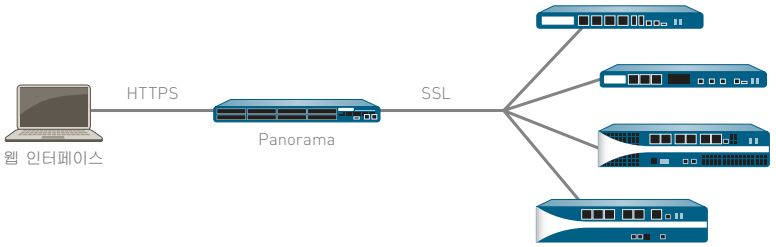
PANORAMA

Panorama는 Palo Alto Networks 차세대 방화벽 네트워크에 대한 중앙 집중식 정책 및 장치 관리 기능을 제공합니다.

- 네트워크의 애플리케이션, 각 사용자, 보안에 미치는 잠재적 영향을 그래프 형태로 요약
- 사용할 회사 정책과 로컬 정책을 중앙에서 배포하여 유연성 극대화
- 역할 기반 관리를 통해 장치 수준에서 또는 전역에서 적절한 관리 권한 위임
- 네트워크 트래픽, 보안 사건 및 관리상의 수정 사항을 중앙에서 분석, 조사 및 보고.



규모가 큰 조직에서는 대개 기업 네트워크를 통해 방화벽을 배포합니다. 그러나 개별 장치들의 다양성과 복잡성으로 인해 이를 관리하고 제어하는 프로세스가 어렵고 번거로우며, 결과적으로 관리 인력의 부담과 관련 비용이 증가하게 됩니다.

Panorama는 Palo Alto Networks 차세대 방화벽에 대한 중앙 집중식 관리 및 가시성을 제공합니다. 관리자는 한 곳에서 애플리케이션, 사용자 및 방화벽을 통과하는 콘텐츠를 파악할 수 있습니다. 이렇게 네트워크에 존재하는 대상을 정확히 파악하고 안전한 애플리케이션 사용 정책을 구현하면 관리상의 수고는 최소화되고 보안 능력은 최대화됩니다. 관리자는 시간별로 집계된 데이터 또는 로컬 방화벽에 저장된 데이터로 중앙에서 분석, 보고 및 포렌식을 수행할 수 있습니다.

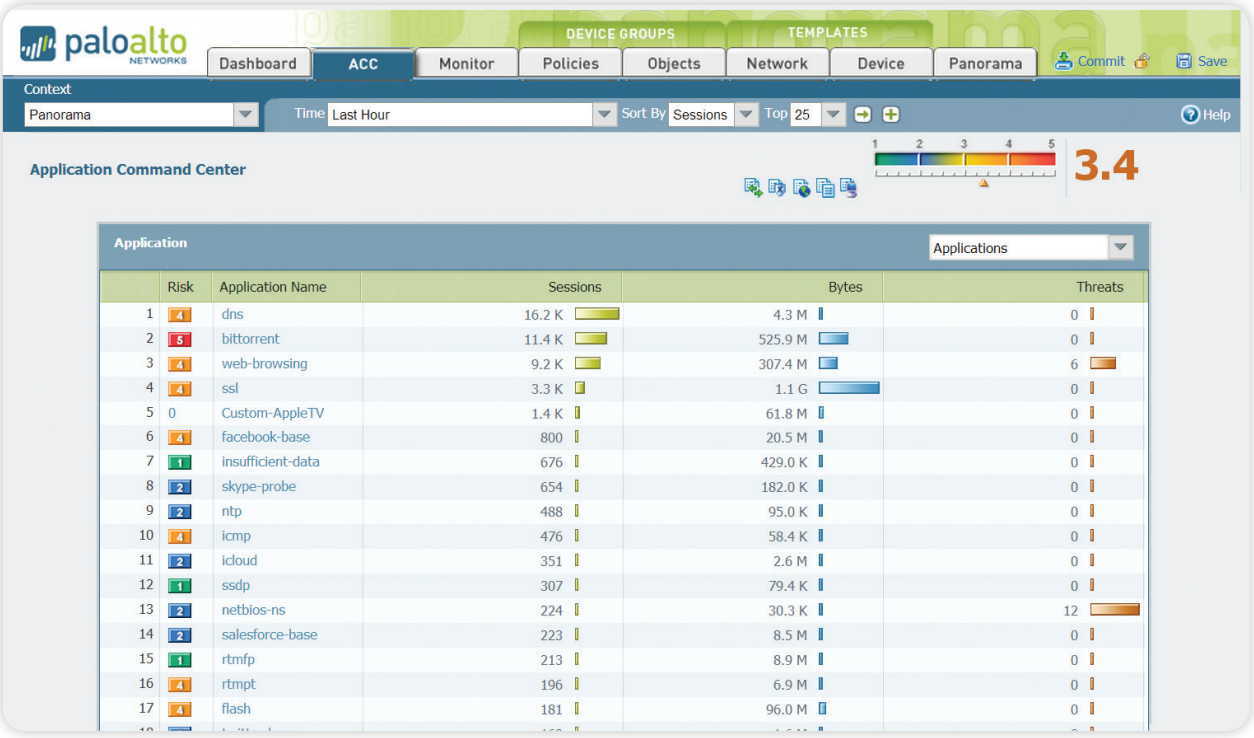
Panorama와 개별 장치는 모두 동일한 웹 기반 UI를 함께 사용하므로 별다른 교육 없이도 실무에 바로 적용할 수 있습니다. Palo Alto Networks는 일관성을 중요하게 여기며, 경쟁사와 뚜렷이 차별화되는 이점을 제공해야 한다는 기업 철학을 충실히 지켜 나가고 있습니다.

