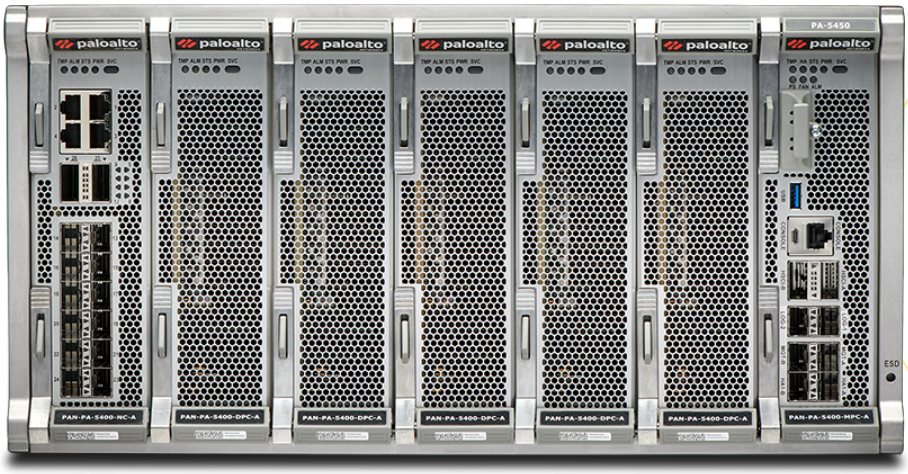

PA-5450

La plataforma de cortafuegos de nueva generación (NGFW, por sus siglas en inglés) con aprendizaje automático PA-5450 de Palo Alto Networks está pensada para implementaciones de centros de datos de gran escala, perímetro de Internet y redes de campus segmentadas. Proporciona un rendimiento excepcional —148 Gb/s de rendimiento de Threat Prevention con los servicios de seguridad activados— y presenta un diseño modular escalable que le permite aumentar el rendimiento cuando lo necesita. El dispositivo PA-5450 ofrece la sencillez de utilizar un único sistema de gestión y concesión de licencias.

Características destacadas

- El primer cortafuegos de nueva generación del mundo con aprendizaje automático
- Líder en el Magic Quadrant® de Gartner para cortafuegos de red en nueve ocasiones
- Líder en el informe The Forrester Wave™: Enterprise Firewalls, T3 2020
- Máxima puntuación en eficacia de la seguridad y 100 % de evasiones bloqueadas en las pruebas a cortafuegos de nueva generación de NSS Labs de 2019
- Arquitectura unificada y escalable
- Seguridad nativa 5G para salvaguardar la transición de las empresas y los proveedores de servicios al 5G y a la computación perimetral multiacceso (MEC, por sus siglas en inglés)
- Visibilidad y seguridad garantizadas de todos los dispositivos, incluidos los no gestionados de IdC, sin necesidad de sensores adicionales
- Compatibilidad con configuraciones de alta disponibilidad (modos activo/activo y activo/pasivo)
- Rendimiento predecible de los servicios de seguridad

El primer cortafuegos de nueva generación con aprendizaje automático ayuda a prevenir las amenazas desconocidas, a ver y proteger todos los dispositivos (incluidos los del Internet de las cosas, o IdC) y a reducir errores gracias a las recomendaciones de políticas automáticas. El elemento de control del dispositivo PA-5450 es PAN-OS®, el mismo software que utilizan todos los cortafuegos de nueva generación de Palo Alto Networks, que clasifica de forma nativa todo el tráfico (incluido el tráfico de 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 —o, lo que es lo mismo, los elementos que hacen funcionar la empresa— sirven como base para las políticas de seguridad, lo que mejora la estrategia de seguridad y reduce los tiempos de respuesta a incidentes.

Principales funciones de seguridad y conectividad

Cortafuegos de nueva generación con aprendizaje automático

- Integra el aprendizaje automático en el propio cortafuegos para prevenir los ataques sin firmas en línea (cuando se producen ataques basados en archivos) e identificar y detener de inmediato los intentos de *phishing* nunca vistos.
- Cuenta con procesos de aprendizaje automático basados en la nube que facilitan firmas sin demora y envían instrucciones al cortafuegos de nueva generación.
- Detecta dispositivos IdC y recomienda políticas analizando el comportamiento mediante un servicio basado en la nube e integrado de forma nativa en el cortafuegos de nueva generación.
- Recomienda políticas automáticamente, lo que ahorra tiempo y reduce la posibilidad de errores humanos.

