며, 그 설정이 모든 Domain Management Server에 적용됩니다.

Multi-Domain Server와 Multi-Domain Log Server

규모가 크면 **Multi-Domain Server(MDS)** 를 깝니다. 마법사 Installation Type에서 **Multi-Domain Server** 를 고른 뒤 **Primary Multi-Domain Server** 를 선택하고, **Leading VIP Interface**(Multi-Domain 환경의 주 인터페이스) 와 GUI Clients(Any host 또는 특정 IP), 그리고 관리자 계정을 정합니다. **Secondary Multi-Domain Server** 는 Primary와 같은 방식이되 Activation Key로 SIC를 세웁니다. 로그 전용인 **Multi-Domain Log Server(MDLS)** 는 Installation Type에서 Multi-Domain Server를 고른 뒤 **Multi-Domain Log Server** 를 선택하고 Leading VIP Interface와 Activation Key를 잡는 식으로, 거의 동일한 흐름을 따릅니다.

Endpoint 서버와 CloudGuard Controller

엔드포인트 보안을 관리하는 **Endpoint Security Management Server** 와, 부하를 나눠 받는 **Endpoint Policy Server** 도 설치 뼈대는 일반 관리 서버와 같습니다 — 마법사에서 Security Management only·Primary를 고르고 라이선스를 넣은 뒤 SmartConsole에서 마무리합니다. Endpoint 환경은 서비스 연결 포트와 디스크 공간 요건이 추가로 있으니(원문 "Connection Port to Services"·"Disk Space" 절), 방화벽 사이에 둘 때 포트 개방을 확인하세요.

CloudGuard Controller 도 일반 Security Management Server로 설치한 뒤, 관리 서버 명령줄에서 `cloudguard on` 으로 켜고, 해당 게이트웨이에서 Identity Awareness Software Blade를 활성화하면 됩니다(상세는 R82 CloudGuard Controller Administration Guide).

Linux 위의 관리 서버

관리 서버는 Gaia 외에 Red Hat Enterprise Linux 위에도 올릴 수 있습니다. 다만 이 경우는 별도 절차가 필요해 sk44925·sk98760을 따르고 Check Point Support의 구체적 설치 지침을 받 아야 합니다.

본부를 세웠으니, 이제 그 본부를 다룰 도구를 깝니다 — SmartConsole 설치로 넘어갑니다.

06 SmartConsole 설치

SmartConsole 설치

SmartConsole 은 Check Point 환경을 관리하는 GUI 클라이언트 입니다. 관리 서버를 깔았다면, 그 서버에 붙어 정책을 만들고 장비를 다루려면 Windows 컴퓨터에 SmartConsole을 깔아야 합니다. 이 장은 설치 파일을 어디서 받고, 어떻게 깔고, 어떻게 로그인하는지 를 간단히 정리합니다.

설치 파일 받기

SmartConsole 설치 패키지는 세 경로로 받을 수 있습니다. **R82 Home Page SK** 의 Downloads 섹션에서 받거나, **Check Point Support Center** 에서 "R82 SmartConsole"을 검색해 받거나, 가장 간편하게는 관리 서버의 **Gaia Portal** Overview 페이지에서 "Download Now!" 로 곧장 내려받습니다. SmartConsole 요구 사항은 R82 Release Notes를 확인하세요.

설치와 로그인

설치는 Windows에서 단순합니다 — 설치 파일을 SmartConsole 클라이언트로 쓸 Windows 컴퓨터로 옮긴 뒤, 관리자 권한으로 실행 하고 화면 지시를 따르면 됩니다.

로그인할 때는 SmartConsole을 열고 Security Management Server·Multi-Domain Server·Domain Management Server의 IP나 호스트 이름 을 넣은 뒤 관리자 자격 증명이나 인증서 파일로 들어갑니다. 첫 로그인에서는 관리 서버가 연결을 인증하며, 설치 때 생성된 fingerprint로 연결을 한 번 확인 하게 됩니다(이후로는 묻지 않음). 여러 관리자가 동시에 로그인할 수도 있습니다.

> 참 고
>
> 접속이 안 되면 SmartConsole 클라이언트가 관리 서버의 포트 **18190·18264·19009** 에 닿을 수 있는지 확인하세요(sk52421: Check Point 소프트웨어가 쓰는 포트).

도구가 준비됐으니, 이제 실제로 트래픽을 막아설 장비를 깝니다 — Security Gateway·VSX Gateway 설치로 넘어갑니다.

07 Security Gateway·VSX Gateway 설치

Security Gateway·VSX Gateway 설치

길목에서 트래픽을 검사하고 정책을 집행하는 장비가 **Security Gateway** 입니다. 이 장은 단일 Security Gateway를 설치해 관리 서버에 붙이는 흐름 과, 그 위에 여러 가상 게이트웨이를 올리는 **Legacy VSX Gateway** 설치를 다룹니다. 이 절차는 Check Point appliance와 open server 모두에 해당 하되, 3000 미만 Small Office 모델에는 적용되지 않습니다. 세부 절차는 원문 해당 절을 참고하세요.

Security Gateway 설치의 두 단계

게이트웨이도 관리 서버처럼 두 단계입니다. 먼저 장비에서 Gaia를 설치하고 첫 구성 마법사를 돌리고, 그다음 SmartConsole에서 게이트웨이 객체를 만들어 관리 서버와 **SIC** 신뢰를 세우는 순서입니다.

첫 구성 마법사에서는 Installation Type에서 Security Gateway and/or Security Management를 고른 뒤 Products에서 **Security Gateway only** 를 선택하고, Unit is a part of a cluster는 체크를 풀어 둡니다(클러스터는 다음 장). 이어 **Dynamically Assigned IP** 로 이 게이트웨이가 DHCP로 IP를 받는 DAIP 게이트웨이인지 정하고, **Secure Internal Communication** 창에서 일회용 Activation Key(4~127자) 를 입력합니다. 마지막으로 유효한 라이선스를 넣습니다(라이선스 관리).

SmartConsole에서 게이트웨이 객체 만들기 — Wizard와 Classic

설치 후에는 이 게이트웨이를 관리할 Security Management Server나 Domain Management Server에 SmartConsole로 접속해, 새 Gateway 객체를 만듭 니다. 두 가지 방식이 있습니다.

Wizard Mode 는 단계별로 안내합니다. 게이트웨이 이름·플랫폼(하드웨어 종류)·IP를 정하는데, 정적 IP라면 첫 구성 마법사의 Management Connection에서 잡은 것과 같은 IPv4·IPv6를 넣 고(DHCP로 받는다면 Classic Mode로 넘어감), Trusted Communication 페이지에서 같은 Activation Key로 신뢰를 지금 세우거나 나중으로 미룰 수 있습니다. 끝에서 "Edit Gateway properties"를 골라 Network Security·Threat Prevention 탭에서 Software Blade를 켭니다.

Classic Mode 는 속성 창에서 직접 채웁니다 — 이름·IP를 넣고(DHCP면 Dynamic Address 선택), Communication에서 Platform(3000 이상 모델·open server는 Open server/Appliance, 3000 미만 Small Office는 Small Office Appliance)을 고른 뒤 같은 Activation Key로 Initialize 합니다. Certificate state가 Established가 되어야 SIC가 선 것 입니다. 만약 안 서면, 게이트웨이 명령줄에서 물리 연결(ping)을 확인하고 `cpconfig` 의 Secure Internal Communication 메뉴에서 키를 바꾼 뒤, SmartConsole에서 Reset → 같은 키 입력 → Initialize 를 다시 합니다. Platform 섹션에서 Hardware·Version(R82)·OS(Gaia)를 맞추고 Blade를 켠 뒤 세션을 Publish합니다.

