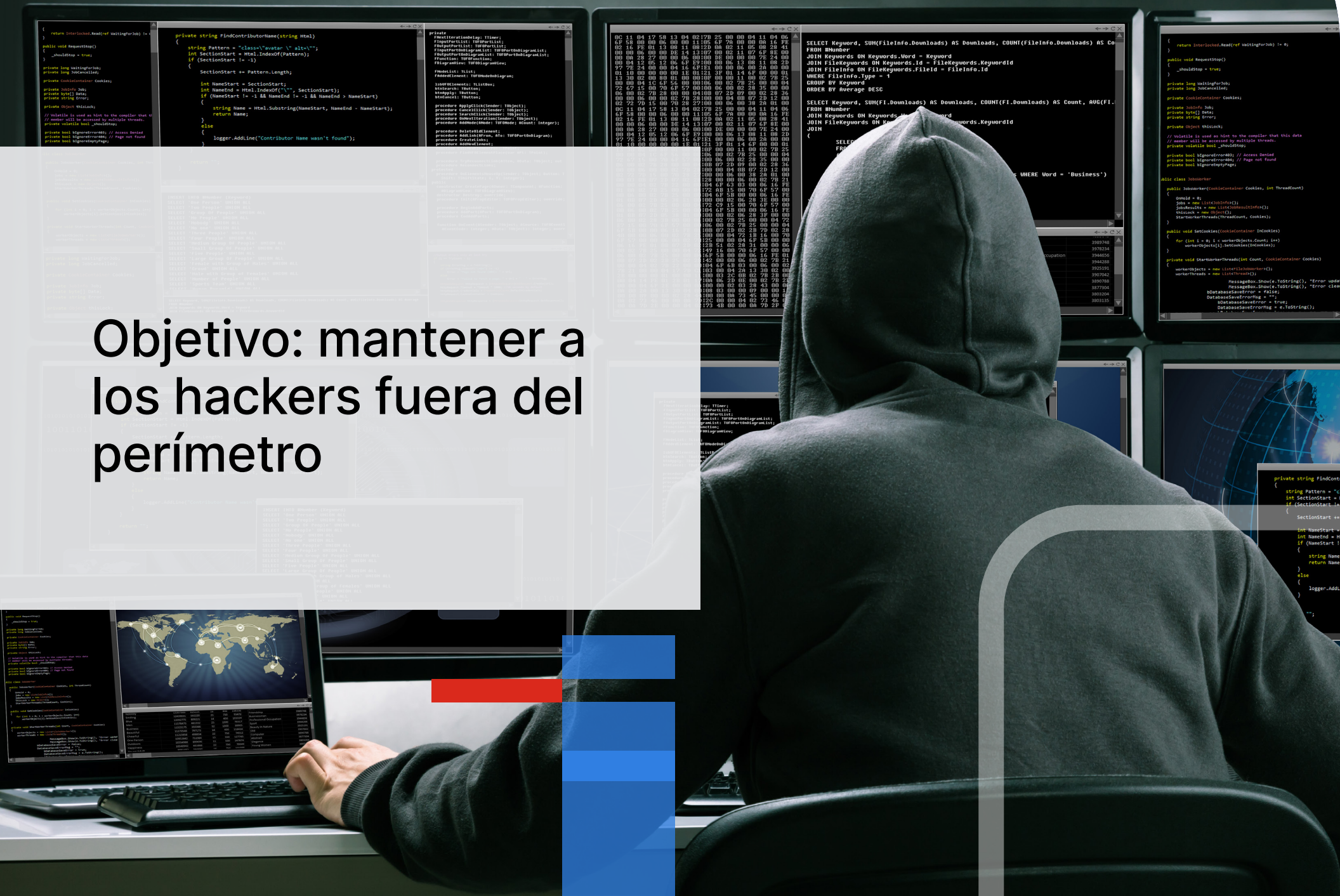
FORTINET



Objetivo: mantener a los hackers fuera del perímetro

Índice

Resumen

En la actualidad, los usuarios necesitan contar con una red que les permita conectarse a cualquier recurso desde cualquier lugar y con cualquier dispositivo. Al mismo tiempo, las redes de campus y de los centros de datos deben funcionar en una arquitectura de TI híbrida que abarca sucursales de nueva generación, redes multi-cloud públicas y privadas, teletrabajadores y soluciones de software como servicio (SaaS). Todo esto pone bajo muchísima presión a los equipos de seguridad de las empresas, de quienes se espera que consigan ofrecer total visibilidad en un entorno de red distribuido y en constante cambio para proteger y supervisar cada dispositivo y a cada usuario que acceda a los datos, aplicaciones y cargas de trabajo. Para los ciberdelincuentes, es la coyuntura perfecta para infiltrarse en su red por el perímetro. Y, una vez dentro, pueden desatar el caos.

Por desgracia, la mayoría de las herramientas de seguridad tradicionales, como los firewalls obsoletos, no se diseñaron para hacer frente a un desafío de tal magnitud, sino como puntos de control de la red estáticos en los que los flujos de trabajo y los datos eran muy predecibles. Pero eso queda ya muy atrás. Lo que hace falta ahora es una solución de firewalls de malla híbrida (HMF) que integre a lo largo de la red firewalls de nueva generación de distintos formatos con el objetivo de centralizar la gestión y coordinar la respuesta a las amenazas. La solución debe, además, proteger los activos y a los usuarios estén donde estén, unificar y consolidar las soluciones distribuidas para reducir gastos, simplificar la gestión, aplicar la automatización y redimensionar los servicios y el ancho de banda de forma dinámica para satisfacer las necesidades del negocio a medida que vayan cambiando.

Problemas nuevos

Los centros de datos siguen siendo esenciales, pero ya no son la principal ubicación de las aplicaciones empresariales, que ahora pueden implementarse en cualquier lugar. Las transacciones o los flujos de trabajo pueden recorrer varios entornos y aplicaciones diferentes, por lo que el origen, el destino y la ruta de los datos pueden cambiar repetidas veces, y así supervisar y proteger la transacción se vuelve imposible.

