# 01 용어 정리

*용어 정리*

로깅과 모니터링을 다루기 전에, 이 가이드 전체에 거듭 나오는 핵심 용어부터 흐름에 따라 짚어 둡니다. 로그가 어디서 만들어져 어디에 쌓이고, 무엇이 그 로그를 이벤트로 바꾸고, 무엇으로 들여다보는가 라는 한 줄기를 잡으면 뒤 장들이 훨씬 수월합니다.

---

## 로그가 흐르는 경로 — Gateway·서버·로그

모든 것의 출발점은 로그입니다. **Audit Log** 는 관리자가 Management Server에서 한 행동(로그인·객체 수정·정책 설치 등)의 기록 이고, 보통 우리가 말하는 보안 로그는 Security Gateway가 트래픽을 검사하며 남기는 기록입니다.

이 로그를 받아 두는 서버가 **Log Server** 입니다. 공식 정의는 이렇습니다.

> *Dedicated Check Point server that runs Check Point software to store and process logs.*
> — AdminGuide, "Glossary" (p.305)

조직이 커지면 **Management Server**(=Security Management Server) 하나로는 부치니, 로그 전용 서버를 따로 두거나, Multi-Domain 환경에서는 도메인별 **Multi-Domain Log Server(MDLS)** 를 둡니다. **Management Server** 는 객체·정책을 관리하는 두뇌이고, **Log Server** 는 로그를 저장·처리하는 창고 라고 보면 됩니다.

## 로그를 다루고 보는 도구 — SmartConsole·SmartView

**SmartConsole** 은 정책 구성부터 이벤트 모니터링까지 다 하는 Check Point의 관리 GUI 입니다. 그 안의 **Logs & Events** 뷰에서 로그를 검색하고, View·Report를 엽니다(View와 Report). **SmartView** 는 클라이언트 설치 없이 브라우저로 같은 로그·이벤트 화면을 보는 웹 애플리케이션 입니다( `https://<서버 IP>/smartview/` ).

빠른 검색을 위해 Log Server는 로그에 **index** 를 만듭니다(SmartLog Indexing). indexing이 켜져 있으면 모든 Log Server의 로그를 한 화면에서 통합 검색 할 수 있고, 끄면 디스크는 아끼지만 서버마다 따로 뒤져야 합니다(시작하기).

## 로그를 이벤트로 — SmartEvent

로그가 수억 건이면 사람이 다 못 봅니다. 그래서 **SmartEvent** 가 로그를 우선순위가 매겨진 보안 이벤트로 압축 해 줍니다. 핵심은 **Event**(이벤트) 와 그것을 만드는 규칙입니다.

> *Record of a security or network incident that is based on one or more logs, and on a customizable set of rules that are defined in the Event Policy.*
>
> — AdminGuide, "Glossary" (p.305)

이 일을 실제로 하는 부품이 **SmartEvent Correlation Unit** 으로, 로그를 분석해 패턴을 찾아 이벤트로 만드는 엔진 입니다. 만들어진 이벤트는 **SmartEvent Server** 의 이벤트 데이터베이스에 쌓입니다. 그 패턴 규칙을 모은 것이 **Event Policy** 이고, 로그를 모아 분석하는 절차를 **Event Correlation** 이라 부릅니다 (SmartEvent로 이벤트 분석).

## 로그를 밖으로 내보내기 — Log Exporter

회사가 별도의 SIEM(Splunk·QRadar 등)을 쓰면 Check Point 로그를 그쪽으로 흘려보내야 합니다. 그 다리가 **Log Exporter** 로, syslog 프로토콜로 로그를 표준 형식(CEF·LEEF·JSON 등)으로 바꿔 외부 서버에 보내는 기능 입니다(Log Exporter).

## 관련 기술 용어 한 묶음

자주 나오는 나머지 용어들입니다. **Software Blade** 는 특정 보안 기능 모듈 로, Logging & Status·SmartEvent Server·SmartEvent Correlation Unit 같은 블레이드를 서버 객체에서 켜고 끕니다. **SIC(Secure Internal Communication)** 는 Check Point 컴포넌트끼리 인증서로 서로를 신뢰하는 메커니즘 이라, Gateway가 Log Server·SmartEvent에 로그를 보내려면 SIC가 먼저 맺혀 있어야 합니다. **System Counter** 는 SmartView Monitor가 보여 주는 제품의 상태·활동·자원 사용량 데이터 이며(트래픽·연결 모니터링), **Cooperative Enforcement** 는 Harmony Endpoint Security 서버와 Security Gateway의 연동 을 가리킵니다. 나머지 블레이드(IPS·Anti-Bot·Threat Emulation 등)의 자세한 뜻은 Threat Prevention 가이드와 관리 가이드를 함께 보세요.

# 02 로깅·모니터링 소개

*로깅·모니터링 소개*

Check Point의 로깅·모니터링은 보안 데이터·이벤트 관리·리포팅·정책 적용을 하나의 SmartConsole 플랫폼으로 묶은 통합 체계입니다. 흩어진 로그를 모아 보기 좋게 시각화하고, 정책 규칙과 로그를 연결해 두어 규칙 하나를 고르면 그 규칙이 만든 로그를 곧바로 볼 수 있게 합니다. 이 장은 가이드 전체가 무엇을 다루는지 한눈에 잡아 주는 길잡이입니다.

---

## 무엇을 할 수 있나

가장 큰 강점은 **속도와 깊이** 입니다. 강력한 free-text 검색으로 수백만 건의 로그에서 몇 초 만에 원하는 결과를 끌어내 고, 거기서 공격 유형·타임라인·애플리케이션·출처 같은 상세 정보로 자유롭게 드릴다운 합니다. 이벤트의 심각도에 따라 무시할지, 조치를 미룰지, 차단할지, 아니면 그 이벤트에 연결된 정책 규칙을 곧바로 손볼지 실시간으로 결정 할 수 있습니다.

리포팅도 통합돼 있어, 경영진·감사자·이해관계자에게 필요한 내용만 추려 맞춤 Report 를 만들 수 있습니다. 그리고 이 모든 기능을 브라우저로 쓰고 싶다면, **SmartView** 가 Management Server나 SmartEvent Server에 접속해 원격으로 로그를 보고 데이터를 모니터링 하게 해 줍니다.

## 이 가이드의 흐름

뒤 장들은 로그가 흐르는 길을 따라갑니다. 먼저 시작하기에서 Log Server와 SmartEvent를 어떻게 배포하는지 본 뒤, View와 Report로 데이터를 시각화하고, 로그 다루기에서 검색·쿼리 언어를 익힙니다. 그다음 SmartEvent로 이벤트 분석에서 로그가 어떻게 이벤트로 바뀌는지, 트래픽·연결 모니터링에서 SmartView Monitor로 상태를 보는 법을 다룹니다. 끝으로 타사 로그 가져오기와 Log Exporter로 외부 시스템과 로그를 주고받는 길을 정리합니다. 요지는 통합된 도구로 사고 조사·정책 개선·리포팅을 빠르게 돌려, 사후 대응이 아니라 선제적 보안 관리를 한다 는 것입니다.

# 03 시작하기 — Log Server·SmartEvent 배포

*시작하기 — Log Server·SmartEvent 배포*

로깅을 시작하려면 로그를 어디에 쌓을지(Log Server)와, 그 로그를 누가 이벤트로 분석할지(SmartEvent)를 먼저 정해 야 합니다. 이 장은 클라이언트 도구의 종류, 로깅의 동작 원리, 그리고 Log Server·SmartEvent를 배포하고 권한을 나누고 과거 로그를 들여오는 과정을 개념 위주로 정리합니다. 화면 단위의 클릭 절차까지는 원문(p.15~53)을 함께 보세요.

---

## 클라이언트 도구 — 무엇으로 보나

로그와 이벤트를 보는 GUI는 크게 셋입니다. 일상적으로 쓰는 것은 **SmartConsole** > **Logs & Events** 로, 예전의 SmartView Tracker·SmartLog를 대체한 통합 로그 뷰 입니다. 설치 없이 브라우저로 같은 화면을 보고 싶으면 **SmartView Web Application**( `https://<서버 IP>/smartview/` )을 쓰고, 게이트웨이나 서버에서 로그 생성·수신·인덱싱·내보내기 속도를 실시간으로 보려면 CLI 도구 **CPView** 를 씁니다.

여전히 쓰이는 전용 GUI도 둘 있습니다. **SmartEvent** GUI는 Correlation Unit·Log Server·도메인·내부망 같은 초기 설정과 Event Policy, Automatic Reaction을 정의 할 때, **SmartView Monitor** 는 터널·사용자 모니터링, Suspicious Activity 규칙, 알림 임계값 을 다룰 때 씁니다. 둘 다 SmartConsole의 Logs & Events에서 새 탭(+)을 열어 **External Apps** 에서 접근합니다.

## 로깅의 동작 원리

Security Gateway는 네트워크 로그를, Management Server는 관리자 행동을 담은 **audit 로그** 를 만듭니다. 어떤 규칙이 로그를 남길지는 그 게이트웨이에 설치된 Security Policy가 정합니다. 이 로그는 세 곳 중 하나에 저장됩니다 — 기본값인 Management Server, 로그가 많은 조직에 권장되는 전용 Log Server, 그리고 게이트웨이 자체(local logging) 입니다.

Log Server는 단순 저장 이상의 일을 합니다. 로그 파일이 최대 크기에 다다르면 새 파일을 시작하고, 내보내기·들여오기용으로 파일을 보관하며, 무엇보다 빠른 검색을 위해 **index** 를 만듭니다. 이 indexing이 켜져 있어야 모든 Log Server의 로그를 SmartConsole에서 하나로 통합 검색할 수 있습니다(끄면 디스크는 아끼지만 서버마다 따로 뒤져야 합니다). 운영자는 **Backup Log Server** 도 지정해, Primary가 모두 끊기면 Backup으로 순서대로 로그를 보내 게 할 수 있습니다.

> 참 고
>
> R81.10부터 **Dynamic Log Distribution** 으로 게이트웨이가 여러 활성 Log Server에 로그를 나눠 보낼 수 있어, 한 서버에 부하가 몰리는 것을 줄입니다. Gateway 객체 > Logs > Log Distribution에서 켭니다.

#### 보관 기간과 디스크 관리

로그는 무한정 쌓을 수 없으니 디스크가 임계치 아래로 떨어지면 가장 오래된 로그부터 자동 삭제 됩니다. 운영자는 "여유 공간이 N MB 아래면 경고", "N MB 아래면 오래된 파일 삭제 시작" 같은 임계치와, **Daily Logs Retention**(indexed 로그를 며칠, 로그 파일을 며칠 더 보관할지)을 서버 객체 > Logs > Storage에서 설정합니다. index와 로그 파일을 합한 최대 보관 기간은 3664일 입니다. 한 가지 기억할 점은 **Management Server의 audit 로그는 디스크 비상 상황에서도 삭제되지 않는다** 는 것입니다.

