Resumen del firewall de nueva generación

Los cambios radicales en el ámbito de las aplicaciones y de las amenazas, el comportamiento de los usuarios y la infraestructura de la red han ido erosionando la seguridad tradicional que desde siempre han ofrecido los firewalls basados en puertos. En su trabajo diario los usuarios acceden a todo tipo de aplicaciones utilizando una amplia gama de dispositivos. Mientras tanto la expansión de los centros de datos, la virtualización, la movilidad y las iniciativas basadas en la nube, están obligando a rediseñar los permisos de acceso de las aplicaciones sin afectar a la protección de la red.

Las respuestas tradicionales incluyen intentos de controlar el tráfico de las aplicaciones a través del uso de una lista interminable de tecnologías, además del firewall, que finalmente entorpecen el funcionamiento de su negocio, o bien permiten todas las aplicaciones, lo que es igualmente inaceptable debido al aumento de los riesgos de seguridad. El reto al que se enfrenta es que su firewall tradicional basado en puertos, incluso con bloqueo de aplicaciones específicas, no ofrece una alternativa a todos y cada uno de los enfoques. Con el fin de lograr un equilibrio entre permitir o denegar todo, es necesario habilitar de forma segura las aplicaciones utilizando elementos relevantes para el negocio, tales como la identidad de la aplicación, quién la está utilizando y el tipo de contenido como criterios clave para las políticas de seguridad del firewall.

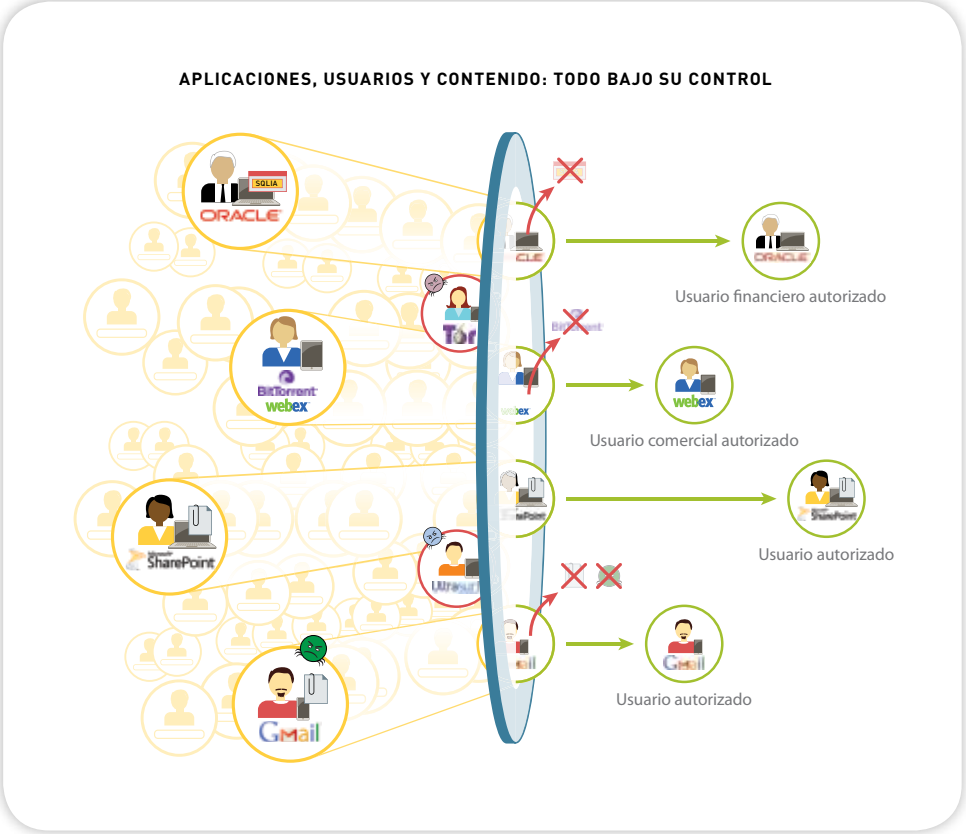
Principales requisitos de la habilitación segura:

- **Identificación de aplicaciones, no de puertos.** Clasificación del tráfico tan pronto como llega al firewall para determinar la identidad de la aplicación, independientemente del protocolo, el cifrado o la táctica evasiva. Utilización de esa identidad como la base de todas las políticas de seguridad.
- **Vinculación del uso de la aplicación a la identidad del usuario, no a la dirección IP, independientemente de la ubicación o del dispositivo.** Utilización de la información del usuario y de los grupos extraídos de los directorios de las empresas, y de otro tipo de almacenes de usuarios, para implementar políticas de habilitación coherentes para todos los usuarios, independientemente de la ubicación o del dispositivo.
- **Prevención de todas las amenazas, tanto conocidas como desconocidas.** Prevención de exploits de vulnerabilidades conocidas, malware, Spyware y URL maliciosas analizando el tráfico y ofreciendo protección automática contra el malware desconocido y selectivo.
- **Simplificación de la administración de políticas.** Habilitación segura de las aplicaciones y reducción del esfuerzo administrativo gracias a sus sencillas herramientas gráficas, un editor unificado de políticas, plantillas y grupos de dispositivos.

Las políticas de habilitación segura de aplicaciones ayudan a mejorar su seguridad, independientemente de la ubicación de la implementación. En la zona perimetral se reducirá la posibilidad de amenazas mediante el bloqueo de una amplia gama de aplicaciones no deseadas y la posterior inspección de las aplicaciones autorizadas buscando posibles amenazas, tanto conocidas como desconocidas. En el centro de datos (tradicional o virtualizado), la habilitación de aplicaciones garantiza que las aplicaciones de los centros de datos solo son utilizadas por usuarios autorizados, protegiendo los contenidos contra amenazas y haciendo frente a los desafíos de seguridad introducidos por la naturaleza dinámica de la infraestructura virtual. Las delegaciones de la empresa y los usuarios remotos estarán protegidos por el mismo conjunto de políticas de habilitación implementadas en la central, lo que garantiza la coherencia de políticas.

Despliegue de políticas de habilitación segura en toda la organización

paloalto NETWORKS
the network security company™



Habilitación de aplicaciones para una mayor robustez de la empresa

La habilitación segura de aplicaciones de los firewall de nueva generación de Palo Alto Networks™ ayuda a hacer frente a los riesgos de seguridad asociados al creciente número de aplicaciones que recorren la red en su empresa. La habilitación de aplicaciones para usuarios o grupos de usuarios, tanto locales, móviles como remotos, y la protección contra amenazas conocidas o desconocidas, mejora el nivel de seguridad permitiendo que el negocio crezca.