Inspecciona todo el tráfico de la capa 7, lo que permite identificar y clasificar todas las aplicaciones, en todos los puertos y en todo momento

- Identifica las aplicaciones presentes en la red independientemente del puerto, el protocolo, las técnicas de evasión o el tipo de cifrado (TLS o SSL) empleados.
- Se basa en la aplicación, no en el puerto, para tomar todas las decisiones de habilitación segura de políticas: permitir, denegar, programar, inspeccionar y aplicar la catalogación del tráfico.
- Permite crear etiquetas App-ID™ personalizadas para aplicaciones que sean propiedad de la organización (o, en el caso de que Palo Alto Networks saque nuevas aplicaciones, solicitar el desarrollo de los App-ID correspondientes).
- Identifica todos los datos de la carga útil de una aplicación (p. ej., archivos y patrones de datos) para bloquear los archivos maliciosos y frustrar los intentos de exfiltración de datos.
- Crea informes de utilización de aplicaciones estándar y personalizados, lo que permite, entre otras cosas, elaborar informes relativos al software como servicio (SaaS, por sus siglas en inglés) con información útil sobre todo el tráfico SaaS —autorizado y no autorizado— que circula por la red.
- Incorpora la función Policy Optimizer, que permite migrar sin riesgos conjuntos de reglas obsoletos de capa 4 a otros basados en App-ID, más seguros y fáciles de gestionar.

Aplica a los usuarios las políticas de seguridad que correspondan, estén donde estén y utilicen el dispositivo que utilicen, y adapta también las políticas en función de la actividad de los usuarios

- Permite ver la actividad asociada a determinados usuarios y grupos (y no solo a ciertas direcciones IP), así como aplicarles políticas de seguridad, elaborar informes sobre ellos o someterlos a investigaciones forenses.
- Se integra fácilmente con un amplio abanico de repositorios que contienen información de los usuarios: controladores LAN inalámbricos, VPN, servidores de directorio, sistemas SIEM, proxies, etc.
- Permite definir grupos de usuarios dinámicos (DUG, por sus siglas en inglés) en el cortafuegos para tomar medidas de seguridad temporales sin esperar a que se aplique ningún cambio a los directorios de usuarios.
- Aplica políticas coherentes estén donde estén los usuarios (en la oficina, en casa, de viaje, etc.) e independientemente del tipo de dispositivo (dispositivos móviles iOS y Android®; equipos de escritorio y portátiles macOS®, Windows® y Linux; infraestructuras de escritorios virtuales [VDI] de Citrix y Microsoft; y servidores de terminales).
- Activa la autenticación multifactor (MFA, por sus siglas en inglés) en la capa de la red de cualquier aplicación, un método que, sin necesidad de hacer cambios en la aplicación, impide que las credenciales corporativas se filtren a sitios web de terceros y que, en caso de robo, alguien pueda reutilizarlas.
- Proporciona medidas de seguridad dinámicas basadas en el comportamiento de los usuarios para imponer restricciones a aquellos que se consideran sospechosos o malintencionados.

Impide ocultar actividad maliciosa en el tráfico cifrado

- Inspecciona y aplica políticas al tráfico cifrado con TLS/SSL, tanto el entrante como el saliente, incluido el que emplea los protocolos TLS 1.3 y HTTP/2.

- Proporciona una visibilidad total del tráfico que se transmite a través del protocolo TLS, lo que permite saber, por ejemplo, cuánto tráfico se cifra y qué versiones de TLS/SSL y conjuntos de cifrados se utilizan. Además, toda esta información se obtiene sin recurrir al descifrado.
- Permite controlar el uso de protocolos TLS obsoletos, tipos de cifrado poco seguros y certificados configurados de manera incorrecta, lo que contribuye a mitigar los riesgos.
- Ayuda a implementar el descifrado con facilidad y permite utilizar los logs integrados para solucionar problemas (p. ej., los relacionados con las aplicaciones con certificados fijos).
- En aras de la privacidad y el cumplimiento normativo, permite activar o desactivar el descifrado libremente en función de la categoría de URL, el origen y el destino, la dirección, el usuario, el grupo de usuarios, el dispositivo y el puerto.
- Permite crear una copia del tráfico descifrado desde el cortafuegos (técnica que recibe el nombre de «reflejo de descifrado») y enviarla a herramientas de recopilación de tráfico para realizar análisis forenses, ir creando un historial de tráfico o prevenir la pérdida de datos.

