FORTINET

WHITE PAPER

Seguridad para pequeñas empresas: 4 pasos para el éxito

Resumen ejecutivo

Una pequeña empresa exitosa se enfoca principalmente en dos cosas: el crecimiento y una inteligente supervisión del flujo de efectivo. Las pequeñas empresas son objetivos atractivos para los hackers y en la era moderna, una seguridad débil puede afectar a ambas cosas.

Muchas pequeñas empresas luchan por implementar una seguridad consistente e integral en sus actividades comerciales por una diversidad de razones y con mucha frecuencia confían en la seguridad fragmentada combinada con productos puntuales de múltiples proveedores que no operan de manera integrada. Al final, esto genera costos inflados y estancamiento en el crecimiento, ya que la seguridad retarda la inversión en tecnología que ayudaría a que aumentar la productividad del negocio.

Afortunadamente, aún con presupuestos y mano de obra limitados, las pequeñas empresas pueden reducir significativamente su riesgo utilizando las tecnologías correctas diseñadas para trabajar juntas y ofrecer una protección segura sin dejar de ser fáciles de usar. A continuación, se describen cuatro pasos para modernizar su empresa y configurarla para el éxito de modo que la seguridad permanezca firme sin afectar el crecimiento.

¿Qué es la SD-WAN?
La red de área amplia definida por software permite a las empresas aprovechar las rutas de Internet disponibles localmente para reducir costos y obtener un mejor rendimiento de las aplicaciones basadas en la nube. La Secure SD-WAN permite esto con seguridad aplicada al tráfico entrante y saliente.

Paso 1: Invierta en conectividad segura y proteja los datos en su red

Con la inversión correcta en la tecnología de firewall de siguiente generación (Next-Generation Firewall; NGFW), puede consolidar su cartera de productos, ahorrar en las licencias necesarias para operar varios productos diferentes y hacer que la administración general de su entorno de TI sea más fácil y rentable.

Considere su NGFW como su herramienta de seguridad más importante. Los NGFW monitorean la red y brindan conocimiento e información sobre los usuarios, dispositivos y aplicaciones. Esta es la inspección de Capa 7 e indica que las empresas pueden consolidar enrutadores heredados y múltiples dispositivos de seguridad en un solo dispositivo. Algunos NGFW incluso permiten a las pequeñas empresas aprovechar las tecnologías de red como la Secure SD-WAN.

CTP por megabyte protegido

Efectividad de seguridad
= Tasa de bloqueo de vulnerabilidades de seguridad x evasiones x estabilidad y confiabilidad

CTP por Mbps protegido
= CTP/(Efectividad de seguridad x Rendimiento probado por NSS)

¿Qué buscar?

Conocer las necesidades de ancho de banda de su empresa y dimensionar con precisión el NGFW para garantizar que puede manejar el tráfico entrante y saliente, así como analizar ese tráfico para buscar amenazas es fundamental. Los NGFW pueden ser caros, pero no tienen que serlo. Prestar mucha atención a la efectividad de la seguridad y comprar según el rendimiento validado y el costo total de propiedad (TCO) por megabyte protegido preparará su negocio para el éxito a largo plazo. Además, la capacidad de ampliar esta seguridad a través de otros componentes de red, como switches y puntos de acceso inalámbricos, puede reducir aún más el riesgo empresarial.

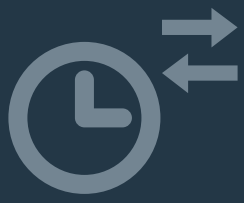
Utilice las siguientes consideraciones como una lista de verificación básica para la evaluación:

- **Validación de terceros acreditada:** Los proveedores siempre pondrán sus productos en la mejor posición, no obstante, deben ser probados por fuentes confiables. Un evaluador externo acreditado, como Gartner o NSS Labs, ofrece validación detallada de soluciones de NGFW y otros productos.

