Akamai

GUÍA DEL COMPRADOR

Cómo seleccionar una puerta de enlace web segura basada en la nube

Proteja a su plantilla remota y simplifique la seguridad empresarial

Tabla de contenido

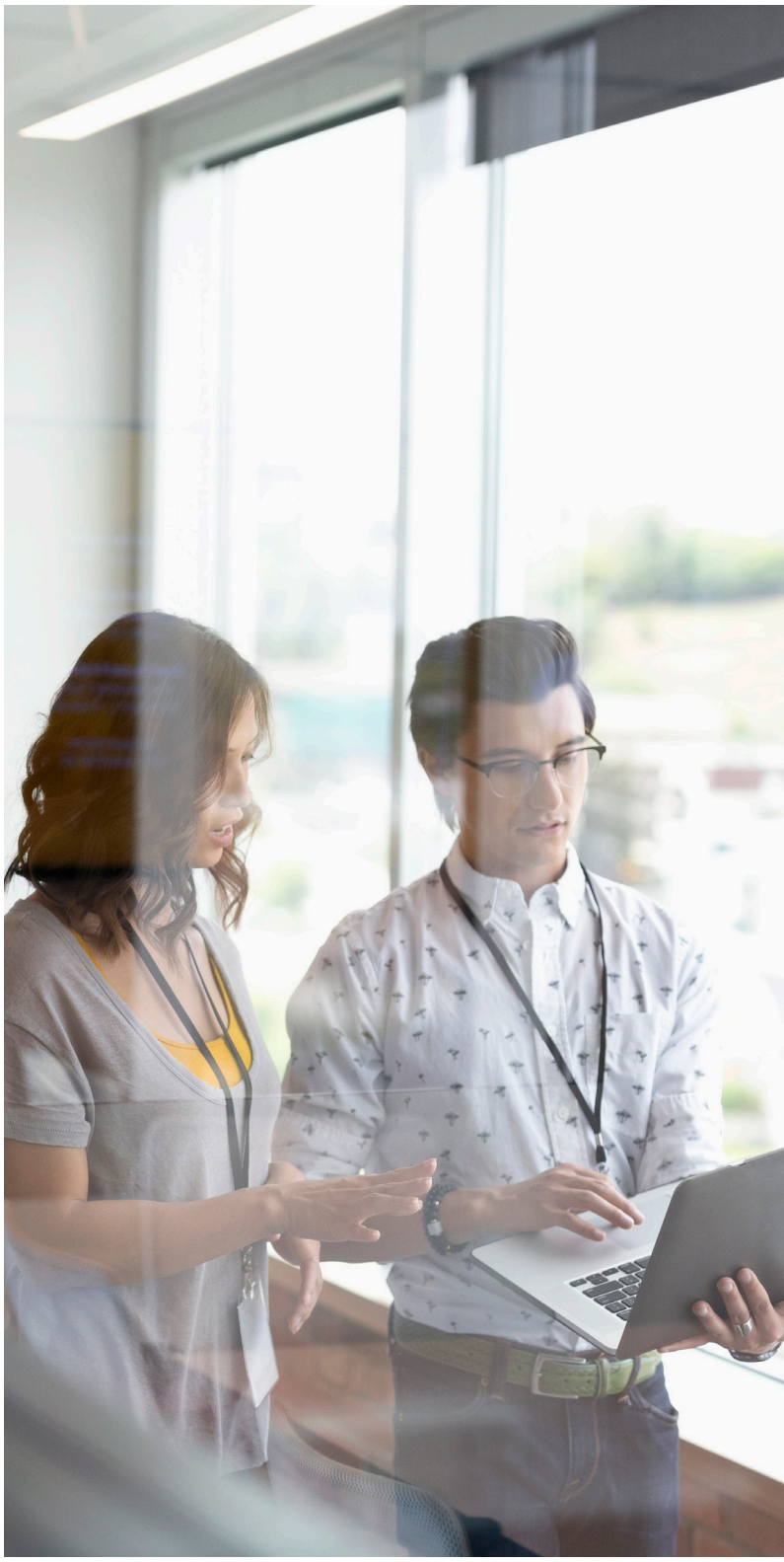
Protección de la empresa moderna: redefinir la red de retorno de los centros de datos

La computación en la nube, el software como servicio (SaaS), la movilidad y las arquitecturas de red actualizadas han revolucionado las prácticas comerciales. Pero también han creado una tormenta perfecta para los equipos de TI que intentan proteger a su plantilla sin limitar el valor de estas nuevas tecnologías. Ahora existe un nuevo desafío: Independientemente de en qué punto de su transformación digital se encontrasen las empresas, muchas tuvieron que reaccionar rápidamente para adaptarse a un aumento drástico en el número de usuarios remotos en 2020.