Ofrece visibilidad y gestión centralizadas

- Centraliza en una sola interfaz de usuario unificada la gestión, configuración y visibilidad de varios cortafuegos de nueva generación de Palo Alto Networks distribuidos (independientemente de su ubicación y escala) mediante el servicio de gestión de la seguridad de la red Panorama™.
- Permite compartir configuraciones de forma ágil en Panorama con plantillas y grupos de dispositivos, e intensifica la recopilación de logs conforme sea necesario.
- Permite a los usuarios obtener información detallada sobre las amenazas y el tráfico de la red mediante el centro de control de aplicaciones (ACC, por sus siglas en inglés).

Detecta y previene amenazas avanzadas con servicios de seguridad en la nube

En la actualidad, los ciberataques son muy sofisticados: pueden llegar a alcanzar las 45 000 variantes en solo 30 minutos y recurren a varios vectores de ataque y técnicas avanzadas para distribuir cargas útiles maliciosas. Las soluciones de seguridad inconexas tradicionales se lo ponen difícil a las organizaciones, pues generan lagunas de seguridad, aumentan la carga de trabajo para los equipos que se ocupan de la seguridad y obstaculizan la productividad debido a la ausencia de visibilidad y acceso integrales.

Nuestros servicios de seguridad en la nube, perfectamente integrados con los NGFW líderes en el sector, aprovechan el efecto de red de 80 000 clientes para coordinar al instante la inteligencia y ofrecer protección ante todas las amenazas y vectores de ataque. Además, cubren las carencias en la cobertura en todas las ubicaciones y ofrecen una seguridad insuperable y coherente en una plataforma, para que esté a salvo incluso de las amenazas más avanzadas y evasivas.

- **Threat Prevention**: esta función va más allá de los sistemas de prevención de intrusos (IPS, por sus siglas en inglés) tradicionales, para evitar las amenazas conocidas de todo el tráfico en un único paso sin sacrificar el rendimiento.
- **Advanced URL Filtering**: garantiza una protección web insuperable y, al mismo tiempo, la máxima eficiencia operativa con el primer motor de protección web en tiempo real del mercado y un sistema *antiphishing* sin rival en el sector.
- **WildFire®**: garantiza la seguridad de los archivos con la prevención y detección automáticas de malware desconocido gracias al sistema de análisis basado en la nube líder del sector y a la inteligencia colectiva que aporta una red de más de 42 000 clientes.
- **DNS Security**: gracias al aprendizaje automático, detecta y previene en tiempo real las amenazas ocultas en el tráfico DNS y proporciona al personal que se ocupa de la seguridad la inteligencia y la información contextual necesarias para elaborar políticas y responder a las amenazas con rapidez y eficacia.
- **IoT Security**: brinda la solución de seguridad de IdC más completa del sector, que ofrece visibilidad, prevención y aplicación de políticas con aprendizaje automático en una sola plataforma.
- **Enterprise DLP**: ofrece el primer servicio de prevención de pérdida de datos (DLP, por sus siglas en inglés) empresarial basado en la nube del sector, que protege de forma coherente los datos confidenciales en cualquier punto de las redes y las nubes, y para todos los usuarios.
- **SaaS Security**: ofrece un sistema de seguridad SaaS integrado que permite ver y proteger las nuevas aplicaciones SaaS, salvaguardar los datos y prevenir las amenazas de día cero por un coste total de propiedad mínimo.

Habilita la funcionalidad de SD-WAN

- Permite incorporar fácilmente una red SD-WAN con solo habilitarla en los cortafuegos existentes.
- Hace posible la implementación segura de la tecnología SD-WAN, que se integra de forma nativa con nuestras soluciones de seguridad líderes del sector.
- Proporciona una experiencia excepcional al usuario final, ya que reduce al mínimo la latencia, la vibración y la pérdida de paquetes.

