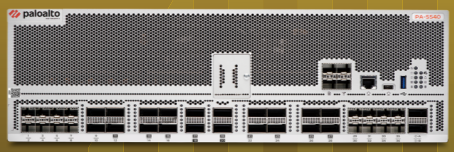
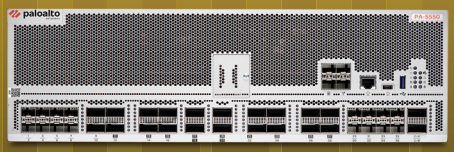
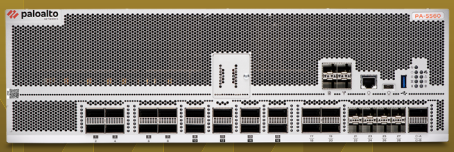
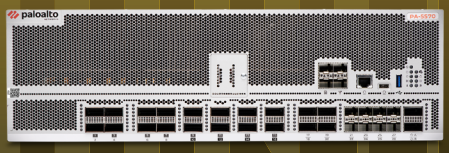
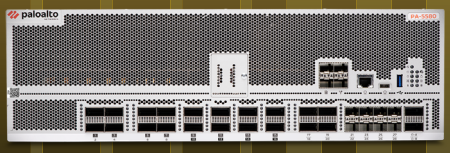
paloalto NETWORKS | STRATA™


PA-5540


PA-5550


PA-5560


PA-5570


PA-5580

PA-5500 시리즈

PA-5580, PA-5570, PA-5560, PA-5550, PA-5540으로 구성된 Palo Alto Networks PA-5500 시리즈 퀀텀 최적화 차세대 방화벽(NGFW)은 고속 데이터센터, 인터넷 게이트웨이 및 서비스 제공업체 구축에 이상적입니다. 이 시리즈는 포스트 양자 암호화 트래픽을 포함한 모든 트래픽에 대한 가시성을 확보하고 보호합니다.

PA-5500 시리즈의 운영 체제는 PAN-OS®로, 모든 Palo Alto Networks NGFW를 실행하는 소프트웨어와 동일합니다. PAN-OS는 기본적으로 애플리케이션, 위협, 콘텐츠를 포함한 모든 트래픽을 분류한 다음 위치나 디바이스 유형에 관계없이 해당 트래픽을 사용자와 연결합니다. 기업을 운영하는 애플리케이션, 콘텐츠 및 사용자는 보안 정책의 기반이 되며, 이를 통해 보안 태세가 강화되고 사고 대응 시간이 단축됩니다. PAN-OS는 방화벽 핵심에 머신 러닝(ML)을 내장하여 파일 기반 공격에 대한 인라인 시그니처리스 공격 방지 기능을 제공하는 동시에 이전에는 발견되지 않았던 피싱 시도를 식별하여 즉시 차단합니다.

하이라이트

- 세계 최초의 양자 최적화된 NGFW.
- 데이터센터를 위한 3랙 유닛 설계에서 높은 처리량을 위해 FE-400 ASIC으로 제작되었습니다.
- 실시간으로 위협을 분석하고 예방하는 획기적인 AI 기반 엔진인 Precision AI® 기반
- 예측 가능한 성능을 제공하기 위해 단일 패스 아키텍처로 구축되었습니다.
- 5G 식별자 기반 가시성 및 시행 기능을 갖춘 Palo Alto Networks 5G 네이티브 보안을 제공합니다.
- NGFW 클러스터링을 통해 높은 가용성을 제공합니다.
- 네트워크 보안을 위한 업계 최초의 AI 기반 통합 관리 및 운영 솔루션인 Strata™ Cloud Manager로 관리
- 2025년 Gartner® Magic Quadrant™ 네트워크 방화벽 리더
- Forrester Wave™의 리더: 엔터프라이즈 방화벽 솔루션, 2024년 4분기.

포스트 양자 암호화 최적화

PA-5500 시리즈는 PAN-OS 12.1을 사용하여 하드웨어 및 소프트웨어에서 양자 안전 보안을 구현하는 데 도움이 되는 포스트 양자 암호화 지원 디바이스입니다. PA-5500 시리즈 NGFW 지원:

- 방화벽에 대한 관리 액세스를 위한 PQC SSL/TLS 복호화, PQC VPN 사이트 간, PQC SSL/TLS 암호 변환 프록시 및 PQC SSL/TLS 서비스 프로필을 위한 포스트 양자 암호화(PQC)입니다.
- ML-KEM, ML-DSA, SLH-DSA와 같은 NIST 표준을 포함한 PQC 알고리즘과 Classic McEliece, BIKE, HQC, Frodo-KEM, NTRU-Prime과 같은 실험적 PQC입니다.
- 향후 양자 컴퓨팅 기능을 추가할 수 있는 새롭게 도입된 PCIe 슬롯입니다.

