Resumen del firewall de nueva generación de Palo Alto Networks

El firewall es el componente de infraestructura de seguridad de red más estratégico, ya que visualiza todo el tráfico y, como tal, se encuentra en la ubicación más efectiva para imponer la política de seguridad. Desafortunadamente, los firewalls tradicionales dependen del puerto y el protocolo para clasificar el tráfico, lo que permite a las aplicaciones y los usuarios expertos en tecnología esquivarlos con facilidad mediante el salto de puertos, el uso de SSL, el acceso a través del puerto 80 o el uso de puertos no estándar.

La pérdida de visibilidad y control resultante sitúa a los administradores en desventaja y expone a las empresas a tiempo de inactividad de la red, incumplimiento de normas, aumento de los gastos operativos y posible pérdida de datos. El enfoque histórico para restaurar la visibilidad y el control precisaba el despliegue individual de "firewall helpers" adicionales como respaldo del firewall o, de forma combinada, mediante la integración de soluciones alternativas de terceras partes. Sin embargo, ninguno de estos enfoques resolvía el problema de visibilidad y control debido a una visibilidad limitada del tráfico y una gestión complicada, así como varios procesos de latencia que provocaban procesos de exploración. La restauración de la visibilidad y el control requiere un enfoque nuevo, renovado y completo. Por tanto, es necesario un firewall de nueva generación.

Requisitos clave que deben cumplir los firewalls de nueva generación:

- **Identificación de aplicaciones, no de puertos.** Identificar con exactitud qué aplicación es, en todos los puertos, independientemente del protocolo, la codificación SSL o la táctica evasiva. La identidad de la aplicación se convierte en la base para todas las políticas de seguridad.
- **Identificación de usuarios y no sólo de direcciones IP.** Aprovechar la información almacenada en los directorios de empresa para la visibilidad, la creación de políticas, la generación de informes y la investigación forense.
- **Inspección del contenido en tiempo real.** Proteger la red de los ataques y el software malicioso incrustado en el tráfico de las aplicaciones con una latencia baja y velocidades altas de rendimiento.
- **Simplificar la gestión de políticas.** Restaurar la visibilidad y el control con herramientas gráficas fáciles de usar y un editor de políticas que vincula aplicaciones, usuarios y contenido, todo ello combinado de manera unificada.
- **Proporcionar un rendimiento multi-gigabit.** Combinar hardware y software de alto rendimiento en una plataforma construida especialmente para permitir un rendimiento multi-gigabit con baja latencia que tiene todos los servicios activados.

Palo Alto Networks fue fundada por el visionario de seguridad Nir Zuk con una misión clara: reinventar el firewall para convertirlo de nuevo en el dispositivo de seguridad de mayor importancia estratégica de la red. La familia de firewalls de nueva generación de Palo Alto Networks permite una visibilidad y control sin precedentes de las aplicaciones y el contenido por usuario (no sólo en la dirección IP), de hasta 10 Gbps. Según la tecnología App-ID™, los firewalls de nueva generación de Palo Alto Networks identifican con gran precisión las aplicaciones con independencia del puerto, el protocolo, la táctica evasiva o la codificación SSL, y exploran el contenido para detener amenazas y prevenir la pérdida de datos. Con Palo Alto Networks, las empresas pueden, por primera vez, adoptar y beneficiarse de una nueva generación de aplicaciones a la vez que mantienen un estado de visibilidad y control completo.

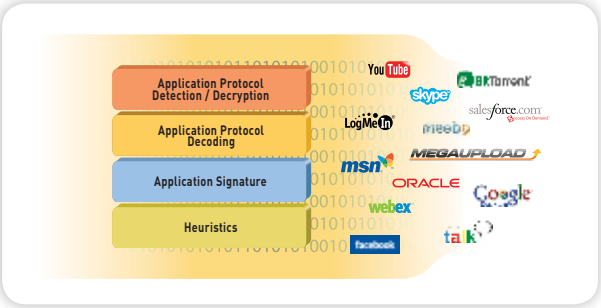
Todas estas funciones están incluidas en la familia de plataformas de alto rendimiento de Palo Alto Networks. Para obtener más información sobre las especificaciones técnicas de cada una de las soluciones de Palo Alto Networks, consulte www.paloaltonetworks.com.

