LAS 13 COSAS QUE DEBE PEDIRLE A SU PRÓXIMO CORTAFUEGOS

La rápida evolución de las tecnologías de la información ha cambiado la fisonomía del perímetro de las redes. Los datos y los usuarios están por todas partes. Los dispositivos proliferan a un ritmo cada vez más rápido, insostenible para la mayoría de las organizaciones. Al mismo tiempo, los equipos de TI, con el fin de agilizar la entrega de nuevas aplicaciones e impulsar el crecimiento empresarial, están incorporando la nube, el análisis de datos masivos y la automatización de procesos. Y, por si no fuera suficiente, la facilidad con que se puede acceder a las aplicaciones complica notablemente la configuración de las redes, lo que plantea un riesgo empresarial considerable. Las organizaciones deben minimizar este riesgo, pero sin ralentizar su actividad.

Es evidente que la ciberseguridad no está cumpliendo su cometido, ya que los ataques continúan interrumpiendo la actividad comercial. El gasto en seguridad nunca es suficiente y, ni con esas, desaparece el riesgo. Implementar herramientas y tecnologías independientes que no se integran entre sí deja la empresa en una posición vulnerable, carne de cañón para las amenazas. Las herramientas de seguridad que no fueron diseñadas para la automatización exigen que los analistas recopilen manualmente información de muchas fuentes inconexas antes de actuar. Urge un enfoque diferente.

Pero no empecemos la casa por el tejado: una estrategia de seguridad en la red eficaz debe cimentarse sobre una plataforma de cortafuegos de nueva generación. Con una arquitectura preventiva, los equipos de seguridad pueden adoptar fácilmente prácticas recomendadas que eviten que los ataques consigan su objetivo, utilicen la automatización y el análisis para reducir el trabajo manual, sustituyan los productos independientes e inconexos de su entorno e implementen unas innovaciones perfectamente integradas que refuercen y simplifiquen la seguridad.

Este documento describe la evolución del cortafuegos de nueva generación y enumera las trece cosas que debe hacer un cortafuegos de este tipo (NGFW, por sus siglas en inglés) para proteger su red y su negocio.

Las 13 cosas que debe pedirle a su próximo cortafuegos

Antes, los cortafuegos de inspección por estados clasificaban el tráfico atendiendo únicamente al puerto de destino, como podía ser el puerto TCP 80 para HTTP. La creciente necesidad de conocer bien el uso que se hace de las aplicaciones hizo que muchos proveedores añadieran visibilidad de las aplicaciones y otros «blades» de software o de hardware a sus cortafuegos de inspección por estados, que después vendieron como ofertas de gestión unificada (UTM, por sus siglas en inglés). Sin embargo, como las funciones se incorporaron como si de meros complementos se tratara (en lugar de integrarse de forma nativa), al final las UTM no mejoraron la seguridad.

A diferencia de las ofertas de UTM, los cortafuegos de nueva generación tienen en cuenta el uso de las aplicaciones para tomar decisiones basadas en las aplicaciones, los usuarios y el contenido. La integración no solo mejora la seguridad, sino que también simplifica las operaciones. Dado el éxito del modelo, el término «NGFW» ahora es sinónimo de «cortafuegos».

Normalmente, la selección del NGFW obedece a tres criterios: funciones de seguridad, operaciones y rendimiento. Las funciones de seguridad se corresponden con la eficacia de los controles de seguridad y la capacidad de su equipo para gestionar los riesgos asociados a las aplicaciones que pasan por su red, sin ralentizar la actividad de la empresa. Desde el punto de vista de las operaciones, la política de las aplicaciones debería ser accesible y fácil de gestionar. Asimismo, habría que aplicar la automatización en aras de reducir el esfuerzo manual y de que los equipos de seguridad puedan centrarse en actividades estratégicas que aporten valor. Los criterios de rendimiento son muy sencillos: el cortafuegos debe hacer lo que se supone que tiene que hacer con la capacidad que necesita su negocio. Además, las innovaciones que se vayan incorporando deben ser fáciles de adoptar e integrarse perfectamente. Aunque, dentro de estos criterios, los requisitos y las prioridades variarán, hay 13 cosas que debe hacer su próximo cortafuegos.

Antes de que termine 2019, el 90 por ciento de las conexiones a Internet empresariales de la base instalada estarán protegidas con cortafuegos de nueva generación.[1]

Requisitos del NGFW

1. Identificar las aplicaciones independientemente del puerto, el protocolo, las tácticas evasivas o el cifrado.
2. Identificar a los usuarios independientemente del dispositivo o de la dirección IP.
3. Descifrar el tráfico cifrado.
4. Proteger en tiempo real frente a las amenazas conocidas y desconocidas incorporadas en las aplicaciones.
5. Proporcionar un rendimiento en línea predecible de varios gigabits.

