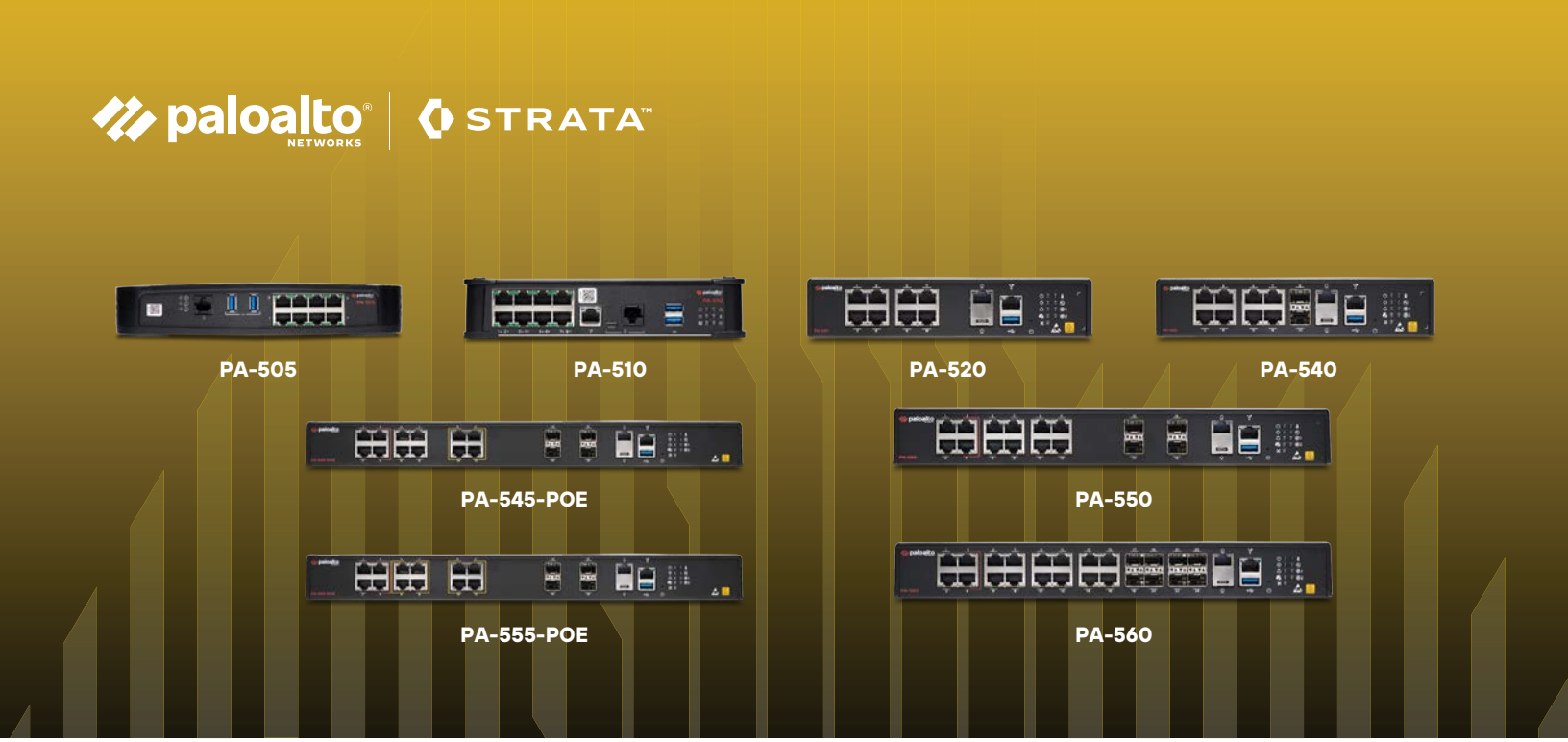

PA-500 Series

Los cortafuegos de nueva generación (NGFW) PA-500 Series de Palo Alto Networks comprenden los modelos PA-505, PA-510, PA-520, PA-540, PA-545-POE, PA-550, PA-555-POE y PA-560. Esta serie lleva las capacidades de los NGFW impulsadas por ML a sucursales empresariales distribuidas, puntos de venta minorista y empresas medianas.

