
paloalto
NETWORKS

Plataformas de cortafuegos

Palo Alto Networks ofrece una completa línea de dispositivos de seguridad de nueva generación, desde la serie PA-200, diseñada para oficinas remotas de una empresa, hasta la serie PA-7050, que es un chasis modular diseñado para centros de datos de alta velocidad. Nuestra arquitectura de plataforma se basa en un motor de software de única pasada y utiliza el procesamiento por funciones para el acceso a la red, la seguridad, la prevención de amenazas y la gestión para ofrecer unos resultados predecibles. Las mismas funciones de cortafuegos de los dispositivos de hardware están disponibles también en los cortafuegos virtuales de la serie VM, con lo que podrá mantener seguros sus entornos virtualizados y de informática basada en la nube utilizando las mismas políticas aplicadas a su perímetro o a cortafuegos de oficinas remotas.

PA-3050

- Rendimiento de firewall a 4 Gbps (con función App-ID[1])
- Rendimiento de la prevención de amenazas a 2 Gbps
- Rendimiento de VPN basada en IPSec a 500 Mbps
- 500.000 sesiones máximas
- 50.000 nuevas sesiones por segundo
- 2.000 interfaces de túnel/túneles de VPN basada en IPSec
- 2.000 usuarios VPN SSL
- 10 enrutadores virtuales
- 1/6 sistemas virtuales (base/máx.[2])
- 40 zonas de seguridad
- 5.000 políticas como máximo

PA-3020

- Rendimiento de firewall a 2 Gbps (con función App-ID[1])
- Rendimiento de la prevención de amenazas a 1 Gbps
- Rendimiento de VPN basada en IPSec a 500 Mbps
- 250.000 sesiones máximas
- 50.000 nuevas sesiones por segundo
- 1.000 interfaces de túnel/túneles de VPN basada en IPSec
- 1.000 usuarios VPN SSL
- 10 enrutadores virtuales
- 1/6 sistemas virtuales (base/máx.[2])
- 40 zonas de seguridad
- 2.500 políticas como máximo

PA-200

- Rendimiento de firewall a 100 Mbps (con función App-ID[1])
- Rendimiento de la prevención de amenazas a 50 Mbps
- Rendimiento de VPN basada en IPSec a 50 Mbps
- 64.000 sesiones máximas
- 1.000 nuevas sesiones por segundo
- 25 interfaces de túnel/túneles de VPN basada en IPSec
- 25 usuarios VPN SSL
- 10 zonas de seguridad
- 250 políticas como máximo

PA-500

- Rendimiento de firewall a 250 Mbps (con función App-ID[1])
- Rendimiento de la prevención de amenazas a 100 Mbps
- Rendimiento de VPN basada en IPSec a 50 Mbps
- 64.000 sesiones máximas
- 7.500 nuevas sesiones por segundo
- 250 interfaces de túnel/túneles de VPN basada en IPSec
- 100 usuarios VPN SSL
- 3 enrutadores virtuales
- Sistemas virtuales (base/máx.) no disponibles
- 20 zonas de seguridad
- 1.000 políticas como máximo

PA-5060

- Rendimiento de firewall a 20 Gbps (con función App-ID[1])
- Rendimiento de la prevención de amenazas a 10 Gbps
- Rendimiento de VPN basada en IPSec a 4 Gbps
- 4.000.000 sesiones máximas
- 120.000 nuevas sesiones por segundo
- 8.000 interfaces de túnel/túneles de VPN basada en IPSec
- 20.000 usuarios VPN SSL
- 225 enrutadores virtuales
- 25/225 sistemas virtuales (base/máx.[2])
- 900 zonas de seguridad
- 40.000 políticas como máximo

PA-5050

- Rendimiento de firewall a 10 Gbps (con función App-ID[1])
- Rendimiento de la prevención de amenazas a 5 Gbps
- Rendimiento de VPN basada en IPSec a 4 Gbps
- 2.000.000 sesiones máximas
- 120.000 nuevas sesiones por segundo
- 4.000 interfaces de túnel/túneles de VPN basada en IPSec
- 10.000 usuarios VPN SSL
- 125 enrutadores virtuales
- 25/125 sistemas virtuales (base/máx.[2])
- 500 zonas de seguridad
- 20.000 políticas como máximo

PA-5020

- Rendimiento de firewall a 5 Gbps (con función App-ID[1])
- Rendimiento de la prevención de amenazas a 2 Gbps
- Rendimiento de VPN basada en IPSec a 2 Gbps
- 1.000.000 sesiones máximas
- 120.000 nuevas sesiones por segundo
- 2.000 interfaces de túnel/túneles de VPN basada en IPSec
- 5.000 usuarios VPN SSL
- 20 enrutadores virtuales
- 10/20 sistemas virtuales (base/máx.[2])
- 80 zonas de seguridad
- 10.000 políticas como máximo

Firewalls virtualizados

La serie VM de Palo Alto Networks cuenta con tres modelos de firewall virtualizado de nueva generación: VM-100, VM-200 y VM-300. Estas plataformas son compatibles con VMware ESXi 4.1, 5.0 y 5.5, y las series SDX 11500 y 17550 de Citrix NetScaler.
Puede implementar la serie VM en servidores ESXi de entornos virtualizados o en la nube para la exploración del tráfico de servidor a servidor. La serie VM en Citrix NetScaler consolida las funciones de control de seguridad y aplicaciones para implementaciones con múltiples usuarios (unidad de negocio, propietario de la aplicación, cliente del proveedor del servicio) o como una solución completa para implementaciones de Citrix XenApp XenDesktop.
Se pueden asignar 2, 4 u 8 núcleos de CPU en sus plataformas de servidores virtualizados para el procesamiento de los firewalls de nueva generación. Con 4 núcleos de CPU en funcionamiento, la serie VM tiene un rendimiento a 1 Gbps con la función App-ID habilitada. Para garantizar que tiene acceso a la gestión cuando hay un tráfico denso, los planos de datos y de control se encuentran separados. Además, nuestra arquitectura de software de pasada única procesa funciones de una única pasada para reducir la latencia.

