

# PA-500

## Características principales del firewall de nueva generación PA-500:

### CLASIFICACIÓN DE LA TOTALIDAD DE LAS APLICACIONES, EN TODOS LOS PUERTOS, EN TODO MOMENTO CON APP-ID™.

- Identificación de la aplicación, independientemente del puerto, el tipo de cifrado (SSL o SSH) o la técnica evasiva empleada.
- Utilización de la aplicación, no del puerto, como base para todas las decisiones sobre políticas de habilitación segura: permitir, denegar, programar, inspeccionar, aplicar control de tráfico.
- Clasificación de las aplicaciones no identificadas por medio de políticas, investigación forense de amenazas, creación personalizada de App-ID o captura de paquetes para investigaciones posteriores.

### PROPAGACIÓN DE LAS POLÍTICAS DE HABILITACIÓN SEGURA DE APLICACIONES A CUALQUIER USUARIO, EN CUALQUIER UBICACIÓN, CON USER-ID™ Y GLOBALPROTECT™.

- Integración sin agente con Active Directory, LDAP, eDirectory Citrix y Microsoft Terminal Services.
- Integración con NAC, redes inalámbricas y otros repositorios de usuarios no estándar a través de una API XML.
- Implementación de políticas coherentes a usuarios en plataformas Microsoft Windows, Mac OS X, Linux, Android o iOS independientemente de su ubicación.

### PROTECCIÓN CONTRA TODAS LAS AMENAZAS, TANTO CONOCIDAS COMO DESCONOCIDAS, CON CONTENT-ID™ Y WILDFIRE™.

- Bloqueo de una amplia gama de amenazas conocidas, como exploits, malware y spyware, en todos los puertos, independientemente de las tácticas comunes de evasión de amenazas utilizadas.
- Limitación de la transferencia no autorizada de archivos y datos sensibles, así como control de la navegación web no relacionada con el trabajo.
- Identificación de malware desconocido, análisis de más de 100 comportamientos maliciosos, así como la generación y distribución de protección automática en la siguiente actualización disponible.



PA-500

El PA-500 de Palo Alto Networks™ está destinado a implementaciones de firewalls de alta velocidad en delegaciones de empresas y en organizaciones medianas. El PA-500 gestiona el flujo de tráfico de red utilizando recursos de computación dedicados para el networking, la seguridad, la prevención de amenazas y la gestión.

El backplane de alta velocidad está dividido en un plano para datos y otro para control, garantizando siempre la disponibilidad del acceso a la gestión independientemente de la carga de tráfico. El elemento de control del firewall de nueva generación PA-500 es PAN-OS™, un sistema operativo orientado específicamente a la seguridad que permite a las organizaciones la habilitación segura de aplicaciones utilizando App-ID, User-ID, Content-ID, GlobalProtect y WildFire.

RENDIMIENTO Y CAPACIDAD <sup>1</sup>	PA-500
Rendimiento del firewall (con función App-ID)	250 Mbps
Rendimiento de la prevención contra amenazas	100 Mbps
Rendimiento de VPN IPSec	5 0 Mbps
Número de sesiones nuevas por segundo	7.500
Número máximo de sesiones	64.000
Interfaces de túnel/túneles VPN IPSec	250
Usuarios simultáneos GlobalProtect (SSL VPN)	100
Sesiones de descifrado SSL	1.000
Certificados para SSL entrante	25
Routers virtuales	3
Zonas de seguridad	20
Número máximo de políticas	1.000

<sup>1</sup> El rendimiento y la capacidad se miden en condiciones de prueba ideales usando PAN-OS 5.0.

Para una descripción completa de las características del firewall de nueva generación PA-500, visite [www.paloaltonetworks.com/literature](http://www.paloaltonetworks.com/literature).