# Log Server 배포

로깅은 Management Server에서 기본으로 켜져 있고(General Properties > Management 탭 > Logging & Status), 로그가 많으면 **전용 Log Server** 를 따로 설치해 SIC로 연결합니다. Log Server를 새로 추가하거나, 게이트웨이의 Log Server를 바꾸거나, 로그 관련 블레이드를 켜고 끄면 반드시 Install Database 를 실행 해 변경을 적용해야 합니다. 게이트웨이 쪽에서는 Gateway 객체 > Logs에서 Management Server로 보낼지, 전용 Log Server로 보낼지, 로컬에 저장할지 를 고른 뒤 정책을 설치합니다. Multi-Domain 환경에서는 도메인 전용 Log Server를 별도 네트워크에 두어 규제 요건을 맞추기도 합니다.

## SmartEvent 배포

**SmartEvent Server** 는 Management Server 구조에 통합돼 있어, Log Server와 통신하며 로그를 읽어 분석합니다. Management Server에서 SmartEvent를 함께 켜거나, 전용 서버로 따로 배포 할 수 있는데, Multi-Domain 환경에서는 반드시 전용 서버에 설치해야 합니다. 켜는 방법은 서버 객체의 Management 탭에서 Logging & Status, SmartEvent Server, SmartEvent Correlation Unit 세 블레이드를 선택 하고 게시·Install Database 하는 것입니다.

> 주 의
>
> SmartEvent 평가판 라이선스가 만료되면 새 라이선스를 넣어도 연결을 받지 않을 수 있습니다. 이때는 라이선스 추가 후 `cpstop;cpstart` 로 서버를 재시작하세요.

전용 SmartEvent Server를 Management Server에 붙이는 흐름은 Check Point Host 객체 생성 → 버전 R82 선택 → SIC 신뢰 → 세 블레이드 활성화 → (권장) Log Server가 아니면 Log Indexing 해제 입니다. 그다음 SmartEvent GUI에서 Correlation Unit 객체와 Internal Network를 정의하고 Event Policy를 설치합니다. 기본 LEA 포트는 18184 이며, 타사 Log Server와 비표준 포트로 주고받을 때만 SmartEvent Server와 Correlation Unit에 새 포트를 수동 지정합니다(Log Exporter를 쓰면 이 절차는 무관).

## 관리자 권한 프로파일

로깅·모니터링 권한은 잘게 나눌 수 있습니다. 관리자(또는 그룹)에게 **Permission Profile**(Manage & Settings > Permission Profiles)을 만들어 부여하는데, 크게 **Monitoring and Logging**(Monitoring·Management Logs·Track Logs·Application/URL Filtering Logs)와 **Events and Reports**(SmartEvent의 Events·Policy·Reports) 로 나뉩니다. 특히 **SmartEvent Reports-Only** 프로파일을 만들면, 그 관리자는 SmartConsole에 들어와도 Logs & Events에서 Report만 볼 수 있고 다른 보안 정보엔 접근하지 못합니다. 외부 컨설턴트나 감사자에게 보고서만 열어 줄 때 유용합니다.

## 과거 로그·오프라인 분석 들여오기

SmartEvent를 설치하기 전의 위협을 되짚어 보고 싶을 때, 예전 로그 파일을 들여와 다시 인덱싱·분석 할 수 있습니다. 기본적으로는 직전 1일치만 들여오지만, Log Server에서 `evstop` 후 `log_indexer -days_to_index <일수>` 로 인덱싱 범위를 늘린 다음 `evstart` 하면 더 오래된 로그도 가져옵니다. 더 나아가 **Offline Job** 을 만들면, 그 로그 파일을 Correlation Unit에 통과시켜 Event Policy에 따라 상관분석 까지 돌릴 수 있습니다(SmartEvent GUI > Policy > General Settings > Initial Settings > Offline Jobs). 성능에 영향을 주니 필요한 일수만 들여오는 것이 좋습니다.

# 04 View와 Report

*View와 Report*

로그를 숫자가 아니라 그림으로 보면 훨씬 빨리 이해됩니다. **View** 와 **Report** 는 로그·이벤트를 쿼리해 차트·표·지도로 그려 주는 시각화 도구 로, SmartConsole의 Logs & Events나 브라우저의 SmartView(`https://<서버 IP>/smartview/`)에서 만들고 편집합니다. 이 장은 둘의 차이, 카탈로그 구성, 그리고 내보내기·공유·스케줄·커스터마이즈를 정리합니다.

---

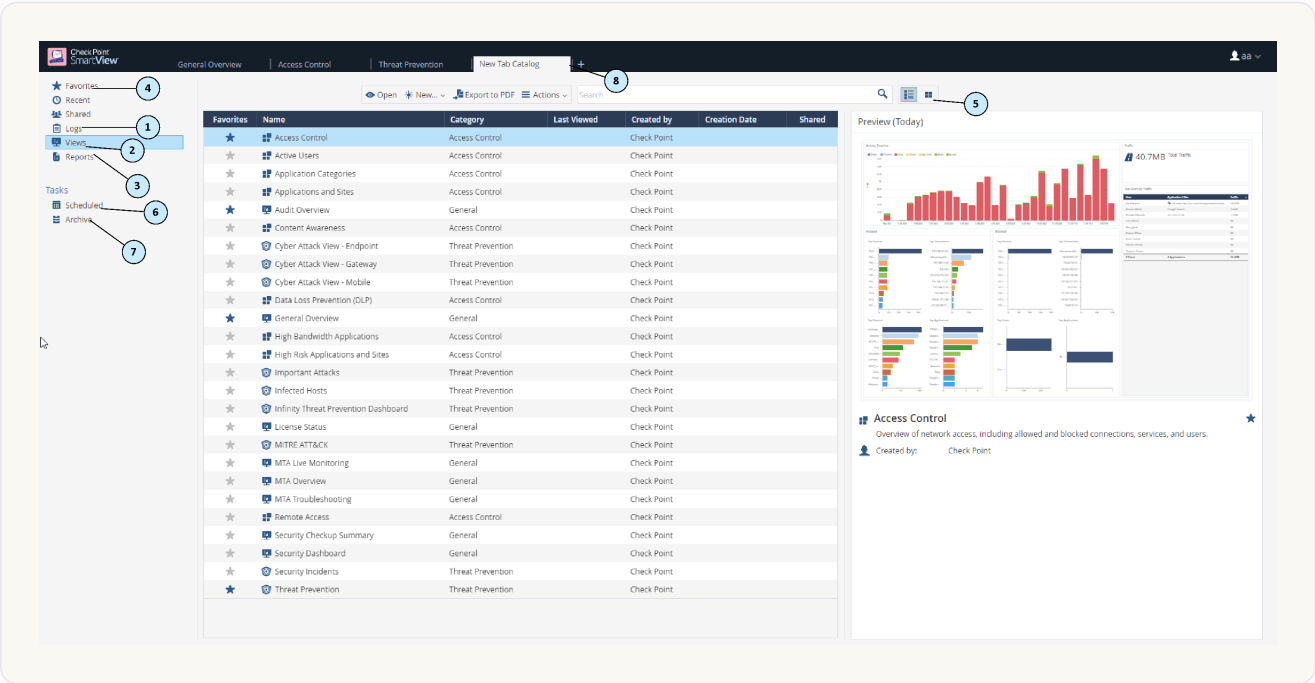
> 참 고
>
> View와 Report를 쓰려면 먼저 SmartEvent Server를 설치·구성해야 합니다(시작하기).

## View와 Report — 무엇이 다른가

**View** 는 여러 widget으로 짜인 대화형 대시보드 입니다. 각 widget은 쿼리 하나의 결과를 차트·표 등으로 보여 주고, widget을 더블클릭하면 더 구체적인 View나 원시 로그로 드릴다운 할 수 있습니다. 반면 **Report** 는 여러 View와 표지를 묶은 문서 라 더 자세하지만, 드릴다운은 할 수 없습니다. 한마디로 View는 파고드는 분석용, Report는 정리해 전달하는 보고용 입니다. 둘 다 미리 정의된 것이 여럿 있고, 새로 만들거나 기존 것을 고칠 수 있습니다.

# 카탈로그 — 모든 View·Report의 입구

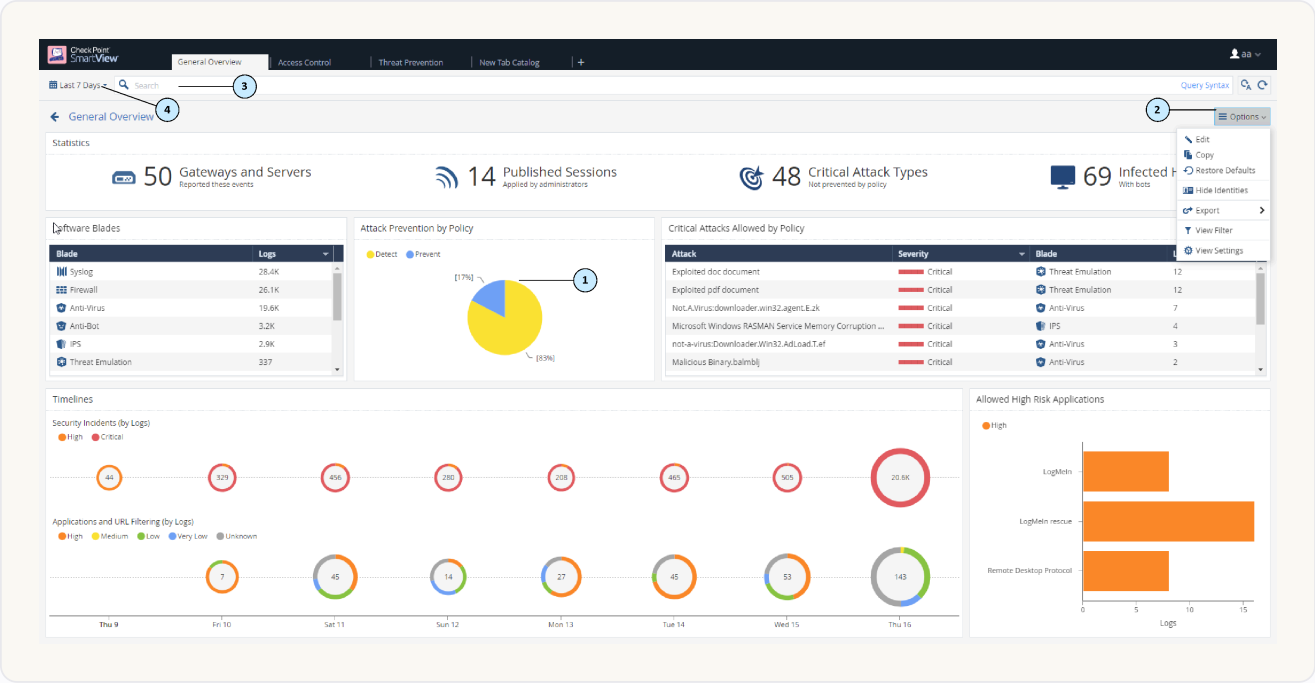
Logs & Events에서 **(+) 탭** 을 누르면 미리 정의된 것과 커스텀을 모은 카탈로그가 열립니다.




