10 cosas

que tiene que hacer su próximo firewall

paloalto NETWORKS®

the network security company™

Dejar de pensar en:

Firewalls tradicionales.

Empezar a pensar en:

Firewalls de nueva generación.

Introducción

Ante el complejo panorama de la ciberseguridad de nuestros días, la elección de su próximo firewall se convierte en mucho más que una simple comparación de características técnicas. Se trata de adoptar un cambio en su papel para convertirse en facilitador, y no en obstáculo, del negocio. Se trata de equilibrar las necesidades de la empresa con el negocio y los riesgos de seguridad asociados a las aplicaciones modernas. Se trata de reconocer que el mundo ha cambiado a su alrededor y que ya no basta con protegerse a sí mismo con un enfoque de la ciberseguridad que funcionaba bien cuando la navegación web y el correo electrónico eran las dos únicas aplicaciones en Internet. Se trata de las 10 cosas que describimos en este folleto y que creemos que debería poder realizar su próximo firewall.

Dejar de pensar en:

Muros.

Empezar a pensar en:

Aire libre, en cualquier lugar.

Identificar y controlar las aplicaciones en cualquier puerto

Los desarrolladores de aplicaciones ya no adoptan el estándar de mapeo puerto/protocolo/aplicación. Cada vez más aplicaciones en su red son capaces de funcionar en puertos no estándar o pueden saltar de puerto (por ejemplo, las aplicaciones de mensajería instantánea, de intercambio de archivos P2P o de VoIP). Además, los usuarios ya tienen los conocimientos suficientes como para forzar que las aplicaciones se ejecuten a través de puertos no estándar (por ejemplo, RDP o SSH). Con el fin de hacer cumplir las políticas específicas de cada aplicación donde los puertos son cada vez más irrelevantes, su próximo firewall debe asumir que cualquier aplicación puede ejecutarse en cualquier puerto.

1

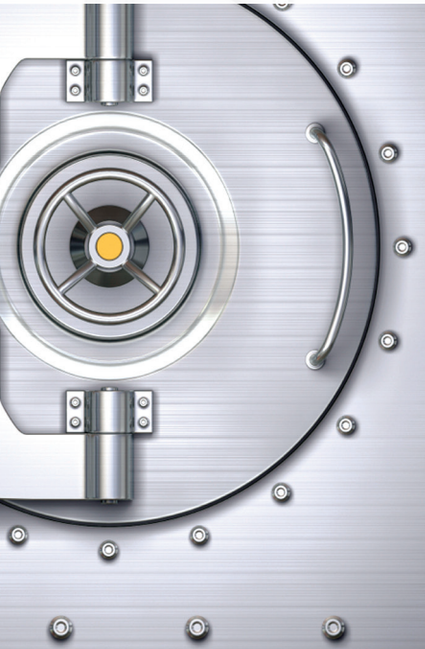
Identificar y controlar la evasión

La mayoría de las organizaciones cuentan con políticas de seguridad que funcionan junto a controles diseñados para hacer cumplir estas políticas. Para eludir los controles de seguridad, como por ejemplo los firewalls, se utilizan proxies externos, herramientas de administración de servidor/escritorio remoto y aplicaciones sobre túneles cifrados. Sin la capacidad para identificar y controlar estas herramientas, la empresa no puede hacer cumplir sus políticas de seguridad, exponiéndose a los mismos ataques cibernéticos para los que sus controles de seguridad fueron diseñados. Su próximo firewall debe ser capaz de hacer frente a estas herramientas de evasión.

2

Dejar de pensar en:

Puertas cerradas.



Empezar a pensar en:

Libertad.

Descifrar el tráfico SSL y controlar el uso de SSH

El número de aplicaciones de uso común en su red que han adoptado el SSL como medio de cifrado de tráfico se sitúa actualmente en torno al 25%. El aumento en el uso del HTTPS por parte de muchas aplicaciones de alto riesgo y alto beneficio para el usuario final, junto con la capacidad de los usuarios para habilitar manualmente el SSL en muchos sitios web, implica que su equipo de seguridad de red tiene un ángulo muerto grande y creciente. Puesto que el cifrado SSH suele ser más utilizado por empleados con conocimientos de tecnología, el ángulo muerto en lo que respecta al cifrado puede ser aún mayor de lo que pensaba. Su próximo firewall ha de ser capaz de descifrar e inspeccionar el tráfico SSL en cualquier puerto; además, debe ser lo suficientemente flexible como para dejar pasar los segmentos seleccionados de tráfico SSL (por ejemplo, el tráfico de Internet de organizaciones de atención sanitaria) y forzar el uso lícito de SSH mediante políticas.

