Documento técnico

Las organizaciones distribuidas y el fin de las puertas de enlace web tradicionales

Las organizaciones se enfrentan constantemente a presiones de la competencia que las obligan a adaptar sus empresas. Si bien las estrategias y los recursos tecnológicos de una organización deben seguir el ritmo de estos cambios, la realidad es que a menudo no lo hacen. Esto crea una brecha entre cómo trabajan las personas y cómo la infraestructura de TI las respalda. Cuando la brecha se vuelve demasiado grande, surgen muchos problemas, como riesgos de seguridad, interrupción de las operaciones, infracciones de cumplimiento, costos exorbitantes y experiencia deficiente del usuario.

Las organizaciones que implementan y usan puertas de enlace web seguras heredadas para proteger sus redes se enfrentan a estos problemas en la actualidad. Carecen de una solución clara, lo que lleva a costos crecientes, imprevisibilidad económica e insatisfacción del usuario.

En este documento, analizamos cómo la mayoría de las organizaciones han cambiado de operaciones centralizadas a operaciones distribuidas y qué significa ese cambio desde la perspectiva de la seguridad cibernética. También analizamos las deficiencias de las soluciones de puerta de enlace web segura tradicionales, en las instalaciones, híbridas y completamente en la nube. Por último, presentamos la plataforma Distributed Gateway Platform de iboss, que redefine la manera en la que se proporcionan y se administran las puertas de enlace web seguras.

Introducción

Históricamente, las organizaciones administraban sus aplicaciones comerciales de manera central. La infraestructura de la TI y los recursos conectados se hospedaban en la sede o en la oficina principal de la empresa. Con el fin de proteger el tráfico de red que entra y sale de la sede, el personal de TI implementó una puerta de enlace web segura (SWG, Secure Web Gateway) basada en dispositivos. Estos dispositivos de puerta de enlace web se colocaron en el sitio, detrás del firewall para filtrar el contenido y protegerlo contra amenazas.

Fue un modelo efectivo durante muchos años, pero luego el mercado cambió rápidamente.

Las sucursales y otras ubicaciones remotas se conectaron a la oficina central en una configuración de red de concentrador y radio. La oficina central se conectó a oficinas remotas mediante conexiones privadas dedicadas, como enlaces MPLS o VPN. Para proporcionar el mismo nivel de seguridad en todas las ubicaciones, los datos de la oficina remota se redireccionaron mediante estos costosos enlaces. Fue un modelo efectivo durante muchos años, pero luego el mercado cambió rápidamente.

Una generación móvil

Hoy en día, el mundo está sumamente distribuido. Con la proliferación de dispositivos móviles y velocidades de ancho de banda cada vez mayores, cada usuario con un teléfono inteligente móvil es, literalmente, su propia oficina remota. De hecho, **de acuerdo con la investigación de mercado de IDC**, la cantidad de trabajadores móviles en los EE. UU. aumentará a 105,4 millones (casi las tres cuartas partes de toda la fuerza laboral de los EE. UU.) para el año 2020.

Además, ahora es posible acceder a la mayoría de las aplicaciones comerciales desde la nube, lo que elimina la necesidad de que los usuarios accedan a las aplicaciones mediante la oficina principal. Por ejemplo, en lugar de acceder al correo electrónico mediante un servidor de Microsoft Exchange en la oficina central, muchos empleados obtienen su correo electrónico directamente desde la nube mediante Office 365.

Con más trabajadores de oficina móviles y remotos que ahora usan aplicaciones basadas en la nube, el enfoque del dispositivo SWG heredado ya no es eficaz. Estos trabajadores están generando más datos que nunca, lo que requiere un costoso redireccionamiento de los datos, más ancho de banda y la compra de dispositivos SWG adicionales y más grandes. Este enfoque es insostenible desde perspectiva técnica y financiera, y no cuenta con capacidad de escaldo a la par de la organización.

Un enfoque híbrido ineficaz

En respuesta a estas tendencias, los proveedores de SWG heredados ofrecen dos enfoques alternativos: híbrido y completamente en la nube. Lamentablemente, estos enfoques son acotados. Intentan preservar los modelos comerciales de los dispositivos en decadencia adicionando las capacidades de la nube o fuerzan un movimiento completo a la nube. Ninguno de estos enfoques es suficiente para cumplir adecuadamente los requisitos más amplios de las empresas distribuidas.

