STORMSHIELD

ARTÍCULOS DE OPINIÓN

CORTAFUEGOS CORPORATIVOS: VUELTA A LO FUNDAMENTAL

Stéphane Prevost
Product Marketing Manager, Stormshield

La importancia de utilizar un cortafuegos en el lugar de trabajo está bien establecida. Pero en respuesta a las sofisticadas amenazas actuales, un cortafuegos perimetral ya no es suficiente. En un entorno en constante evolución, ¿cómo integrar un cortafuegos en su arquitectura de red? ¿Y cómo sacarle el máximo partido?

Dónde ubicar un cortafuegos, cómo segmentar una red, el enfoque de «*Zero Trust*», la gestión y supervisión centralizadas; le contamos todo lo que necesita saber para hacer el mejor uso de un cortafuegos en su arquitectura de red.

ENTENDER LA NECESIDAD Y EL PERÍMETRO DE PROTECCIÓN

El cortafuegos es uno de los pilares fundamentales de la seguridad perimetral de las empresas. Concebido históricamente como un muro impenetrable alrededor del borde de la red, su función ha evolucionado considerablemente desde entonces. Para responder al cambiante panorama de las amenazas y bloquear todos los intentos de movimiento lateral del malware, los administradores de sistemas han tenido que replantearse el uso de los cortafuegos, añadiendo nuevas capas de protección.

El lugar correcto para un cortafuegos en una arquitectura de red depende de la necesidad de seguridad. Y el cortafuegos tradicional en el borde de la red – aunque sigue siendo una parte esencial del arsenal de seguridad – ya no es suficiente para proporcionar un buen nivel de protección. Los cambios en los modelos de trabajo (nómadas digitales, teletrabajo, SaaS y otras infraestructuras en la nube), junto con las ciberamenazas cada vez más sofisticadas, han obligado a las empresas a ampliar el uso de cortafuegos. Ahora es necesario ir más allá y desplegar cortafuegos en diferentes puntos del perímetro de seguridad de la empresa. Pero este perímetro de seguridad está evolucionando y se compone de una gran variedad de elementos, tanto internos como externos.

Entonces, ¿cuáles son las **ubicaciones estratégicas para un cortafuegos?** En un punto de conexión a Internet, en el borde o en el centro de la red, en la nube... las opciones son numerosas, y dependerán de sus objetivos de seguridad y de la capacidad de sus cortafuegos. Tenga en cuenta que, de acuerdo con el principio de defensa en profundidad, es aconsejable instalar al menos dos cortafuegos para crear una DMZ (zona desmilitarizada). Esta doble barrera proporciona un sello adicional contra los flujos de datos (potencialmente maliciosos). El objetivo es implantar varios niveles de confianza, desde Internet a la LAN, e incluso a los centros de datos y otros entornos en la nube.

Y los cortafuegos de nueva generación (NGFW) pueden llevar aún más lejos la seguridad de la arquitectura de red; por ejemplo, con la segmentación de red y el enfoque de *Zero Trust*. Le explicamos cómo..

LA IMPORTANCIA DE LA SEGMENTACIÓN DE RED Y EL ZERO TRUST

¿Por qué es tan importante la segmentación de la red? Porque el modus operandi de los ciberdelincuentes incluye una fase de reconocimiento. Una vez comprometida e infiltrada una máquina, escanean los equipos conectados a la red para preparar un posible ataque de rebote. Para evitar cualquier propagación, debe aplicarse una segmentación estricta en la red principal y en las subredes. Dividiendo esta área en zonas distintas, un administrador puede aplicar estrictos controles de acceso y flujo.

La creación de una DMZ, como se ha mencionado anteriormente, es un «*caso especial de segmentación*», según **Simon Dansette**, jefe de producto de Stormshield. «*Tiene la ventaja de poder compartimentar la red para una necesidad específica bloqueando todas las opciones de movimiento lateral*». Como señala **Sébastien Viou**,

director de ciberseguridad y gestión de producto de Stormshield, «*la interrupción de protocolos es un principio diseñado para interrumpir todos los flujos de red, transporte y aplicaciones interpretándolos y reescribiéndolos. En esencia, debe ser imposible realizar un enrutamiento directo entre los dos cortafuegos*». El principio de la doble barrera no consiste en acumular una serie de cortafuegos «*pensando que el primero de ellos bloqueará las vulnerabilidades del otro*», sino en «*crear zonas de confianza y aplicar reglas de seguridad coherentes mientras se controlan los flujos de datos*». En entornos industriales sensibles, esta segmentación de la red permite tomar una serie de medidas. En primer lugar, aísla los entornos de TI y OT, deteniendo el movimiento lateral del ransomware que ha infectado una infraestructura de TI y trata de propagarse a los entornos de producción. En segundo lugar, esta segmentación puede llegar hasta el corazón de la OT, lo más cerca posible de las máquinas y los PLC, con la aplicación de un filtrado granular de los flujos, hasta el comando individual enviado.

