01 Maestro 개요

Maestro Overview

Maestro를 한마디로 하면 여러 대의 Quantum Security Gateway를 하나의 시스템처럼 묶어 쓰는 기술 입니다. 클라우드에서 서버를 필요할 때 늘리듯, 기존 게이트웨이의 용량을 필요에 따라 키울 수 있게 해 줍니다.

> *Check Point Maestro introduces to the industry a new way to utilize current hardware investment and maximize appliance capacity in an easy-to-manage HyperScale network security solution to bring our networks and data center to the world of hybrid clouds.*
>
> — Scalable Platforms AdminGuide, "Maestro Overview" (p.39)

핵심 동작은 이렇습니다. **Quantum Maestro Orchestrator** 가 내·외부 트래픽을 여러 Quantum Security Gateway에 고르게 분배하고, 그 게이트웨이들은 공통 정책과 기능을 가진 하나의 그룹으로 관리됩니다. 이 묶음을 떠받치는 것이 Check Point의 **HyperSync** 기술 기반 **N+1 클러스터링**입니다. 즉 겉으로는 한 대처럼 보이지만 안에서는 여러 대가 함께 일하며, 한 대가 빠져도 나머지가 이어받습니다.

Maestro가 주는 이점은 세 가지로 정리됩니다. 첫째 **HyperScale 보안** — 오케스트레이터·어플라이언스 모델에 따라 최대 52대의 게이트웨이로 1.5Tbps급 위협 방어 성능 까지 확장됩니다. 둘째 **유연한 운영** — 보안 수요가 늘면 새 게이트웨이를 필요할 때 즉시 투입(spin up)할 수 있습니다. 셋째 **클라우드 수준의 효율** — 완전한 Active/Active 이중화 라 놀고 있는 장비 없이 모든 하드웨어 자원을 다 씁니다.

정리하면 Maestro는 "장비를 더 사서 따로 관리"하는 대신, 기존 게이트웨이들을 오케스트레이터 아래 하나로 묶어 용량·이중화·관리를 한꺼번에 얻는 방식입니다. 이 게이트웨이 묶음을 실제로 다루는 단위가 Maestro Security Group이며, 그 구성 방법은 Security Group 구성 장에서 자세히 다룹니다.

> **참 고**
>
> 이 가이드는 Maestro에만 해당하는 절차를 다룹니다. 모든 Scalable Platform(Maestro·Scalable Chassis)에 공통인 절차는 원문의 "Common Procedures for Scalable Platforms" 장에 있습니다.

02 Maestro Security Group

Maestro Security Groups

Maestro에서 실제로 다루는 단위가 **Security Group** 입니다. 여러 Security Appliance를 묶어 하나의 Active/Active 클러스터로 동작시키는 논리 그룹 으로, 다른 Security Group과는 완전히 분리됩니다.

> *Each Security Group is a logical group of Security Appliances providing Active/Active cluster functionally segregated from other Security Groups.*
>
> — Scalable Platforms AdminGuide, "Maestro Security Groups" (p.40)

각 Security Group은 전용 내·외부 인터페이스를 갖고, 그룹마다 다른 설정과 정책 을 가질 수 있습니다. 예를 들어 데이터센터를 보호하는 Access Control용 Security Group 하나, 경계 방어를 맡는 Threat Prevention용 Security Group 하나를 따로 둘 수 있습니다. 또 컴퓨팅 자원(어플라이언스)을 그룹 안에서, 또는 그룹 사이에서 동적으로 더하거나 뺄 수 있어 수요에 맞춰 용량을 조절합니다.

구성 큰 그림

Security Group을 세우는 흐름은 이렇습니다. 먼저 **Quantum Maestro Orchestrator** 들을 네트워크에 연결하는데, 오케스트레이터끼리는 sync 포트로(같은 Site는 internal sync, Site 간은 external sync), 데이터망은 uplink 포트로 잇습니다. 그다음 Check Point Security Appliance들을 오케스트레이터의 **downlink 포트** 에 연결합니다. 케이블이 정리되면 오케스트레이터 한 대에서 원하는 Security Group을 구성합니다.