1. Identificar a los usuarios y habilitar el nivel de acceso adecuado

El problema

Dentro de su red, y también de Internet, los empleados, los clientes y los socios se conectan a distintos repositorios de información. Estas personas y los numerosos dispositivos que utilizan representan los usuarios de su red. El riesgo de su organización está determinado, en gran medida, por su capacidad tanto para identificar a los usuarios más allá de la dirección IP como para reconocer los riesgos que entrañan según los dispositivos que utilicen, sobre todo si se han burlado las políticas de seguridad o se han introducido nuevas amenazas en la red. Además, los usuarios se mueven constantemente de un lado a otro y utilizan distintos dispositivos, sistemas operativos y versiones de aplicaciones para acceder a los datos que necesitan. Por otra parte, las subredes de direcciones IP solo se pueden asignar a las ubicaciones físicas, no a los usuarios, por lo que si esos usuarios se desplazan (aunque ni siquiera salgan de la oficina) la política no los sigue.

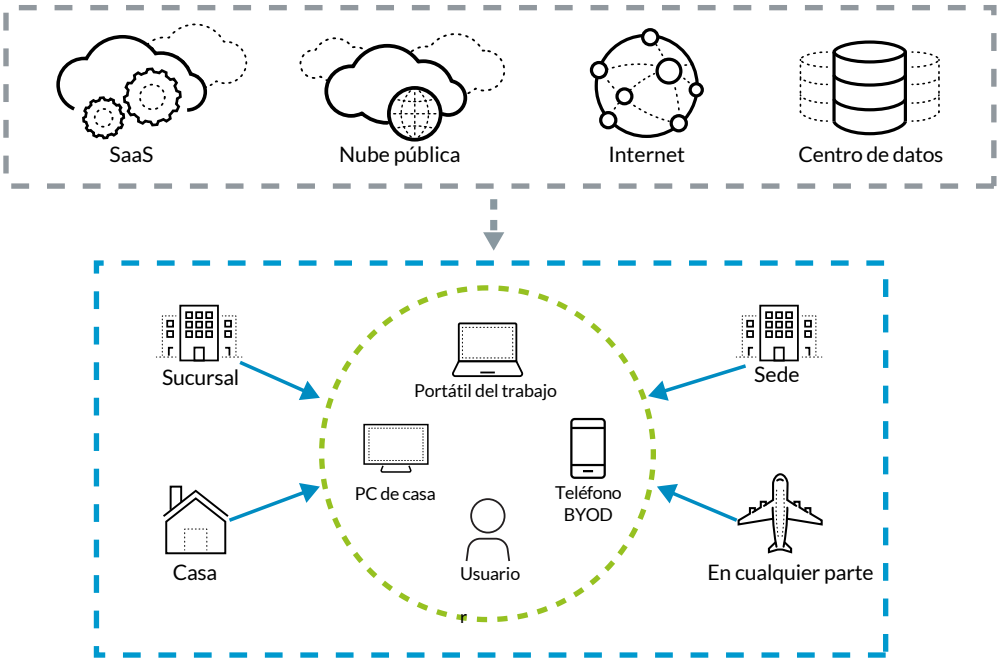

Figura 1: Los usuarios acceden a los datos desde distintos dispositivos y ubicaciones

1. Adam Hils, Jeremy D'Hoinne y Rajpreet Kaur, «Gartner Magic Quadrant for Enterprise Network Firewalls» (Cuadrante Mágico de Gartner para cortafuegos de redes empresariales, en inglés), 10 de julio de 2017.

Cómo se resuelve el problema

La información de los usuarios y los grupos debe integrarse directamente con las plataformas tecnológicas que protegen a las organizaciones modernas. Su próximo cortafuegos debe ser capaz de reconocer la identidad de los usuarios a partir de distintas fuentes, como la red VPN, los controladores de acceso a la WLAN, los servidores de directorio, los servidores de correo electrónico y los portales cautivos. Saber quién usa las aplicaciones de su red y quién puede estar transmitiendo una amenaza o transfiriendo archivos refuerza las políticas de seguridad y mejora los tiempos de respuesta en caso de incidente. El cortafuegos debe permitir la puesta en vigor de políticas que habiliten las aplicaciones de forma segura en función de los usuarios o de los grupos de usuarios, ya sea en el sentido entrante o saliente; por ejemplo, permitiendo configurar una política según la cual el departamento de TI sea el único grupo con acceso a ciertas herramientas, como SSH, telnet y FTP. Las políticas basadas en el usuario siguen a los usuarios, con independencia del dispositivo que utilicen o de si se encuentran en la sede central de la empresa, en una sucursal o en casa. Aun así, el problema de la identidad de los usuarios no se resuelve con clasificar a los usuarios y reflejarlo en informes que den cuenta de su actividad.