① Open Log View / Audit Logs View ② Views(+Compliance View) ③ Reports ④ Favorites·Recent ⑤ Table/Thumbnails 전환 ⑥ Scheduled Tasks ⑦ Archive(내보낸 결과 다운로드) ⑧ Catalog 새 탭 — 카탈로그 구성

*① Open Log View는 모든 Log Server의 로그를, Audit Logs View는 관리자 행동 기록을 보여 준다(이 둘은 Log Server에서, Compliance View를 뺀 나머지는 SmartEvent Server에서 온다). ② View 목록과 규제 준수를 돕는 Compliance View. ③ Report 목록. ④ 자주 쓰는 것 모음과 최근 항목. ⑤ 표/썸네일 보기 전환. ⑥ 예약 작업. ⑦ 내보낸 결과 다운로드. ⑧ 새 카탈로그 탭.*

View를 열면 widget·옵션·쿼리 검색줄·기간이 한 화면에 배치됩니다.




① Widget(쿼리 결과, 더블클릭 드릴다운) ② Options(편집·기본값 복원·신원 숨기기·내보내기) ③ 쿼리 검색줄 ④ Time Period — View 화면 구성

여는 절차는 간단합니다 — 카탈로그에서 Views나 Reports를 누르고, 항목을 골라 Open한 뒤, 기간(timeframe)을 정하고 검색줄에서 필터링 하면 됩니다. SmartEvent는 인터넷이 연결돼 있으면 미리 정의된 View·Report를 자동으로 내려받고 업데이트 합니다.

## MITRE ATT&CK View

보안 사고를 공격자가 쓴 전술(tactic)과 기법(technique) 관점 으로 들여다보고 싶을 때 **MITRE ATT&CK View** 를 씁니다. 쓰려면 SmartEvent와 함께 Threat Emulation·IPS·Anti-Bot 중 하나 이상 이 켜져 있어야 합니다. 카탈로그의 Views에서 이 View를 열면 색이 진할수록 공격 시도가 많은 heat map 이 나오고, 가장 진한 칸을 더블클릭해 개별 악성 메일·파일 다운로드까지 파고든 다음, 로그 안에서 그 공격에 쓰인 전체 기법·전술 목록을 확인할 수 있습니다. 더 깊은 설명은 Threat Prevention 가이드의 Cyber Attack View·MITRE를 함께 보세요.

## 내보내기·공유·스케줄

만든 View·Report는 PDF나 CSV로 내보낼 수 있습니다(CSV는 표만 내보내짐). 결과는 카탈로그의 **Tasks** > **Archive** 에서 받습니다. 대표적인 예가 **Network Activity Report** 로, 상위 출처·목적지·서비스 같은 주요 Firewall 연결을 보여 주는데, 이를 만들려면 SmartEvent가 Firewall 로그를 인덱싱 해야 하고, 정책 규칙의 Track 설정에 **per Session** 을 더해야 합니다(로그 다루기의 Track 설명 참고).

만든 Report는 내보내기 없이 팀과 **공유(Share)** 할 수도 있습니다 — 일반 관리자가 공유하면 같은 도메인의 모든 관리자에게, Multi-Domain의 super admin이 공유하면 모든 도메인 사용자에게 보입니다. 레이아웃과 widget 정의만 파일로 빼낸 **Template** 을 만들어 다른 서버·관리자에게 전달할 수도 있습니다. 정기 보고가 필요하면 **Schedule PDF/CSV** 로 반복 주기·기간·필터를 정하고, 이메일로 자동 발송 하게 설정합니다(이메일 서버 설정은 관리자마다 한 번만 하면 됨).

## 커스터마이즈와 widget

기존 View·Report는 Open 후 **Options** > **Edit** 에서 고칩니다. widget을 드래그&드롭으로 더하거나 옮기고, 필터를 정의 합니다. 한 가지 알아 둘 점은 timeframe과 검색줄은 View·Report 정의에 저장되지 않으므로, 생성할 때마다 지정 한다는 것입니다. 또 View를 template으로 삼아(Use View as template) "사용자별"처럼 한 기준으로 쪼갠 세분 보기 를 한 번에 뽑을 수도 있습니다.

widget은 종류가 다양합니다 — chart(막대·파이·영역·선), timeline, table, map(국가별), infographic(큰 의미값), container(여러 widget을 한 틀로 묶음) 입니다. widget이나 View는 복사해 다른 위치에 붙일 수 있는데, 복사하면 원본의 필터는 따라오지 않고 그 widget·View 자체의 필터만 따라옵니다.

마지막으로 **필터** 는 세 층으로 겹칩니다 — 전체 Report에 적용하는 필터, 한 View(페이지)와 그 안 모든 widget에 적용하는 필터, 그리고 선택한 widget에만 적용하는 필터 입니다. 검색줄로 즉석에서 거를 수도, 정의에 저장할 수도 있습니다. Active Directory 그룹으로 거르려면 Access Role을 만들어 정책을 설치한 뒤, Identity Awareness 로그에서 그룹 이름(보통 `ad_` 접두사)을 복사해 **User Group** 필드 필터에 넣습니다.

# 05 로그 다루기와 쿼리 언어

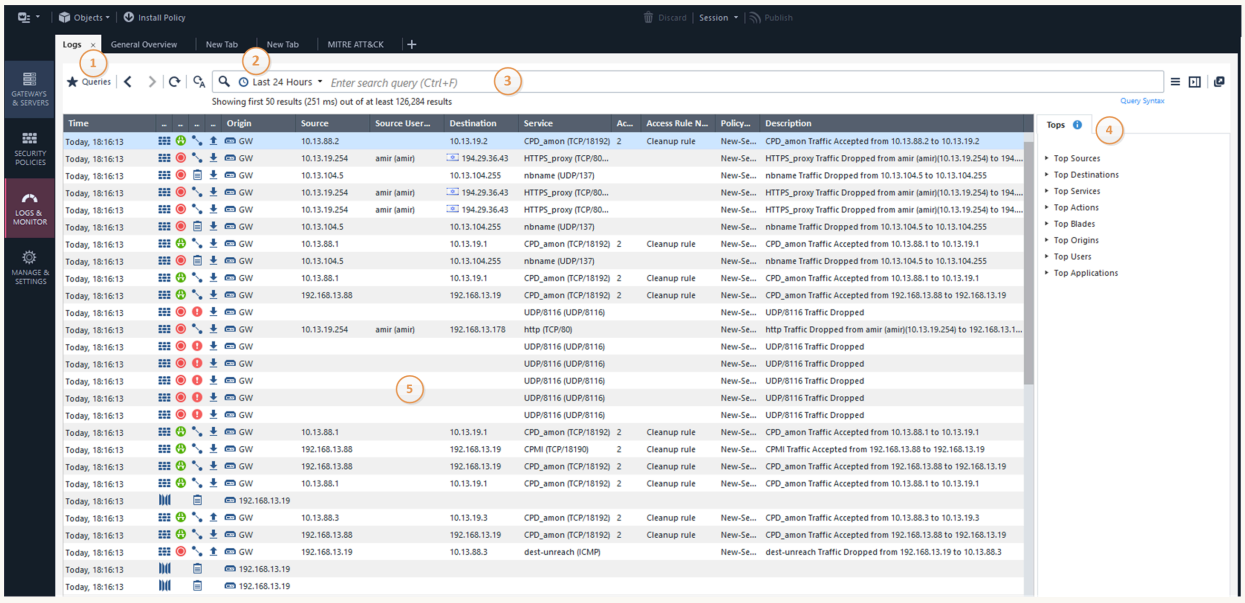
*로그 다루기와 쿼리 언어*

로그가 쓸모 있으려면 원하는 기록을 빠르게 찾아내 야 합니다. SmartConsole은 Google 검색처럼 간단히, 또는 강력한 쿼리 언어로 정교하게 로그를 뒤질 수 있게 해 줍니다. 이 장은 Logs 뷰의 구성, 어떤 규칙이 어떤 로그를 남기게 할지 정하는 **Track** 옵션, 그리고 검색·쿼리 언어를 정리합니다.

---

## Logs 뷰 — 어디서 보나

로그는 SmartConsole의 **Logs & Events** > **Logs** 탭에 뜹니다. Management Server의 IP로 접속하면 모든 Log Server의 로그를 통합해 보고 (indexing이 켜진 경우), 특정 규칙을 골라 아래 창의 Logs를 누르면 그 규칙이 만든 로그만 추려 줍니다.




① Queries(미리 정의·즐겨찾기 쿼리) ② Time Period ③ 쿼리 검색줄 ④ Log statistics 창(상위 결과) ⑤ Results 창(로그 항목) — Logs 뷰 구성

> 참 고
>
> Management Server는 indexing이 꺼져 있고 전용 Log Server는 켜져 있는 혼합 상황에서 Management Server에 접속하면, 통합 보기가 아니라 개별 로그 파일 단위로만 보입니다.

# Track — 무엇을 로그로 남길까

로그는 정책 규칙의 **Track** 열에서 정합니다. 규칙을 우클릭해 옵션을 고르고 정책을 설치하면 됩니다. 다만 모든 규칙을 추적하면 로그가 폭증해 디스크와 관리 부담이 커지니, 보안·사용자 행동 이해·리포트에 정말 쓸모 있는 규칙만 추적하는 것이 좋습니다.

기본 옵션은 이렇습니다 — **None**(로그 없음), **Log**(기본값, 출처·목적지·포트 등 매칭 정보를 기록), **Accounting**(10분 간격으로 업로드·다운로드 바이트와 browse time 갱신) 입니다. 레이어에 Application & URL Filtering·Content Awareness·Mobile Access 중 하나가 켜져 있으면 고급 옵션도 열립니다 — **Detailed Log**(규칙이 앱을 지정하지 않아도 매칭된 앱까지 표시), **Extended Log**(거기에 URL·파일 전체 목록까지) 인데, 이 둘은 패킷·연결을 더 깊이 검사하므로 성능 부담이 더 큽니다.

로그를 연결마다 하나씩(**per Connection**, Firewall 전용 레이어 기본값) 만들지, 한 세션을 하나로(**per Session**, App/URL·Content Awareness 레이어 기본값) 묶을지 도 고릅니다. 중요한 점은 SmartEvent가 per Connection 로그는 인덱싱하지 않는다 는 것입니다. 끝으로 **Alert** 옵션으로 팝업·이메일·SNMP trap·사용자 스크립트 를 트리거할 수 있고, 그 동작은 Global Properties > Log and Alert > Alerts에서 정의합니다.

