PA-3260

PA-3250

PA-3220

PA-3200 Series

Los NGFW PA-3200 Series con tecnología de aprendizaje automático (ML) de Palo Alto Networks (que incluyen PA-3260, PA-3250 y PA-3220) se dirigen a implementaciones de gateways de Internet de alta velocidad. Los dispositivos PA-3200 Series protegen todo el tráfico, incluso el tráfico cifrado, a través de procesamiento y memoria dedicados para el funcionamiento de la red, la seguridad, la prevención y la gestión de amenazas.

Aspectos destacados

- El primer NGFW con tecnología de aprendizaje automático (ML)
- Once veces líderes en Magic Quadrant de Gartner sobre firewalls de redes
- Líder en The Forrester Wave: Enterprise Firewalls, cuarto trimestre de 2022
- Máxima puntuación de eficacia de seguridad en el informe sobre pruebas de NGFW de 2019 de NSS Labs con 100 % de las evasiones bloqueadas
- Aumenta la visibilidad y la seguridad de todos los dispositivos, incluidos los dispositivos de IoT no gestionados, sin la necesidad de implementar sensores adicionales
- Admite la alta disponibilidad con los modos activo/activo y activo/pasivo
- Ofrece un rendimiento predecible con servicios de seguridad
- Simplifica la implementación de grandes cantidades de firewalls con aprovisionamiento cero táctil (ZTP) opcional
- Admite la administración centralizada con la gestión de seguridad de red de Panorama
- Maximiza las inversiones en seguridad y evita las interrupciones de los negocios con AIOps

El elemento de control de PA-3200 Series es PAN-OS, el mismo software que ejecuta todos los firewalls de nueva generación (NGFW) de Palo Alto Networks. PAN-OS clasifica de forma nativa todo el tráfico, incluso de las aplicaciones, las amenazas y el contenido, y lo vincula con el usuario sin importar la ubicación o el tipo de dispositivo. La aplicación, el contenido y el usuario (los elementos que hacen funcionar a su empresa) sirven como base de sus políticas de seguridad, lo que se traduce en una mejor postura de seguridad y una reducción en el tiempo de respuesta ante incidentes.

Funciones clave de seguridad y conectividad

Firewall de nueva generación con aprendizaje automático

- Integra el aprendizaje automático (ML) en el núcleo del firewall a fin de proporcionar una prevención interna de ataques sin firma para los ataques basados en archivos, mientras identifica y detiene de inmediato los intentos de phishing nunca antes vistos.
- Aprovecha los procesos de ML basados en la nube para enviar instrucciones y firmas sin demora al NGFW.
- Usa el análisis de comportamiento para detectar dispositivos de Internet de las cosas (IoT) y ofrecer recomendaciones de políticas; un servicio integrado de forma nativa y entregado en la nube en el NGFW.
- Automatiza las recomendaciones de políticas que ahorran tiempo y reducen los errores humanos.

Identificación y categorización de todas las aplicaciones en todos los puertos, en todo momento, con inspección completa de la Capa 7

- Identifica las aplicaciones que atraviesan su red, independientemente del puerto, el protocolo, las técnicas de evasión o el cifrado (TLS/SSL).
- Descubre y controla automáticamente las nuevas aplicaciones para seguir el ritmo de la explosión de SaaS con la suscripción a SaaS Security.
- Usa la aplicación, no el puerto, como base para todas las decisiones de políticas de habilitación segura: permitir, denegar, programar, inspeccionar y aplicar el control de tráfico.
- Proporciona la capacidad de crear etiquetas de App-ID personalizadas para las aplicaciones exclusivas o solicita el desarrollo de App-ID para las nuevas aplicaciones de Palo Alto Networks.
- Identifica todos los datos de la carga útil dentro de una aplicación (por ejemplo, los patrones de datos y archivos) para bloquear los archivos malintencionados y frustrar los ataques de exfiltración de datos.
- Crea informes de uso de aplicaciones estándar y personalizados, incluidos informes de Software as a Service (Software como servicio - SaaS) que proporcionan información sobre todo el tráfico SaaS autorizado y no autorizado en su red.
- Habilita la migración segura de conjuntos de reglas de Capa 4 heredados a las reglas basadas en App-ID con un optimizador de políticas incorporado que ofrece un conjunto de reglas más seguro y fácil de administrar.

