

PA-4000 시리즈

PA-4000 시리즈 차세대 방화벽 핵심 기능:

모든 포트에서 항상 APP-ID™로 모든 애플리케이션 분류

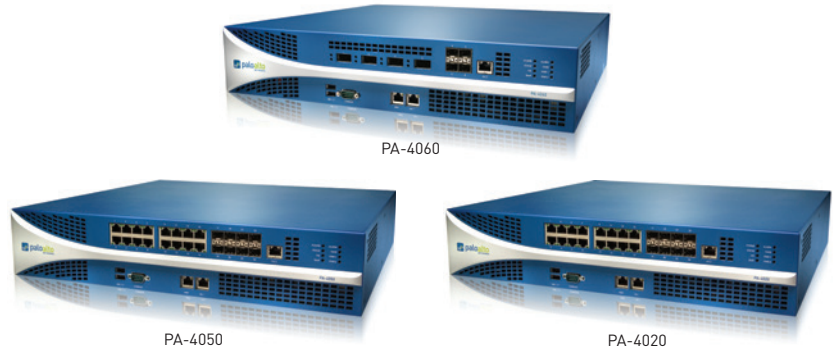
- 포트, 암호화(SSL 또는 SSH) 또는 우회 기법과 관계없이 애플리케이션을 식별합니다.
- 포트가 아닌 애플리케이션을 기반으로 트래픽 허용, 차단, 스케줄링, 위협탐지 및 트래픽 셰이핑 적용 등의 모든 애플리케이션 보안 정책을 결정합니다.
- 정책 제어, 위협 포렌식, 사용자 정의 App-ID 생성 또는 App-ID 개발에 대한 패킷 캡처에 대해 식별되지 않은 애플리케이션을 분류합니다.

USER-ID™ 및 GLOBALPROTECT™를 사용하여 모든 위치에 있는 모든 사용자에게 애플리케이션 보안 정책 강화

- Active Directory, LDAP, eDirectory Citrix 및 Microsoft Terminal Services와 에이전트 없이 연동됩니다.
- NAC, 802.1X 무선 및 기타 비표준 사용자 리포지토리를 XML API와 통합합니다.
- Microsoft Windows, Mac OS X, Linux, Android 또는 iOS 플랫폼을 실행하는 로컬 및 원격 사용자에게 일관성 있는 정책을 배포합니다.

CONTENT-ID™ 및 WILDFIRE™를 사용하여 알려진, 또는 알려지지 않은 모든 위협으로부터 보호

- 일반적으로 사용되는 우회 기술에 관계없이 취약성 공격, 맬웨어 및 스파이웨어 등의 알려진 다양한 위협을 모든 포트에서 차단합니다.
- 파일과 민감한 데이터의 인증되지 않은 전송을 제한하고 업무와 관련 없는 웹 서핑을 제어합니다.
- 알려지지 않은 맬웨어를 식별하여 100 개 이상의 악의적인 행위를 기반으로 분석한 후, 자동으로 시그니처를 생성하여 다음 업데이트를 통해 배포합니다.



Palo Alto Networks™의 PA-4000 시리즈는 고속의 데이터센터 및 인터넷 게이트웨이를 목표로 하는 3가지 고성능 플랫폼인 PA-4060, PA-4050 및 PA-4020으로 구성됩니다. PA-4000 시리즈는 네트워킹, 보안, 위협 방지 및 관리의 주요 기능 영역에 대한 전용 프로세서 및 메모리를 사용하여 최대 10Gbps의 처리량을 제공합니다.

고속 백플레인 은 별도의 데이터와 제어 플레인 으로 세분화되므로 관리 액세스는 트래픽 부하와 관계없이 항상 사용할 수 있습니다. PA-4000 시리즈 컨트롤의 핵심은 보안 전용 OS인 PAN-OS™로서, 이는 App-ID, User-ID, Content-ID, GlobalProtect 및 WildFire를 사용하여 애플리케이션을 안전하게 사용할 수 있도록 합니다.