여기서 관리의 핵심 개념인 **SMO(Single Management Object)** 가 등장합니다. SmartConsole에서는 이 Security Group 전체를 대표하는 게이트웨이 객체 하나(SMO)만 만들어 정책을 설치 하면 됩니다. 즉 여러 어플라이언스를 일일이 관리하는 게 아니라, 하나의 객체로 그룹 전체를 다루는 것입니다. 정책을 설치하고 라우팅 같은 추가 설정을 한 뒤 어플라이언스를 더 넣으면, 새 어플라이언스가 SMO 멤버로부터 소프트웨어 패키지·설정·정책을 자동으로 복제 해 곧바로 그룹의 일원이 됩니다.

이처럼 "한 객체(SMO)로 묶음 전체를 관리하고, 멤버는 자동 복제로 합류"하는 구조가 Maestro 운영의 골격입니다. 실제 구성 절차는 Security Group 구성, 운영·관리는 Security Group 관리 장에서 다룹니다. 최초 물리 설치·배선은 별도의 Quantum Maestro Getting Started Guide를 따릅니다.

03 Maestro 소개

Introduction to Maestro

Quantum Maestro Orchestrator 는 여러 Check Point Security Appliance를 하나의 통합 시스템으로 오케스트레이션해 세계 최대 규모의 네트워크까지 보호 하는 확장형 보안 시스템입니다.

> *Quantum Maestro Orchestrator is a scalable Network Security System built to secure the largest networks in the world by orchestrating multiple Check Point Security Appliances into a unified system.*
>
> — Scalable Platforms AdminGuide, "Introduction to Maestro" (p.41)

오케스트레이터가 제공하는 것은 세 가지입니다. 첫째 사실상 무한한 확장의 보안 이고, 둘째 **이중화** 로 — 오케스트레이터가 Security Group에 배정된 어플라이언스들에 트래픽을 자동으로 분배합니다. 셋째 기존 Security Group에 어플라이언스를 더 연결해 그 자원을 손쉽게 추가 할 수 있다는 점입니다. 결국 개요에서 본 "여러 대를 하나처럼"이라는 성질을, 트래픽 분배·이중화·손쉬운 증설이라는 세 가지로 실현하는 것이 오케스트레이터입니다.

> 참 고
>
> Maestro가 지원하는 항목별 최대 수치는 R82 Release Notes의 "Maximum Supported Items"에서 확인합니다.

알아두면 좋은 링크

Maestro를 다룰 때 자주 참고하는 공식 자료는 다음과 같습니다. 제품·소프트웨어 정보는 R82 홈페이지(`sk181127`) 에 모여 있고, 운영 전에 반드시 봐야 할 R82 Known Limitations는 `sk181128` 입니다. Scalable Platform 버전 간 차이는 `sk173183` , Maestro 라이선스 기능은 `sk180461` 에 정리돼 있습니다.

04 Maestro 시작하기

Getting Started with Maestro

Maestro를 처음 구축할 때 무엇을 먼저 하고 무엇을 나중에 하는지 전체 흐름을 잡는 챕터입니다. 세부 절차는 각 장으로 연결됩니다.

가장 먼저 물리 설치 입니다. Quantum Maestro Orchestrator와 Security Appliance를 설치하고 케이블을 모두 연결하는데, 이 단계는 별도의 **Quantum Maestro Getting Started Guide** 를 따릅니다(sync·uplink·downlink 배선은 Security Group 장 참고).

물리 준비가 끝나면 Security Group의 핵심 개념부터 익힙니다 — 그룹 전체를 대표하는 **SMO(Single Management Object)** 와 정책 관리 방식입니다. 이 개념이 손에 잡혀야 이후가 수월합니다. 그다음 실제로 Security Group을 구성 하고, 운영에 들어가면 모니터링 과 최적화 로 상태를 살피고 성능을 다듬습니다.

운영 중에는 Hotfix 설치 와 트러블슈팅 도 알아둬야 합니다. Maestro에서 Hotfix를 설치·제거하는 방법은 Security Group 관리 장에, 문제 해결은 Maestro 트러블슈팅 장에 정리돼 있습니다.

정리하면 물리 설치 → SMO·정책 개념 → Security Group 구성 → 모니터링·최적화 → Hotfix·트러블슈팅 의 순서입니다. 각 단계의 상세는 해당 장에서 풀어 설명합니다. (모니터링·최적화·트러블슈팅은 Maestro 전용 절차 외에, 모든 Scalable Platform 공통 절차가 원문 별도 장에 더 있습니다.)