#### 세션 로그와 Packet Capture

**Session** 은 사용자가 한 사이트·앱에서 한 활동 묶음 으로, 그 세션의 모든 활동이 하나의 세션 로그에 담깁니다( `type:Session` 으로 검색). 세션 로그의 아래 창에서 Connections·URLs·Files 탭을 보면, 각각 per Connection / Extended Log 설정에 따라 연결·URL·파일 내역이 보입니다. 기본적으로 세션이 3시간 이어지면 새 세션 로그가 시작됩니다. 한편 **Packet Capture** 를 켜면 로그를 만든 트래픽의 실제 패킷까지 캡처 파일로 Log Server에 함께 보내 져, 로그를 열어 그 안을 직접 들여다볼 수 있습니다(일부 Threat Prevention 블레이드는 기본으로 켜져 있음).

## 검색과 쿼리 언어

검색은 두 갈래입니다. 미리 정의된 쿼리를 골라 쓰거나, 검색줄에 직접 조건을 입력합니다. `Ctrl+F` 로 검색을 시작하고, `F5` 로 새로고침, `F6` 으로 5초마다 자동 갱신 합니다(자동 갱신 중 5초에 100건이 넘으면 집계 요약으로 보여 줌). 자주 쓰는 쿼리는 **Queries** > **Add to Favorites** 로 저장합니다. 결과 창은 성능을 위해 처음엔 50건만 보여 주고, 스크롤하면 인덱스에서 더 끌어옵니다. 오른쪽 Tops 창은 상위 통계를 보여 주는데, 이는 화면에 이미 나온 부분 결과로 추정한 값이지 전체 기간을 계산한 것은 아닙니다.

쿼리 언어의 기본 꼴은 `[<필드>:] <조건>` 이고, 여러 조건은 `AND` · `OR` · `NOT` 으로 잇습니다(조건만 나열하면 AND가 자동 적용). 한 단어가 아니라 구절이면 따옴표로 감쌉니다(예: `"John Doe"` ). 대부분 대소문자를 가리지 않지만 `source:` 처럼 예외가 있어, 결과가 안 나오면 대소문자를 바꿔 보세요.

IP는 한 단어로 세며, 와일드카드와 네트워크 표기를 함께 씁니다 — 예컨대 `src:192.168.1.0/24` 나 `src:192.168.2.*` 는 그 범위 전체를 매칭합니다. 와일드카드는 `?` 가 한 글자, `*` 가 문자열 을 뜻해, `Jo?` 는 Joe·Jon을, `Jo*` 는 Joseph·John까지 잡습니다. 자주 쓰는 필드 키워드로는 `severity` · `action` · `blade` (= `product` )· `source` (= `src` )· `destination` (= `dst` )· `service` · `user` · `origin` 등이 있고, 규칙 번호는 `rule:7.1` , 규칙 이름은 필드 없이 자유 텍스트로 찾습니다.

> 팁
>
> 특정 규칙이 만든 로그만 빠르게 보려면, SmartConsole에서 규칙 번호를 우클릭해 **Copy Rule UID** 한 뒤 검색줄에 layer_uuid_rule_uuid:*_<UID> 형식으로 붙여 넣으면 일반 붙여넣기보다 빠릅니다.

복합 예시 몇 개로 감을 잡으면 됩니다 — `blade:"application control" AND action:block` (앱 차단 로그), `(blade:Firewall OR blade:IPS OR blade:VPN) AND NOT action:drop` (드롭되지 않은 그 세 블레이드 로그), `source:(192.168.2.1 OR 192.168.2.2) AND destination:17.168.8.2` . 필드에 값을 여러 개 줄 때는 Boolean 연산자를 명시하고 괄호로 묶어야 합니다. Action 필터는 종류가 많은데, Accept·Drop(통보 없이 차단)·Reject(TCP RST로 통보)·Detect(탐지만)·Prevent·Decrypt/Encrypt 등 각 동작의 뜻은 원문 표 (p.97~)에 정리돼 있습니다.

## 결과 보기와 컬럼 프로파일

결과 창에 어떤 열이 보일지는 **Column Profile** 이 정합니다. 쿼리 결과에서 가장 자주 나온 블레이드에 맞춰 자동 선택(Automatic Profile Selection) 되며, 우클릭으로 수동 지정하거나 Edit Profile로 열을 더하고 빼고 순서를 바꿀 수 있습니다. 바꾼 폭·구성은 우클릭 > Save Profile로 다음 세션까지 유지됩니다.

## SmartView Web Application으로 보기

클라이언트 설치가 부담스러우면 브라우저로 같은 화면을 봅니다 — `https://<Management Server IP>/smartview/` ( `/smartview/` 는 대소문자 구분, Chrome·Firefox 지원). SmartView의 강점은 비관리자도 쓸 수 있고, 최대 100만 건까지 로그를 내보낼 수 있다는 점입니다. 다만 로그인은 SmartConsole 관리자 객체에 설정된 Check Point Password 인증만 지원하고, Standalone 서버에서 SmartView를 열면 Gaia Portal·API 문서·Web SmartConsole 포털이 멈추니 주의하세요. 로그는 현재 CSV로만 내보낼 수 있습니다.

## 로그 고가용성과 Syslog 서버

게이트웨이가 한 Log Server에 로그를 못 보내면 보조 Log Server로 보내게 할 수 있고, 두 Log Server를 한 SmartEvent Correlation Unit에 묶으면 끊김 없는 로그 스트림으로 계속 상관분석 합니다. 한편 외부 분석 도구를 쓰려고 게이트웨이가 **syslog 서버** 로 직접 로그를 보내게 할 수도 있습니다 — Check Point는 RFC 3164(구)와 RFC 5424(신) 를 지원하며(IPv6 로그·Software Blade 로그는 미지원), SmartConsole에서 Host와 Syslog Server 객체를 만들어 Gateway 객체 > Logs에 추가합니다. syslog는 암호화되지 않으므로 게이트웨이와 수신 측을 가까이, 안전한 망에서 통신시키세요. 더 깊은 파싱은 Syslog 수동 파싱을, 형식 변환 없는 SIEM 연동은 Log Exporter를 보세요.

> 참 고
>
> 고로그율 환경에서 커널 파라미터 `fwsyslog_enable=1` 로 Gaia 커널이 syslog를 직접 보내게 해 성능을 높일 수 있으나, Check Point Support의 명시적 지시가 있을 때만 켜세요.

# 06 SmartEvent로 이벤트 분석

*SmartEvent로 이벤트 분석*

로그가 수십억 건이면 사람이 다 못 봅니다. **SmartEvent** 는 그 로그를 우선순위가 매겨진 보안 이벤트로 압축해, 실시간 그래픽으로 보여 주는 통합 이벤트 관리·분석 솔루션입니다. 이 장은 이벤트가 무엇이고 로그가 어떻게 이벤트로 바뀌는지, SmartEvent의 구조, 그리고 Event Policy를 어떻게 손보는지를 정리합니다. 세부 절차는 원문 (p.123~166)을 함께 보세요.

---

> 주 의
>
> SmartEvent는 Full High Availability 클러스터 구성에서는 지원되지 않습니다.

## 이벤트란 무엇인가

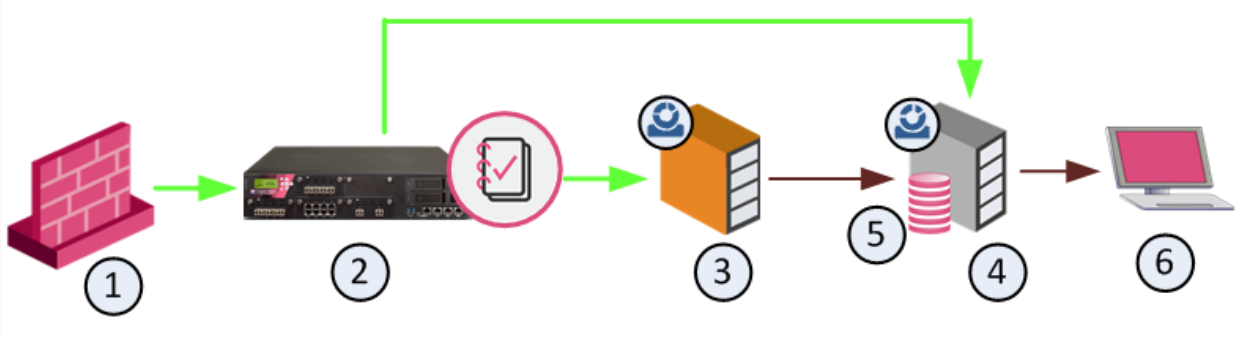
> *An event is a record of a security incident. It is based on one or more logs, and on rules that are defined in the Event Policy.*
>
> — AdminGuide, "What is an Event?" (p.123)

핵심은 이벤트가 하나 이상의 로그 + Event Policy의 규칙 으로 만들어진다는 점입니다. 로그 하나로 되는 이벤트도 있고(예: 심각도 High인 Anti-Bot 로그 하나 → High Severity Anti-Bot 이벤트), 여러 로그가 모여야 되는 이벤트도 있습니다(예: 같은 인증서로 다른 사용자가 로그인한 로그 둘 → Certificate Sharing 이벤트).

로그가 이벤트로 바뀌는 방식은 둘입니다. Firewall·VPN·HTTPS Inspection이 아닌 로그는 SmartEvent가 자동으로 이벤트로 정의 하고, 하나 이상의 로그가 만드는 의심스러운 패턴은 Correlation Unit이 상관분석해 이벤트(correlated event)로 생성 합니다. 반대로 대부분을 차지하는 Firewall·VPN·HTTPS 로그는 성능을 위해 기본적으로 이벤트로 만들지 않습니다.

# SmartEvent의 구조

여러 부품이 협력해 위협을 추적합니다.




① SmartEvent/SmartConsole 클라이언트가 SmartEvent Server를 관리 ② Log Server가 로그 저장 ③ Correlation Unit이 로그를 분석해 이벤트 식별 ④ SmartEvent Server가 이벤트 DB 보유 ⑤ Events Database ⑥ 클라이언트가 이벤트 표시 — 로그·이벤트 데이터 흐름

흐름을 따라가면 이렇습니다 — Security Gateway(①)가 로그를 **Log Server**(②)에 보내면, **SmartEvent Correlation Unit**(③)이 각 로그 항목을 분석해 Event Policy의 패턴과 맞는지 보고, 위협 패턴을 찾으면 이벤트를 만들어 SmartEvent Server로 전달 합니다. **SmartEvent Server**(④)는 SmartView용 로그 인덱싱, Event Policy 정의, Correlation Unit 관리 를 맡고, 그 이벤트를 **Events Database**(⑤)에 담습니다. 운영자는 **SmartConsole이나 SmartView**(⑥)로 이벤트를 보고 필터·종료하고 정책을 설치합니다.

규모가 크면 부품을 여러 컴퓨터에 나눠 배포(distributed) 하길 권하며, 한 Correlation Unit이 여러 Log Server의 로그를 분석 할 수 있습니다. 반대로 여러 Correlation Unit이 같은 Log Server를 읽게 해 한쪽이 죽어도 이어지는 중복(HA) 도 가능한데, 이때 같은 이벤트가 DB에 중복되니 **Detected By** 필드로 어느 Unit이 탐지했는지 구분합니다.