성능 및 용량 ¹	PA-4060	PA-4050	PA-4020
방화벽 처리량(App-ID 사용)	10Gbps	10Gbps	2Gbps
Threat Prevention 처리량	5Gbps	5Gbps	2Gbps
IPSec VPN 처리량	2Gbps	2Gbps	1Gbps
초당 새로운 세션	60,000	60,000	60,000
최대 세션	2,000,000	2,000,000	500,000
IPSec VPN 터널 인터페이스	4,000	4,000	2,000
GlobalProtect(SSL VPN) 동시 사용자	10,000	10,000	5,000
SSL 암호 해독 세션	23,000	23,000	7,500
SSL 인바운드 인증서	300	300	25
가상 라우터	125	125	20
가상 시스템(base/max ²)	25/125	25/125	10/20
보안 영역	500	500	80
최대 정책 수	20,000	20,000	10,000

¹ 성능 및 용량은 PAN-OS 5.0을 사용하여 이상적인 테스트 조건에서 측정됩니다.

² 가상 시스템을 기본 수량에 추가하려면 별도로 라이선스를 구입해야 합니다.

PA-4000 시리즈 차세대 방화벽 기능에 대한 자세한 설명은 www.paloaltonetworks.com/literature 를 참조하십시오.

하드웨어 사양

I/O

- PA-4060: (4) 10기가비트 XFP, (4)기가비트 SFP
- PA-4050, PA-4020: (16) 10/100/1000, (8)기가비트 SFP

관리 I/O

- (2) 10/100/1000 HA 포트, (1) 10/100/1000 대역 외 관리, (1) DB9 콘솔 포트

저장소 용량

- 160GB HDD

전원 공급 장치(평균/최대 전력 소모)

- Redundant 400W AC(175W/200W)

시간당 최대 BTU

- 682

입력 전압(입력 주파수)

- 100-240VAC (50-60Hz)

최대 전류 소모

- 2.5A@100VAC

MEAN TIME BETWEEN FAILURE (MTBF)

- 7.18년

최대 돌입 전류

- 50A@230VAC; 30A@115VAC

탑재 가능 랙(크기)

- 2U, 19" 표준 랙(3.5"H x 16.5"D x 17.5"W)

무게(독립 실행형 장치/출하 당시)

- 33lbs/40lbs

안전

- UL, CUL, CB

EMI

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

인증

- FIPS 140 레벨 2, 일반 기준 EAL2, ICESA, UCAPL

환경

- 작동 온도: 32~122F, 0~50C
- 비작동 온도: -4~158F, -20~70C

네트워킹

인터페이스 모드:

- L2, L3, Tap, Virtual wire (transparent mode)

라우팅

- 모드: OSPF, RIP, BGP, Static
- 포워딩 테이블 크기(장치당/VR당 엔트리): 20,000/20,000(PA-4060, PA-4050), 10,000/10,000(PA-4020)
- 정책 기반 포워딩
- PPPoE(Point-to-Point Protocol over Ethernet)
- Jumbo 프레임: 9,210바이트 최대 프레임 크기
- 멀티캐스트: PIM-SM, PIM-SSM, IGMP v1, v2 및 v3

고가용성

- 모드: 액티브/액티브, 액티브/패시브
- 오류 감지: 경로 모니터링, 인터페이스 모니터링

주소 할당

- 장치의 주소 할당: DHCP 클라이언트/PPPoE/정적
- 사용자의 주소 할당: DHCP 서버/DHCP 릴레이/정적

IPv6

- L2, L3, tap, virtual wire (transparent mode)
- 기능: App-ID, User-ID, Content-ID, WildFire 및 SSL 암호 해독

VLANS

- 장치당/인터페이스당 802.1q VLAN 태그: 4,094/4,094
- 최대 인터페이스: 4,096(PA-4060, PA-4050), 2,048(PA-4020)
- Aggregate interfaces (802.3ad)

NAT/PAT

- 최대 NAT 룰: 4,000(PA-4060, PA-4050), 1,000(PA-4020)
- 최대 NAT 룰(DIPP): 250(PA-4060, PA-4050), 200(PA-4020)
- 동적 IP 및 포트 풀: 254
- 동적 IP 풀: 16,234
- NAT 모드: 1:1 NAT, n:n NAT, m:n NAT
- DIPP 초과 구독(소스 포트 및 IP당 고유 대상 IP): 8(PA-4060, PA-4050), 4(PA-4020)
- NAT64

가상 와이어

- 최대 가상 와이어: 12
- 가상 와이어에 매핑되는 인터페이스 유형: 물리적 및 서버 인터페이스

L2 전달

- ARP 테이블 크기/장치: 20,000(PA-4060, PA-4050), 10,000(PA-4020)
- MAC 테이블 크기/장치: 20,000(PA-4060, PA-4050), 10,000(PA-4020)
- IPv6 인접 테이블 크기: 5,000(PA-4060, PA-4050), 2,000(PA-4020)

