Orange
Cyberdefense

SASE : el habilitador de negocios para su fuerza de trabajo

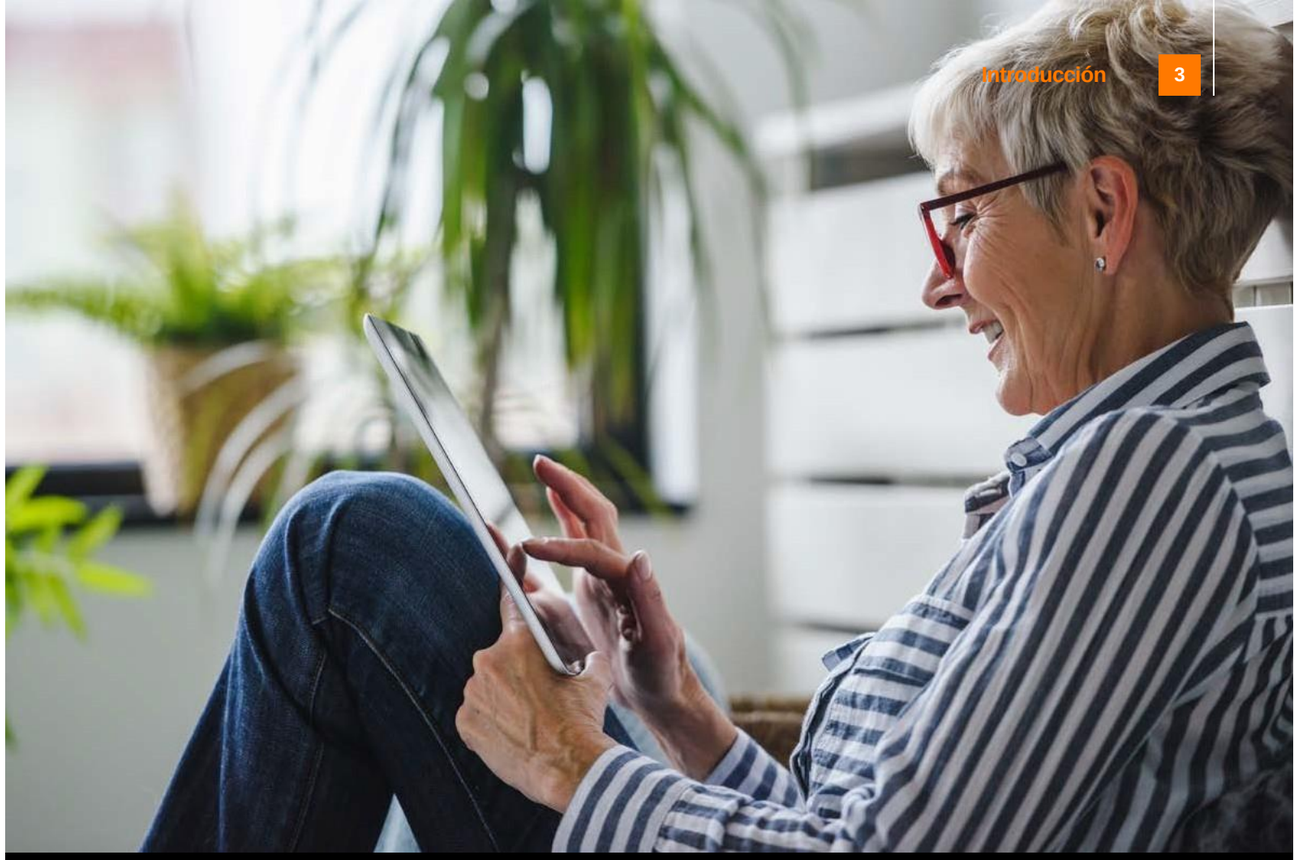
Simplificando la arquitectura de seguridad de su red para el futuro

Simplificando la arquitectura de seguridad de su red para el futuro

Este es un momento de cambios sin precedentes para las organizaciones a medida que trasladan sus servicios a la nube y sus empleados se vuelven más dispersos. Para dar soporte a este nuevo modelo, Internet se está convirtiendo en la nueva red corporativa. La arquitectura de seguridad tradicional centrada en la red es demasiado compleja para manejar este nuevo paradigma. Se está convirtiendo en un cuello de botella que inhibe las necesidades del negocio digital. Es hora de una nueva arquitectura de seguridad.