마지막으로 정책을 만듭니다 — Security Policies에서 새 정책과 레이어를 만들고, Access Control 규칙을 짜 게이트웨이에 설치하고, 이어 Threat Prevention 규칙도 만들어 설치 합니다(상세는 R82 Security Management·Threat Prevention Administration Guide).

Legacy VSX Gateway 설치 — VSNext와의 갈림길

한 물리 장비 위에 여러 가상 게이트웨이를 올리는 것이 **VSX** 입니다. R82부터 VSX에는 두 모드가 있습니다 — 새로운 **VSNext**(ElasticXL 기반, 클러스터 장에서 다룸)와, 기존 방식인 **Legacy VSX** 입니다. 여기서는 Legacy VSX Gateway의 Clean Install을 다룹니다(실패한 VSX 복구나 non-DMI 구성은 R82 VSX Administration Guide).

Gaia 설치와 첫 구성 마법사는 일반 Security Gateway와 똑같습니다 — Security Gateway only, 클러스터 해제, DAIP 선택, Activation Key, 라이선스. 다른 점은 SmartConsole 단계입니다. 일반 Gateway가 아니라 **VSX** > **Gateway** 객체를 만들어 VSX Gateway Wizard 를 띄우고, 이름·IPv4·IPv6·Version(R82)을 정한 뒤 Activation Key로 SIC를 Initialize합니다(Trust established 안 되면 동일하게 `cpconfig` 로 복구). 이어 Physical Interfaces Usage 페이지에서 물리 인터페이스를 확인 하고(한 물리 인터페이스에 여러 Virtual System을 직접 붙이려면 그 인터페이스를 **VLAN Trunk** 로 지정), 필요하면 첫 Virtual Switch·Virtual Router를 만들고(나중으로 미루는 것을 권장), VS0의 관리 접근 규칙을 정한 뒤 마칩니다.

> 중요
>
> 이 관리 접근 규칙은 VSX Gateway 자체(VS0의 맥락)에만 적용됩니다. VS0은 production 트래픽을 흘려보내는 용도가 아닙니다.

만든 뒤에는 Expert 모드에서 `vsx stat -v` 로 VSX 구성 상태를 확인 하는 습관이 중요합니다 — 각 단계마다 이 명령으로 점검합니다. VS0 객체에서 Network Security 탭의 Blade를 켜고(sk79700: VSX 지원 기능 참고), `<VSX Gateway 이름>_VSX` 라는 기본 정책을 설치 한 뒤 Threat Prevention 정책까지 깝니다. 그다음 각 Legacy Virtual Device(Virtual System·Switch·Router)를 구성하고, 각자의 Access Control·Threat Prevention 정책을 설치 합니다. VSX의 자세한 운영은 R82 VSX 관리자 가이드를 참고하세요.

여러 대를 묶어 가용성을 높이려면 다음 장으로 — ClusterXL·VSX·VRRP 클러스터 설치로 이어집니다.

08 ClusterXL·VSX·VRRP 클러스터 설치

ClusterXL·VSX·VRRP 클러스터 설치

게이트웨이 한 대가 죽으면 길목이 통째로 막힙니다. 그래서 게이트웨이를 여러 대 묶어 가용성과 성능을 높이는 것이 **클러스터** 입니다. 이 장은 R82이 지원하는 네 갈래의 클러스터 — 새로운 가상화 모드 **VSNext**, 표준인 **ClusterXL**, 기존 가상화 방식 **Legacy VSX Cluster**, 그리고 **VRRP Cluster** — 와, appliance 두 대로 관리·집행을 한꺼번에 묶는 **Full High Availability** 를 어떻게 설치하는지 개념·선택지 위주로 정리합니다. 세부 절차는 원문 해당 절과 R82 ClusterXL 관리자 가이드를 참고하세요.

클러스터 설치의 공통 뼈대

종류는 달라도 흐름은 단일 Security Gateway 설치의 연장입니다. 각 멤버에서 Gaia를 깔고 첫 구성 마법사에서 클러스터 멤버로 지정한 뒤, SmartConsole에서 **클러스터 객체** 를 만들어 각 멤버를 추가하고 SIC를 세우고, 인터페이스 역할(Cluster Virtual IP·동기화·private)을 정하는 순서입니다.

마법사 차이는 작습니다 — Products에서 Security Gateway only를 고른 뒤 **Unit is a part of a cluster** 를 켜고 클러스터 종류(ElasticXL·ClusterXL·VRRP)를 선택 합니다. 핵심은 클러스터가 외부에 보이는 **Cluster Virtual IP(VIP)** 와, 각 멤버의 고유 물리 IP 를 구분해 두는 것입니다. VIP를 멤버 물리 IP와 다른 네트워크에 두려면 멤버에 static route를 잡아야 합니다.

VSNext — ElasticXL·Maestro 위의 새 가상화 모드

R82부터 VSX에는 두 모드가 있습니다 — 새로운 **VSNext** 와 기존 **Legacy VSX** 입니다. VSNext는 **ElasticXL Cluster** 나 **Maestro Security Group** 에서만 켤 수 있습니다. 플랫폼을 깔 때(ElasticXL은 R82 Scalable Platforms Administration Guide, Maestro는 Quantum Maestro Getting Started Guide) 첫 구성 마법사에서 Unit is a part of a cluster → ElasticXL을 고르고 Gateway Virtualization에서 **Install as VSNext** 를 선택 합니다(Maestro는 Security Group 생성 시 Install as VSNext/VSX 선택). 한 번 VSNext로 깔면 나중에 전환할 수 없습니다.

플랫폼이 준비되면 필요한 Virtual Switch·Virtual Gateway를 구성하고(R82 VSX Administration Guide의 VSNext 장), SmartConsole에서 각 Virtual Gateway마다 **VSX > Gateway** 객체를 만들되 "VSNext mode on Scalable Platform cluster" 를 선택 해 객체를 잇습니다.

ClusterXL Cluster — 표준 클러스터

가장 일반적인 것이 **ClusterXL** 입니다. 각 멤버를 깐 뒤 SmartConsole에서 클러스터 객체를 만들 때 **Check Point ClusterXL** 을 고르고 모드(**High Availability** 또는 **Load Sharing**)를 정 합니다. 그다음 Cluster Members 페이지에서 멤버를 하나씩 추가 하는데, 각 멤버의 물리 IP를 첫 구성 마법사에서 잡은 값과 똑같이 넣고 같은 Activation Key로 Initialize해 Trust State가 Trust established가 되도록 합니다(안 되면 멤버에서 `cpconfig` 의 Secure Internal Communication으로 키를 바꾸고 Reset → Initialize).

핵심 단계는 **Cluster Topology** 입니다. 인터페이스마다 역할을 정합니다 — 트래픽 인터페이스는 "Representing a cluster interface"로 두고 Cluster Virtual IP·넷마스크를 잡고, 동기화 인터페이스는 "Cluster Synchronization > Primary only"(클러스터는 동기화 네트워크를 하나만 지원), 트래픽을 안 흘리는 인터페이스는 "Private use of each member" 로 둡니다. 마지막으로 Platform(Hardware·Version R82·OS Gaia)을 맞추고 ClusterXL Software Blade가 켜졌는지 확인한 뒤 정책을 설치합니다.

