



Los usuarios hacen lo que quieren en la red, contrólelos...

Se ha confiado en los firewalls stateful para controlar el acceso a la red, pero esta tecnología tiene 15 años de haber sido creada y las aplicaciones han cambiado.

Las aplicaciones tradicionales cliente/servidor corriendo en puertos únicos permitían clasificarlas en base al tráfico. Las aplicaciones actuales evaden la detección de los firewalls existentes porque su diseño de protección está basado en el número de puerto TCP/UDP.

El tráfico web, por ejemplo, usa el Puerto 80 y el firewall debe permitir todo lo que aparenta ser tráfico web. Pero ¿se trata realmente de tráfico relacionado con el negocio (Skype, Webex, P2P, malware...)? ¿Web 2.0?

Otro ejemplo son las aplicaciones encriptadas SSL que corren en el puerto 443. Los firewalls existentes están ciegos ante el tráfico SSL encriptado.

Adicionalmente un gran número de aplicaciones han incorporado más técnicas evasivas como port hopping, tunneling, emulación de aplicaciones válidas, etc.

Como resultado de esto, los Responsables de IT no pueden identificar o controlar las aplicaciones que están corriendo en su red.

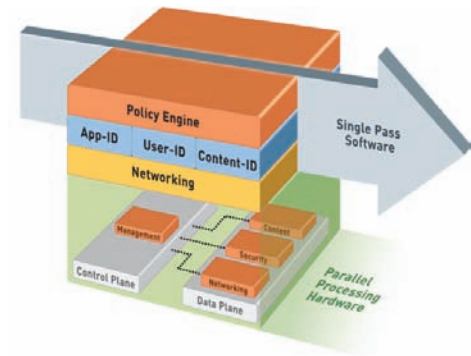
- Aumento de las amenazas: Malware, vulnerabilidades, fugas de información, pérdida de productividad.
- Aumento de los pasivos: Gran cantidad de cajas de seguridad, licencias, administradores, renovaciones.
- Aumento de costos: Incremento del consumo de ancho de banda en actividades basura, lentitud, caídas del sistema, sobre carga de las áreas técnicas, etc.

UTM no significa visibilidad y control.

Arquitectura SP3 (Single Pass Parallel Processing)



Los firewalls de nueva generación de Palo Alto Networks están basados en una arquitectura de procesamiento en paralelo de un solo paso (SP3) que entregan un alto rendimiento y seguridad a su red con baja latencia.

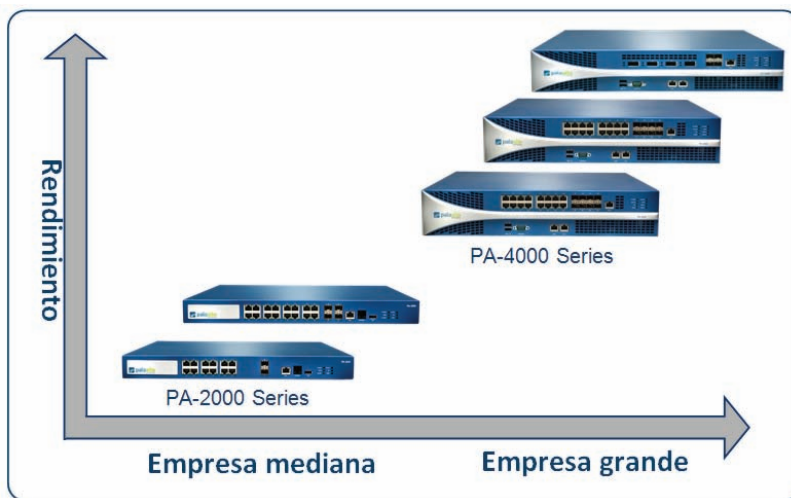


Solución de Palo Alto Networks



La serie Palo Alto Networks es un dispositivo de seguridad que permite:

1. Clasificar el tráfico basándose en la identificación exacta de la aplicación no sólo información de Puerto/Protocolo (AppID™ traffic classification technology)
2. Clasificar, controlar e inspeccionar aplicaciones y tráfico encriptadas (AppID™ traffic classification technology with SSL forward proxy).
3. Visualización gráfica de qué aplicaciones están corriendo en la red con información de usuario, grupo y red, categorizado, asimismo por sesiones, bytes, puertos, amenazas y tiempo (ACC – Application Command Center).
4. Protección en tiempo real con baja latencia contra virus, spyware y vulnerabilidades de aplicaciones gracias a un motor de prevención de amenazas (FlashMatch™ Real-Time Threat Prevention Engine).
5. Alto Rendimiento con baja latencia para toda clase de servicios, incluso bajo carga. (Hardware dedicado de procesamiento para seguridad, networking, prevención de ataques y gestión)
6. Tres diferentes opciones de implementación.
7. Reducción de costos capitales al reducir los pasivos y costos de operación provocados por un aumento



Esta combinación única de innovación en la tecnología y desempeño de la plataforma ayudaron a Palo Alto Networks a ganar el premio a lo mejor del Show Interop 2008, colocándose sobre más de 1,000 productos de otras 500 compañías de networking durante la exhibición.



Gartner también nombró a Palo Alto Networks como "Cool Company" del 2008. Y más de 200 clientes enterprise están ahora protegiendo sus redes con los Firewalls de Palo Alto Networks.

ITStrap

IT Solutions & Training Professionals, S.A. de C.V.

Para mayor información sobre Palo Alto Networks:

ITStrap - www.itstrap.net

Tel: 56-87-26-30

Email: paloaltonetworks@itstrap.net