Contenido

Escrito por: José Araujo, Group CTO, Orange Cyberdefense © Orange Cyberdefense, con la apoyo de: Étienne Greeff, Grupo CTO, Orange Cyberdefense y Tomás Surdon, Estrategic Marketing and Innovation Director, Connectivity Business Unit, Orange Business Services



Introducción

El contexto empresarial actual exige un acceso seguro a los datos y las aplicaciones desde cualquier lugar, momento, dispositivo y dondequiera que se alojen esos activos. El modelo de seguridad de red tradicional no es compatible con esto. Fue creado para dispositivos y usuarios que rara vez abandonan el refugio de la red de la empresa. Esos dispositivos estaban protegidos por un perímetro duro que ofrecía seguridad a todo lo que había dentro.

Actualmente usuarios, dispositivos y aplicaciones se trasladaron fuera de la la red. El modelo basado en el perímetro se volvió menos relevante a medida que la computación en la nube y la tecnología móvil avanzaba.

En Agosto 2019, Gartner propuesto a nuevo modelo: Secure Access Service Edge (SASE). Reformuló el concepto de las redes y la arquitectura de seguridad de la red para ayudar a las organizaciones a hacer frente a los cambiantes requisitos de seguridad que enfrenta la empresa distribuida.

SASE es una iniciativa desafiante y de largo alcance. El mercado aún se está poniendo al día con estas ideas a medida que los proveedores luchan por ofrecer las soluciones necesarias para respaldar este modelo.

Mientras esperamos que esta solución alcance la maduréz, podemos aprovechar la oportunidad para iniciar la conversación y participar donde podamos, monitoreando los desarrollos del mercado relacionados con SASE y ayudando a nuestros clientes a desarrollar estrategias de adopción a largo plazo con nuestro enfoque basado en inteligencia.

Este documento técnico explica el concepto SASE y sus beneficios, abordando los desafíos actuales para adoptar este modelo y proteger su negocio digital distribuido.

¿Qué es SASE?

SASE es un concepto, no una solución. Une la red y la seguridad de la red, ofreciendo acceso seguro a todos los usuarios desde cualquier lugar. No es simplemente una solución que las empresas pueden instalar y utilizar. Es un modelo que necesita monitoreo, detección y respuesta continuos impulsados por una inteligencia de amenazas en constante evolución.

SASE transfiere múltiples protecciones a los servicios de seguridad que se encuentran en el borde de la WAN, cerca de las ubicaciones de los usuarios. Este modelo se basa en gran medida en la identidad del usuario al otorgar acceso a datos y aplicaciones en lugar de confiar en dispositivos o redes individuales.

Este nuevo enfoque redefine el perímetro tradicional, reemplazando los sistemas de ciberseguridad on-premise por servicios integrados en la nube. Redefine estos servicios de seguridad de red en software, creando una plataforma única que puede aplicar políticas de seguridad unificadas por sesión para un control de seguridad granular.

Este ecosistema de seguridad de red unificado abarca la red global, lo que permite a los usuarios acceder a los servicios de forma segura y consistente desde cualquier lugar. También es flexible, lo que permite a las empresas ofrecer más servicios de seguridad a medida que evolucionan las necesidades del negocio.

¿Por qué necesitamos este enfoque?

SASE representa un cambio radical en la forma en que abordamos la seguridad, junto con una gran inversión en tiempo y esfuerzo. ¿Por qué las empresas lo requerirán?

En un mundo donde las prácticas de trabajo y las infraestructuras se enfrentan a cambios profundos, las organizaciones deben encontrar nuevas formas de mantener el control de sus datos. Deben respaldar una nueva era en la que dispositivos que no son confiables se conectan a recursos de TI distribuidos desde redes no controladas.

Las organizaciones necesitan SASE para hacer frente a la complejidad adicional que esto crea. Ofrece una red integrada y una infraestructura de seguridad de red para gestionar el rendimiento y la seguridad desde un único punto mediante una política unificada. La transformación de la nube es un impulsor importante para el modelo SASE.

> “ IDC predice que el gasto global total en productos y servicios en la nube mantendrá una tasa de crecimiento anual compuesta (CAGR) del **15,7%** hasta 2024.[1]

Los servicios de seguridad deben proteger las aplicaciones y los datos dondequiera que estén, y éstos se están trasladando cada vez más a la nube. IDC predice que el gasto mundial total en productos y servicios en la nube mantendrá una tasa de crecimiento anual compuesta (CAGR) del 15,7% hasta 2024.[1] Este nuevo enfoque para la seguridad de la red se volverá más importante a medida que más aplicaciones se vuelvan nativas de la nube.

> “ La Comisión Europea calcula que cerca del **40%** de los trabajadores de la UE trabajaron de forma remota a tiempo completo durante el brote de COVID-19.[2]

SASE también se vuelve más necesario a medida que cambian nuestros patrones de trabajo. La pandemia aceleró una tendencia creciente de teletrabajo, con cifras de la Comisión Europea que encontraron que cerca del 40% de los trabajadores en la UE trabajaron en forma remota a tiempo completo durante el brote de COVID-19. Eso es un aumento masivo, dado que solo el 15% de los trabajadores de la UE habían teletrabajado antes de la crisis.