El primer enfoque alternativo es el modelo híbrido.En las soluciones híbridas, dos sistemas diferentes se combinan y operan en conjunto.Los dispositivos heredados conocidos se encuentran en el centro de datos y procesan el tráfico en la oficina central. Una SWG independiente y basada en la nube administra el tráfico remoto y móvil. Sin embargo, esto a menudo es solo una versión virtualizada del dispositivo en las instalaciones. El problema de las SWG híbridas es doble:

1 Los administradores deben iniciar sesión en dos sistemas separados. Esto significa que tienen que importar, exportar y normalizar manualmente los registros entre los dos sistemas: un ejercicio frustrante y que consume mucho tiempo. Además, las políticas a menudo se sincronizan solo en una dirección, con lo cual se crean inconsistencias y otros inconvenientes en la administración.

2 El segundo problema afecta la experiencia del usuario.Las políticas, las funciones, la capacidad de uso y el rendimiento carecen de paridad entre la nube y los dispositivos en las instalaciones. Esto causa numerosos problemas en las operaciones, una seguridad debilitada y experiencias de usuario incoherentes.

La incorporación de la nube

La segunda alternativa ofrece una solución de SWG que está diseñada y creada “en la nube”. En este enfoque extremo, se eliminan los dispositivos físicos en las instalaciones y se reemplazan por una SWG solo en la nube.Todos los datos de una organización se canalizan directamente en la nube para el análisis y el procesamiento de seguridad.

Al trasladar la seguridad a la nube, los equipos de compras y de TI esperan eliminar los costosos dispositivos de SWG heredados y el ancho de banda y la infraestructura costosos del redireccionamiento. Sin embargo, para eliminar los enlaces de redireccionamiento y mover toda la seguridad a la nube, el personal de TI debe reformar la red. Los equipos, los enrutadores y los firewalls se deben reconfigurar para redirigir todo el tráfico a las SWG basadas en la nube. Esto lleva mucho tiempo y es costoso, por lo que es necesario volver a crear la arquitectura de la red.

Las soluciones de SWG solo en la nube también causan problemas de cumplimiento. Muchas empresas, especialmente las que pertenecen a sectores regulados, necesitan proteger los datos dentro del perímetro de la red corporativa. Es posible que estas organizaciones también necesiten adherirse a las leyes de seguridad y privacidad de datos específicas de cada país, que requieren que los datos se mantengan dentro de una geografía física o un país específicos.En ambos casos, esos requisitos hacen que una opción totalmente en la nube sea técnicamente difícil y económicamente insostenible.

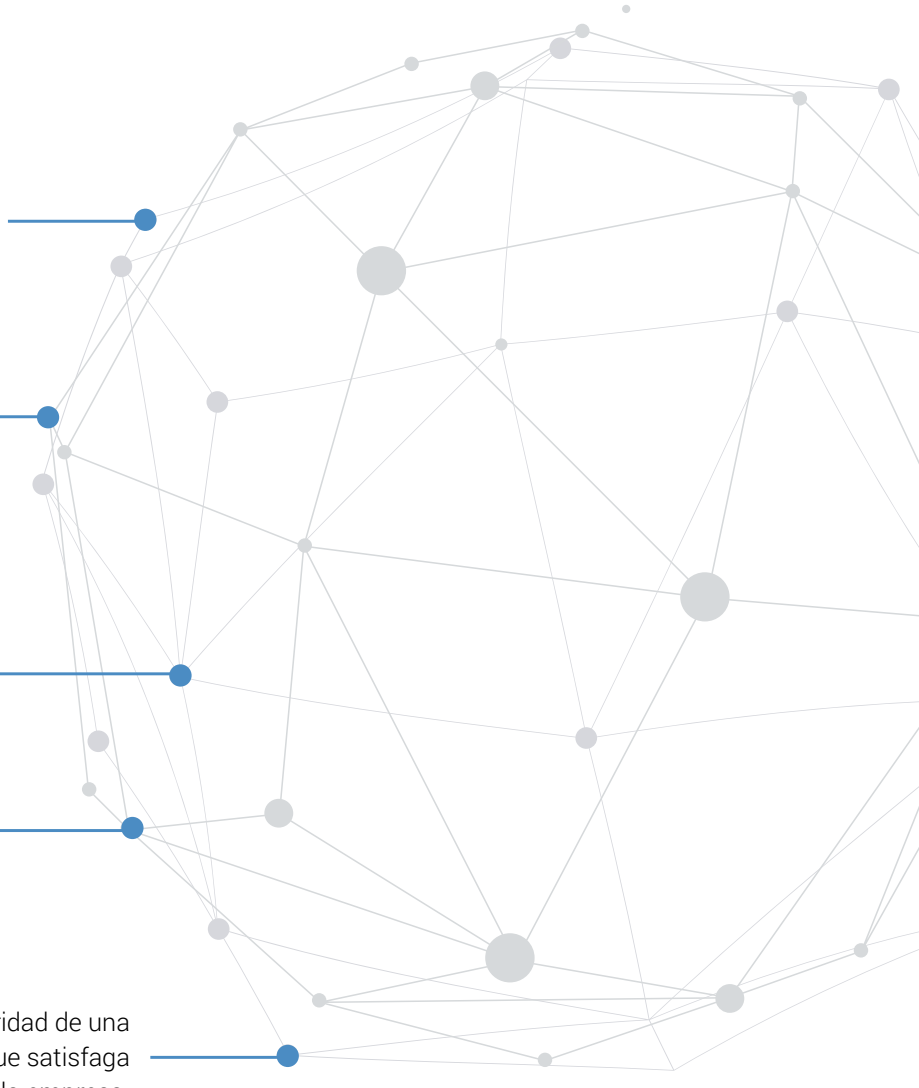
Por último, las arquitecturas multiempresa de las soluciones SWG solo en la nube plantean problemas de seguridad operativa. Por ejemplo, los proveedores de SWG en la nube indican cuándo se realizan las actualizaciones y los cambios de versiones del sistema, lo que le quita el control de la administración de cambios al personal de TI. Esto es problemático, especialmente para organizaciones con una fuerte estacionalidad o con horarios de funcionamiento inusuales, como los minoristas y los hospitales. Estos cambios generan un tiempo de inactividad, ya que desconectan efectivamente toda la red mientras se realiza la actualización o si surgen problemas durante la actualización.