Refuerzo de la seguridad de los usuarios en cualquier ubicación, en cualquier dispositivo, y adaptación de políticas basada en la actividad de los usuarios

- Habilita la visibilidad, las políticas de seguridad, los informes y las investigaciones forenses en función de los usuarios y los grupos, no solo las direcciones IP.
- Se integra fácilmente en una amplia gama de repositorios para aprovechar la información de los usuarios: controladores de LAN inalámbricos, VPN, servidores de directorios, SIEM, proxies y más.
- Permite definir grupos de usuarios dinámicos (DUG) en el firewall para adoptar medidas de seguridad con plazos determinados sin esperar a que los cambios se apliquen en los directorios de usuarios.
- Aplica políticas sistemáticas independientemente de las ubicaciones (oficina, hogar, viaje, etc.) y los dispositivos (dispositivos móviles iOS y Android, macOS, Windows, computadoras de escritorio Linux, computadoras portátiles; servidores de terminales, y VDI Citrix y Microsoft) de los usuarios.
- Evita la filtración de credenciales corporativas a sitios web de terceros y la reutilización de credenciales sustraídas mediante la habilitación de la autenticación de varios factores (MFA) en la capa de la red para cualquier aplicación sin cambios.
- Proporciona acciones de seguridad dinámicas basadas en el comportamiento del usuario para restringir a los usuarios sospechosos o malintencionados.
- Autentifica y autoriza a sus usuarios de forma sistemática, independientemente de la ubicación y de dónde se encuentren los almacenes de identidades de los usuarios, para avanzar rápidamente hacia una postura de seguridad de Confianza Cero con el motor de identidad en la nube, una arquitectura totalmente nueva basada en la nube para la seguridad basada en la identidad. Consulte el informe de la solución de motor de identidad en la nube para obtener más información.

Prevención de actividades malintencionadas ocultas en el tráfico cifrado

- Inspecciona y aplica políticas al tráfico cifrado con TLS/SSL, tanto entrante como saliente, incluido el tráfico que usa TLS 1.3 y HTTP/2.
- Ofrece visibilidad enriquecida del tráfico de TLS, por ejemplo, la cantidad de tráfico cifrado, las versiones de TLS/SSL, los conjuntos de cifrado y mucho más, sin descifrado.
- Permite el control sobre el uso de protocolos TLS heredados, cifrados inseguros y certificados configurados incorrectamente para mitigar los riesgos.
- Facilita la implementación del descifrado y permite usar registros incorporados para solucionar problemas, como aplicaciones con certificados bloqueados.
- Permite habilitar o deshabilitar la flexibilidad del descifrado en función de la categoría de URL, la zona de origen y destino, la dirección, el usuario, el grupo de usuarios, el dispositivo y el puerto con fines de privacidad y cumplimiento normativo.
- Permite crear una copia del tráfico descifrado del firewall (reflejo de descifrado) y enviarla a las herramientas de recopilación de tráfico para investigaciones forenses, fines históricos o data loss prevention (prevención de pérdida de datos - DLP).
- Permite reenviar de forma inteligente todo el tráfico (TLS descifrado, TLS no descifrado y no TLS) a herramientas de seguridad de terceros con Network Packet Broker, optimizar el rendimiento de su red y reducir los gastos operativos.
- Consulte este informe técnico sobre descifrado para saber dónde, cuándo y cómo descifrar para prevenir amenazas y proteger su empresa.

Ofrece visibilidad y gestión centralizadas

- Se beneficia de la gestión, la configuración y la visibilidad centralizadas para múltiples NGFW de Palo Alto Networks distribuidos (independientemente de la ubicación o la escala) a través de la gestión de seguridad de redes de Panorama, en una interfaz de usuario unificada.
- Agiliza el uso compartido de la configuración a través de Panorama con plantillas y grupos de dispositivos, y escala la recopilación de registros a medida que aumentan las necesidades de registro.
- Permite a los usuarios obtener una visibilidad profunda e información integral del tráfico de red y las amenazas, gracias al Application Command Center (Centro de comando de aplicación - ACC).

Maximización de su inversión en seguridad y prevención de interrupción de negocios con AIOps

- AIOps para NGFW ofrece recomendaciones continuas sobre mejores prácticas adaptadas a su implementación única para reforzar su postura de seguridad y aprovechar al máximo su inversión en seguridad.
- Predice de forma inteligente los problemas de salud, el rendimiento y la capacidad de los firewalls basándose en ML, con la ayuda de datos de telemetría avanzados. También proporciona información accionable para resolver las interrupciones previstas.

Detección y prevención de amenazas avanzadas con servicios de seguridad en la nube

Los sofisticados ciberataques de la actualidad pueden generar 45.000 variantes en 30 minutos con múltiples vectores de amenaza y técnicas avanzadas para entregar cargas útiles malintencionadas. La seguridad aislada tradicional plantea problemas a las organizaciones, ya que introduce brechas de seguridad, aumenta la sobrecarga de los equipos de seguridad y obstaculiza la productividad de la empresa con un acceso y una visibilidad inconstantes.