El elemento de control de los cortafuegos NGFW PA-500 Series es PAN-OS®, el mismo software que utilizan todos los NGFW de Palo Alto Networks, que clasifica de forma nativa todo el tráfico (incluido el de las aplicaciones, amenazas y contenido) y lo vincula al usuario, independientemente de su ubicación o del tipo de dispositivo que utilice. La aplicación, el contenido y el usuario —los elementos que hacen funcionar su empresa— sirven como base para sus políticas de seguridad, lo que se traduce en una mejora de la estrategia de seguridad y una reducción del tiempo de respuesta ante incidentes. OPAN-OS integra el aprendizaje automático (ML) en el propio cortafuegos para prevenir los ataques sin firmas de forma integrada (cuando se producen ataques basados en archivos) e identificar y detener de inmediato los intentos de phishing nunca vistos.

Características destacadas

- Serie de cortafuegos NGFW de alto rendimiento para sucursales empresariales.
- Desarrollado por Precision AI®, un innovador motor impulsado por IA que analiza y previene amenazas en tiempo real.
- Alta densidad de puertos con hasta 24 interfaces de cobre y fibra.
- Admite alimentación a través de Ethernet (PoE) de hasta 330 W.
- Compatibilidad con IEEE 802.3bt con un máximo de 90 W de potencia por puerto PoE.
- Simplifica la implementación con Zero Touch Provisioning (ZTP).
- Compatibilidad con configuraciones de alta disponibilidad (modos activo/activo y activo/pasivo).
- Fabricado con una arquitectura de un único paso para proporcionar un rendimiento predecible con los servicios de seguridad.
- Gestionado con Strata™ Cloud Manager, la primera solución de gestión y operaciones unificada basada en IA del sector para la seguridad de la red.
- Líder en el Magic Quadrant™ de Gartner® 2025 para cortafuegos de malla híbrida.
- Líder en el informe The Forrester Wave™: Enterprise Firewall Solutions, Q4 2024 (disponible en inglés).

Identificación y categorización de aplicaciones con inspección completa de Capa 7

App-ID™ identifica y categoriza todas las aplicaciones, en todos los puertos, todo el tiempo, con inspección completa de Capa 7, admitiendo las siguientes capacidades:

- Utiliza técnicas avanzadas, como decodificación de protocolos, heurística y coincidencia de firmas, para identificar con precisión las aplicaciones en toda la red, independientemente del puerto, el protocolo o los métodos de cifrado utilizados. El servicio opcional App-ID Cloud Engine (ACE) proporciona App-ID a pedido para aplicaciones SaaS.
- Proporciona una comprensión integral de los riesgos y valores asociados con diversas aplicaciones, lo que ayuda a tomar decisiones informadas sobre las políticas de seguridad de la red.
- Permite la aplicación efectiva de políticas de seguridad adaptadas a aplicaciones específicas, al centralizar la identificación y el control de las aplicaciones a nivel de cortafuegos.
- Identifica y gestiona aplicaciones evasivas o personalizadas que normalmente eluden las medidas de seguridad tradicionales.
- Actualiza continuamente las identificaciones de su aplicación, garantizando que se mantenga eficaz frente a las últimas tendencias y tácticas de aplicaciones.
- Utiliza técnicas de IA de vanguardia para mejorar la precisión en la identificación y categorización de aplicaciones impulsadas por IA. Estas técnicas garantizan que incluso las aplicaciones más avanzadas y dinámicas sean reconocidas con precisión y gestionadas adecuadamente dentro de la red.

Para obtener más información, consulte nuestro resumen técnico de App-ID.