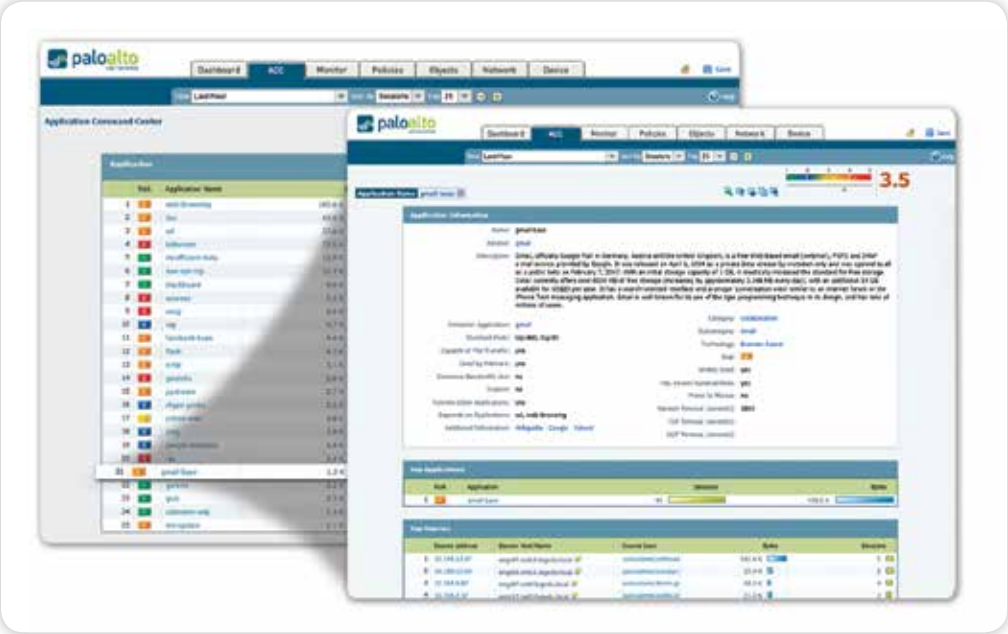
- **Clasificación de todas las aplicaciones, en todos los puertos, en todo momento.** La clasificación rigurosa del tráfico es la clave de cualquier firewall y en ello se basan las políticas de seguridad. Actualmente las aplicaciones pueden esquivar con facilidad un firewall basado en puertos mediante el salto de puertos, el uso de SSL y SSH, el acceso a través del puerto 80 o el uso de puertos no estándar. App-ID™ aborda las limitaciones de visibilidad de clasificación del tráfico que afectan a los firewalls tradicionales mediante la aplicación de diversos mecanismos de clasificación del flujo de tráfico, tan pronto como el firewall los detecta, para determinar la identidad exacta de la aplicación que atraviesa la red, independientemente del puerto, el cifrado (SSL o SSH) o la técnica evasiva empleada. El conocimiento exacto de las aplicaciones que están pasando por la red, no solo el puerto y el protocolo, se convierte en la base para todas las decisiones de las políticas de seguridad. Las aplicaciones no identificadas, por lo general un pequeño porcentaje del tráfico pero con un alto riesgo potencial, se clasifican automáticamente para su gestión sistemática, que puede incluir control e inspección de políticas, análisis forense de amenazas, creación de una App-ID personalizada o una captura de paquetes para el desarrollo de una App-ID por Palo Alto Networks.

- **Integración de usuarios y dispositivos en las políticas, no solo de direcciones IP**. La creación y administración de políticas de seguridad basadas en la aplicación y en la identidad de los usuarios, independientemente del dispositivo o la ubicación, es un medio mucho más eficaz de proteger su red en lugar de confiar únicamente en el puerto y la dirección IP. La integración con una amplia gama de repositorios de usuarios empresariales (Microsoft Windows, Mac OS X, Linux, Android, iOS) proporciona la identificación del usuario para su acceso a la aplicación. Los usuarios que viajan o que trabajan de forma remota están perfectamente protegidos con las mismas políticas coherentes que se usan en su red local o corporativa. La combinación de visibilidad y control sobre la actividad de las aplicaciones de los usuarios significa que se puede habilitar de forma segura el uso de Oracle, BitTorrent o Gmail, o de cualquier otra aplicación que atraviese la red, sin importar desde dónde o la forma en la que el usuario acceda a ella.

- **Prevención contra todas las amenazas, tanto conocidas como desconocidas.** Para proteger las redes modernas, es necesario poder combatir una combinación de exploits, malware y spyware conocidos, así como amenazas desconocidas y selectivas. Este proceso comienza reduciendo la superficie de ataque de la red autorizando aplicaciones específicas y denegando todas las demás tanto de forma implícita a través de una estrategia de "denegar todo excepto", o mediante políticas explícitas. La prevención coordinada de amenazas se puede aplicar a todo el tráfico autorizado, bloqueando sitios conocidos de malware, exploits de vulnerabilidades, virus, spyware y consultas DNS maliciosas en un solo paso. El malware personalizado o desconocido se analiza e identifica activamente bien ejecutando los archivos desconocidos o bien mediante la observación directa de más de 100 comportamientos maliciosos en un entorno virtualizado de pruebas. Cuando se descubre nuevo malware, se genera y entrega automáticamente una firma para el archivo infectado y para el tráfico relacionado. El análisis de prevención de amenazas utiliza el contexto del protocolo y la aplicación, garantizando que las amenazas están siempre localizadas incluso si tratan de eludir la seguridad ocultándose en túneles, en contenido comprimido o en puertos no estándar.