중앙 집중식 가시성: ACC(Application Command Center)

Panorama의 ACC(Application Command Center)는 관리 중인 애플리케이션, URL, 모든 Palo Alto Networks 장치를 통과하는 위협 및 데이터(파일 및 패턴)를 그래픽으로 보여 줍니다. ACC는 각 장치에서 동적으로 데이터를 가져오므로 네트워크의 애플리케이션, 애플리케이션을 사용 중인 사람, 위험을 초래할 수 있는 잠재적 위협에 대한 최신 정보가 관리자에게 제공됩니다. 관리자는 새롭거나 낯선 애플리케이션이 있을 때 클릭 한 번으로 애플리케이션의 설명, 핵심 기능, 동작의 특징 및 현재 사용하는 사람 등, 세부 정보를 볼 수 있습니다.

URL 범주 및 위협에 대한 추가 데이터는 네트워크 활동에 대한 완벽하고 포괄적인 정보를 제공합니다. 관리자는 ACC를 통해 네트워크 상황을 정확하게 파악함으로써 현명한 결정을 내리고 잠재적인 보안 위협에 신속하게 대처할 수 있습니다.

paloalto NETWORKS
the network security company™



Application Command Center는 애플리케이션 트래픽의 글로벌 및 로컬 보기를 제공하며, 현재 활동에 대한 세부 정보를 볼 수 있는 드릴다운 기능을 갖추고 있습니다.

글로벌 정책 제어: 애플리케이션 보안 구현

애플리케이션에 보안을 구현한다는 것은 특정한 위협 차단 정책 및 파일/데이터/ URL 필터링 정책을 적용한 상태로 애플리케이션에 대한 액세스를 허용한다는 의미입니다. Panorama는 관리자가 중앙 집중식으로 규칙을 관리하도록 함으로써 방화벽으로 보호되는 전체 네트워크에서 애플리케이션 보안을 구현합니다.

Panorama 기반의 공유 정책은 로컬 장치 규칙이 보안과 유연성을 모두 유지하면서 내부 또는 규정 요구 사항을 준수하도록 지원합니다. 즉, 중앙 관리와 로컬 관리를 결합한 형태로 정책 및 개체를 제어하기 때문에 글로벌 수준의 일관된 보안과 로컬 수준의 유연성 간에 조화를 이룰 수 있습니다.

관리자는 애플리케이션별 위협 방지로 콘텐츠와 네트워크를 보호하는 동시에 디렉터리 서비스 통합을 통해 사용자를 기반으로 애플리케이션 또는 애플리케이션 기능에 보안을 구현하는 정책을 배포할 수 있습니다. IP 주소가 아니라 사용자를 기반으로 애플리케이션 보안을 구현하는 단일 정책을 설정할 경우 조직이 필요로 하는 정책의 수가 크게 줄어듭니다. 또한 디렉터리 서비스 통합으로, 매일 발생하는 직원 입사, 부서 이동 및 변동으로 인한 관리 부담을 덜 수 있으며, 직원이 부서를 옮기더라도 보안 정책이 안정적으로 유지됩니다.

트래픽 모니터링: 분석, 보고 및 포렌식

Panorama는 로컬 장치 관리 수준에서 사용 가능한 것과 동일한 모니터링 및 보고 도구 집합을 활용하며, 활동에 대한 종합적 보기를 제공하여 네트워크 전반에 대한 가시성을 추가합니다. 관리자가 로그 쿼리를 수행하고 보고서를 생성하면 Panorama는 관리 중인 방화벽이나 Panorama로 전달된 로그에서 직접 가장 최근 데이터를 동적으로 끌어옵니다. 모든 장치에서 가장 최근 정보에 액세스함으로써 관리자는 보안 사건을 해결할 뿐 아니라 사전 대응적인 조치를 취하여 회사 자산을 보호할 수 있습니다.

