Resumen de la solución

Las tres principales ventajas de SASE y cómo beneficiarse de ellas

¿Por qué es mejor secure access service edge (SASE)?

Los modelos de negocio digitales modernos permiten nuevos niveles de participación de clientes y empleados al ofrecer un acceso a las aplicaciones y servicios que está disponible en todo el mundo y de forma constante, independientemente de dónde se conecten los empleados y clientes o de los dispositivos que utilicen.

La noción de seguridad de red cuando sus usuarios y aplicaciones están distribuidos ya no es viable en un mundo digital. Gartner desarrolló un nuevo modelo de redes y seguridad que se adapta a los requisitos de la empresa digital. Lo llaman perímetro de servicio de acceso seguro (SASE).

> “La arquitectura SASE es importante. Lo ideal es que la oferta esté en la nube y esté basada en microservicios con la capacidad de escalarse según sea necesario. Para minimizar la latencia, los paquetes deben copiarse en la memoria, se debe actuar en consecuencia y se deben reenviar/bloquear, no pasar de una máquina virtual (VM) a otra o de una nube a otra. La pila de software no debe tener ninguna dependencia específica del hardware y debe crear instancias cuando y donde sea necesario para ofrecer las capacidades optimizadas para el riesgo y basadas en políticas para la identidad del punto final." – **Gartner1**[1]

#1 Reduce el costo y la complejidad de TI

Con los datos repartidos entre las aplicaciones en la nube y los servicios SaaS, y los usuarios que suelen trabajar desde cualquier lugar, el modelo tradicional de seguridad basado en la red ha llegado a su límite. Para compensarlo, las organizaciones se han visto obligadas a implementar servicios adicionales para cubrir las lagunas de su seguridad, al tiempo que aumentaban enormemente los costos de implementación, gestión y funcionamiento con un equipo que no crece lo suficientemente rápido. Incluso con este aumento del costo y la complejidad, el modelo de seguridad de la red sigue sin poder escalarse, no es ágil y simplemente no es eficaz en un mundo digital.

En lugar de intentar utilizar un concepto heredado para resolver un problema moderno, Zero Trust SASE invierte el modelo de seguridad. Mientras que los modelos heredados se centraban en crear 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 niega dinámicamente conexiones al servicio según las reglas comerciales o de agencia definidas por una organización. Todo se hace a través de un único servicio que unifica una serie de funciones previamente separadas, como SWG, ZTNA, etc.

QUÉ DEBEMOS BUSCAR

El componente más importante de una gran oferta SASE es la arquitectura sobre la que se construye. Gartner fue concreto en cuanto al tipo de arquitectura necesaria para cumplir la promesa de SASE. Lo más importante es que debe construirse desde cero para abordar la escala requerida para un servicio de seguridad totalmente prestado en la nube.

Esto significa que debe ser una oferta distribuida que admita múltiples usuarios, lo que le permitirá escalarla global y dinámicamente en función de la demanda. Debe alejarse de los conceptos tradicionales de creación de redes de políticas y niveles de políticas y, en cambio, basarse en políticas organizacionales. Por último, esta arquitectura debe proporcionar una plataforma verdaderamente integrada con una gestión unificada en la nube.

QUÉ DEBE EVITAR

Gartner advierte específicamente contra los modelos tradicionales de seguridad de redes que utilizan ofertas basadas en VM que se ejecutan en infraestructuras de proveedores de nube. El uso de estos modelos basados en VM en un entorno informático IaaS tendrá dificultades para escalarse y proporcionará una experiencia de usuario irregular debido a la división necesaria entre los proveedores de la nube y las aplicaciones a las que acceden los usuarios.

Este modelo se basa en una arquitectura de inquilino único que intenta utilizar políticas de acceso basadas en la red en un modelo SASE basado en el acceso de los usuarios, lo cual crea implementaciones mucho más complejas que no son compatibles con un modelo SASE. Además, estos modelos se basan a menudo en múltiples productos que no están verdaderamente integrados, sino que se unen mediante una interfaz de usuario superpuesta de servicios independientes adquiridos a menudo mediante adquisiciones.

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

#2 Ofrece una gran experiencia de usuario

Hay una buena razón por la que el modelo principal de SASE es la experiencia del usuario. Cuando los usuarios estaban en la red, las aplicaciones en el centro de datos y los servidores y la infraestructura eran propiedad de TI, que se encargaba de su gestión, era fácil controlar y predecir la experiencia de los usuarios. Ahora que las aplicaciones están distribuidas en varias nubes, su método de acceso a estas aplicaciones sigue basándose en el antiguo modelo de una VPN que se conecta a una red por seguridad. Este modelo acerca el usuario a la seguridad y no la seguridad al usuario, lo cual es necesario para una gran experiencia de usuario. Zero Trust SASE exige que la seguridad se cumpla cerca de los usuarios, gestionando de forma inteligente sus conexiones en las centrales de Internet y optimizando las conexiones directas (peering) a las aplicaciones y servicios en la nube para garantizar un ancho de banda óptimo y una baja latencia.

QUÉ DEBEMOS BUSCAR

La clave para ofrecer una gran experiencia de usuario se reduce a proporcionar un ancho de banda óptimo con la menor latencia. La única forma de hacerlo eficazmente es reducir los saltos para llegar a las aplicaciones y garantizar que se asigne el ancho de banda adecuado mediante controles de ancho de banda.

