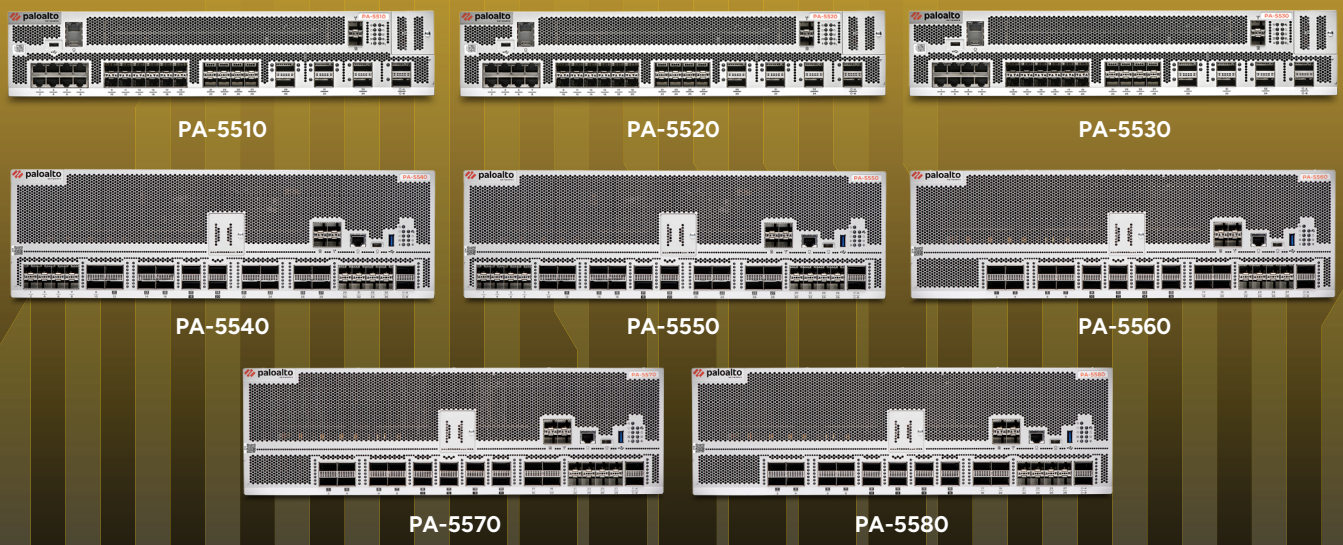


PA-5500 Series Quantum-Optimized NGFWs

Palo Alto Networks PA-5500 Series Quantum-Optimized NGFWs comprise the PA-5580, PA-5570, PA-5560, PA-5550, PA-5540, PA-5530, PA-5520, and PA-5510 models. This scalable series targets enterprise and hyperscale data centers, high-speed internet gateways, and service provider deployments. It provides complete visibility into and secures all traffic across your network, including post-quantum encrypted traffic.

PAN-OS®, the operating system of the PA-5500 Series, runs all Palo Alto Networks NGFWs. PAN-OS natively classifies all traffic—including applications, threats, and content—and then ties that traffic to the user regardless of location or device type. This traffic serves as the basis of your security policies, resulting in an improved security posture and reduced incident response time. Our OS embeds AI in the firewall core to provide inline signatureless attack prevention for file-based attacks while identifying and immediately stopping never-before-seen phishing attempts.

Post-Quantum Cryptography Optimizations

PA-5500 Series is a post-quantum cryptography-optimized device that provides quantum-safe security in hardware and software. PA-5500 Series NGFWs support:

- **Post-quantum cryptography (PQC)** for PQC TLS decryption, PQC VPN site-to-site, PQC-Classical TLS Cipher Translation Proxy, and PQC TLS Service Profile for Management Access to the firewall. Also, PQC GlobalProtect® for end-user remote access VPN.
- **PQC algorithms**, including NIST standards, like ML-KEM, ML-DSA, and SLH-DSA, as well as emerging and experimental PQCs like Classic McEliece, BIKE, HQC, Frodo-KEM, and NTRU-Prime. Support also for hybrid post-quantum classical and pure PQC algorithms.
- **An additional PCIe slot** for future post-quantum capabilities.