3

Proporcionar control funcional de las aplicaciones

Existe una gran cantidad de aplicaciones con funciones significativamente diferentes, lo que supone para su organización una gran variedad de perfiles de riesgo y valor. Existen muchos ejemplos orientados tanto a la empresa como al usuario final. WebEx frente a WebEx Desktop Sharing y Google Mail frente a Google Talk. Si su empresa depende en gran medida de la propiedad intelectual, las aplicaciones externas para compartir el escritorio y para la transferencia de archivos pueden representar riesgos para la seguridad y para el cumplimiento de normativas. Su próximo firewall debe evaluar continuamente el tráfico y controlar los posibles cambios. Si se introduce una función o característica diferente en la sesión, el firewall debe ser capaz de reconocer el cambio y llevar a cabo una comprobación de políticas.

1

Dejar de pensar en:

¿Qué hay en la red?

Empezar a pensar en:

La red es segura.

Administrar sistemáticamente el tráfico desconocido

Existe siempre una pequeña cantidad de tráfico desconocido en todas las redes. Puede ser una aplicación personalizada, una aplicación comercial no identificada o una amenaza. Sea cual sea el tráfico desconocido, éste representa importantes riesgos para la seguridad y para su negocio. Bloquear todo el tráfico desconocido impedirá el normal desarrollo de su negocio. Permitirlo a ciegas es un riesgo muy alto. Un enfoque equilibrado pasa por aplicar la clasificación, el análisis y las políticas de control al tráfico de una manera sistemática para reducir el riesgo sin afectar a la actividad del negocio. Su próximo firewall debe ser capaz de clasificar todo el tráfico, caracterizar fácilmente las aplicaciones personalizadas para que sean "conocidas" por las políticas de seguridad de red, analizar el tráfico para ver si se trata de una amenaza y proporcionar visibilidad predecible y políticas de control sobre el tráfico que siga considerándose desconocido.

5

Bloquear las amenazas conocidas y desconocidas en las aplicaciones permitidas

Las empresas adoptan una amplia gama de aplicaciones para el desarrollo del negocio, bien alojadas internamente o fuera de su ubicación física. Independientemente de que se trate de servicios alojados de SharePoint, Box.com, Google Docs, Microsoft Office365 o de una aplicación de extranet alojada por uno de sus socios, su organización debe poder utilizar una aplicación que funcione en puertos no estándar, que utilice SSL o que comparta archivos. Estas aplicaciones permiten el desarrollo del negocio, pero representan riesgos de seguridad para el mismo. Su próximo firewall debe ser capaz de habilitar dichas aplicaciones de forma segura, lo que significa que debe permitir el funcionamiento de una aplicación a la vez que controla la transferencia por tipos de archivo y ser capaz de explorar la aplicación en busca de posibles amenazas, tanto conocidas como desconocidas, sobre todos los puertos.

6

Dejar de pensar en:

Confinado.

Empezar a pensar en:

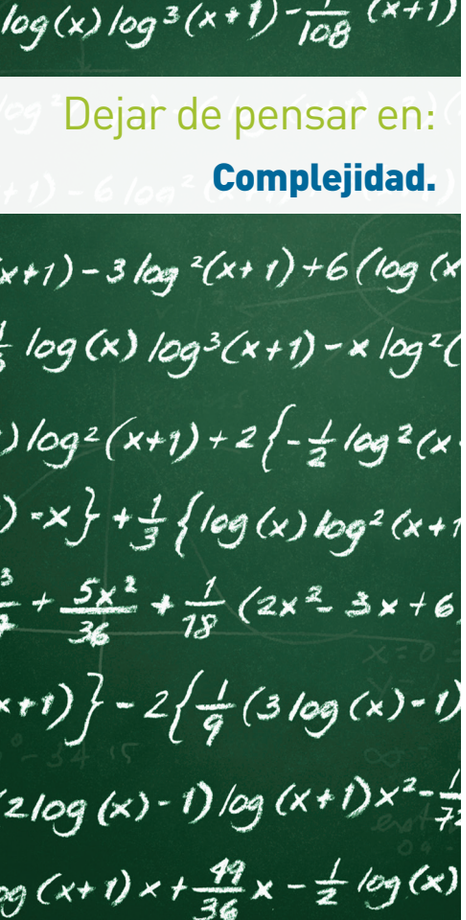
Libertad de movimientos.