En solo unos meses, ya hemos visto brechas en la seguridad perimetral tradicional a medida que las empresas luchan por atender a una nueva fuerza laboral remota. Por ejemplo, el Centro Nacional de Seguridad Cibernética del Reino Unido y la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) de EE. UU. emitieron un aviso conjunto en abril de 2020 advirtiendo de varios ataques relacionados con COVID-19 dirigidos a infraestructuras de acceso remoto y trabajadores remotos.

En el mundo pospandemia, las personas son el nuevo perímetro. Los trabajadores remotos necesitan un acceso más rápido, sencillo y seguro a sus aplicaciones, incluso cuando no utilizan dispositivos de confianza. SASE es la clave para ese acceso seguro.

El crecimiento de IoT también está creando la necesidad del modelo SASE. Según IDC, para 2025 habrá 55 mil millones de dispositivos conectados en todo el mundo, el 75% de los cuales se conectará a una plataforma IoT.[4] Eso crea una gran cantidad de datos que las organizaciones deben manejar de forma segura. Los volúmenes de datos de IoT aumentarán a 73 zettabytes en 2025 de 18 zettabytes en 2019, advirtió la compañía analista.

Éste rápido crecimiento está acelerando el acceso perimetral para una avalancha de nuevos dispositivos. Los grandes volúmenes de dispositivos y equipos hacen que la seguridad de IoT de los endpoints sea un desafío para implementar. Mover la seguridad al borde de la nube ayuda a resolver estos problemas de volumen y complejidad de la infraestructura.

Beneficios

SASE brindará un amplio conjunto de servicios de seguridad de red de manera consistente e integrada para respaldar la transformación digital del negocio, el edge computing y la movilidad de la fuerza laboral. Adoptarlo traerá los siguientes beneficios:

Flexibilidad
SASE permite a las organizaciones dirigir el tráfico a la nube desde cualquier sitio en lugar de enrutarlo a través del centro de datos, lo que elimina un importante cuello de botella.

Ahorro de costos
Poner la seguridad de la red en la nube ayuda a reducir los gastos de capital para la infraestructura local. Las empresas que adopten un modelo SASE disfrutarán de gastos operativos predecibles gracias a un modelo de seguridad basado en servicios.

Complejidad reducida
Las organizaciones pueden hacer que el personal de seguridad pase de administrar dispositivos individuales a brindar servicios de seguridad basados en políticas desde un solo punto, lo que les permite configurar estructuras de seguridad y de red de extremo a extremo de manera más simple y coherente.

Mayor automatización
La infraestructura definida por software es un principio clave de la propuesta SASE. Crea una plataforma de tecnología convergente que admite la aplicación de políticas unificadas mediante programación. Así como los desarrolladores de software disfrutaron de DevOps, los administradores pueden disfrutar de un modelo de operaciones de seguridad automatizado de extremo a extremo.

Mejor prestación
SASE mejora y acelera el acceso a los recursos de Internet a través de una infraestructura de red global optimizada de baja latencia, alta capacidad y alta disponibilidad.

Confianza Zero
La confianza cero se encuentra en el corazón del modelo operativo SASE. Ofrece acceso seguro a aplicaciones privadas en nubes públicas y centros de datos en lugar de acceso a nivel de red.

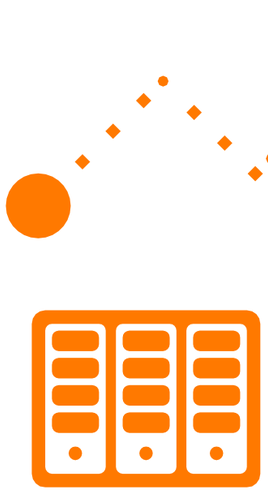
Protección contra amenazas
Al poner la seguridad en el borde de la red entre el usuario y la nube, SASE permite a las empresas detectar y prevenir ataques como el phishing en la nube, el malware, el ransomware y los infiltrados malintencionados.

Protección de Datos
Al centrar la seguridad en la identidad, SASE ofrece protección a nivel de datos, otorgando a las personas acceso a activos clave con privilegios mínimos como parte de un estricto proceso de verificación de identidad. Esto protege los datos en todas partes, desde el interior de la organización hasta la nube pública, en redes que no son de confianza y más allá.

La arquitectura SASE propuesta

Durante años, las redes conectaron a los usuarios con aplicaciones en el centro de datos. Estos perímetros de red usaban múltiples controles de seguridad para proteger las aplicaciones y los datos un ataque externo. En ocasiones, las organizaciones agregaron segmentación junto con dispositivos de seguridad avanzados dentro del perímetro para agregar capas adicionales de protección.