Aplicación de políticas de seguridad

Los NGFW PA-500 Series refuerzan la seguridad de los usuarios en cualquier ubicación, en cualquier dispositivo, al tiempo que adaptan las políticas en función de su actividad. Incluyen la capacidad de:

- Habilitar la visibilidad, las políticas de seguridad, la elaboración de informes e investigaciones forenses en base a los usuarios, grupos y direcciones IP.
- Aplicar políticas coherentes independientemente de la ubicación de los usuarios (oficina, hogar, viajes, etc.) y los dispositivos. Estos dispositivos incluyen dispositivos móviles iOS y Android; equipos de sobremesa y portátiles macOS, Windows y Linux; VDI Citrix y Microsoft; y servidores de terminales.
- Aprovechar la geolocalización de IP para aplicar automáticamente políticas de seguridad basadas en la ubicación geográfica, lo que le permitirá reducir la superficie de ataque, cumplir con los requisitos de cumplimiento y controlar el acceso a las aplicaciones bloqueando el tráfico hacia y desde países o regiones específicos.
- Autenticar y otorgar autorizaciones a los usuarios de forma coherente, independientemente de dónde estén y de dónde resida su almacén de identidades (directorios locales o en la nube, o ambos), para acelerar la transición a una estrategia de seguridad Zero Trust (confianza cero) con Cloud Identity Engine, una arquitectura en la nube para la seguridad basada en la identidad.
- Proteger todas las aplicaciones con autenticación sin contraseña, ya sea local, SaaS o híbrida.
- Proporcione acciones de seguridad dinámicas basadas en el comportamiento del usuario para restringir usuarios sospechosos o maliciosos al definir grupos de usuarios dinámicos en la nube (CDUG) en el cortafuegos para tomar acciones de seguridad basadas en riesgos y con límites de tiempo sin tener que esperar para aplicar cambios en los directorios de usuarios.
- Evitar tanto la filtración de credenciales corporativas en sitios web de terceros como la reutilización de credenciales robadas habilitando la autenticación multifactor (MFA) en la capa de red para cualquier aplicación, sin necesidad de realizar cambios.

- Integrar fácilmente con una amplia gama de repositorios para trabajar con información del usuario, incluidos controladores de LAN inalámbrica, VPN, servidores de directorio y herramientas de gestión de eventos e información de seguridad (SIEM).
- Automatizar recomendaciones de políticas que ahorran tiempo y reducen la posibilidad de errores humanos.

Consulte nuestro resumen de la solución Cloud Identity Engine para obtener más información.

Enfoque único para el procesamiento de paquetes

Los NGFW PA-500 Series procesan paquetes utilizando una arquitectura de un solo paso. Utilizando este enfoque, los NGFW pueden:

- Ejecutar funciones de red, búsqueda de políticas, decodificación y control de aplicaciones, así como coincidencia de firmas —para todas las amenazas y el contenido— en una sola pasada. De este modo, se reduce de forma considerable la carga de trabajo de procesamiento necesaria para ejecutar varias funciones en un solo dispositivo de seguridad.
- Evitar introducir latencia al analizar el tráfico en busca de todas las firmas en una sola pasada, utilizando coincidencia uniforme de firmas basada en flujos.
- Ofrecer un rendimiento constante y predecible cuando las suscripciones de seguridad están habilitadas (véase la tabla 1).

Listo para la criptografía postcuántica

El PA-500 Series es un dispositivo preparado para criptografía poscuántica que le ayuda a lograr seguridad cuántica en hardware y software con PAN-OS 12.1. Los NGFW PA-500 series son compatibles con:

- Criptografía postcuántica (PQC) para descifrado PQC SSL/TLS, VPN PQC de sitio a sitio, proxy de traducción de cifrado PQC SSL/TLS y perfil de servicio PQC SSL/TLS para acceso de gestión al cortafuegos.
- Algoritmos PQC, incluidos estándares NIST, como ML-KEM, ML-DSA y SLH-DSA, así como PQC preestándar, como Classic McEliece, BIKE, HQC, Frodo-KEM y NTRU-Prime.