Como resultado de todos estos problemas, las soluciones exclusivas para la nube no satisfacen las necesidades de los equipos comerciales y de TI.

La necesidad de un enfoque más moderno

Las opciones de SWG heredadas, híbridas y totalmente en la nube traen desafíos y problemas; esto coloca a los profesionales de TI y de seguridad en un lugar difícil. Un mejor enfoque requiere considerar el problema de manera diferente para abordar los desafíos de las empresas distribuidas.

Las empresas de hoy en día requieren un enfoque de seguridad con una arquitectura moderna y distribuida "creada para la nube". Se debe aprovechar un sistema de puertas de enlace distribuidas que continuamente identifican, aseguran y protegen todos los dispositivos y equipos conectados a Internet. Básicamente, las empresas distribuidas necesitan seguridad para:



- Eliminar el costo y los inconvenientes del redireccionamiento de los datos móviles y de la oficina central sin tener que volver a generar por completo la arquitectura de sus redes.
- Ofrecer la misma experiencia de usuario a los empleados, dondequiera que se encuentren y en cualquier entorno en el que estén trabajando.
- Proteger la organización distribuida y la fuerza de trabajo móvil con el más alto nivel de eficacia de seguridad disponible, independientemente de la ubicación.
- Gestionar y administrar desde un único panel un sistema con un conjunto de políticas, funciones y protecciones centralizadas en la nube.
- Proporcionar y administrar la seguridad de una manera escalable, flexible y rentable que satisfaga las demandas cambiantes de la empresa.

Introducción de Distributed Gateway Platform de iboss

iboss resuelve los desafíos de las organizaciones distribuidas de hoy en día de una manera completamente diferente. La plataforma Distributed Gateway Platform de iboss está creada para la nube, de modo que puede defender las redes complejas y distribuidas de hoy en día. Cuenta con una arquitectura única basada en nodos que redefine de manera fundamental la forma en la que se ofrece y se administra la seguridad cibernética mediante un servicio de suscripción al 100 %.

Al permitir una mayor flexibilidad de implementación que cualquier otra solución, la plataforma Distributed Gateway Platform de iboss, mediante puertas de enlace en la nube y puertas de enlace físicas opcionales proporcionadas en la nube, elimina la necesidad de rediseñar la arquitectura de la red o de volver a comprar hardware.

Las **puertas de enlace en la nube** protegen a los usuarios móviles y las oficinas remotas sin el costo y los inconvenientes asociados con el redireccionamiento de datos.