Una puerta de enlace web segura es un componente fundamental para proteger al personal corporativo, pero muchas empresas aún utilizan dispositivos físicos implementados en centros de datos. Este hardware requiere administración, mantenimiento y actualizaciones constantes, y utiliza una redirección de tráfico laberíntica para inspeccionar y controlar el tráfico web, lo que termina disminuyendo el rendimiento.

Las organizaciones necesitan un enfoque moderno y optimizado para proteger la nueva realidad del entorno corporativo distribuido. La solución: prescindir de dispositivos de hardware y migrar esa capacidad de la puerta de enlace web segura a la nube.

En esta guía del comprador se describen las ventajas de las puertas de enlace web seguras basadas en la nube y las capacidades que se deben buscar en una tecnología moderna de puertas de enlace web.



El aumento del teletrabajo crea nuevas exigencias de TI y seguridad

Durante la última década, las organizaciones han ido aumentando progresivamente su plantilla remota. Esta tendencia no hizo más que consolidarse a consecuencia de la COVID-19 y se prevé que continúe mucho después de la pandemia. Gartner determinó que el 74 % de los directores financieros encuestados trasladarán al menos el 5 % de su plantilla presencial a puestos remotos permanentes cuando termine la pandemia.[1]

Al mismo tiempo, la cantidad de ataques sofisticados dirigidos, como el phishing, el ransomware y el malware, ha ido creciendo vertiginosamente. El cincuenta y tres por ciento de las personas que respondieron a una encuesta reciente afirmó haber experimentado un aumento en la actividad de phishing desde el inicio de la COVID-19.[2] Un comunicado reciente del Departamento del Tesoro de Estados Unidos informaba de que la exigencia de pagos de ransomware había aumentado durante la pandemia de la COVID-19, debido a que los cibercriminales utilizan como blanco sistemas online en los que las personas confían para desarrollar su actividad empresarial.[3]

Tradicionalmente, las organizaciones protegían el acceso a Internet para los usuarios in situ, tanto en las ubicaciones principales como en las sucursales, instalando dispositivos de seguridad, como puertas de enlace web seguras, en sus centros de datos. Tras ello, devolvían todo el tráfico web a esa ubicación central para su inspección y control.

Las empresas han utilizado estas puertas de enlace web seguras para filtrar el malware no deseado del tráfico web iniciado por el usuario, evitar que los usuarios accedan a sitios web maliciosos y hacer cumplir las políticas normativas y de la empresa.

Estas soluciones de puerta de enlace se diseñaron e implementaron originalmente en entornos en los que la mayoría de los trabajadores utilizaban dispositivos administrados por la empresa en sus escritorios. Sin embargo, a medida que la cantidad de usuarios que trabajan de forma remota y en sucursales crecía y se dirigía más tráfico a la red pública de Internet para acceder a las aplicaciones SaaS, las organizaciones comenzaron a instalar más y más puertas de enlace web seguras y redundantes en el centro de datos para mantener un rendimiento satisfactorio. La compra y administración de estas soluciones se volvió cada vez más compleja, costosa y tediosa.

> **"El porcentaje del presupuesto de TI dedicado a los centros de datos ha disminuido durante los últimos años, y ahora representa solo el 17 % del total".**
>
> — Gartner, 2019 Indicadores clave sobre TI

Como alternativa, las organizaciones añadieron dispositivos de puerta de enlace web segura a sus sucursales mientras redirigían el tráfico de todos los usuarios remotos. Dicha redundancia llevó a una proliferación adicional de los dispositivos y de sus costes auxiliares, así como a una complicada administración e implementación.

También se hizo cada vez más difícil mantener políticas de seguridad coherentes en tal cantidad de ubicaciones. Incluso cuando las organizaciones implementaban dispositivos virtualizados para reducir la proliferación de dispositivos, se vieron igualmente obligadas a implementar y administrar hardware adicional.

Un tercer enfoque fue la implementación híbrida, en la que las organizaciones continuaban utilizando puertas de enlace web seguras en las instalaciones de las ubicaciones principales y enviaban el tráfico web de sucursales a una puerta de enlace web segura basada en la nube, mientras seguían redirigiendo el tráfico de los empleados remotos. Este enfoque permitió aprovechar la inversión en hardware ya realizada en equipos locales. Sin embargo, incrementó la complejidad, ya que las organizaciones acabaron administrando sistemas dispares. El problema no era solamente que los equipos y la administración adicionales fueran mucho más costosos que un enfoque puro en la nube, sino que también era difícil mantener políticas coherentes en todos los sistemas locales y basados en la nube.