Prevención de la actividad maliciosa oculta en el tráfico cifrado

Los NGFW PA-500 Series proporcionan la capacidad de:

- Inspeccionar y aplicar la política al tráfico cifrado SSL/TLS (tanto entrante como saliente), al tráfico que utiliza SSLv3, TLSv1.1, TLSv1.2 y TLSv1.3, así como a los protocolos de aplicación SMTP, WebSocket, gRPC, HTTP/1.0, HTTP/1.1 y HTTP/2.
- Descifrar e inspeccionar sesiones SSL/TLS con los algoritmos de intercambio de claves clásicos RSA, ECDHE, DHE y los estándares de intercambio de claves postcuánticos ML-KEM, HQC, así como los experimentales BIKE y Frodo-KEM.
- Recopilar métricas sobre el tráfico TLS, como la cantidad de tráfico cifrado, las versiones de SSL/TLS y los cifrados.
- Admite suites como los intercambios de claves clásicos RSA, ECDHE y DHE, así como los intercambios de claves post-cuánticas ML-KEM y HQC, sin necesidad de descifrado, lo que aporta mayor visibilidad a la información criptográfica de todas las sesiones SSL/TLS que pasan por el cortafuegos.
- Habilitar el control sobre el uso de protocolos TLS heredados, cifrados no seguros y obsoletos, y certificados mal configurados, incluida una indicación de nombre de servidor (SNI) no coincidente con el nombre común del certificado (CN), para mitigar los riesgos.

- Facilitar la implementación de descifrado fácil y permitirle usar logs integrados mejorados para solucionar problemas en las sesiones del lado del cliente y del lado del servidor de forma independiente para una experiencia de resolución de problemas perfecta, ya sea que se trate de certificados intermedios faltantes o certificados anclados.
- Habilitar y deshabilitar el descifrado de manera flexible, en función de la categoría de la URL, la zona de origen o destino, la dirección, el usuario, el grupo de usuarios, el dispositivo o el puerto, garantizando la privacidad y el cumplimiento normativo.

Además, esta función proporciona «reflejo de descifrado», que le permite crear una copia del tráfico descifrado desde el cortafuegos y enviarla a herramientas de recopilación de tráfico para realizar análisis forenses, crear un historial de tráfico o prevenir la pérdida de datos (DLP).

Lea el Descifrado: Libro blanco "Por qué, dónde y cómo" para aprender sobre el descifrado para prevenir amenazas y proteger su negocio.

Gestión y operaciones unificadas basadas en la IA con Strata Cloud Manager

Administre sus NGFW PA-500 Series con Strata Cloud Manager, que le permite:

- **Obtener una visibilidad completa de la seguridad de su red:** Consiga una visibilidad completa y en tiempo real de todo el entorno de seguridad de su red, incluidos todos los usuarios, aplicaciones, dispositivos y las amenazas más críticas que requieren atención a través de una interfaz unificada.
- **Habilitar un modelo de operaciones y gestión de la seguridad de la red sencillo y coherente:** Gestione de forma centralizada la configuración y las políticas en todos los puntos de aplicación, incluidos SASE, cortafuegos físicos y virtuales, y servicios de seguridad, para garantizar la coherencia y reducir la carga operativa.
- **Fortalecer la postura de seguridad en tiempo real:** Aproveche el análisis basado en IA para detectar, resolver y optimizar anomalías en las políticas, como políticas redundantes y en la sombra y reglas excesivamente permisivas o no utilizadas. Mejore su postura de seguridad con recomendaciones integradas de prácticas recomendadas y mantenga el cumplimiento normativo de las normas del sector y de InfoSec.
- **Resolver de forma proactiva las interrupciones de la red y mejorar la experiencia del usuario:** Predecir, diagnosticar y resolver problemas del estado de la red, como problemas de experiencia de usuario, cuellos de botella de capacidad, vulnerabilidades de CVE, problemas de conexión de servicios y otras 130 categorías de problemas, con hasta 90 días de antelación para garantizar un funcionamiento sin problemas.
- **Resolver problemas rápidamente con conocimiento instantáneo al alcance de su mano:** Con Strata Copilot™, nuestro asistente basado en IA que cuenta con una interfaz de lenguaje natural, puede encontrar, comprender y abordar rápidamente los retos operativos y de seguridad antes de que se agraven. Además, con sus capacidades de creación de casos simplificadas puede obtener una asistencia rápida cuando más la necesita.