For more information, see Support for Post-Quantum Features in TechDocs.

Prevention of Malicious Activity Concealed in Encrypted Traffic

PA-5500 Series NGFWs provide the ability to:

- **Inspect and apply policies** to SSL/TLS-encrypted traffic (both inbound and outbound), traffic that uses SSLv3, TLSv1.1, TLSv1.2, and TLSv1.3, as well as application protocols SMTP, WebSocket, gRPC, HTTP/1.0, HTTP/1.1, HTTP/2, and QUIC/HTTP3.
- **Decrypt and inspect SSL/TLS sessions** with the classical key exchange algorithms RSA, ECDHE, DHE, and post-quantum key exchange standards ML-KEM, HQC, as well as experimental BIKE and Frodo-KEM.
- **Enable or disable decryption flexibly**—based on URL category, source and destination zone, address, user, user group, device, and port—for privacy and regulatory compliance purposes.

Read the *Decryption: Why, Where and How* whitepaper to learn about decryption to prevent threats and secure your business.

Highlights

- **The world's first quantum-optimized NGFW:** Engineered to secure post-quantum encrypted traffic and protect long-life data against future decryption threats.
- **Built with FE400 and FE100X ASICs:** Custom silicon hardware delivers consistent high throughput, massive session scale, and ultra-low latency across the entire model lineup.
- **Powered by Precision AI®:** A groundbreaking AI-driven engine that analyzes, classifies, and prevents zero-day and evasive threats inline and in real time.
- **Built with a single-pass architecture:** Conducts networking, policy enforcement, decryption, and threat inspection in a single pass to deliver predictable performance under heavy loads.
- **Scalable deployment flexibility:** Offers a broad hardware portfolio spanning midtier enterprise perimeters (PA-5510 to PA-5530) to hyperscale data centers (PA-5540 to PA-5580).
- **Delivers Palo Alto Networks 5G-Native Security:** Features 5G identifier-based visibility, traffic correlation, and security enforcement capabilities.
- **Offers high availability with NGFW clustering:** Provides active/active clustering and active/passive HA to ensure resilient, uninterrupted NGFW clustering will be offered.
- **Managed with Strata™ Cloud Manager:** The industry's first AI-powered unified management and operations solution for end-to-end network security.
- **Leader in the 2025 Gartner® Magic Quadrant™** for Hybrid Mesh Firewalls.
- **Leader in The Forrester Wave:** Enterprise Firewall Solutions, Q4 2024.

Application Identification and Categorization with Full Layer 7 Inspection

App-ID™ identifies and categorizes all applications, on all ports, all the time, with full Layer 7 inspection, supporting the following capabilities:

- Uses advanced techniques, such as protocol decoding, heuristics, and signature matching, to accurately identify applications across the network, regardless of the port, protocol, or encryption methods used. The optional App-ID Cloud Engine (ACE) service provides on-demand App-IDs for SaaS applications.
- Allows for the effective enforcement of security policies tailored to specific applications by centralizing the identification and control of applications at the firewall level.
- Uses cutting-edge AI techniques to enhance precision in identifying and categorizing AI-powered applications. These techniques ensure that the most advanced and dynamic applications are accurately recognized and appropriately managed within the network.

For more information, see the *App-ID* tech brief.