암호화된 트래픽에 숨겨진 악성 활동 방지

PA-5500 시리즈 NGFW는 다음과 같은 기능을 제공합니다.

- SSL/TLS 암호화 트래픽(인바운드 및 아웃바운드 모두), SSLv3, TLSv1.1, TLSv1.2, TLSv1.3을 사용하는 트래픽, 그리고 SMTP, WebSocket, gRPC, HTTP/1.0, HTTP/1.1, HTTP/2와 같은 애플리케이션 프로토콜에 대한 정책을 검사하고 적용합니다.
- 기존 키 교환 알고리즘인 RSA, ECDHE, DHE와 포스트 양자 키 교환 표준인 ML-KEM, HQC, 그리고 실험적 BIKE와 Frodo-KEM을 사용하여 SSL/TLS 세션을 해독하고 검사합니다.
- 암호화된 트래픽 양, SSL/TLS 버전, 암호문 등 TLS 트래픽에 대한 측정 항목을 수집합니다.
- 복호화가 필요 없이 RSA, ECDHE, DHE와 같은 클래식 키 교환과 ML-KEM 및 HQC와 같은 포스트 양자 키 교환을 지원하여 방화벽을 통과하는 모든 SSL/TLS 세션의 암호화 정보에 대한 가시성을 높입니다.
- 위험을 완화하기 위해 기존 TLS 프로토콜, 안전하지 않고 더 이상 사용되지 않는 암호, 잘못 구성된 인증서(인증서 일반 이름(CN)에 대한 서버 이름 표시기(SNI) 불일치 포함) 사용에 대한 제어를 활성화합니다.
- 간편한 복호화 배포를 용이하게 하고 향상된 내장 로그를 사용하여 클라이언트 측과 서버 측 세션에서 독립적으로 문제를 해결하여 누락된 중간 인증서나 고정된 인증서 등 원활한 문제 해결 환경을 제공합니다.
- 개인 정보 보호 및 규정 준수를 위해 URL 범주, 소스 및 대상 영역, 주소, 사용자, 사용자 그룹, 디바이스 및 포트를 기반으로 유연하게 복호화를 활성화하거나 비활성화할 수 있습니다.

복호화: 왜, 어디서, 어떻게 백서를 읽고 위협을 예방하고 비즈니스를 보호하기 위한 복호화 방법에 대해 알아보세요.

전체 7계층 검사를 통한 애플리케이션 식별 및 분류

App-ID™는 모든 포트의 모든 애플리케이션을 항상 완전한 7계층 검사로 식별하고 분류하며, 다음 기능을 지원합니다.

- 프로토콜 디코딩, 휴리스틱, 서명 매칭과 같은 고급 기술을 사용하여 포트, 프로토콜 또는 암호화 방법에 관계없이 네트워크 전체에서 애플리케이션을 정확하게 식별합니다. 선택 사항인 App-ID Cloud Engine(ACE) 서비스는 SaaS 애플리케이션에 대한 주문형 App-ID를 제공합니다.
- 다양한 애플리케이션과 관련된 위험과 가치에 대한 포괄적인 이해를 제공하여 네트워크 보안 정책에 대한 정보에 입각한 의사 결정을 내리는 데 도움이 됩니다.

- 방화벽 수준에서 애플리케이션 식별 및 제어를 중앙화하여 특정 애플리케이션에 맞는 보안 정책을 효과적으로 시행할 수 있습니다.
- 일반적으로 기존 보안 조치를 우회하는 회피적 또는 맞춤형 애플리케이션을 식별하고 관리합니다.
- 최신 애플리케이션 동향과 전략에 맞춰 효율성을 유지하기 위해 애플리케이션 식별 정보를 지속적으로 업데이트합니다.
- 최첨단 AI 기술을 사용하여 AI 기반 애플리케이션을 식별하고 분류하는 데 있어 정확도를 높입니다. 이러한 기술을 사용하면 가장 진보되고 동적인 애플리케이션도 네트워크 내에서 정확하게 인식되고 적절하게 관리될 수 있습니다.