Nuestros servicios de seguridad en la nube, que están perfectamente integrados con nuestros NGFW líderes del sector, utilizan el efecto de la red de 80.000 clientes para coordinar instantáneamente la información y proporcionar protección contra todas las amenazas en todos los vectores. Elimine las brechas de cobertura en todas sus ubicaciones y aproveche la seguridad de la más alta calidad suministrada de forma constante en una plataforma, para poder estar a salvo incluso de las amenazas más avanzadas y evasivas. Los servicios incluyen:

- **Advanced Threat Prevention**: Detenga los exploits conocidos, el malware, el spyware y las amenazas de comando y control (C2) a la vez que utiliza la primera prevención del sector de ataques de día cero: evite un 60 % más de ataques de inyección desconocidos y un 48 % más de tráfico de comando y control altamente evasivo que las soluciones IPS tradicionales.
- **WildFire avanzado**: Garantice la seguridad de los archivos previniendo automáticamente el malware conocido, desconocido y altamente evasivo 60 veces más rápido con el mayor motor de inteligencia de amenazas y prevención de malware del sector.
- **Advanced URL Filtering**: Garantice un acceso seguro a Internet y evite un 40 % más de ataques basados en Internet con la primera prevención en tiempo real de amenazas conocidas y desconocidas del sector, que detiene el 88 % de las URL malintencionadas al menos 48 horas antes que otros proveedores.
- **DNS Security**: Obtenga un 40 % más de cobertura frente a amenazas y detenga el 85 % del malware que utilizan el DNS para ataques de comando y control y el robo de datos sin necesidad de realizar cambios en su infraestructura.

- **Enterprise DLP**: Minimice el riesgo de una filtración de datos, detenga las transferencias de datos fuera de política y permita el cumplimiento normativo de forma sistemática en toda la empresa, con una cobertura dos veces mayor que la de cualquier DLP empresarial en la nube.
- **SaaS Security**: Adelántese a la explosión de SaaS con el único Cloud Access Security Broker (CASB, agente de seguridad de acceso a la nube) de nueva generación del sector para ver y proteger automáticamente todas las aplicaciones en todos los protocolos.
- **IoT Security**: Proteja cada "cosa" e implemente seguridad de dispositivos de Confianza Cero 20 veces más rápido con la seguridad más inteligente del sector para dispositivos inteligentes.

Un enfoque exclusivo para el procesamiento de paquetes con arquitectura de paso único

- Lleva a cabo la conexión de redes, la búsqueda de políticas, la aplicación, la decodificación y la comparación de firmas para todas las amenazas y el contenido en un solo paso. Esto reduce en gran medida la sobrecarga de procesamiento necesaria para realizar varias funciones en un solo dispositivo de seguridad.
- Evita la introducción de latencia mediante el escaneo del tráfico para todas las firmas en un único paso mediante la comparación de firmas uniforme basada en flujos.
- Permite un rendimiento predecible y constante cuando se habilitan las suscripciones de seguridad. (En la Tabla 1, el "Rendimiento de Threat Prevention" se mide con varias suscripciones habilitadas).

Habilitación de la funcionalidad SD-WAN

- Permite la adopción simple de SD-WAN mediante su habilitación en los firewalls existentes.
- Permite la implementación de SD-WAN de manera segura, la integración de forma nativa con nuestra seguridad líder en el sector.
- Ofrece una experiencia excepcional para el usuario final al minimizar la latencia, la fluctuación y la pérdida de paquetes.

Tabla 1: Rendimiento y capacidad de PA-3200 Series

	PA-3220	PA-3250	PA-3260
Rendimiento del firewall (HTTP/Appmix)*	3,7/4,2 Gbps	4,6/5,0 Gbps	6,9/7,8 Gbps
Rendimiento de Threat Prevention (HTTP/Appmix)†	1,9/2,3 Gbps	2,4/2,7 Gbps	3,6/4,3 Gbps
Rendimiento de VPN IPSec‡	2,4 Gbps	2,6 Gbps	4,4 Gbps
Sesiones máximas	1 millón	2 millones	2,2 millones
Sesiones nuevas por segundo§	46000	58000	84000
Sistemas virtuales (base/máx)||	1/6	1/6	1/6

Nota: Los resultados se midieron en PAN-OS 11.0.

* El rendimiento del firewall se mide con App-ID y registros habilitados, mediante el uso de transacciones HTTP/AppMix de 64 KB.
† El rendimiento de Threat Prevention se mide con App-ID, IPS, antivirus, antispyware, WildFire, DNS Security, bloqueo de archivos y registros habilitados mediante el uso de transacciones HTTP/appmix de 64 KB.
‡ El rendimiento de VPN IPSec se mide mediante el uso de transacciones HTTP de 64 KB y registros habilitados.
§ Las nuevas sesiones por segundo se miden mediante la cancelación de la aplicación que utiliza transacciones HTTP de 1 byte.
|| La incorporación de sistemas virtuales por encima de la cantidad base requiere una licencia adquirida por separado.