Tabla 1: Rendimiento y capacidad del dispositivo PA-5450		
	Sistema configurado PA-5450*	Un solo PA-5400-DPC-A
Rendimiento del cortafuegos (HTTP/combinación de aplicaciones)***	200/200 Gb/s	64,3/68 Gb/s
Rendimiento de Threat Prevention (HTTP/combinación de aplicaciones)†	120/148 Gb/s	30,2/37 Gb/s
Rendimiento de VPN IPsec‡	79 Gb/s**	15,8 Gb/s
Número máximo de sesiones	100 mill.**	20 mill.
Nuevas sesiones por segundo§	3,5 mill.**	700 000
Sistemas virtuales (base/máx.)||	25/225	—

Nota: Los resultados se midieron con PAN-OS 10.1.

* Todas las pruebas se han realizado con 2 tarjetas de red + 4 tarjetas de procesamiento de datos insertadas, a menos que se especifique lo contrario.

** Esta prueba se ha realizado con 1 tarjeta de red + 5 tarjetas de procesamiento de datos insertadas.

*** El rendimiento del cortafuegos se calcula con App-ID y la creación de logs activados usando transacciones HTTP/combinación de aplicaciones de 64 kB.

† El rendimiento de Threat Prevention se calcula con App-ID, el sistema de prevención de intrusiones, la protección antivirus y antispyware, WildFire, DNS Security, el bloqueo de archivos y la creación de logs activados usando transacciones HTTP/combinación de aplicaciones de 64 kB.

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

§ 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.

La arquitectura de un único paso procesa los paquetes de un modo especial

- La conexión de red, la búsqueda de políticas y la identificación y descodificación de la aplicación, así como el cotejo de firmas para todos los contenidos y amenazas, se realizan en un solo paso. 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.
- Utiliza un formato de firmas uniforme para analizar el tráfico y cotejar todas las firmas en el propio flujo,
  en un solo paso y sin generar latencia.
- Al habilitarse las suscripciones de seguridad, se consigue un rendimiento coherente y predecible. (En la tabla 1, el «rendimiento de Threat Prevention» se ha medido con varias suscripciones activadas).

Arquitectura del dispositivo PA-5450

Por su arquitectura flexible, el dispositivo PA-5450 permite aplicar el tipo y la cantidad de potencia de procesamiento adecuados a las principales tareas de conexión a la red, seguridad y gestión. El dispositivo se gestiona como un solo sistema unificado, lo que le permite dedicar fácilmente todos los recursos disponibles a la protección de sus datos. El dispositivo PA-5450 distribuye de forma inteligente las necesidades de procesamiento en tres subsistemas, cada uno de los cuales dispone de grandes cantidades de capacidad informática y memoria dedicada: la tarjeta de red, la tarjeta de procesamiento de datos y la tarjeta de procesamiento de gestión (NC, DPC y MPC, respectivamente, por sus siglas en inglés).

El dispositivo PA-5450 ofrece un total de seis ranuras para NC y DPC.

Tarjetas de red

Para disfrutar de conectividad de red con el dispositivo PA-5450, se necesita una tarjeta NC como mínimo (PA-5400-NC-A). Para utilizar una segunda NC, debe haber al menos dos DPC instaladas en el sistema. Se pueden instalar dos NC como máximo. Las NC se encargan de ejecutar las tareas de entrada y salida de paquetes.

Cada PA-5400-NC-A ofrece varios puertos de conectividad, tal como se enumera en la tabla 3: (4) puertos 100/1000/10 Gb de cobre, (12) puertos SFP/SFP+ de 1 Gb/10 Gb y (2) puertos QSFP28 de 40 Gb/100 Gb.

Tarjetas de procesamiento de datos

Para el procesamiento de paquetes y operaciones de seguridad, el dispositivo PA-5450 utiliza DPC (PA-5400-DPC-A), con un mínimo de una DPC y hasta cinco DPC, que se pueden instalar en las seis ranuras.

Tarjetas de procesamiento de gestión

El subsistema MPC (PAN-PA-5400-MPC-A) actúa como punto de contacto dedicado para controlar todos los aspectos del PA-5450.

