Puerta de enlace segura a internet

RESUMEN DE LA SOLUCIÓN

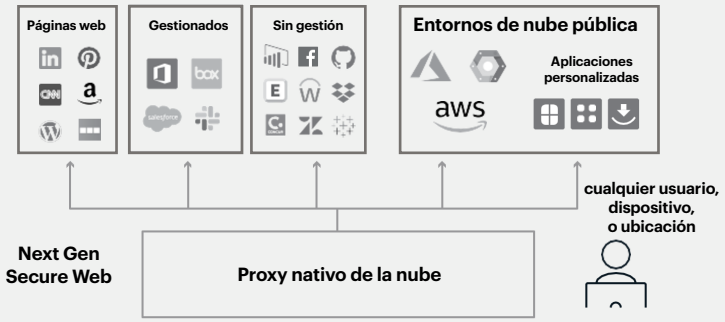
Obtenta capacidades de gateway web seguro de próxima generación (Next Gen SWG) para prevenir malware, detectar amenazas avanzadas, filtrar sitios web por categoría, proteger datos y controlar aplicaciones y servicios en la nube para cualquier usuario, ubicación o dispositivo. Proxy en línea sin igual por su capacidad para decodificar el tráfico en la nube y en la web, incluyendo la instancia y la actividad.

BENEFICIOS:

- **Controles de políticas granulares en la Web y en la nube que incluyen instancias, actividades y datos.**
- **Protección avanzada de datos y amenazas de un solo paso con detección de anomalías de comportamiento.**
- **Una única consola en la nube con controles de políticas compartidas para SWG, Cloud/SaaS y DLP.**
- **Proxy en línea maduro que protege a clientes de Fortune 100 desde hace más de ocho años.**
- **Rendimiento en la nube y escala global para proteger a cualquier usuario, dispositivo o ubicación.**

Hoy en día, las empresas utilizan una media de 2.415 aplicaciones, con un 89% de sus usuarios activos en la nube. Más del 98 % de estas aplicaciones no están gestionadas y mientras que la protección tradicional de API se limita a las aplicaciones gestionadas, nuestra solución SWG (puerta de enlace segura) de Netskope decodifica miles de aplicaciones en la nube. Las amenazas habilitadas para la nube abarcan todas las etapas de la cadena de ataque en más de 1.609 aplicaciones, lo que representa el 44% de las amenazas detectadas en 2019. El SaaS se ha convertido en el principal objetivo de los ataques que utilizan dominios de confianza y certificados válidos para evadir las defensas *legacy,* que a menudo se ven obstaculizadas por la lista blanca.

La adopción de la nube también conlleva cruces de límites que las defensas web heredadas no detectan debido a una falta de visibilidad o a controles de bloqueo y politicas muy generales. Los datos pueden fluir entre las instancias personales y empresariales de las aplicaciones en la nube, entre aplicaciones en la nube gestionadas y no gestionadas, y entre aplicaciones en la nube de bajo riesgo y alto riesgo. Más allá de la conciencia de las instancias, es necesario comprender la actividad y sus anomalías, así como el contenido en sí y el contexto general. Con nuestra solución Next Gen SWG proporciona contexto de los datos y controles de política granulares para la nube y la web al encontrarse en el núcleo de la arquitectura de borde de servicio de acceso seguro para la nube (SASE).



Next Gen SWGs secure web and cloud

- **Acceso a sitios web y URL**
- **Aplicaciones en la nube gestionadas y personalizadas**
- **Miles de aplicaciones en la nube no gestionadas**
- **Entornos de nube pública**
- **Dispositivos gestionados y BYOD**

CONTROLES DE POLÍTICAS GRANULARES CON CLOUD XD

Los sitios web dinámicos de hoy utilizan el mismo lenguaje subyacente que las aplicaciones y servicios en la nube. La capacidad de decodificar este lenguaje es una capacidad crítica para las soluciones SWG de próxima generación, para la visibilidad tanto de las amenazas habilitadas para la nube como del movimiento de datos sensibles en la nube. El flujo de datos en aplicaciones no gestionadas impulsa la adopción de implementaciones de SWG basadas en la nube que pueden proteger a los usuarios en cualquier ubicación y en cualquier dispositivo. Esto, a su vez, impulsa la convergencia de las capacidades de SWG, Cloud/SaaS en línea y DLP para ofrecer protección avanzada contra amenazas y datos para el tráfico de la nube y la web.

Las políticas "permitir" o "bloquear" de las defensas web heredadas están siendo reemplazadas por una comprensión del contenido y el contexto para el usuario, la aplicación, la instancia, la clasificación de riesgo, los datos y la actividad en controles de políticas granulares. Una actividad en una instancia de una aplicación empresarial para datos confidenciales puede tener sentido, mientras que la misma actividad dentro de una instancia personal podría ser una fuga de datos o un robo por parte de un empleado.

