Resumen de la solución

Las tres principales ventajas de SASE y cómo beneficiarse de ellas

¿Por qué Secure Access Service Edge (SASE)?

Los modelos empresariales digitales modernos permiten nuevos niveles de participación de los clientes y los empleados al ofrecer un acceso disponible globalmente de modo sistemático a aplicaciones y servicios, sin importar dónde se conecten los empleados y los clientes, o qué dispositivos estén utilizando.

La seguridad de la red ya no se cumple cuando sus usuarios y aplicaciones se encuentran en lugares diferentes del mundo digital. Gartner desarrolló un nuevo modelo de trabajo en red y seguridad que se ajusta a los requisitos de la empresa digital. Lo llaman perímetro de servicio de acceso seguro o SASE (Secure Access Service Edge).

> “La arquitectura SASE tiene relevancia. Lo ideal es que la oferta sea nativa de la nube y esté basada en microservicios que tengan la capacidad de escalarse según sea necesario. Para minimizar la latencia, los paquetes deben copiarse en la memoria, actuar sobre ellos y reenviarse/bloquearse, no pasarlos de una máquina virtual (VM) a otra, o de una nube a otra. La pila de software no debe tener una dependencia específica del hardware y debe crearse una instancia cuando y donde sea necesario para ofrecer capacidades basadas en políticas y optimizadas para riesgos a la identidad del punto final”.— **Gartner**[1]

N.º1

Reduce el coste y la complejidad de TI

Con datos distribuidos en aplicaciones en la nube y servicios SaaS, y usuarios que a menudo trabajan desde cualquier lugar, el modelo de seguridad tradicional basado en la red ha alcanzado su límite. Las organizaciones se han visto obligadas a implementar servicios adicionales para cubrir las brechas en su seguridad, lo que ha hecho que aumentaran enormemente los costes de despliegue, administración y funcionamiento con un equipo humano que no está creciendo lo suficientemente rápido. Incluso con este aumento del coste y la complejidad, el modelo de seguridad de la red sigue sin poder ampliarse, no es ágil y simplemente no es eficaz en un mundo digital.

En lugar de intentar usar un concepto heredado para resolver un problema moderno, SASE de confianza cero da la vuelta al modelo de seguridad. Si bien los enfoques heredados se centran en la creación de perímetros alrededor de las aplicaciones, SASE se centra en las entidades, como los usuarios, que acceden a las aplicaciones, y lleva la seguridad lo más cerca posible de la entidad. Como servicio en la nube, SASE permite o deniega dinámicamente las conexiones al servicio en función de las reglas empresariales definidas por la organización o la agencia. Todo se realiza a través de un solo servicio que unifica una serie de funciones previamente separadas, como SWG, ZTNA, etc.

QUÉ TENER EN CUENTA

El componente más importante de una buena oferta de SASE es la arquitectura sobre la que se basa. Gartner especificó el tipo de arquitectura necesaria para conseguir un buen modelo SASE. Lo más importante es que debe construirse desde cero para tener la escala que necesita un servicio de seguridad totalmente entregado en la nube.

Esto significa que debe ser una oferta distribuida que admite varios usuarios para ajustarse globalmente y de forma dinámica en función de la demanda. Debe alejarse de los conceptos tradicionales de trabajo en red con políticas y capas de políticas y, en su lugar, basarse en políticas organizativas. Por último, esta arquitectura debe admitir una plataforma verdaderamente integrada con una gestión unificada en la nube.

ASPECTOS A EVITAR

Gartner desaconseja específicamente los enfoques tradicionales de seguridad de redes que utilizan las ofertas basadas en VM que se ejecutan en infraestructuras de proveedores de nube. Estos enfoques basados en VM en un entorno informático IaaS tendrán dificultades para escalarse y proporcionarán una experiencia de usuario inestable debido a los bucles invertidos necesarios entre los proveedores de la nube y las aplicaciones a las que acceden los usuarios.

Este modelo se basa en una arquitectura de un único inquilino que intenta utilizar políticas de acceso basadas en la red en un modelo SASE centrado en el acceso de los usuarios, lo que crea despliegues mucho más complejos que no se traducen en un modelo SASE. Además, estos enfoques se basan a menudo en múltiples productos que no están verdaderamente integrados, sino que están vinculados a través de una UI superpuesta de servicios independientes a menudo adquiridos a través de adquisiciones.