2. Prevenir robos y el uso abusivo de las credenciales corporativas

El problema

Los usuarios y sus credenciales son dos de los eslabones más débiles de la infraestructura de seguridad de una organización. Según el «Informe sobre investigaciones de brechas en los datos» de 2017 de Verizon, durante el periodo de 12 meses cubierto por el informe, el 81 % de las brechas relacionadas con incidentes de hacking utilizó contraseñas robadas o débiles.[2] Cuando los atacantes disponen de credenciales robadas, la probabilidad de conseguir sus objetivos aumenta, mientras que el riesgo de que los descubran disminuye. Para evitar el robo de credenciales, la mayoría de las organizaciones confía en la preparación técnica de los empleados, por lo que entra en juego el error humano. Los productos tecnológicos, sin embargo, suelen identificar los sitios de *phishing* conocidos y filtrar el correo electrónico.

El problema es que estos métodos no siempre son fiables: buscar sitios web maliciosos conocidos pasa por alto los que se han creado recientemente y los atacantes puede evadir la tecnología de filtrado de correo enviando enlaces a través de las redes sociales. Los atacantes pueden robar credenciales con facilidad gracias a las técnicas de *phishing*, a la ingeniería social y a la fuerza bruta, e incluso pueden comprarlas en el mercado negro. Los atacantes utilizan estas credenciales para introducirse en una red, desplazarse de forma lateral y obtener privilegios de mayor nivel para acceder a aplicaciones y datos de forma no autorizada.

Figura 2: Conclusiones del informe sobre investigaciones de brechas en los datos (DBIR) de 2017 de Verizon en cuanto al uso de contraseñas atacadas

Cómo se resuelve el problema

Las organizaciones deberían buscar un cortafuegos con funciones de análisis basadas en el aprendizaje automático para identificar los sitios web que roban credenciales. Si el análisis identifica un sitio como malicioso, el cortafuegos debería actualizarse y bloquearlo. Aun así, siempre habrá sitios web de *phishing* nunca vistos a los que tratará como «desconocidos». Su próximo cortafuegos debería permitirle bloquear el envío de credenciales corporativas a sitios web desconocidos. Por otra parte, es fundamental que proteja las aplicaciones y los datos confidenciales aplicando una política de autenticación multifactor (MFA, por sus siglas en inglés) que evite que los atacantes hagan un uso abusivo de las credenciales robadas. Integrado con los proveedores de MFA más conocidos, el cortafuegos puede proteger las aplicaciones (incluso las antiguas) que contengan datos confidenciales.

3. Habilitar todas las aplicaciones y funciones de control de forma segura

El problema

Cada vez son más las aplicaciones de su red que son capaces de funcionar en puertos no estándar o saltar de puerto (por ejemplo, las aplicaciones de mensajería instantánea, de intercambio de archivos P2P o de VoIP). Además, ahora los usuarios acceden a diversos tipos de aplicaciones, incluidas las de software como servicio o SaaS, desde distintos dispositivos y ubicaciones. El uso de esas aplicaciones puede estar autorizado, tolerado o no autorizado, y los usuarios ya tienen conocimientos suficientes como para forzar que las aplicaciones se ejecuten a través de puertos no estándar (por ejemplo, RDP o SSH). De hecho, las nuevas aplicaciones proporcionan a los usuarios un buen número de funciones que, aunque ayudan a reforzar la lealtad del usuario, pueden representar distintos perfiles de riesgo. Por ejemplo, Webex® es una herramienta valiosa en la empresa, pero utilizar la opción de uso compartido del escritorio para tomar el control del escritorio de un empleado desde un origen externo puede infringir el cumplimiento de normas internas o reglamentarias. Gmail® y Google Drive son otros dos buenos ejemplos. Una vez que los usuarios inician sesión en Gmail, que puede estar permitido por las políticas, lo tienen muy fácil para cambiar a YouTube® o Google Fotos, que no tienen por qué estarlo. Los administradores de seguridad quieren disfrutar de todo el control sobre el uso de estas aplicaciones y definir políticas que permitan o restrinjan el uso de ciertos tipos de aplicaciones y funciones mientras deniegan otros.

Cómo se resuelve el problema

Su próximo cortafuegos debe clasificar el tráfico por aplicación en todos los puertos en todo momento, de manera predeterminada, sin que por ello tenga que estar investigando todos y cada uno de los puertos que suele usar cada aplicación. El cortafuegos debe ofrecer, por una parte, visibilidad total del uso de las aplicaciones y, por otra, recursos para entender y controlar su uso (véase la figura 3). Por ejemplo, debería entender el uso de las funciones de las aplicaciones, como la transmisión de audio, el acceso remoto y la publicación de documentos, y aplicar controles detallados sobre ese uso, ya sea para los permisos de carga y descarga o el

2. "2017 Data Breach Investigations Report," Verizon, 2017, www.knowbe4.com/hubfs/rp_DBIR_2017_Report_execsummary_en_xg.pdf.

chat y la transferencia de archivos, entre otros. Pero se trata de un trabajo continuo. El concepto de clasificación de tráfico sobre la premisa «crear una regla estricta según la primera vez» no es una opción, ya que pasa por alto el hecho de que estas aplicaciones de uso general comparten sesiones y dan soporte a múltiples funciones. Si se introduce una función o característica diferente en la sesión, el cortafuegos debe realizar una comprobación de políticas. La supervisión continua del estado para comprender las funciones que cada aplicación puede admitir, y los diferentes riesgos asociados, es un requisito fundamental que debe cumplir su próximo cortafuegos.