자세한 내용은 App-ID 기술 간략 설명서를 참조하세요.

사용자 보안 시행

PA-5500 시리즈 NGFW는 사용자의 활동에 따라 정책을 적용하는 동시에, 어떤 위치에서 어떤 디바이스를 사용하든 보안을 강화합니다. 여기에는 다음 기능이 포함됩니다.

- 사용자, 그룹 및 IP 주소를 기반으로 가시성, 보안 정책, 보고 및 포렌식을 활성화합니다.
- 사용자의 위치(사무실, 집, 여행 등) 및 디바이스에 관계없이 일관된 정책을 적용합니다. 이러한 디바이스에는 iOS 및 Android 모바일 디바이스, macOS, Windows 및 Linux 데스크톱과 노트북, Citrix 및 Microsoft VDI, 터미널 서버가 포함됩니다.
- IP 지리적 위치를 활용하여 지리적 위치에 따라 보안 정책을 자동으로 시행하면 공격 표면을 줄이고, 규정 준수 요구 사항을 충족하고, 특정 국가나 지역에서의 트래픽을 차단하여 애플리케이션 액세스를 제어할 수 있습니다.
- Cloud Identity Engine(ID 기반 보안을 위한 클라우드 기반 아키텍처)을 사용하면 위치와 사용자 ID가 저장된 위치(클라우드 및 온프레미스 디렉터리 또는 둘 다)에 관계없이 사용자를 지속적으로 인증하고 권한을 부여하여 신속하게 제로 트러스트 보안 태세로 전환할 수 있습니다.
- 온프레미스, SaaS 또는 하이브리드 여부에 관계없이 암호 없는 인증으로 모든 애플리케이션을 보호하세요.
- 방화벽에 클라우드 동적 사용자 그룹(CDUG)을 정의하여 사용자 디렉토리에 변경 사항을 적용할 때까지 기다리지 않고 위험 기반의 시간 제한 보안 조치를 취함으로써 의심스럽거나 악의적인 사용자를 제한하는 사용자 동작에 따라 동적 보안 조치를 제공합니다.
- 변경 없이 모든 애플리케이션에 대해 네트워크 계층에서 다중 요소 인증(MFA)을 활성화하여 기업 자격 증명이 타사 웹사이트로 유출되는 것과 도난당한 자격 증명이 재사용되는 것을 방지합니다.
- 무선 LAN 컨트롤러, VPN, 디렉토리 서버, 보안 정보 및 이벤트 관리(SIEM) 도구 등 사용자 정보를 처리하기 위해 광범위한 저장소와 쉽게 통합할 수 있습니다.
- 시간을 절약하고 인적 오류 가능성을 줄이는 자동화된 정책 권장 사항을 제공합니다.

자세한 내용은 Cloud Identity Engine 솔루션 간략 설명서를 참조하세요.

패킷 처리에 대한 고유한 접근 방식

PA-5500 시리즈 NGFW는 단일 패스 아키텍처를 사용하여 패킷을 처리합니다. 이 접근 방식을 사용하면 NGFW는 다음을 수행할 수 있습니다.

- 모든 위협과 콘텐츠에 대해 네트워킹, 정책 조회, 애플리케이션 및 디코딩, 시그니처 매칭을 한 번에 수행합니다. 이를 통해 하나의 보안 디바이스에서 여러 기능을 수행하는 데 필요한 처리 오버헤드가 크게 줄어듭니다.

- 스트림 기반의 균일한 서명 매칭을 사용하여 단일 패스에서 모든 서명에 대한 트래픽을 스캔하여 지연이 발생하지 않도록 합니다.
- 보안 구독이 활성화되면 일관되고 예측 가능한 성능을 생성합니다(표 1 참조).

Strata Cloud Manager를 통한 AI 기반 통합 관리 및 운영

Strata Cloud Manager를 사용하면 PA-5500 시리즈 NGFW를 관리할 수 있습니다. 다음과 같은 기능이 제공됩니다.