**ESPECIFICACIONES DEL HARDWARE****E/S**

- (8) 10/100/1000

**GESTIÓN DE E/S**

- (1) puerto de administración fuera de banda 10/100/1000,  
(1) puerto de consola RJ-45

**CAPACIDAD DE ALMACENAMIENTO**

- Unidad de estado sólido (SSD) de 160 GB

**FUENTE DE ALIMENTACIÓN (CONSUMO ELÉCTRICO MEDIO/MÁXIMO)**

- 180 W (40 W / 75 W)

**BTU/H MÁXIMO**

- 256

**VOLTAJE DE ENTRADA (FRECUENCIA DE ENTRADA)**

- 100-240 VAC (50-60 Hz)

**CONSUMO MÁXIMO DE CORRIENTE**

- 1 A a 100 VAC

**TIEMPO MEDIO ENTRE FALLOS (MTBF)**

- 10,16 años

**CORRIENTE MÁXIMA DE ENTRADA**

- 110 A a 230 VAC; 51 A a 115 VAC

**PREPARADO PARA MONTAJE EN BASTIDOR (DIMENSIONES)**

- 1U, bastidor estándar de 19"  
(4,45 x 25,4 x 43,18 cm – 1,75 x 10 x 17 pulgadas)

**DIMENSIONES (SOLO DISPOSITIVO/DISPOSITIVO PREPARADO PARA ENVÍO)**

- 3,63 Kg / 5,90 Kg

**SEGURIDAD**

- UL, CUL, CB

**INTERFERENCIA ELECTROMAGNÉTICA**

- Clase A de FCC, Clase A de CE, Clase A de VCCI, TUV

**CERTIFICACIONES**

- FIPS 140 nivel 2, ICSA, UCAPL

**ENTORNO**

- Temperatura de funcionamiento: De 0 a 50 °C (de 32 a 122 °F)
- Temperatura de almacenamiento: De -20 a 70 °C (de -4 a 158 °F)

**CONEXIÓN A RED****MODOS DE LOS INTERFACES**

- L2, L3, Tap, Virtual Wire (modo transparente)

**ENRUTAMIENTO**

- Modos: OSPF, RIP, BGP, estático
- Tamaño de la tabla de reenvío (entradas por dispositivo/por VR):  
1.250/1.250
- Reenvío basado en políticas
- Protocolo punto a punto sobre Ethernet (PPPoE)
- Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, y v3

**ALTA DISPONIBILIDAD**

- Modos: Activo/Activo, Activo/Pasivo
- Detección de fallos: monitorización de ruta, monitorización de interfaz

**ASIGNACIÓN DE DIRECCIONES**

- Asignación de direcciones por dispositivo: cliente DHCP/PPPoE/ Estática
- Asignación de direcciones por usuarios: servidor DHCP/Relay DHCP/Estática

**IPv6**

- L2, L3, Tap, Virtual Wire (modo transparente)
- Funciones: App-ID, User-ID, Content-ID, WildFire y descifrado SSL

**VLAN**

- Etiquetas VLAN 802.1q por dispositivo / por interfaz: 4.094/4.094
- Número máximo de interfaces: 250
- Interfaces de agregado (802.3ad)

**NAT/PAT**

- Número máximo de reglas NAT: 125
- Número máximo de reglas NAT (DIPP): 125
- Intervalo de direcciones IP y puertos dinámicos: 254
- Intervalo de direcciones IP dinámicas: 16.234
- Modos NAT: NAT 1:1, NAT n:n, NAT m:n
- Sobresuscripción DIPP (direcciones IP de destino único por dirección IP y puerto de origen): 1
- NAT64

**VIRTUAL WIRE**

- Número máximo de Virtual Wires: 125
- Tipos de interfaz asignados a Virtual Wires: físicos y subinterfaces

**REENVÍO DE NIVEL 2**

- Tamaño de tabla ARP por dispositivo: 500
- Tamaño de tabla MAC por dispositivo: 500
- Tamaño de tabla de vecino de IPv6: 500

## SEGURIDAD

### FIREWALL

- Control de las aplicaciones, los usuarios y los contenidos basado en políticas
- Protección de paquetes fragmentados
- Protección de escaneos de reconocimiento
- Protección frente a denegación de servicio (DoS) y denegación de servicio distribuido (DDoS)
- Descifrado: SSL (entrante y saliente), SSH

### WILDFIRE

- Identifica y analiza archivos específicos y desconocidos pudiendo reconocer más de 100 conductas maliciosas.
- Genera y ofrece una protección automática contra malware recién descubierto a través de actualizaciones de firmas.
- Distribución de actualizaciones de firmas en menos de 1 hora. Logging y generación de informes integrado. Acceso a la API de WildFire para el envío programado de hasta 100 muestras al día y de hasta 250 consultas al día de informes por archivo hash (se requiere suscripción).