> **Gartner predice que, para el 2025, el 80 % de las empresas cerrarán sus centros de datos tradicionales.[4]**

Para empeorar las cosas, mientras las organizaciones adoptaban estas soluciones cada vez más complejas, empezaron a enfrentarse a una escasez de recursos de ciberseguridad. Un estudio de (ISC)[2] puso de manifiesto que en Estados Unidos se necesitaría un aumento del 62 % para cubrir la escasez actual de empleados de seguridad necesarios.[5]

¿Por qué una puerta de enlace web segura basada en la nube?

Las organizaciones necesitan un enfoque moderno de cara a la seguridad web, basado en la estrategia de nube de la empresa, que adopte y posibilite el trabajo remoto. Una puerta de enlace web segura basada en la nube ofrece a las organizaciones un alto nivel de seguridad y, al mismo tiempo, reduce la complejidad mediante la conexión directa a Internet, evitando así la necesidad de disponer de varios dispositivos y de redirigir el tráfico.

Con una puerta de enlace web segura basada en la nube, las organizaciones pueden beneficiarse de:

Menor complejidad de la seguridad: ya que se trata de un servicio en la nube, las puertas de enlace web seguras eliminan la necesidad de implementar hardware o dispositivos virtuales, así como de configurar, administrar y reemplazar o actualizar el hardware cada tres años.

Mínimo de cuellos de botella de rendimiento: una puerta de enlace web segura basada en Internet elimina la necesidad de añadir dispositivos adicionales para hacer frente a mayores cargas de tráfico web y de niveles de tráfico cifrado en aumento. Los clientes pueden simplemente agregar servicios adicionales según sea necesario, con un impacto mínimo en el rendimiento.

Menor coste de redirección y conexión entre nodos de tráfico: las puertas de enlace web seguras basadas en la nube aplican seguridad al tráfico web sin necesidad de redirigir el tráfico para permitir la conexión directa a Internet, lo que reduce el coste de red MPLS (conmutación por etiquetas multiprotocolo).

Mayor eficiencia del equipo de seguridad: ya que las puertas de enlace web seguras en la nube no requieren mantenimiento continuo del hardware o software, los limitados recursos de seguridad tienen más tiempo para centrarse en otras medidas de seguridad proactivas.

Políticas de seguridad coherentes: las organizaciones pueden utilizar políticas administradas centralmente e implementadas globalmente para todos los usuarios que se conecten desde cualquier dispositivo. Incluso si la organización tiene políticas diferentes para regiones distintas, puede utilizar la misma interfaz de usuario para administrarlas todas.

Requisitos clave de una puerta de enlace web segura

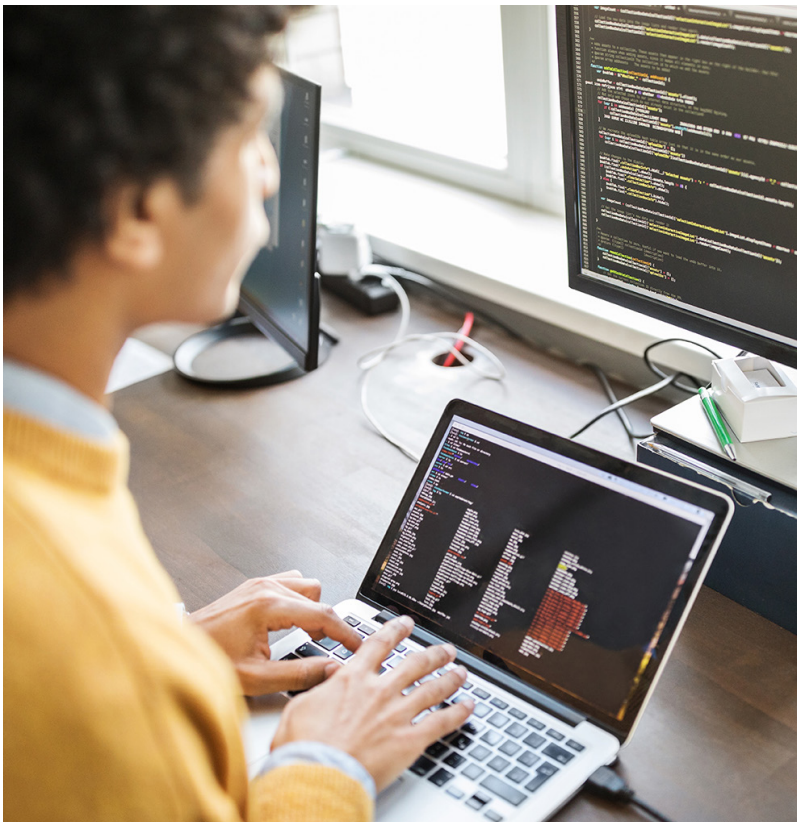
Al seleccionar una puerta de enlace web segura basada en la nube, es importante tener presente que la seguridad es el requisito clave. Muchas puertas de enlace web seguras heredadas incluyen capacidades para resolver problemas que ya no existen. Por ejemplo, incluyen control del ancho de banda, que se diseñó para una época en la que el ancho de banda era costoso. O bloquean el acceso de los empleados a YouTube o Facebook durante las horas de trabajo. Hoy en día estas funciones ya no son necesarias, porque el ancho de banda es abundante y hay tantas personas utilizando sus dispositivos móviles que las organizaciones ya no se preocupan por restringir estos servicios en los dispositivos corporativos.