La serie VM en los servidores ESXi admite 10 interfaces de red virtuales mientras que la serie VM en Citrix NetScaler SDX admite 24 interfaces de red virtuales.
La serie VM se ejecuta en PAN-OS™, un sistema operativo diseñado para la seguridad que:

- Habilita de forma segura todas las aplicaciones, independientemente de los puertos, protocolos y tácticas evasivas
- Protege contra todas las amenazas conocidas y desconocidas
- Se integra de una forma flexible en el entorno virtualizado en las capas 1, 2, o 3

Las funciones de nuestro firewall de nueva generación de PAN-OS, como los grupos de direcciones dinámicas y la monitorización de las máquinas virtuales, le permitirán vincular sus políticas de seguridad a las ampliaciones, movimientos y cambios de las máquinas virtuales y crear políticas de seguridad que se sincronicen de forma instantánea con la creación de volumen de trabajo virtual.

VM-1000-HV

- 250,000 max sessions
- 2,000 IPSec VPN tunnels/tunnel interfaces
- 500 SSL VPN Users
- 40 security zones
- 10,000 max number of policies
- 10,000 address objects
- 1Gbps Firewall Throughput (App-ID enabled)*
- 600 Mbps Threat Prevention Throughput*
- 250 Mbps IPSec VPN Throughput*
- 8,000 New sessions per second*

VM-300

- 250,000 max sessions
- 2,000 IPSec VPN tunnels/tunnel interfaces
- 500 SSL VPN Users
- 40 security zones
- 5,000 max number of policies
- 10,000 address objects
- 1Gbps Firewall Throughput (App-ID enabled)*
- 600 Mbps Threat Prevention Throughput*
- 250 Mbps IPSec VPN Throughput*
- 8,000 New sessions per second*

VM-200

- 100,000 max sessions
- 500 IPSec VPN tunnels/tunnel interfaces
- 200 SSL VPN Users
- 20 security zones
- 2,000 max number of policies
- 4,000 address objects
- 1Gbps Firewall Throughput (App-ID enabled)*
- 600 Mbps Threat Prevention Throughput*
- 250 Mbps IPSec VPN Throughput*
- 8,000 New sessions per second*

Gestión centralizada

Panorama le ofrece la posibilidad de gestionar su red de firewalls desde una ubicación centralizada. Podrá visualizar todo el tráfico de su firewall, gestionar todas las cuestiones relacionadas con la configuración del dispositivo, aplicar políticas generales y generar informes sobre los patrones de tráfico y las incidencias de seguridad; todo ello desde una ubicación central. Panorama está disponible como dispositivo de gestión exclusivo o como máquina virtual.

M-100

M-100 le permite realizar la gestión y las funciones de logging de Panorama en un solo dispositivo o puede separar las funciones de una forma distribuida para un mayor rendimiento y ampliación.

DISPOSITIVO VIRTUAL

Panorama puede implementarse como un dispositivo virtual en VMware ESX(i), lo que le permite consolidar el espacio en los racks.

GP-100 for GlobalProtect Mobile Security Manager

GP-100

GlobalProtect Mobile Security Manager is available on the GP-100 platform, and provides device management, malware detection and shares device state information with GlobalProtect Gateway.

Plataforma WildFire

Los ataques informáticos actuales y las APT se basan en el sigilo, la persistencia y la evasión de las medidas de seguridad tradicionales durante el ciclo de vida del ataque. Palo Alto Networks ofrece un procedimiento integral que aprovecha la visibilidad única de nuestro firewall de nueva generación, en combinación con un entorno de análisis de malware basado en la nube en el que se puede ejecutar malware novedoso y desconocido para posteriormente ser identificado.

Puede utilizar de forma predeterminada la infraestructura de WildFire de Palo Alto Networks que se aloja de forma pública en la nube, con lo que permitirá a cualquier firewall de Palo Alto Networks añadir la función de detectar y bloquear malware desconocido. Sin embargo, si prefiere no utilizar servicios públicos en la nube, WF-500 le ofrece la posibilidad de implementar WildFire como una nube privada en su propia red.

Existe la opción de que múltiples firewalls utilicen un único dispositivo WF-500 parara analizar malware desconocido. De esta forma, podrá implementar un entorno virtual de gran tamaño para analizar el malware compartido a través de todos los firewalls, en vez de implementar un hardware de uso único en cada punto de entrada/salida y punto de presencia de red.

WF-500

Las organizaciones que prefieran no utilizar aplicaciones públicas en la nube por motivos de normativas y privacidad pueden implementar WildFire como una nube privada utilizando el WF-500.