La adopción del 5G se lo ha puesto muy difícil a los firewalls tradicionales, sobre todo teniendo en cuenta que, en la actualidad, se cifra el 95 % del tráfico.[1] El tráfico cifrado, y en especial los túneles SSL/TLS (capa de sockets seguros/seguridad de la capa de transporte), se utiliza comúnmente para proteger las transacciones y los accesos remotos. El problema es que los ciberdelincuentes también recurren al cifrado para ocultar actividades maliciosas con el objetivo de, por ejemplo, robar datos y secretos empresariales o perpetrar ataques de ransomware. La mayoría de los firewalls no pueden descifrar el tráfico e inspeccionarlo sin que el rendimiento y la experiencia del usuario se vean seriamente afectados. Y, en consecuencia, la mayor parte del tráfico cifrado —sobre todo los datos que se transmiten a velocidades muy altas— se queda sin inspeccionar.

Los entornos multi-cloud y el trabajo híbrido también están cambiando los requisitos en materia de seguridad. La nube hace posible el desarrollo ágil de aplicaciones y la escalabilidad horizontal y vertical para hacer frente a una mayor demanda de acceso a las aplicaciones por parte de los teletrabajadores. Aun así, sigue siendo necesario alojar en el centro de datos on-prem muchas de las aplicaciones críticas para la empresa, entre otras cosas, por motivos de cumplimiento o privacidad o para proteger la propiedad intelectual y los registros confidenciales. Sin embargo, la mayoría de los firewalls tradicionales no cubren las necesidades de los centros de datos híbridos y dificultan el uso de los modelos de interconexión del usuario al centro de datos, del centro de datos a la nube, del usuario a la nube o de un centro de datos a otro, por poner unos ejemplos.

Al final lo que pasa es que las empresas acaban recurriendo a soluciones enrevesadas para intentar que varios productos dispares funcionen más o menos juntos. Esto hace que la infraestructura del centro de datos se vuelva más compleja, ya que hay que intentar que los datos se transmitan con fluidez entre los distintos sistemas y aplicaciones en un entorno con cada vez más dispositivos, servidores, conmutadores, enrutadores, firewalls, equilibradores de carga y demás componentes interconectados. A medida que aumentan el número de dispositivos y el volumen de tráfico de datos, crece también la complejidad de la red, y gestionar, supervisar y solucionar los problemas se vuelve más complicado.

