¿Qué es un perímetro definido por Software?

¿Qué es un perímetro definido por Software? Un perímetro definido por software es un enfoque de seguridad informática que micro-segmenta el acceso a la red. Establece conexiones directas entre los usuarios y los recursos a los que acceden. Un perímetro definido por software se centra en tres pilares principales:

Cero confianza

Utiliza la microsegmentación para instalar el axioma de menor privilegio en una red. Elimina la superficie de ataque.

Centrado en la identidad

Opera en torno a la identidad de un usuario y no a la dirección IP de un usuario.

Diseñado para la nube

Opera en redes en la nube y proporciona seguridad expandible. El software SDP autentica y autoriza todos los puntos finales que intentan acceder a una infraestructura particular. También hace que las redes no autorizadas sean inaccesibles. Esto reduce la superficie de ataque al ocultar los recursos de la red a usuarios no autenticados o no autorizados.

Definición de seguridad del perímetro de red

La seguridad de la red se refiere a un límite entre un lado local y privado de propiedad y administración de una red.

¿Cuáles son los usos de los SDP?

Los SDP pueden autenticar PC y portátiles, así como dispositivos móviles y dispositivos IoT (Internet de las cosas). Los SDP restringen las conexiones de dispositivos no válidos o no autorizados.

Los SDP impiden el acceso amplio a la red

Los SDP impiden que las entidades individuales no puedan acceder a subredes o segmentos de red amplios. Por lo tanto, los dispositivos solo pueden acceder a hosts y servicios específicos que son permisos de políticas. Esto reduce la superficie de ataque de la red. También evita el escaneo de vulnerabilidades por software malicioso y usuarios maliciosos.

Los SDP admiten una política más amplia basada en el riesgo

SDP otorga acceso según los criterios de riesgo especificados. Estos incluyen nuevos softwares, inteligencia de amenazas y brotes de malware.

Los SDP pueden conectar cualquier cosa

La seguridad definida por software permite la conectividad a los recursos de TI requeridos por los miembros del personal.

También elimina los costos de hardware de montaje y los onerosos requisitos de administración.

Los SDP permiten el control de acceso, servicios y aplicaciones

Los SDP son expertos en controlar qué dispositivos y aplicaciones pueden acceder a un servicio determinado. Esto reduce la superficie de ataque y evita que el malware malicioso o los usuarios se conecten a los recursos.

¿Cómo funciona un perímetro definido por software?

El primer componente necesario para acceder a un recurso (entidad) o una aplicación es un cliente. La entidad no tiene entrada de DNS, que es una característica de seguridad significativa. Por lo tanto, permanece oculto y no tiene acceso directo. Por el contrario, el cliente recibe un medio de comunicación sin agente o habilitado para SDP con segundos componentes.

Este es un controlador SDP que arbitra la conectividad entre los usuarios y los dispositivos IoT. El controlador contiene una lista limitada de usuarios autorizados. También tiene una lista de dispositivos registrados.

El controlador comprende el estado de seguridad del dispositivo y quién es el usuario al comunicarse con el cliente. Esta información luego se verifica al compararla con un control de acceso basado en roles. Después de la verificación, se intercambian los certificados de seguridad.

El controlador luego le informa a la puerta de enlace que un cliente enviará una comunicación autenticada. La puerta de enlace y el cliente establecen una comunicación segura.

La arquitectura definida por software crea un método de acceso

estricto para recursos y aplicaciones particulares. También hay una superficie de amenaza reducida porque las entidades objetivo permanecen ocultas y el controlador debe verificar a los usuarios. El firewall definido por software elimina el robo de credenciales, los ataques internos a la red, el malware y los ataques de intermediarios.

Casos de uso de perímetro diseñado por software

A continuación se presentan algunos casos de uso de SDP:

DevOps

SDP proporciona acceso seguro que permite a los usuarios de DevOps aislar cargas de trabajo y acceder a recursos clave.

Segmentación de red o aplicación

El grupo de seguridad perimetral minimiza la superficie de ataque y la propagación de malware dentro de entornos de nube y centros de datos.

Acceso BYOD simplificado

SDP proporciona acceso seguro, fácil y directo a aplicaciones en la nube. También permite un fácil acceso a los recursos desde el dispositivo preferido de un usuario.