- **네트워크 보안 자산 전반에 대한 완벽한 가시성 확보:** 통합 인터페이스를 통해 모든 사용자, 애플리케이션, 디바이스 및 주의가 필요한 가장 중요한 위협을 포함한 전체 네트워크 보안 환경에 대한 실시간 종합 가시성을 확보합니다.
- 간**단하고 일관된 네트워크 보안 수명 주기 관리:** 일관성을 보장하고 운영 오버헤드를 줄이기 위해 SASE, 하드웨어 및 소프트웨어 방화벽, 모든 보안 서비스를 포함한 모든 시행 지점에서 구성 및 정책 관리를 관리합니다.
- 실**시간 보안 태세 강화:** AI 기반 분석을 활용하여 섀도 및 중복 정책, 과도한 권한이 부여되었거나 사용되지 않는 규칙과 같은 정책 이상 징후를 감지, 해결 및 최적화할 수 있습니다. 통합 모범 사례 권장 사항으로 보안 태세를 개선하고 업계 및 InfoSec 표준을 준수합니다.
- 네**트워크 중단을 능동적으로 해결하고 사용자 경험 향상:** 사용자 경험 문제, 용량 병목 현상, CVE 취약성, 서비스 연결 문제, 기타 130가지 카테고리의 문제 등 네트워크 상태 문제를 최대 90일 전에 예측, 진단, 해결하여 원활한 운영을 보장합니다.
- 손**끝에 있는 즉각적인 지식으로 빠르게 문제 해결:** 자연어 인터페이스를 갖춘 AI 기반 어시스턴트인 Strata Copilot™을 사용하면 보안 및 운영상의 문제가 확대되기 전에 빠르게 찾아내고 이해하며 해결할 수 있습니다. 또한 간소화된 사례 생성 기능으로 가장 필요할 때 신속하게 지원할 수 있습니다.

NGFW 클러스터링과 고가용성 요소의 결합

NGFW 클러스터링은 높은 중복성과 복원력을 갖춘 솔루션을 유지하면서 리소스 사용을 최적화하고 처리량을 늘립니다. 이 솔루션은 고가용성 네트워크에 대한 효율적인 수평적 확장을 가능하게 합니다.

자세한 내용은 NGFW 클러스터링으로 마이그레이션 백서를 참조하세요.

정밀 AI 기반 최고 수준의 클라우드 기반 보안 서비스

PA-5500 시리즈 NGFW는 클라우드 제공 보안 서비스(CDSS)를 통해 동급 최고의 보안을 제공합니다. CDSS의 핵심은 정밀 AI입니다. 기존의 반응형 도구와 달리 Precision AI는 사전 예방적 위협 탐지, 인라인 예방 및 자동화된 대응을 통해 방어력을 강화하여 가장 교묘하고 이전에 본 적이 없는 공격도 피해를 입히기 전에 차단합니다. 전 세계 70,000명 이상의 고객으로부터 얻은 위협 인텔리전스를 바탕으로, 당사의 클라우드 제공 서비스는 지속적으로 학습하고, 적응하며, 진화합니다. NGFW 및 SASE 플랫폼과 완벽하게 통합된 CDSS는 사용자나 데이터가 어디에 있든 웹, DNS, 이메일, 애플리케이션 등 전반에 걸쳐 통합된 보호 기능을 제공합니다.

하이브리드 작업을 탐색하든, 클라우드 전환을 도입하든, 정교한 적대 세력에 맞서 방어하든, Precision AI 기반의 CDSS는 앞서 나가는 데 필요한 가시성, 자동화 및 확신을 제공합니다.

고급 위협 방지

매일 최대 6억 7,300만 개의 새로운 세션을 분석하고 제로데이 익스플로잇, 멀웨어, 명령 및 제어(C2) 트래픽, 회피 기술 등 282억 개의 위협을 실시간으로 사전에 차단하여 전례 없는 규모의 최첨단 보안을 제공합니다.

고급 WildFire

업계에서 가장 강력한 멀웨어 방지 엔진을 통해 매일 최대 450,000건의 새로운 위협을 사전에 차단하세요. Advanced WildFire®는 제로데이 멀웨어, 랜섬웨어, 원격 액세스 트로이 목마(RAT), 무기화된 문서 및 기타 회피적 공격 기법을 포함한 광범위한 지능형 위협을 조직에 영향을 미치기 전에 식별하고 차단합니다.

고급 URL 필터링

매일 최대 1억 5,100만 건의 위협을 직접 차단하고, 매일 38억 개의 새로운 URL을 분석하여 웹 액세스를 보호하세요. 고급 URL 필터링은 피싱, 멀웨어, 랜섬웨어, C2 통신 및 회피적인 웹 기반 공격으로부터 보호합니다.

