Transformación segura: sustitución de redes VPN de acceso remoto por Prisma Access

Durante años, las VPN de acceso remoto han sido un elemento fundamental de las redes empresariales y, de hecho, para mucha gente «acceso remoto» y «VPN» son sinónimos. Sin embargo, las empresas están adoptando rápidamente aplicaciones en la nube que están cambiando los requisitos de la seguridad y las redes. Los equipos de redes y seguridad están preguntando cómo proteger el acceso a todas las aplicaciones, no solo a las que están alojadas en el centro de datos.

En vista de estos nuevos requisitos, ¿siguen siendo relevantes las VPN de acceso remoto? ¿O ha llegado el momento de reevaluar el papel del acceso remoto y utilizar una arquitectura mejor?

Limitaciones del acceso remoto

El acceso remoto tiene un objetivo fundamental: servir de puerta de enlace para que los usuarios ubicados fuera del cortafuegos perimetral puedan acceder a los recursos del centro de datos.

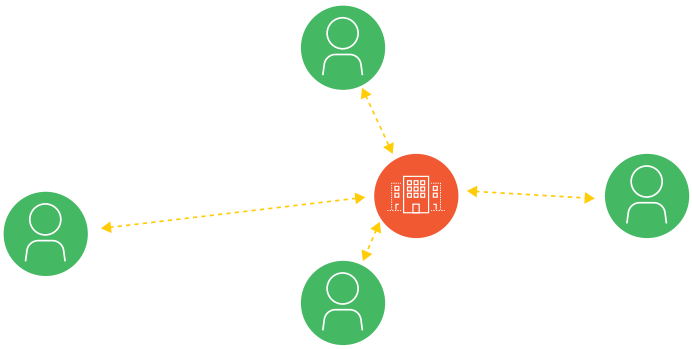

Figura 1: Arquitectura de VPN tradicional de acceso remoto

Una VPN de acceso remoto es una arquitectura radial, con los usuarios situados en radios de diversa longitud, según la distancia que los separa del núcleo (el centro de datos interno). Aunque la distancia degrada el rendimiento e introduce problemas de latencia, sigue siendo la mejor arquitectura para las aplicaciones del centro de datos, ya que el objetivo es llegar al centro de datos interno.

Este modelo no sirve si en el entorno se mezclan diversas aplicaciones en la nube. En una VPN de acceso remoto, el tráfico siempre va primero a la puerta de enlace VPN, aunque la aplicación esté alojada en la nube. El proceso es el siguiente: el tráfico va a la puerta de enlace VPN de la sede central, luego sale del cortafuegos perimetral corporativo a Internet y la respuesta de la aplicación vuelve a la sede central antes de enviarse al usuario. El tráfico sigue un camino de ida y vuelta similar al de un trombón: para llegar a una ubicación con acceso a Internet, tiene que hacer antes un largo viaje a la sede central. Aunque este método tiene sentido desde el punto de vista de la seguridad (siempre que la sede central cuente con inspección del tráfico en el perímetro de Internet), no ayuda en absoluto a optimizar la red.

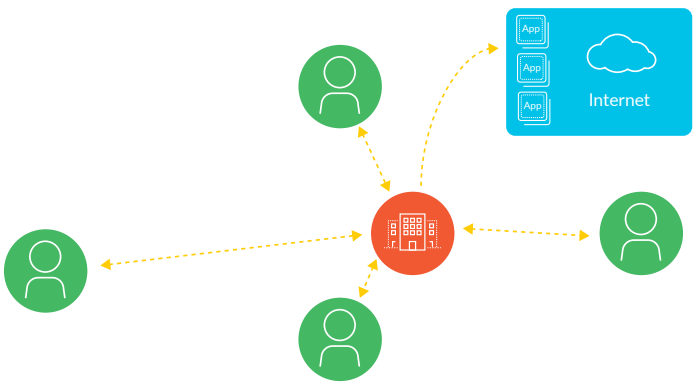

Figura 2: VPN tradicional de acceso remoto, donde el tráfico se desvía a la sede central mediante una red de retorno para luego redireccionarlo a la nube

Utilizar una VPN de acceso remoto para conectarse a las aplicaciones alojadas en la nube puede empeorar la experiencia de los usuarios. Estos, por lo tanto, tienden a evitar este método siempre que sea posible. En cambio, se conectan para acceder al centro de datos interno y permanecen desconectados el resto del tiempo, lo que causa problemas en cuanto a la aplicación de las políticas de seguridad. Cuando los usuarios no están conectados, la organización pierde visibilidad sobre el uso de las aplicaciones, no tiene manera de controlar el acceso a las aplicaciones no autorizadas y tampoco puede aplicar medidas de seguridad.

Añadir más puertas de enlace VPN no soluciona el problema. En el contexto de las VPN de acceso remoto, una puerta de enlace no es más que el final del túnel, donde el tráfico no se somete a inspección alguna. Aunque se implementasen más puertas de enlace VPN, no podrían inspeccionar el tráfico sin más medidas de seguridad.

Soluciones poco satisfactorias

Para compensar los problemas de red que causan las VPN de acceso remoto, las organizaciones suelen optar por soluciones parciales que acaban afectando negativamente a la seguridad.