> “El perímetro de servicio de acceso seguro es una oferta emergente que combina capacidades integrales de WAN con funciones de seguridad de red globales (como SWG, CASB, FWaaS y ZTNA) para satisfacer las necesidades dinámicas de acceso seguro de las empresas digitales”. **– Gartner**[1]

N.º2

Proporciona una gran experiencia de usuario

Hay una buena razón por la que el enfoque principal de SASE es la experiencia del usuario. Cuando los usuarios estaban en la red, las aplicaciones estaban en el centro de datos y los servidores y la infraestructura eran propiedad de TI, que era quien la administraba, era fácil controlar y predecir la experiencia del usuario. Ahora que las aplicaciones se distribuyen en múltiples nubes, su método de acceso a estas aplicaciones sigue basado en el modelo anterior, que es una VPN que se conecta a una red para obtener seguridad. Este modelo lleva al usuario a la seguridad y no la seguridad al usuario, algo que es necesario si se quiere una buena experiencia de usuario. SASE de confianza cero exige que la seguridad se aplique cerca de los usuarios, que se gestionen de forma inteligente las conexiones de los usuarios en los intercambios de Internet y que se optimicen las conexiones directas (de interconexión) a las aplicaciones y servicios en la nube para garantizar un ancho de banda óptimo y una baja latencia.

QUÉ TENER EN CUENTA

La clave para ofrecer una excelente experiencia de usuario se reduce a proporcionar un ancho de banda óptimo con la latencia más baja. La única forma de hacerlo de forma eficaz es reducir los saltos para llegar a las aplicaciones y garantizar que se asigne el ancho de banda correcto mediante controles del mismo.

El enfoque correcto coloca la pila de seguridad lo más cerca posible del usuario en los intercambios de Internet en una implementación geográfica ampliamente distribuida. El acceso a las aplicaciones desde estas centrales requiere la capacidad de dirigir el tráfico de forma inteligente a la ubicación geográfica más cercana de la aplicación a través de la interconexión directa.

ASPECTOS A EVITAR

Las ofertas basadas en máquinas virtuales que se ejecutan en proveedores de nube o IaaS requerirán retorno de tráfico. En el documento de SASE, se indica específicamente que este tipo de ofertas no se pueden definir como una solución SASE y deben evitarse.

Esto se debe principalmente a que las arquitecturas basadas en VM no se ajustan y no controlan la conexión desde el usuario, sino que lo hacen desde el entorno informático de la aplicación y, por lo tanto, no pueden garantizar una buena experiencia de usuario. Además, estas ofertas no se pueden ajustar dinámicamente y requieren planificación de uso, por lo que no permiten hacer cambios más adelante si no hay paradas de inactividad programadas.

> “Las capacidades de aplicación y decisión de políticas de SASE deben estar en todos los lugares donde se ubiquen las identidades de los puntos finales. Las ofertas de SASE que utilizan solo la capacidad troncal de Internet de IaaS, pero no tienen capacidades de PoP local/perímetro, se enfrentan a latencia, problemas de rendimiento y la consiguiente insatisfacción del usuario final”. — **Gartner**[1]

N.º3 Reduce el riesgo

La seguridad se basa en identificar y evitar riesgos. Como servicio en la nube, SASE de confianza cero está diseñado para abordar los desafíos exclusivos que supone el riesgo en la nueva realidad de los usuarios y las aplicaciones distribuidos. Al definir la seguridad como una función integrada en el propio tejido del modelo y no como una función separada de la conectividad de los servicios, se garantiza que todas las conexiones se inspeccionan y protegen, independientemente de dónde se conecten los usuarios, a qué aplicaciones accedan o del cifrado que se utilice.

QUÉ TENER EN CUENTA

La clave para la reducción de riesgos es la capacidad de abandonar los conceptos de conectividad basada en red y, en su lugar, conectar a los usuarios a aplicaciones basándose en un verdadero acceso a la red de confianza cero (ZTNA). ZTNA garantiza que solo los usuarios que están autorizados a acceder a una aplicación puedan hacerlo, y esta autorización se define a través de políticas organizativas y no de definiciones complejas de políticas de múltiples capas.