05 Maestro를 R82로 업그레이드

Upgrading Maestro to R82

Maestro 환경(Orchestrator + Security Group)을 무중단(Zero Downtime)으로 R82로 올리는 방법을 다루는 챕터입니다. 핵심은 **MVC(Multi-Version Cluster)** — 서로 다른 버전이 잠시 한 클러스터에 공존하며 순차로 올라가는 방식입니다. 지원 경로는 Security Group 기준 R81.10 → R82, R81.20 → R82 입니다.

가장 중요한 원칙은 **순서** 입니다. Orchestrator를 전부 먼저, 한 대씩 올린 뒤에 Security Group을 올립니다. 그리고 Orchestrator의 메이저 버전은 관리하는 Security Group의 메이저 버전보다 같거나 높아야 합니다(낮으면 안 됨). 모든 Site의 오케스트레이터에 대해 점검 창(maintenance window)을 잡는 것이 권장되며, 업그레이드는 오케스트레이터의 현재 설정을 그대로 유지합니다.

Dual Site는 페일오버로

Dual Site(또는 Dual Chassis) 환경에서는 한 Site씩 넘기며 올립니다. 먼저 **Standby Site(Site 2)** 의 오케스트레이터를 업그레이드하고, 각 Security Group에서 Active를 Site 1 → Site 2로 페일오버 시킨 뒤, 이제 Standby가 된 Site 1의 오케스트레이터를 업그레이드합니다.

```
# 각 Security Group의 Expert 모드에서 페일오버
chassis_admin -c <현재 Active Site ID> down
chassis_admin -c <기존 Active Site ID> up
```

Security Group은 멤버를 나눠 굴린다

Security Group을 올리기 전에 반드시 그 Security Group을 관리하는 **Management Server를 먼저 R82로** 업그레이드 해야 합니다(R82 Installation and Upgrade Guide 참고). 이 절차는 Gateway 모드와 Legacy VSX 모드 모두에 적용되며, Legacy VSX 모드에서는 모든 명령을 VS0 컨텍스트에서 실행합니다(gClish `set virtual-system 0`, Expert `vsenv 0`).

무중단의 핵심은 한 Security Group의 멤버를 동시에 다 올리지 않는 것 입니다. 멤버를 둘 이상의 논리 그룹(예: A·B)으로 최대한 같은 수로 나눠, 한 그룹을 올리는 동안 나머지 그룹이 트래픽을 계속 처리 하게 합니다. 한 그룹이 끝나면 다음 그룹을 올립니다.

업그레이드 진행 중에는 하면 안 되는 것들 이 있습니다. 절차가 명시적으로 시키지 않는 한 정책 설치·멤버 재부팅·Security Group(및 멤버) 설정 변경·Hotfix/Jumbo Hotfix 설치를 금지 합니다(Hotfix·Jumbo는 Check Point Support나 R&D가 지시할 때만).

롤백

업그레이드가 실패하면 되돌리는 절차가 따로 있습니다 — 오케스트레이터 롤백 과 Security Group(MVC) 롤백 은 원문의 "Rolling Back a Failed Upgrade…" 절을 따릅니다(Security Group 롤백은 Scalable Platform 공통 절차에 위치).

06 Orchestrator 간 인증

Authentication between Maestro Orchestrators

R82부터 Maestro Site 안의 모든 Orchestrator끼리 상호 인증 을 설정해, Sync 포트(같은 Site는 Internal Sync, Site 간은 External Sync)로 오가는 통신을 암호화할 수 있습니다.

> *Starting in R82, you can configure mutual authentication between all Maestro Orchestrators on your Maestro Sites to make sure their communication is secure and encrypted over Internal Sync ports and External Sync ports.*
>
> — Scalable Platforms AdminGuide, "Authentication between Maestro Orchestrators" (p.68)

이 인증은 SSH 키와 SSL 인증서 기반이며, SSL 인증서는 1년 유효하되 오케스트레이터가 자동 갱신합니다. 그리고 양방향 메시(two-way mesh) 라, 각 오케스트레이터가 나머지 모두를 서로 인증합니다(Dual Site 4대면 1_1·1_2·2_1·2_2가 서로서로).

