

Serie VM

Características principales de los firewalls de nueva generación de la serie VM:

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

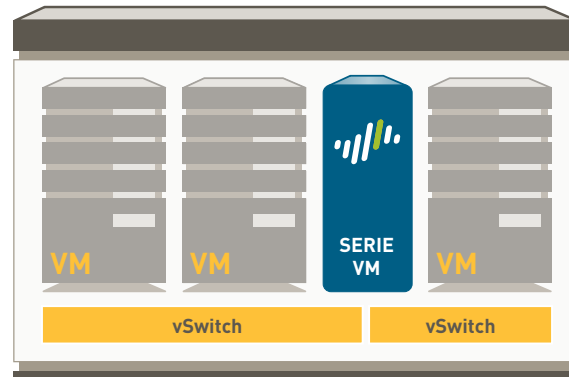
- Identificación de la aplicación, independientemente del puerto, el tipo de cifrado (SSL o SSH) o la técnica evasiva empleada.
- Utilización de la aplicación, no del puerto, como base para todas las decisiones sobre políticas de habilitación segura: permitir, denegar, programar, inspeccionar, aplicar 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, incluyendo el análisis de más de 100 comportamientos maliciosos, así como la generación y distribución de protección automática en la siguiente actualización disponible.



Firewall virtual VM-Series

La serie VM de Palo Alto Networks™ extiende la habilitación segura de aplicaciones a entornos virtualizados abordando los principales retos de seguridad de la virtualización: seguimiento de las políticas de seguridad con los movimientos de la máquina virtual, gracias al uso de objetos de dirección dinámica e integración con los sistemas de orquestación utilizando una potente API de administración XML.

La serie VM está compuesta por tres modelos de alto rendimiento: el VM-100, el VM-200 y el VM-300, utilizando todos ellos una arquitectura software de paso único para minimizar la latencia en entornos de datacenter. Los planos de control y de datos están separados de modo que los usuarios pueden asignar CPUs dedicadas a cada una de ellas como medio para garantizar el acceso permanente a la administración, independientemente de la carga de tráfico. El elemento de control de la serie VM 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.

CAPACIDAD ¹	VM-300	VM-200	VM-100
Número máximo de sesiones	250.000	100.000	50.000
Interfases de túnel/túneles VPN IPSec	2.000	500	25
Usuarios simultáneos GlobalProtect (SSL VPN)	500	200	25
Sesiones de descifrado SSL	1.024	1.024	1.024
Certificados para SSL entrante	25	25	25
Routers virtuales	3	3	3
Zonas de seguridad	40	20	10
Número máximo de políticas	5.000	2.000	250
Objetos de direcciones	10.000	4.000	2.500
ESPECIFICACIONES DE RENDIMIENTO ¹			
Rendimiento del firewall (con función App-ID)		1 Gbps	
Capacidad de prevención contra amenazas		600 Mbps	
Rendimiento de VPN IPSec		250 Mbps	
Número de sesiones nuevas por segundo		8.000	

¹ El rendimiento y la capacidad se miden en condiciones de prueba ideales usando PAN-OS 5.0 y 4 núcleos de CPU.

VIRTUALIZACIÓN

HyperVisor
 Controlador de red
 Núcleos de CPU
 Memoria (mínimo)
 Capacidad de la unidad de disco (Mín./Máx.)

VM-300	VM-200	VM-100
--------	--------	--------

VMware ESXi 4.1 y ESXi 5.0		
VMXNet3		
2, 4 u 8		
4 GB		
40 GB/2 TB		

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): 1000/1000
- Reenvío basado en políticas
- Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, y v3

ALTA DISPONIBILIDAD

- Modos: Activo/Pasivo sin sincronización de sesiones
- 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: 2.000 (VM-300), 500 (VM-200), 100 (VM-100)

NAT/PAT

- Número máximo de reglas NAT: 1.000 (VM-300), 1.000 (VM-200), 125 (VM-100)
- Número máximo de reglas NAT (DIPP): 200 (VM-300), 200 (VM-200), 125 (VM-100)
- Intervalo de direcciones IP y puertos dinámicos: 254
- Intervalo de direcciones IP dinámicas: 32,000
- 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): 2 (VM-300), 1 (VM-200), 1 (VM-100)
- NAT64

VIRTUAL WIRE

- Número máximo de Virtual Wires: 1.000 (VM-300), 250 (VM-200), 50 (VM-100)
- Tipos de interfaz asignados a Virtual Wires: físicos y subinterfaces

REENVÍO DE NIVEL 2

- Tamaño de tabla ARP por dispositivo: 2.500 (VM-300), 500 (VM-200), 500 (VM-100)
- Tamaño de tabla MAC por dispositivo: 2,500 (VM-300), 500 (VM-200), 500 (VM-100)
- Tamaño de tabla de vecinos IPV6: 1.000 (VM-300), 500 (VM-200), 500 (VM-100)

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 1.000 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 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 físicos soportados por QoS: 6 (VM-300, VM-200), 4 (VM-100)

VPN/ACCESO REMOTO SSL (GLOBALPROTECT)

- Gateway GlobalProtect
- Portal GlobalProtect
- Transporte: IPsec con fall-back SSL
- 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 registros de filtrado de datos
- Generación de informes totalmente personalizable

Para una descripción completa de las características de los firewalls de nueva generación de la serie VM, visite www.paloaltonetworks.com/literature.