Actualmente, las organizaciones necesitan una puerta de enlace web segura basada en la nube que esté diseñada específicamente para solucionar los desafíos de seguridad modernos. Concretamente, la solución debe seguir una estrategia de defensa detallada que utilice múltiples medidas de seguridad para ofrecer el más alto nivel de protección. Este enfoque debe abarcar todos los aspectos de la ciberseguridad y proporcionar medidas de seguridad redundantes. De este modo, si una línea de defensa se ve comprometida, se implementan capas de defensa adicionales para evitar que los ataques atraviesen los puntos débiles. Este enfoque por capas garantiza que las amenazas como el malware, el ransomware y el phishing se bloqueen más rápido y antes de que el dispositivo del usuario quede expuesto.

Una puerta de enlace web segura que implemente una estrategia de defensa exhaustiva debe ofrecer las siguientes capacidades de seguridad:

Evaluación de todas las solicitudes de DNS y URL

Una solución de puerta de enlace web segura basada en la nube debe evaluar todas las solicitudes de URL y DNS en términos de inteligencia contra



amenazas en tiempo real y bloquear las solicitudes maliciosas en una fase temprana de la cadena de eliminación. Si la puerta de enlace web segura puede bloquear amenazas antes de que se establezca una conexión saliente, el recurso web no necesita abrir ni inspeccionar ningún contenido devuelto. Esta eficiencia evita un proceso de computación intensiva y reduce la cantidad de tráfico que debe analizar la puerta de enlace web segura en la etapa de carga. ¿El resultado? Un mejor rendimiento general de la puerta de enlace web segura.

La inteligencia contra amenazas debe proteger contra malware, ransomware, phishing y exfiltración de datos basada en DNS de bajo rendimiento. También debe estar diseñada específicamente para ofrecer protección que sea actual, pertinente y proporcione tasas bajas de falsos positivos.

Técnicas de análisis de carga múltiples

Debido a que todas las amenazas son diferentes y, por lo tanto, ninguna técnica o enfoque de detección único puede abordar todos los tipos de malware, la solución de puerta de enlace web segura debe incluir varios motores de análisis de malware. Estos motores deben escanear las cargas útiles de HTTP y HTTPS en línea o sin conexión utilizando diversas técnicas de identificación, entre las que se incluyen la detección de malware con y sin firma, el aprendizaje automático y los entornos de pruebas. Este análisis ofrecerá una protección completa de día cero contra archivos potencialmente maliciosos, como ejecutables y archivos de documentos.

Detección de phishing de día cero

Los empleados remotos siguen enfrentándose a un aumento de los ataques de phishing desde el brote de COVID-19. Los agentes maliciosos inician estos ataques de phishing a través de correo electrónico, redes sociales y aplicaciones de mensajería instantánea, así como mediante el intercambio de archivos y los canales de colaboración online, para robar credenciales corporativas que les dan acceso a la red empresarial. A partir de ahí, los atacantes pueden moverse lateralmente para encontrar y exfiltrar datos y propiedad intelectual, o para difundir campañas de ransomware.

Para identificar y bloquear el acceso a una página de phishing, la mayoría de los proveedores de seguridad hacen lo siguiente:

1. **Observar tráfico inusual que llega a un dominio**
2. **Analizar ese dominio**
3. **Determinar si se trata de un dominio de phishing**
4. **Agregarlo a la lista de bloqueo**
5. **Desplegar una lista de bloqueo actualizada para los clientes**

Este proceso puede tardar horas. Pero lo que es todavía más grave es que los cibercriminales de hoy en día usan kits de phishing para crear y lanzar fácilmente ataques de corta duración, lo que hace aún más difícil la detección. Para cuando se encuentra el dominio o la URL de phishing, el ataque ha terminado. De hecho, cuanto más sofisticado y dirigido sea el ataque de phishing, menor será su duración.

Sin embargo, aunque estas campañas terminan rápidamente, un motor avanzado de detección de phishing de día cero puede identificarlas y bloquearlas. Los elementos recurrentes de estos ataques basados en kits se pueden ver en el código de las páginas de phishing. Con esta información, es posible identificar las "huellas" de estas páginas que permiten una identificación precisa.