Servicios de seguridad en la nube insuperable con tecnología Precision AI

Los NGFW PA-500 Series brindan la mejor seguridad de su clase con servicios de seguridad entregados en la nube (CDSS). En el corazón de nuestro CDSS se encuentra la Precision AI. A diferencia de las herramientas reactivas tradicionales, Precision AI fortalece sus defensas con detección proactiva de amenazas, prevención en línea y respuesta automatizada, deteniendo incluso los ataques más evasivos y nunca antes vistos antes de que causen daños. Con el respaldo de la inteligencia sobre amenazas de nuestros más de 70 000 clientes en todo el mundo, nuestros servicios distribuidos en la nube aprenden, se adaptan y evolucionan continuamente. Integrado perfectamente con nuestras plataformas NGFW y SASE, CDSS ofrece protección unificada en la web, DNS, correo electrónico, aplicaciones y más, sin importar dónde residan sus usuarios o datos.

Ya sea que esté navegando por el trabajo híbrido, adoptando la transformación a la nube o defendiéndose contra adversarios sofisticados, CDSS impulsado por Precision AI le brinda la visibilidad, la automatización y la confianza para mantenerse a la vanguardia.

Advanced Threat Prevention

Analice hasta 673 millones de nuevas sesiones diariamente y bloquee de forma proactiva 28,2 mil millones de amenazas en tiempo real, incluidos exploits de día cero, malware, tráfico de comando y control (C2) y técnicas evasivas, para brindar seguridad de vanguardia a una escala sin precedentes.

Advanced WildFire

Detenga de forma proactiva hasta 450.000 nuevas amenazas cada día con los motores de prevención de malware más potentes de la industria. Advanced WildFire® identifica y bloquea una amplia gama de amenazas avanzadas, incluido malware de día cero, ransomware, troyanos de acceso remoto (RAT), documentos armados y otras técnicas de ataque evasivas, antes de que afecten a su organización.

Advanced URL Filtering

Proteja el acceso a la web bloqueando hasta 151 millones de amenazas en línea todos los días, mientras analiza 3.800 millones de URL nuevas diariamente. Advanced URL Filtering protege contra phishing, malware, ransomware, comunicaciones C2 y ataques evasivos basados en la web.

Advanced DNS Security

Advanced DNS Security ofrece protección en tiempo real que bloquea instantáneamente amenazas sofisticadas basadas en solicitudes y respuestas de DNS, incluidos el secuestro de DNS, los algoritmos de generación de dominios (DGA), la tunelización de DNS y las devoluciones de llamadas C2. Analiza más de 1.100 millones de dominios nuevos diariamente e identifica hasta 7,7 millones de dominios nuevos maliciosos, previniendo más de 2 mil millones de amenazas en línea. Esta poderosa primera línea de defensa identifica y detiene las amenazas en la capa DNS, ya sea que se originen desde fuera o dentro de la red.

Seguridad de los dispositivos

Proteja cada dispositivo conectado con una solución adaptada al sector (incluyendo fabricación, venta minorista, atención médica, alta tecnología y empresas en general) y logre una tasa de descubrimiento de dispositivos del 90 % en 48 horas, proporcionando evaluaciones priorizadas de vulnerabilidad y riesgo. Además, identifique anomalías, obtenga recomendaciones de políticas de seguridad de control de acceso con privilegios mínimos y prácticamente corrija vulnerabilidades, todo en una única plataforma NetSec.

SaaS Security

Descubra y controle todo el consumo de SaaS con visibilidad en más de 75 000 aplicaciones SaaS y controles DLP para más de 150 aplicaciones SaaS. Evite configuraciones incorrectas de SaaS con la gestión de la postura para más de 117 aplicaciones SaaS, así como con el control de tenencia en línea de SaaS para 39 aplicaciones.

AI Access Security

Habilite el uso seguro de GenAI con visibilidad en tiempo real de las aplicaciones GenAI, controles de acceso de usuarios, protección de datos y supervisión continua de riesgos. AI Access Security™ ofrece un catálogo líder del sector de más de 2500 aplicaciones GenAI, incluidos más de 15 atributos de aplicaciones específicos de GenAI para identificar y mitigar el riesgo con precisión. Incluye gestión de postura para más de 13 aplicaciones GenAI y control de tenencia en línea SaaS para 11 aplicaciones.

