



PA-850

Serie PA-800 Series

Los cortafuegos de nueva generación con aprendizaje automático de la serie PA-800 Series de Palo Alto Networks, que incluye los modelos PA-820 y PA-850, están diseñados para proteger sucursales de organizaciones y empresas medianas.

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 once ocasiones
- Líder en el informe The Forrester Wave: Enterprise Firewalls, Q4 2022
- 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
- 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
- Útil para implementar fácilmente grandes cantidades de cortafuegos mediante un sistema opcional de aprovisionamiento sin intervención manual (ZTP, por sus siglas en inglés)
- Administración centralizada con el servicio de gestión de la seguridad de la red Panorama
- Rentabilidad máxima de la inversión en seguridad y prevención de las interrupciones de la actividad empresarial con la tecnología AIOps

El elemento de control de la serie PA-800 Series es PAN-OS, el mismo software que utilizan todos los cortafuegos de nueva generación (NGFW, por sus siglas en inglés) 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 de forma integrada (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.
- Detecta y controla las nuevas aplicaciones automáticamente mediante la suscripción al servicio SaaS Security para seguir el ritmo al boom del SaaS.
- 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.
- Consulte el [informe tecnológico de App-ID](#) para obtener más información.

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.
- Autentica y otorga autorizaciones a los usuarios de forma coherente, independientemente de dónde estén y de dónde resida su almacén de identidades, para acelerar la transición a una estrategia de seguridad Zero Trust (confianza cero) con Cloud Identity Engine, una novedosa arquitectura en la nube para la seguridad basada en la identidad. Consulte el [resumen de la solución Cloud Identity Engine](#) para obtener más información.

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.
- Permite desviar todo el tráfico (TLS descifrado, TLS sin descifrar y tráfico que no se transmite a través del protocolo TLS) a herramientas de seguridad de terceros de forma inteligente con Network Packet Broker, así como optimizar el rendimiento de la red y reducir el gasto operativo.
- Consulte este [informe técnico dedicado al descifrado](#) para aprenderlo todo sobre dónde, cuándo y cómo descifrar el tráfico para evitar las amenazas y proteger su negocio.

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).

Rentabilice al máximo su inversión en seguridad y evite las interrupciones de la actividad empresarial con la tecnología AIOps

- La AIOps para NGFW sugiere continuamente prácticas recomendadas adaptadas a su implementación particular para reforzar su estrategia de seguridad y rentabilizar al máximo su inversión en este ámbito.
- Predice de forma inteligente los problemas relativos al estado, el rendimiento y la capacidad de los cortafuegos gracias al aprendizaje automático basado en datos de telemetría avanzados. Además, ofrece información útil para resolver las interrupciones previstas.

Detecta y previene las 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 gracias a los siguientes servicios:

- **Advanced Threat Prevention:** detenga las amenazas conocidas de exploits, malware, spyware y comando y control, utilizando la prevención de ataques de día cero pionera en el sector. Prevenga un 60 % más de ataques por inyección desconocidos y un 48 % más de tráfico de comando y control muy evasivo que con las soluciones IPS tradicionales.
- **Advanced WildFire:** garantice la seguridad de los archivos previniendo automáticamente el malware conocido, desconocido y muy evasivo con una rapidez 60 veces superior gracias al mayor motor de inteligencia sobre amenazas y prevención de malware del sector.
- **Advanced URL Filtering:** garantice el acceso seguro a internet y evite un 40 % más de ataques basados en la web con el primer sistema de prevención en tiempo real de amenazas conocidas y desconocidas del sector, que detiene el 88 % de las URL maliciosas al menos 48 horas antes que otros proveedores.
- **DNS Security:** obtenga un 40 % más de cobertura frente a las amenazas y detenga el 85 % del malware que utiliza DNS para perpetrar ataques de comando y control y robos de datos, sin necesidad de realizar cambios en la infraestructura.
- **Enterprise DLP:** reduzca al mínimo el riesgo de que se produzcan brechas de datos, detenga las transferencias de datos que infrinjan las políticas y garantice el cumplimiento normativo de forma coherente en toda la empresa con el doble de cobertura que cualquier otra solución DLP empresarial en la nube.

