Plataforma de Seguridad de Palo Alto Networks

Hoy día los departamentos de TI se enfrentan a una problemática creciente, con usuarios –tanto externos como internos- que utilizan una nueva generación de aplicaciones, capaces de evadir la detección que ofrecen los firewalls tradicionales. Las soluciones actuales de seguridad perimetral – firewalls – permiten establecer políticas de seguridad basadas fundamentalmente en puertos y protocolos. Hasta hace no mucho, esta aproximación era válida pues lo normal era que por el puerto 80 pasara sólo la navegación web y por el puerto 443, el tráfico SSL. Sin embargo, las nuevas aplicaciones de la Web 2.0 tales como Facebook, YouSendIt, Salesforce, Messenger, Skype, etc. se han convertido en un verdadero fenómeno social y su uso se ha extendido tanto en ámbitos privados como profesionales. Muchas de estas aplicaciones utilizan técnicas evasivas como port hopping, tunelización/emulación de otras aplicaciones, etc. para burlarse de las reglas tradicionales, basadas en puertos y protocolos. Muchas de ellas se esconden incluso bajo tráfico cifrado para ocultar su identidad.

Como resultado de todo ello, los responsables de TI no pueden identificar o controlar las aplicaciones que están corriendo realmente en la red y esta falta de visibilidad y control impacta negativamente en el negocio, generando:

- ✓ Incumplimiento de regulaciones y políticas internas
- ✓ Fuga de datos
- ✓ Incremento del consumo de ancho de banda
- ✓ Aumento de las amenazas (virus, spyware, worms y otras vulnerabilidades)
- ✓ Desaprovechamiento de los recursos (tanto humanos como de equipamiento)

Los responsables de TI necesitan por tanto una nueva aproximación, que les permita identificar con precisión las aplicaciones actuales, y no solamente los puertos que usan, a través de una inspección completa del tráfico.

La siguiente figura, muestra un ejemplo de la cantidad de aplicaciones de propósito muy diferente, que pueden circular a través de los puertos tradicionales (80 y 443). La mayoría de estas aplicaciones son “invisibles” para los firewalls de primera generación, que consideran que todo lo que llega por el puerto 80 se corresponde con tráfico HTTP (de navegación) y todo lo que circula por el 443 es SSL (navegación segura):

Figura 1.- Ejemplo de diversas aplicaciones sobre puertos 80 y/ó 443

Palo Alto Networks redefine el concepto de Firewall aportando un control y visibilidad sin precedentes, sobre todo el tráfico IP en las redes corporativas. Para conseguir este objetivo, se decidió diseñar un producto completamente nuevo, orientado desde el comienzo en sus especificaciones hardware y software para cubrir los siguientes requisitos:

- ✓ Identificación de las aplicaciones, independientemente del puerto o protocolo de base que utilicen, incluso aunque vayan codificadas bajo SSL o empleen alguna táctica evasiva.
- ✓ Identificación de los usuarios en base a su rol en la corporación, independientemente de qué dirección IP puedan tener en un momento determinado.
- ✓ Protección en tiempo real frente a los ataques y al software malicioso, embebido en el tráfico de las aplicaciones.
- ✓ Facilidad en la gestión de las políticas con herramientas de visualización potentes y un editor de políticas unificado.
- ✓ Rendimiento multi-gigabit sin degradación al utilizarlo en línea.

La siguiente figura, esquematiza los cuatro pilares básicos sobre los que se sustentan los firewalls de nueva generación de Palo Alto Networks:

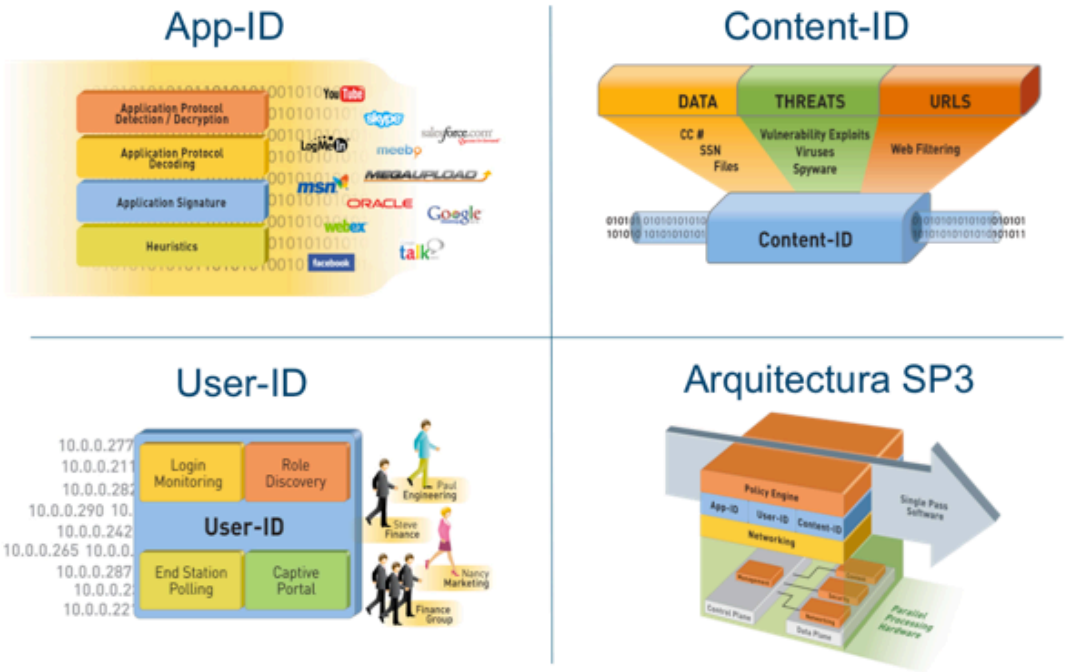

Figura 2.- Pilares básicos de los firewalls de Palo Alto networks

A continuación se ofrece un resumen de las funcionalidades de cada módulo básico:

App-ID es una tecnología de clasificación del tráfico, que detecta con precisión qué aplicaciones están corriendo en la red a través de diversas técnicas de identificación. La identidad de la aplicación sirve de base para todas las decisiones relativas a la política como la utilización apropiada y la inspección de contenidos. Es por tanto la tecnología base que utilizan los firewalls de Palo Alto Networks, en contraposición a la tecnología stateful inspection que utilizan otros fabricantes, y que desde Palo Alto Networks consideramos totalmente insuficiente para categorizar y proteger el panorama actual de aplicaciones.

La tecnología **User-ID** de Palo Alto Networks se integra con el directorio corporativo, para vincular dinámicamente la dirección IP con la información de usuario y de grupo (rol corporativo). Si las empresas tienen acceso a la actividad del usuario, pueden supervisar y controlar las aplicaciones y los contenidos que recorren la red, de una forma mucho más efectiva que por una simple dirección IP (que normalmente es además cambiante (DHCP, movilidad, etc.).

Control de los contenidos: La tecnología **Content-ID** de Palo Alto Networks combina un motor de prevención de amenazas en tiempo real con una base de datos URL integral y elementos de identificación de aplicaciones, para limitar las transferencias de archivos sin autorización, detectar y bloquear gran número de amenazas y controlar la navegación por Internet no relacionada con el trabajo.

Content ID funciona en coordinación con **App-ID** lo que mejora la eficacia del proceso de identificación de los contenidos.

La arquitectura SP3 – Single Pass Parallel Architecture – ofrece un rendimiento no conocido hasta la fecha gracias a la utilización de hardware paralelo, de modo que cada paquete es analizado una única vez a través de todos los módulos de la política de seguridad. A diferencia de muchas soluciones actuales, que utilizan una única CPU o una combinación de ASICs y CPUs, los firewalls de PAN utilizan una arquitectura construida a propósito, y desde cero, con procesamiento dedicado para la prevención de amenazas junto con procesamiento específico y memoria dedicada para las tareas de red, seguridad y gestión. La utilización de cuatro tipos diferentes de procesadores implica que las funcionalidades clave no compiten por ciclos de reloj con otras funciones de seguridad, como ocurre en el caso de equipos monoprocesador. El resultado final es una latencia muy baja y un gran throughput, con todos los servicios de seguridad habilitados.

Un potente conjunto de herramientas de visualización facilita a los administradores información completa sobre las aplicaciones que recorren la red, quién las utiliza y el impacto que pueden tener sobre la seguridad de la corporación.