Advanced SD-WAN

Implemente SD-WAN de forma sencilla activándola en sus cortafuegos actuales, con seguridad integrada. Obtenga una experiencia de usuario final excepcional y garantice los SLA mediante el uso de mediciones de ruta SD-WAN y capacidades de dirección de aplicaciones para dirigir de manera inteligente las aplicaciones hacia las rutas con mejor rendimiento.

Especificaciones de la serie PA-500 Series

Tabla 1. Rendimiento y capacidad de la serie PA-500 Series								
	PA-505	**PA-510**	**PA-520**	**PA-540**	**PA-545-POE**	**PA-550**	**PA-555-POE**	**PA-560**
Rendimiento del cortafuegos (combinación de aplicaciones)*	1,2 Gb/s	1,8 Gbps	2,8 Gb/s	3,8 Gbps	5,0 Gbps	6,5 Gbps	7,5 Gbps	8,5 Gbps
Rendimiento de Threat Prevention (combinación de aplicaciones)†	0,8 Gbps	1,2 Gb/s	1,8 Gbps	2,2 Gb/s	3,0 Gbps	4,5 Gbps	5,0 Gbps	6,0 Gbps
Rendimiento de VPN IPsec ‡	0,4 Gbps	0,8 Gbps	1,5 Gbps	2,0 Gb/s	3,0 Gbps	4,0 Gbps	4,5 Gbps	5,5 Gbps
Número máximo de sesiones simultáneas§	64 000	98 mil	148 mil	248 mil	298 mil	398 mil	448 mil	598 mil
Nuevas sesiones por segundo‖	10 000	15 mil	25 mil	50K	55 mil	70 mil	75 mil	100 000
Sistemas virtuales (base/máx.)#	—	—	—	1/2	1/2	1/5	1/5	1/5

Nota: Los resultados se midieron con PAN-OS 12.1.

* El rendimiento del cortafuegos se calcula con App-ID y la creación de logs activados usando transacciones de combinación de aplicaciones.

† El rendimiento de Threat Prevention se calcula con App-ID, el sistema de prevención de intrusiones, la protección antivirus y antispyware, WildFire, el bloqueo de archivos y la creación de logs activados usando transacciones de combinación de aplicaciones.

‡ El rendimiento de VPN IPsec se calcula con transacciones HTTP de 64 kB y la creación de logs activada.

§ El número máximo de sesiones simultáneas se calcula usando transacciones HTTP.

‖ El cálculo de las nuevas sesiones por segundo se realiza con cancelación de aplicación usando transacciones HTTP de 1 byte.

Para añadir sistemas virtuales a la cantidad base, es preciso adquirir una licencia por separado.

Tabla 2. Funciones de red de la serie PA-500 Series
Modos de interfaz
Modo L2 (no disponible en interfaces agregadas MC-LAG), L3, tap y cable virtual (modo transparente).
Enrutamiento
OSPFv2/v3 y MP-BGP con reinicio correcto, RIP y enrutamiento estático.
Reenvío basado en políticas.
Los clientes PPPoE y DHCP son compatibles con la asignación dinámica de direcciones tanto para IPv4 como para IPv6.
Servidor DHCPv4.
Multidifusión: PIM-SM, PIM-SSM, IGMPv2 y v3.
Advanced SD-WAN
Medición de la calidad de la ruta (vibración, pérdida de paquetes y latencia).
Supervisión de ancho de banda.
Intercambio de claves: Clave manual, IKEv1 e IKEv2 (clave precompartida y autenticación basada en certificados).
PPK postcuántico.
Compatibilidad con Multi-VR y LR a través de la superposición SD-WAN.
Prisma® Access Hub (SASE híbrido).
Gestión autónoma de la experiencia digital (ADEM) para la compatibilidad con NGFW.
IPv6
Inspección de IPv6 en modo L2, L3, tap y cable virtual (modo transparente).
Soporte para redes de doble pila y solo IPv6.
Características: Geolocalización IPv6, OSPFv3, MP-BGP, NAT64 y NPTv6.
Cliente DHCPv6 con soporte para delegación de prefijo (PD). Compatibilidad con servidor de configuración automática de direcciones sin estado (SLAAC).