- **Rendimiento de protección contra amenazas:** Cuando el NGFW tiene toda su seguridad habilitada, es decir que ofrece firewall, prevención de intrusiones, antivirus, descifrado y capacidades de control de aplicaciones, entre otros, ¿qué impacto tiene sobre la velocidad de la red? ¿Es capaz de mantener la seguridad sin sacrificar el rendimiento?
- **Precio frente a rendimiento:** Equilibrar el costo de un NGFW con su rendimiento puede ser complicado. Si bien algunos NGFWs fueron diseñados con funciones avanzadas para empresas globales, la mayoría de las pequeñas empresas simplemente no las necesitan. Encontrar un proveedor que pueda ofrecer soluciones del tamaño correcto y funcionalidad modular garantizará que su equipo pueda consumir la tecnología que ya tienen sin gastar demasiado.
- **Capacidad de inspección de SSL:** Según la mayoría de las cuentas, aproximadamente el 80 % de todo el tráfico de Internet está cifrado. Al no descifrar ni analizar este tráfico, las amenazas se pueden ocultar e invadir su empresa. Los NGFWs deben ofrecer funcionalidad adecuada de inspección y descifrado de SSL y al mismo tiempo poder realizar análisis y ofrecer un rendimiento adecuado.
- **Rendimiento de VPN de IPsec:** ¿Puede brindar conexiones seguras a los recursos de la empresa cuando los usuarios no están en la oficina principal sino en una sucursal o trabajando de forma remota?
- **Seguridad extensible:** Si bien el NGFW puede analizar el tráfico que entra y sale de la oficina, los ataques no basados en Internet pueden propagarse rápidamente a otros usuarios y dispositivos a través de switches y puntos de acceso. ¿Puede habilitar estos dispositivos para que actúen como sensores de seguridad adicionales derivados del NGFW?
- **Fácil administración en un solo panel:** Si no puede administrar todos sus NGFWs desde una sola aplicación, usted obstaculiza la productividad de su equipo a medida que cambian de un portal a otro.
- **A prueba del futuro:** A medida que su empresa crece y se necesitan funciones más avanzadas, como la Secure SD-WAN para acceder de manera efectiva y segura a las aplicaciones basadas en la nube, ¿su NGFW cuenta con estás funciones y características? O ¿necesitará reemplazarlo por el de un proveedor con más capacidad más adelante y deberá aprender sobre una plataforma completamente diferente?

Paso 2: Invierta en proteger las aplicaciones distribuidas desde la nube

Dado que la computación en la nube y el software como servicio (SaaS) ofrecen a las empresas flexibilidad y accesibilidad, muchas pequeñas empresas no son conscientes de que la responsabilidad de proteger la información que fluye a través de estos servicios y sus usuarios recae sobre ellas. El SaaS libera en gran medida a los clientes de las responsabilidades de supervisión y mantenimiento continuo, sin embargo, esto genera una pérdida de visibilidad de lo que sucede, así como la capacidad de controlar cómo se utilizan los datos. Una solución con un buen agente de seguridad de acceso a la nube (CASB) ayuda a solucionar este problema.



Rendimiento: La cantidad de datos que se puede transferir de una ubicación a otra en un período de tiempo determinado**.**

Seguridad mejorada para correo electrónico de SaaS

A medida que más empresas recurren a Microsoft Office 365 y Google Mail para manejar sus requerimientos de correo electrónico, también lo hacen los atacantes. Actualmente, existen múltiples amenazas diseñadas para eludir la seguridad incluida con estos servicios, como ShurL0ckr y Cerber. De hecho, el ransomware por lo general ataca a empresas que usan correo electrónico,[1] el 46 % de todas las pequeñas empresas han sido blanco de un ataque de ransomware.[2] Como práctica recomendada, la introducción de seguridad específicamente diseñada para manejar el correo electrónico y eliminar el spam y otras comunicaciones maliciosas es un paso seguro para proteger su empresa del principal método de ataque.

¿Qué buscar?