Figura 3: Controlar el uso de las aplicaciones sin infringir las políticas

4. Cerrar las peligrosas brechas en las políticas

El problema

Los cortafuegos de antes permitían o bloqueaban el tráfico en función de los puertos y las direcciones IP. Este enfoque es inadecuado, ya que las reglas basadas en puertos permiten que las aplicaciones atraviesen el cortafuegos, sean o no legítimas. Para una aplicación es muy fácil atravesar un cortafuegos basado en puertos: basta con pasarse a otro puerto (con SSL y SSH) o utilizar puertos abiertos conocidos, como el 80 y el 443. Con el tiempo, los clientes acumulan miles de reglas basadas en puertos en sus cortafuegos, reglas que suelen migrar tal cuales a los cortafuegos de nueva generación. Estas reglas dejan brechas muy peligrosas en las políticas. Si quieren disfrutar de una seguridad eficaz, los clientes saben que deben migrar a las reglas basadas en aplicaciones, pero para ello hace falta hacer un esfuerzo manual significativo y, dada la escasez de profesionales cualificados, la mayoría de las organizaciones no tiene los recursos necesarios. Esto se convierte, así, en un riesgo de seguridad muy alto que puede originar interrupciones en la actividad empresarial. De hecho, según Gartner, hasta 2023, el 99 % de las brechas de seguridad en los cortafuegos estarán provocadas por errores de configuración, no por fallos en los propios cortafuegos.[3]

Cómo se resuelve el problema

Al evaluar su cortafuegos de nueva generación, busque uno que reduzca la complejidad de la gestión de las reglas y las políticas. Para ello, debe mostrarle qué aplicaciones se están ejecutando en la red, saber qué reglas del otro cortafuegos se les deben asignar y sustituirlas por unas nuevas. Un NGFW debería facilitar a su equipo de seguridad la sustitución de las reglas del cortafuegos anterior por unas políticas intuitivas basadas en las aplicaciones. Como las reglas basadas en el ID de las aplicaciones son fáciles de crear, entender y modificar en función de las necesidades que tenga la empresa en cada momento, minimizan los errores de configuración que dejan a su organización a merced de las brechas en los datos. Por su parte, estas políticas refuerzan la seguridad y son mucho más rápidas de gestionar.

5. Proteger el tráfico cifrado

El problema

Hoy en día, la mayoría del tráfico web de las empresas está cifrado y los atacantes utilizan técnicas de cifrado para ocultar las amenazas a los dispositivos de seguridad. Esto significa que, si no supervisan el tráfico cifrado, hasta las empresas que cuentan con unas medidas de seguridad maduras y exhaustivas pueden ser víctimas de ataques. Además, el protocolo SSH es de uso prácticamente universal y los usuarios finales pueden configurarlo fácilmente para ocultar la actividad que no esté relacionada con el trabajo.

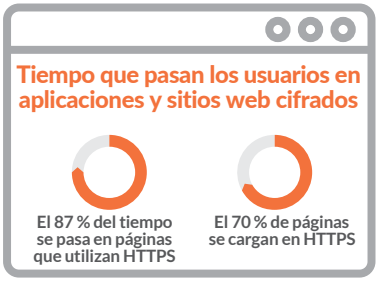

Figura 4: Conclusión sobre el tráfico cifrado de Google (2019)[4]

Cómo se resuelve el problema

La capacidad para descifrar el tráfico SSL y SSH es una función de seguridad básica. Los elementos clave necesarios son el reconocimiento y descifrado en cualquier puerto, tanto de entrada como de salida; unas políticas de control sobre el descifrado y los elementos de hardware y software necesarios para realizar el descifrado en decenas de miles de conexiones SSL simultáneas

3. Rajpreet Kaur, Adam Hils y John Watts, «Technology Insight for Network Security Policy Management» (en inglés), Gartner, 21 de febrero de 2019, www.gartner.com/doc/3902564/technology-insight-network-security-policy.
4. «Informe de transparencia de Google: Cifrado HTTPS en la Web». Fecha de acceso: 8 de septiembre de 2019, transparencyreport.google.com/https/overview?hl=en.

con rendimiento predecible. Sin embargo, su próximo cortafuegos debería ser lo suficientemente flexible como para descifrar fácilmente ciertos tipos de tráfico cifrado (como el HTTPS de sitios web sin clasificar) por medio de políticas, mientras que el de otros tipos (como el proveniente de organizaciones de servicios financieros conocidas) se deja intacto, con arreglo a los estándares de privacidad. Para reforzar la aplicación de políticas, el cortafuegos de nueva generación debe implantar medidas de seguridad y de equilibrio de cargas en los flujos descifrados que circulan entre varias pilas de dispositivos de seguridad. Esto permite prescindir del uso de descargadores de SSL dedicados, lo que reduce la complejidad de la red y facilita las operaciones de descifrado. Lea **Descifrado: por qué, dónde y cómo** para obtener una descripción general de esta importante función.