Al principio, las redes de área amplia que conectaban a los usuarios con los centros de datos usaban líneas dedicadas lentas y costosas. Luego, sucedieron varias cosas en concierto: las aplicaciones se trasladaron a la nube, las redes de borde se hicieron más frecuentes a medida que evolucionaba la tecnología IoT y el mundo cambió a utilizar conexiones de Internet más baratas y rápidas. Más recientemente, los usuarios se sumaron a estas presiones, moviéndose fuera del perímetro de manera más permanente a medida que cambiaban los patrones de trabajo.



1

El problema de la arquitectura actual

La seguridad de red basada en el perímetro ya no puede soportar este nuevo contexto. De hecho, agrega complejidad y costo. Todavía fuerza las conexiones a través del centro de datos, incluso para las aplicaciones en la nube, lo que convierte al centro de datos en un costoso cuello de botella.

Los dispositivos de ciberseguridad en el centro de datos son inflexibles. Dependen de la ubicación, se basan en el tráfico que pasa a través de una red específica y no son escalables fácilmente. Rara vez utilizan una capa de control definida por software , lo que los hace complejos de configurar y difíciles de integrar. Eso dificulta la aplicación y el mantenimiento de una seguridad constante, lo que crea brechas en la postura de seguridad.

Si bien este modelo puede haber funcionado para el trabajo en la oficina , debemos repensarlo en un entorno pospandémico que coloca a la mayoría de los empleados fuera de los controles de seguridad heredados. Debemos reevaluar nuestros planes de respuesta a incidentes y reevaluar la responsabilidad de la seguridad en este nuevo entorno de trabajo.

2

Cómo avanza SASE

En un negocio digital moderno centrado en la nube, los usuarios y los dispositivos están dispersos, al igual que los recursos a los que necesitan acceder. También necesitamos servicios de acceso seguro en todas partes, integrados en una red global que esté lista para servir a los usuarios dondequiera que estén.

En este tejido mundial, los servicios de seguridad basados en contenedores se ejecutan en la nube en puntos de presencia (POP) basados en el perímetro. Estos servicios incluyen firewalls, puertas de enlace web seguras (SWG), agentes de seguridad de acceso a la nube (CASB), acceso a la red de confianza cero (ZTNA), DNS seguro, DHCP y administración de direcciones IP (DDI).

SASE se basa en estos servicios definidos por software con características de seguridad adicionales que ofrecen protección de red de extremo a extremo. Esto protege los datos a lo largo de su viaje desde el usuario hasta la aplicación, independientemente de su ubicación.

En este modelo, el tráfico se enruta dinámicamente según los requisitos de la sesión. Permite el acceso directo a las aplicaciones en la nube sin enrutamiento a través del centro de datos, lo que reduce la latencia y la carga de los recursos corporativos al tiempo que refuerza la seguridad.

Este modelo de seguridad basado en la periferia acerca los servicios de ciberseguridad a los activos que protegen. Estos podrían ser sucursales, pero también podrían ser usuarios individuales o incluso dispositivos IoT. La seguridad de red basada en edge es compatible con todos.

La identidad es clave para la autenticación en este modelo de acceso a la red de confianza cero. En lugar de depender de dispositivos confiables para la autenticación, estos servicios de ciberseguridad basados en el borde se enfocan en la identidad de lo que sea que esté haciendo la conexión.

Este enfoque protege a los usuarios en redes domésticas y públicas inseguras, no solo en las corporativas. Los usuarios que acceden a SASE desde redes domésticas suelen utilizar un agente de gestión de endpoint en su dispositivo que lo protege de ataques y potencialmente protegería los datos de los activos personales. Sin embargo, es posible admitir dispositivos completamente no administrados enrutándolos a entornos de espacio aislado a través del POP.

> “ La identidad es clave para la autenticación en este modelo de acceso a la red de confianza cero. En lugar de depender de dispositivos confiables para la autenticación, estos servicios de ciberseguridad basados en el borde se enfocan en la identidad de lo que sea que esté haciendo la conexión.

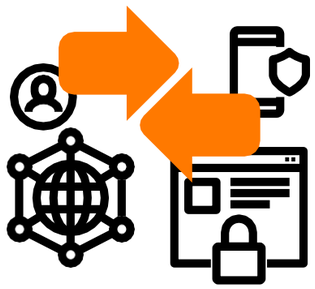
Trabajar desde casa implica cambios culturales más amplios que requieren capas de seguridad adicionales. Las redes domésticas albergan dispositivos que no son de confianza, como PCs domésticas y televisores inteligentes. Las arquitecturas de seguridad deben reconocerlos.
Las organizaciones deben considerar lo que comprende la red corporativa en un mundo de trabajo remoto. ¿Son los hogares de los empleados una extensión de la red corporativa? ¿Deberían los empleadores tratar las amenazas en el entorno doméstico de manera similar a las de la red corporativa? ¿Deberían incluir el entorno doméstico en sus programas de gestión de vulnerabilidades? Estas son cuestiones arquitectónicas importantes.