Otra forma en la que una plataforma SASE reduce el riesgo es eliminando la superficie de ataque. Al ocultar a Internet la red corporativa y las identidades de origen, SASE evita que los adversarios se dirijan a usted con ataques como los DDoS.

El modelo SASE se entrega a través de una arquitectura basada en proxy que gestiona todas las comunicaciones entre usuarios y aplicaciones. Esta arquitectura garantiza que se pueda descifrar e inspeccionar todo el tráfico y proporciona una visibilidad completa. Por último, la arquitectura SASE se construye con un contexto en el que la totalidad de los datos se intercambian entre entidades y aplicaciones para garantizar que todas las conexiones cumplan con los requisitos de cumplimiento y control de datos.

ASPECTOS A EVITAR

Los enfoques tradicionales de seguridad perimetral utilizaban un modelo basado en cortafuegos que analizaba los flujos de paquetes y determinaba el riesgo basándose en la inspección de dichos flujos. Si bien este modelo funcionó para la seguridad basada en perímetros, fracasa con los nuevos desafíos que plantea una implementación basada en SASE.

El mayor problema es que una arquitectura de cortafuegos que se ejecuta como servicio determina las amenazas a posteriori, permitiendo que lleguen al destino antes de ser descubiertas. La razón es sencilla: son incapaces de retener los datos y determinar sus resultados antes de enviarlos. Esta limitación hace que el descifrado de la sesión y la protección de los datos resulten excepcionalmente difíciles, ya que son funciones que requieren que el flujo se retenga y se vuelva a ensamblar, de forma similar a un proxy.

Con un servicio de cortafuegos, las funciones de descifrado, inspección y reensamblaje requieren un proceso separado que se desacople del servicio y que complica la aplicación de políticas, introduce latencia y genera un rendimiento deficiente. Además, a menudo permite una funcionalidad limitada cuando se implementa. SASE requiere una arquitectura de un solo paso para procesar todo el contenido a la vez. Las ofertas de cortafuegos basados en flujos también exponen la dirección IP de origen de la red anfitriona a posibles adversarios, lo que visibiliza la superficie de ataque y puede conducir a ataques dirigidos.

El enfoque Zscaler a SASE

La plataforma de seguridad en la nube con IA de Zscaler es un servicio SASE construido desde cero para conseguir rendimiento y escalabilidad. Como plataforma distribuida globalmente, los usuarios siempre están a poca distancia de sus aplicaciones. A través de la interconexión con cientos de socios en los principales intercambios de Internet de todo el mundo, Zscaler proporciona un rendimiento y confiabilidad óptimos para sus usuarios, cargas de trabajo, socios empresariales y ubicaciones.

Zscaler Zero Trust SASE se basa en la plataforma SSE más probada de la industria con un nuevo enfoque para SD-WAN. Hoy en día, más del 30 % de las organizaciones de la Forbes Global 2000 confían en Zscaler para llevarlas a la era digital de forma segura.

Debido al tiempo que lleva en el mercado, Zscaler ha demostrado que su arquitectura se construyó para escalar y actualmente procesa más de 360 000 millones de transacciones por día y más de 500 billones de señales diarias por el efecto de la nube con IA/ML.

La arquitectura de Zscaler Zero Trust SASE se entrega a través de 150 centros de datos en todo el mundo, lo que garantiza que los usuarios obtengan conexiones seguras, rápidas y locales sin importar dónde se conecten.

Para obtener más información sobre el enfoque de Zscaler sobre SASE, visite zscaler.es/capabilities/secure-access-service-edge

[1] Gartner, El futuro de la seguridad de la red está en la nube. Lawrence Orans, Joe Skorupa, Neil MacDonald.

zscaler™ | Experience your world, secured.™

Acerca de Zscaler
Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de los ciberataques y la pérdida de datos mediante la conexión segura de usuarios, dispositivos y aplicaciones en cualquier lugar. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basada en SSE es la mayor plataforma de seguridad en la nube en línea del mundo. Obtenga más información en **zscaler.es** o síganos en Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.es