6. Detener las amenazas avanzadas para evitar que los ciberataques consigan sus objetivos

El problema

La mayor parte del malware moderno, incluidas las variantes de ransomware, utiliza técnicas avanzadas (p. ej., ocultando cargas maliciosas en archivos legítimos o empaquetando archivos para eludir la detección) con el objetivo de transportar ataques o exploits a través de dispositivos y herramientas de seguridad de red. Cada vez son más las organizaciones que implementan sandboxes virtuales para ejecutar análisis dinámicos, de modo que los atacantes han evolucionado para desarrollar técnicas que los evadan. Estas técnicas buscan actividades de usuarios, configuraciones del sistema o indicadores de tecnologías de virtualización específicas válidos. Con el aumento de la ciberdelincuencia sumergida, cualquier atacante, con independencia de su grado de pericia, puede comprar amenazas listas para usar capaces de identificar y eludir los entornos de análisis de malware.

Cómo se resuelve el problema

Su cortafuegos debería bloquear las amenazas conocidas de forma automática mediante el uso de servicios de seguridad integrados. A su vez, las amenazas desconocidas tienen que analizarse y contrarrestarse de manera automática. Su organización necesita un servicio que busque amenazas en todos los puntos del ciclo de vida del ciberataque, no solo cuando las amenazas entran en su red por primera vez. Una forma de reducir la exposición al riesgo es bloquear tipos de archivos de riesgo conocidos o acceder a URL maliciosas antes de poner en riesgo la seguridad de su red. Su cortafuegos debería proteger a su organización de los exploits de vulnerabilidades, del malware y de la actividad de comando y control (C2) sin necesidad de que usted tenga que gestionar ni mantener varios dispositivos de una sola función. Las firmas deben actualizarse automáticamente en cuanto se detecta nuevo malware, para que sus equipos de seguridad y de respuesta a incidentes puedan centrarse en lo importante mientras que su organización está protegida.

Figura 5: Disrupción en todos los pasos para impedir que los ataques consigan sus objetivos

Un cortafuegos de nueva generación que utilice distintos tipos de análisis para detectar amenazas desconocidas (análisis estático con aprendizaje automático, análisis dinámico y análisis de hardware) será capaz de llevar a cabo funciones de detección de alta fidelidad y resistente a las evasiones. Conviene que las firmas utilizadas por el cortafuegos estén basadas en el contenido y no en atributos específicos, con el fin de detectar las variantes de un mismo archivo, el malware polimórfico o la actividad de comando y control. Además, las firmas de comando y control basadas en el análisis de patrones de comunicación saliente son medidas de protección mucho más efectivas que, cuando se crean automáticamente, se adaptan a las velocidades que requieren las empresas. Por último, la infraestructura de seguridad basada en la nube es fundamental para la aplicación de políticas de seguridad. No solo permite detectar y prevenir amenazas a gran escala en toda la red, todos los endpoints y todas las nubes, sino que pone a su disposición todo un ecosistema abierto de innovaciones desarrolladas por proveedores de confianza.

7. Poner fin a los ataques que utilizan DNS

El problema

El protocolo DNS tiende a subestimarse, pero lo cierto es que ofrece un canal de ataque enorme y puede utilizarse para la distribución de malware, las actividades de comando y control o la exfiltración de datos. Al estar en todas partes, puede utilizarse en distintas fases de un ataque. Según el equipo de investigación de amenazas de Palo Alto Networks, Unit 42, casi el 80 % del malware utiliza DNS para conectarse a servidores de comando y control. Los atacantes lo usan para crear canales de comando difíciles de desmantelar o detectar, pues resulta sumamente eficaz para mantener la conexión con los servidores DNS. Una vez establecida la conexión, los atacantes pueden usar el tráfico DNS para distribuir malware en una red o canalizar la salida de los datos. Además, los atacantes desarrollan algoritmos de generación de dominios (DGA, por sus siglas en inglés), que crean automáticamente miles de dominios maliciosos que se pueden usar para llevar a cabo actividades de comando y control. Por desgracia, los ataques automáticos son cada vez más habituales, lo que hace prácticamente imposible descubrir o detener las amenazas.

Cómo se resuelve el problema

Su organización no puede limitarse a crear listas negras de ataques por DNS, pues esta táctica suele depender de canales de amenazas estáticos procedentes de dominios maliciosos conocidos. Sin la ayuda del análisis, es imposible prever de forma dinámica qué dominios podrían llegar a usarse para atacar. Detener un ataque que utilice DNS requiere un cortafuegos de nueva generación que pueda aplicar técnicas de análisis predictivo y de aprendizaje automático para identificar dominios maliciosos desconocidos de forma dinámica.