Las **puertas de enlace físicas proporcionadas en la nube *opcionales*** brindan un reemplazo inmediato de los dispositivos de SWG heredados y no requieren que se reestructure la red existente.

Independientemente de las puertas de enlace que implemente una organización (en la nube, físicas o una combinación de ambas), todas las características, funciones y políticas son coherentes en toda la empresa distribuida y en todos los dispositivos y las ubicaciones. Este revolucionario diseño brinda un tiempo de valorización más rápido, ya que reduce el tiempo, el costo y el riesgo asociados con el traslado desde dispositivos de puerta de enlace web segura.

Al ofrecer la puerta de enlace web como un servicio, la plataforma Distributed Gateway Platform ofrece seguridad de puerta de enlace web esencial de manera coherente en todas las ubicaciones, los usuarios y los dispositivos con la previsibilidad financiera de un servicio de suscripción.

Beneficios para los clientes

La plataforma Distributed Gateway Platform de iboss ofrece una variedad de beneficios operativos, financieros y tecnológicos, por ejemplo:

Elimina los costos de redireccionamiento

La plataforma Distributed Gateway Platform elimina la necesidad de redireccionamiento de dispositivos y enlaces de VPN y MPLS costosos y brinda un retorno de la inversión inmediato. Esto también reduce los costos futuros debido al aumento del ancho de banda del redireccionamiento.

No requiere reconfiguración de la red

La arquitectura única permite el reemplazo inmediato de los dispositivos de SWG heredados sin interrupciones en la topología de red existente, la configuración ni los procesos. Esto acorta el tiempo de implementación y reduce los costos.

Control completo

Las puertas de enlace locales y en la nube únicas y no compartidas brindan el control de los programas de administración de cambios y mejoran la seguridad general del sistema.

Administración desde un único panel

Independientemente de cómo un cliente decida implementar sus puertas de enlace, la plataforma Distributed Gateway Platform de iboss se administra con una sola interfaz, lo que facilita la creación y el establecimiento de políticas de seguridad para toda la organización.

Escalado sencillo

El escalado flexible permite a los clientes agregar y dirigir fácilmente las capacidades a medida que sus requisitos y preferencias crecen o cambian.

Experiencia del usuario sin inconvenientes

Al proporcionar políticas, capacidades, experiencias de usuario y administración de sistemas uniformes en toda la empresa, la plataforma Distributed Gateway Platform de iboss mejora la seguridad general y, a la vez, reduce considerablemente la complejidad.

Tiempo de valorización más rápido

Proporciona un retorno de la inversión inmediato al eliminar la necesidad de comprar dispositivos caros y los costos del redireccionamiento de datos, y al crear previsibilidad financiera mediante precios basados en suscripción.

Conclusión

A medida que las empresas se distribuyen más, se necesita un nuevo enfoque de seguridad. Confiar en las soluciones heredadas de puertas de enlace web seguras ya no es técnica ni económicamente factible. Estos sistemas hacen que sea extremadamente costoso proteger a los trabajadores remotos y móviles.

Para enfrentar estos desafíos, iboss ofrece la primera y única plataforma de puerta de enlace distribuida. Está diseñada exclusivamente para resolver el doble desafío de proporcionar seguridad avanzada para las organizaciones distribuidas de hoy y de escalar el servicio para satisfacer las necesidades de ancho de banda cada vez mayores del futuro.

Además, iboss facilita a las organizaciones la compra de la plataforma Distributed Gateway Platform con su modelo de precios basado en suscripciones. Los clientes ya no necesitarán comprar ni administrar dispositivos de SWG nunca más y dejarán el paradigma heredado para iniciar un nuevo enfoque “como servicio”.

¿Desea obtener más información? Solicite una demostración.

Acerca de iboss

La plataforma Distributed Gateway Platform de iboss es un servicio de puerta de enlace web diseñado específicamente para resolver los desafíos que presenta la protección de las organizaciones distribuidas. El servicio de iboss fue creado para la nube y aprovecha una arquitectura revolucionaria basada en nodos que se amplía fácilmente para satisfacer las crecientes necesidades de ancho de banda y se administra a través de una única interfaz. La plataforma Distributed Gateway Platform de iboss está respaldada por más de 110 patentes y protege a más de 4000 organizaciones de todo el mundo. Esto convierte a iboss en una de las empresas de seguridad cibernética de más rápido crecimiento del mundo.

Para obtener más información, visite www.iboss.com o comuníquese con iboss escribiendo a sales@iboss.com.

LN - 11 - 17