paloalto NETWORKS

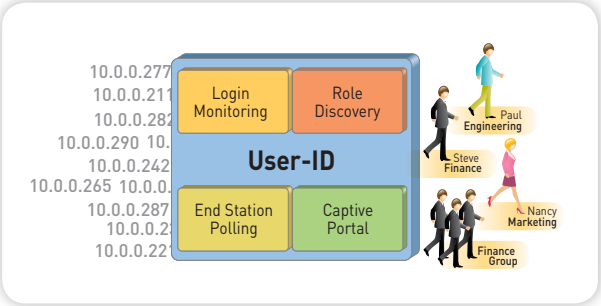
Firewall de nueva generación con tecnologías de identificación exclusivas

Existen tres tecnologías exclusivas dentro de la familia de firewalls de nueva generación de Palo Alto Networks que facilitan la visibilidad y el control de aplicaciones, usuarios y contenido: App-ID, User-ID y Content-ID. Cada una de estas tres tecnologías es pionera en la industria y se presenta como una plataforma construida especialmente para el firewall que ayuda a los administradores a restaurar la visibilidad y el control sobre aplicaciones, usuarios y contenidos.

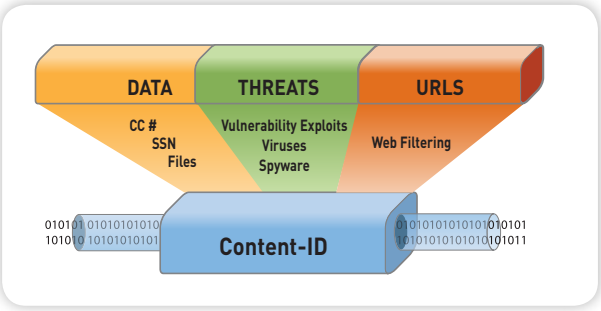
- **App-ID™:** el primer motor de clasificación del tráfico que permite identificar con precisión qué aplicaciones se están ejecutando en la red, independientemente del puerto, el protocolo, la codificación SSL o la táctica evasiva empleados. Esta tecnología emplea cuatro mecanismos distintos de identificación de aplicaciones. Una vez determinada la identidad de la aplicación, la información obtenida se utiliza como base para todas las decisiones relativas a la política de firewall.



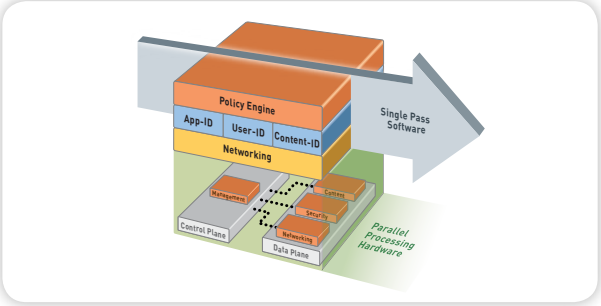
- **User-ID:** la perfecta integración con servicios de directorio de empresa como Active Directory, eDirectory, LDAP y Citrix es exclusiva de Palo Alto Networks y permite que los administradores puedan ver y controlar el uso de la aplicación según usuarios individuales y grupos de usuarios, en lugar de sólo direcciones IP. La información de usuario predomina en todas las funciones, incluidas la visibilidad de aplicaciones y amenazas, la creación de políticas, la investigación forense y la generación de informes.