8. Proteger unos trabajadores itinerantes cada vez más numerosos

El problema

Los trabajadores itinerantes continúan creciendo y, con ello, el uso de dispositivos móviles para conectarse a las aplicaciones empresariales, por lo general a través de redes públicas y dispositivos que están abiertos a amenazas avanzadas. Fuera de las instalaciones de la organización, el riesgo aumenta, pues no hay ningún cortafuegos de red que detenga los ataques. Y para rizar el rizo, la nube y el uso de dispositivos personales por parte de los empleados (BYOD, por sus siglas en inglés) complican aún más el asunto. Además, las ubicaciones remotas y las sucursales pequeñas a menudo prescinden de una seguridad homogénea porque, desde el punto de vista operativo, resulta ineficiente y tremendamente caro implementar cortafuegos o desviar el tráfico a la sede central.

Cómo se resuelve el problema

Más allá de la red de su organización, los trabajadores itinerantes y las ubicaciones remotas necesitan acceder a las aplicaciones. Como también necesitan protegerse de los ciberataques dirigidos, las aplicaciones y los sitios web maliciosos, el *phishing*, el tráfico de comando y control, y demás amenazas desconocidas. Y sin una seguridad homogénea, esto es imposible. Es fundamental que su próximo cortafuegos ofrezca unos niveles mínimos de visibilidad, prevención de amenazas y aplicación de políticas de seguridad para proteger a los usuarios y ubicaciones que se encuentran fuera de la sede central de la organización. La respuesta está en un cortafuegos de nueva generación en la nube que vele por su seguridad sin necesidad de implementar hardware físico.

Cobertura completa para todos los sistemas operativos

Dada la avalancha de iniciativas BYOD y el aumento de los trabajadores itinerantes, ya no es una opción dar cobertura a los entornos y cargas de trabajo de Windows®, macOS®, Android® y Linux. De esta forma, las organizaciones pueden prevenir el malware conocido y desconocido con confianza, sin importar qué sistemas operativos prefieren sus usuarios.

9. Llevar la seguridad a entornos de nube en constante cambio

El problema

Los datos y las aplicaciones residen en todas partes: en su red y en la nube. Según el informe «RightScale 2018 State of the Cloud Report™» (en inglés), el 81 % de las empresas utiliza de media cinco nubes, ya sean públicas, privadas o híbridas.[5] En combinación con los entornos SaaS, las organizaciones deben proteger los datos confidenciales de la red y de un amplio abanico de entornos de nube. Además, las herramientas y técnicas de seguridad de antes, que estaban diseñadas para redes estáticas, ya no funcionan con las herramientas y las funciones nativas para la nube. Es más, lo normal es que los servicios de seguridad nativos de los propios proveedores de nube, como Google Cloud Platform (GCP™), Amazon Web Services (AWS®) y Microsoft Azure®, proporcionen funciones de protección para la capa 4 nada más y sirvan únicamente para ese proveedor de nube.

Cómo se resuelve el problema

Proteger su organización de manera eficaz pasa por implantar una seguridad en la nube que lleve la política desde la red hasta la nube, impida el acceso y el desplazamiento lateral (horizontal) del malware en la nube, simplifique la gestión y minimice el desfase en las políticas de seguridad a medida que cambian las cargas de trabajo virtuales. Su próximo cortafuegos debe proteger las aplicaciones y los datos residentes con la misma estrategia de seguridad que pueda haber establecido en su red física. Para proteger las implementaciones con varias nubes, el cortafuegos debe ser compatible con diversos entornos de nube y virtualización, incluidos los principales proveedores de nube pública y nubes privadas virtualizadas. El cortafuegos debe integrarse con servicios de nube nativos, como Amazon Lambda y Azure, y con herramientas de automatización, como Ansible® y Terraform®, para integrar la seguridad con sus proyectos de desarrollo basados en la nube.

Figura 6: Conclusiones de RightScale sobre las estrategias de varias nubes

5. «2018 State of the Cloud Report» (en inglés), RightScale, 2018, www.suse.com/media/report/rightscale_2018_state_of_the_cloud_report.pdf.

10. Usar una estrategia basada en el modelo Zero Trust (confianza cero)

El problema

Los modelos de seguridad convencionales siguen dando por supuesto que todo lo que se encuentra en la red de una organización es digno de confianza. Sin embargo, dado que los ataques y las amenazas que vienen de dentro son cada vez más sofisticados, es necesario adoptar nuevas medidas de seguridad que eviten su propagación interna. En los modelos de seguridad tradicionales, que están diseñados para proteger el perímetro, las amenazas que penetran en la red no se inspeccionan y permanecen ocultas, lo que les permite transformarse y moverse libremente para intentar extraer datos confidenciales de gran valor para la empresa. En el mundo digital, la confianza no es sino una vulnerabilidad.