### FILTRADO DE ARCHIVOS Y DATOS

- Transferencia de archivos: control bidireccional sobre más de 60 tipos de archivo únicos
- Transferencia de datos: control bidireccional sobre la transferencia no autorizada de números de tarjetas de crédito y seguridad social
- Protección contra descargas "drive-by download".

### INTEGRACIÓN DE USUARIOS (USER-ID)

- Microsoft Active Directory, Novell eDirectory, Sun One y otros directorios basados en LDAP
- Microsoft Windows Server 2003/2008/2008r2, Microsoft Exchange Server 2003/2007/2010
- Microsoft Terminal Services, Citrix XenApp
- API XML para facilitar la integración con repositorios de usuario no estándar

### VPN IPSEC (SITE-TO-SITE)

- Intercambio de claves: clave manual, IKE v1
- Cifrado: 3DES, AES (128 bits, 192 bits, 256 bits)
- Autenticación: MD5, SHA-1, SHA-256, SHA-384, SHA-512
- Creación de túneles VPN dinámicos (GlobalProtect)

### PREVENCIÓN DE AMENAZAS (SE REQUIERE SUSCRIPCIÓN)

- Protección contra exploits de vulnerabilidades del sistema operativo y de aplicaciones
- Protección basada en flujos contra virus, spyware y gusanos (incluidos los incrustados en HTML, Javascript, archivos PDF y archivos comprimidos)

### FILTRADO DE URL (SE REQUIERE SUSCRIPCIÓN)

- Categorías de URL predefinidas y personalizadas
- Memoria caché para las URL a las que se ha accedido recientemente
- Categorías de URL como parte del criterio de coincidencia de las políticas de seguridad
- Información del tiempo de navegación

### CALIDAD DEL SERVICIO (QOS)

- Control del tráfico basado en políticas por aplicación, usuario, origen, destino, interfaz, túnel de VPN IPsec, etc.
- 8 clases de tráfico con parámetros de ancho de banda garantizado, máximo y prioritario
- Supervisión de ancho de banda en tiempo real
- Por marcado de Diffserv de política
- Interfaces físicas compatibles con QoS: 4

### VPN/ACCESO REMOTO SSL (GLOBALPROTECT)

- Gateway GlobalProtect
- Portal GlobalProtect
- Transporte: IPsec con SSL fall-back
- Autenticación: LDAP, SecurID o base de datos local
- Sistema operativo cliente: Mac OS X 10.6, 10.7 (32/64 bits), 10.8 (32/64 bits), Windows XP, Windows Vista (32/64 bits), Windows 7 (32/64 bits)
- Soporte de cliente de terceros: Apple iOS, Android 4.0 y posterior, VPNC IPsec para Linux

### ADMINISTRACIÓN, GENERACIÓN DE INFORMES, HERRAMIENTAS DE VISIBILIDAD

- Interfaz web integrada, CLI o administración central (Panorama)
- Interfaz de usuario en varios idiomas
- Syslog, Netflow v9 y SNMP v2/v3
- REST API basada en XML
- Resumen gráfico de aplicaciones, categorías de URL, amenazas y datos (ACC)
- Visualizar, filtrar y exportar tráfico, amenazas, WildFire, URL y logs de filtrado de datos
- Generación de informes totalmente personalizable

Para una descripción completa de las características del firewall de nueva generación PA-500, visite [www.paloaltonetworks.com/literature](http://www.paloaltonetworks.com/literature).