ESPACIO PARA EL LOGOTIPO DEL SOCIO

10 GRANDES capacidades que debe buscar en un proveedor de SASE

En un mundo ideal, podríamos realizar la transición a una arquitectura de SASE con solo presionar un botón y, de esa forma, migrar toda la red a un entorno seguro en la nube. Si bien ese no es el mundo en el que vivimos, las transiciones no tienen por qué ser complicadas o agobiantes.

Para poder adoptar una arquitectura de SASE de forma eficaz, lo primero que debe hacer es buscar al proveedor adecuado para el proceso. El proveedor de SASE debe poner en práctica su experiencia y brindarle ayuda para que aproveche sus inversiones actuales y para que adopte un modelo de seguridad basado en la nube de manera sencilla y segura y al ritmo que mejor se ajuste a su empresa.

1 ADMINISTRACIÓN DE POLÍTICAS UNIFICADA

Gestione la seguridad en todo lugar, ya sea de forma local o en la nube, desde una única interfaz de usuario.

La administración de políticas unificada garantiza una experiencia segura, ya que permite que las políticas sigan a los usuarios, los dispositivos y las aplicaciones adonde sea que vayan.

2 PROTECCIÓN RÁPIDA Y EFICAZ CONTRA AMENAZAS AVANZADAS

Protéjase de las amenazas invisibles y desconocidas, incluso aunque estén cifradas.

Encuentre un servicio basado en la nube que identifique el software malicioso de forma estática y dinámica y que bloquee incluso las amenazas más sofisticadas y evasivas a los pocos segundos de haberlas detectado.

3 RESILIENCIA Y ESCALABILIDAD

Amplíe el servicio a entornos de seguridad físicos, virtuales y basados en la nube de forma fácil y eficaz.

Es fundamental contar con una simplicidad operativa y un sistema de seguridad a gran escala que sean invisibles para los usuarios finales y que nunca afecten su experiencia de modo negativo.

4 ARQUITECTURA DE PILA ÚNICA CON UN MARCO DE POLÍTICA ÚNICA

Saque provecho de sus inversiones actuales y úselas como trampolín para acceder a servicios de seguridad en la nube que son indispensables para su empresa.

Cree las políticas una sola vez y aplíquelas en cualquier lugar gracias a la administración unificada, que abarca el acceso basado en los usuarios y las aplicaciones, los sistemas de prevención de intrusiones (IPS), la protección contra el software malicioso y el acceso web seguro, todo enmarcado por una única política.

5 UN MISMO NIVEL DE SEGURIDAD PARA SU PLANTILLA DISTRIBUIDA

Proporcione a los trabajadores remotos acceso seguro a las aplicaciones y los recursos que necesitan para cumplir con sus responsabilidades de forma eficaz.

Es importante contar con políticas de seguridad coherentes que sigan a los usuarios, los dispositivos y las aplicaciones sin que sea necesario duplicar o recrear conjuntos de reglas.

6 COMPATIBILIDAD CON ENTORNOS HÍBRIDOS

El proveedor de SASE no debería preocuparse por si su infraestructura está basada en la nube, si está instalada de forma local o si corresponde a un sistema híbrido, sino que debería poder abordar todo tipo de entornos.

El proveedor debe poder brindarle ayuda para que la transición a la arquitectura de SASE sea sencilla y segura y para que la implemente al ritmo que sea más adecuado para su empresa.

7 ÚNICA FUENTE DE IDENTIDAD

Se integra a la perfección con cualquier proveedor de soluciones de identidad del mercado.

Debe poder elegir la solución de identidad que mejor se adapte a sus necesidades empresariales, y no a las del proveedor de SASE.

8 SEGMENTACIÓN DINÁMICA DE LOS USUARIOS

Asegúrese de que los usuarios reciban protección estén donde estén.

Incorpore políticas que sigan a los usuarios y ofrezca un control de acceso automatizado y basado en el riesgo por medio de una política detallada que ve al acceso externo como una amenaza potencial y lo bloquea, lo que, a su vez, reduce la superficie de ataque en el borde.

9 EFICACIA DEMOSTRADA EN MATERIA DE SEGURIDAD

Haga su propia investigación y encuentre un proveedor de SASE que realmente haya demostrado ser eficaz en términos de seguridad.

El proveedor debe ofrecer una protección efectiva contra las amenazas, incluidos el ransomware, los botnets, la tunelización de DNS y los exploits del lado del cliente y del servidor. Además, tiene que adoptar medidas proactivas con respecto a las amenazas y contener los ataques en sus entornos locales y en la nube como servicio.

10 TRANSICIÓN SENCILLA Y PERSONALIZADA A UN SISTEMA DE SEGURIDAD EN LA NUBE

Nadie debería obligarlo a migrar a una arquitectura de SASE si aún no está en condiciones de hacerlo.

Realice la transición a una arquitectura de seguridad en la nube de manera sencilla y a su propio ritmo desde la misma IU de administración, que cuenta con políticas unificadas y asistentes de implementación intuitivos. Orqueste, aprovisione y gestione los servicios de políticas de forma sencilla y eficaz sin importar dónde se encuentren.

11 VENTAJA ADICIONAL: GARANTÍA DE SEGURIDAD

Realice cambios con confianza en las reglas de las políticas y asegúrese de que se implementen.

Tanto si son reglas para políticas tradicionales de firewall o políticas suministradas como servicio, es fundamental que se implementen en el orden correcto para que sean eficaces. El proveedor de SASE debe ayudar a que el equipo de TI comprenda bien estos conjuntos de reglas e identificar de forma automática las reglas duplicadas y similares antes de que se implementen.

Si bien el proceso de SASE es distinto para cada organización, en definitiva es usted quien decide cómo diseñar, desarrollar y mantener esta nueva arquitectura para optimizar la experiencia de los usuarios, los servicios y el acceso permanente a los datos. Independientemente de la opción que seleccione, es fundamental que el proveedor lo ayude a implementar el modelo de SASE y lo guíe a lo largo de todo el proceso.

Sede corporativa y de ventas

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089 EE. UU.

Teléfono: 888 JUNIPER

(+1 888 586 4737)

o +1 408 745 2000

Fax: +1 408 745 2100

www.juniper.net/mx/es

Sedes en APAC y EMEA

Juniper Networks International B.V.

Boeing Avenue 240

1119 PZ Schiphol-Rijk

Ámsterdam, Países Bajos

Teléfono: +31 0 207 125 700

Fax: +31 0 207 125 701

Juniper Networks | Driven by Experience™

3050168-001-ES Agosto de 2023