Una solución de puerta de enlace web segura debe incluir un motor de detección de phishing de día cero que pueda analizar las páginas web solicitadas y compararlas con "huellas" de páginas de phishing vistas previamente.

Inspección de tráfico cifrado

Internet es un canal intrínsecamente inseguro para la transferencia de datos. Por lo tanto, hoy en día el cifrado del tráfico web se utiliza de manera habitual para disuadir a los atacantes que intentan interceptar, falsificar o manipular el tráfico. La seguridad de capa de transporte (TLS) es el estándar de cifrado por excelencia para ofrecer una navegación web segura. TLS crea un túnel seguro entre dos extremos, como el navegador de un cliente y un servidor web.

> **El porcentaje de tráfico web cifrado en Internet ha ido aumentando de forma constante, de aproximadamente un 50 % en 2014 a un 80 %-90 % en la actualidad. La mayoría (96 %) de los principales 100 sitios web del mundo utilizan HTTPS de forma predeterminada.**
>
> — Informe de transparencia de Google, 2020

Pero no todo el tráfico HTTPS es inofensivo. Los atacantes y los programadores de malware también utilizan el cifrado para ocultar sus actividades, evitar que los usuarios accedan a los archivos (mediante ransomware) y proteger la comunicación de red maliciosa. En un estudio reciente, se puso de manifiesto que casi una cuarta parte del malware que estableció una conexión a Internet utilizó TLS para comunicarse.[6]

Para inspeccionar y controlar de forma proactiva el tráfico web de HTTPS, es necesario mirar en el interior del túnel seguro y examinar el tráfico cifrado mediante un servidor proxy (intermediario de confianza). El servidor proxy debe descifrar el tráfico HTTPS en texto sin formato, analizarlo, volver a cifrar el tráfico y, a continuación, crear otra conexión segura mediante una técnica de tipo máquina intermediaria ("machine in the middle"/ MITM). MITM inspecciona las direcciones URL solicitadas para determinar si son seguras o maliciosas, proporciona visibilidad del tráfico cifrado TLS y protege a la empresa contra amenazas, a la vez que preserva la confidencialidad e integridad del tráfico a los sitios web de origen.

Las inspecciones MITM requieren una capacidad de procesamiento considerable. Por lo tanto, la navegación web puede ralentizarse debido a la latencia. La puerta de enlace web segura debe ofrecer servicios que mejoren el rendimiento de las aplicaciones. Debe incluir una red de servidores distribuida a nivel mundial y software inteligente ubicado cerca de los usuarios y centros de datos de todo el mundo para permitir optimizaciones web que mejoren el rendimiento y la disponibilidad de las aplicaciones.

Además, debe comprobar que el proveedor de puerta de enlace web segura en la nube mantenga una lista centralizada de dominios y direcciones URL que no funcionan correctamente y que deben omitirse. Asimismo, la puerta de enlace web segura en la nube debe ser capaz de omitir la inspección MITM para determinados tipos de contenido web confidencial, como servicios financieros y sanitarios.

Prevención de pérdida de datos integrada

Prevenir de manera proactiva la pérdida de datos personales y otros datos confidenciales de la empresa es fundamental debido al potencial de pérdidas financieras o de reputación que entraña. La puerta de enlace web segura en la nube debe incluir una prevención integrada de pérdida de datos que sea fácil de configurar y de rápida implementación. Los diccionarios que se actualizan con frecuencia deben abarcar las normas de privacidad y protección de datos, como PII, PCI DSS e HIPAA, mientras que las organizaciones deben tener la capacidad de crear diccionarios personalizados fácilmente.

Identificación y gestión de TI en la sombra

Los usuarios tienen a su alcance cientos de miles de aplicaciones para descargar, instalar y usar en dispositivos administrados sin el conocimiento del equipo de seguridad de la empresa. Sin embargo, el uso de aplicaciones no autorizadas puede ampliar significativamente la superficie de ataque de la organización y aumentar su perfil de riesgo.

> **La empresa promedio utiliza más de 1295 aplicaciones y servicios en la nube. Más del 95 % de estos no están administrados y no cuentan con derechos de administración de TI.**
>
> — Cybersecurity Insiders,
> Informe sobre seguridad en la nube, 2019

Una puerta de enlace web segura en la nube debe ser capaz de identificar qué aplicaciones se están utilizando, detectar cuántos usuarios han instalado aplicaciones específicas y destacar las aplicaciones que pueden presentar un riesgo de seguridad potencialmente grave. Una vez que se identifica, la solución debería poder bloquear toda la aplicación u operaciones específicas de la aplicación (por ejemplo, permitir cargas, pero no descargas).

