Cortafuegos de nueva generación de Palo Alto Networks (serie PA-7000)

Debido a la expansión de los centros de datos, la segmentación de la red, la virtualización y las iniciativas de movilidad le obligan a replantearse cómo habilitar el acceso a las aplicaciones y los datos a la vez que protege su red contra una clase más sofisticada de amenazas avanzadas que eluden los mecanismos de seguridad tradicionales.

Los cortafuegos de última generación (NGFW) permiten organizaciones a escala empresarial y proveedores de servicios implementar la seguridad en entornos de alto rendimiento, como grandes centros de datos y gran ancho de banda perímetros de red.

Diseñado para manejar el crecimiento necesidades de rendimiento para aplicaciones, usuarios y datos generados por dispositivos, estos sistemas ofrecen increíbles rendimiento, capacidades de prevención para detener el ciberataques más

avanzados y de alto rendimiento descifrado para detener las amenazas que se esconden bajo el velo de encriptación.

Diseñado para maximizar el procesamiento de seguridad utilización de recursos y escalar automáticamente como nuevo el poder de cómputo está disponible, la serie PA-7000 ofrece simplicidad definida por un solo sistema enfoque de gestión y concesión de licencias.

La serie PA-7000 está impulsada por una arquitectura escalable con el fin de aplicar el tipo y volumen apropiados de potencia de procesamiento a las tareas funcionales clave de redes, seguridad y administración. La serie PA-7000 se administra como un único sistema unificado, lo que le permite dirigir fácilmente todos los recursos disponibles para proteger sus datos. El chasis de la serie PA-7000 distribuye de manera inteligente las demandas de procesamiento en tres subsistemas, cada uno con cantidades masivas de potencia informática y memoria dedicada: la(s) tarjeta(s) de procesamiento, la tarjeta de administración del conmutador y la tarjeta de registro dedicada.

Características de la serie PA-7000

- Incorpora el aprendizaje automático (ML) en el núcleo del firewall para proporcionar prevención de ataques sin firma en línea para ataques basados en archivos al mismo tiempo que identifica y detiene inmediatamente intentos de phishing nunca antes vistos.
- Aprovecha los procesos de aprendizaje automático basados en la nube.
- Utiliza análisis de comportamiento para detectar dispositivos de Internet de las cosas (IoT) y hacer recomendaciones de políticas; servicio entregado en la nube e integrado de forma nativa en NGFW.

- Automatiza las recomendaciones de políticas que ahorran tiempo y reducen la posibilidad de error humano.
- Identifica las aplicaciones que atraviesan su red independientemente del puerto, el protocolo, las técnicas evasivas o el cifrado (TLS/SSL).
- Utiliza la aplicación, no el puerto, como base para todas sus decisiones de política de habilitación segura: permitir, denegar, programar, inspeccionar y aplicar modelado de tráfico.
- Identifica todos los datos de carga dentro de la aplicación (por ejemplo, archivos y patrones de datos) para bloquear archivos maliciosos y frustrar los intentos de exfiltración de datos.
- Crea informes de uso de aplicaciones estándar y personalizados, incluidos informes de software como servicio (SaaS) que brindan información sobre todo el tráfico de SaaS autorizado y no autorizado en su red.
- Permite la migración segura de conjuntos de reglas de capa 4 heredadas a reglas basadas en App-ID con Policy Optimizer integrado, lo que le brinda un conjunto de reglas que es más seguro y más fácil de administrar.
- Inspecciona y aplica la política al tráfico cifrado con TLS/SSL, tanto entrante como saliente, incluido el tráfico que utiliza TLS 1.3 y HTTP/2.
- Ofrece una gran visibilidad del tráfico TLS, como la cantidad de tráfico cifrado, las versiones de TLS/SSL, conjuntos de cifrado y más, sin descifrar.
- Permite controlar el uso de protocolos TLS heredados, cifrados inseguros y certificados mal configurados para mitigar los riesgos.
- Facilita la implementación sencilla del descifrado y le permite usar registros integrados para solucionar problemas, como aplicaciones con certificados anclados.
- Le permite habilitar o deshabilitar el descifrado de manera flexible en función de la categoría de URL y 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.

- Le permite crear una copia del tráfico descifrado del cortafuegos (es decir, duplicación de descifrado) y enviarlo a las herramientas de recopilación de tráfico con fines forenses, históricos o de prevención de pérdida de datos (DLP).

Rendimiento y capacidades de la serie PA-7000

Table 1: PA-7000 Series Performance and Capacities

	PA-7080*	PA-7050*	PA-7000 DPC-A	PA-7000-100G-NPC-A
Firewall throughput (HTTP/appmix)†	610/687 Gbps	370/400 Gbps	73.8/83.1 Gbps	55.5/62.5 Gbps
Threat Prevention throughput (HTTP/appmix)§	342/405 Gbps	200/243 Gbps	38.5/46.3 Gbps	27.7/34.6 Gbps
IPsec VPN throughput‖	334 Gbps	200 Gbps	37.1 Gbps	28 Gbps
Max sessions	416M	245M	43M	32M
New sessions per second**	6M	4M	825,000	624,000
Virtual systems (base/max)††	25/225	25/225	–	–

Note: Results were measured on PAN-OS 10.1.

* Results in this column were derived from an optimum combination of PA-7000-DPC-A and PA-7000-100G-NPC-A cards populated in all available slots.

† Throughput is measured with App-ID and logging enabled, with 64 KB HTTP/appmix transactions.

§ Threat Prevention throughput measured with App-ID, IPS, antivirus, anti-spyware, WildFire, DNS Security, file blocking, and logging enabled, utilizing 64 KB HTTP/appmix transactions.

‖ IPsec VPN throughput is measured with 64 KB HTTP transactions, and logging enabled.

** New sessions per second is measured with application override, utilizing 1 byte HTTP transactions.

†† The base system includes 25 virtual systems at no cost, and up to 200 additional licenses may be purchased. The maximum number of virtual systems supported is 225.

Precio

Una estimación del precio es: comienza en **$300,000** para una configuración de hardware básica que admite un rendimiento de 20 Gbps. Se pueden agregar al chasis hasta 10 NPC, con un precio de **$150,000 cada uno** , lo que permite que el dispositivo de seguridad de la red se amplíe a 200 Gbps. En total, un PA-7080 completamente cargado costará **1,65 millones de dólares** sin suscripciones.