El modelo correcto sitúa la pila de seguridad lo más cerca posible del usuario en los intercambios por Internet mediante una implementación geográfica ampliamente distribuido. Para tener acceso a las aplicaciones desde estos intercambios se requiere la capacidad de enrutar el tráfico de manera inteligente a la ubicación geográfica más cercana de la aplicación a través del emparejamiento directo.

QUÉ SE DEBE EVITAR

Las ofertas basadas en máquinas virtuales que se ejecutan en proveedores de nube o IaaS requerirán conexiones entre nodos para el tráfico. Tales ofertas se señalan específicamente en el documento SASE como no cualificadas para ser definidas como una solución SASE y deben evitarse.

Esto se debe principalmente a que las arquitecturas basadas en máquinas virtuales no escalan y no controlan la conexión desde el usuario, sino que lo hacen desde el entorno informático de la aplicación y, por tanto, no pueden garantizar una buena experiencia de usuario. Además, estas ofertas no pueden escalarse dinámicamente y requieren una planificación del uso que carece de la capacidad de permitir cambios posteriores sin tiempos de inactividad programados.

> “Las capacidades de decisión y aplicación de políticas de SASE deben estar en todos los lugares donde se ubicarán las identidades de los puntos finales. Las ofertas de SASE que utilizan únicamente la capacidad de la red troncal de Internet de IaaS, pero sin capacidades POP/edge locales, corren el riesgo de sufrir problemas de latencia, rendimiento y la consiguiente insatisfacción del usuario final." — **Gartner**[1]

#3 Reduce el riesgo

La seguridad consiste en identificar y evitar los riesgos. Zero Trust SASE como servicio en la nube está diseñado para hacer frente a los desafíos únicos del riesgo en la nueva realidad de usuarios y aplicaciones tan dispersos. 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 sean inspeccionadas y aseguradas, independientemente de dónde se conecten los usuarios, a qué aplicaciones accedan o de la encriptación que se utilice.

QUÉ DEBEMOS BUSCAR

La clave para la reducción de riesgos es la capacidad de no tener en cuenta los conceptos de conectividad basados en la red y, en su lugar, conectar a los usuarios con las aplicaciones basándose en un verdadero acceso a la red de confianza cero (ZTNA). El ZTNA garantiza que solo los usuarios autorizados a acceder a una aplicación puedan hacerlo, y esta autorización se define mediante políticas organizativas y no mediante complejas definiciones de políticas de varios niveles.

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

El modelo SASE se ofrece a través de una arquitectura basada en proxy que gestiona todas las comunicaciones entre los usuarios y las aplicaciones. Esta arquitectura garantiza que todo el tráfico pueda descifrarse e inspeccionarse y proporciona visibilidad total. Por último, la arquitectura SASE está diseñada con un contexto de datos completo que se intercambia entre entidades y aplicaciones para garantizar que todas las conexiones cumplan los requisitos de conformidad y gobernanza de datos.

QUÉ SE DEBE EVITAR

Los modelos tradicionales de la seguridad perimetral utilizaban un modelo basado en firewalls que examinaba los flujos de paquetes y determinaba el riesgo en función de la inspección de dichos flujos. Aunque este modelo funcionaba para la seguridad basada en el perímetro, fracasa ante los nuevos riesgos de una implementación basada en SASE.

El principal problema es que una arquitectura de firewall que funcione como un servicio determina las amenazas a posteriori, permitiéndoles llegar al destino antes de ser descubiertas. La razón es simple: son incapaces de retener los datos y determinar sus resultados antes de enviarlos. Esta limitación dificulta excepcionalmente el descifrado de sesiones y la protección de datos, ya que se trata de funciones que requieren que el flujo se retenga y se vuelva a ensamblar, de forma similar a un proxy.

Con un servicio de firewall, las funciones de descifrado, inspección y reensamblado requieren un proceso separado que está desacoplado del servicio, lo que complica las políticas, genera latencia y da lugar a un rendimiento deficiente, y a menudo permite una funcionalidad limitada cuando se implementa. Además, SASE requiere una arquitectura de paso único para procesar todo el contenido a la vez. Las ofertas de firewall basados en secuencias también exponen la dirección IP de origen de la red del host a los adversarios potenciales, publicitando eficazmente su superficie de ataque, lo que puede dar lugar a ataques dirigidos.

El modelo de Zscaler para SASE

La plataforma de seguridad en la nube con IA de Zscaler es un servicio SASE creado desde cero para el rendimiento y la escalabilidad. Como plataforma distribuida globalmente, los usuarios siempre están a un paso de sus aplicaciones, y a través del trabajo en red con cientos de socios en los principales intercambios de Internet de todo el mundo, Zscaler garantiza un rendimiento y una fiabilidad óptimos para sus usuarios, cargas de trabajo, socios comerciales y ubicaciones.

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

Debido a su tiempo en el mercado, Zscaler ha demostrado que su arquitectura fue diseñada para escalar, procesando en la actualidad más de 360,000 millones de transacciones al día, y más de 500T de señales diarias para el uso de IA/ML en la nube.

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

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

[1] Gartner, The Future of Network Security Is in the Cloud; 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, fuertes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de ataques cibernéticos y pérdida de datos al conectar de forma segura usuarios, dispositivos y aplicaciones en cualquier ubicación. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SSE es la plataforma de seguridad en la nube en línea más grande del mundo.
Obtenga más información en **zscaler.com.mx** o síganos en Twitter **@zscaler** .

+1 408.533.0288 Zscaler, Inc. (Oficinas centrales) • 120 Holger Way • San José, CA 95134 zscaler.com.mx