Tabla 2. Funciones de red de la serie PA-500 Series (continuación)
IPsec y VPN SSL
Intercambio de claves: Clave manual, IKEv1 e IKEv2 (clave precompartida y autenticación basada en certificados).
Cifrado: 3DES y AES (128 bits, 192 bits y 256 bits).
Autenticación: MD5, SHA-1, SHA-256, SHA-384 y SHA-512.
Acceso seguro mediante túneles IPsec y VPN SSL con la puerta de enlace y los portales de GlobalProtect®*
Redes VLAN
Etiquetas VLAN 802.1q por dispositivo/interfaz: 4.094/4.094.
Interfaces agregadas (802.3ad) y LACP.

* Requiere una licencia de GlobalProtect.

Tabla 3. Especificaciones del hardware de la serie PA-500 Series	
E/S	
PA-505: Puertos RJ-45 de 1 Gb (7) PA-510: 1G RJ45 (8) PA-520: 1G RJ45 (8) PA-540: 1G RJ45 (8), 1G SFP (2) PA-545-POE: 1G RJ45 (8), 1G/2.5G (4)/PoE, 1G SFP (4) PA-550: 1G RJ45 (12), 1G SFP (2), 1G/10G SFP/SFP+ (2) PA-555-POE: 1G RJ45 (4), 1G RJ45 (4)/PoE, 1G/2.5G (4)/PoE, 1G SFP (2), 1G/10G SFP/SFP+ (2) PA-560: 1G RJ45 (16), 1G SFP (4), 1G/10G SFP/SFP+ (4)	
Gestión de E/S	
PA-505: Puerto de gestión fuera de banda 10/100/1000 (1), puertos USB (2) y puerto de consola RJ-45 (1) PA-510: Puerto de gestión fuera de banda 10/100/1000 (1), puerto USB (2), puerto de consola RJ-45 (1) y puerto de consola micro-USB (1) PA-520, PA-540, PA-545-POE, PA-550, PA-555-POE, PA-560: Puerto de gestión fuera de banda 10/100/1000 (1), puerto USB (1), puerto de consola RJ-45 y puerto de consola micro-USB (1)	
Capacidad de almacenamiento	
PA-505, PA-510: 128 GB PA-520, PA-540, PA-545-POE, PA-550, PA-555-POE: 120 GB PA-560: 240 GB	
Módulo de plataforma segura (TPM)	
Integrado con TPM para arranque seguro, raíz de confianza de hardware y protección de secretos del sistema.	
Alimentación a través de Ethernet	
PA-545-POE Presupuesto total de PoE: 181 W, puertos PoE (4), carga máxima en un solo puerto: 90 W PA-555-POE Presupuesto total de PoE: 330 W, puertos PoE (8), carga máxima en un solo puerto: 90 W	
Consumo de energía	
Modelo	**Consumo de energía máximo**
PA-505	23 W
PA-510	34,3 W
PA-520 o PA-540	30 W
PA-545-POE*	336 W (con salida PoE de 181 W)
PA-550	57 W
PA-555-POE*	503 W (con salida PoE de 332 W)
PA-560	106 W

* Con uno o más adaptadores de CA proporcionados.