- **로그 뷰어:** Panorama 관리자는 개별 장치 또는 모든 장치에 대해 셀 값을 클릭하거나 식 작성기로 정렬 기준을 정의하여 동적 로그 필터링을 사용함으로써 로그 활동을 빠르게 확인할 수 있습니다. 결과는 향후 쿼리를 위해 저장하거나 향후 분석을 위해 내보낼 수 있습니다.
- **사용자 정의 보고:** 기본 제공되는 보고서를 그대로 사용하거나, 필요에 따라 사용자 정의하거나, 하나로 묶을 수 있습니다.
- **사용자 활동 보고서:** Panorama에서 사용자 활동 보고서에는 사용된 애플리케이션, 방문한 URL 범주, 방문한 웹 사이트 및 개별 사용자가 지정된 기간 동안 방문한 모든 URL이 표시됩니다. Panorama는 보호하는 방화벽이나 사용 중인 IP 또는 장치에 상관없이 사용자의 활동에 대한 종합 보기를 사용하여 보고서를 구성합니다.

Panorama 관리 아키텍처

Panorama는 중앙 관리와 로컬 제어를 모두 제공하는 모델을 사용하여 조직에서 Palo Alto Networks 방화벽을 관리할 수 있도록 합니다. 이를 위해 다음과 같은 다양한 도구가 제공됩니다.

- **템플릿**: Panorama는 템플릿을 통해 장치 및 네트워크에서 공통된 구성을 관리합니다. 템플릿은 관리자가 중앙에서 구성을 관리하고, 관리 중인 모든 방화벽에 변경 사항을 푸시하는 데 사용됩니다. 이 접근 방식을 사용하면 동일한 개별 방화벽이 여러 장치를 반복적으로 변경되지 않습니다. 장치별로 동일한 변경을 수행하지 않고, 수백 개의 방화벽 전반에서 공통된 DNS 및 NTP 서버 설정을 푸시하는 것이 그러한 사용의 예입니다.

- **장치 그룹**: Panorama는 장치 그룹을 통해 공통된 정책 및 개체를 관리합니다. 장치 그룹은 공통된 요구 사항을 가진 여러 장치의 규칙을 중앙에서 관리하는 데 사용됩니다. 장치를 그룹화하는 방식의 예는 지역(유럽 및 북미) 또는 기능(네트워크 주변 또는 데이터 센터) 위주일 수 있습니다. 장치 그룹 내에서 가상 시스템은 실제 방화벽과 동일한 수준에서 개별 장치로 인식됩니다. 이를 통해 장치의 서로 다른 가상 시스템 간에 공통된 규칙을 공유할 수 있습니다.