User Security Enforcement

PA-5500 Series NGFWs enforce security for users at any location, on any device, while adapting policies based on their activity. They include the ability to:

- **Unify identity and policy enforcement:** Bridge on-premises and cloud identity stores to enforce consistent user-based policies everywhere via the Cloud Identity Engine, and block malicious traffic sources automatically by using IP geolocation.
- **Automate dynamic risk control:** Apply dynamic security actions based on user behavior and risk scores using Cloud Dynamic User Groups (CDUGs)—without depending on directory updates. Also, leverage automated policy recommendations to save time and reduce human error when restricting suspicious activity.
- **Secure credentials:** Prevent credential theft and abuse by enforcing multifactor authentication (MFA) at the network layer for any application, including legacy and nonweb apps, without requiring application changes.

For more information, see the *Cloud Identity Engine* solution brief.

Single-Pass Architecture

PA-5500 Series NGFWs process packets by using a single-pass architecture, enabling the NGFWs to:

- Perform networking, policy lookup, application decoding, and signature matching—for all threats and content—in a single pass. This approach significantly reduces the amount of processing overhead required to perform multiple functions in one security device.
- Avoid introducing latency by scanning traffic for all signatures in a single pass, using stream-based, uniform signature matching.
- Produce consistent and predictable performance when security subscriptions are enabled.

For more information, see the *Single-Pass Architecture* whitepaper.

AI-Powered Unified Management and Operations with Strata Cloud Manager

Manage your PA-5500 Series NGFWs with Strata Cloud Manager, which enables you to:

- **Gain complete visibility across your network security estate:** Achieve real-time, comprehensive visibility of your entire network security landscape, including all users, applications, devices, and the most critical threats that need attention through a unified interface.
- **Enable simple and consistent network security lifecycle management:** Manage configuration and policy management across all enforcement points, including SASE, hardware and software firewalls, as well as all security services to ensure consistency and reduce operational overhead.
- **Strengthen security posture in real time:** Use AI-powered analysis to detect, resolve, and optimize policy anomalies like shadow and redundant policies and overly permissive or unused rules. Improve your security posture with integrated best practice recommendations and maintain compliance with industry and InfoSec standards.

For more information, see the *Strata Cloud Manager* datasheet.

Combined NGFW Clustering and High Availability Elements

NGFW clustering optimizes resource usage and increases throughput while maintaining a highly redundant and resilient solution. This solution enables efficient horizontal scaling for highly available networks.

For more information, see the *Migrating to NGFW Clustering* whitepaper.

Best-in-Class Cloud-Delivered Security Services Powered by Precision AI

PA-5500 Series NGFWs provide best-in-class security with Cloud-Delivered Security Services (CDSS). Unlike traditional reactive tools, Precision AI at the heart of CDSS empowers your defenses with proactive threat detection, inline prevention, and automated response—stopping the most evasive, never-before-seen attacks before they cause damage. Backed by threat intelligence from our global customer base, our cloud-delivered services continuously learn, adapt, and evolve. Integrated seamlessly with our NGFW and SASE platforms, CDSS delivers unified protection across applications, DNS, email, IP infrastructure, web, and more—no matter where your users or data reside.

Whether you're navigating hybrid work, embracing cloud transformation, or defending against sophisticated adversaries, CDSS powered by Precision AI gives you the visibility, protection, and confidence to stay ahead.

Advanced Threat Prevention

Advanced Threat Prevention is the first intrusion prevention system (IPS) that stops zero-day command-and-control (C2) attacks and unknown exploits inline. In addition to traditional IPS capabilities, it delivers industry-leading protection against known and unknown threats.

For more information, see the *Advanced Threat Prevention* datasheet.

Advanced WildFire

Advanced WildFire® is the industry's largest cloud-based malware prevention engine. It protects organizations from highly evasive threats by using patented ML detection engines, enabling automated protections across networks, cloud, and customer application endpoints.

For more information, see the *Advanced WildFire* datasheet.

Advanced URL Filtering

Advanced URL Filtering analyzes URL strings and web content in real time and classifies them into benign or malicious categories, which teams can build into NGFW policies to control web traffic. It protects against phishing, malware, ransomware, C2 communications, and evasive web-based attacks.