3 Simplificando la red

SASE promete más que solo seguridad; promete simplicidad. Las redes actuales a menudo se ven sobrecargadas por una combinación de productos de seguridad de diferentes proveedores. Estas carteras crecen orgánicamente ó mediante adquisiciones, creando conjuntos de soluciones complejas e incompatibles que son difíciles de administrar y consumen mucho tiempo . Afectan el rendimiento de la red y dificultan la seguridad.

El modelo SASE consolida estos entornos de ciberseguridad fragmentados en una plataforma unificada más simple que involucra a un conjunto más pequeño de proveedores. Eso garantiza una seguridad óptima en todas partes de la red y fomenta la interoperabilidad, detectando las amenazas antes de que se escapen. También reduce el impacto de las herramientas de seguridad en el rendimiento y el costo.

4 Más allá de SD - WAN



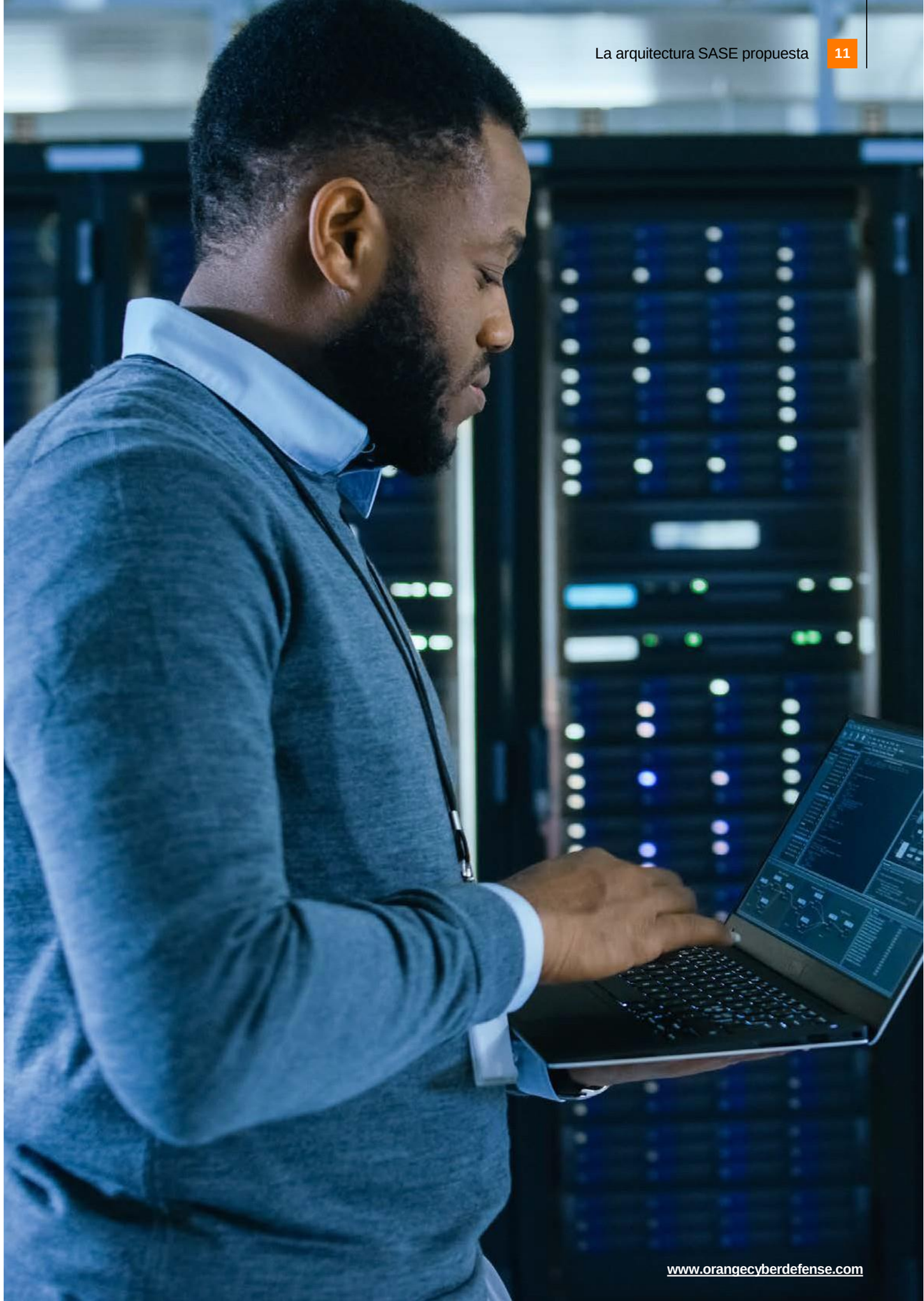
Habiendo pasado algún tiempo definiendo qué es SASE, es importante articular lo que no es. SASE no es solo SD-WAN.