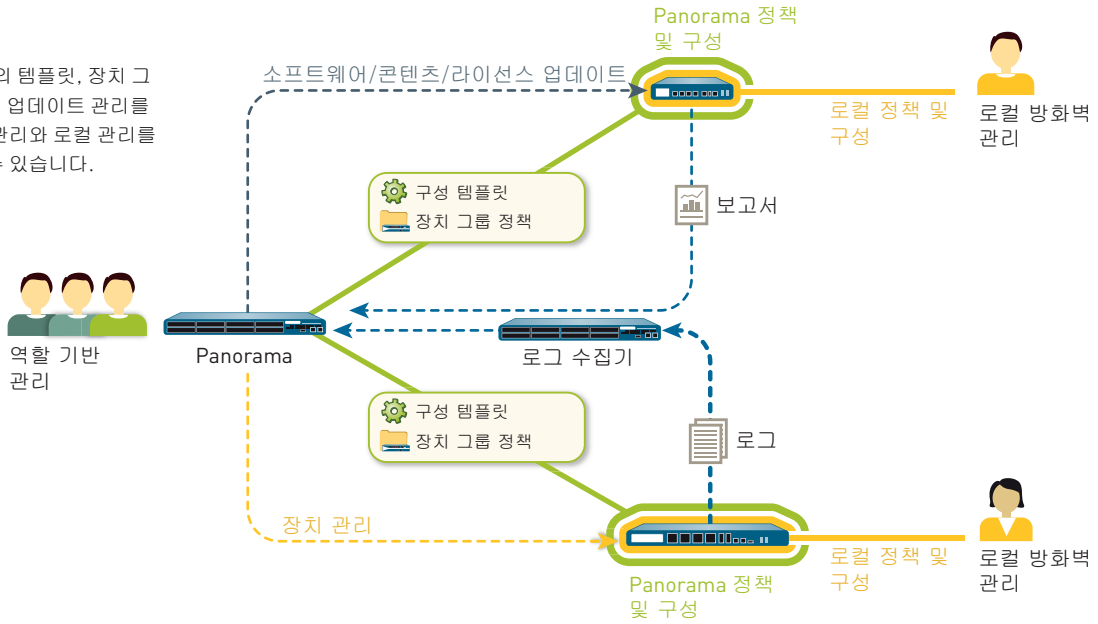
  조직은 방화벽 관리자에게 로컬 요구 사항에 맞춰 자체 수정 권한을 부여하는 동시에 중앙 제어를 위한 공유 정책을 사용할 수 있습니다. 장치 그룹 수준에서 관리자는 첫 번째 규칙 집합(사전 규칙) 및 마지막 규칙 집합(사후 규칙)으로 정의되는 공유 정책을 만들고 일치 기준과 비교하여 평가할 수 있습니다. 사전 규칙 및 사후 규칙은 관리되는 방화벽에서 볼 수 있으나, 정의된 관리자 역할의 컨텍스트 내에서 Panorama를 통해서만 편집할 수 있습니다. 사전 규칙과 사후 규칙 사이의) 로컬 장치 규칙은 로컬 관리자, 또는 로컬 방화벽 컨텍스트로 전환한 Panorama 관리자가 편집할 수 있습니다. 아울러 조직에서는 로컬로 관리되는 장치 규칙이 참조할 수 있는, Panorama 관리자가 정의한 공유 개체를 사용할 수 있습니다.

- **역할 기반 관리**: 조직에서는 역할 기반 관리를 사용하여 구성원마다 다른 기능 수준의 관리 권한(사용, 읽기 전용, 사용 안 함 및 보기에서 숨김)을 위임할 수 있습니다. 특정 관리자에게는 업무와 관련된 작업에 대한 적절한 액세스 권한을 주고, 그 외 다른 작업에 대해서는 숨김 또는 읽기 전용 권한을 줄 수 있습니다. 보안 관리자와 네트워크 관리자처럼 기업 내에서 별개의 업무를 담당하는 직원에게 서로 다른 역할을 정의하기 위해 이러한 액세스 제어 방식을 사용하는 것을 예로 들 수 있습니다. 관리자가 수행하는 모든 변경 사항은 발생 시간, 관리자 이름, 사용한 관리 인터페이스(웹 UI, CLI, Panorama), 사용한 명령 또는 작업과 함께 기록됩니다.

- **소프트웨어, 콘텐츠 및 라이선스 업데이트 관리**: 배포 규모가 커지면 조직에서 업데이트를 체계적으로 관리해야 합니다. 예를 들어, 보안 팀의 경우 소프트웨어 업데이트를 Panorama를 통해 모든 프로덕션 방화벽으로 일시에 전달하기 전에 중앙에서 적격성을 확인하는 과정이 필요합니다. Panorama를 사용하면 소프트웨어 업데이트, 콘텐츠(애플리케이션 업데이트, 바이러스 백신 시그니처, 업데이트 프로세스, 위협 시그니처, URL 필터링 데이터베이스 등) 및 라이선스에 대한 업데이트 프로세스를 중앙 집중식으로 관리할 수 있습니다.

템플릿, 장치 그룹, 역할 기반 관리, 업데이트 관리를 통해 조직은 가상화 도구, 정책 수립, 보고 및 로그 기록 등, 모든 관리 기능에 대해 글로벌 수준과 로컬 수준 모두에서 적절한 액세스 권한을 위임할 수 있습니다.

조직은 **Panorama**의 템플릿, 장치 그룹, 역할 기반 관리, 업데이트 관리를 통해 중앙 집중식 관리와 로컬 관리를 조화롭게 수행할 수 있습니다.



배포 유연성

Panorama를 사용하면 하드웨어 어플라이언스 또는 가상 어플라이언스를 배포할 수 있습니다.

하드웨어 어플라이언스

고성능 전용 하드웨어에서 Panorama를 배포하려고 하거나, Panorama 관리와 대량의 로그 데이터 기록 기능을 분리하려는 조직에서는 M-100 하드웨어 어플라이언스를 사용하는 것이 적합합니다. M-100에서 실행되는 Panorama는 다음 방식으로 배포할 수 있습니다.