# Correlation Unit이 로그를 이벤트로 바꾸는 단계

Correlation Unit이 로그를 받으면 정해진 순서로 거릅니다. 먼저 **Global Exclusions**(이벤트에 기여하지 않을 로그)와 맞는지 보고, 맞으면 버립니다. 그다음 각 **Event Definition** 의 필터와 견줍니다 — 필터는 제품별로 나뉘어, 로그의 Product 값이 허용 목록에 있는지 먼저 보고, 있으면 그 제품의 세부 조건(Action·Event Type·Port 등)을 확인 합니다. 맞으면 그 로그는 **Event Candidate**(이벤트 후보)에 더해집니다.

# Event Candidate 10.1.1.5

| Product | Security Gateway |
|---|---|
| Action | reject |
| Port | 83 |
| Protocol | TCP |
| Source | 10.1.1.5 |

| Product | Endpoint Security |
|---|---|
| Action | block |
| Type | firewall |
| Port | 84 |
| Protocol | TCP |
| Source | 10.1.1.5 |

| Product | Endpoint Security |
|---|---|
| Action | block |
| Type | firewall |
| Port | 80 |
| Protocol | TCP |
| Source | 10.1.1.5 |

| Product | Security Gateway |
|---|---|
| Action | drop |
| Port | 83 |
| Protocol | TCP |
| Source | 10.1.1.5 |

Event Candidate 식별 흐름 — 로그를 Event Definition 필터와 매칭

후보는 "몇 초 안에 몇 건"이라는 임계(threshold)를 넘을 때까지 로그를 추적 하는 임시 묶음입니다. 같은 Event Definition이라도 출처(source) 같은 속성이 다르면 별도의 후보가 새로 생겨, 후보들이 모인 풀(Event Candidate Pool) 을 이룹니다. 예컨대 "차단 연결 급증" 이벤트는 게이트웨이마다 후보를 두어, 한 게이트웨이의 차단 로그가 임계를 넘으면 그 후보가 이벤트로 승격 됩니다. 승격 직전 **Event Exclusion** 과도 한 번 더 견주어, 맞으면 이벤트를 만들지 않습니다. 이벤트가 생긴 뒤에도 관련 로그가 임계 기간 동안 계속 들어오면 그 이벤트에 더해, 같은 사건을 하나로 묶고 시작·종료 시각을 정확히 유지합니다.

# Event Policy 손보기

Event Policy는 **SmartEvent GUI**(Logs & Events > + > SmartEvent Settings & Policy)의 Policy 탭에서 다룹니다. 화면은 왼쪽 Selector Tree(탐색), 가운데 Detail 창(설정), 오른쪽 Description 창(설명) 으로 나뉩니다. 중요한 점은 변경은 저장(File > Save)하고 Correlation Unit에 설치(Actions > Install Event Policy)해야 적용 된다는 것이며, 저장 전이라면 File > Revert Changes로 되돌릴 수 있습니다.

이벤트마다 손볼 수 있는 요소는 **Threshold**(몇 초 안에 몇 건이면 이벤트), **Severity**(Critical·Medium 등), **Automatic Reaction**, **Exception**, **Time Object**(Working Hours) 입니다. 오탐(false alarm)이 많으면 임계의 건수나 기간을 늘려 줄입니다. 다만 Threat Prevention 로그 기반 이벤트의 심각도는 여기 설정이 아니라 protection 타입에서 가져옵니다(원하면 Event Format 탭에서 덮어쓰기 가능).

### Automatic Reaction — 이벤트가 떴을 때 자동으로

이벤트 탐지 시 **Automatic Reaction** 을 발동시킬 수 있습니다. 종류는 **Mail**(관리자에게 이메일), **Block Source**(그 출처 IP를 일정 시간 차단), **Block Event Activity**(여러 출처·목적지의 분산 공격 차단), **External Script**(직접 만든 스크립트 실행), **SNMP Trap** 입니다. 만드는 흐름은 Reaction 객체 생성 → 이벤트(또는 예외)에 할당 → 저장 → Correlation Unit에 Event Policy 설치 입니다. External Script는 `$RTDIR/bin/ext_commands/` 아래에 두고 실행 권한을 주며, 10분을 넘기면 SmartEvent Server가 강제 종료합니다. 스크립트 안에서는 `EVENT=$(cat)` 으로 이벤트를 받아 `awk` · `sed` 로 필드를 파싱하는데, 이벤트는 `(name: value; ...)` 꼴의 name-value 집합입니다.

### Working Hours·Exception으로 정교하게

**Working Hours**(Time Object)는 근무 시간 외의 비정상 접근을 잡는 데 씁니다. **Exception** 은 같은 이벤트라도 특정 출처·목적지·서비스에만 다른 기준을 적용 하게 합니다(예: "내부망 Port Scan"이 60초에 30건이면 이벤트인데, 호스트 A에서는 10초에 2건도 이벤트로). 직접 새 이벤트를 만들려면 기존 정의를 우클릭하거나 Actions > New Custom Event로 마법사를 띄워, 한 로그로 볼지 여러 로그로 볼지, 어떤 제품·필드로 매칭할지, 임계와 후보 구분 필드를 무엇으로 할지 를 정합니다. 미리 정의된 이벤트를 고치면 결과는 새 User Defined Event로 저장됩니다.

## 오탐 줄이기

네트워크 스캔 소프트웨어나 바쁜 웹 서버처럼 정상인데도 트래픽이 많아 이벤트로 오인되는 경우가 있습니다. 이럴 때는 그 출처를 스캔 이벤트에서 제외하거나, 그 서버의 허용 연결률을 높여 줍니다. 원문에는 SNMP·DNS·LDAP·HTTP Proxy·SMTP·Anti-Virus 정의 서버 등 서버 종류별로 흔히 오탐을 내는 이벤트와 그 이유를 정리한 표(p.153~) 가 있으니, 임계·예외를 조정할 때 바탕으로 삼으세요. SmartEvent 시스템 관리(Correlation Unit·Log Server 추가, Internal Network 정의, 객체 생성)는 Policy 탭의 General Settings에서 합니다 — 특히 **Internal Network** 를 정의해야 SmartEvent가 트래픽의 방향(Incoming·Outgoing·Internal)을 판단 할 수 있고, 이는 초기 sync가 끝난 뒤에야 가능합니다.

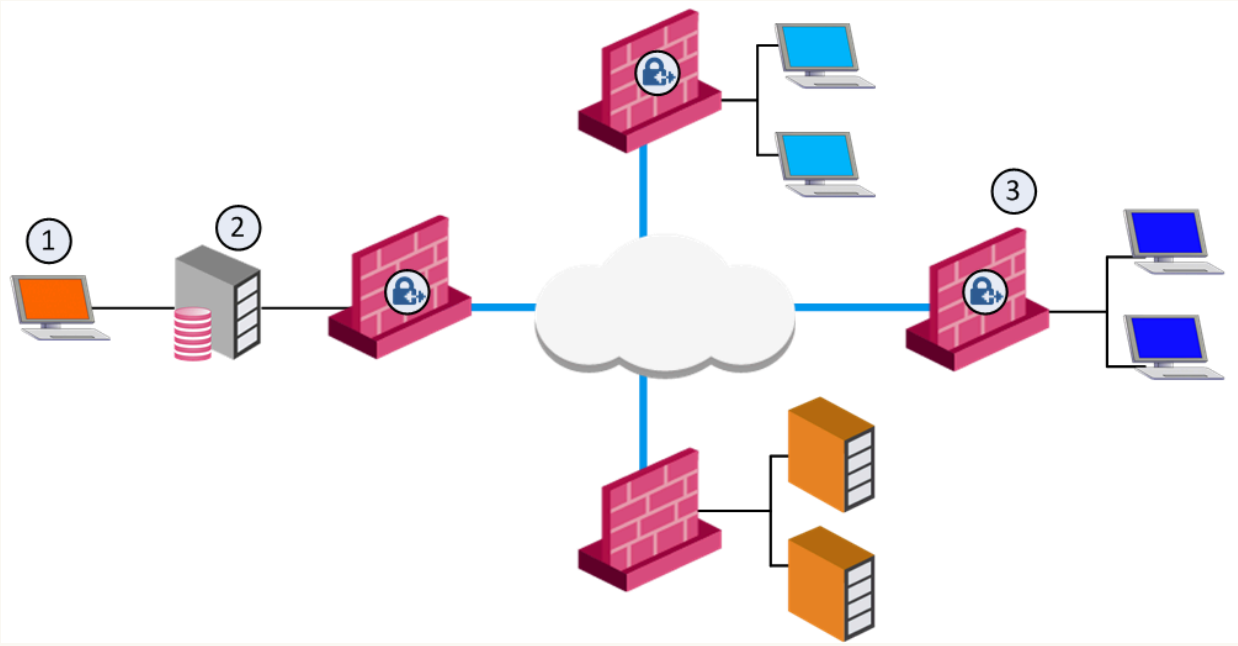
# 07 트래픽·연결 모니터링 (SmartView Monitor)

*트래픽·연결 모니터링 (SmartView Monitor)*

로그가 "지나간 일"의 기록이라면, 모니터링은 "지금 무슨 일이 벌어지는가"를 봅니다. **SmartView Monitor** 는 게이트웨이·터널·원격 사용자·트래픽 흐름의 상태와 성능을 한 화면에서 실시간으로 보여 주는 네트워크·보안 분석 시스템입니다. 이 장은 그 동작 원리, 즉각 조치와 Suspicious Activity 규칙, 알림·임계값, 그리고 장치·VPN·사용자 모니터링을 개념 위주로 정리합니다. 세부 절차는 원문(p.167~215)을 보세요.

## 어떻게 동작하나 — AMON 프로토콜

상태 데이터는 Management Server가 모아 SmartView Monitor가 보여 줍니다. 대상은 Check Point Security Gateway, OPSEC Gateway, 그리고 VPN·ClusterXL 같은 Software Blade 입니다.




① SmartView Monitor가 Management Server에서 데이터를 받음 ② Security Management Server ③ 로컬·원격 Security Gateway — AMON으로 상태를 수집하는 흐름

흐름은 이렇습니다 — 게이트웨이(③)와 Management Server(②) 사이에 SIC가 맺히면, Management Server가 **AMON(Application Monitoring) 프로토콜** 로 각 블레이드의 상태를 가져오고, SmartView Monitor(①)가 그 데이터를 받습니다. 즉 Management Server는 AMON 클라이언트, 각 게이트웨이는 AMON 서버 역할이며, AMON은 SIC 기반이라 SIC가 초기화돼야만 데이터를 모읍니다. 수집 주기는 기본 60초이고, Global Properties > Log and Alert > Time Settings에서 바꿉니다.

모니터링 화면을 여는 길은 둘입니다 — SmartConsole의 Gateways & Servers에서 게이트웨이를 골라 **Monitor** 를 누르면 Device Status·License·System Counter·Traffic 이 뜨고, 더 풍부한 **SmartView Monitor** 는 Logs & Events에서 새 탭을 열어 **Tunnel & User Monitoring** 으로 엽니다.