Flexibilidad de implementación y administración

Funcionalidad de habilitación segura de aplicaciones disponible en plataforma de hardware especialmente diseñada o de forma virtualizada. Al implementar múltiples firewalls de Palo Alto Networks, ya sea en forma de hardware o virtualizada, puede utilizarse Panorama, que ofrece una administración centralizada opcional para ganar visibilidad en los patrones de tráfico, implementar políticas, generar informes y realizar actualizaciones de contenido desde una ubicación central.



Visibilidad de aplicaciones: Visualización de la actividad de la aplicación en un formato claro e inteligible. Añadir y eliminar filtros para obtener información adicional sobre las aplicaciones, sus funciones y quién las utiliza.

Habilitación segura de aplicaciones: un enfoque integral

Las seguridad de las aplicaciones requiere un enfoque integral para garantizar la seguridad y el crecimiento de su negocio que comienza con un profundo conocimiento de las aplicaciones de la red: quién es el usuario, independientemente de la plataforma o de la ubicación, y qué contenido, si es el caso, lleva la aplicación. Con un conocimiento más completo de la actividad de la red, se pueden crear políticas de seguridad más coherentes que se basen en elementos de aplicación, usuario y contenido relevantes para su negocio. La ubicación del usuario, su plataforma y el lugar de la implementación de la política (centro de datos tradicional o virtualizado, entorno perimetral, delegación o usuario remoto) no influyen, o influyen poco, en la forma de crear la política. Ahora puede habilitar de forma segura cualquier aplicación, usuario y contenido.

El conocimiento integral equivale a políticas de seguridad más estrictas

Las buenas prácticas de seguridad dicen que un conocimiento más completo de lo que hay en su red es beneficioso para la implementación de políticas de seguridad más estrictas. Por ejemplo, saber exactamente qué aplicaciones están recorriendo su red, en comparación con el conjunto más amplio de tráfico basado en puertos, permite que sus administradores autoricen de forma específica las aplicaciones que hacen funcionar su negocio y bloqueen las aplicaciones no deseadas. El conocimiento de quién es el usuario, y no solo su dirección IP, añade otro criterio a las políticas permitiéndole ser más específico en su asignación.

- Mediante un potente conjunto de herramientas de visualización gráfica, sus administradores pueden obtener una imagen más completa de la actividad de la aplicación y del impacto potencial de seguridad, y tomar decisiones sobre las políticas de una forma más eficaz. Las aplicaciones se clasifican continuamente y, a medida que cambia su estado, los resúmenes gráficos se van actualizando dinámicamente para mostrar la información en una interfaz basada en web muy sencilla de utilizar.
- Las aplicaciones nuevas o con las que no esté familiarizado se pueden investigar rápidamente con un solo clic que muestra la descripción de la aplicación, sus características de comportamiento y quién las utiliza.
- La visibilidad adicional de las categorías de URL, las amenazas y los patrones de datos proporcionan un panorama completo y detallado de la actividad de la red.
- Las aplicaciones desconocidas, que normalmente son un pequeño porcentaje en cada red, pero aun así suponen un riesgo potencial, se clasifican para su análisis y así determinar si son aplicaciones internas, aplicaciones comerciales aún sin identificar, o amenazas.

