Serie PA-7000 Series

Los cortafuegos de nueva generación (NGFW, por sus siglas en inglés) con aprendizaje automático de la serie PA-7000 Series de Palo Alto Networks ayudan a los proveedores de servicios y a las organizaciones de escala empresarial a proteger sus entornos de alto rendimiento, como centros de datos de gran tamaño y perímetros de red con un consumo de ancho de banda elevado. La gran cantidad de datos que generan las aplicaciones, los usuarios y los dispositivos no supone un problema para estos sistemas, dotados de un rendimiento espectacular, funciones de prevención capaces de detener los ciberataques más avanzados y técnicas de descifrado que neutralizan con eficacia las amenazas que se ocultan tras la máscara del cifrado. La serie PA-7000 Series se caracteriza por su sencillez. Las tareas de gestión y concesión de licencias se realizan mediante un único sistema creado para aprovechar al máximo los recursos de procesamiento de seguridad y utilizar automáticamente toda la capacidad informática disponible en cada momento.

Características destacadas

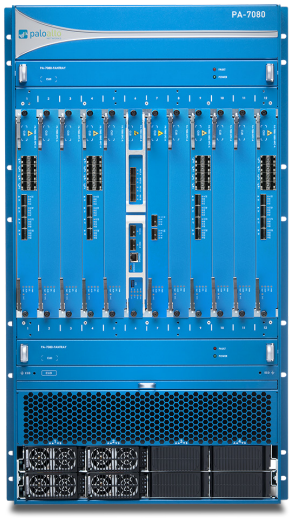
- El primer cortafuegos de nueva generación del mundo con aprendizaje automático
- Líder en el Magic Quadrant® de Gartner para cortafuegos de red en nueve ocasiones
- Líder en el informe The Forrester Wave™: Enterprise Firewalls, T3 2020
- Máxima puntuación en eficacia de la seguridad y 100 % de evasiones 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 elemento de control de la serie PA-7000 Series 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, agiliza la respuesta a incidentes y reduce el trabajo administrativo que supone mantener al día las políticas de seguridad en un entorno muy dinámico.

Principales funciones de seguridad y conectividad

Cortafuegos de nueva generación con aprendizaje automático

PA-7050



PA-7080

- 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 de Internet de las cosas (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.

Tabla 1: Rendimiento y capacidad de la serie PA-7000 Series

	PA-7080*	PA-7050*	PA-7000 DPC-A	PA-7000-100G-NPC-A
Rendimiento del cortafuegos (HTTP/combinación de aplicaciones)†	610/687 Gb/s	370/400 Gb/s	73,8/83,1 Gb/s	55,5/62,5 Gb/s
Rendimiento de Threat Prevention (HTTP/combinación de aplicaciones)§	342/405 Gb/s	200/243 Gb/s	38,5/46,3 Gb/s	27,7/34,6 Gb/s
Rendimiento de VPN IPsec‖	334 Gb/s	200 Gb/s	37,1 Gb/s	28 Gb/s
Número máximo de sesiones	416 mill.	245 mill.	43 mill.	32 mill.
Nuevas sesiones por segundo**	6 mill.	4 mill.	825 000	624 000
Sistemas virtuales (base/máx.)††	25/225	25/225	–	–

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

* Los resultados de esta columna se obtuvieron con una combinación óptima de tarjetas PA-7000-DPC-A y PA-7000-100G-NPC-A insertadas en todas las ranuras disponibles.

† El rendimiento 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.

†† El precio del sistema base incluye 25 sistemas virtuales, pero pueden comprarse hasta 200 licencias adicionales por separado. Se admiten 225 sistemas virtuales como máximo.

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 las amenazas 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

gracias a los siguientes servicios:

- **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.

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).

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.

Arquitectura de la serie PA-7000 Series

Por su arquitectura flexible, la serie PA-7000 Series permite aplicar el tipo y la cantidad de potencia de procesamiento adecuados a las principales tareas de conexión a la red, seguridad y gestión. La serie PA-7000 Series se gestiona como un solo sistema unificado, lo que le permite dedicar fácilmente todos los recursos disponibles a la protección de sus datos. El chasis de la serie PA-7000 Series 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(s) tarjeta(s) de procesamiento de red, la tarjeta de gestión de conmutadores y la tarjeta de logs dedicada.

Tarjetas de procesamiento

El modelo PA-7080 tiene diez ranuras para tarjetas de procesamiento; el PA-7050, seis. Pueden utilizarse tanto tarjetas de procesamiento de red como tarjetas de procesamiento de datos (NPC y DPC, respectivamente, por sus siglas en inglés). Las primeras combinan el procesamiento de datos con otras funciones de red, mientras que con las segundas se consigue un rendimiento óptimo a la hora de procesar los datos. Para disfrutar de conectividad de red con la serie PA-7000 Series, se necesita una tarjeta NPC como mínimo.

Tarjeta de procesamiento de red

La tarjeta de procesamiento de red (NPC, por sus siglas en inglés) se dedica a ejecutar todas las tareas relacionadas con el procesamiento de paquetes, incluidas las conexiones a la red, la clasificación del tráfico y la prevención de amenazas. La tarjeta 100G-NPC (PA-7000-100G-NPC-A) cuenta con 144 núcleos de procesamiento (tres CPU de 48 núcleos) y ofrece la posibilidad de descargar ciertas tareas de procesamiento. El objetivo es proteger la red a 66 Gb/s por NPC. La tarjeta PA-7000-100G-NPC-A ofrece varias opciones de conectividad: 100 Gb, 40 Gb, 10 Gb y 1 Gb.