- **중앙 집중형**: 이 시나리오에서 모든 Panorama 관리와 로그 기록 기능은 고가용성 옵션을 사용하여 단일 장치에 통합됩니다.
- **분산형**: 여러 장치에서 관리 기능과 로그 기록 기능을 분리하려는 조직에서 사용합니다. 이 구성에서는 기능이 관리자와 로그 수집기로 분리됩니다.
  - **Panorama 관리자**: Panorama 관리자는 관리되는 모든 장치 전반에서 정책 및 장치 구성과 관련된 작업의 처리를 담당합니다. 관리자는 로그 데이터를 로컬로 저장하지 않는 대신 별도의 로그 수집기를 사용하여 로그 데이터를 처리하고, 중앙에 보고하기 위해 로그 수집기에 저장된 데이터를 분석합니다.
  - **Panorama 로그 수집기**: 로그 기록의 양과 보유 요구 사항이 많은 조직에서는 관리되는 여러 방화벽에서 로그 정보를 집계할 전용 Panorama 로그 수집기 장치를 배포할 수 있습니다.

관리와 로그 수집을 분리함으로써, 조직은 확장성과 조직 또는 지역적 요구 사항을 충족하도록 배포를 최적화할 수 있습니다.

가상 어플라이언스

Panorama는 VMware ESX(i)에 가상 어플라이언스로 배포할 수 있습니다. 이를 통해 조직에서는 가상화 이니셔티브를 지원하고, 데이터 센터에서 공간을 차지하거나 관리 비용이 많이 드는 물리적인 랙을 줄일 수 있습니다. 가상 어플라이언스는 두 가지 방식으로 배포됩니다.

- **중앙 집중형**: 모든 Panorama 관리와 로그 기록 기능은 고가용성 옵션을 사용하여 단일 가상 장치에 통합됩니다.
- **분산형**: Panorama 분산형 로그 수집은 하드웨어와 가상 어플라이언스를 함께 사용할 수 있도록 지원합니다.
  - **Panorama 관리자**: 가상 어플라이언스는 Panorama 관리자의 역할을 수행하며, 관리되는 모든 장치 전반에서 정책 및 장치 구성과 관련된 작업의 처리를 담당합니다.
  - **Panorama 로그 수집기**: Panorama 로그 수집기는 과도한 로그 수집 및 처리 작업의 부하를 처리하며, M-100을 사용하여 배포될 수 있습니다. 가상 어플라이언스는 Panorama 로그 수집기로 사용할 수 없습니다.

조직은 하드웨어 또는 가상 플랫폼 중에서 선택할 수 있고, Panorama 기능을 결합하거나 분리하도록 선택할 수 있어 분산 네트워크 환경에서 여러 Palo Alto Networks 방화벽을 최대한 유연하게 관리할 수 있습니다.

PANORAMA 사양

지원되는 장치 수	최대 1,000개
고가용성	액티브/패시브
관리자 인증	로컬 데이터베이스
	RADIUS

M-100 관리 어플라이언스 사양

I/O

- (1) 10/100/1000, (3) 10/100/1000(향후 사용), (1) DB9 콘솔 직렬 포트

저장소(2개 옵션)

- M-100 1TB RAID: 2 x 1TB RAID 인증 HDD(1TB RAID 저장소)
- M-100 4TB RAID: 8 x 1TB RAID 인증 HDD(4TB RAID 저장소)

전원 공급 장치/최대 전력 소모

- 500W/500W

시간당 최대 BTU

- 1,705 BTU/시

입력 전압(입력 주파수)

- 100-240VAC (50-60Hz)

최대 전류 소모

- 10A@100VAC

MTBF(MEAN TIME BETWEEN FAILURE)

- 14.5 년

탑재 가능 랙(크기)

- 1U, 19" 표준 랙(1.75"H x 23"D x 17.2"W)

무게(독립 실행형 장치/출하 당시)

- 26.7lbs/35lbs

안전

- UL, CUL, CB

EMI

- FCC Class A, CE Class A, VCCI Class A

환경

- 작동 온도: 40~158F, 5~70C
- 비작동 온도: -40~149F, -40~65C

가상 어플라이언스 사양

최소 서버 요구 사항

- 40GB 하드 드라이브
- 4GB RAM
- Quad-Core CPU (2GHz+)

VMWARE 지원

- VMware ESX 4.1 이상

브라우저 지원

- IE v7 이상
- Firefox v3.6 이상
- Safari v5.0 이상
- Chrome v11.0 이상

로그 저장소

- VMware 가상 디스크: 최대 2TB
- NFS

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Accueil : +1.408.573.4000
Ventes : +1.866.320.4788
Assistance : +1.866.898.9087

www.paloaltonetworks.com

PAN_SS_P_051413