보안

방화벽

- 애플리케이션, 사용자 및 콘텐츠에 대한 정책 기반 제어
- 조각 난 패킷 보호
- 사전 검사 보호
- 서비스 거부(DoS)/분산 서비스 거부(DDoS) 보호
- 암호 해독: SSL(인바운드 및 아웃바운드), SSH

WILDFIRE

- 100개 이상의 악의적인 행위에 대해 목표가 설정된 알 수 없는 파일을 식별하고 분석합니다.
- 시그니처 업데이트를 통해 새로 탐지된 맬웨어에 대한 보호를 생성하고 자동으로 제공합니다.
- WildFire 시그니처 업데이트를 통합된 로깅/보고를 1시간 이내에 전달하고 일일 최대 100개의 샘플과 일일 파일 해시에 의한 최대 250개 보고서 쿼리를 프로그램 방식 제출을 위해 WildFire API에 액세스합니다(구독 필수).

파일 및 데이터 필터링

- 파일 전송: 60개 이상의 고유한 파일 유형에 대한 양방향 제어
- 데이터 전송: CC# 및 SSN의 인증되지 않은 전송에 대한 양방향 제어
- 드라이브 바이(Drive-by) 다운로드 보호

사용자 통합(USER-ID)

- Microsoft Active Directory, Novell eDirectory, Sun One 및 기타 LDAP 기반 디렉터리
- Microsoft Windows Server 2003/2008/2008r2, Microsoft Exchange Server 2003/2007/2010
- Microsoft Terminal Services, Citrix XenApp
- 비 표준 사용자 리포지토리와 통합을 용이하게 해주는 XML API

IPSEC VPN(사이트 간)

- 키 교환: 수동 키, IKE v1
- 암호화: 3DES, AES(128비트, 192비트, 256비트)
- 인증: MD5, SHA-1, SHA-256, SHA-384, SHA-512
- 동적 VPN 터널 생성(GlobalProtect)

위협 예방(구독 필수)

- 애플리케이션, 운영 체제 취약성 공격 방지
- 바이러스(HTML, Javascript, PDF 및 압축 파일에 내장된 바이러스 포함), 스파이웨어, 웜에 대한 스트림 기반 방지

URL 필터링(구독 필수)

- 미리 정의된 사용자 정의 URL 범주
- 가장 최근에 액세스한 URL의 장치 캐시
- 보안 정책을 위한 일치 기준의 일련으로 사용되는 URL 범주
- 시간 정보 찾아보기

서비스 품질(QoS)

- 애플리케이션, 사용자, 소스, 대상, 인터페이스, IPsec VPN 터널 등의 기준별 정책 기반 트래픽 셰이핑
- 최대 및 우선 순위 대역폭 매개변수를 보장하는 8개의 트래픽 등급
- 실시간 대역폭 모니터
- 정책 DiffServ 표시당
- QoS에 지원되는 물리적 인터페이스: 12

SSL VPN/원격 액세스(GLOBALPROTECT)

- GlobalProtect 게이트웨이
- GlobalProtect 포털
- 전송: 대체 SSL이 있는 IPsec
- 인증: LDAP, SecurID 또는 로컬 DB
- 클라이언트 OS: Mac OS X 10.6, 10.7(32/64비트), 10.8(32/64비트), Windows XP, Windows Vista(32/64비트), Windows 7(32/64비트)
- 타사 클라이언트 지원: Apple iOS, Android 4.0 이상, Linux용 VPNC IPsec

관리, 보고, 가시성 도구

- 통합 웹 인터페이스, CLI 또는 중앙 관리(Panorama)
- 다국어 사용자 인터페이스
- Syslog 및 SNMP v2/v3
- XML 기반 REST API
- 애플리케이션, URL 범주, 위협 및 데이터(ACC)의 그래픽 요약
- 트래픽, 위협, WildFire, URL 및 데이터 필터링 로그 보기, 필터링 및 내보내기
- 완전 사용자 정의 가능 보고

PA-4000 시리즈 차세대 방화벽 기능에 대한 자세한 설명은 www.paloaltonetworks.com/literature를 참조하십시오.