시작 전 주의

순서와 단독 작업이 중요합니다. Security Group을 구성하기 전에 모든 오케스트레이터가 인증을 마쳤는지 먼저 확인 해야 동기화 문제가 안 생기고, 한 번에 한 관리자만 인증을 설정해야 서로 다른 오케스트레이터에서 동시에 건드리는 충돌을 막습니다. 또 오케스트레이터를 클린 설치·공장 초기화했거나, 교체했거나, Site ID/Orchestrator ID가 바뀌면 인증을 다시 설정해야 합니다.

상태는 Gaia Portal·CLI에서 네 가지로 표시됩니다 — **Authenticated**(상대를 인증함), **Unknown**(상태 판단 불가), **Unreachable**(Sync 포트로 연결 안 됨), **Untrusted**(상대를 신뢰 안 함). 아직 인증 안 된 오케스트레이터가 있으면 Gaia Portal 접속 시 "N개가 인증 대기 중, 지금 인증할까요?" 팝업이 뜹니다.

설정 방법 (Gaia Portal 권장)

먼저 한 가지 — Gaia에 Two-Factor Authentication을 켰다면, 신뢰를 맺기 전에 각 오케스트레이터에서 2FA를 끄고, 다 맺은 뒤 다시 켜야 합니다.

절차는 이렇습니다. 먼저 각 오케스트레이터의 **지문(fingerprint)** 을 확인합니다(Gaia Portal의 Orchestrator Management > Security Groups > Authentication에서, 또는 Gaia Clish의 `show ssh pubkey host localhost`). 그다음 오케스트레이터 한 대(예: 1_1)의 Gaia Portal에서 Orchestrator Management > Security Groups > 우측 상단 Authentication 으로 들어가, 나머지 오케스트레이터(1_2, 2_1, 2_2) 각각의 섹션에서 **Trust** 를 누릅니다. 이때 Expert 모드 비밀번호를 입력하는데, 이 비밀번호는 최초 인증에만 쓰이고 이후 저장되지 않습니다. 한 대에서 나머지를 모두 Trust하면 메시 인증이 완성됩니다.

```
show ssh pubkey host localhost   # Gaia Clish에서 지문 확인
orchd restart                    # 기존 환경에 새로 추가한 오케스트레이터라면 Expert 모드에서
```

기존 Maestro 환경에 새 오케스트레이터를 추가해 신뢰를 맺었다면, 그 새 오케스트레이터에서 `orchd restart` 를 실행합니다. (Gaia Clish/Expert 모드 CLI로도 같은 인증을 할 수 있습니다.)

07 Security Group 구성

Configuring Security Groups in Maestro

Maestro의 핵심 작업 — Security Group을 만들고 설정하는 전체 흐름 을 다루는 챕터입니다(분량이 가장 큰 장). 물리 설치·배선은 이미 끝났다고 전제합니다(Quantum Maestro Getting Started Guide). 전체는 5단계 로 흐릅니다.

큰 그림 — 5단계

1. **오케스트레이터에서 Security Group 구성** — 오케스트레이터는 한 대에서만 설정하면 나머지가 자동 동기화 됩니다. 각 Security Group에는 ① Security Appliance 한 대 이상(연결하면 Downlink 포트가 자동 배정), ② 관리 서버로 가는 **전용 Management 포트**(예: `eth1-Mgmt1`), ③ 외부·내부 트래픽망을 연결한 **Uplink 포트** 가 들어갑니다. 2. **Security Group의 Gaia OS 설정** 3. **SmartConsole에서 설정** (정책 객체) 4. **라이선스 설치** 5. **트래픽 확인** + **특수 시나리오 설정**

Step 1 — 오케스트레이터에서 그룹 만들기

Gaia Portal 또는 Gaia Clish로 진행하며, 순서는 이렇습니다. 새 Security Group 생성 → 네트워크 구성 추가 → First Time Wizard 설정(여기선 제한된 항목만 잡음) → 가용 Security Appliance 배정 → 오케스트레이터 포트(Uplink·Management) 배정.