> 팁
>
> High Availability에서는 **Use State Synchronization** 을 켜 두는 것이 좋습니다. 페일오버 뒤 연결이 끊기지 않게 하기 때문입니다.

설치 마법사의 **ClusterXL and VRRP** 단계에서는 세부 동작을 고릅니다. 모드는 High Availability, Load Sharing(Multicast 또는 Unicast), Active-Active 중에서 정하고, High Availability라면 추가로 — 짧은 연결의 동기화를 늦춰 성능을 지키는 "Start synchronizing N seconds after connection initiation"(기본 3초, 2~60초), VIP에 같은 가상 MAC을 묶는 **Use Virtual MAC**(sk50840), 페일오버 복구 시 어느 멤버를 Active로 둘지 정하는 recovery 방식(현재 Active 유지 vs 우선순위 높은 멤버로 전환) 을 정합니다.

Legacy VSX Cluster와 VRRP Cluster

Legacy VSX Cluster 는 Legacy VSX Gateway를 클러스터로 묶은 것으로, R81.20 이하에서 그냥 "VSX"라 부르던 방식입니다. VSNext를 쓰지 않는 환경에서 여러 VSX Gateway를 묶을 때 씁니다(상세는 R82 VSX 관리자 가이드).

VRRP Cluster 는 ClusterXL 대신 업계 표준 VRRP(Virtual Router Redundancy Protocol)로 가용성을 구현 하는 Gaia 클러스터입니다. 멤버 설치와 SIC 세우기는 ClusterXL과 같되, 클러스터 객체에서 VRRP 모드를 골라 구성합니다. 멀티벤더 라우팅 환경 등 VRRP가 더 맞는 곳에서 선택합니다.

Full High Availability — 관리와 집행을 한 묶음으로

가장 촘촘한 형태가 **Full High Availability Cluster** 입니다. Check Point appliance 두 대가 각각 ClusterXL Cluster Member이면서 동시에 Security Management Server로 동작 해, 게이트웨이의 가용성과 관리 서버의 가용성을 한꺼번에 얻습니다. 한 appliance의 관리 서버가 Primary·ClusterXL이 Active로, 다른 쪽이 Secondary·Standby로 돌며 동기화 연결로 트래픽 정보를 주고받습니다.

> 중요
>
> Full High Availability는 Standalone 구성을 지원하는 Check Point appliance에서만 배포·구성할 수 있습니다(Standalone 설치, R82 Release Notes 참고).

이 구성은 관리와 집행이 한 장비에 얹혀 있어 로깅 옵션을 신중히 골라야 합니다(원문 "Recommended Logging Options" 절). 두 장비뿐이라 단순하지만, 그만큼 관리 서버 부하와 게이트웨이 부하가 같은 하드웨어를 나눠 쓴다는 점 을 감안해 규모를 잡아야 합니다.

클러스터까지 세웠다면, 더 작은 배포 형태와 설치 후 마무리로 넘어갑니다 — Standalone·Scalable Platform·설치 후 구성입니다.

09 Standalone·Scalable Platform·설치 후 구성

Standalone·Scalable Platform·설치 후 구성

여기서는 설치의 나머지 갈래와 마무리를 한자리에 모았습니다 — 관리와 집행을 한 대에 합치는 **Standalone**, 대규모로 확장하는 **Scalable Platform**, 설치 직후 챙기는 **Post-Installation Configuration**, 그리고 소프트웨어 패키지를 깔고 업데이트하는 **CPUSE** 입니다. 세부 절차는 원문 해당 절을 참고하세요.

Standalone — 한 대에 모두 담기

Standalone 배포에서는 한 Check Point 컴퓨터가 Security Gateway와 Security Management Server를 동시에 돌립 니다. Standalone 배포를 지원하는 Check Point appliance, 모든 open server, 그리고 가상 머신에서 쓸 수 있습니다(요구 사항은 R82 Release Notes).

구성 방식은 둘입니다. **Standard Mode** 는 가장 일반적입니다 — Gaia를 설치하고 첫 구성 마법사에서 Products의 **Security Gateway와 Security Management 를 둘 다** 선택하고, 클러스터는 끄고 Define Security Management as 는 Primary 로 둡니다. 이어 관리자 계정과 GUI Clients를 정하고, SmartConsole에서 Standalone 객체를 열어 Platform(Hardware·Version R82·OS Gaia)을 맞추고 Network Security·Threat Prevention·Management 탭의 Software Blade를 켠 뒤, Access Control 정책을 만들어 설치합니다.

또 하나는 **Quick Setup Mode** 로, Standalone을 지원하는 Check Point appliance에서만 쓸 수 있고 게이트웨이를 Bridge Mode로 설치합니다(상세는 sk102231). 기존 토폴로지에 손쉽게 끼워 넣고 싶을 때 유용합니다.

Scalable Platform — 대규모로 확장하기

Scalable Platform 은 처리 용량을 크게 키우는 플랫폼을 통칭합니다 — **ElasticXL Cluster**, **Maestro** 구성의 Security Group, **Scalable Chassis** 의 Security Group 입니다. 이들의 설치·구성은 이 가이드 범위를 넘어 별도 문서에서 다룹니다 — R82 Scalable Platforms Administration Guide, Quantum Maestro Getting Started Guide, 그리고 R82 Maestro 가이드를 참고하세요. 앞서 본 VSNext 클러스터도 이 Scalable Platform 위에서 동작합니다.

설치 후 구성 — Check Point Configuration Tool

설치를 마치고 재부팅했다면, **Check Point Configuration Tool** 로 마무리 설정을 챙기고 CPUSE에서 권장·가용 패키지를 확인 합니다. 이 도구는 장비 종류에 따라 명령과 메뉴가 다릅니다.

Security Management Server·전용 Log/SmartEvent Server 에서는 `cpconfig` 로 — Licenses and contracts, Administrator, GUI Clients, Random Pool, **Certificate Authority**(ICA 초기화·CA의 FQDN 설정), Certificate's Fingerprint(SmartConsole 연결 시 서버 신원 확인용), 자동 시작 — 을 다룹니다(SNMP Extension은 이제 쓰지 않고 Gaia Administration Guide의 SNMP를 사용).

Multi-Domain Server·MDLS 에서는 `mdsenv` 후 `mdsconfig` 로 — Leading VIP Interfaces(Domain Management Server의 가상 IP에 쓰는 외부 인터페이스), Licenses, Groups, Administrators, GUI Clients, Multi-Domain Server 자동 시작·시작 암호, MDS와 기존 Domain Management Server의 IPv6 지원 — 을 다룹니다(P1Shell은 지원 종료).

Security Gateway·Cluster Member 에서는 `cpconfig` 로 — Licenses, PKCS#11 Token, Random Pool, **Secure Internal Communication**(SIC 관리, Check Point 서비스 재시작 필요), 클러스터 멤버십 활성·비활성(재부팅 필요), VSX Cluster Member의 Per Virtual System State, Bridge Active/Standby용 ClusterXL, **CoreXL** 관리(변경 후 재부팅 필요), 자동 시작 — 을 다룹니다. SIC를 다시 세워야 할 때 여기서 합니다(sk65764: SIC 리셋 방법).

소프트웨어 패키지 설치 — CPUSE와 Central Deployment

Gaia에 핫픽스나 버전 패키지를 까는 방법은 크게 중앙 배포와 로컬 설치 로 나뉩니다.