For more information, see the *Advanced URL Filtering* datasheet.

Advanced DNS Security

Advanced DNS Security delivers real-time protection that instantly blocks sophisticated DNS requests and response-based threats—including DNS hijacking, domain generation algorithms (DGA), DNS tunneling, and C2 callbacks. It uses inline, AI-powered detection models to analyze every DNS request and response in real time. These models enable precise identification of never-before-seen malicious domains, DNS tunneling, C2 activity, and network-level DNS hijacking. This powerful first line of defense identifies and stops threats at the DNS layer—whether they originate outside or inside the network.

For more information, see the *Advanced DNS Security* datasheet.

Advanced IP Defense

Advanced IP Defense combines real-time IP intelligence with direct-to-IP detection to stop threats that bypass traditional DNS-based and URL-based security controls. Advanced IP Defense implements zero trust DNS to block direct-to-IP C2 connections and exfiltration attempts by correlating outbound traffic with DNS history. Advanced IP Defense uses Precision AI IP Intelligence to identify attacker infrastructure in real time using full-lifecycle telemetry.

For more information, see the *Advanced IP Defense* datasheet.

Device Security

Device Security delivers a unified, AI-first solution that provides comprehensive protection and monitoring across your entire attack surface. It discovers all connected devices and then identifies and mitigates hidden risks that would otherwise remain invisible or elusive to the most seasoned InfoSec professionals.

For more information, see the *Device Security* solution brief.

SaaS Security

SaaS Security delivers broad visibility and real-time control over all SaaS applications, including GenAI apps. Moreover, SaaS Security provides robust data protection by monitoring and securing the unapproved movement and storage of sensitive data across various SaaS platforms.

For more information, see the *SaaS Security* solution brief.

AI Access Security

AI Access Security™ empowers organizations to monitor the adoption and usage of sanctioned and unsanctioned GenAI apps. It proactively prevents sensitive data leakage and provides continuous risk monitoring so organizations can safely adopt and use third-party GenAI tools.

For more information, see the *AI Access Security* datasheet.

Advanced SD-WAN

Easily adopt SD-WAN by simply enabling it on your existing firewalls with integrated security. Get an exceptional end-user experience and ensure SLAs by using SD-WAN path measurements and application steering capabilities to intelligently steer applications to the best performing paths.

For more information, see the SD-WAN documentation in TechDocs.

Table 1. Performance and Capacities of PA-5500 Series Quantum Optimized NGFWs								
	PA-5510	PA-5520	PA-5530	PA-5540	PA-5550	PA-5560	PA-5570	PA-5580
Firewall throughput (appmix)*	65 Gbps	75 Gbps	100 Gbps	150 Gbps	175 Gbps	240 Gbps	300 Gbps	375 Gbps
Threat Prevention throughput (appmix)†	45 Gbps	55 Gbps	65 Gbps	90 Gbps	120 Gbps	180 Gbps	240 Gbps	300 Gbps
IPsec VPN throughput‡	34 Gbps	36 Gbps	38 Gbps	80 Gbps	100 Gbps	125 Gbps	150 Gbps	170 Gbps
Max concurrent sessions§	7M	12M	14M	39M	49M	74M	89M	99M
New sessions per second‖	600K	971K	1.01M	1.33M	1.67M	2.5M	3M	3.3M
Virtual systems (base/max)#	10/20	15/65	25/125	25/225	25/225	25/225	25/225	25/225

Note: Results were measured on PAN-OS 12.2. Scale numbers and capacity limits vary across software releases and may change over time as new features and capabilities are introduced.

* Firewall throughput is measured with App-ID and logging enabled, by using appmix transactions.

† Threat Prevention throughput is measured with App-ID, IPS, antivirus, antispyware, WildFire, file blocking, and logging enabled, by using appmix transactions.

‡ IPsec VPN throughput is measured with 64 KB HTTP transactions and logging enabled.