고급 DNS 보안

Advanced DNS Security는 DNS 하이재킹, 도메인 생성 알고리즘(DGA), DNS 터널링, C2 콜백을 포함한 정교한 DNS 요청 및 응답 기반 위협을 즉시 차단하는 실시간 보호 기능을 제공합니다. 매일 11억 개 이상의 새로운 도메인을 분석하고 최대 770만 개의 새로운 악성 도메인을 식별하여 20억 개 이상의 위협을 인라인으로 차단합니다. 이 강력한 1차 방어선은 네트워크 외부나 내부에서 발생하는 모든 위협을 DNS 계층에서 식별하고 차단합니다.

디바이스 보안

제조, 소매, 의료, 첨단 기술, 일반 기업 등 산업에 맞춤형 솔루션으로 모든 연결된 디바이스를 보호하고, 48시간 이내에 90%의 디바이스 발견률을 달성하세요. 우선순위가 지정된 취약성 및 위험 평가를 제공합니다. 또한, 이상 징후를 식별하고, 권한이 가장 낮은 액세스 제어 보안 정책 권장 사항을 얻고, 모든 취약점을 단일 NetSec 플랫폼에서 가상으로 패치합니다.

SaaS 보안

75,000개 이상의 SaaS 앱에 대한 가시성과 150개 이상의 SaaS 앱에 대한 데이터 유출 방지(DLP) 제어를 통해 모든 SaaS 소비를 파악하고 제어합니다. 117개 이상의 SaaS 앱에 대한 포스처 관리와 39개 앱에 대한 SaaS 인라인 테넌시 제어를 통해 SaaS의 잘못된 구성을 방지합니다.

AI Access Security

GenAI 앱에 대한 실시간 가시성, 사용자 액세스 제어, 데이터 보호 및 지속적인 위험 모니터링을 통해 GenAI를 안전하게 사용할 수 있도록 지원합니다. AI Access Security™는 2,500개가 넘는 GenAI 앱으로 구성된 업계 최고 수준의 카탈로그를 제공하며, 여기에는 위험을 정확하게 식별하고 완화하는 데 필요한 15개 이상의 GenAI 특정 애플리케이션 속성이 포함됩니다. 여기에는 13개 이상의 GenAI 앱에 대한 포스처 관리와 11개 앱에 대한 SaaS 인라인 테넌시 제어가 포함됩니다.

고급 SD-WAN

기존 방화벽에 통합 보안 기능을 활성화하여 SD-WAN을 손쉽게 도입하세요. SD-WAN 경로 측정 및 애플리케이션 조정 기능을 사용하여 애플리케이션을 가장 성능이 좋은 경로로 지능적으로 조정함으로써 탁월한 최종 사용자 경험을 얻고 SLA를 보장하세요.

표 1. PA-5500 시리즈 양자 최적화 NGFW의 성능 및 용량					
	PA-5540	PA-5550	PA-5560	PA-5570	PA-5580
방화벽 처리량(appmix)*	150Gbps	175Gbps	240Gbps	300Gbps	375Gbps
위협 방지 처리량(appmix)†	90Gbps	120Gbps	180Gbps	240Gbps	300Gbps
IPsec VPN 처리량‡	80Gbps	100Gbps	125Gbps	150Gbps	170Gbps
최대 동시 세션§	39M	49M	74M	89M	99M
초당 새로운 세션‖	1.33M	1.67M	2.5M	3M	3.3M
가상 시스템(기본/최대)#	25/225	25/225	25/225	25/225	25/225

참고: 결과는 PAN-OS 12.1에서 측정되었습니다.

* 방화벽 처리량은 AppMix 트랜잭션을 사용하여 App-ID와 로깅을 활성화하여 측정됩니다.

† 위협 방지 처리량은 AppMix 트랜잭션을 사용하여 App-ID, IPS, 안티바이러스, 안티스파이웨어, WildFire, 파일 차단 및 로깅을 활성화하여 측정됩니다.

‡ IPsec VPN 처리량은 64KB HTTP 트랜잭션과 로깅이 활성화된 상태로 측정됩니다.

§ 최대 동시 세션은 HTTP 트랜잭션을 사용하여 측정됩니다.

‖ 초당 새로운 세션은 1바이트 HTTP 트랜잭션을 사용하여 애플리케이션 오버라이드로 측정됩니다.

