

Características destacadas

- Intervalo ampliado de la temperatura de funcionamiento.
- Certificación conforme a los estándares IEC 61850-3 e IEEE 1613 de requisitos ambientales y de pruebas en lo que respecta a vibración, temperatura e inmunidad ante las interferencias electromagnéticas.
- Alimentación CC doble (12-48 V).
- Configuración del cortafuegos de alta disponibilidad (activo/activo y activo/pasivo).
- Diseño sin ventilador y sin partes móviles.
- E/S flexible compatible con cables de cobre y de fibra a través de puertos SFP.
- Opciones de montaje flexible: incluidos carril DIN, bastidor y soporte de pared.
- Implementación en sitios remotos simplificada mediante arranque basado en USB.

PA-220R

PA-220R de Palo Alto Networks es un robusto cortafuegos de nueva generación que incorpora las capacidades de los cortafuegos de nueva generación a las aplicaciones industriales en entornos extremos.



PA-220R

El robusto dispositivo PA-220R protege redes industriales y de defensa en una amplia gama de entornos extremos, como subestaciones de servicios públicos, centrales eléctricas, plantas de fabricación, instalaciones de petróleo y gas, sistemas de gestión de edificios y redes sanitarias.

El elemento de control del PA-220R Series es PAN-OS®, 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 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.

Principales funciones de seguridad y conectividad

Clasifica todas las aplicaciones, en todos los puertos, en todo momento

- Emplea los App-ID para protocolos y aplicaciones industriales como Modbus, DNP3, IEC 60870-5-104, Siemens S7, OSIsoft PI®, etc.
- Identifica la aplicación independientemente del puerto, el tipo de cifrado (SSL o SSH) o la técnica de evasión empleada.
- 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.
- Clasifica por categorías las aplicaciones no identificadas, lo que facilita el control de políticas, la investigación forense de amenazas o el desarrollo de la tecnología App-ID™.
- Proporciona visibilidad completa de los detalles de todas las conexiones cifradas con TLS y detiene las amenazas ocultas en el tráfico cifrado, incluido el tráfico que utilizan los protocolos TLS 1.3 y HTTP/2.

Aplica políticas de seguridad para cualquier usuario y en cualquier ubicación

- Implementa políticas coherentes a usuarios locales y remotos que trabajan en plataformas de Windows®, macOS®, Linux, Android® o iOS de Apple.

- Permite la integración sin agentes de Active Directory® y Terminal Services de Microsoft, LDAP, Novell eDirectory™ y Citrix.
- Integra fácilmente sus políticas de cortafuegos con el estándar 802.1X inalámbrico, los servidores proxy, el control de acceso a la red y cualquier otra fuente de información sobre la identidad del usuario.

Amplía la protección nativa frente a todos los vectores de ataque con suscripciones de seguridad basadas en la nube

- **Prevención de amenazas:** inspecciona todo el tráfico para bloquear automáticamente las vulnerabilidades conocidas, el malware, los exploits, el spyware, el malware mando y control (C2) y las firmas del sistema de prevención de intrusos (IPS) personalizado.
- **WildFire® malware prevention:** protege contra amenazas desconocidas basadas en archivos, proporcionando prevención automatizada en segundos para la mayoría de las nuevas amenazas en redes, endpoints y nubes.
- **Filtrado de URL:** impide el acceso a sitios mal intencionados y protege a los usuarios contra las amenazas basadas en web.
- **Seguridad de DNS:** detecta y bloquea las amenazas conocidas y desconocidas sobre DNS, mientras que el análisis predictivo interrumpe los ataques que utilizan DNS para el mando y control (C2) o el robo de datos.
- **Seguridad de IdC:** descubre todos los dispositivos no gestionados en su red, identifica riesgos y vulnerabilidades, y automatiza las políticas de cumplimiento para su cortafuegos de nueva generación utilizando un nuevo sistema de políticas Device-ID™.