§ Maximum concurrent sessions are measured by using HTTP transactions.

‖ New sessions per second is measured with application override, by using 1-byte HTTP transactions.

Adding virtual systems over the base quantity requires a separately purchased license. An active/active NGFW cluster supports a maximum of 25 virtual systems.

Table 2. PA-5500 Series Networking Features
Interface Modes
L2 mode (not available on MC-LAG aggregate interfaces), L3 mode, tap, and virtual wire (transparent mode).
Routing
The advanced routing engine is the only routing engine supported.
OSPFv2/v3 and MP-BGP with graceful restart, RIP, and static routing.
Policy-based forwarding.
PPPoE and DHCP client are supported for dynamic address assignment for both IPv4 and IPv6.
DHCPv4 server and DHCPv4 relay.
Multicast: PIM-SM, PIM-SSM, IGMPv2, and v3.
Bidirectional Forwarding Detection (BFD) and multihop BFD.
Advanced SD-WAN
Path quality measurement (jitter, packet loss, and latency).
Bandwidth monitoring.
Key exchange: Manual key, IKEv1, and IKEv2 (pre-shared key and certificate-based authentication).
Post-quantum PPK.
Multi-VR and LR support over the SD-WAN overlay.
Prisma® Access Hub (hybrid SASE).
Autonomous Digital Experience Management (ADEM) for NGFW support.
IPv6
IPv6 inspection in L2, L3, tap, and virtual wire mode (transparent mode).
Support for dual-stack and IPv6-only networks.
Features: IPv6 geolocalization, OSPFv3, MP-BGP, NAT64, and NPTv6.
DHCPv6 client with prefix delegation (PD) support. Stateless address autoconfiguration (SLAAC) server support.

Table 2. PA-5500 Series Networking Features (continued)
IPsec and SSL VPN
Key exchange: Manual key, IKEv1, and IKEv2 (pre-shared key and certificate-based authentication).
Encryption: 3DES, AES (128-bit, 192-bit, and 256-bit).
Authentication: MD5, SHA-1, SHA-256, SHA-384, and SHA-512.
GlobalProtect Large Scale VPN for simplified configuration and management.†
Secure remote access over IPsec and SSL VPN tunnels using GlobalProtect gateway and portals including post-quantum cryptography (PQC).†
VLANs
802.1Q VLAN tags per device or per interface: 4,094/4,094.
Aggregate interfaces (802.3ad) and LACP.
Network Address Translation
NAT modes (IPv4): static IP, dynamic IP, and port (port address translation).
NAT64 and NPTv6.
Additional NAT features: Dynamic IP reservation, tunable dynamic IP, and port oversubscription.
High Availability and Clustering
NGFW clustering with active/active. HA active/passive. NGFW clustering maintains a dual-active data plane with a single control plane, support for MC-LAG (aggregate Ethernet interfaces with members on both systems).
Mobile Network Infrastructure‡
5G security.

† Requires a GlobalProtect license.

‡ For additional information, see the ML-Powered NGFWs for 5G datasheet.

Table 3. PA-5500 Series Hardware Specifications
I/O
PA-5510, PA-5520, PA-5530: 10GE Cu mGig (10), 10GE SFP+ (12), 10G/25G SFP28 (8), 40G/100G QSFP28 (6)
PA-5540, PA-5550: 10G/25G SFP28 (16), 40G/100G QSFP28 (16), and 100G/400G QSFP-DD (4)
PA-5560, PA-5570, PA-5580: 10G/25G SFP28 (8), 40G/100G QSFP28 (12), and 100G/400G QSFP-DD (8)
Management I/O
PA-5510, PA-5520, PA-5530: Out-of-band management: 1G/10G SFP+ Console: RJ-45 console port (1) Console: USB-C Bootstrap: USB-C HSCI: 40G/100G (2) Log: 10G SFP+
PA-5540, PA-5550, PA-5560, PA-5570, PA-5580: Out-of-band management: 1G/10G SFP+ (2) Console: RJ-45 console port (1) Console: USB-C Bootstrap: USB 3.2 Gen1 Type A HSCI: 100G/400G QSFP-DD (2) Log: 10G SFP+ (2)