기본 수량 이상의 가상 시스템을 추가하려면 별도로 라이선스를 구매해야 합니다. NGFW 클러스터 A/A는 최대 25개의 가상 시스템을 지원합니다.

표 2. PA-5500 시리즈 네트워킹 기능
인터페이스 모드
L2 모드(MC-LAG 집계 인터페이스에서는 사용할 수 없음), L3 모드, 탭 및 가상 와이어(투명 모드).
라우팅
고급 라우팅 엔진은 지원되는 유일한 라우팅 엔진입니다.
서버 끊김 없이 재시작, RIP 및 정적 라우팅을 갖춘 OSPFv2/v3 및 MP-BGP.
정책 기반 포워딩 정책.
IPv4와 IPv6 모두에 대한 동적 주소 할당을 위해 PPPoE(Point-to-Point Protocol over Ethernet) 및 DHCP 클라이언트가 지원됩니다.
DHCPv4 서버 및 DHCPv4 릴레이.
멀티캐스트: PIM-SM, PIM-SSM, IGMPv2 및 v3.
양방향 전달 감지(BFD) 및 멀티홉 BFD.
고급 SD-WAN
경로 품질 측정(지터, 패킷 손실, 지연 시간)
대역폭 모니터링.
키 교환: 수동 키, IKEv1* 및 IKEv2(사전 공유 키 및 인증서 기반 인증).
포스트 양자 PPK.
SD-WAN 오버레이를 통한 다중 VR 및 LR 지원.
Prisma® Access Hub(하이브리드 SASE).
자율적 디지털 경험 관리(ADEM)로 얻을 수 있는 이점
IPv6
L2, L3, 탭 및 가상 와이어 모드(투명 모드)에서 IPv6 검사를 수행합니다.
듀얼 스택 및 IPv6 전용 네트워크 지원.
특징: IPv6 지리적 위치 지정, OSPFv3, MP-BGP, NAT64 및 NPTv6.
접두사 위임(PD)을 지원하는 DHCPv6 클라이언트입니다. 상태 비저장 주소 자동 구성(SLAAC) 서버 지원.
IPsec VPN
키 교환: 수동 키, IKEv1* 및 IKEv2(사전 공유 키 및 인증서 기반 인증).
암호화: 3des, AES(128비트, 192비트, 256비트).
인증: MD5, SHA-1, SHA-256, SHA-384 및 SHA-512.
GlobalProtect® 대규모 VPN으로 구성과 관리가 간소화되었습니다.†
GlobalProtect 게이트웨이와 포털을 사용하여 IPsec 및 SSL VPN 터널을 통한 보안 액세스를 확보하세요.†

표 2. PA-5500 시리즈 네트워킹 기능(계속)
VLAN
디바이스당 또는 인터페이스당 802.1Q VLAN 태그: 4,094/4,094.
집계 인터페이스(802.3ad) 및 LACP.
네트워크 주소 변환
NAT 모드(IPv4): 고정 IP, 동적 IP, 동적 IP 및 포트(포트 주소 변환).
NAT64와 NPTv6.
추가 NAT 기능: 동적 IP 예약, 조정 가능한 동적 IP 및 포트 오버서브스크립션.
고가용성 및 클러스터링
활성/활성을 갖춘 NGFW 클러스터링. HA 활성/수동.‡ NGFW 클러스터링은 단일 제어 평면을 갖춘 듀얼 활성 데이터 평면을 유지하고 MC-LAG(두 시스템의 멤버가 있는 집계 이더넷 인터페이스)를 지원합니다.
모바일 네트워크 인프라§
5G 보안.

*NGFW 클러스터링에서는 지원되지 않습니다.

† GlobalProtect 라이센스가 필요합니다.

‡ 추후 출시됩니다.

§ 자세한 내용은 5G용 ML 기반 NGFW 데이터시트를 참조하세요 .