어플라이언스 배정에 주의가 있습니다. 같은 Security Group에는 지원되는(서로 호환되는) 어플라이언스만 배정 할 수 있고(sk162373), 배정된 어플라이언스는 설정 적용 후 자동 재부팅 됩니다. Dual Site라면 각 Site에서 가능한 한 같은 수의 어플라이언스를 배정 해야 — 페일오버 시 새 Active Site가 전체 트래픽을 감당할 수 있습니다. 설정 후 오케스트레이터에 Gaia 백업을 떠 두는 것이 권장됩니다.

> 참 고
>
> 새 Security Group을 만들 때 오케스트레이터의 마법사에서는 Gaia GRUB 비밀번호를 설정할 수 없습니다. Security Group의 Gaia 최초 설정 마법사를 마친 뒤에 따로 설정합니다.

Step 2 — Security Group의 Gaia 설정

새로 만든 Security Group에서 Gaia OS 설정(네트워크·시스템 등)을 잡습니다. 여기서도 Gaia 백업을 떠 두면 좋습니다.

Step 3 — SmartConsole에서 정책

여기서 SMO 개념이 실제로 쓰입니다. 모드에 따라 만드는 객체가 다릅니다.

- **Gateway 모드** — Security Gateway 객체 하나 를 만들고, 보안 정책을 설정해 그 객체에 설치합니다. - **VSX 모드** — VSX Gateway 객체 하나 를 만들고 그 안에 Virtual System들을 만든 뒤, 각 VS에 정책을 설치합니다.

어느 쪽이든 Security Group 전체를 객체 하나(SMO)로 다룬다 는 원리는 같습니다.

Step 4 — 라이선스 설치

Security Group에 적용할 라이선스를 설치합니다.

Step 5 — 확인과 특수 시나리오

마지막으로 이 Security Group을 지나야 하는 연결을 실제로 일으켜 트래픽이 정상 통과하는지 확인 합니다. 필요하면 특수 구성을 더하는데, 고가용성(HA)·Security Group 관리·시스템 최적화 외에 Monitor 모드 배포 나 Bridge 모드 배포 같은 시나리오가 있습니다(이들 상세 절차는 분량이 커서 원문 해당 절을 참고).

정리하면 오케스트레이터에서 그룹·포트·어플라이언스를 잡고(Step 1~2) → SmartConsole에서 SMO 객체로 정책을 입히고(Step 3) → 라이선스를 넣고(Step 4) → 트래픽을 확인(Step 5) 하는 흐름입니다. 이 한 줄기만 잡으면 세부 화면 절차는 그 위에 얹히는 디테일입니다.

08 Security Group 관리

Managing Security Groups in Maestro

Security Group을 운영하면서 다루는 기본 작업들 — 특정 멤버에 접속하기, Site별 고유 IP, 오케스트레이터 포트 관리, Hotfix 설치 — 을 모은 챕터입니다.

특정 멤버에 접속하기

Security Group은 하나의 객체(SMO)로 관리하지만, 개별 Security Group Member의 CLI에 직접 들어가야 할 때가 있습니다. 오케스트레이터에서 들어가려면 먼저 `show maestro security-group id <SG ID>` 로 그룹과 멤버를 확인한 뒤, Expert 모드에서 `member <SG ID> <Member ID>` (줄여서 `m`) 로 접속합니다. 한 멤버에서 같은 그룹의 다른 멤버로도 같은 `member` / `m` 명령으로 이동할 수 있고, 외부에서는 Security Group IP로 SSH하면 그 Security Group에 배정된 오케스트레이터 관리 인터페이스를 거쳐 들어갑니다.

```
show maestro security-group id <SG ID>   # 그룹·멤버 확인 (오케스트레이터)
member <SG ID> <Member ID>               # 해당 멤버 CLI로 (예: member 1 3)
```

Dual Site의 Site별 고유 IP (UIPS)

Dual Site에서는 Active Site에 부하가 몰리면 SMO 연결이 어려워지거나, Standby Site의 특정 멤버(예: DOWN 상태)를 직접 들여다봐야 하는 상황이 생깁니다. **UIPS(Unique IP per Site)** 는 Site마다 고유 IP를 줘서 원하는 Site에 직접 접속 할 수 있게 해, 이런 트러블슈팅·관리를 수월하게 합니다.