Los centros de datos siguen siendo esenciales, pero ya no son la principal ubicación de las aplicaciones empresariales, que ahora pueden implementarse en cualquier lugar.

Soluciones nuevas

Para dar cabida a las arquitecturas híbridas y protegerlas, es necesario poder ver desde un solo lugar todo lo que ocurre en la red distribuida. Esto incluye saber qué usuarios y dispositivos están conectados a la red y a qué recursos y aplicaciones acceden. Pero no solo eso: hay que tener la capacidad de detectar los comportamientos anómalos y la actividad maliciosa en cualquier lugar del entorno en el que puedan aparecer. Otra de las claves para detener las amenazas es reunir todos los recursos de seguridad necesarios para coordinar la respuesta de manera oportuna. Para adaptarse a estas redes en expansión y proteger todos sus perímetros, muchas empresas han empezado a adoptar soluciones SASE (Secure Access Service Edge), SD-WAN (red de área extensa definida por software) y ZTNA (acceso Zero Trust a la red) independientes. Esto no solo genera complejidad, sino que, además, fractura la visibilidad, deteriora la experiencia de usuario y limita la capacidad de responder eficazmente a los ataques.

Lo que hace falta es un modelo basado en firewalls de nueva generación (NGFW) que integre estas funciones y ofrezca una seguridad coordinada en función del contexto para toda la red. Las soluciones HMF combinan soluciones on-prem y nativas en la nube con un componente de gestión unificada. Las soluciones de seguridad unificadas proporcionan una protección coordinada para diferentes elementos de la informática empresarial, como los sitios corporativos, las sucursales, los campus, los centros de datos, las nubes públicas y privadas y los teletrabajadores. Gracias a la interoperabilidad nativa que ofrecen, las implementaciones de HMF simplifican las operaciones, garantizan el cumplimiento, reducen la complejidad y permiten automatizar una gran cantidad de aspectos para mejorar la eficiencia operativa. Da igual si todos sus firewalls son on-prem, si están todos alojados en la nube o si utiliza una combinación de ambos: el valor de una solución así radica en que permite gestionarlos todos de manera centralizada y unificada.

Otro punto positivo es que tampoco importa dónde necesite implementar la solución de seguridad (en un campus, en un centro de datos, en una red multi-cloud, en una sucursal, en casa de sus empleados, etc.), porque los casos de uso son muy similares. Para entenderlos, es necesario descomponer la seguridad en tres funciones básicas: protección, convergencia y escalabilidad. Cuando tenga claros estos tres conceptos, podrá poner en marcha una estrategia de seguridad diseñada para ofrecer una experiencia de usuario impecable y una protección coherente con los objetivos empresariales.

Protección

Obviamente, el principal objetivo es evitar que las amenazas entren en la red; pero, cuando esto no es posible, lo primero que habrá que hacer será minimizar las interrupciones de la actividad empresarial lo antes posible. Los NGFW deben tener en cuenta todo el ciclo de vida de las aplicaciones, incluidas sus interacciones con las herramientas que se utilicen para acelerar tanto el acceso a ellas como su uso. Será necesario, entre otras cosas, ofrecer filtrado web básico en combinación con funciones avanzadas de reconocimiento de imágenes y filtrado de contenido web para garantizar que se haga un uso aceptable de las aplicaciones y que se cumpla la normativa en todo momento.

Una solución NGFW también debe incluir funciones de seguridad avanzadas para prevenir los ataques conocidos, desconocidos y de día cero mediante sistemas de prevención de intrusiones (IPS) y antimalware integrados. Además, debe poder recibir de forma ininterrumpida flujos de inteligencia de amenazas compartida procedentes de productos complementarios, como sistemas de seguridad del correo electrónico y sandboxes, para detectar y prevenir las amenazas más nuevas.

