FORTINET
NSE Training Institute

NSE 2 SASE Scripts—Spanish Version

¡Hola! En esta clase, presentaremos el Secure Access Service Edge, o SASE, y explicaremos cómo ha evolucionado.

SASE es una tecnología que combina las capacidades de la red como servicio (NaaS) y de la seguridad como servicio (SECaaS). SASE se entrega mediante la nube con un modelo de consumo como servicio, a fin de proporcionar un acceso seguro a las redes empresariales actuales, ya sean distribuidas o híbridas.

La seguridad de red es la prioridad número uno para la mayoría de las organizaciones. Sin embargo, se han presentado nuevos desafíos. La velocidad y el carácter revolucionario de la innovación han dado como resultado:

- Un borde delgado en expansión, definido por pequeñas sucursales que están conectadas a la red principal.
- Un número cada vez mayor de usuarios externos a la red que tienen acceso al centro de datos principal.
- Desafíos en la experiencia de usuario para los usuarios externos a la red.
- Una superficie de ataque cada vez más amplia.
- Requisitos de cumplimiento normativo de distintos niveles.
- Amenazas cibernéticas cada vez más complejas.

A medida que los entornos de trabajo han ido evolucionando, también lo han hecho el comportamiento del usuario y los requisitos de protección de los dispositivos terminales. Los usuarios ya no acceden a la información desde una estación de trabajo dedicada dentro de un perímetro de red predefinido que se encuentra restringido a la oficina de una empresa. En cambio, lo hacen desde distintas ubicaciones, como el hogar, un avión o un hotel. También pueden acceder a la información desde diferentes dispositivos, como estaciones de trabajo de escritorio, computadoras portátiles, tabletas y dispositivos móviles. Además de esta complejidad propia de la red, está cada vez más extendida la práctica BYOD ("Traiga su propio dispositivo"), según la cual los usuarios acceden a los sistemas de la empresa mediante dispositivos personales que no forman parte de la infraestructura de la organización.

En la actualidad, las empresas requieren que los usuarios tengan un acceso inmediato, continuo y seguro a los datos y a los recursos en la red y en la nube, incluidas las aplicaciones críticas para la organización, cualquiera sea la ubicación, el dispositivo o el momento. Las empresas deben brindar este tipo de acceso de un modo ampliable y elástico que integre los sitios de red de borde delgado y los usuarios remotos en la infraestructura principal. También deben favorecer la optimización de las operaciones y la adopción de un modelo "as-a-service", es decir, basado en servicios.

La búsqueda de soluciones que satisfagan estos requisitos es todo un desafío.

Las razones de ello son claras.

En primer lugar, si bien las redes han evolucionado y admiten flujos de trabajo para usuarios y dispositivos terminales remotos, muchas soluciones de seguridad de red han quedado obsoletas y no son flexibles. Por esta razón, no pueden ampliarse hacia fuera del centro de datos para cubrir el perímetro de red ni, en consecuencia, la superficie de ataque cada vez más extensa. Con la llegada de las nuevas redes de borde delgado, este desafío es aún mayor.

En segundo lugar, estas soluciones de redes convergentes y de supervisión de la seguridad requieren que todo el tráfico, ya sea que provenga de ubicaciones en el borde delgado o de usuarios externos a la red, fluya a través del centro de datos principal para su inspección. Como resultado, se obtienen:

- costos elevados,
- una mayor complejidad,
- una gran exposición al riesgo,
- una mayor latencia y una experiencia de usuario de baja calidad cuando se accede a aplicaciones y datos basados en nubes múltiples.

Por último, el entorno de red de múltiples bordes que se utiliza en la actualidad puso de manifiesto las limitaciones de las soluciones basadas únicamente en una VPN. Estas no son compatibles con las políticas de seguridad, detección de amenazas y acceso de red de confianza cero que se implementan en las redes locales de las empresas. Las soluciones basadas únicamente en VPN no pueden ampliarse para admitir el número creciente de usuarios y dispositivos, por lo que la seguridad no es homogénea en todos los bordes.

Una nueva solución convergente que sea ampliable y elástica es necesaria para lograr un acceso a la red seguro y confiable, tanto para los usuarios como para los dispositivos endpoints. Una solución de este tipo debe ofrecer seguridad a muchas organizaciones híbridas, definidas por sistemas y usuarios distribuidos en la red de la empresa y en la red remota. SASE es esta solución.

Una solución de SASE proporciona capacidades de red **y de seguridad** integradas, e incluye lo siguiente:

- Intercambio de tráfico (peering), que permite establecer conexiones de red e intercambiar tráfico directamente a través de Internet, sin tener que pagar a un tercero.
- Un firewall físico de próxima generación NGFW, o un firewall como servicio basado en la nube, FWaaS , que incluyen capacidades de seguridad, como el sistema de prevención de intrusos, o IPS, antimalware, inspección SSL y sandbox.
- Un gateway seguro de web, que protege a los usuarios y dispositivos de amenazas de seguridad en línea mediante el filtrado de malware y la implementación de políticas de seguridad en Internet y de cumplimiento normativo.
- Zero Trust Access Network, o ZTNA, según el cual ningún dispositivo ni usuario es confiable de manera automática. Todo intento de acceder a un sistema, ya sea desde el interior o desde el exterior, es objetado y verificado antes de se conceda el permiso. Este tipo de conexión está integrada por varias tecnologías, incluida la autenticación multifactor, o MFA, el control de acceso seguro a la red, o NAC, y la implementación de políticas de acceso.
- Un sistema de prevención de pérdida de datos, o DLP, que impide que los usuarios finales muevan información clave hacia el exterior de la red. Estos sistemas informan acerca de la inspección del contenido de las aplicaciones de mensajería y correo electrónico que operan en la red.
- Un sistema de nombres de dominios, o DNS, que actúa como una agenda telefónica para Internet y proporciona un SASE con capacidades de detección de amenazas para analizar y evaluar los dominios peligrosos.

Esos servicios ofrecen lo siguiente:

- Rutas optimizadas para todos los usuarios y acceso a todas las nubes, lo que mejora el rendimiento y la agilidad.
- Seguridad homogénea para fuerzas de trabajo móviles.
- Seguridad homogénea para todos los bordes.
- Administración consolidada de las operaciones de seguridad y de red.

Si bien SASE es considerado una arquitectura basada en la nube, existen casos de uso comunes que pueden requerir la adopción combinada de algunas soluciones físicas y otras basadas en la nube. Para que SASE pueda ser implementado con éxito en este tipo de contextos, una conectividad segura con controles de acceso a la red debe extenderse desde la infraestructura WAN física hacia el borde de la nube. Por ejemplo, para dar acceso a SASE en una sucursal, puede que el servicio de SASE tenga que depender de dispositivos de red físicos, como repetidores inalámbricos (LTE o 5G), prolongadores de cable de red (Ethernet) o puntos de acceso Wi-Fi.

El objetivo de SASE es satisfacer las necesidades de acceso dinámico y seguro de las organizaciones actuales. Un servicio de SASE adecuado permite a las empresas ampliar las características de seguridad y de redes de tipo empresarial a los siguientes casos:

- El borde de la nube, donde usuarios remotos y externos acceden a la red.
- El borde delgado, por ejemplo, pequeñas sucursales.

El servicio SASE de Fortinet basado en la nube se llama FortiSASE™.

Gracias por su tiempo, y no olvide responder las preguntas a continuación.