Tabla 2: Funciones de red de PA-3200 Series

Modos de interfaz
L2, L3, tap, virtual wire (modo transparente)
Enrutamiento
OSPFv2/v3 con reinicio cuidadoso, BGP con reinicio cuidadoso, RIP, enrutamiento estático
Policy-based forwarding (reenvío basado en políticas - PBF)
Protocolo punto a punto sobre Ethernet (PPPoE)
Multidifusión: PIM-SM, PIM-SSM, IGMP v1, v2 y v3
SD-WAN
Medición de la calidad de ruta (fluctuación, pérdida de paquetes, latencia)
Selección de ruta inicial (PBF)
Cambio dinámico de ruta
IPv6
L2, L3, tap, virtual wire (modo transparente)
Funciones: App-ID, User-ID, Content-ID, WildFire y descifrado de SSL
SLAAC

Tabla 2: Funciones de red de PA-3200 Series (continuación)
IPSec VPN
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, SHA-512
VLAN
Etiquetas VLAN 802.1Q por dispositivo/por interfaz: 4094/4094
Interfaces agregadas (802.3ad), LACP
Network address translation (traducción de dirección de red - NAT)
Modos NAT (IPv4): IP estática, IP dinámica, IP y puerto dinámicos (traducción de direcciones de puertos)
NAT64, NPTv6
Funciones adicionales de la NAT: reserva de IP dinámica, IP y puerto dinámicos con túnel y sobresuscripción
Alta disponibilidad
Modos: activo/activo, activo/pasivo, clúster de HA
Detección de fallas: monitoreo de rutas, supervisión de interfaz
Aprovisionamiento cero táctil (ZTP)
Disponible con SKU ZTP (PA-3260-ZTP, PA-3250-ZTP, PA-3220-ZTP). Requiere Panorama 9.1.3 o posterior

Tabla 3: Especificaciones del hardware de PA-3200 Series
E/S
PA-3220: 10/100/1000 (12), 1G SFP (4), 1G/10G SFP/SFP+ (4)
PA-3250: 10/100/1000 (12), 1G/10G SFP/SFP+ (8)
PA-3260: 10/100/1000 (12), 1G/10G SFP/SFP+ (8), 40G QSFP+ (4)
E/S de gestión
Puerto de gestión fuera de banda 10/100/1000 (1), alta disponibilidad 10/100/1000 (2), alta disponibilidad 10G SFP+ (1), puerto de consola RJ-45 (1), Micro USB (1)
Capacidad de almacenamiento
SSD de 240 GB
Fuente de alimentación (consumo de energía promedio/máximo)
CA o CC redundante de 650 vatios (195/240)
BTU/h máximo
819
Tensión de entrada (frecuencia de entrada)
CA: De 100 a 240 V CA (de 50 a 60 Hz)
CC: De -48 V a -60 V
Consumo de corriente máximo
CA: 2,3 A a 100 V CA, 1,0 A a 240 V CA
CC: -48 V a 4,7 A, -60 V a 3,8 A
Mean time between failures (tiempo medio entre fallos - MTBF)
14 años
Montaje en rack (dimensiones)
2U, rack estándar de 19" (48,26 cm) (3,5" de alto x 20,53" de prof. x 17,34" de ancho [8,89 cm de alto x 52,15 cm de prof. x 44,04 cm de ancho])
Peso (solo dispositivo/dispositivo preparado para envío)
29 lb/ 41,5 lb (13,15 kg/23,36 kg)
Seguridad
cTUVus, CB
EMI
Clase A FCC, Clase A CE, Clase A VCCI

Tabla 3: Especificaciones del hardware de la serie PA-3200 (continuación)
Certificaciones
Consulte paloaltonetworks.com/company/certifications.html
Entorno
Temperatura operativa: de 32 °F a 122 °F, de 0 °C a 50 °C
Temperatura no operativa: de -4 °F a 158 °F, de -20 °C a 70 °C
Tolerancia a la humedad: Entre 10 % y 90 %
Altitud máxima: 10.000 ft/3048 m
Flujo de aire: de adelante hacia atrás

3000 Tannery Way
Santa Clara, CA 95054

Teléfono principal: +1.408.753.4000
Teléfono de Ventas: +1.866.320.4788
Teléfono de Asistencia: +1.866.898.9087

www.paloaltonetworks.com