> 참 고
>
> Management 데이터베이스에 객체가 15,000개를 넘으면 SmartView Monitor가 안 열릴 수 있습니다.

## 무엇을 볼 수 있나

미리 정의된 뷰로 게이트웨이 상태, 원격 사용자, System Counter, VPN 터널, Cooperative Enforcement, 트래픽 을 실시간·과거 그래프로 봅니다. 활용 예를 들면, 인터넷이 느린 원인을 찾을 때 특정 서비스·규칙·객체별 Traffic 뷰로 P2P나 HTTP 과다 사용을 짚 거나, 원격 직원이 접속을 못 할 때 CPU 사용률 Counter 뷰로 동시 접속 한계를 의심 하는 식입니다. SmartView Monitor에서는 직접 커스텀 뷰도 만들 수 있습니다.

## 즉각 조치와 Suspicious Activity 규칙

상태에 문제가 보이면 그 객체에 바로 손을 쓸 수 있습니다 — SmartConsole 클라이언트 연결 끊기, Cluster Member 시작·정지, 그리고 의심 트래픽 차단 입니다.

특히 **SAM(Suspicious Activity Monitoring)** 은 SmartView Monitor에 통합된, 의심 활동을 즉시 차단하는 도구 입니다. 핵심은 SAM 규칙이 정책 설치 없이 바로 적용된다 는 점이라, 명백한 침입자를 조사하는 동안 빠르게 막을 수 있습니다. 다만 SAM 규칙은 CPU를 쓰므로 만료 시간(Expiration)을 꼭 정해 성능에 부담을 주지 않게 합니다. 출처·목적지·서비스로 차단 대상을 정하고, **Advanced** 에서 동작을 Notify(통보만)·Drop(응답 없이 폐기)·Reject(RST 보내고 종료) 중에 고르며 Track(No Log·Log·Alert)을 설정합니다.

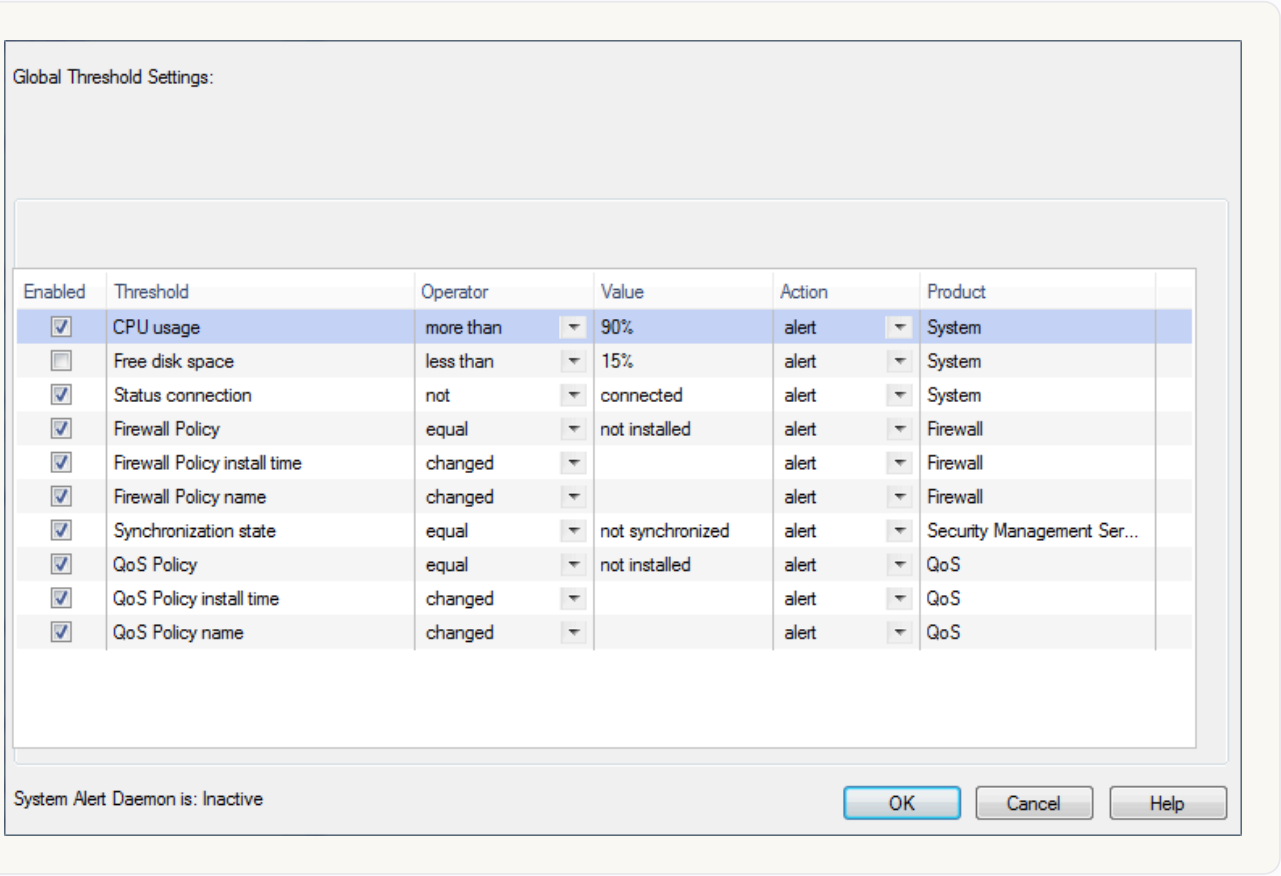
> 팁
>
> Traffic 뷰(Top Sources·Top P2P Users 등)에서 의심 결과의 막대를 우클릭해 **Block Source** 를 누르면, 그 사용자 IP와 해당 서비스로 SAM 규칙이 자동으로 짜여 바로 적용됩니다. 예컨대 P2P 사용자를 한 시간 동안 차단·로깅하며 당사자에게 연락하는 식입니다.

이미 적용된 규칙은 **Enforced Suspicious Activity Rules** 창에서 관리하며, 충돌하는 규칙이 있으면 한쪽만 보입니다(예: drop과 reject 규칙이 겹치면 drop만 표시). CLI에서는 `sam_alert` 유틸리티로 SAM 동작을 실행할 수 있습니다(자세히는 R82 CLI Reference Guide).

## 알림과 임계값

**Alert** 는 잠재적 위협을 실시간으로 알리는 장치입니다. 게이트웨이가 알림을 Management Server로 보내면, 그것이 SmartView Monitor로 전달되고 기본적으로 관리자 화면에 팝업으로 뜹니다. 알림이 발생하는 경우는 둘 — alert로 추적하게 설정한 규칙·속성이 매칭될 때, 그리고 System Alert(예: 여유 디스크 10% 미만, 정책 변경)의 임계값을 넘을 때 입니다. 알림 명령은 SmartConsole의 Global Properties > Log and Alert > Alerts에서 정의하고, System Alert 모니터링은 SmartView Monitor의 Tools > Start/Stop System Alert Daemon으로 켜고 끕니다.

**임계값(Threshold)** 은 게이트웨이별로 정합니다 — Gateways Status 뷰에서 객체를 우클릭해 Configure Thresholds를 열고, 전역 설정을 따를지(Use global settings), 끌지(None), 따로 정할지(Custom) 고릅니다.




임계값 초과 시의 Action 선택 — Global Threshold Settings 창

임계를 넘었을 때의 Action은 none·log·alert(팝업)·mail·snmptrap·useralert(스크립트) 중에서 고릅니다. 한편 **SNMP 모니터링 임계값** 을 쓰면 각 장치에 일일이 묻지 않고도 Hardware·High Availability·Networking·Resources 같은 범주를 SNMP trap으로 자동 감시 할 수 있습니다.

# 장치·VPN·사용자 모니터링

SmartView Monitor의 나머지 뷰들은 운영 상태를 깊이 들여다봅니다. **Device Status** 는 게이트웨이·블레이드의 동작 여부를, **VPN Tunnels** 는 터널이 살아 있는지, 어떤 커뮤니티·피어와 연결돼 있는지 를, **Users** 는 현재 접속한 원격 사용자 를, **Traffic / System Counters** 는 대역폭 상위 호스트와 제품별 자원 사용량 을 보여 줍니다. VPN 터널의 의미와 구성은 Site-to-Site VPN 가이드와 Remote Access VPN 가이드를, 클러스터 상태는 ClusterXL 가이드를 함께 보면 좋습니다.

끝으로 **Cooperative Enforcement** 는 온프레미스 Harmony Endpoint Security 서버와 Security Gateway를 연동 해, 단말의 준수 상태를 게이트웨이 차원에서 강제하는 기능입니다. 요지는 SmartView Monitor로 실시간 상태를 보고, 이상이 보이면 SAM으로 즉시 막고, 임계값·알림으로 자동 감시 체계를 갖춘다 는 것입니다.

# 08 타사 로그 가져오기 — Syslog·Windows·SNMP

*타사 로그 가져오기 — Syslog·Windows·SNMP*

Check Point만 로그를 만드는 것은 아닙니다. 라우터·스위치·서버·IDS 등 타사 장비의 로그를 Log Server로 끌어와, Check Point 로그처럼 분석 하면 한곳에서 통합 관제가 됩니다. 가져올 수 있는 형식은 크게 셋입니다 — Syslog 메시지, Windows Event, SNMP Trap 입니다. Log Server가 이를 Check Point 로그 형식으로 변환하면, SmartEvent가 그 로그를 다시 보안 이벤트로 바꿀 수 있습니다.

---

## Syslog 메시지 가져오기

많은 타사 장비가 syslog 형식으로 로그를 남깁니다. Log Server는 **syslog parser**(파서)로 raw 데이터를 Check Point 로그 형식으로 재구성 합니다. 기본 지원되지 않는 제품은 직접 파서를 만들어 Log Server에 설치해야 하는데, 그 방법( `sk55020` )은 샘플 syslog를 **Log Parsing Editor** 에 들여오기 → syslog 필드와 Check Point 로그 필드를 매핑 → 파서를 Log Server에 설치 순입니다. 들여온 메시지는 SmartConsole의 Logs & Events > Logs 탭에서 보입니다.

> 참 고
>
> Access Control 규칙이 syslog 컴퓨터와 Log Server 사이의 **ELA** 트래픽을 허용해야 합니다.

들여온 syslog를 이벤트로 만들려면, SmartEvent Server가 그 Log Server의 로그를 읽게 설정 한 뒤 **Product Name** 필드로 필터링합니다 — 이 필드가 syslog에서 만들어진 이벤트를 고유하게 식별해 줍니다. 파서를 GUI 대신 손으로 짜는 방법은 Syslog 수동 파싱에서 다룹니다.