Habilita la funcionalidad de SD-WAN

- Le permite incorporar fácilmente una red SD-WAN con solo habilitarla en los cortafuegos existentes.
- Le permite implementar SD-WAN de forma segura, integrada 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 capacidades de PA-220R¹

Rendimiento del cortafuegos (HTTP/combinación de aplicaciones) ²	575/540 Mb/s
Rendimiento de Threat Prevention (HTTP/combinación de aplicaciones) ³	275/320 Mb/s
Rendimiento de VPN de IPsec	540 Mb/s
Número máximo de sesiones	64.000
Número de sesiones nuevas por segundo ⁵	4.300

1. Los resultados se midieron con PAN-OS 10.0.
2. El rendimiento del cortafuegos se calcula con App-ID y la creación de logs activados usando transacciones HTTP/combinación de aplicaciones de 64 kB.
3. 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 HTTP/combinación de aplicaciones de 64 kB.
4. El rendimiento de VPN IPsec se calcula con transacciones HTTP de 64 kB y la creación de logs activada.
5. El cálculo de las nuevas sesiones por segundo se realiza con cancelación de aplicación usando transacciones HTTP de 1 byte.

La serie PA-220R es compatible 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 PA-220R

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)
Multicast: PIM-SM, PIM-SSM, IGMP versiones 1, 2 y 3
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)
Características: App-ID, User-ID, Content-ID, WildFire y descifrado SSL
SLAAC

Tabla 2: Funciones de red de PA-220R (Continuación)

VPN IPsec
Intercambio de claves: clave manual, IKEv1 y IKEv2 (clave precompartida y 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: 4.094/4.094
Traducción de direcciones de red (NAT)
Modos de NAT (IPv4): IP estática, IP dinámica, IP dinámica y puerto (traducción de direcciones de puerto)
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 fallos: supervisión de rutas y supervisión de interfaz
Protocolos y aplicaciones industriales
paloaltonetworks.com/resources/whitepapers/app-ids-industrial-control-systems-scada-networks
Aprovisionamiento sin contacto (ZTP)
Disponible con los SKU -ZTP (PA-220R-ZTP)
Requiere Panorama 9.1.3 o superior

Tabla 3: Especificaciones de hardware del PA-220R

E/S
10/100/1000 (6), SFP (2)
Gestión de E/S
Puerto de gestión fuera de banda 10/100/1000 (1)
puerto de consola RJ-45 (1)
Puerto USB (1)
Puerto de consola micro-USB (1)
Capacidad de almacenamiento
32 GB en eMMC

Tabla 3: Especificaciones de hardware del PA-220R (Continuación)

Fuente de alimentación (consumo de energía medio/máx.)
Opcional: Sistema de alimentación de CC redundante doble (13 W/16 W)
BTU/h máximo
55
Tensión de entrada (frecuencia de entrada)
12-48 V CC, 1,4 A, 50-60 Hz.
Consumo máximo de corriente
Cortafuegos: 1,4 A a 12 V CC Corriente máxima de entrada: 4,9 A a 12 V CC
Dimensiones
5,1 cm (alt.) x 22 cm (prof.) x 23,5 cm (an.) Opciones de montaje flexible: incluidos carril DIN, bastidor y soporte de pared.
Peso (solo dispositivo/preparado para envío)
2,0 kg/2,7 kg
Seguridad
cTUVus, CB
Interferencia electromagnética
Clase A de FCC, Clase A de CE y Clase A de VCCI
Certificaciones
Estándares de requisitos ambientales y de pruebas IEC 61850-3 e IEEE 1613. Para más certificaciones, consulte paloaltonetworks.com/company/certifications.html .
Entorno
Temperatura de funcionamiento: de -40 a 70 °C (de -40 a 158 °F) Temperatura de almacenamiento: de -40 a 75 °C (de -40 a 167 °F) Refrigeración pasiva

Para obtener más información acerca de las funciones y capacidades asociadas del PA-220R, visite paloaltonetworks.com/network-security/next-generation-firewall/pa-220r.