표 3. PA-5500 시리즈 하드웨어 사양
I/O
PA-5540/PA-5550: 10G/25G SFP28(16), 40G/100G QSFP28(16), 100G/400G QSFP-DD(4) PA-5560/PA-5570/PA-5580: 10G/25G SFP28(8), 40G/100G QSFP28(12), 100G/400G QSFP-DD(8)
관리 I/O
대역 외 관리: 1G/10G SFP+(2) 콘솔: RJ-45 콘솔 포트(1) 콘솔: USB-C 부트스트랩: USB 3.2 Gen1 타입 A HSCI: 100G/400G QSFP-DD(2) 로그: 10G SFP+ (2)
저장 용량
시스템 및 로그 저장을 위한 옵션 3.84TB RAID1 SSD 쌍이 콜드 스왑으로 지원됩니다.
전원 공급 장치(평균/최대 전력 소비)
2,100 W/3,100 W
시간당 최대 BTU
1638
전원 공급 장치
220V 및 DC용 2+2 중복 110V용 3+1 중복
입력 전압
AC: 100~240VAC(50~60Hz) DC: -40VDC ~ -60VDC
전원 공급 장치 출력
AC: 220V의 경우 2,700W/전원 공급 장치 또는 110V의 경우 1,200W/전원 공급 장치 DC: 2,200W/전원 공급 장치
최대 전류 소비량
AC: 20.3 A @ 110 VAC와 9.3 A @ 240 VAC DC: 43.7 A @ 54 VDC

표 3. PA-5500 시리즈 하드웨어 사양(계속)
최대 돌입 전류
AC: 50 A @ 230 VAC와 50 A @ 120 VAC DC: 25 A @ 54 VDC
평균 고장 간격(MTBF)
PA-5540/PA-5550: 8.1년 PA-5560/PA-5570/PA-5580: 6.3년
랙 마운트 치수
전원 공급 장치가 삽입된 3U, 19인치 표준 랙(높이 5.2인치 x 깊이 29.8인치 x 너비 17.3인치)
무게(독립형 디바이스/배송 시)
70파운드/116파운드(액세서리 키트, 랙 키트, 포장재, 팔레트 포함).
안전
cTUVus, CB
EMI
FCC 등급 A, CE 등급 A, VCCI 등급 A
인증
규정 준수 페이지를 참조하세요.
환경
작동 온도: 32°F~122°F, 0°C~50°C **비작동 온도:** -4°F~158°F, -20°C~70°C **습도 내성:** 10%~90% **최대 고도:** 10,000피트/3,048m **공기 흐름:** 앞에서 뒤로(포트 쪽에서 전원 공급 쪽까지)

표 2. PA-5500 시리즈 주문 정보	
부품 번호	**디테일**
PAN-PA-5540-AC PAN-PA-5550-AC PAN-PA-5560-AC PAN-PA-5570-AC PAN-PA-5580-AC	포함: 4x PAN-PA-5500-PWR-2700-AC 5x PAN-PA-FAN-2RU-A 1x PAN-PA-5500-ACC-A 액세서리 키트 1x PAN-PA-3RU-RACK-A 2x PAN-SFP-CG 1x PAN-PA-5500-SSD-3.84TB-PAIR
PAN-PA-5540-DC PAN-PA-5550-DC PAN-PA-5560-DC PAN-PA-5570-DC PAN-PA-5580-DC	포함: 4x PAN-PA-5500-PWR-2000-DC 5x PAN-PA-FAN-2RU-A 1x PAN-PA-5500-ACC-B 액세서리 키트 1x PAN-PA-3RU-RACK-A 2x PAN-SFP-CG 1x PAN-PA-5500-SSD-3.84TB-PAIR
PAN-PA-5500-SSD-3.84TB-PAIR	예비 교체 드라이브.
PAN-PA-5500-ACC-A	예비 액세서리 키트에는 4개의 PAN-PWR-C19-US-120V 케이블, 1개의 USB 케이블, 1개의 Cat6 케이블이 포함되어 있습니다.
PAN-PA-5500-ACC-B	예비 액세서리 키트에는 4개의 PAN-PWR-DC-CBL-C 케이블, 1개의 USB 케이블, 1개의 Cat6 케이블이 포함되어 있습니다.

표 4에는 PA-5500 시리즈의 주요 SKU가 나열되어 있습니다. LAB 번들, 예비 부품, 소프트웨어 구독 및 지원을 포함한 전체 SKU 목록에 대한 자세한 내용은 Palo Alto Networks 계정 팀과 NextWave 채널 파트너에게 문의하세요.

3000 Tannery Way
Santa Clara, CA 95054

대표 전화: +1.408.753.4000
판매 문의: +1.866.320.4788
지원 문의: +1.866.898.9087

www.paloaltonetworks.com

strata_ds_pa-5500-series_090425