Protección en cualquier lugar para cualquier dispositivo

La flexibilidad en la forma de trabajar ha experimentado una enorme tendencia ascendente durante la última década. Los usuarios ahora trabajan desde cualquier lugar, en cualquier dispositivo. Y, como resultado del teletrabajo durante la pandemia, el 59 % de la informática para usuario final de las empresas está migrando hacia los dispositivos móviles, que complementan o reemplazan a los PC y portátiles. Se prevé que este cambio continúe incluso después de que se vuelva a trabajar en la oficina.[7]

El cambio a dispositivos móviles y el aumento del uso de redes Wi-Fi pueden dar lugar a puntos débiles en la estrategia de seguridad de cualquier organización. Las empresas deben poder aplicar un nivel de seguridad uniforme y universal, sin sacrificar el rendimiento del dispositivo.

Una puerta de enlace web segura en la nube debe identificar, bloquear y mitigar de forma proactiva las amenazas dirigidas, como malware, ransomware, phishing, exfiltración de datos vía DNS y ataques de día cero a cualquier dispositivo (iOS, Android OS, Chrome OS), en cualquier red a la que se conecte el usuario. La solución de puerta de enlace debe ofrecer controles universales y administración simplificada a nivel global, preservando al mismo tiempo un rendimiento óptimo del dispositivo.

Acceso seguro a todas las aplicaciones empresariales

Una puerta de enlace web segura en la nube protege a los usuarios y dispositivos contra el malware mientras acceden al Internet público. Pero para una empresa, se trata tan solo de una pieza dentro del rompecabezas de seguridad.

Para crear un enfoque de seguridad integral para toda la empresa, las organizaciones también necesitan proteger contra agentes maliciosos las aplicaciones corporativas que administran, independientemente de si estas residen en el centro de datos corporativo o en un entorno IaaS. Las herramientas tradicionales de seguridad de red protegen el perímetro de la red, pero si los atacantes vulneran el perímetro (por ejemplo, al robar las credenciales de usuario o al instalar malware en un dispositivo de usuario), pueden moverse libremente dentro de la red.

Las organizaciones necesitan una puerta de enlace web segura en la nube que también ofrezca tecnología de "acceso de red Zero Trust" (ZTNA) para proteger las aplicaciones corporativas. ZTNA es un componente fundamental en la adopción de la seguridad Zero Trust, que otorga a los usuarios acceso solo a aplicaciones específicas (no a redes o segmentos completos) en función de su identidad. La solución protege la identidad del usuario integrándola con la gestión de identidad y acceso, la autenticación multifactorial (MFA) y las tecnologías de inicio de sesión único. Mediante el uso de una herramienta ZTNA, las organizaciones eliminan la complejidad de administrar de forma segura los dispositivos o de mantener una red de área extensa compleja o una conectividad de red privada virtual. Una vez autenticados correctamente, los usuarios solo tienen acceso a las aplicaciones y datos que

Los ataques de phishing a empresas van en aumento

Ataques observados, de marzo a octubre de 2020

AUMENTO DE ATAQUES CONTRA

EMPRESAS

AUMENTO DE ATAQUES CONTRA

CONSUMIDORES

Fuente: Puerta de enlace web segura Akamai Enterprise Threat Protector

necesitan, lo que reduce a cero la superficie de ataque de la aplicación y minimiza el riesgo de movimiento lateral. Cuando las organizaciones evalúan una puerta de enlace web segura en la nube, deben considerar las capacidades del servicio ZTNA del proveedor. ¿Puede proporcionar acceso a aplicaciones web modernas y a aplicaciones no web heredadas? ¿Se puede integrar con el servicio proveedor de identidades existente de la organización? ¿Es compatible con MFA?