게이트웨이·Cluster Member에 여러 대를 한꺼번에 깔 때는 **Central Deployment** 를 권장합니다 — SmartConsole의 Central Deployment로 관리되는 게이트웨이·클러스터에 패키지를 배포하며(Check Point Cloud 또는 관리 서버의 Package Repository에서), 명령줄 버전인 Central Deployment Tool(sk111158)도 있습니다.

한 대씩 직접 깔 때는 각 Gaia 컴퓨터에서 **CPUSE** 를 씁니다(sk92449). 인터넷에 연결돼 있으면 **Online** — Gaia Portal·Clish에서 패키지를 확인·다운로드·설치 하고, 연결이 없으면 **Offline** — 다른 컴퓨터로 R82 Home Page에서 패키지를 받아 Gaia로 옮긴(Import) 뒤 확인·설치 합니다.

> 참 고
>
> R80.20 이상에서 CPUSE로 R82 업그레이드를 할 때는, Gaia Portal의 Upgrades (CPUSE) > Status and Actions에서 R82 Upgrade 패키지를 골라 실시간 업그레이드 보고서를 볼 수 있습니다(관리 서버·Endpoint 서버·CloudGuard Controller·MDS·Log Server·MDLS·Standalone 구성 지원).

설치의 전 과정을 마쳤습니다. 이제 기존 환경을 R82으로 옮기는 업그레이드로 넘어갑니다 — 업그레이드 옵션과 사전 준비부터 시작합니다.

10 업그레이드 옵션과 사전 준비

업그레이드 옵션과 사전 준비

기존 환경을 R82으로 올리는 일은 새 설치보다 까다롭습니다 — 데이터를 지키면서 버전을 바꿔야 하기 때문입니다. 이 장은 업그레이드 전에 반드시 챙길 사전 조건과, R82이 지원하는 업그레이드 방식(CPUSE·Advanced Upgrade·Migration·Central Deployment), 그리고 이를 떠받치는 Upgrade Tools와 계약 확인 을 정리합니다. 세부 절차는 원문 해당 절을 참고하세요.

가장 중요한 순서 규칙

업그레이드에는 절대 어기면 안 되는 순서 가 있습니다. **관리 서버를 먼저 올린 뒤에야 그것이 관리하는 게이트웨이·Cluster Member를 올릴 수** 있습니다. 또 관리 서버가 거느린 전용 Log Server·SmartEvent Server는 관리 서버와 같은 버전으로 올려야 하고(SmartEvent Server는 Log Server와 같거나 높은 버전 가능), Multi-Domain Log Server는 Multi-Domain Server와 같은 버전으로 올려야 합니다. 이 순서를 지키지 않으면 관리가 어긋납니다.

지원되는 업그레이드 경로·최소 하드웨어·지원 게이트웨이는 R82 Release Notes에서, 알려진 제한은 R82 Known Limitations SK에서 반드시 먼저 확인하세요. 또 소스·대상 모든 컴퓨터에 유효한 라이선스와, 소프트웨어 업그레이드·메이저 릴리스를 포함하는 Service Contract 가 등록돼 있어야 합니다(라이선스 관리, sk33089).

업그레이드 전 점검 — 백업·커스텀 설정·로그 보존

가장 먼저 백업을 챙기고, 그다음 커스텀 설정을 따로 적어 둡니다. 업그레이드 과정은 기존 파일을 모두 기본 파일로 덮어쓰므로, 옛 버전의 커스텀 구성 파일을 새 버전에 그대로 복사하면 안 됩니다 — 버전마다 파일이 다를 수 있기 때문입니다. 그래서 `$FWDIR/conf/` · `$FWDIR/lib/` · `$CVPNDIR/conf/` · `$MDSDIR/conf/` 같은 디렉터리와 `fwkern.conf` · `fwaffinity.conf` · `local.arp` 같은 파일의 커스텀 변경을 기록해 두고, 업그레이드 후에 새 파일에 직접 다시 적용 해야 합니다(`.CPprofile.sh` 등 프로파일 스크립트에 특히 주의). VSX 환경에서는 이 디렉터리·파일 일부가 각 Virtual Device의 맥락에 따로 존재한다는 점도 유의하세요.

로그 보존 범위도 미리 정합니다. R81.20부터 관리 서버·Log Server를 올릴 때 로그 마이그레이션이 최근 180일치로 제한 됩니다. 이를 30~360일 사이로 바꾸려면 Expert 모드에서 `$FWDIR/conf/upgradeLogData.xml` 파일을 만들어 `<ImportLogDays>` 값을 지정합니다. 외부 저장 장치가 연결돼 있다면 sk66003에 따라 업그레이드 전에 장치를 분리하고, 올린 뒤 다시 연결해 로그 인덱스 설정을 복구 합니다.

> 중 요
>
> Mobile Access Software Blade를 커스텀해 쓴다면, 올리기 전에 `cvpnd.C`·`httpd.conf`·로컬 인증서·OTP 전화 목록 등 커스텀 설정을 검토·기록하고, 관리 서버 업그레이드 후 새 파일에 다시 적용하세요(자세히는 원문 해당 절).

Multi-Domain 환경에서는 업그레이드를 최적화하는 사전 작업이 권장됩니다 — Global Domain에서 쓰지 않는 Threat Prevention Profile을 지우고, IPS protection의 Staging Mode를 끄는 것입니다(sk142432). 그리고 업그레이드·마이그레이션을 시작하기 전에 연결된 모든 SmartConsole을 닫 아야 합니다.

High Availability 환경의 업그레이드 계획

가용성 구성은 순서를 신중히 잡아야 합니다. Security Management Server HA에서는 Primary를 먼저 올린 뒤, 두 서버가 통신하고 SIC가 정상인지 확인(sk179794)하고 Secondary를 올립 니다(R80.20.M1 소스라면 Secondary는 clean install 후 Primary에 연결). Multi-Domain Server HA에서는 모든 소스 서버에서 Pre-Upgrade Verifier를 돌려 문제를 고치고, Primary에서 Global Domain이 Active인지 확인한 뒤 Primary를 올리고, 통신·SIC를 확인하고 Secondary를 올립 니다. 어느 경우든 일관성을 위해 HA 환경의 모든 서버 백업·스냅샷은 같은 시점에 함께 수집·복원합니다.

디스크 공간 요건도 봅니다 — 대상 서버의 `/var/log/` 파티션은 소스의 최소 25% 이상 이어야 하고, Advanced Upgrade·Migration이라면 하드 디스크가 내보낸 데이터베이스 크기의 최소 5배 여야 합니다. 소스가 IPv4만(또는 IPv6만) 쓴다면 대상도 같은 IP 구성을 써야 합니다(업그레이드 후 변경은 가능).

업그레이드 방식 — 어느 길을 고를까

대상에 따라 쓸 수 있는 방식이 다릅니다.

게이트웨이·Cluster Member 는 **Central Deployment**(권장) — SmartConsole에서 Check Point Cloud나 Package Repository의 패키지를 관리되는 장비에 배포 하거나, 명령줄 버전인 **Central Deployment Tool**(sk111158), 또는 각 Gaia에서 직접 **CPUSE** 로 올립니다.