Cómo se resuelve el problema

A la hora de evaluar un cortafuegos de nueva generación, busque uno que pueda actuar como una puerta de enlace de segmentación que haga posible una arquitectura Zero Trust, una estrategia diseñada alrededor de la premisa de que nunca hay que confiar en los usuarios, las aplicaciones y los datos, y que sus acciones deben verificarse siempre en un entorno. El principal objetivo del modelo Zero Trust consiste en no confiar nunca en un sistema y evitar que los atacantes saquen tajada de las vulnerabilidades ocultas en las aplicaciones de confianza. Con este enfoque, se limita el alcance de un ataque y se bloquea el movimiento lateral gracias a la microsegmentación basada en los usuarios, los datos y la ubicación. Una plataforma de cortafuegos de nueva generación debería ayudarle con estos pasos y habilitar el acceso seguro para todos los usuarios, con independencia de su ubicación; inspeccionar todo el tráfico; regirse por el criterio del mínimo privilegio para la aplicación de políticas de control de acceso, y detectar las amenazas avanzadas para bloquearlas. De este modo, se reduce drásticamente el número de vías de acceso a los datos y aplicaciones más esenciales de la empresa, lo que dificulta los ataques externos e internos. Le invitamos a ver este seminario web, en el que se explica cómo implementar una estrategia Zero Trust.

11. Mantener una política homogénea en nubes y redes locales, remotas y móviles

El problema

Normalmente, cada producto de seguridad viene con sus propias aplicaciones de gestión. Para configurar sus funciones de seguridad, los operadores de seguridad deben trabajar con distintos dispositivos de gestión. Según el informe de servicios informáticos en Estados Unidos de 2017 elaborado por ResearchCorp, cerca del 72 % de las organizaciones utiliza estos productos de tres o más proveedores distintos para proteger su infraestructura de red.[5] Estos productos están desconectados y no pueden compartir información útil. Además, para las organizaciones es todo un reto incorporar nuevos cortafuegos, mantener unas políticas de seguridad homogéneas e implementar cambios urgentes en miles de cortafuegos a la vez. Esto, que complica aún más la seguridad, termina por llevar a los equipos de TI al límite.

Cómo se resuelve el problema

Debe tener la capacidad de coordinar la implementación de políticas de seguridad centralizadas homogéneas en decenas de miles de cortafuegos repartidos por entornos locales y en la nube (incluidas las ubicaciones remotas, los usuarios itinerantes y las aplicaciones SaaS) a través de un sistema de gestión centralizada, la ejecución de tareas de seguridad básicas consolidadas y el uso de funciones optimizadas. Por ejemplo, lo ideal sería disponer de una única consola para ver todo el tráfico de red, gestionar la configuración, aplicar políticas globales y generar informes sobre patrones de tráficos o incidentes de seguridad. Sus capacidades de elaboración de informes deben permitir a su personal de seguridad examinar a fondo el comportamiento de las redes, las aplicaciones y los usuarios de manera que cuenten con el contexto necesario para tomar decisiones informadas.

Si estas capacidades proceden de la nube, sus equipos pueden crear la arquitectura de seguridad adecuada para prevenir las amenazas, conocidas y desconocidas, que acechan en cada esquina de su red ampliada. En el cambiante panorama de las amenazas de hoy, utilizar un solo proveedor de seguridad para responder al amplio espectro de necesidades de seguridad y empresariales no siempre resulta práctico. En este caso, es fundamental tener la posibilidad de adoptar e integrar en su infraestructura la información y las innovaciones de terceros. Al evaluar futuros proveedores de seguridad, tenga en cuenta las posibilidades de ampliación y programabilidad de lo que ofrecen.

12. Automatizar las tareas rutinarias y centrarse en resolver las amenazas graves

El problema

Según una encuesta realizada por el Enterprise Strategy Group, el 51 % de los profesionales del ámbito de la ciberseguridad considera que sus organizaciones se enfrentan a una escasez de personal cualificado preocupante.6 Esto se une a la necesidad de usar demasiados procesos manuales en sus operaciones de seguridad cotidianas (por ejemplo, localizar datos, investigar falsos positivos o gestionar tareas relacionadas con la solución de problemas. Analizar y correlacionar de forma manual el enorme número de eventos de seguridad demora su mitigación, aumenta la probabilidad de error y dificulta su ampliación. Los equipos de seguridad enseguida se ven desbordados por una avalancha de alertas y tienden a pasar por alto las que son más importantes y útiles. Muy pronto, no habrá suficientes profesionales de la ciberseguridad, lo que agrava aún más la situación. Aunque el análisis de datos masivos saca a la luz patrones ocultos, correlaciones y datos útiles que los equipos de seguridad pueden aprovechar en tiempo real, sigue necesitando los datos adecuados; datos procedentes de todo el entorno (las redes, los endpoints, las aplicaciones SaaS, las nubes públicas y privadas, los centros de datos, etc.) en un formato que permita analizarlos.