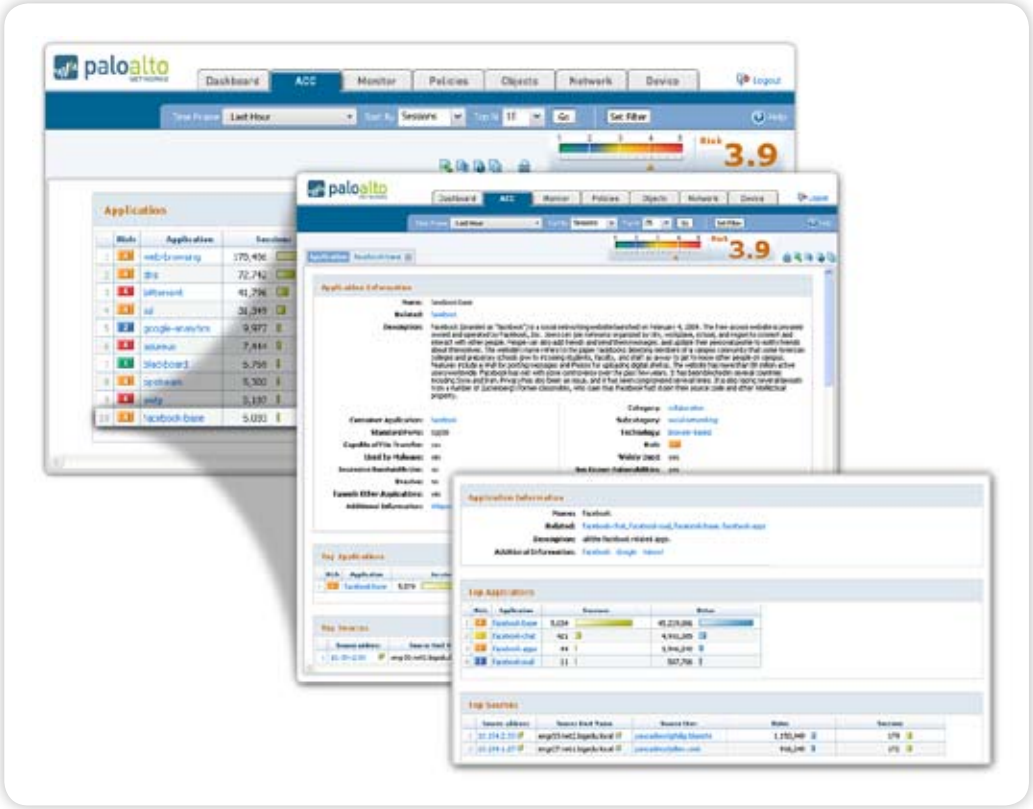
- **Content-ID:** se trata de un motor de exploración basada en el flujo que utiliza un formato de firma uniforme para la prevención de un gran número de amenazas, y limita la transferencia no autorizada de archivos y datos confidenciales al tiempo que una extensa base de datos URL controla la navegación por Internet. La amplitud de la prevención de amenazas, efectuada de una pasada, es exclusiva de Palo Alto Networks y cuando se combina con la visibilidad y control de la aplicación proporcionada por App-ID, hace que el departamento de TI retome de nuevo el control sobre las aplicaciones y las amenazas relacionadas.



- **Plataforma construida especialmente:** la funcionalidad multi-Gbps se proporciona a través del procesamiento específico de redes para ofrecer seguridad, prevención de amenazas y gestión, las cuales están estrechamente integradas con un motor de software de única pasada con el fin de maximizar el rendimiento. Un plano de datos (Data Plane) de 10 Gbps facilita el flujo de tráfico entre los procesadores, mientras que la separación física entre el plano de control (Control Plane) y el de datos asegura que el acceso de gestión siempre está disponible, independientemente de la carga de tráfico.



Visibilidad de aplicaciones
Visualice la actividad de la aplicación en un formato claro e inteligible. Añada y elimine filtros para obtener información adicional sobre la aplicación, sus funciones y quién las utiliza.



Visibilidad de las aplicaciones, usuarios y contenido

Los administradores se encuentran en una carrera vertiginosa para mantenerse al ritmo de los usuarios que cada vez cuentan con más conocimientos técnicos, así como de la aparición de aplicaciones con características muy avanzadas técnicamente al tiempo que fáciles de utilizar. Asimismo, la complejidad de esta carrera virtual es mayor si tenemos en cuenta que las herramientas con las que cuenta el administrador no pueden facilitarle información actualizada sobre la actividad de la red. Con un firewall de nueva generación de Palo Alto Networks, los administradores pueden usar un conjunto de herramientas de visualización para detectar rápidamente las aplicaciones que recorren la red, quién las utiliza y el impacto que pueden tener en la seguridad. La visibilidad que proporciona Application Command Center (ACC), App-Score, el visualizador de registros y el informe personalizable por completo puede capacitar a los administradores para implementar más políticas de seguridad de importancia empresarial.