Tabla 3. Especificaciones del hardware de la serie PA-500 Series (continuación)
Máximo BTU/hora
PA-505: 78 PA-510: 117 PA-520 o PA-540: 102 PA-545-POE: 1145 (con salida PoE de 181 W) PA-550: 195 PA-555-POE: 1715 (con salida PoE de 332 W) PA-560: 361
Tensión de entrada (frecuencia de entrada)
100–240 V CA (50-60 Hz)
Consumo máximo de corriente
PA-505: 2 A a 12 V CC PA-510: 2,5 A a 12 V CC PA-520 o PA-540: 4 A a 12 V CC PA-545-POE: 6 A a 54 V CC PA-550: 5 A a 12 V CC PA-555-POE: 9 A a 54 V CC PA-560: 8 A a 12 V CC
Dimensiones
PA-505: 43,9 mm de alto x 163 mm de profundidad x 242 mm de ancho (1,63" de alto x 6,42" de profundidad x 9,53" de ancho) PA-510: 43,9 mm de alto x 224 mm de profundidad x 205 mm de ancho (1,74" de alto x 8,83" de profundidad x 8,07" de ancho) PA-520 o PA-540: 43,9 mm de alto x 265 mm de profundidad x 203 mm de ancho (1,74" de alto x 10,4" de profundidad x 8" de ancho) PA-550 o PA-560: 43,9 mm de alto x 37 mm de profundidad x 330 mm de ancho (1,74" de alto x 12,1" de profundidad x 13" de ancho) PA-545-POE o PA-555-POE: 43,9 mm de alto x 314 mm de profundidad x 409 mm de ancho (1,75" de alto x 12,6" de profundidad x 16,1" de ancho)
Peso (solo dispositivo/embalado)
PA-505: 1,41 kg/2,68 kg PA-510: 2,27 kg/3,54 kg PA-520 o PA-540: 2,6 kg/3,63 kg PA-545-POE: 6,12 kg/8,98 kg PA-550: 5,0 kg/7,07 kg PA-555-POE: 6,12 kg/9,16 kg PA-560: 5,0 kg/7,07 kg
Seguridad
cTUVus, CB
EMI
PA-505, PA-510: FCC Clase B, CE Clase B y VCCI Clase B PA-520, PA-540, PA-545-POE, PA-550, PA-555-POE, PA-560: FCC Clase A, CE Clase A y VCCI Clase A
Certificaciones
Consulte nuestra Página de cumplimiento.
recomendado
Temperatura de funcionamiento: de 0 °C a 40 °C Temperatura de almacenamiento: de -20 °C a 70 °C Refrigeración pasiva: PA-505, PA-510, PA-520, PA-540, PA-545-POE, PA-550 y PA-555-POE Refrigeración activa: PA-560

Tabla 4. Información para pedidos de la serie PA-500 Series		
Accesorio	**Descripción corta**	**Modelos**
PAN-PWR-25W-AC	Adaptador de corriente de repuesto de 25 W	PA-505
PAN-PWR-50W-AC*	Adaptador de corriente de repuesto de 50 W *	PA-510
PAN-PWR-150W-12V-AC-A	Adaptador de corriente de repuesto de 150 W	PA-520, PA-540, PA-550 y PA-560
PAN-PWR-350W-54V-AC-A	Adaptador de corriente de repuesto de 350 W	PA-545-POE
PAN-PWR-550W-54V-AC-A	Adaptador de corriente de repuesto de 550 W	PA-555-POE
PAN-PA-400-RACKTRAY*	Montaje en rack de 4 postes y 1 unidad de rack (RU) para: dos PA-510 y cuatro adaptadores de corriente	PA-510
PAN-1RU-4POST-RACK-11	Montaje en rack de 4 postes y 1 unidad de rack (RU) para: Un PA-560 y dos adaptadores de corriente, Un PA-550 y dos adaptadores de corriente, Dos PA-540 y cuatro adaptadores de corriente, Dos PA-520 y cuatro adaptadores de corriente.	PA-520, PA-540, PA-550 y PA-560
PAN-1RU-4POST-RACK-12	Montaje en rack de 4 postes y 1 unidad de rack (RU) para: Un PA-555-POE y dos adaptadores de corriente, un PA-545-POE y dos adaptadores de corriente	PA-545-POE y PA-555-POE

* Se debe realizar presupuesto por separado.

Oval Tower
De Entrée 99 - 197

Tel.: +31 20 888 1883
Ventas: +1.866.320.4788
Asistencia técnica: +1.866.898.9087

www.paloaltonetworks.es

strata_ds_pa-500-series_090825