SD-WAN es todavía un término lo suficientemente joven como para que las implementaciones de los proveedores varíen enormemente, lo que dificulta la entrega de un componente de seguridad cibernética confiable y consistente. Muchos de ellos brindan servicios de seguridad a través de equipos en las instalaciones del cliente que pueden ser costosos de implementar.

Tampoco es solo seguridad basada en la nube . Los servicios de ciberseguridad basados en la nube que no se integran a la perfección con la funcionalidad de red definida por software pierden las ventajas de la protección de confianza cero, el rendimiento y la política de seguridad uniforme de SASE.

La combinación de ofertas de red y seguridad de SASE es un enfoque más simple, económico y flexible de la ciberseguridad que pensar en SD-WAN y seguridad por separado. Poner los servicios de ciberseguridad en la red definida por software como servicios nativos en la nube en los POP basados en el borde hace que sea más fácil de implementar y administrar .

> “ La combinación de ofertas de red y seguridad de SASE es un enfoque más simple, económico y flexible de la ciberseguridad que pensar en SD-WAN y seguridad por separado.



La importancia de la identidad

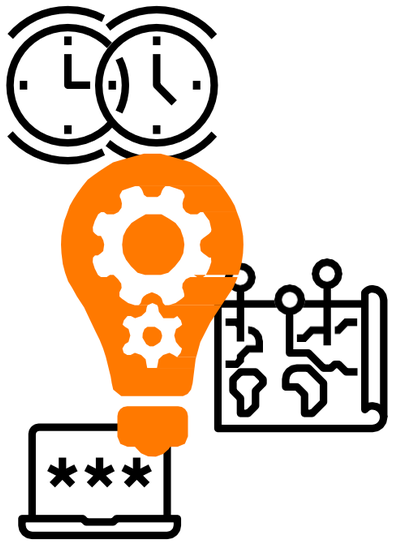
SASE combina red y seguridad, entregando ambos como un servicio basado en la nube, pero nuestro enfoque en este e-book está en la seguridad de la red.

La identidad sustenta esos servicios de seguridad de red en un entorno SASE. Esta es la clave que hace posible la aplicación automática de políticas.

SASE toma decisiones basadas en el contexto cuando aplica políticas que rigen la seguridad y los privilegios de acceso. El dato principal que contribuye a ese contexto es la identidad del usuario, dispositivo o servicio que accede al recurso. Otros parámetros, como la ubicación, el tiempo de acceso, el nivel de confianza y los datos solicitados, también afectan ese contexto.

Debido a que todos estos parámetros pueden cambiar entre sesiones, las políticas de seguridad cibernética se adaptan por sesión en un entorno SASE.

> “La identidad sustenta los servicios de seguridad de la red en un entorno SASE. Esta es la clave que hace posible la aplicación automática de políticas.



Orientación

Hemos discutido el entorno SASE ideal, pero debemos ser realistas; ir de aquí para allá implicará mucho trabajo. Los caminos hacia una solución SASE también son variados y los detalles de implementación dependerán del contexto y los objetivos de la empresa.

Gartner describe numerosos riesgos en su informe, y muchos de ellos se derivan de la misma preocupación central: la falta de capacidad del proveedor.

Le recomendamos que discuta sus planes de arquitectura SASE a largo plazo con los MSPs centrados en la seguridad. Piense más allá de sus opciones de tecnología, considerando también las políticas y los perfiles de seguridad que admitirán esas tecnologías relacionadas con SASE. La inspección y aplicación dinámica del tráfico basada en el contexto, uno de los principios básicos de una solución de acceso a la red de confianza cero, debe ser una prioridad al visualizar una arquitectura SASE.

Una iniciativa SASE será un largo recorrido. Redefine cómo la mayoría de las organizaciones abordan la seguridad en un nivel básico y toca cada parte de su infraestructura. Una mezcla de inercia organizacional, inversión deprimida y retrasada hacen de este proyecto una propuesta a largo plazo.

Manténgase ágil

Con esto en mente, el cambio a SASE será una serie de pasos incrementales. Tenga en cuenta los requisitos básicos de este modelo cuando renueve proyectos existentes o implemente otros nuevos, especialmente en torno a servicios de seguridad como SWG, CASB y VPN.