Table 3. PA-5500 Series Hardware Specifications (continued)
Storage Capacity
PA-5510, PA-5520, PA-5530: 960 GB RAID1 SSD pair for system and log storage supported as cold swap Optional 3.84 TB RAID1 SSD pair for system and log storage supported as cold swap
PA-5540, PA-5550, PA-5560, PA-5570, PA-5580: 3.84 TB RAID1 SSD pair for system and log storage supported as cold swap
Power Supply (Avg/Max Power Consumption)
PA-5510, PA-5520, PA-5530: TBD
PA-5540, PA-5550, PA-5560, PA-5570, PA-5580: 2,100 W/3,100 W
Max BTU/hr
PA-5510, PA-5520, PA-5530: TBD
PA-5540, PA-5550, PA-5560, PA-5570, PA-5580: 7,633
Power Supplies
PA-5510, PA-5520, PA-5530: 1+1 redundant for 110–220 V and DC
PA-5540, PA-5550, PA-5560, PA-5570, PA-5580: 2+2 redundant for 220 V and DC 3+1 redundant for 110 V
Input Voltage
PA-5510, PA-5520, PA-5530: AC: 100 to 120 VAC (50-60 Hz), 200 to 240 VAC (50-60 Hz) DC: -48 VDC to -60 VDC
PA-5540, PA-5550, PA-5560, PA-5570, PA-5580: AC: 100–240 VAC (50–60 Hz) DC: -40 VDC to -60 VDC
Power Supply Output
PA-5510, PA-5520, PA-5530: AC: 1200 W/power supply DC: 1200 W/power supply
PA-5540, PA-5550, PA-5560, PA-5570, PA-5580: AC: 2,700 W/power supply with 220 V or 1,200 W/power supply with 110 V DC: 2,200 W/power supply
Max Current Consumption
PA-5510, PA-5520, PA-5530: AC: 12 A @ 120 VAC, 7A @ 240 VAC DC: 30 A @ -60 VDC
PA-5540, PA-5550, PA-5560, PA-5570, PA-5580: AC: 20.3 A @ 110 VAC and 9.3 A @ 240 VAC DC: 43.7 A @ 54 VDC
Max Inrush Current
PA-5510, PA-5520, PA-5530: TBD
PA-5540, PA-5550, PA-5560, PA-5570, PA-5580: AC: 50 A @ 230 VAC and 50 A @ 120 VAC DC: 25 A @ 54 VDC

Table 3. PA-5500 Series Hardware Specifications (continued)
Mean Time Between Failure (MTBF)
PA-5510, PA-5520, PA-5530: TBD
PA-5540, PA-5550: 8.1 years
PA-5560, PA-5570, PA-5580: 6.3 years
Rack Mount Dimensions
PA-5510, PA-5520, PA-5530: 2U, 19" standard rack (3.4" H x 18.7" D x 17.3" W)
PA-5540, PA-5550, PA-5560, PA-5570, PA-5580: 3U, 19" standard rack (5.2" H x 29.8" D x 17.3" W) with power supply inserted
Weight (Standalone Device/As Shipped)
PA-5510, PA-5520, PA-5530: 36.9 lbs
PA-5540, PA-5550, PA-5560, PA-5570, PA-5580: 70 lbs/116 lbs (includes accessory kit, rack kit, packaging, and pallet).
Safety
cTUVus, CB
EMI
FCC Class A, CE Class A, VCCI Class A
Certifications
See our Compliance page.
Environment
Operating temperature: 32°F to 122°F, 0°C to 50°C Nonoperating temperature: -4°F to 158°F, -20°C to 70°C Humidity tolerance: 10%–90% Maximum altitude: 10,000 ft/3,048 m Airflow: Front to back (port side to power supply side)

PA-5500 Series Ordering Information

Table 4 lists key SKUs for the PA-5500 Series. For detailed information about the complete SKU list, including LAB bundles, spares, software subscriptions, and support, work with your Palo Alto Networks account team and NextWave partners.