오케스트레이터 포트 관리

오케스트레이터의 포트(uplink·downlink 등)는 Gaia Portal에서 관리하고, Gaia Clish·Expert 모드에서 상태를 관리·모니터링할 수 있습니다. 어떤 포트가 어디에 쓰이는지 확인하고 활성/비활성을 조정하는 일이 여기에 해당합니다.

Hotfix 설치·제거

Hotfix는 오케스트레이터와 Security Group Member 양쪽에 각각 설치·제거합니다. 둘은 절차가 다르므로(오케스트레이터용 / 멤버용) 대상에 맞는 절차를 따릅니다. 멤버에 설치할 때는 업그레이드에서 본 것처럼 무중단을 위해 한 번에 전체 멤버를 건드리지 않는 원칙이 그대로 적용됩니다. (Maestro 전용 절차 외에, 모든 Scalable Platform 공통 Hotfix 절차가 원문 별도 장에 더 있습니다.)

09 Maestro 시스템 모니터링

System Monitoring in Maestro

Maestro 환경을 감시하는 핵심 수단은 **SNMP** 입니다. 대상에 따라 두 갈래인데, Maestro Orchestrator 자체 와 Security Group 을 각각 모니터링합니다(Security Group 쪽은 모든 Scalable Platform 공통 절차로, 원문의 "Working with SNMP"를 참고).

Orchestrator를 SNMP로 보기

오케스트레이터에서는 SNMP로 소프트웨어 버전 과 주요 성능 지표(KPI) 를 볼 수 있습니다. 다만 분명한 한계가 있는데, 오케스트레이터의 하드웨어 모니터링은 SNMP로 지원되지 않습니다.

설정 흐름은 단순합니다. 먼저 오케스트레이터의 Gaia Portal 또는 Gaia gClish에서 **SNMP 에이전트를 켜고** 설정을 잡습니다 — 보안상 SNMP v3만 쓰는 것이 권장 됩니다(자세한 설정은 R82 Gaia Administration Guide의 SNMP 절). 그다음 Security Group에서 Check Point MIB 파일을 받아 서드파티 SNMP 모니터링 소프트웨어에 올립니다.

```
$CPDIR/lib/snmp/chkpnt.mib          # SNMP MIB
$CPDIR/lib/snmp/chkpnt-trap.mib     # SNMP Trap MIB
# 주의: /etc/snmp/GaiaTrapsMIB.mib 는 지원되지 않음
```

오케스트레이터에서 지원되는 OID 가지(branch)는 제한적 입니다. 조회용으로는 `svn` (`.1.3.6.1.4.1.2620.1.6`)과 `mngmt` (`.1.3.6.1.4.1.2620.1.7`) 두 가지만 지원됩니다. 트랩(trap)으로는 `chkpntTrapInfo` · `chkpntTrapNet` · `chkpntTrapDisk` · `chkpntTrapCPU` · `chkpntTrapMemory` (`.1.3.6.1.4.1.2620.1.2000.0~4`) 가 지원됩니다.

마지막으로 두 가지를 기억하면 됩니다 — `/etc/snmp/GaiaTrapsMIB.mib` 파일과 `set snmp traps` 명령은 오케스트레이터에서 지원되지 않습니다. Security Group이나 그 멤버의 SNMP 모니터링은 별도 절차(공통 Scalable Platform 절)를 따릅니다.

10 Maestro 시스템 최적화

System Optimization in Maestro

Maestro Security Group의 성능과 운영을 끌어올리는 기능들을 다루는 챕터입니다. 두 가지 대표 기능 — **Auto-Scaling** 과 **Fastforward** — 이 핵심이고, 그 밖에 로깅 포트·고가용성·신원 기반 제어가 있습니다.

Auto-Scaling — 용량 자동 확장

Maestro Auto-Scaling 은 특정 조건이 충족되면 가용 Security Appliance(Scale Unit)를 Security Group에 자동으로 투입하는 기능입니다. 그 조건은 오케스트레이터에서 Security Group별로 설정합니다. 부하가 오르면 사람이 손대지 않아도 장비가 그룹에 합류해 용량이 늘어나는, Maestro의 "클라우드 같은 탄력"을 실현하는 기능입니다.