6. «2017 U.S. IT Services Report» (en inglés), ResearchCorp.org, 2017, www.fidelus.com/wp-content/uploads/2017/12/researchcorp-fidelus_us_it_servicesreport_full_report.pdf.

El uso de análisis precisos que faciliten la automatización tiene grandes ventajas. Le permite adoptar fácilmente prácticas recomendadas como el modelo Zero Trust y le ayuda a centrarse en las prioridades de la empresa, ya se trate de agilizar la distribución de aplicaciones, de mejorar los procesos o de detectar las amenazas. La automatización se puede considerar desde tres puntos de vista:

- **Automatización de los flujos de trabajo:** el cortafuegos debe exponer interfaces API estándar para poder programarlo desde otras herramientas y scripts que pueda estar utilizando. En la nube, debe integrarse con herramientas como Ansible y Terraform. Además, el cortafuegos debe iniciar flujos de trabajo en otros dispositivos de su ecosistema de seguridad mediante el uso de sus API y sin intervención manual.
- **Automatización de las políticas:** el cortafuegos debe adaptar las políticas a los cambios en el entorno, como el movimiento de aplicaciones por varias máquinas virtuales. También debe ser capaz de procesar la inteligencia sobre amenazas facilitada por fuentes de terceros y responder automáticamente de acuerdo con esa inteligencia.
- **Automatización de la seguridad:** su entorno debe ser capaz de descubrir las amenazas desconocidas y proporcionar medidas de protección al cortafuegos para que bloquee automáticamente las nuevas.

Figura 7: Conclusiones de ResearchCorp 2018 sobre varios proveedores de seguridad para redes

Algunas amenazas pueden permanecer ocultas en los datos. Al examinar en profundidad los datos de distintos lugares e implementaciones, es posible encontrar amenazas que, de lo contrario, pasarían inadvertidas. Con la automatización, puede identificar con precisión las amenazas, aplicar medidas de prevención rápidas, mejorar la eficiencia, aprovechar mejor el talento de su personal especializado y mejorar la estrategia de seguridad de su organización en general.

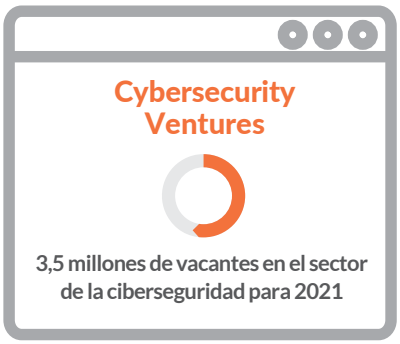

Figura 8: Conclusiones de Cybersecurity Ventures sobre las previsiones de empleo en el sector de la ciberseguridad

13. Adoptar las innovaciones en seguridad fácilmente conforme aparecen en el mercado

El problema

Adoptar las innovaciones de ciberseguridad es una tarea ardua. Las organizaciones pierden mucho tiempo añadiendo componentes de hardware o de software cada vez que quieren beneficiarse de las ventajas de una tecnología de seguridad nueva. Invierten más recursos gestionando una infraestructura de seguridad que, de todos modos, no deja de crecer, que en mejorar sus controles de seguridad para mantenerse por delante de los atacantes y prevenir las amenazas.

Cómo se resuelve el problema

Conforme aumenta el número de funciones de seguridad necesarias, hay dos opciones: añadir más productos específicos independientes o reutilizar un dispositivo para que incorpore nuevas capacidades. Si su cortafuegos puede funcionar como un sensor y punto de aplicación de políticas para tecnologías de terceros, tiene la posibilidad de adoptar las innovaciones conforme surgen sin que sea necesario implementar o gestionar un número infinito de dispositivos nuevos. Su próximo cortafuegos debería permitir a los equipos de seguridad descubrir, evaluar y usar las nuevas tecnologías de seguridad rápidamente. Hay que poner en manos de los equipos recursos que les permitan colaborar entre varias aplicaciones, compartir la inteligencia sobre amenazas y su contexto, y automatizar la respuesta y la aplicación de políticas con un software perfectamente integrado. De esta manera, disponen de los mejores medios técnicos para resolver los problemas de seguridad más acuciantes sin el gasto ni el esfuerzo que supone crear una infraestructura distinta para cada función nueva. Le invitamos a ver este vídeo, en el que se explica cómo descubrir nuevas aplicaciones y funciones innovadoras gracias a una plataforma de seguridad basada en la inteligencia artificial abierta e integrada.

¿Listo para evaluar su próximo cortafuegos? Participe en un taller técnico de pruebas «Ultimate Test Drive».

Palo Alto Networks
Oval Tower, De Entrée 99 -179
1101HE Amsterdam
Países Bajos
Tel.: +31 20 888 1883
www.paloaltonetworks.es