- **Application Command Center (ACC):** una función estándar que no requiere configuración, ACC muestra gráficamente abundante información sobre la actividad actual de la red incluidas aplicaciones, categorías de URL, amenazas y datos. Si aparece una nueva aplicación en ACC, un sólo clic muestra una descripción de la aplicación, sus funciones clave, sus características de comportamiento, quién está utilizando la aplicación y qué reglas de seguridad permiten que se utilice. Se pueden añadir más filtros para obtener información adicional sobre el uso de la aplicación para usuarios individuales junto con las amenazas detectadas en el tráfico de la aplicación. En cuestión de sólo unos minutos, ACC proporciona a los administradores los datos necesarios para tomar decisiones de política de seguridad más fundamentadas.
- **App-Scope:** para complementar la vista en tiempo real de aplicaciones y contenido proporcionada por ACC, App-Scope ofrece una vista de la aplicación dinámica que el usuario puede personalizar, así como la actividad del tráfico y las amenazas a lo largo de un periodo de tiempo.
- **Gestión:** con el fin de ajustarse a los diversos estilos de gestión, requisitos y dotación de personal, los administradores pueden utilizar la interfaz basada en Internet, una completa interfaz de línea de comandos (CLI) o una solución de gestión centralizada (Panorama) para controlar todos los aspectos del firewall de Palo Alto Networks. En aquellos entornos en los que existan distintos miembros de la plantilla que precisen diferentes niveles de acceso a la interfaz de gestión, la administración basada en funciones de los tres mecanismos de gestión permite la delegación de funciones administrativas al individuo adecuado. Las interfaces syslog basadas en los estándares y las interfaces SNMP permiten la integración con herramientas de gestión de terceros.
- **Generación de registros e informes:** el filtrado en tiempo real facilita la rápida investigación forense de cada sesión que recorre la red. Los informes predefinidos, programables y personalizables por completo ofrecen vistas detalladas de las aplicaciones, los usuarios y las amenazas existentes en la red.

Habilitación de políticas de uso de la aplicación adecuada

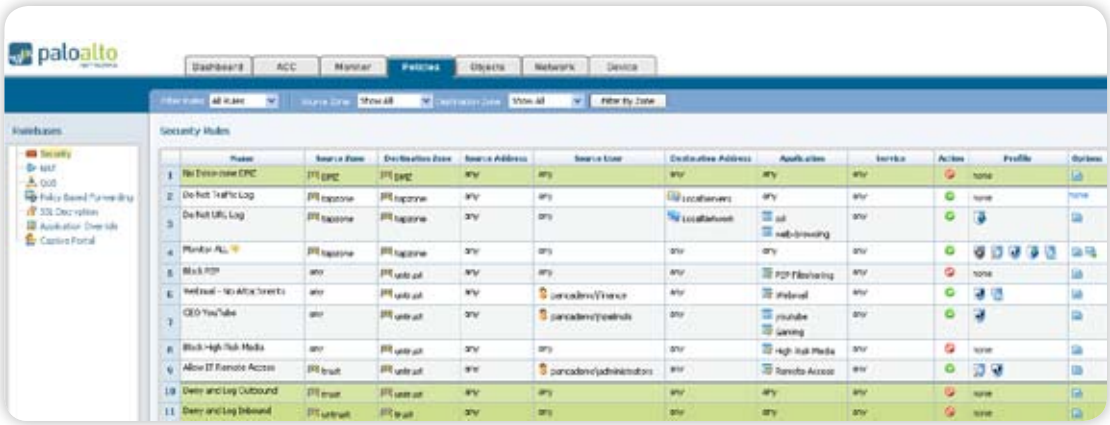
Acceso inmediato a información sobre qué aplicaciones recorren la red, quién las utiliza y el riesgo potencial de seguridad que capacita a los administradores para determinar de forma rápida y fácil la respuesta adecuada. Con estos puntos de datos, los administradores pueden aplicar políticas con un rango de respuestas más detallado que va más allá de las simples opciones de permitir o denegar. Entre las respuestas de control de política se incluyen:

- Permitir o denegar
- Permitir, pero explorar el contenido para detectar virus y otras amenazas
- Permitir según el programa, los usuarios o los grupos
- Descodificar e inspeccionar
- Aplicar catalogación de tráfico mediante la política de QoS
- Aplicar desvío basado en política
- Permitir determinadas funciones de la aplicación
- Cualquier combinación de las anteriores

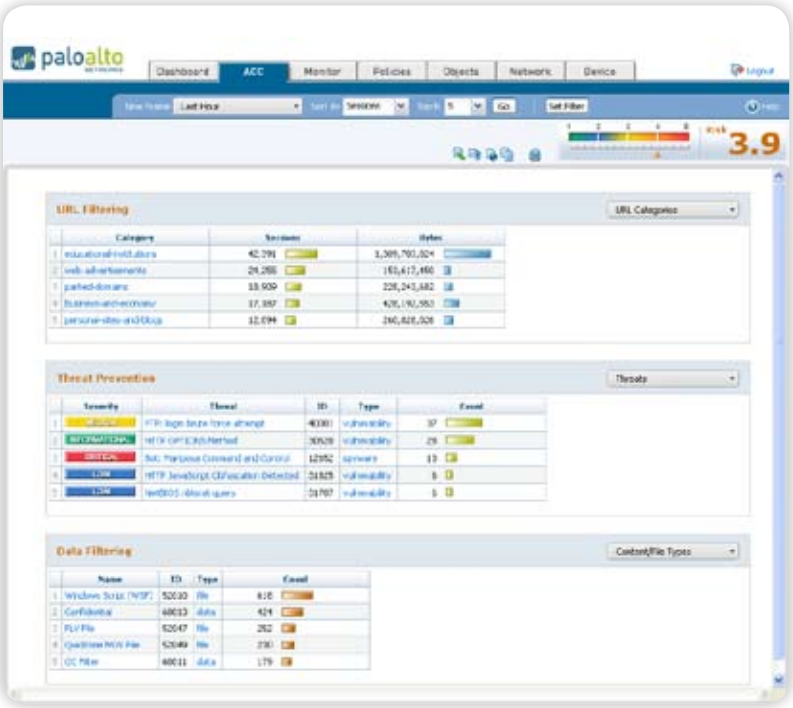
Al utilizar un editor de políticas con un aspecto familiar, los administradores de firewalls pueden crear de forma rápida políticas de firewalls flexibles tales como:

- Asignar Saleforce.com y Oracle para acceder a los grupos de ventas y marketing aprovechando la integración con Active Directory.
- Permitir sólo al grupo de TI el uso de un conjunto establecido de aplicaciones de gestión, como SSH, Telnet y RDP.
- Bloquear aplicaciones maliciosas como el uso compartido de archivos P2P, circumventors y proxies externos.
- Definir e imponer una política corporativa que permita e inspeccione el uso específico de webmail y mensajería instantánea.
- Utilizar el desvío basado en política para forzar el tráfico de la aplicación Facebook a través de una ruta específica.
- Controlar las funciones de transferencia de archivos de cada aplicación, permitiendo el uso de la aplicación pero vetando la transferencia de archivos.
- Identificar la transferencia de información confidencial, como los números de tarjetas de crédito o de la Seguridad Social, en formato de texto o archivo.
- Desplegar políticas de filtrado de URL que bloqueen el acceso a páginas obviamente no relacionadas con el trabajo, supervisar las páginas cuestionables y "controlar" el acceso a otras.
- Implementar políticas de QoS (Quality of Service o calidad de servicio) que permitan aplicaciones multimedia y otras aplicaciones de uso intensivo del ancho de banda pero que limiten su impacto en aplicaciones empresariales críticas.

Con un firewall de nueva generación de Palo Alto Networks instalado, los clientes podrán desplegar políticas de modelo de aplicación positiva para bloquear aplicaciones maliciosas, explorar las aplicaciones empresariales para detectar amenazas y promover el uso seguro de aplicaciones de usuario final. Por otra parte, una solución basada en IPS sólo dispondrá de dos opciones: permitir o denegar, lo cual limita la posibilidad de permitir el uso de aplicaciones de forma positiva, segura y controlada.



Creación de políticas
Su aspecto familiar permite crear y desplegar de forma rápida políticas que controlen las aplicaciones, los usuarios y el contenido.