Así como usted puede escanear su red para analizar el cumplimiento y las amenazas y profundizar en el uso de las aplicaciones, dispositivos y usuarios en su propia red con un NGFW bien diseñado, una solución CASB con acceso basado en la interfaz de programación de aplicaciones (API) ofrece a los administradores la capacidad de hacer lo mismo con las aplicaciones de SaaS. Adicionalmente, los informes listos para usar para cumplimiento común y requerimientos reglamentarios ayudan a acelerar las auditorías y poder monitorear si los usuarios comparten información que no deberían desde la aplicación.

Paso 3: Invierta en proteger a sus usuarios donde sea que estén trabajando

Cada vez más, los usuarios trabajan y acceden a los recursos de la empresa fuera de la oficina. Asegurarse de que tengan la capacidad de comunicarse a través de una red privada virtual (VPN) garantiza que la seguridad de la red en la que ha invertido los mantenga seguros. Al combinarse con la seguridad en la terminal, sus usuarios estarán protegidos independientemente de si olvidan utilizar la VPN o si el ataque se origina en una fuente que no sea Internet.

¿Qué buscar?

La capacidad de la VPN no debería ser un servicio adicional, sino que debería incluirse como parte de la solución del NGFW o de la terminal. Lo importante es que el NGFW pueda descifrar el tráfico entrante de la VPN a una velocidad que no afecte el rendimiento del usuario (lo que hace que quiera deshabilitarlo) y los usuarios pueden verificar rápidamente su identidad con una autenticación fácil de dos factores.

Busque seguridad en terminales que no solo ofrezca aprendizaje automático e inteligencia artificial para detectar y detener nuevos ataques, sino que también se comunique con la seguridad de su red y otros productos de seguridad para reducir las alertas falsas y mejorar la capacidad total de su solución para identificar amenazas.

Paso 4: Controle los costos simplificando y optimizando la seguridad, la administración y las operaciones continuas

Uno de los mayores asesinos de la productividad que enfrentan todos los equipos de TI es la administración, especialmente cuando los productos y soluciones de múltiples proveedores no se diseñaron para trabajar juntos de manera inmediata. Si bien las mejores soluciones se pueden unir con la tecnología de información de seguridad y administración de eventos (SIEM) o mediante la creación de un centro de operaciones de seguridad (SOC), estas requieren cuantiosos recursos para su implementación y mantenimiento.

¿Qué buscar?

Cuando los productos se diseñaron para usarse juntos con el mismo conjunto de políticas y reglas, la administración de una solución de seguridad completa desde una vista de un solo panel basado en la nube, es decir, una ventana, permite a los equipos de TI monitorear el estado de la red y la actividad del usuario desde cualquier lugar donde tengan acceso a Internet y corregir los problemas con unos pocos clics.

Del mismo modo, si su empresa ya está invirtiendo en SaaS y se siente cómodo con las características y controles detallados anteriores, la seguridad como servicio (SECaaS) es otra opción de control de costos. Sin embargo, a diferencia de las aplicaciones de SaaS típicas, cuya efectividad no se ve afectada por la inteligencia frente a amenazas integrada, un proveedor que sea capaz de proporcionar una plataforma SECaaS completa le permitirá mantener una plataforma de seguridad sólida y proactiva basada en la automatización y el intercambio de inteligencia para reducir tanto el riesgo como los costos a largo plazo.

Conclusión

Las pequeñas empresas son objetivos atractivos para los hackers, pero no tienen por qué serlo. Al invertir en las herramientas de seguridad y redes correctas, las pequeñas empresas pueden reducir significativamente su riesgo utilizando las tecnologías que fueron diseñadas para trabajar juntas, ofrecen una protección consistente y son fáciles de usar y administrar. Las buenas decisiones de inversión que tome hoy, lo prepararán bien para el futuro y le garantizarán la satisfacción de sus necesidades en cada etapa de crecimiento.

[1] J. Clement, "Leading cause of ransomware infection, 2019", Statista, 3 de diciembre de 2019.

[2] "More Than 1 in 5 SMBs Lacks Proper Data Protection", Infrascale, 1 de abril de 2020.

FORTINET

www.fortinet.com

agosto 25, 2020 10:52 p. m.

700979-0-0-ES

wp-small-business-security_ES