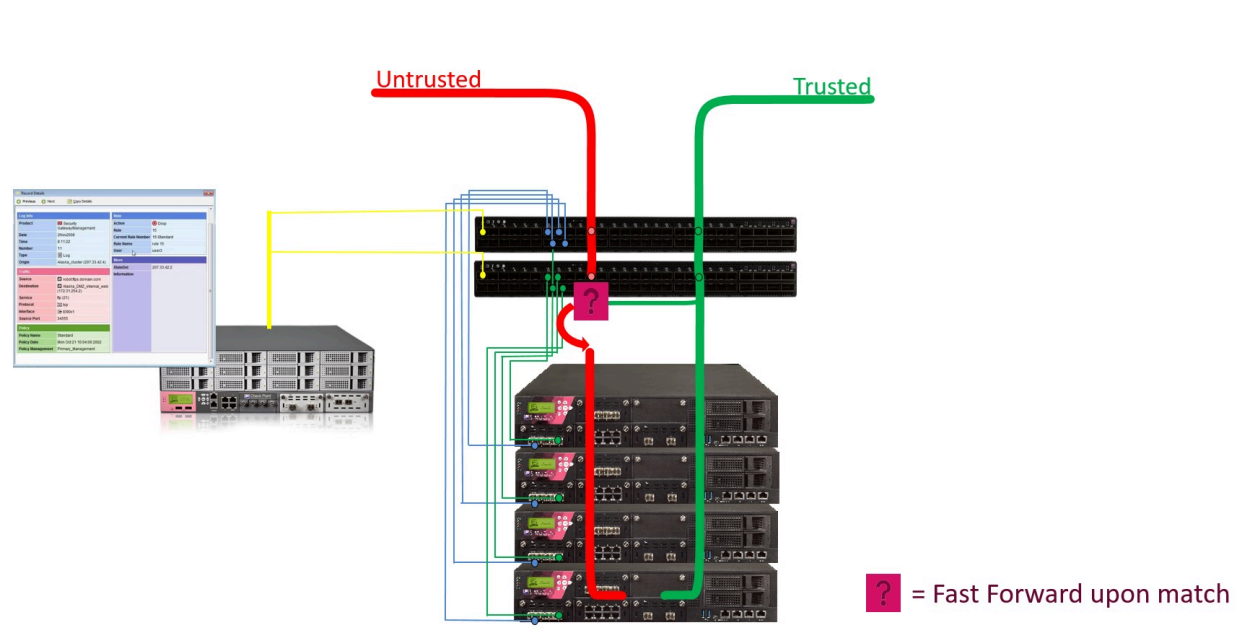
쓰기 전 전제가 있습니다. 그룹의 어플라이언스가 모두 같은 모델 이어야 하고, **SMO Image Cloning** 을 켜야 하며(`set cluster configuration image auto-clone state on`), Scale Unit이 User Center에서 라이선스를 받아오도록 인터넷 연결이 있어야 합니다. 한계로는 서로 다른 모델이 섞이면 Auto-Scaling 설정 불가, 그리고 CPU 사용률이 높으면 오케스트레이터가 멤버를 "Expired"로 볼 수 있다는 점입니다.

```
set cluster configuration image auto-clone state on   # SMO Image Cloning (Auto-Scaling 전제)
show cluster configuration image auto-clone state
```

> 주 의
>
> 일부 소프트웨어 설치 절차는 SMO Image Cloning을 꺼야 합니다. 설치를 마치면 다시 켜야 Auto-Scaling이 동작합니다.

Fastforward — 신뢰 트래픽 하드웨어 가속

Maestro Fastforward 는 신뢰된 연결의 일부 정책 규칙(accept/drop)을 오케스트레이터로 내려보내 하드웨어로 가속 하는 기능입니다. 핵심 이점은 마이크로초 미만의 초저지연 과 포트 라인레이트 처리량(한 연결로 최대 200Gbps) 입니다. 음성·트레이딩·내부 신뢰 서버 간 통신·백업처럼 신뢰할 수 있는 대용량 흐름 에 켜면 좋고, 트러블슈팅 시 특정 흐름을 우회시키는 용도로도 씁니다.



Maestro Fastforward 개요

원문은 Fastforward의 동작 원리, 토폴로지, 라우팅·정책 처리 방식, 알려진 한계, 트러블슈팅까지 길게 다룹니다. 요지는 신뢰 흐름을 방화벽 소프트웨어 경로 대신 오케스트레이터 하드웨어로 흘려 지연을 없애고 회선 속도를 뽑는다 는 것입니다.