관리 서버·Log Server 는 세 갈래입니다. **CPUSE** 는 현재 Gaia에서 도는 컴퓨터를 같은 자리에서 그대로 올리 고(가장 단순, sk92449), **Advanced Upgrade** 는 같은 컴퓨터에서 R82 Management Server Migration Tool로 데이터베이스를 export한 뒤, Gaia면 업그레이드·다른 OS면 clean install하고 다시 import 하며, **Migration and Upgrade** 는 소스에서 데이터베이스를 export해 별도의 새 R82 컴퓨터에 import 합니다. CPUSE는 현재 Gaia에서 도는 경우에만 쓸 수 있 으므로, OS를 바꾸거나 하드웨어를 옮긴다면 Advanced Upgrade나 Migration을 택합니다.

> 참 고
>
> R80.20.M1·R80.20·R80.20.M2·R80.30 이상에서 R82으로 올릴 때는, 각 단계마다 업그레이드 보고서가 만들어집니다 — Gaia Portal에서 실시간으로 보거나 `$MDS_FWDIR/log/upgrade_report-<날짜시간>.html` 에서 확인합니다.

계약 확인 — Contract Verification

관리 서버를 R82으로 올리기 전에 소프트웨어 업그레이드·메이저 릴리스를 포함하는 유효한 Support Contract가 User Center 계정에 등록돼 있어야 합니다. 업그레이드 과정은 Contract File이 있는지 확인하는데, 대개는 관리 서버가 User Center와 자동으로 통신해 최신 파일을 내려받으므로 신경 쓸 일이 없 습니다. 없으면 User Center에서 수동으로 받아 import하면 됩니다(인터넷이 없는 서버는 다른 컴퓨터에서 받아 옮겨 "Import a local contracts file"). 계약이 서버를 덮지 않으면 자격 없음 메시지가 뜨지만, 유효한 Contract File이 없어도 업그레이드 자체가 막히지는 않 습니다(라이선스 위반이 될 수 있으니 나중에라도 받아 두세요).

Upgrade Tools — Pre-Upgrade Verifier와 migrate_server

업그레이드를 떠받치는 도구가 **Upgrade Tools** 입니다. 항상 sk135172의 최신 버전을 써야 하며, 인터넷에 연결돼 "Allow Download" 동의 플래그가 켜져 있으면 서버가 자동으로 최신 버전을 받아 깝니다(없으면 수동 설치).

이 도구는 현재 관리 데이터베이스를 문제없이 올릴 수 있는지 검사(**Pre-Upgrade Verifier**, PUV)하고, 업그레이드를 실패시킬 수 있는 문제 목록을 담은 보고서를 생성 합니다. 보고서는 세 갈래로 나뉩니다 — 업그레이드 **전에** 고칠 항목(잘못된 정책 이름 같은 에러), 업그레이드 **후에** 고칠 항목, 그리고 단순 정보 메시지 입니다. 핵심 파일은 데이터베이스와 구성을 export·import하는 `migrate_server` 와, Advanced Upgrade·Database Migration 설정을 담는 `migrate.conf` 입니다.

사전 준비를 마쳤으니, 이제 대상별 실제 업그레이드로 들어갑니다 — 먼저 관리 서버 업그레이드부터입니다.

11 관리 서버 업그레이드

관리 서버 업그레이드

이 장은 관리 서버 계열 — Security Management Server·Log Server·SmartEvent Server·CloudGuard Controller, Multi-Domain Server·Multi-Domain Log Server, 그리고 Endpoint Security Management Server·Endpoint Policy Server — 를 R80.20 이상에서 R82으로 올리는 흐름을 한자리에 모았습니다. 종류마다 절은 나뉘지만 택할 방식(CPUSE·Advanced Upgrade·Migration)과 큰 흐름은 모두 같습니다. 시작하기 전에 업그레이드 옵션과 사전 준비를 반드시 먼저 읽으세요. 세부 절차는 원문 해당 절(추가 정보 sk163814)을 참고하세요.

어느 방식을 고를까 — CPUSE·Advanced·Migration

세 방식의 차이는 앞 장에서 본 그대로입니다. **CPUSE** 는 같은 컴퓨터에서 그대로 올리는 가장 단순한 방식 으로 현재 Gaia에서 도는 서버에 씁니다. **Advanced Upgrade** 는 같은 컴퓨터에서 데이터베이스를 export한 뒤 다시 import 하고, **Migration and Upgrade** 는 소스에서 export해 별도의 새 R82 컴퓨터에 import 합니다. 하드웨어를 바꾸거나 OS를 옮긴다면 Advanced나 Migration이 답입니다. 이 안내는 Security Management Server·CloudGuard Controller·전용 Log Server·전용 SmartEvent Server에 똑같이 적용됩니다.

공통 사전 점검

어느 방식이든 시작 전에 챙길 것이 있습니다. 현재 구성을 백업하고, 보류 중인 변경이 있으면 세션을 Publish 합니다(최신 published 데이터베이스 리비전만 업그레이드됨). 연결된 모든 SmartConsole을 닫 고, sk92449에서 최신 CPUSE를 깔며(Upgrade Tools 패키지를 지원하기 위함), 모든 소스 서버에서 **Pre-Upgrade Verifier** 를 돌려 문제를 고친 뒤 시작합니다. Management High Availability라면 Primary가 먼저 올라가 돌고 있어야 다른 서버를 올릴 수 있습니다.

그다음 Upgrade Tools를 준비합니다 — 인터넷에 연결돼 있으면 자동으로 최신 버전이 깔리고, 아니면 sk135172에서 R82 Upgrade Tools(CPUSE Offline 패키지)를 받아 깐 뒤 `cpprod_util CPPROD_GetValue CPupgrade-tools-R82 BuildNumber 1` 로 빌드 번호가 맞는지 확인합니다. `migrate_server` 는 항상 Check Point Cloud에 연결을 시도해 최신 도구를 보장 하므로, 인터넷이 없으면 수동 설치가 필요합니다.

> 참 고
>
> 같은 Security Management 환경의 서버 중 단 하나라도 IP가 바뀌면, 모든 서버(Log Server·SmartEvent Server 포함)에 같은 JSON 구성 파일을 적용해야 합니다. IP가 그대로면 이 단계는 건너뜁니다.

Multi-Domain Server와 Multi-Domain Log Server

Multi-Domain Server(MDS) 도 같은 세 방식(CPUSE·Advanced·Migration)을 따르되, 규모가 크고 도메인이 여럿이라 단계가 더 촘촘 합니다. 핵심 순서는 Primary에서 Global Domain이 Active인지 확인하고 Primary MDS를 먼저 올린 뒤, 통신·SIC를 확인(sk179794)하고 Secondary를 올리는 것입니다. 업그레이드 중 Domain Management Server를 어떻게 다룰지 도 별도로 다뤄집니다(원문 "Managing Domain Management Servers During the Upgrade Process").

Multi-Domain Log Server(MDLS) 는 반드시 Multi-Domain Server를 먼저 올린 뒤, 같은 버전으로 올립니다. MDLS 역시 CPUSE·Advanced·Migration 세 방식이 있습니다.

Endpoint 서버

Endpoint Security Management Server 와 **Endpoint Policy Server** 도 동일한 패턴 — CPUSE·Advanced Upgrade·Migration — 으로 R80.20 이상에서 R82으로 올립니다. Management High Availability 구성이라면 일반 관리 서버와 마찬가지로 Primary를 먼저 올리고 통신·SIC를 확인한 뒤 Secondary 를 올립니다.