- **Túnel iniciado por el usuario:** otro modelo habitual de VPN de acceso remoto permite a los usuarios iniciar el túnel cuando lo necesiten para acceder al centro de datos interno. Por lo general, se conectan un rato para usar una determinada aplicación y se desconectan al terminar el trabajo. Cuando no están conectados, de nuevo pueden acceder directamente a Internet sin que se inspeccione el tráfico.
- **VPN de túnel dividido:** otra forma de implementar las VPN de acceso remoto, pero no por habitual menos peligrosa, es configurar un túnel dividido. Con una configuración de este tipo, el tráfico dirigido al dominio corporativo pasa por el túnel VPN, mientras que todo lo demás va directamente a Internet. Pese a la reducción de la latencia del tráfico de Internet, hay un claro inconveniente: el tráfico de Internet y de la nube no se inspecciona en absoluto.
- **Proxy web:** muchas organizaciones han probado a proteger la red de otras maneras cuando el usuario no está conectado a la VPN, como utilizar un proxy para el navegador web. Por definición, sin embargo, un proxy web no inspecciona el tráfico de red de forma exhaustiva. Lo que es peor, el tráfico que sí inspecciona no tiene nada que ver con el inspeccionado en la sede central y sus resultados varían según dónde esté el usuario.

Con la rápida generalización de los trabajadores itinerantes y las aplicaciones basadas en la nube, las organizaciones están viendo que sus VPN de acceso remoto no están optimizadas para la nube ni son seguras. Hace falta un nuevo enfoque que tenga en cuenta la mezcla de aplicaciones que se usa en la actualidad.

Una arquitectura moderna para los trabajadores itinerantes

Un trabajador itinerante necesita acceder al centro de datos, a Internet y a las aplicaciones alojadas en los entornos de nube pública, privada e híbrida. En todos estos casos, una arquitectura adecuada debería mejorar el acceso, estén donde estén las aplicaciones y quienes las usan. Prisma™ Access es una infraestructura de seguridad basada en la nube que permite conectar a los usuarios con una puerta de enlace en la nube próxima a ellos. Además de ofrecer acceso seguro a todas las aplicaciones, muestra e inspecciona de forma exhaustiva el tráfico registrado en todos los puertos y protocolos.

En el caso de los dispositivos móviles gestionados

Los dispositivos gestionados de los usuarios (ordenadores portátiles, teléfonos móviles o tabletas) tienen instalada la aplicación GlobalProtect™. La aplicación se conecta a Prisma Access automáticamente siempre que haya acceso a Internet, sin que intervenga el usuario.

Prisma Access conecta las aplicaciones alojadas en distintas ubicaciones a través de su capa de conectividad para que los usuarios tengan acceso a cualquier aplicación, ya esté en la nube o en el centro de datos. La capa de conectividad se ocupa de garantizar un acceso seguro (mediante políticas basadas en las tecnologías App-ID™ y User-ID™) a la nube pública, el software como servicio y las aplicaciones del centro de datos.

Figura 3: Protección basada en la nube para todos los usuarios, estén donde estén

Prisma Access ofrece protección mediante la capa del servicio de seguridad para garantizar la seguridad que siempre brinda la plataforma Security Operating Platform® de Palo Alto Networks: protección frente al malware conocido y desconocido, los exploits, el tráfico de comando y control, y los ataques basados en credenciales.

En el caso de los dispositivos móviles no gestionados o personales

Puede implementar Prisma Access e integrarlo con un sistema de gestión de dispositivos móviles (MDM, por sus siglas en inglés) que permita utilizar dispositivos personales. Esta integración habilita, además, otras funciones, como una VPN para cada aplicación. Los usuarios con dispositivos no gestionados (p. ej., contratistas o empleados con derecho a usar dispositivos personales) pueden utilizar una VPN sin cliente para acceder al centro de datos de forma remota. De este modo, es posible acceder de forma segura a las aplicaciones SaaS desde dispositivos no gestionados, gracias a la integración de un proxy SAML con protección lineal.

Creado para el futuro

Si está reevaluando su implementación de VPN de acceso remoto, tal vez le convenga migrar a una arquitectura diseñada para ofrecer acceso seguro a todas las aplicaciones y evitar que los ciberataques consigan sus objetivos. Con Prisma Access, su organización podrá dejar atrás las limitaciones de las VPN de acceso remoto tradicionales y dar facilidades a los usuarios para trabajar con todas las aplicaciones que necesiten.

Para obtener más información, visite paloaltonetworks.es/prisma/access.

paloalto® NETWORKS

Oval Tower, De Entrée 99 - 197
1101HE Ámsterdam
Países Bajos

Tel.: +31 20 888 1883

www.paloaltonetworks.es

© 2020 Palo Alto Networks, Inc. Palo Alto Networks es una marca comercial registrada de Palo Alto Networks. Hay una lista de nuestras marcas comerciales disponible en https://www.paloaltonetworks.com/company/trademarks.html. El resto de las marcas mencionadas en este documento pueden ser marcas comerciales de sus respectivas empresas. secure-transformation-replacing-vpn-with-prisma-access-sb-100820-es