Table 4. PA-5500 Series Ordering Information

Part Number	Details
PAN-PA-5540-AC PAN-PA-5550-AC PAN-PA-5560-AC PAN-PA-5570-AC PAN-PA-5580-AC	Includes: 4x PAN-PA-5500-PWR-2700-AC 5x PAN-PA-FAN-2RU-A 1x PAN-PA-5500-ACC-A accessory kit 1x PAN-PA-3RU-RACK-A 2x PAN-SFP-CG 1x PAN-PA-5500-SSD-3.84TB-PAIR
PAN-PA-5510-AC PAN-PA-5520-AC PAN-PA-5530-AC	Includes: 2x PAN-PWR-1200W-AC-A 1x PAN-PA-3500-5500-ACC-A 1x PAN-PA-2RU-RACK4 1x PAN-SFP-CG
PAN-PA-5540-DC PAN-PA-5550-DC PAN-PA-5560-DC PAN-PA-5570-DC PAN-PA-5580-DC	Includes: 4x PAN-PA-5500-PWR-2000-DC 5x PAN-PA-FAN-2RU-A 1x PAN-PA-5500-ACC-B accessory kit 1x PAN-PA-3RU-RACK-A 2x PAN-SFP-CG 1x PAN-PA-5500-SSD-3.84TB-PAIR
PAN-PA-5510-DC PAN-PA-5520-DC PAN-PA-5530-DC	Includes: 2x PAN-PWR-1200W-DC-A 1x PAN-PA-3500-5500-ACC-A 1x PAN-PA-2RU-RACK4 1x PAN-SFP-CG
PAN-PA-5500-SSD-3.84TB-PAIR	Spare replacement drive.
PAN-PA-5500-ACC-A	Spare accessory kit (PA-5540/PA-5550/PA-5560/PA-5570/PA-5580) includes a 4x PAN-PWR-C19-US-120V cable, 1x USB cable, and 1x Cat6 cable.
PAN-PA-5500-ACC-B	Spare accessory kit (PA-5540/PA-5550/PA-5560/PA-5570/PA-5580) includes a 4x PAN-PWR-DC-CBL-C cable, 1x USB cable, and 1x Cat6 cable.
PAN-PA-3500-5500-ACC-A	Spare accessory kit (PA-5510/PA-5520/PA-5530) includes a 2x PAN-PWR-CORD-C15-US cable, 1x USB Type C to Type C cable, and 1x Cat6 cable.

Forward-Looking Statement

This document contains forward-looking statements that involve risks, uncertainties and assumptions, including, without limitation, statements regarding the benefits, impact, or performance or potential benefits, impact or performance of our products and technologies or future products and technologies. These forward-looking statements are not guarantees of future performance, and there are a significant number of factors that could cause actual results to differ materially from statements made in this document. We identify certain important risks and uncertainties that could affect our results and performance in our most recent Annual Report on Form 10-K, our most recent Quarterly Report on Form 10-Q, and our other filings with the U.S. Securities and Exchange Commission from time-to-time, each of which are available on our website at investors.paloaltonetworks.com and on the SEC's website at www.sec.gov. All forward-looking statements in this document are based on information available to us as of the date hereof, and we do not assume any obligation to update the forward-looking statements provided to reflect events that occur or circumstances that exist after the date on which they were made.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: **+1.408.753.4000**
Sales: **+1.866.320.4788**
Support: **+1.866.898.9087**

www.paloaltonetworks.com

© 2026 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

strata_ds_pa-5500-series_081926