- **SaaS Security:** adelántese a la proliferación de aplicaciones SaaS con el único CASB de nueva generación del sector que ve y protege automáticamente todas las aplicaciones, sea cual sea el protocolo utilizado.
- **IoT Security:** protéjalo todo e implemente un modelo de seguridad Zero Trust (confianza cero) para los dispositivos 20 veces más rápido y con la seguridad más eficaz del sector para dispositivos inteligentes.

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.

Tabla 1: Rendimiento y capacidad de la serie PA-800 Series*

	PA-820	PA-850
Rendimiento del cortafuegos (HTTP/combinación de aplicaciones) [†]	1,6/1,5 Gb/s	2,0/1,9 Gb/s
Rendimiento de Threat Prevention (HTTP/combinación de aplicaciones) [‡]	790/840 Mb/s	1,0/1,0 Gb/s
Rendimiento de VPN IPsec [§]	1,4 Gb/s	1,8 Gb/s
Número máximo de sesiones	128 000	192 000
Nuevas sesiones por segundo	8100	13 100

* Los resultados se midieron con PAN-OS 11.0.

† 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.

Los cortafuegos de nueva generación con aprendizaje automático de la serie PA-800 Series son compatibles con una amplia gama de funciones de red que le permiten integrar más fácilmente nuestras funciones de seguridad en su red existente.

Tabla 2: Funciones de red de la serie PA-800 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
Protocolo punto a punto sobre Ethernet (PPPoE)
Multidifusión: PIM-SM, PIM-SSM, IGMP versiones 1, 2 y 3

Tabla 2: Funciones de red de la serie PA-800 Series (continuación)

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
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
Detección de errores: supervisión de rutas y supervisión de interfaces
Aprovisionamiento sin intervención manual (ZTP)
Disponible con los SKU -ZTP (PA-220-ZTP)
Requiere Panorama 9.1.3 o superior

Tabla 3: Especificaciones del hardware de la serie PA-800 Series

E/S
PA-820: (4) puertos 10/100/1000, (8) puertos SFP Gigabit PA-850: (4) puertos 10/100/1000, (8) puertos SFP Gigabit PA-850: (4) puertos 10/100/1000, (4) puertos SFP Gigabit, (4) puertos SFP+ 10 Gigabit
Gestión de E/S
(1) puerto de gestión fuera de banda 10/100/1000 (2) puertos 10/100/1000 de alta disponibilidad (1) puerto de consola RJ-45 (1) puerto USB (1) puerto de consola micro-USB
Capacidad de almacenamiento
240 GB en disco SSD

Tabla 3: Especificaciones del hardware de la serie PA-800 Series (continuación)**Fuente de alimentación**

PA-820: (1) fuente de alimentación fija de CA de 200 W
PA-850: (2) fuentes de alimentación de CA de 450 W (una de ellas redundante)

Consumo de energía

Máximo - PA-820: 120 W; PA-850: 240 W
Medio - PA-820: 41 W; PA-850: 64 W

BTU/h máximo

256

Tensión de entrada (frecuencia de entrada)

100-240 V CA (50-60 Hz)

Consumo máximo de corriente

PA-820: 1,0 A a 100 V CA, 0,5 A a 240 V CA
PA-850: 2,0 A a 100 V CA, 1,0 A a 240 V CA

Corriente máxima de entrada

PA-820: 0,4 A a 230 V CA, 0,96 A a 120 V CA
PA-850: 1,0 A a 230 V CA, 1,84 A a 120 V CA

Montaje en bastidor (dimensiones)

PA-820: 1U, bastidor estándar de 48,3 cm (4,45 cm [alt.] x 35,56 cm [prof.] x 43,50 cm [an.])
PA-850: 1U, bastidor estándar de 48,3 cm (4,45 cm [alt.] x 36,83 cm [prof.] x 43,50 cm [an.])

Peso (solo dispositivo/embalado)

PA-820: 4,99 kg/8,16 kg
PA-850: 6,12 kg / 9,75 kg

Seguridad

cTUVus, CB

EMI

Clase A de FCC, Clase A de CE, Clase A de VCCI

Certificaciones

Consulte la página [paloaltonetworks.com/company/certifications.html](https://www.paloaltonetworks.com/company/certifications.html)

Entorno

Temperatura de funcionamiento: de 0 °C a 40 °C
Temperatura de almacenamiento: de -20 °C a 70 °C

Flujo de aire

De delante a atrás