Busque oportunidades de consolidación a corto plazo cuando evalúe estas renovaciones, reemplazos y nuevos desarrollos. Ahora es el momento de mudar los servicios existentes, simplificar y de duplicar la funcionalidad. Explore las decisiones de compra desde un punto de vista estratégico, entendiendo cómo se insertarán en la arquitectura SASE más amplia en lugar de centrarse solo en características aisladas del producto.

Cualquier compra o actualización es una oportunidad para hacer la transición de los servicios heredados a una arquitectura definida por software, manejable desde una sola consola. Concéntrese en la destrucción de silos de seguridad y la integración de productos para respaldar políticas unificadas.

Estas decisiones arquitectónicas informarán la capacidad de escalar de la infraestructura de seguridad y mejorarán su respuesta a las amenazas y presiones cambiantes.

Adopte un enfoque mini-platform

Si bien un modelo SASE enfatiza la consolidación, creemos que no es realista confiar en un solo proveedor para proporcionar todas estas partes móviles. Aunque las empresas podrán reducir la cantidad de proveedores de ciberseguridad con los que trabajan, no podrán adquirir una solución de un solo proveedor que cubra todas sus bases.

Por ejemplo, un requisito de una solución SASE es la inspección del tráfico cifrado a escala. Esto es especialmente importante en un entorno que aplica múltiples protecciones de ciberseguridad. No todos los proveedores admitirán esta inspección del tráfico cifrado para el procesamiento multiservicio de un solo paso al nivel que usted espera.

> “ Lo ideal es impulsar contratos a corto plazo con licencias flexibles al negociar con los proveedores para mantener sus opciones abiertas durante un período de rápida evolución y cambio.

Otras demandas de los proveedores incluyen el conocimiento del contexto de los datos, que va más allá de la inspección del tráfico encriptado para ver cómo se utilizan los datos en un entorno de nube. Eso requiere una inspección de los entornos del proveedor de servicios en la nube frente a las interfaces de programación de aplicaciones. No todos los proveedores lograrán esto.

La capacidad de los proveedores para jugar bien en la nube también es una preocupación clave para Gartner. Le preocupa que los proveedores con sus raíces en los dispositivos de hardware puedan tener dificultades para hacer la transición a la prestación de servicios nativos de la nube, tan crucial en un entorno SASE.

En lugar de depender de un solo proveedor, adopte un enfoque de miniplataforma, reduciendo sus carteras de proveedores. Encuentre conjuntos de soluciones que dependan de entre tres y cinco proveedores y reemplácelos con soluciones de un solo proveedor. Esto equilibra las mejores capacidades de su clase con eficiencias operativas.

Lo ideal es impulsar contratos a corto plazo con licencias flexibles cuando negocien con los proveedores para mantener sus opciones abiertas durante un período de rápida evolución y cambio.

Aunque muchas de estas decisiones de compra no se materializarán durante algún tiempo, puede comenzar a desafiar a los proveedores ahora con estos requisitos emergentes y dar a conocer sus criterios de compra. Analice su estrategia tecnológica con proveedores de servicios de red y seguridad para identificar soluciones SD-WAN, SWG, CASB y ZTNA a corto y largo plazo. Un enfoque en la estrategia de integración debería ser una parte clave de estas conversaciones porque los proveedores a menudo desarrollarán sus ofertas de SASE a través de la adquisición.

Impulse la seguridad desde arriba

SASE es una iniciativa cultural, no solo técnica. Su éxito se basa en la cooperación de múltiples equipos en toda la organización, muchos de los cuales pueden estar arraigados y ser ambivalentes sobre el cambio.

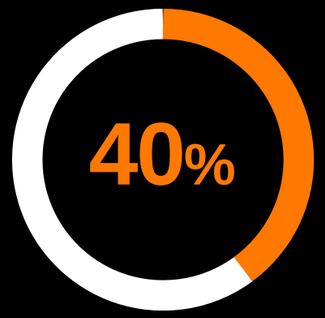
Las empresas que se toman en serio SASE deben estar dispuestas a impulsar la seguridad desde arriba, asegurando la aceptación de la alta dirección. Designe ejecutivos C-suite con el poder de impulsar el cambio y superar la resistencia política a nivel de equipo. Esté preparado para el largo plazo, ya que esta transición cultural requerirá tiempo, persistencia y paciencia.

Involucrar al CISO desde el inicio

SASE impulsa la seguridad en la infraestructura de la red, convirtiéndola en un componente fundamental de cada flujo de trabajo corporativo. Ahora más que nunca, el equipo de seguridad necesita un asiento en la mesa.

El CISO debe participar en todas las discusiones que involucren la adquisición o transformación de una nueva red o solución de seguridad de red, internamente y con proveedores y arquitectos principales. Este equipo debería ayudar a evaluar las ofertas y las hojas de ruta de cada proveedor.