Para garantizar que los usuarios y las máquinas que se conectan a las redes son legítimos, las empresas también pueden aplicar el concepto de *Zero Trust*. **Esta filosofía de *Zero Trust* se basa en el principio de que no debe suponerse que los usuarios y los componentes de la red son confiables por defecto, sino que deben demostrar su identidad y legitimidad cada vez que solicitan acceso a los recursos**. La arquitectura Zero Trust Network Access (acceso a la red basado en *Zero Trust* o ZTNA) incluye tanto a usuarios como a dispositivos en la autenticación y autorización del acceso a la red. El acceso es entonces granular y específico para las necesidades del usuario. «*En una arquitectura de Zero Trust, el cortafuegos debe estar vinculado en primer lugar a tecnologías de autenticación sólidas para identificar al usuario. Pero también debe comprobar que el puesto de trabajo que se va a autenticar está en buen estado*», explica Dansette. Los últimos modelos de cortafuegos utilizan esta filosofía para permitir el control de acceso de los usuarios, en lugar de filtrar únicamente en función de la IP (como hacían los cortafuegos tradicionales). Las reglas de filtrado del tráfico permiten aplicar políticas de seguridad granulares y en tiempo real. Dansette explica que «*ahora existen interacciones entre las soluciones de tipo EDR y los cortafuegos que autorizan a un usuario a conectarse. Estos mecanismos llevan el proceso de autenticación un paso más allá*». El cortafuegos de nueva generación se convierte así en un elemento clave de la arquitectura de *Zero Trust*.

Mediante la aplicación de reglas específicas o comunes, la actualización de los equipos y la monitorización y supervisión, ya sea física o virtualizada, la proliferación de cortafuegos en las empresas está obligando a los administradores de sistemas a replantearse la forma de gestionarlos, en un paso de la gestión unitaria a la centralizada. Se trata de una herramienta que se ha convertido en una necesidad.

LA NECESIDAD DE UNA GESTIÓN CENTRALIZADA DE CORTAFUEGOS

Ya sea en el borde o en el centro de una red, cerca de los equipos industriales o alojados en la nube, el número de cortafuegos y sus ubicaciones se han multiplicado hasta tal punto que gestionarlos puede convertirse rápidamente en una tarea compleja. Despliegue, configuración, mantenimiento, gestión de parches... Según Dansette, la gestión centralizada permite «*reducir la complejidad de la gestión de las distintas conexiones de cortafuegos y reducir el tiempo de administración de la red y, por tanto, los costes inherentes*».

La gestión centralizada también simplifica el proceso de cumplimiento de las normas de seguridad, garantizando que todas las políticas de seguridad se aplican de manera uniforme a todos los cortafuegos de la red. Esta es una gran ventaja para los MSSP y los distribuidores de TI. **La gestión centralizada permite gestionar la configuración de varios cortafuegos con una sola herramienta y administrarlos todos desde una única plataforma**. Los cambios pueden realizarse de forma rápida y sencilla, lo que aporta seguridad a sus clientes y aumenta la productividad de sus equipos humanos.

Además, al centralizar la gestión de los registros de log, los indicadores pueden visualizarse desde una única interfaz, lo que facilita la supervisión y la elaboración de informes. Cuando los registros de log se recopilan, almacenan y archivan en una única plataforma, los administradores de sistemas pueden encontrar y corregir más fácilmente los problemas de configuración. Según Dansette, «*la centralización proporciona una visión de conjunto que facilita el análisis de dónde radica el problema y su posterior corrección en el cortafuegos infractor. Esto facilita la fase de resolución de problemas a los administradores de sistemas y ahorra tiempo en momentos de gran tensión*».

¿Y qué hay del futuro? Está claro que los puntos de protección de red no son la única área de crecimiento dentro de la empresa; los puntos de protección de puestos de trabajo siguen la misma tendencia. Sin embargo, el éxito recurrente de los ciberataques demuestra la ineficacia de este enfoque. Y es que la proliferación de soluciones de detección provoca numerosos eventos variados con patrones de comportamiento difíciles de interpretar y correlacionar para los administradores. Esta falta de visibilidad limita la capacidad de reacción, lo que en la práctica se traduce en un menor nivel de protección. Para responder a este problema y permitir una gestión más completa, se han desarrollado ofertas XDR (eXtended Detection & Response). El objetivo es triple: reducir los riesgos, correlacionar los eventos notificados por las distintas soluciones de ciberseguridad y mejorar la productividad ciber-operativa de las organizaciones.

STORMSHIELD

Stormshield ofrece innovadoras soluciones de seguridad integrales para proteger las redes (Stormshield Network Security), los puestos de trabajo (Stormshield Endpoint Security) y los datos (Stormshield Data Security). **www.stormshield.com**