Habilitación de aplicaciones y reducción de los riesgos

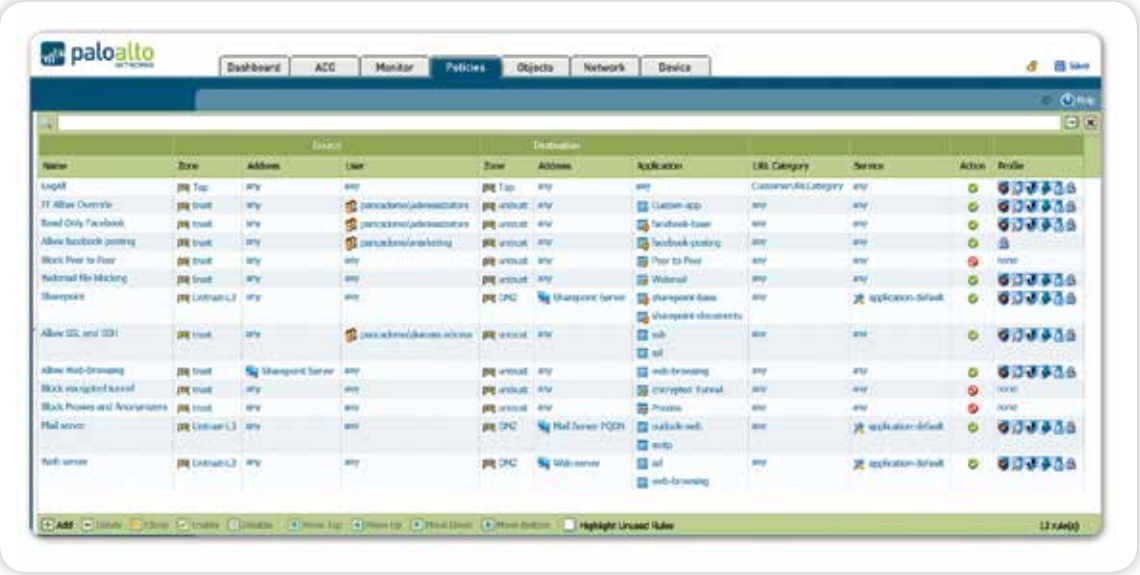
La habilitación segura de aplicaciones utiliza criterios de decisión de políticas que incluyen aplicación/función de la aplicación, usuarios y grupos y contenido como medio para lograr el equilibrio entre la denegación de todas las aplicaciones (lo cual limita el desarrollo del negocio) y permitir todas las aplicaciones (lo cual es una alternativa de alto riesgo).

En la zona perimetral, incluidos los usuarios remotos, móviles y de delegaciones, las políticas de habilitación se centran en identificar todo el tráfico y, a continuación, permitir de forma selectiva el tráfico en función de la identidad del usuario, para posteriormente explorar el tráfico en busca de amenazas. Algunos ejemplos de políticas serían:

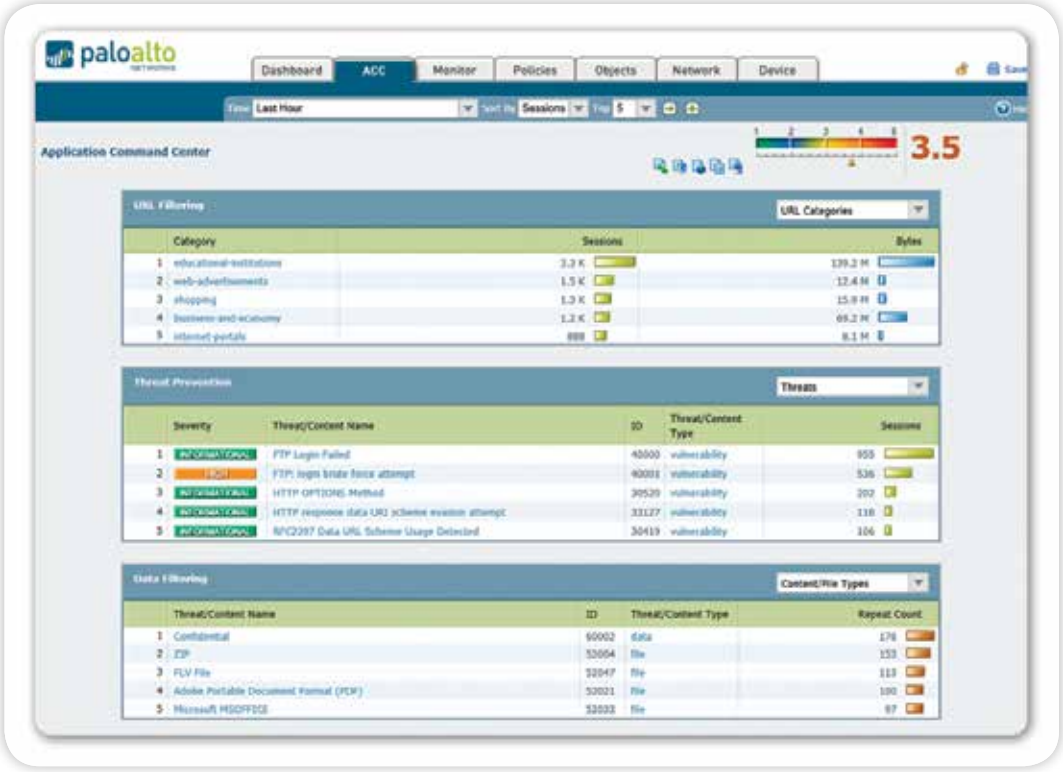
- Limitar el uso del correo web y de la mensajería instantánea a unas pocas variantes seleccionadas; descifrar las que usan SSL, inspeccionar el tráfico en busca de exploits y cargar archivos desconocidos en WildFire para su análisis y para el desarrollo de firmas.
- Permitir las aplicaciones y sitios web de streaming pero aplicar QoS y prevención de malware para limitar el impacto sobre las aplicaciones de voz sobre IP y proteger su red.
- Controlar Facebook permitiendo que todos los usuarios "naveguen", bloqueando todos los juegos y plugins sociales de Facebook y permitiendo los comentarios de Facebook solo para marketing. Explorar todo el tráfico de Facebook en busca de malware y exploits.
- Controlar la navegación web permitiendo y explorando el tráfico a sitios web relacionados con el trabajo y bloquear el acceso a sitios web claramente no relacionados con el trabajo; "controlar" el acceso a sitios cuestionables mediante el bloqueo personalizado de páginas.
- Aplicar una seguridad consistente implementando de forma transparente las mismas políticas a todos los usuarios, locales, móviles o remotos, con GlobalProtect™.
- Usar una estrategia implícita de denegar todo lo demás o bloquear explícitamente las aplicaciones no deseadas como P2P, circunventores y tráfico de países determinados para reducir el tráfico de las aplicaciones que introducen riesgos de seguridad para el negocio.

En el centro de datos (tradicional, virtualizado o una combinación de ambos), los ejemplos de habilitación se centran en confirmar aplicaciones, buscar aplicaciones no apropiadas y proteger los datos.

- Aislar el repositorio de números de tarjeta de crédito basado en Oracle en su propia zona de seguridad; controlar el acceso a grupos de finanzas, obligar al tráfico a pasar por sus puertos estándar e inspeccionar el tráfico en busca de vulnerabilidades de aplicación.
- Habilitar solo al grupo de TI el acceso al centro de datos usando un conjunto establecido de aplicaciones de administración remotas (ej., SSH, RDP, Telnet), a través de sus puertos estándar.
- Permitir el uso de Microsoft SharePoint Administration solo al equipo de administración y permitir el acceso a Microsoft SharePoint Documents a todos los demás usuarios.



Editor unificado de políticas: su aspecto familiar permite crear e implementar de forma rápida políticas que controlen las aplicaciones, los usuarios y el contenido.