업그레이드 보고서로 확인하기

세 방식 모두, R80.20.M1·R80.20·R80.20.M2·R80.30 이상에서 R82으로 올릴 때 각 단계마다 업그레이드 보고서가 생성 됩니다 — Gaia Portal에서 실시간으로 보거나 `$MDS_FWDIR/log/upgrade_report_<날짜시간>.html` 에서 확인합니다. 보고서의 "전에 고칠 항목"을 모두 해결한 뒤에야 안전하게 진행하세요. 업그레이드가 끝나면 기록해 둔 커스텀 설정을 새 파일에 직접 다시 적용 하는 것을 잊지 마세요(옛 파일을 복사하면 안 됨).

관리 서버를 모두 올렸다면, 이제 그것이 관리하는 장비를 올릴 차례입니다 — Security Gateway·클러스터 업그레이드로 넘어갑니다.

12 Security Gateway·클러스터 업그레이드

Security Gateway·클러스터 업그레이드

관리 서버를 올렸다면 이제 그것이 관리하는 장비 차례입니다. 이 장은 단일 Security Gateway·VSX Gateway, 그리고 ClusterXL·VSX·VRRP 클러스터와 Full High Availability 클러스터를 R82으로 올리는 흐름을 다룹니다. 단일 게이트웨이는 단순하지만, 클러스터는 "다운타임을 얼마나 허용하느냐"에 따라 방식이 갈리는 것이 핵심입니다. 세부 절차는 원문 해당 절을 참고하세요.

시작 전 — 관리 서버부터

다시 강조하지만 게이트웨이·Cluster Member를 올리기 전에 반드시 관리 서버와 Log Server를 먼저 올려야 합니다(앞 장). 그다음 백업을 받고, 필요하면 게이트웨이 라이선스를 올리고(라이선스 관리), VSX Cluster라면 관리 서버에서 VSX Cluster 객체 구성을 R82으로 먼저 올립 니다.

단일 Security Gateway·VSX Gateway 업그레이드

단일 장비는 CPUSE나 Central Deployment(권장)로 올립니다. Central Deployment는 SmartConsole에서 Check Point Cloud나 Package Repository의 패키지를 장비에 배포 하므로 여러 대를 한꺼번에 다루기 좋고, CPUSE는 각 Gaia에서 직접 올릴 때 씁니다. VSX Gateway도 CPUSE로 올릴 수 있되, 앞서 말한 대로 관리 서버 쪽 VSX 객체 구성을 먼저 R82으로 맞춰 두어야 합니다.

클러스터 업그레이드 계획

클러스터가 까다로운 이유는 분명합니다 — 업그레이드는 멤버의 모든 Check Point 서비스를 멈추므로, 그동안 클러스터가 연결을 검사·동기화하지 못 합니다. 게다가 서로 다른 버전의 멤버는 연결을 동기화하지 못 합니다. 그래서 다운타임 허용 범위에 맞춰 방식을 고릅니다.

시작 전 점검도 더 깐깐합니다. 전체 유지보수 창(maintenance window)을 잡아 업그레이드 후 커스텀 설정을 다시 적용할 시간을 확보 하고(기본 파일로 덮어써 커스텀이 사라지면 멤버가 서로를 못 보거나 트래픽이 끊길 수 있음), 모든 멤버에서 필수 커널 파라미터 값이 같은지 확인 합니다 — Cluster Member는 `cphaprob mmagic` 로 "MAC magic"·"MAC forward magic"을, VSX Cluster Member는 `fwha_add_vsid_to_ccp_mac` 값을 봅니다(sk25977).

세 가지 클러스터 업그레이드 방식

다운타임을 기준으로 세 갈래입니다. ClusterXL·VSX Cluster·VRRP(Gaia 위 3rd party) 클러스터 모두에 쓸 수 있습니다.

Multi-Version Cluster(MVC) Upgrade 는 연결 유지가 최우선일 때 고릅니다. 업그레이드 전에 시작된 연결을 새 버전 멤버와 동기화해 끊김을 보장하지 않습니다 — 즉 연결 페일오버가 보장 되고 다운타임 창도 필요 없으며 소요 시간도 짧습니다. 다만 특정 업그레이드 경로만 지원하고, 페일오버 뒤 살아남지 못하는 연결 유형이 많 다는 제약이 있습니다(원문의 지원 버전·제한 절 확인). Gateway 모드와 VSX 모드 절차가 각각 있습니다.

Minimum Effort Upgrade(Simple Upgrade)는 다운타임이 허용될 때 쓰는 가장 단순한 방식입니다. 각 Cluster Member를 독립된 Security Gateway처럼 따로 올리 므로 절차가 쉽지만, 업그레이드 전에 시작된 모든 연결이 끊기 고 멤버를 다 올릴 때까지 상당한 다운타임이 필요합니다.

Minimum Downtime Upgrade 는 다운타임을 거의 둘 수 없을 때 쓰는 절충안입니다. 업그레이드 내내 트래픽을 처리하는 Active 멤버가 항상 하나 이상 있어 네트워크 연결은 유지 되지만, 옛 버전 멤버를 거쳐 시작된 연결은 그 멤버를 올릴 때 끊깁 니다(버전이 다른 멤버끼리 동기화가 안 되기 때문). 새로 올린 멤버를 거친 연결은 끊기지 않습니다. 짧은 다운타임 창만 있으면 되지만, Dynamic Routing 연결은 지원하지 않 습니다.

> 참 고
>
> MVC를 끈 상태에서 서로 다른 버전의 멤버가 같은 네트워크에 있으면, 새 버전 멤버는 **Ready** 상태로 머뭅니다. Ready 상태의 멤버는 트래픽을 처리하지도, 동기화하지도 않습니다. 이를 피하려면 업그레이드하는 멤버를 콘솔로 접속해 네트워크에서 물리적으로 분리한 뒤 올립니다.

Full High Availability 클러스터 업그레이드

Full High Availability 클러스터는 관리 서버와 게이트웨이가 같은 두 appliance에 얹혀 있어 업그레이드 순서가 특별합니다. 관리 서버 업그레이드와 클러스터 업그레이드의 성격을 모두 갖 기 때문에, 원문 "Upgrading a Full High Availability Cluster" 절의 순서를 그대로 따라야 합니다.

여기까지가 표준 설치·업그레이드입니다. 이제 평범하지 않은 상황들을 다룹니다 — 먼저 관리 서버 특수 시나리오로 넘어갑니다.

13 관리 서버 특수 시나리오

관리 서버 특수 시나리오

표준 설치·업그레이드를 벗어난, 데이터를 옮기고 도메인을 다루는 상황들이 있습니다. 이 장은 Domain 백업·복원, Domain Management Server를 옮기기, 관리 서버 사이의 데이터베이스 이전, Multi-Domain Server와 Domain의 IP 변경 같은 관리 서버 특수 시나리오를 개념 위주로 정리합니다. 이들 대부분은 Management API나 Upgrade Tools의 `migrate_server` 로 수행합니다. 세부 절차는 원문 해당 절과 Check Point Management API Reference를 참고하세요.

Domain 백업과 복원

Multi-Domain 환경에서는 도메인 단위로 백업·복원할 수 있습니다. `backup-domain` API로 한 Domain을 백업하고, 나중에 같은 Multi-Domain Server에서만 복원 할 수 있습니다(Global Policy가 할당된 Domain은 백업 때 Global Domain Revision을 purge하지 않은 경우에만 복원 가능).