Visibilidad de contenido y amenazas
Visualice la URL, la amenaza y la actividad de transferencia de datos o archivos en un formato claro e inteligible. Añada y elimine filtros para obtener información adicional sobre elementos individuales.

Protección de la red frente a amenazas

La recuperación de la visibilidad y el control del tráfico de las aplicaciones resuelve parte de los retos de seguridad de la red a los que se enfrentan los departamentos de TI en un entorno tan centrado en Internet como el actual. Inspeccionar el tráfico de aplicaciones permitidas es el siguiente gran reto dentro del marco de un motor de prevención de amenazas, el cual se encuentra perfectamente integrado con el firewall y combina un formato de firma uniforme con una exploración basada en flujo para bloquear exploits de vulnerabilidad, virus y spyware de una pasada.

- **Sistema de prevención de intrusiones (IPS):** la protección de vulnerabilidades integra un completo conjunto de funciones del sistema de prevención de intrusiones (Intrusion Prevention System, IPS) para bloquear exploits de vulnerabilidad, tanto conocidos como desconocidos, en la capa de aplicación y en la red, desbordamientos en la memoria intermedia, ataques DoS y exploraciones de puertos para evitar peligros y daños en los recursos de información empresarial. Entre los mecanismos IPS se encuentran:
  - Análisis de descifrador de protocolo
  - Comparación de patrones de estado
  - Detección de anomalías de protocolo
  - Análisis heurístico
  - Detección de anomalías estadísticas
  - Desfragmentación de IP y reensamblaje de TCP
  - Bloqueo de paquetes no válidos o malformados
  - Firmas de vulnerabilidad personalizadas
- **Antivirus de red:** la protección en línea frente a virus detecta y bloquea la mayoría de los tipos de software malicioso en la puerta de enlace. La protección frente a virus aprovecha el formato de firma uniforme y el motor basado en flujo para proteger las empresas frente a millones de variantes de software malicioso. La exploración basada en flujo ayuda a proteger la red sin que ello conlleve un nivel de latencia alto, lo que en otras tecnologías antivirus de red que dependen de la exploración basada en proxy constituye un problema. Además, el motor basado en flujo puede realizar acciones de descompresión en línea, y de este modo, proteger a las empresas de amenazas comprimidas y en archivos comprimidos (en zip). Asimismo y dado que los firewalls de nueva generación de Palo Alto Networks cuentan con la capacidad de descodificar SSL definido por política, las organizaciones tienen una mayor protección frente a software malicioso que se desplaza a través de los vectores de aplicaciones con codificación SSL.

Filtrado de URL

Una base de datos de filtrado de URL personalizable y totalmente integrada de más de 20 millones de URLs divididas en categorías permite a los administradores aplicar políticas granulares de navegación por Internet, complementar la visibilidad de las aplicaciones y las políticas de control, y proteger a la empresa de todo un espectro de riesgos legales, reguladores y de productividad. Se pueden crear categorías personalizadas para complementar la base de datos de URLs incluida y atender los requisitos de los clientes exclusivos. Para adaptarse a los patrones de tráfico de la comunidad de usuarios local, la base de datos incluida puede ampliarse con una base de datos de la memoria caché de un millón de URLs dinámicas por separado generada desde una base de datos de URL alojada con más de 180 millones de URLs.

Filtrado de datos

Las funciones de filtrado de datos permiten a los administradores implementar políticas para reducir los riesgos asociados a la transferencia no autorizada de archivos basados en el tipo (en contraposición a la observación exclusiva de la extensión del archivo), y patrones de datos confidenciales (números de tarjetas de crédito y de la Seguridad Social).

Flexibilidad de despliegue de la red

Una arquitectura de red flexible que incluye enrutamiento dinámico, switching, alta disponibilidad y compatibilidad con VPN permite el despliegue en casi cualquier entorno de red.