Una estrategia de adopción de SASE



Gartner anticipa que el 40% de las empresas tendrán una estrategia SASE para 2024, pero hay un largo camino entre la estrategia y la realidad. Las empresas deben comenzar a prepararse ahora para un cambio arquitectónico y cultural tan amplio como SASE.

De hecho, muchos de ellos tienen pocas opciones porque la pandemia los ha forzado a adoptar algunos elementos de SASE, como el acceso a la red de confianza cero en respuesta a la necesidad de trabajar a distancia. Siguen algunos elementos a tener en cuenta a la hora de la adopción.

1 Haga el caso de negocios

Comience por presentar SASE entre los tomadores de decisiones clave . Esto implica tanto el rumbo estratégico a largo plazo como propuestas más reducidas e inmediatas como parte de un despliegue incremental .

2 Genere sinergia entre los equipos de seguridad y red

Los equipos de seguridad y redes a menudo trabajan en silos, pero cuando diseñan e implementan el modelo SASE, es necesario que tengan buen diálogo. Comience a generar sinergia entre estos grupos lo antes posible para facilitar el trabajo de integración en el futuro.

3 Evalúe el impacto operativo y organizacional en las redes y la seguridad

Al elaborar una propuesta de arquitectura a largo plazo para SASE, los equipos de diseño deben considerar el impacto operativo en sus sistemas.

4 Comience la transformación SD - WAN

SASE necesita una plataforma de red definida por software para la implementación de servicios basados en la nube perimetral. Esto implica pasar a una arquitectura SD - WAN, incluida la transición de MPLS a conexiones de Internet. Es crucial abordar esta etapa teniendo en cuenta los servicios de seguridad de red definidos por software, abarcando una solución de acceso remoto en el tejido SD - WAN en una etapa temprana para garantizar seguridad constante para los trabajadores remotos.

5 Migre los servicios de ciberseguridad del centro de datos heredado a la nube

Con una solución SD-WAN implementada, es hora de planificar la migración de los servicios de seguridad heredados on-premises a los POP shabilitados para la nube que se ejecutan en la red definida por software . Esto significa hacer la transición a un proveedor de seguridad en la nube.

6 Modifique la postura y el diseño de seguridad a acceso a la red zero-trust

Al realizar la migración a los servicios de seguridad basados en la nube hay que tener en cuenta el acceso a la red de confianza cero. Esto incluye la planificación del ingreso basado en la identidad a todas las aplicaciones. Desarrolle componentes que incluyan gestión de acceso e identidad y marcos de gestión del ciclo de vida de la identidad que respaldarán la transición al acceso basado en la identidad . Ahora también es un buen momento para considerar tecnologías complementarias como la autenticación multifactor y el control basado en dispositivos para proteger los dispositivos móviles administrados que acceden a las aplicaciones corporativas.

7 Desarrolle un marco de automatización

Con un tejido de seguridad de red definido por software , estará bien posicionado para impulsar nuevas eficiencias en su infraestructura de seguridad mediante la automatización. Invertir en la creación y el perfeccionamiento de un plano de control de seguridad y una red definida por software que constituirá la base de una operación de seguridad robusta y adaptable.

Sobre Orange Cyberdefense

Orange Cyberdefense es la unidad de negocio experta en ciberseguridad del Grupo Orange. Como proveedor de seguridad de referencia en Europa, nos esforzamos por construir una sociedad digital más segura.

Somos un proveedor de seguridad basado en la inteligencia y la investigación de amenazas que ofrece un abordaje sin precedentes a las amenazas actuales y emergentes.

Orange Cyberdefense conserva un historial de más de 25 años en seguridad de la información, más de 250 investigadores y analistas, 18 SOC, 11 CyberSOC y 4 CERT distribuidos en todo el mundo y soporte de ventas y servicios en 160 países. Nos enorgullece decir que podemos ofrecer protección global con experiencia local y ayudar a nuestros clientes durante todo el ciclo de vida de sus amenazas.

Twitter: @OrangeCyberDef

Fuentes:
1. IDC - https://www.idc.com/getdoc.jsp?containerId=prUS46934120 European Commission – https://ec.europa.eu/jrc/sites/jrcsh/files/jrc120945_policy_brief_-_covid_and_telework_final.pdf
2. IDC Webinar - Envisioning a Resilient Cloud Based Digital Infrastructure webinar April 2020
3. US Cybersecurity and Infrastructure Security Agencies - https://us-cert.cisa.gov/ncas/alerts/aa20-099a
4. IDC - https://www.idc.com/getdoc.jsp?containerId=prAP46737220#:~:text=IDC%20estimates%20data%20generated%20from,significant%20portion%20of%20this%20data

Orange
Cyberdefense

orange™