Habilitar seguridad sistemática para todos los usuarios y dispositivos

Un número significativo de sus usuarios está trabajando remotamente y espera conectarse a sus aplicaciones a través de la WiFi, la banda ancha inalámbrica o cualquier medio disponible; además, desea hacerlo sin problemas y de forma sistemática. Independientemente de la ubicación del usuario o del dispositivo que esté utilizando, debe aplicarse el mismo estándar de control de aplicaciones. Si su próximo firewall permite la visibilidad de aplicaciones y el control del tráfico dentro de las cuatro paredes de la empresa pero no en el exterior, dejará de tener el control sobre el tráfico con mayor riesgo potencial.

Simplificar la seguridad de red

Su equipo de seguridad está sobrecargado porque gestiona múltiples fuentes de información, varias políticas de seguridad y las interfaces de gestión de los dispositivos asociados. Añadir aún más elementos a un equipo ya sobrecargado no será de ayuda en absoluto. Dado que las instalaciones típicas de firewall tienen miles de reglas, su próximo firewall ha de facilitar el trabajo a sus equipos de seguridad gracias a su capacidad de identificar, controlar, investigar e informar sobre las aplicaciones, los usuarios y los contenidos que atraviesan la red.



Dejar de pensar en:

Complejidad.

Empezar a pensar en:

Simplicidad.

Ofrecer la misma capacidad y rendimiento con un control total de aplicaciones

Muchas empresas luchan por hallar un equilibrio entre rendimiento y seguridad. Con demasiada frecuencia, habilitar funciones de seguridad de red significa degradar la capacidad y el rendimiento. Si su próximo firewall está diseñado correctamente, este compromiso no es necesario. Dada la necesidad de realizar tareas de alta intensidad computacional (como por ejemplo la identificación de aplicaciones) ejecutadas sobre altos volúmenes de tráfico con baja latencia, su próximo firewall debe poseer un hardware optimizado para tareas específicas, tales como networking, seguridad y análisis de contenidos.

9

Dar soporte a las mismas características, ya sea de forma hardware o virtualizada

Las ventajas de la virtualización son importantes, pero también lo son los problemas de seguridad asociados. Los firewalls tradicionales no gestionan con eficacia los procesos automáticos de levantar y cerrar instancias de máquinas virtuales debido a su dependencia de puertos y protocolos. La naturaleza dinámica de los centros de datos virtualizados dicta que el flujo de tráfico en el entorno virtual (tráfico este-oeste) deba protegerse también de manera dinámica y automática. Su próximo firewall debe soportar las mismas características tanto en formato virtual como hardware y debe integrarse con el entorno de virtualización para simplificar la creación de políticas basadas en aplicaciones, conforme se levantan y se cierran máquinas virtuales y aplicaciones.

10

Dejar de pensar en:

Ellos.

Empezar a pensar en:

Nosotros.

En conclusión

Las aplicaciones son el medio con el que los usuarios realizan su trabajo, en un equilibrio constante entre las prioridades personales y profesionales. A medida que los usuarios siguen adoptando nuevas aplicaciones y tecnologías, introducen, de forma involuntaria, nuevos riesgos de ciberseguridad. Permitir todo es irracional y obstaculizar su adopción puede impedir el normal desarrollo de su negocio. Por este motivo, la habilitación segura de aplicaciones es la mejor forma de establecer correctamente las políticas. La habilitación segura de las aplicaciones se implementa mejor si se usa un enfoque sistemático en la determinación de los patrones de uso y la necesidad del negocio y, a continuación, se documenta el uso adecuado con políticas evolutivas y se obliga a su uso con la tecnología. La guía "10 cosas que su próximo firewall debe hacer" puede ayudarle a establecer los controles necesarios, especialmente en un ámbito muy variado y heterogéneo de aplicaciones y amenazas. Sin una infraestructura de seguridad de red que haga frente a tal diversidad, no se puede habilitar de forma segura las aplicaciones necesarias y gestionar el riesgo. Un firewall de última generación que cumpla con estas 10 capacidades es en realidad todo lo que necesita.

paloalto NETWORKS®

la compañía de seguridad en la red™

¿Desea obtener más información?

Vea una demostración:

http://www.paloaltonetworks.com/demo

Solicite una evaluación de seguridad de red:

http://www.paloaltonetworks.com/avr