Tarjeta de procesamiento de datos

La tarjeta DPC-A (PA-7000-DPC-A) optimiza el procesamiento de las operaciones de seguridad. Una sola tarjeta de este tipo tiene 192 núcleos de procesamiento (cuatro CPU de 48 núcleos) y puede proteger su red a velocidades de hasta 86 Gb/s. Su diseño, basado en el de la tarjeta 100G-NPC, añade un cuarto complejo de computación y un procesador de descarga adicional (en sustitución de E/S Ethernet).

Tarjeta de gestión de conmutadores

La tarjeta de gestión de conmutadores (PA-7000-SMC-B), que actúa como el centro de control de la serie PA-7000 Series, supervisa todo el tráfico de forma inteligente y ejecuta todas las funciones de gestión mediante una combinación de tres elementos: el procesador de primer paquete (FPP, por sus siglas en inglés), un backplane de alta velocidad y el subsistema de gestión.

Procesador de primer paquete

El FPP, fundamental para que la serie PA-7000 Series rinda lo mejor posible y ofrezca escalabilidad lineal, rastrea constantemente el grupo compartido de recursos de E/S y de procesamiento disponibles en todas las tarjetas NPC y DPC, y dirige el tráfico entrante de forma inteligente a los procesadores de datos adecuados, en función de las políticas configuradas. A medida que se añaden tarjetas de procesamiento para aumentar el rendimiento y la capacidad, el FPP detecta automáticamente los nuevos recursos añadidos al sistema y pasa a utilizarlos, por lo que no es necesario realizar cambios de gestión del tráfico ni volver a conectar los cables o configurar de nuevo la serie PA-7000 Series. Para alcanzar el máximo rendimiento (700 Gb/s con el modelo PA-7080 o 416 Gb/s con el PA-7050), basta con añadir otra tarjeta DPC-A o 100G-NPC. El FPP determinará por sí solo la mejor forma de usar la potencia de procesamiento resultante.

Backplane de alta velocidad

Gracias al backplane de alta velocidad, cada tarjeta de procesamiento tiene acceso a más de 100 Gb/s de capacidad de tráfico, sin bloqueo.

Subsistema de gestión

Este subsistema actúa como punto de contacto dedicado para controlar todos los aspectos de la serie PA-7000 Series.

Tarjeta de logs dedicada

La tarjeta de reenvío de logs (PA-7000-LFC-A), elemento fundamental de cualquier sistema, utiliza un diseño con varias CPU. De esta forma, se crea un subsistema dedicado a gestionar la gran cantidad de logs que genera la serie PA-7000 Series. La PA-7000-LFC-A es una tarjeta de alto rendimiento dedicada a la exportación de mensajes de log. Permite reenviar logs a Panorama (nuestro servicio de gestión de la seguridad de la red), a Cortex® Data Lake y a Syslog, para luego analizarlos sin conexión.

Tabla 2: Funciones de red de la serie PA-7000 Series
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
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) (intra o intertarjeta) y 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 de la serie PA-7000 Series			
	NPC de PA-7000	Sistema completo PA-7080	Sistema completo PA-7050
PA-7000-100G-NPC-A	(8) puertos SFP/SFP+, (4) puertos QSFP+/ QSFP28	(80) puertos SFP/SFP+, (40) puertos QSFP+/QSFP28	(48) puertos SFP/SFP+, (24) puertos QSFP+/QSFP28
PA-7050-SMC-B PA-7080-SMC-B	–	(2) puertos SFP MGT, (2) puertos SFP HA1, (2) puertos QSFP+/QSFP28 HSCI HA2/HA3, (1) puerto de consola en serie RJ-45, (1) puerto de consola en serie micro-USB	
PA-7000-LFC-A	–	(2) unidades del sistema SSD de 240 GB cada una (480 GB en total), RAID 1	
Tensión de entrada de CA	–	100–240 V CA (50–60 Hz)	100–240 V CA (50–60 Hz)
Corriente nominal de entrada	–	65-27 A	27-12 A
Salida de fuente de alimentación de CA	–	2500 W a 240 V CA 1200 W a 120 V CA	2500 W a 240 V CA 1200 W a 120 V CA
Tensión de entrada de CC	–	De -40 a -60 V CC	De -40 a -60 V CC
Corriente nominal de entrada	–	135 A	60 A
Salida de alimentación de CC	–	2500 W/fuente de alimentación	2500 W/fuente de alimentación
Corriente máxima/fuente de alimentación	–	12 A a 240 V CA de entrada 75 A a >40 V CC de entrada	16 A a 180 V CA de entrada 75 A a 37,5 V CC de entrada
Fuentes de alimentación (base/máx.)	–	4/8	4/4
Corriente máxima de entrada/fuente de alimentación	–	30 A CA/100 A CC en pico	50 A CA/75 A CC en pico
Tiempo medio entre fallos (MTBF)	Depende de la configuración; póngase en contacto con su representante de Palo Alto Networks para obtener más información al respecto.		
BTU/h máximo	–	20 132	10 236
Montaje en bastidor (dimensiones)	–	19U, bastidor estándar de 19" (81,84 cm [alt.] × 48,26 cm [an.] × 62,64 cm [prof.])	9U, bastidor estándar de 19" (40,01 cm [alt.] × 48,26 cm [an.] × 60,96 cm [prof.])
Peso (solo dispositivo/embalado)	–	135,76 kg (CA) / 135,31 kg (CC)	85 kg (CA) / 83,91 kg (CC)
Seguridad	–	cTUVus, CB	
EMI	–	Clase A de FCC, Clase A de CE, Clase A de VCCI	
Certificaciones	–	NEBS de nivel 3	
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 de la serie PA-7000 Series y sus capacidades asociadas, visite paloaltonetworks.com/network-security/next-generation-firewall/pa-7000-series.

paloalto NETWORKS

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

www.paloaltonetworks.es