Tabla 2: Funciones de red del dispositivo PA-5450
Modos de interfaz
L2, L3, TAP, cable virtual (modo transparente)
Enrutamiento
OSPF v2/v3 con reinicio correcto, BGP con reinicio correcto, RIP y enrutamiento estático
Reenvío basado en políticas
Enrutamiento
Compatible con el protocolo punto a punto sobre Ethernet (PPPoE) y DHCP para la asignación dinámica de direcciones
Multidifusión: PIM-SM, PIM-SSM, IGMP versiones 1, 2 y 3
Detección de reenvío bidireccional (BFD)
SD-WAN
Cálculo de calidad de la ruta (vibración, pérdida de paquetes y latencia)
Selección de ruta inicial (PBF)
Cambio dinámico de la ruta
IPv6
L2, L3, TAP, cable virtual (modo transparente)
Funciones: App-ID, User-ID, Content-ID, WildFire y SSL Decryption
SLAAC
VPN IPsec
Intercambio de claves: clave manual, IKEv1 e IKEv2 (clave precompartida, autenticación basada en certificados)
Cifrado: 3DES, AES (128 bits, 192 bits, 256 bits)
Autenticación: MD5, SHA-1, SHA-256, SHA-384 y SHA-512
VPN a gran escala de GlobalProtect para una configuración y una gestión más sencillas
Redes VLAN
Etiquetas VLAN 802.1Q por dispositivo/interfaz: 4094/4094
Interfaces agregadas (802.3ad), LACP
Traducción de direcciones de red (NAT)
Modos de NAT (IPv4): IP estática, IP dinámica, IP dinámica y puerto (traducción de direcciones de puertos)
NAT64, NPTv6
Funciones NAT adicionales: reserva de IP dinámica, IP dinámica optimizable y sobresuscripción de puertos
Alta disponibilidad
Modos: activo/activo, activo/pasivo, clúster de alta disponibilidad
Detección de errores: supervisión de rutas y supervisión de interfaces
Infraestructura de la red móvil*
Seguridad de GTP
Seguridad de SCTP

* Para obtener más información, consulte la ficha técnica de los cortafuegos de nueva generación con aprendizaje automático para 5G.

Tabla 3: Especificaciones del hardware del dispositivo PA-5450
E/S de red del dispositivo PA-5400-NC-A
(4) puertos 100/1000/10 Gb de cobre, (12) puertos SFP/SFP+ de 1 Gb/10 Gb y (2) puertos QSFP28 de 40 Gb/100 Gb; 1 NC como mínimo y 2 NC como máximo por sistema; para usar 2 NC, debe haber un mínimo de 2 DPC instaladas.
Gestión de E/S del dispositivo PAN-PA-5400-MPC-A
(2) puertos SFP/SFP+ MGT, (2) puertos SFP/SPF+ HA1, (2) puertos QSFP+/QSFP28 HSCI HA2/HA3, (1) puerto de consola en serie RJ-45, (1) puerto de consola en serie micro-USB
Capacidad de almacenamiento
480 GB en disco SSD, RAID 1, 4 TB en disco SSD para almacenamiento del sistema, almacenamiento para logs (opcional)
BTU/h máximo
8828
Fuentes de alimentación (base/máx.)
2/4
Tensión de entrada de CA (frecuencia de entrada)
100–120 V CA y 200–240 V CA (50–60 Hz)
Salida de fuente de alimentación de CA
2200 W/fuente de alimentación
Consumo máximo de corriente
CA: 100–120 V CA, ~14 A máx. por entrada 200–240 V CA, ~12,5 A máx. por entrada
CC: 48-60 V CC, 52 A máx. por entrada
Corriente máxima de entrada
CA: 35 A a 230 V CA, 35 A a 120 V CA
CC: 50 A a 72 V CC
Montaje en bastidor (dimensiones)
5U, bastidor estándar de 19” (22,23 cm [alt.] x 76,84 cm [prof.] x 44,14 cm [an.])
Tiempo máximo entre fallos (MTBF)
Depende de la configuración; póngase en contacto con su representante de Palo Alto Networks para obtener más información al respecto.
Seguridad
cTUVus, CB
EMI
Clase A de FCC, Clase A de CE, Clase A de VCCI, Clase A de KCC, Clase A de BSMI
Certificaciones
Consulte la página paloaltonetworks.com/company/certifications.html
Entorno
Temperatura de funcionamiento: de 0 °C a 50 °C (de 32 °F a 122 °F)
Temperatura de almacenamiento: de -20 °C a 70 °C (de -4 °F a 158 °F)

Para obtener más información sobre las funciones del dispositivo PA-5450 y sus capacidades asociadas, visite paloaltonetworks.com/network-security/next-generation-firewall/pa-5450.

Oval Tower
De Entrée 99 - 197
1101HE Ámsterdam
Países Bajos
Tel.: +31 20 888 1883
www.paloaltonetworks.es