그 밖의 최적화

- **전용 로깅 포트** — Maestro에서 로그 전송 전용 포트를 지정해 로깅 트래픽을 분리할 수 있습니다. - **Security Group 고가용성** — 가중치(HA Factor) 로 어느 Security Group/멤버가 우선 Active가 될지 정하고, **Quality Grade Differential** 로 페일오버를 일으킬 품질 차이 기준을 조정합니다. - **신원 기반 제어** — Maestro에서 Identity Awareness 기반 Access Control·Threat Prevention 을 설정해, 사용자·신원 단위로 정책을 적용할 수 있습니다.

11 Maestro 트러블슈팅

Troubleshooting in Maestro

Maestro 문제를 다룰 때 쓰는 명령과 절차를 모은 챕터입니다. 먼저 알아둘 제약 하나 — 오케스트레이터는 Gaia 부트 메뉴의 Hardware Diagnostic 도구를 지원하지 않습니다(Known Limitation MBS-17809).

오케스트레이터에 Gaia 새로 설치하기

오케스트레이터를 깨끗이 다시 깔아야 할 때는 두 가지 길이 있습니다 — 공장 초기화(factory defaults) 또는 부팅 USB로 클린 설치 입니다.

공장 초기화 는 마지막으로 클린 설치된 Gaia로 되돌리며, 기존 설정을 모두 지웁니다. 시리얼 콘솔로 접속해 Gaia Clish에서 `reboot` 한 뒤, 부팅 중 5초 안에 아무 키나 눌러 Boot 메뉴로 들어가 "Reset to factory defaults"를 고르고 `yes` 를 입력합니다. 재부팅 후 MGMT 포트 IP로 Gaia Portal에 접속해 최초 설정 마법사를 돌립니다.

```
reboot          # Gaia Clish에서
# 부팅 중 아무 키 → Boot 메뉴 → Reset to factory defaults → yes
```

USB 클린 설치 는 더 근본적인 재설치입니다. 먼저 Check Point Support에 연락해 오케스트레이터가 USB로 부팅하도록 설정하고, `sk181127` 에서 Maestro용 클린 설치 ISO를 받아 `sk65205` 대로 부팅 USB를 만듭니다(항상 최신 ISOmorphic Tool 빌드를 쓰고, "Open Server with console" 옵션을 선택). USB를 꽂고 콘솔로 접속해 재부팅하면 USB로 부팅되며, "Open Server with console"로 Gaia를 설치합니다. 재부팅 전에 USB를 뽑고, 부팅 후 Gaia Portal에서 최초 설정 마법사를 돌립니다.

로그·설정 파일 보기

문제를 파고들 때 들여다볼 로그가 Security Group 멤버 쪽과 오케스트레이터 쪽으로 나뉩니다. 전부 외울 필요는 없고, 증상별로 골라 보면 됩니다.

멤버 쪽에서 자주 보는 것은 클러스터 정보 `$FWDIR/log/cpha_policy.log.*` , 명령 감사 `/var/log/asgaudit.log*` , 핵심 데몬 로그(CPD `$CPDIR/log/cpd.elg` , FWD `$FWDIR/log/fwd.elg` , VPND `$FWDIR/log/vpnd.elg*` , VSX의 FWK `$FWDIR/log/fwk.elg.*`), 분배 모드 `/var/log/dist_mode.log*` , 새 멤버 추가 시 silent install `/var/log/silent_install.log.dbg` , 그리고 일반 로그 `/var/log/messages*` 입니다. 전용 로그가 없는 것들은 `/var/log/junk.log.dbg` 에 모입니다.

오케스트레이터 쪽에서는 Security Group 설정 적용 `/var/log/ssm_sg.log.dbg` , Security Group 정보 `/etc/sgdb.json` , 감지된 멤버 정보 `/etc/rsrcdb.json` , LLDP 업데이트 `/var/log/smartd.log.dbg` (또는 `lldpctl` 명령)를 봅니다.

오케스트레이터 교체

오케스트레이터 하드웨어를 교체해야 하면 `sk174202` 의 절차 를 따릅니다.