Visibilidad de contenido y de amenazas: Visualización de la URL, las amenazas y la actividad de transferencia de datos o archivos en un formato claro e inteligible. Añadir y eliminar filtros para obtener información adicional sobre elementos individuales.

Protección de aplicaciones habilitadas

La habilitación segura de aplicaciones significa permitir el acceso a ciertas aplicaciones y, a continuación, aplicar políticas específicas para bloquear exploits conocidos y malware y spyware conocido o desconocido; controlar la transferencia de archivos o datos y la actividad de la navegación web. Se combaten tácticas comunes de evasión de amenazas, como el salto de puertos y el tunneling, mediante la ejecución de políticas de prevención de amenazas que usan el contexto de aplicación y protocolo generado por los decodificadores en App-ID. Como contrapunto, las soluciones UTM toman un enfoque basado en núcleos para la prevención de amenazas y cada función, firewall, IPS, AV, filtrado de URL explora el tráfico sin compartir contexto, de forma que son más susceptibles al comportamiento evasivo.

- **Bloqueo de amenazas conocidas: IPS y antivirus y anti-spyware de red.** Un formato de firma uniforme y un motor de exploración basado en flujos le permiten proteger su red de una amplia gama de amenazas. El sistema de prevención de intrusiones (IPS) cuenta con sistemas contra exploits de vulnerabilidades de aplicación y de red, desbordamientos de búfer, ataques de denegación de servicio y exploración de puertos. Protección antivirus y anti-spyware que bloquea millones de variantes de malware, así como cualquier tráfico "command-and-control" generado por malware, virus en PDF y malware oculto en archivos comprimidos o tráfico web (comprimido HTTP/HTTPS). Descifrado SSL basado en políticas para cualquier aplicación en cualquier puerto que protege contra el malware que se mueve en aplicaciones con cifrado SSL.
- **Bloqueo de malware desconocido y selectivo: Wildfire™.** El malware desconocido o selectivo es identificado y analizado por WildFire, que directamente ejecuta y observa los archivos conocidos en un entorno de pruebas virtualizado y basado en la nube. WildFire supervisa más de 100 comportamientos maliciosos y el resultado se envía directamente al administrador en forma de alerta. Existe una suscripción a WildFire opcional que ofrece una mayor protección, generación de registros e informes. Como suscriptor, estará protegido en el plazo máximo de una hora cuando se encuentre un elemento de malware en cualquier parte del mundo, para detener de forma eficaz la expansión del nuevo malware antes de que le afecte a usted. Como suscriptor, también obtendrá acceso a la generación de registros e informes integrada en WildFire y a una API para enviar muestras a la nube de WildFire para ser analizadas.

- **Identificación de hosts infectados por bots.** App-ID clasifica todas las aplicaciones, en todos los puertos, incluido cualquier tráfico desconocido, que a menudo pueda revelar anomalías o amenazas en su red. El informe de botnet basado en comportamiento vincula el tráfico desconocido, las consultas de DNS y URL sospechosas y varios comportamientos de red inusuales, para revelar dispositivos que probablemente estén infectados con malware. Los resultados se muestran en forma de una lista de hosts potencialmente infectados que pueden investigarse como posibles miembros de una botnet.
- **Limitación de transferencias de datos y archivos no autorizados.** Las funciones de filtrado de datos permiten a sus administradores implementar políticas que reduzcan los riesgos asociados a las transferencias de archivos y datos no autorizadas. Las transferencias de archivos se pueden controlar explorando el interior del archivo (en lugar de comprobar simplemente la extensión del archivo), para determinar si se debe permitir la transferencia o no. Los archivos ejecutables, que por lo general se encuentran en descargas "drive-by download", se pueden bloquear para proteger la red de la propagación de software malicioso oculto. Las funciones de filtrado de datos pueden detectar y controlar el flujo de patrones de datos confidenciales (números de tarjetas de crédito o de la Seguridad Social y patrones personalizados).
- **Control de la navegación web.** Un motor de filtrado de URL personalizable y totalmente integrado permite a los administradores aplicar políticas granulares de navegación por Internet, complementando la visibilidad de las aplicaciones y las políticas de control y proteger a la empresa de todo un espectro de riesgos legales, normativos y de productividad. Además, las categorías de URL se pueden integrar en las políticas para proporcionar una mayor granularidad en el control del descifrado SSL, la calidad de servicio u otras bases de reglas.