# Windows Event 가져오기

Windows 서버의 이벤트는 **Check Point Windows Event Service**(WinEventToCPLog)가 끌어옵니다 — Windows 서버에서 이벤트를 읽어 Check Point 로그로 변환해 Log Server에 넣는 Windows 서비스 애플리케이션 입니다. 핵심은 이 프로세스는 Windows 컴퓨터에만 설치되지만, Log Server 자체는 다른 플랫폼이어도 된다 는 점이라, 한 대의 중앙 WinEventToCPLog 서버가 여러 Windows 호스트의 이벤트를 모아 보낼 수 있습니다.

큰 흐름은 이렇습니다 — Support Center에서 WinEventToCPLog 에이전트를 받아 Windows 서버에 설치 → Windows 서버와 Management Server 사이에 SIC 생성 → 어느 컴퓨터의 이벤트를 모을지 설정 입니다. 원격 컴퓨터의 이벤트까지 읽으려면 `WinEventToCPLog -s` 로 그 컴퓨터에 접근할 권한을 가진 관리자 계정 을 등록해야 합니다(로컬 관리자 이름을 맞추거나, 도메인 관리자로 등록하면 도메인 전체 접근).

설정은 크게 세 가지입니다. 먼저 SmartConsole에서 **OPSEC Application 객체**(Client Entities에서 ELA 선택)를 만들고 Activation Key로 신뢰를 초기화 합니다. 그다음 Windows 호스트에서 패키지 설치 후 `-pull_cert` 로 인증서를 받아 신뢰를 맺 고, 끝으로 Windows Audit Policy 를 설정(예: Logon 이벤트 감사)하고 `-l` (Log Server IP)· `-a` (이벤트를 보내는 컴퓨터 IP)· `-s` (관리자 계정) 명령으로 어디서 어디로 보낼지를 지정 합니다. 더 고급 설정은 `sk98861` 을 보세요.

> 참 고
>
> 여기서도 Access Control 규칙이 Windows 컴퓨터와 Log Server 사이의 ELA 트래픽을 허용해야 합니다.

# SNMP

**SNMP(Simple Network Management Protocol)** 는 관리 데이터를 네트워크 장치와 주고받는 인터넷 표준 프로토콜 입니다. SNMP를 지원하는 장치(agent)는 자기 정보를 **MIB(Management Information Base)** 에 담아 두었다가 요청자에게 보냅니다. Gaia의 SNMP 구성 자체는 이 가이드의 범위를 벗어나니, 자세히는 Gaia 가이드의 SNMP 또는 R82 Gaia Administration Guide의 System Management > SNMP 절을 참고하세요. 모니터링 임계를 SNMP trap으로 보내는 법은 트래픽·연결 모니터링에서 다뤘습니다.

# 09 Log Exporter — SIEM 으로 로그 내보내기

*Log Exporter — SIEM으로 로그 내보내기*

회사가 Splunk·QRadar·ArcSight 같은 별도의 SIEM을 쓴다면, Check Point 로그를 그쪽으로 흘려보내야 합니다. **Log Exporter** 가 그 다리로, Management Server나 Log Server에서 syslog 프로토콜로 로그를 표준 형식으로 바꿔 외부로 보내는, 쉽고 안전한 방법 입니다. 이 장은 그 동작 원리와 설정의 큰 줄기를 정리합니다. 명령 옵션·SIEM 별 세부는 워낙 방대하니(p.223~277) 개념을 잡은 뒤 원문과 sk122323을 함께 보세요.

---

## 무엇을 지원하나

Log Exporter는 폭넓게 받쳐 줍니다 — syslog agent를 돌릴 수 있는 여러 SIEM, TCP/UDP 위의 syslog, 여러 형식(Syslog·CEF·LEEF·JSON 등), TLS 1.2 기반 상호 인증, Security 로그·Audit 로그 또는 둘 다, 로그 필터링, 그리고 SmartView의 해당 로그 카드 링크와 첨부(Forensics·Threat Emulation 리포트 등)까지 내보내기 입니다. Splunk용 Check Point App도 내부적으로 Log Exporter를 써서 로그를 보냅니다.

## 어떻게 동작하나 — E-T-L

Log Exporter는 Log Server에서 도는 멀티스레드 데몬 서비스 로, 각 로그를 읽어 원하는 형식·매핑으로 바꿔 대상 서버로 보냅니다. 내부 절차는 **E-T-L** 입니다 — **Extract**(들어오는 로그를 읽음) → **Transform**(설정대로 변형) → **Export**(대상 서버로 전송) 입니다. Multi-Domain 환경에서는 도메인마다 자기 Log Exporter 데몬을, 대상이 여럿이면 대상마다 데몬 을 따로 둡니다.

특히 똑똑한 점은 끊김 대응입니다 — 3rd party 서버와 끊기면 내보내기를 멈추고 마지막 위치를 기억했다가, 다시 연결되면 그 지점부터 자동으로 이어 갑니다. 또 온라인·오프라인(밀린) 로그를 병렬로 보내되, 대상 서버가 느리면 오프라인 전송 속도를 늦춰 실시간 로그를 우선 합니다. R81.20부터는 내보내기 속도를 CPView로 모니터링할 수 있습니다.

## SmartConsole에서 설정하기 (R81 이상)

R81부터는 SmartConsole에서 직접 Log Exporter를 만들어 Log Server에 연결합니다. 큰 흐름은 이렇습니다.

먼저 **Log Exporter/SIEM 객체** 를 만듭니다(Objects > More object types > Server > Log Exporter/SIEM). General 페이지에서 Export를 **Enabled** 로 켜고, 대상 서버 IP/FQDN·포트·프로토콜(UDP 기본 또는 TCP) 을 넣습니다. Data Manipulation 페이지에서 형식(Syslog 기본·CEF·LEEF·Generic·Splunk·LogRhythm·Json) 을 고르는데, 기본적으로 갱신 로그는 직전 로그와 달라진 부분만 담으므로, 매번 전체 데이터를 보내려면 **Aggregate log updates before export** 를 켭니다. Attachments 페이지에서는 SmartView의 로그 상세·첨부 링크나 Attachment ID를 함께 보낼지 를 고릅니다(첨부는 기본적으로 포함되지 않음).

그다음 Management Server / 전용 Log Server / SmartEvent Server 객체의 Logs > Export 에서 방금 만든 객체를 추가 하고, **Install database** 로 적용합니다. 업그레이드 후에는 반드시 Install database를 다시 한 번 돌려야 하며, Multi-Domain에서 Global Domain에 설정했다면 해당 Domain Management Server에 접속해 설치합니다.

## CLI에서 설정하기 — cp_log_export

GUI 대신 Expert 모드 CLI로도 다룹니다. 핵심 명령이 `cp_log_export` 입니다. 새 대상을 만드는 기본 꼴은 이렇습니다.

```
cp_log_export add name <설정 이름> [domain-server {mds | all}] \
  target-server <대상 IP/호스트명> target-port <포트> \
  protocol {tcp | udp} \
  format {cef | generic | json | leef | logrhythm | rsa | splunk | syslog} [--apply-now]
```

이름에는 Latin 문자·숫자· `-` · `_` · `.` 만 쓰고 문자로 시작 해야 하며, 이 명령이 `$EXPORTERDIR/targets/` 아래에 그 이름의 대상 디렉터리를 만듭니다. Multi-Domain에서는 `domain-server` 가 필수 인데, `mds` 는 메인 MDS 레벨의 audit 로그만, `all` 은 모든 도메인의 audit 로그를 내보냅니다. 이후 `cp_log_export set ...` 으로 값을 바꾸고, `cp_log_export restart name <이름>` 으로 설정을 반영 합니다. 자세한 옵션·예시·고급 파라미터는 원문(p.228~)과 sk를 보세요.

# TLS·SIEM별 설정·예전 방식에서 전환

전송을 암호화하려면 **TLS** 를 구성합니다 — TLS 1.2 기반 상호 인증 으로, 인증서를 두고 대상과 안전하게 주고받습니다(syslog 자체는 평문이므로 외부로 보낼 때 권장). 원문에는 Splunk·QRadar·ArcSight·RSA·LogRhythm 등 주요 SIEM별 권장 형식과 설정(p.266~) 이 정리돼 있으니, 쓰는 제품에 맞춰 따르면 됩니다.

예전 방식을 쓰던 환경을 위한 전환 안내도 있습니다 — **LEA**(Log Export API)에서 Log Exporter로, 그리고 **CPLogToSyslog** 에서 Log Exporter로 옮기는 절차입니다. 요지는 R82에서는 Log Exporter가 표준 경로이므로, 구식 LEA·CPLogToSyslog 대신 Log Exporter로 통일 하는 것입니다(비표준 LEA 포트 같은 옛 설정은 시작하기 참고). 그 밖에 부록(Appendix, p.273~)에 추가 형식·매핑 참고가 담겨 있습니다.

밀리초 단위 시각으로 내보내는 특수 옵션은 밀리초 단위 로그에서, 첨부를 자동으로 가져오는 API는 로그 API와 첨부 파일 API에서 이어집니다.

# 10 밀리초 단위 로그

*밀리초 단위 로그*

로그를 외부로 많이 내보내는 환경에서는, 같은 1초 안에 로그가 여럿 도착해 순서를 가릴 수 없는 문제가 생깁니다. 사건의 흐름을 정확히 재구성하려면 어느 로그가 먼저 왔는지 알아야 하므로, R82는 도착 시각을 밀리초(0.001초) 단위까지 담아 보내는 옵션을 둡니다. Log Exporter를 쓰면서 로그율이 높은 환경 을 위한 기능이며, **기본적으로 꺼져 있습니다.**

---

## Security Gateway 쪽에서 켜기

게이트웨이(클러스터라면 각 Member)에서 켭니다. Expert 모드로 들어가 `$FWDIR/scripts/` 디렉터리에서 스크립트를 실행하는데, `enable_disable_time_in_milli.sh 1` 이면 켜고, `0` 이면 끕니다.

```
cd $FWDIR/scripts/
enable_disable_time_in_milli.sh {1 | 0}
```

> 주 의
>
> 이 절차는 FWD 프로세스를 재시작합니다.

## Log Server 쪽에서 켜기

Log Server에서는 Log Exporter 설정에 `time-in-milli` 옵션을 넣습니다. 새 exporter를 만들 때는 `cp_log_export add ... time-in-milli true` , 기존 것을 고칠 때는 `cp_log_export set name <이름> time-in-milli true` 로 바꾼 뒤 `cp_log_export restart name <이름>` 으로 반영합니다( `cp_log_export` 의 일반 사용법은 Log Exporter 참고).

설정하면 시각 필드에 밀리초 자리가 더해져 내보내집니다. 한 가지 알아 둘 점은, 이 기능이 켜지지 않은 게이트웨이에서 온 로그는 그 추가 자리가 `000` 으로 채워진다 는 것입니다 — 즉 형식은 통일되되, 실제 밀리초 정밀도는 기능을 켠 게이트웨이의 로그에만 담깁니다.