복원은 순서가 정해져 있습니다. 먼저 `restore-domain` 을 `verify-only` 플래그로 돌려 복원이 가능한지 확인 하고, 현재 Domain을 삭제(SmartConsole 또는 `delete domain` API)한 뒤, `restore-domain` 으로 Active Domain Management Server를 복원 합니다. 그다음 Standby Domain Management Server와 Domain Log Server를 복원하는데, 이들은 반드시 백업 당시와 같은 IP 를 가져야 하며 `set-domain` API로 백업 파일 경로를 지정해 다시 붙입니다.

Domain·데이터베이스 옮기기

여러 이전 시나리오가 `migrate_server` 또는 API로 지원됩니다. **Domain Management Server를 R82 Multi-Domain Server 사이에서 옮기** 거나, **R82 Security Management Server 사이에서 데이터베이스를 옮기** 거나, **Security Management Server의 데이터베이스를 Multi-Domain Server의 한 Domain으로**(또는 그 반대로) 옮길 수 있습니다. 이들 작업에는 항상 sk135172의 최신 Upgrade Tools 를 써야 합니다. 단일 관리에서 Multi-Domain으로 옮겨 가거나, 반대로 한 도메인을 떼어 독립 관리 서버로 만들 때 쓰는 길입니다.

Multi-Domain Server·Domain의 IP 변경

운영 중 IP를 바꿔야 할 때도 있습니다. **Multi-Domain Server나 Multi-Domain Log Server의 IP 변경**, **Domain Management Server나 Domain Log Server의 IP 변경** 이 각각 별도 절차로 다뤄집니다. IP는 관리 환경 전체의 통신·SIC와 얽혀 있으므로, 한 서버의 IP를 바꾸면 연관된 서버들에도 영향이 미친다는 점을 염두에 두고 원문 절차를 그대로 따라야 합니다.

> 참 고
>
> Multi-Domain 환경에서 IPS는 별도의 고려가 필요합니다(원문 "IPS in Multi-Domain Server Environment" 절). Global Domain과 각 Domain의 IPS 구성이 어떻게 맞물리는지를 확인하세요.

이런 작업들은 대개 일회성·고위험이라, 반드시 백업을 먼저 받고 진행하세요. 다음은 게이트웨이 쪽의 특수 배포 — Monitor·Bridge Mode입니다.

14 Security Gateway 특수 시나리오 — Monitor·Bridge Mode

Security Gateway 특수 시나리오 — Monitor·Bridge Mode

게이트웨이를 평범하게 길목에 끼우는 것 말고도, 기존 환경을 건드리지 않고 트래픽을 관찰하거나, IP 구조를 바꾸지 않고 보안 장비를 끼워 넣는 특수 배포가 있습니다. 이 장은 **Monitor Mode**, **Bridge Mode**, 그리고 게이트웨이가 부팅·업그레이드 중에도 스스로를 지키는 **Security Before Firewall Activation** 을 다룹니다. 세부 절차는 원문 해당 절과 R82 Gaia 관리자 가이드를 참고하세요.

Monitor Mode — 환경을 건드리지 않고 관찰하기

Monitor Mode 는 운영 환경을 바꾸지 않고 네트워크 트래픽을 분석 하는 배포입니다. 게이트웨이 인터페이스 하나를 스위치의 **Mirror Port**(SPAN Port)에 연결해, 복제된 트래픽을 듣기만 합니다. 그 인터페이스에서는 어떤 보안 정책도 집행하지 않고(prevent/drop/reject 없음), 도착한 패킷을 전부 종료할 뿐 다시 내보내지 않 습니다. Software Blade의 성능을 평가하거나, 애플리케이션 사용을 상시 모니터링할 때 유용합니다.

장점은 분명합니다 — 운영 환경에 위험이 없고, 설정이 최소이며, 값비싼 TAP 장비가 필요 없 습니다.

!① mirror/SPAN 포트로 모든 입출력 패킷을 복제하는 스위치 ② 서버 ③ 클라이언트 ④ Monitor Mode 인터페이스를 가진 Security Gateway ⑤ 게이트웨이를 관리하는 Security Management Server — Monitor Mode 토폴로지 *① mirror/SPAN 포트가 있는 스위치 ② 서버 ③ 클라이언트 ④ Monitor Mode Security Gateway ⑤ Security Management Server*

> 중 요
>
> Check Point Cluster는 Monitor Mode를 지원하지 않습니다.

단일 Security Gateway나 단일 VSX Gateway에 구성할 수 있으며, 일부 Blade는 Monitor Mode 지원에 제약이 있습니다 — 예를 들어 IPS의 SYN Attack 보호(SYNDefender) 같은 능동적 기능은 동작하지 않 습니다. Threat Prevention·Application Control·URL Filtering·DLP 등은 Monitor Mode용으로 따로 구성하는 절(원문 참고)이 있고, 프록시 뒤에 둘 때의 구성도 별도로 다룹니다. 설정 후에는 Expert 모드에서 `grep -A 3 -r fw_span_port_mode $FWDIR/state/local/*` 로 정책에 `:val (true)` 가 들어갔는지 확인 하고, Monitor Mode 인터페이스를 스위치의 mirror/SPAN 포트에 연결하면 됩니다.

Bridge Mode — IP 구조를 그대로 둔 채 끼워 넣기

기존 네트워크를 IP가 다른 여러 네트워크로 나눌 수 없을 때 **Bridge Mode** 로 게이트웨이(또는 ClusterXL)를 설치 합니다. Bridge Mode의 게이트웨이는 Layer 3 트래픽에 보이지 않 습니다 — 한 bridge subordinate 인터페이스로 트래픽이 들어오면 게이트웨이가 그것을 검사한 뒤 두 번째 subordinate 인터페이스로 넘깁 니다. 즉 라우팅 구조를 다시 짜지 않고도 두 포트 사이에 보안 검사를 끼워 넣는 셈입니다(Gaia의 Bridge 인터페이스 개념과 같은 맥락).

Bridge Mode는 단일 Security Gateway뿐 아니라 ClusterXL에도 구성 할 수 있습니다 — 스위치 두 대를 쓰는 **Active/Standby**, 스위치 두세넷 대를 쓰는 **Active/Active** 토폴로지가 있습니다. Firewall·IPS·URL Filtering·DLP·Anti-Bot·Anti-Virus·Application Control 등 많은 Blade가 지원되되, HTTPS Inspection·Identity Awareness·일부 Anti-Virus 기능은 조건부 입니다(원문 표의 각주 참고). 그밖에 특정 프로토콜의 Ethernet 프레임을 허용·차단하기, Bridge 인터페이스를 통한 라우팅·관리, IPv6 Neighbor Discovery, **Link State Propagation(LSP)** 같은 세부 동작을 함께 구성합니다. LSP는 한쪽 링크가 끊기면 반대쪽도 내려 페일오버가 제때 일어나게 하는 기능으로, Bridge 환경에서 중요합니다.

Security Before Firewall Activation — 부팅·전환 중의 보호

게이트웨이가 정책을 아직 못 받은 순간에도 무방비여선 안 됩니다. **Boot Security** 는 부팅 중 게이트웨이와 그 네트워크를 보호 합니다 — Linux 커널의 IP Forwarding을 끄고 **Default Filter Policy** 를 적재 해, 정책이 처음 설치되기 전이나 정책 적재에 실패했을 때를 메웁니다 (Default Filter 템플릿이 세 가지 있음).