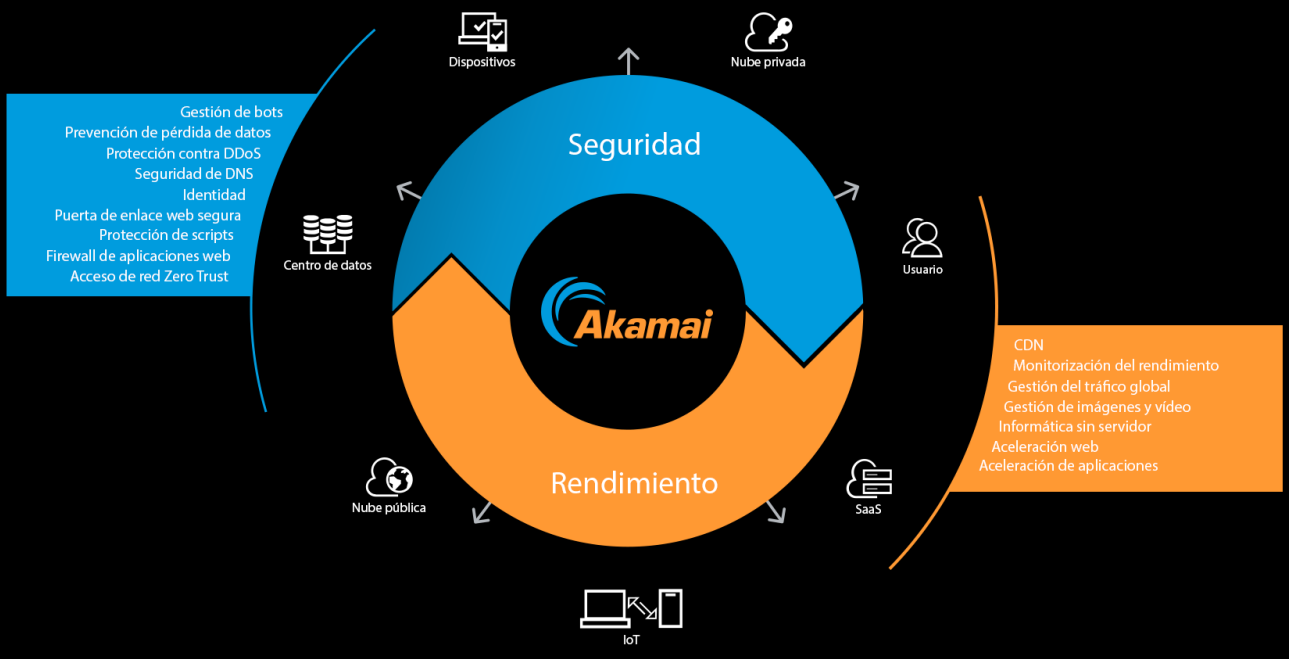
La puerta de enlace web segura debe integrarse y trabajar en combinación con el servicio ZTNA de forma que, si un dispositivo se encuentra en situación de riesgo, no pueda acceder a ninguna aplicación corporativa. Los registros de una puerta de enlace web segura pueden aumentar otras señales de amenaza para ofrecer una imagen más precisa del estado de seguridad de un dispositivo. Por ejemplo, si el dispositivo llama a los servidores de comando y control, la solución debe utilizarlo como una señal para limitar el acceso a las aplicaciones hasta que se este se repare.

Al añadir la puerta de enlace web segura y las capacidades ZTNA, las organizaciones dan un paso hacia la adopción de un marco Secure Access Service Edge (SASE). SASE aleja el foco de las iniciativas de seguridad de una organización del centro de datos y de las arquitecturas de seguridad centradas en dispositivos de hardware que ya no funcionan en el entorno empresarial y laboral altamente distribuido de hoy. En su lugar, SASE ofrece un acceso mediante políticas basado en la identidad del usuario o dispositivo. SASE también proporciona una amplia gama de controles de seguridad adicionales que incluyen el firewall de aplicaciones web, la seguridad de API, la administración de bots y la protección contra DDoS para aplicaciones web.

> **ZTNA mejora la flexibilidad, la agilidad y la escalabilidad del acceso a las aplicaciones, lo que permite que las empresas digitales se desarrollen sin exponer las aplicaciones internas directamente a Internet, para reducir el riesgo de ataque.**
>
> — Gartner, Market Guide for Zero Trust Network Access, Steve Riley, Neil MacDonald, Lawrence Orans, 8 de junio de 2020

Además, los controles de seguridad están disponibles en la plataforma SASE, a un solo salto de Internet del usuario para ofrecer acceso de baja latencia en cualquier lugar a usuarios, dispositivos y servicios en la nube.

SASE basado en la nube de Akamai



Rendimiento óptimo

Aunque la seguridad es primordial, no puede comprometer la experiencia del usuario si conlleva un rendimiento lento. Además de ofrecer un planteamiento de defensa en profundidad en lo relativo a la seguridad, una puerta de enlace web segura basada en la nube debe proporcionar los servicios mencionados anteriormente sin introducir latencia.

Para evitar la latencia, la puerta de enlace web segura en la nube se debe implementar a nivel global con puntos de presencia cerca de donde se conectan todos los usuarios. Después de todo, no tiene sentido reemplazar un tipo de redirección por otro.

La plataforma en la nube también debe poder adaptarse a escala rápidamente para no afectar a la experiencia del usuario final, incluso durante picos de tráfico. Esta capacidad es especialmente importante cuando se trata de inspeccionar el tráfico HTTPS, que crece exponencialmente y terminará constituyendo cerca del 100 % de todo el tráfico web. Es fundamental inspeccionar el tráfico cifrado con un impacto mínimo en los usuarios finales, ya que la gran mayoría del malware se envía ahora a través de HTTPS. La plataforma también debe proporcionar un acuerdo de nivel de servicio (SLA) con el 100 % de disponibilidad.