Acceso de usuario privilegiado y de terceros

Los socios de seguridad perimetral permiten el acceso privilegiado y de terceros a los sistemas desde cualquier ubicación.

Marco SDP

La tecnología SDP permite un perímetro seguro mediante el uso de políticas que aíslan el servicio de las redes inseguras. El SDP de CSA hace tres cosas:

Proporciona una red con espacio de aire, aprovisionado y bajo demanda.
Segmenta los recursos de red en perímetros de red definidos.
Autentica dispositivos y usuarios antes de autorizar la combinación dispositivo / usuario antes de conectarse a un servicio aislado. El marco SDP garantiza que los dispositivos y usuarios no autorizados no puedan conectarse a servicios aislados.
Una vez que se completa la autenticación, los dispositivos confiables reciben una conexión única y momentánea a una infraestructura de red. La gestión definida por software permite a las empresas optimizar las operaciones relacionadas con la seguridad de las aplicaciones y la autenticación de usuarios.

Modelos de implementación de SDP

Los modelos de implementación de SDP se centran en cómo

estructuran las interacciones entre puertas de enlace, servidores y clientes. Los principales enfoques adoptados al implementar la tecnología SDP incluyen:

Implementación de cliente a puerta de enlace

La implementación de cliente a puerta de enlace coloca servidores detrás de un host de aceptación. Esto sirve como puerta de enlace entre los clientes y los servidores protegidos. Client to Gateway también se implementa dentro de una red SDP para minimizar los ataques de movimiento lateral.

Los ataques de movimiento lateral incluyen exploits de vulnerabilidad de aplicaciones, escaneo de servidores y ataques de hombre en el medio. Client to Gateway también se implementa en línea para mitigar los ataques y aislar a los usuarios protegidos de los usuarios ilegales.

Implementación de cliente a servidor

La implementación del cliente al servidor y la implementación del cliente a la puerta de enlace son similares. La única diferencia es que el servidor protegido por el SDP en la implementación de cliente a servidor es el sistema que ejecuta el host de aceptación. La elección entre la implementación de Cliente a Servidor y las implementaciones de Cliente a Puerta de Enlace depende de varios factores. Éstos incluyen:

La elasticidad de los servidores,

La adaptabilidad de los servidores en la nube definidos por software para cambiar,
Y la cantidad de servidores necesarios para salvaguardar el SDP.

Despliegue de cliente a servidor a cliente

La implementación de Cliente a Servidor a Cliente depende de una relación P2P (punto a punto). Los clientes pueden usar la relación P2P para aplicaciones, incluidas videoconferencias, chat y telefonía IP. En esta implementación, el SDP oscurece las direcciones IP de los clientes que se conectan. El servidor actúa como intermediario para los clientes.

Implementación de servidor a servidor

La implementación de servidor a servidor utiliza servidores que:

Proporcionar API (interfaz de programación de aplicaciones) a través de Internet,
Tener una alta capacidad de protección contra dispositivos y usuarios no autorizados en la red,
Incluya un servicio SOAP (Protocolo simple de acceso a objetos) simple ,
Incluya un RPC (Llamada a procedimiento remoto) y
Incluya un servicio REST (Representational State Transfer).
La implementación de servidor a servidor utiliza servidores

que ofrecen cualquiera de estas aplicaciones para comunicarse entre el host iniciador y el host aceptante.

En la sociedad contemporánea, hay deficiencias en los diseños perimetrales actualizados. Las empresas han estado exponiendo sus servicios, incluidas las API, RDP y HTTP / S. Incluso con capas adicionales de seguridad; los piratas informáticos aún pueden derribar o infiltrarse en los servicios a través de ataques de seguridad.

Los SDP son capaces de prevenir tales ataques al evitar el acceso no autorizado. Maximizan la seguridad del usuario al mejorar la seguridad a través de su principal centro de tecnología. Los SDP también ocultan los servicios en línea hasta que sea necesario permitir que los usuarios accedan al servicio.

Consultara también:Copia de seguridad, restauración y recuperación de Bare Metal: 7 cosas que los profesionales de TI deben saber; ¿Por qué es importante la seguridad del sitio web?; ¿Qué es la seguridad web? Definición, significado, concepto