Administración y análisis constantes

Las buenas prácticas de seguridad dictan que los administradores deben lograr un equilibrio entre la administración proactiva del firewall, tanto si es un único dispositivo como si son cientos, y ser reactivos, investigar, analizar y elaborar informes sobre incidentes de seguridad.

- **Administración:** cada una de las plataformas de Palo Alto Networks puede ser administrada individualmente mediante una interfaz de línea de comandos (CLI) o una interfaz basada en web con funciones muy completas. Para implementaciones a gran escala, se puede obtener una licencia de Panorama e implementarlo como solución de administración centralizada que le permita equilibrar un control centralizado global con la necesidad de flexibilidad de las políticas locales mediante funciones como plantillas y una política compartida. Adicionalmente también se soportan herramientas basadas en normas como REST API y SNMP, lo que le permite obtener la integración con soluciones de administración de terceros. Tanto si utiliza la interfaz web del dispositivo como la de Panorama, el aspecto de ambas es idéntico, para no tener emplear tiempo de aprendizaje al pasar de una a otra. Sus administradores pueden usar cualquiera de las interfaces suministradas para realizar cambios en cualquier momento sin necesidad de preocuparse por los problemas de sincronización. Se admite la administración basada en funciones para todos los medios de administración, para que se puedan asignar características y funciones a personas concretas.
- **Generación de informes:** los informes predefinidos se pueden utilizar tal y como están, o bien pueden personalizarse o agruparse en un solo informe con el fin de adaptarse a los requisitos específicos. Todos los informes se pueden exportar a formato CSV o PDF y se pueden ejecutar y enviar por correo electrónico de forma programada.
- **Generación de logs:** el filtrado de logs en tiempo real facilita la rápida investigación forense de cada sesión que viaja por su red. Los resultados del filtrado del log pueden exportarse a un archivo CSV o enviarse a un servidor syslog para poder archivarlo fuera de línea o realizar análisis adicionales.

Plataforma de hardware diseñada específicamente o plataforma virtualizada

Palo Alto Networks ofrece una gama completa de plataformas hardware diseñadas específicamente que van desde el PA-200, para oficinas remotas, hasta el PA-5060, diseñado para centros de datos de alta velocidad. La arquitectura de la plataforma se basa en un motor de software de paso único y utiliza procesamiento específico de función para la red, la seguridad, la prevención de amenazas y la administración para conseguir un rendimiento óptimo. La misma funcionalidad de firewall suministrado en las plataformas de hardware también está disponible en el firewall virtual de la serie VM, permitiéndole proteger sus entornos de computación virtualizados y basados en la nube mediante las mismas políticas aplicadas tanto en sus firewalls perimetrales como en los de oficinas remotas.

paloalto NETWORKS

the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Accueil : +1.408.573.4000
Ventes : +1.866.320.4788
Assistance : +1.866.898.9087

www.paloaltonetworks.com

Copyright ©2012, Palo Alto Networks, Inc. Todos los derechos reservados. Palo Alto Networks, el logotipo de Palo Alto Networks, PAN-OS, App-ID y Panorama son marcas comerciales de Palo Alto Networks, Inc. Todas las especificaciones están sujetas a modificaciones sin previo aviso. Palo Alto Networks no asume ninguna responsabilidad por imprecisiones en este documento ni por la obligación de actualizar la información de este documento. Palo Alto Networks se reserva el derecho a cambiar, modificar, transferir o revisar de otro modo esta publicación sin previo aviso. **PAN_DS_FFOV_112712**