> **Hoy en día, los usuarios de Office 365 conforman más de la mitad del 81 % de organizaciones que se han mudado a los servicios en la nube.[8]**

Integración con Office 365: Es especialmente importante garantizar un alto nivel de seguridad y rendimiento para Microsoft Office 365, ya que muchas organizaciones confían en este servicio como conjunto esencial de aplicaciones de productividad. Un desafío presente a la hora de implementar una puerta de enlace segura en la nube es que O365, al igual que muchas otras aplicaciones SaaS populares, tiene un rendimiento deficiente cuando los usuarios acceden a sus aplicaciones a través de un proxy de reenvío, que se encarga de la inspección MITM de TLS.

Para evitar un impacto en el rendimiento de O365, es fundamental que la puerta de enlace segura en la nube se ofrezca a través de una plataforma global al borde de la red que pueda:

- Utilizar la dirección IP de origen de la solicitud para dirigirla al centro de datos de Microsoft O365 más cercano geográficamente, en lugar de las soluciones DNS de redirección que la dirigirían al servicio de resolución de DNS corporativo más cercano; por ejemplo, un usuario que accede a O365 desde Singapur y al que se le redirige a un servidor de O365 en Nueva York tendría una experiencia de usuario pésima.

- Garantizar que las ubicaciones de los servidores de puerta de enlace web segura estén situadas cerca de los centros de datos de Microsoft O365 y que, idealmente, estos servidores y centros de datos estén interconectados.

- Proporcionar una configuración de un solo clic para optimizar el tráfico de O365 que utilice una lista de dominios y direcciones IP de O365 publicados y actualizados por Microsoft. Las solicitudes a estos dominios deben enviarse directamente a los servidores de O365 en línea con las recomendaciones de Microsoft, lo que ahorra tiempo y esfuerzo al eliminar la necesidad de actualizar manualmente los firewalls y otros productos de seguridad cada vez que Microsoft agregue nuevos dominios o direcciones IP.

Trasladar la seguridad al borde de Internet

Las plantillas remotas, en rápido aumento, son cada vez más vulnerables a los ciberataques, y estos, a su vez, son cada vez más frecuentes y graves. Las mejores soluciones de puerta de enlace web segura basadas en la nube se centrarán exclusivamente en satisfacer estas demandas modernas de seguridad, ya que ofrecen funciones comprobadas de defensa en profundidad. También permitirán modelos modernos de seguridad empresarial, como Zero Trust y SASE, ya que protegen el acceso a Internet para todos los usuarios sin importar dónde se encuentren.

Una puerta de enlace web segura en la nube integral debe evaluar todas las solicitudes de DNS y URL, proporcionar técnicas de análisis de carga múltiples, combatir el phishing de día cero, inspeccionar el tráfico cifrado, integrar la prevención de pérdida de datos, identificar y administrar TI en la sombra y proporcionar protección en cualquier lugar y en cualquier dispositivo, todo ello mientras ofrece un alto nivel de rendimiento e integración con tecnologías de seguridad para aplicaciones empresariales. Con una solución de este nivel, las organizaciones pueden disminuir la complejidad de la seguridad, eliminar costosos procesos de redirección de tráfico, mejorar la eficiencia del equipo de seguridad y respaldar políticas de seguridad coherentes.

Obtenga más información acerca de Secure Internet Access, la puerta de enlace web segura de la nube de Akamai, y comience una prueba gratuita en akamai.com.

1. https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2
2. https://www.helpnetsecurity.com/2020/09/02/phishing-attacks-pandemic/
3. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
4. https://blogs.gartner.com/david_cappuccio/2018/07/26/the-data-center-is-dead/
5. https://www.brinknews.com/a-global-shortage-of-cybersecurity-professionals-leaves-businesses-at-risk/
6. https://news.sophos.com/en-us/2020/02/18/nearly-a-quarter-of-malware-now-communicates-using-tls/
7. https://www.mobolize.com/2020/10/29/mobolize-announces-technology-partnership-with-akamai-to-enable-security-on-mobile-devices/
8. https://blog.goptg.com/microsoft-office-365-statistics#:~:text=According%20to%20Bitglass%2C%20usage%20of,the%20shift%20to%20cloud%20services

Akamai

Akamai potencia y protege la vida online. Las empresas líderes de todo el mundo eligen Akamai para crear, proteger y ofrecer sus experiencias digitales, ayudando así a millones de personas a vivir, trabajar y jugar cada día. Gracias a la plataforma informática más distribuida del mundo, de la nube al Edge, nuestros clientes pueden desarrollar y ejecutar las aplicaciones con facilidad, mientras acercamos las experiencias a los usuarios y mantenemos las amenazas a raya. Para obtener más información acerca de las soluciones de seguridad, informática y distribución de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en Twitter y LinkedIn. Publicado en junio de 2022.