그다음 단계가 **The Initial Policy** 입니다. 관리자가 처음으로 정책을 설치하기 전까지는 Initial Policy가 보안을 집행 하는데, Default Filter에 미리 정의된 implied rule을 더해 대부분의 통신을 막되 정책 설치에 필요한 통신만 허용 합니다. 특히 Check Point 제품 업그레이드, 게이트웨이의 SIC 인증서 리셋, 라이선스 만료 시에도 Initial Policy가 게이트웨이를 보호 합니다 — 이때는 Initial Policy가 사용자 정의 정책을 덮어씁니다. 그래서 업그레이드나 SIC 재설정 중에도 게이트웨이가 완전히 열려 버리는 일이 없습니다. 만약 재부팅이 완료되지 않으면 원문 "Troubleshooting: Cannot Complete Reboot" 절을 참고하세요.

다음은 마지막 — 환경 전반을 떠받치는 라이선스 관리와 클라우드 서비스입니다.

15 라이선스 관리와 클라우드 서비스

라이선스 관리와 클라우드 서비스

Check Point의 기능은 라이선스가 떠받칩니다 — 설치·업그레이드 곳곳에서 "유효한 라이선스를 넣으라"는 말이 나왔던 이유입니다. 이 장은 라이선스를 어디서 보고·더하고·지우는지, IP가 바뀌면 어떻게 옮기는지, 옛 도구 **SmartUpdate** 는 언제 쓰는지, 그리고 Check Point 클라우드 서비스가 무엇을 자동으로 주고받는지 를 정리합니다. 세부 절차는 원문 해당 절과 R82 CLI Reference Guide를 참고하세요.

라이선스를 다루는 네 갈래

라이선스는 여러 곳에서 관리할 수 있습니다. **SmartConsole** 에서 활성화·추가·삭제 하고, **Gaia Portal**(Maintenance > Licenses)에서 추가·삭제 하며, **Gaia Clish·Expert 모드** 에서는 `cplic` 명령 으로 더하고 지웁니다. 게이트웨이가 인터넷에 연결돼 있으면 SmartUpdate 없이도 스스로 라이선스·계약을 받아 갱신 하지만, 연결이 없는 게이트웨이라면 SmartUpdate로 추가·삭제·attach·detach 합니다.

> 참 고
>
> R81부터는 SmartConsole에서 라이선스를 수동으로 더하고 지울 수 있습니다 — Gateways & Servers에서 객체를 고르고 아래 **Licenses** 탭에서 License File이나 License String으로 추가합니다(이 작업에는 관리자 프로필에 "Run One-Time Scripts" 권한이 필요).

라이선스 상태 읽기

SmartConsole의 Gateways & Servers에서 Licenses 열을 켜면 객체별 라이선스 상태 를 한눈에 봅니다. 전반 상태는 **OK**(모든 Blade 라이선스 유효), **Not Activated**(SIC 수립 후 첫 15일 동안만 가능하며 이후엔 오류), **Error with N blade(s)**(미설치·무효), **Warning with N blade(s)**, **N/A** 로 나뉩니다. 각 Software Blade 단위로는 **Active**(활성·유효), **Available**(비활성·유효), **No License**(활성인데 무효), **Expired**(만료), **About to Expire**(30일 이내, 평가판은 7일 이내 만료 예정), **Quota Exceeded/Warning**(쿼터 초과·90% 도달) 같은 상태를 보여 줍니다.

이 정보는 License Status·License Inventory 보고서로 보고 Excel·PDF로 내보낼 수 있습니다 — Gateways & Servers의 Actions > License Report, 또는 Logs & Events 뷰의 Views·Reports에서 띄우고 필터를 걸어 객체·계약 만료일을 추적합니다. VSX는 Virtual System·Virtual Router 객체가 아니라 VSX Gateway·VSX Cluster 객체를 골라야 라이선스를 제대로 봅니다.

IP가 바뀌면 — 라이선스 옮기기

Check Point 라이선스는 서버의 주 IP 주소에 대해 발급 됩니다. 그래서 서버 IP를 바꿨거나 IP가 다른 서버로 데이터베이스를 옮겼다면 라이선스를 다시 맞춰야 합니다(관리 서버 IP 변경과 함께 일어나는 일).

흐름은 어느 서버든 비슷합니다 — User Center에서 새 IP로 새 라이선스를 발급해 설치하고, 옛 IP의 라이선스를 제거 합니다. Security Management Server·전용 Log/SmartEvent Server라면 `cpstop` 후 `cpstart` 로 서비스를 재시작 하고, SmartConsole에서 객체의 Network Management에서 IP·토폴로지를 갱신한 뒤 Install database 합니다(전용 Log/SmartEvent Server는 그 로그를 보내는 게이트웨이들에 Access Control 정책도 다시 설치). Multi-Domain Server·MDLS는 Leading Interface 변경 절차를 함께 따릅니다. 마지막으로 DNS 서버에서 호스트 이름을 새 IP에 매핑 하는 것을 잊지 마세요.

옛 도구 SmartUpdate

SmartUpdate 는 라이선스와 계약을 관리하던 옛 GUI 클라이언트 입니다. 게이트웨이가 인터넷에 연결돼 있으면 굳이 쓸 필요가 없지만, 연결이 없는 환경에서는 여전히 유용 합니다. SmartUpdate에서는 **Licenses & Contracts Repository** 에 새 라이선스를 더하고·지우고, 게이트웨이에 attach·detach하고, 게이트웨이에서 라이선스를 가져오고(Get), 파일로 내보내고, 만료 라이선스를 점검 할 수 있습니다. Quantum Spark appliance처럼 SmartConsole에서 라이선스가 안 보이는 경우의 우회 수단 으로도 SmartUpdate를 씁니다. 세부 작업은 원문 "Using Legacy SmartUpdate" 절을 참고하세요.

Check Point 클라우드 서비스 — 자동 다운로드·데이터 전송

Check Point 제품은 클라우드 서비스와 정보를 주고받습니다. **Automatic Downloads** 는 첫 구성 마법사의 Products 페이지에서 켜고 끄며, 켜 두기를 권장합니다 — 그래야 **Blade Contracts**(Software Blade의 연간 라이선스), **CPUSE** 업그레이드, 그리고 Application Control·URL Filtering·Threat Prevention(Anti-Bot·Anti-Virus·Anti-Spam·IPS·Threat Emulation)·HTTPS Inspection·Compliance 등이 필요로 하는 데이터 업데이트 를 받을 수 있기 때문입니다(유효한 Blade contract가 없으면 해당 Blade는 제한적으로만 동작). 이 기능은 관리 서버·Multi-Domain Server·Log Server·게이트웨이에 적용되며, 마법사에서 꺼 뒀다면 SmartConsole의 Menu > Global properties > Security Management Access에서 "Automatically download Contracts and other important data" 로 다시 켤 수 있습니다(sk94508).

반대 방향인 **Sending Data to Check Point** 는 첫 구성 마법사 Summary 페이지에서 정하며 기본으로 켜져 있습니다(CPUSE 통계에 필요). 이 설정은 Check Point User Center Synchronization Tool을 켜, 게이트웨이의 정보로 User Center 계정을 갱신하고 SKU를 실제 배포에 매핑 합니다. 관리 서버의 이 설정은 그것이 관리하는 모든 게이트웨이(R77 이상)에 적용되며, SmartConsole의 같은 Global properties에서 "Improve product experience by sending data to Check Point"로 끄고 켤 수 있습니다(sk94509).

여기까지가 Check Point R82의 설치·업그레이드 전 과정입니다. 처음으로 돌아가 용어 정리나 시작하기를 다시 짚어 보며 전체 그림을 굳혀도 좋습니다.