- **Switching y enrutamiento:** la compatibilidad con las arquitecturas L2, L3 y el modo mixto, junto con la seguridad basada en zonas, permiten el despliegue en un gran número de entornos de red. Los protocolos de enrutamiento dinámico (BGP, OSPF y RIP) y una compatibilidad total con 802.1Q VLAN están disponibles para L2 y L3.
- **Virtual Wire:** une de forma lógica dos puertos y pasa todo el tráfico al otro puerto sin switching ni enrutamiento, por lo que la inspección y el control son totales sin afectar a los demás dispositivos.
- **Desvío basado en política:** desvía el tráfico en función de la política definida por la aplicación, es decir: origen de zona/interfaz, dirección de origen/destino, origen de usuario/grupo y servicio.
- **Sistemas virtuales:** crea varios "firewalls" virtuales dentro de un dispositivo único como medio de soporte para departamentos o clientes específicos. Cada sistema virtual puede incluir cuentas administrativas, interfaces, configuración de red, zonas de seguridad y políticas dedicadas para el tráfico de red asociado.
- **Alta disponibilidad activa/pasiva:** conmutación por error subsegunda con total compatibilidad para la sincronización de configuración y sesión.
- **IPv6:** compatibilidad con la visibilidad completa de aplicaciones, el control, la inspección, la supervisión y la generación de registros para aplicaciones que utilizan IPv6 (sólo en el modo "Virtual Wire").
- **Tramas gigantes (sólo para la Serie PA-4000):** compatibilidad con tramas gigantes (hasta 9.216 bytes).

Conectividad segura

- **VPN site-to-site:** la conectividad de IPSec VPN basada en los estándares, combinada con la visibilidad y el control de las aplicaciones permite proteger la comunicación entre uno o más dispositivos de Palo Alto Networks o el dispositivo IPSec VPN de otro proveedor.
- **VPN de acceso remoto:** VPN por túnel SSL proporciona un acceso de red seguro a usuarios remotos y amplía a éstos la visibilidad y el control basados en políticas de aplicaciones, usuarios y contenido.

Supervisión y control de ancho de banda

- **Calidad de servicio (Quality of Service, QoS):** la catalogación del tráfico amplía los controles de política de habilitación positiva para ofrecer a los administradores la posibilidad de permitir aplicaciones de uso intensivo del ancho de banda, tales como las aplicaciones multimedia de flujo continuo, al tiempo que se mantiene el rendimiento de las aplicaciones empresariales. Las políticas de catalogación del tráfico (garantizado, máximo y prioritario) se pueden imponer en función de la aplicación, el usuario, el programa, etc. También existe compatibilidad con el marcador diffserv, lo cual permite el control del tráfico de la aplicación mediante un dispositivo de bajada o subida.
- **Control de ancho de banda en tiempo real:** visualización gráfica en tiempo real del consumo del ancho de banda y la sesión para aplicaciones y usuarios de una clase de QoS seleccionada.

Generación de informes y registros

Potentes funciones de generación de informes y registros permiten analizar incidentes de seguridad, uso de aplicaciones y patrones de tráfico.

- **Generación de informes:** los informes predefinidos se pueden utilizar tal como están, o bien pueden personalizarse o agruparse en un solo informe con el fin de adaptarse a los requisitos específicos. Un informe de actividades detallado muestra las aplicaciones utilizadas, las categorías de URLs visitadas, las páginas de Internet visitadas y un informe detallado de todas las URLs visitadas durante un periodo de tiempo determinado y para un usuario concreto. Todos los informes se pueden exportar a formato CSV o PDF y se pueden enviar por correo electrónico de forma programada.
- **Generación de registros:** los administradores pueden ver la actividad de las aplicaciones, las amenazas y los usuarios por medio de funciones de filtrado dinámicas, activadas con sólo hacer clic en el valor de una celda o utilizando el generador de expresiones para definir los criterios de filtrado. Los resultados del filtro de registro pueden exportarse a un archivo CSV o enviarse a un servidor syslog para poder archivarlos fuera de línea o realizar análisis adicionales.
- **Herramienta de seguimiento de sesión:** acelera la investigación forense o de incidentes con una vista centralizada y correlacionada a través de todos los registros de tráfico, amenazas, URLs y aplicaciones relacionadas con una sesión individual.

paloalto NETWORKS

Palo Alto Networks
232 E. Java Drive
Sunnyvale, CA. 94089
Ventas 866.320.4788
o 408.738.7700
www.paloaltonetworks.com

840-000001-00D