DEFINIENDO LA PRÓXIMA GENERACIÓN DE SWG

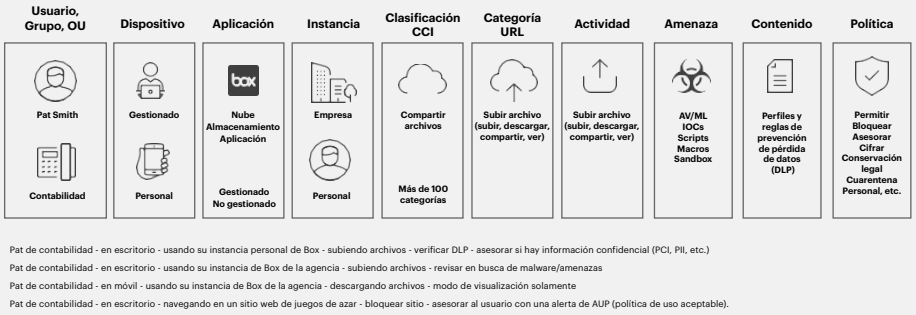
Intentar resolver los desafíos de seguridad con defensas heredadas deja muchos vacíos. Mientras que un SWG heredado enfocado en el tráfico web emparejado con un CASB que utiliza la protección de API de aplicaciones en la nube gestionadas suena completo, este conjunto de soluciones no aborda las miles de aplicaciones en la nube no gestionadas que son libremente adoptadas por unidades de negocio y usuarios como parte de su transformación digital. Agregar controles de permitir/bloquear para estas aplicaciones de nube con un SWG heredado, o usar un firewall de próxima generación (NGFW), simplemente permite las aplicaciones en la nube, sin tener en cuenta los flujos de datos, las amenazas en la nube y el contexto. Incluso usar calificaciones de riesgo de aplicaciones en la nube para bloquear aplicaciones de alto riesgo, y guiar a los usuarios hacia alternativas más seguras, todavía requiere que se permitan algunas aplicaciones en la nube, y se pierde información sobre la actividad, el contenido y el contexto.

La verdad es que los SWG heredados, NGFW e incluso las defensas de endpoints están perdiendo visibilidad debido a la adopción de la nube y la movilidad, y ya no son tan efectivos.

Hay muchas razones por las cuales los datos y el contexto son el núcleo de los SWG de próxima generación, y por qué también son un principio fundamental de la arquitectura SASE. La protección de datos en la nube es el futuro, ya que más usuarios y datos están fuera de los centros de datos que dentro de ellos hoy en día. Los usuarios acceden a la web, aplicaciones gestionadas, aplicaciones no gestionadas, nubes públicas y aplicaciones privadas basadas en la nube todos los días. Estos cinco destinos tienen flujos de datos que las reglas y políticas de cloud DLP en línea pueden proteger. Las amenazas también se han habilitado para la nube en todas las etapas de la cadena de ataque, y técnicas como el phishing en la nube están comprometiendo el acceso y evadiendo las defensas heredadas, incluyendo la protección de endpoints. El SWG de próxima generación va más allá de los registros web heredados, proporcionando metadatos ricos para impulsar la detección de anomalías basada en aprendizaje automático (ML) para amenazas y comportamientos en el tráfico de la nube y la web.la movilidad, y ya no son tan efectivos.

CONTROLES GRANULARES, METADATOS Y DETECCIÓN DE ANOMALÍAS DE COMPORTAMIENTO

En un mundo perfecto, la prevención resolvería todo, sin embargo, la realidad es que los equipos de seguridad necesitan detectar, investigar y responder, además de aplicar retrospectivamente nuevas inteligencias de amenazas. Esto requiere metadatos ricos para el tráfico web y en la nube, incluyendo aplicaciones, instancias, datos y actividades proporcionados por los SWGs de próxima generación. Los metadatos también impulsan modelos de aprendizaje automático para detectar amenazas avanzadas y anomalías en el comportamiento del usuario, incluyendo amenazas internas y compromisos de cuentas. Permitir/bloquear ya no funciona, la respuesta es "permitir" con controles granulares y recopilar metadatos ricos para desarrollar bases de referencia para la detección de anomalías basada en el aprendizaje automático, además de permitir la investigación y respuesta. Los SWGs de próxima generación tienen la visibilidad en el tráfico web y en la nube para los datos y el contexto que se requieren y que no son posibles con los



Pat de contabilidad - en escritorio - usando su instancia personal de Box - subiendo archivos - verificar DLP - asesorar si hay información confidencial (PCI, PII, etc.)
Pat de contabilidad - en escritorio - usando su instancia de Box de la agencia - subiendo archivos - revisar en busca de malware/amenazas
Pat de contabilidad - en móvil - usando su instancia de Box de la agencia - descargando archivos - modo de visualización solamente
Pat de contabilidad - en escritorio - navegando en un sitio web de juegos de azar - bloquear sitio - asesorar al usuario con una alerta de AUP (política de uso aceptable).

Cloud XD permite un contexto de política rico en detalles:

- Usuario, grupo y OU
- Dispositivo gestionado o personal URL, aplicación, categoría y calificación de riesgo
- Instancia de la compañía o personal
- Actividad y contenido para el contexto
- Protección avanzada contra amenazas
- Reglas y políticas avanzadas de prevención de pérdida de datos (DLP)
- Amenazas internas y anomalías de comportamiento

FLEXIBILIDAD PARA CONSTRUIR SU ARQUITECTURA SASE

Los cambios llevan tiempo, y un plan arquitectónico sólido comienza desde el núcleo. El Netskope Next Gen SWG proporciona un núcleo nativo en la nube con microservicios expandibles para adoptar más capacidades de seguridad a medida que avanza su transformación de seguridad. Combinar Netskope Private Access con Next Gen SWG proporciona una solución completa para los cinco destinos mencionados anteriormente, además de acceso a redes de confianza cero (ZTNA) para acceso seguro a aplicaciones privadas en centros de datos y nubes públicas. Las opciones de protección contra amenazas incluyen análisis estándar, avanzado y de comportamiento; mientras que las opciones de prevención de pérdida de datos (DLP) incluyen opciones estándar y avanzadas. Estas defensas y políticas de plataforma comunes también se pueden aplicar a la inspección basada en API de CASB de aplicaciones en la nube gestionadas y a la gestión de la postura de seguridad en la nube (CSPM) para entornos de nube pública, todo desde una sola consola.

SIJISA

FATIMA LAZCANO
INSIDE SALES
fatima.lazcano@sijisa.mx
M. 55 4063 7398
Of. 55 5358 2477 Ext. 6018

www.sijisa.mx