Por último, debe ser compatible con otras soluciones, como productos de detección y respuesta en el endpoint

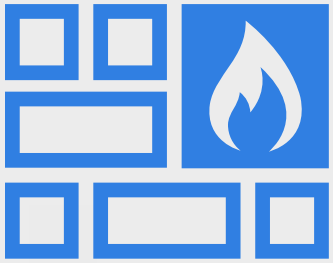
(EDR), firewalls de aplicaciones web (WAF) y demás sistemas de seguridad. Esta combinación (protección nativa contra amenazas más integración con otras tecnologías) garantiza que la red esté bien protegida frente a todas las amenazas actuales y emergentes.

Convergencia

Otra de las cosas que debería hacer un NGFW es ofrecer total visibilidad de los ataques sofisticados que se esconden en los canales HTTPS seguros para robar información y cargar ransomware. También debería integrar funciones de seguridad y de red básicas como un todo en una solución unificada —independientemente de que se entregue como NGFW on-prem o como un SASE en la nube— que combine funciones de enrutamiento y de conectividad avanzadas con herramientas de seguridad dinámicas.

Por otra parte, debe poder identificar cualquier dispositivo, aplicación o usuario que solicite acceso a la red y asignarle automáticamente el segmento correspondiente, para lo que se necesitan servicios de proxy integrados de forma nativa. Cuando un dispositivo solicita acceso por primera vez, el firewall tiene que trabajar con clientes de endpoint (en el caso de los usuarios y los servidores) y soluciones de control de acceso a la red (en el caso de los dispositivos de Internet de las cosas [IoT] o de Internet industrial de las cosas [IIoT]). Además, debe admitir la autenticación multifactor para determinar el papel de los usuarios o dispositivos, vincularlos con las políticas correspondientes y darles acceso únicamente a las aplicaciones o segmentos de la red que necesitan para hacer su trabajo.

En el caso de las aplicaciones y los flujos de trabajo que van de un entorno a otro, el NGFW debe poder identificar qué políticas necesitan y aplicarles las mismas en todas partes. Con este modelo basado en la orquestación y aplicación de políticas coherentes y la gestión centralizada, la seguridad sigue a las aplicaciones, los flujos de trabajo y demás transacciones allá donde vayan.



En el caso de las aplicaciones y los flujos de trabajo que van de un entorno a otro, el NGFW debe poder identificar qué políticas necesitan y aplicarles las mismas en todas partes.

Escalabilidad

Independientemente de dónde se implemente un firewall, una cosa está clara: tiene que ser rápido. Y, en el futuro, tendrá que serlo aún más. Esto es así porque los centros de datos modernos generan y procesan cantidades ingentes de datos a gran velocidad para, por ejemplo, crear modelos avanzados de big data, conseguir las latencias bajas que necesitan para ciertas transacciones financieras de alta velocidad u ofrecer un rendimiento extraordinario para entornos extremadamente grandes y con un gran número de usuarios.

Cuando hablamos de «velocidad», nos referimos a lo rápido que puede inspeccionar los datos el firewall y a su capacidad de aplicar la automatización. Los NGFW deben proteger la red de los ataques de alta velocidad con funciones de seguridad avanzadas y coordinadas, sin que aprovisionarlos obligue a realizar tareas manuales lentas. Las operaciones manuales ralentizan las cosas y pueden dar lugar a errores de configuración que los ciberdelincuentes no dudarán en aprovechar para perpetrar ataques de ransomware o de otro tipo.

El problema es que la mayoría de los firewalls tradicionales ya no dan más de sí, por lo que no es posible ampliar su capacidad para responder a las necesidades empresariales, cada vez más exigentes. Esto es así porque no están diseñados para ofrecer el hiperrendimiento necesario hoy en día. Pero su mayor punto débil es otro: ejecutan procesadores estándar, mientras que ahora todo (tarjetas gráficas, teléfonos inteligentes, servidores de nube, etc.) viene con chips a medida. Y la seguridad requiere una gran potencia de procesamiento. La escalabilidad, tan necesaria para responder a los requisitos de rendimiento actuales, pasa por poder ofrecer todas las funciones de los firewalls sin sacrificar el rendimiento ni agotar los limitados presupuestos de TI y de seguridad.

[1] «Cifrado HTTPS en la Web», Informe de transparencia de Google, consultado el 1 de junio de 2023.

www.fortinet.com/es

4 de diciembre de 2023

2170366-0-0-ES