# 11 로그 API와 첨부 파일 API

*로그 API와 첨부 파일 API*

SmartConsole을 열지 않고 자동화 스크립트로 로그를 가져오고 싶을 때, 두 개의 management API가 쓰입니다. **API for Logs** 는 명령 하나로 로그나 상위 통계를 조회 하고, **Log Attachments API** 는 그 로그에 딸린 첨부(패킷 캡처·Threat Emulation 리포트 등)를 자동으로 가져옵니다. 둘 다 Management Server에서 실행합니다.

---

## API for Logs — 로그를 명령으로 조회

이 API의 강점은 SmartConsole의 Logs 탭 검색줄과 똑같은 필터 문법을 그대로 쓴다 는 점입니다. SmartConsole 접근 권한이 없거나, management API에 익숙한 운영자가 자동화 안에서 로그를 끌어와 통계를 내려고 할 때 유용합니다. 권한은 로그인한 사용자 프로파일대로 적용됩니다.

할 수 있는 일은 이렇습니다. **로그 가져오기** 는 환경의 어느 Log Server에서든 명령 하나로 로그를 끌어오며, 선택 파라미터로 로그 종류(Traffic/Audit)·기간·필터·대상 Log Server·결과 수 제한 을 줍니다. 결과가 많으면 Log Server에 부담을 주지 않도록 작은 묶음(기본·최대 100건)으로 페이지를 나눠 가져오는데, 다음 페이지는 앞서 받은 `query-id` 로 이어 받습니다. **상위 통계** 는 sources·destinations·services·blades·users 등 여러 필드의 top 값 을 조회합니다. 또 각 로그가 첨부를 가졌는지도 알려 줘, 그 ID로 첨부 API를 호출하게 합니다. SmartConsole에서는 버튼 하나로 현재 Logs 탭의 쿼리(기간·Log Server·필터·기본 50건 제한)를 그대로 API 명령으로 생성 할 수도 있습니다.

명령의 기본 꼴은 `mgmt_cli show-logs new-query.filter <필터> new-query.time-frame <기간> ...` 입니다. `time-frame` 은 last-hour·today·last-24-hours·this-week·last-30-days·all-time·custom 등 을 받고, custom이면 ISO 형식의 `custom-start` · `custom-end` 를 줍니다. `type` 으로 logs/audit를, `log-servers` 로 특정 서버를, `max-logs-per-request` (1~100)로 건수를 지정합니다. 상위 통계는 `new-query.top.field <필드> new-query.top.count <수>` 를, 다음 페이지는 `query-id <id>` 를 씁니다.

> 참 고
>
> time-frame 은 yyyymmddThhmmssZ 형식을 입력으로 받지 않으며, non-index 모드의 로그 쿼리는 지원하지 않습니다.

# Log Attachments API — 첨부를 자동으로 가져오기

블레이드마다 첨부의 종류가 다릅니다 — IPS 로그에는 패킷 캡처, Threat Emulation 로그에는 요약 리포트가 딸립니다. 트래픽 부담을 줄이려 로그는 보통 첨부 없이 내보내지므로, 첨부가 필요하면 이 API로 따로 가져옵니다. Log Exporter로 외부 syslog에 첨부를 끌어와 자동화에 쓰거나, 사용자에게 SmartConsole 접근을 주지 않으려는 경우에 맞습니다. 모든 게이트웨이 버전을 지원합니다.

가져오는 길은 두 가지입니다. **Log Exporter** 경로에서는, `export-attachment-ids true` 로 켜면 내보낸 로그에 `log-attachment-id` 가 붙 고(여러 첨부 ID를 공백으로 구분), 그 ID를 `mgmt_cli get-attachment attachment-id "<id>"` 에 넣어 받습니다. 응답은 base64로 인코딩된 JSON 이라, 디코딩해 지정한 폴더에 풀어야 씁니다. **API for Logs** 경로에서는, `mgmt_cli show-logs` 응답 안의 각 로그 `id` 를 가져와 `mgmt_cli get-attachment id "<log id>"` 로 그 로그의 첨부를 모두 받습니다.

# 12 Syslog 수동 파싱

*Syslog 수동 파싱*

타사 장비의 syslog를 들여올 때, GUI **Log Parsing Editor** 대신 파싱 파일을 손으로 작성 할 수도 있습니다. 이 장은 그 수동 파싱의 사전 준비, Log Server에서 파싱이 일어나는 절차, 파일을 만들고 검증하는 흐름, 그리고 파싱 언어의 얼개를 개념 위주로 정리합니다. 문법 세부는 워낙 깊으니(p.287~304) 큰 그림을 잡은 뒤 원문을 보세요.

---

> 주 의
>
> 기본 제공 파싱 파일을 직접 고치면 업그레이드 때 자동으로 보존되지 않습니다. 바꾼 부분에 주석을 달아 무엇을 고쳤는지 남겨 두세요.

## 시작 전에 — 준비와 고려사항

좋은 파서를 짜려면 장비가 만드는 로그의 구조를 정확히 알아야 합니다. 그래서 벤더의 로깅 가이드(모든 로그 종류와 구조 파악용)와, 실제 장비에서 뽑은 로그 샘플(가능한 한 많이, 파서 검증·튜닝용) 을 함께 준비합니다. 그다음 Free Text Parsing 언어와 Log Server 위 파싱 파일들의 위치를 익히고, 비슷한 제품의 기존 파싱 파일과 견주어 봅니다. 끝으로 어떤 필드를 뽑을지 고릅니다 — 같은 부류의 장비는 보통 비슷한 필드를 갖습니다(예: 방화벽·라우터는 출발지/목적지 IP·포트·프로토콜·accept/reject, IDS/IPS는 공격 이름/ID).

## Log Server에서 파싱이 일어나는 절차

파싱은 Log Server에서 syslog 데몬이 syslog를 받아 파싱을 호출하며 시작됩니다. 파싱 파일들은 `$FWDIR/conf/syslog/` 에 있고, 출발점은 `syslog_free_text_parser.C` 입니다 — 이 파일이 모든 syslog에 공통인 필드(PRI·날짜·시각)와, 그 syslog를 만든 머신·애플리케이션을 먼저 뽑습니다.

그다음 `allDevices.C` 를 거치는데, 이 파일은 두 갈래를 참조합니다 — 사용자가 정의한 장치 파일 목록 ( `UserDefined/UserDefinedSyslogDevices.C` )과, Check Point가 정의한 목록 ( `CPdefined/CPdefinedSyslogDevices.C` ) 입니다. `allDevices.C` 는 장치 파싱 파일들을 차례로 훑어, 들어온 syslog와 형식이 맞는 파일을 찾습니다. 한 파일이 예비 파싱에 성공하면(=그 syslog의 출처로 판명되면) 나머지를 그 파일이 마저 파싱하고, 못 맞추면 Check Point 장치 파일들로 계속 넘어가 매칭될 때까지 시도합니다.

## 파싱 파일 만들고 검증하기

직접 만드는 흐름은 이렇습니다. `<제품명>.C` 파일을 만들어 `$FWDIR/conf/syslog/UserDefined` 에 두고, `UserDefinedSyslogDevices.C` 에 그 파일을 include하는 줄( `:cmd_name (include)` … `:file_name ("...")` )을 더합니다. 필요하면 **dictionary 파일**( `<제품명>_dict.ini` )도 만드는데, dictionary는 서로 다른 장비에서 같은 의미를 가진 값들을 공통 값으로 번역해, Event Definition에서 그 공통 값을 쓰게 해 줍니다. 이 역시 `UserDefinedSyslogDictionaries.C` 에 include 줄을 더합니다.

만든 파서는 실제 syslog 샘플을 Log Server에 보내 검증 합니다 — SmartConsole에서 Logs and Masters > Additional Logging Configuration 의 **Accept Syslog messages** 를 켜고, Log Server 객체를 편집한 뒤 `cpstop & cpstart` (또는 `fw kill fwd & fwd -n` )로 Log Server의 fwd를 재시작합니다. 그다음 장비나 syslog 생성기(예: Kiwi Syslog Message Generator)로 샘플을 보냅니다.

> 팁
>
> 로그가 기대대로 안 보이면 파싱 파일에 문제가 있는 것입니다. 구문 오류는 `fwd -n` 전에 `TDERROR_ALL_FTPARSER` 값을 5로 두면 메시지를 자세히 볼 수 있고, SmartConsole에 **'Product syslog'** 로 뜨면 제대로 파싱되지 않고 일반 syslog로 처리된 것입니다. 뽑은 필드는 일부가 Information 섹션이나 More Columns에서만 보일 수 있습니다.

## Free Text Parsing 언어의 얼개

이 언어는 입력 문자열을 파싱해 정보를 뽑고 로그 필드를 정의 합니다 — 이 필드가 Check Point 로그의 일부로 나타나고 이벤트 정의에 쓰입니다. 각 파싱 파일은 **명령(command)의 트리** 로 이뤄지며, 명령마다 입력의 일부를 검사·파싱하고(때로 필드를 더하고) 성공·실패에 따라 다음으로 넘어갈지를 정합니다.

명령은 네 부분으로 이뤄집니다 — `cmd_name` (명령 이름), command arguments(동작을 정의하는 인자), `on_success` (성공 시 다음 명령), `on_fail` (실패 시 다음 명령) 입니다. 예컨대 `try` 명령은 인자로 무언가를 시도하고, 성공하면 `on_success` 안의 명령을, 실패하면 `on_fail` 안의 명령을 실행하는 식으로 가지를 칩니다. 사용 가능한 명령들과 dictionary의 자세한 문법은 원문(p.292~)에 정리돼 있으니, 실제로 파서를 짤 때 참고하세요. GUI로 더 쉽게 파서를 만드는 길은 타사 로그 가져오기의 Log Parsing Editor를 보세요.

# 13 명령줄 참조

*명령줄 참조*

로깅·모니터링과 관련된 CLI 명령들의 전체 참조는, 다른 가이드와 마찬가지로 전용 문서로 넘깁니다.

---

> *See the R82 CLI Reference Guide.*
>
> — AdminGuide, "Command Line Reference" (p.286)

이 가이드 곳곳에서 이미 핵심 명령들을 맥락과 함께 다뤘습니다 — Log Exporter를 다루는 `cp_log_export` (Log Exporter), 밀리초 로그를 켜는 `enable_disable_time_in_milli.sh` (밀리초 단위 로그), 로그·첨부를 조회하는 `mgmt_cli show-logs` · `mgmt_cli get-attachment` (로그 API와 첨부 파일 API), 오프라인 로그 인덱싱의 `evstop` / `evstart` · `log_indexer` (시작하기), SAM 동작을 실행하는 `sam_alert` (트래픽·연결 모니터링)가 그것입니다.

여기에 나오지 않은 명령의 정확한 구문·옵션·예시는 **R82 CLI Reference Guide** 에서 확인하세요. 요지는 일상 로깅·모니터링은 SmartConsole·SmartView로 충분하고, CLI는 Log Exporter 설정·오프라인 인덱싱·자동화처럼 특정 작업에 보조로 쓰며, 전체 명령 목록은 별도 CLI 가이드가 정본 이라는 것입니다.