Libro electrónico

Los 6 casos de uso más convincentes

para la sustitución completa de la VPN heredada

netskope

Introducción

La infraestructura de VPN heredada para el acceso remoto ha sido durante mucho tiempo un lastre para la seguridad. Su amplia conectividad de red atrae a los atacantes y permite movimientos laterales no autorizados. Obligar a los usuarios remotos a redirigir el tráfico no local a través de la VPN para volver a Internet da lugar a una mala experiencia de usuario y conlleva un elevado coste y complejidad de enrutamiento.

Para las empresas que planean modernizar la conectividad para los trabajadores híbridos, el ZTNA es la alternativa moderna a la VPN heredada para el acceso remoto. Pero no todas las soluciones ZTNA permiten sustituir completamente las VPN.

Para pasar con éxito de una VPN heredada al ZTNA, nuestra recomendación es identificar y priorizar los casos de uso clave a la hora de planificar una migración completa. Una planificación útil, combinada con las inversiones en tecnología adecuadas, permitirá a los equipos cumplir por fin la promesa de la retirada total de la VPN.

1. Capacitar a los trabajadores híbridos

Dado que la mayoría de los empleados se inclinan ahora por un modelo de trabajo híbrido, las soluciones de VPN heredadas resultan inadecuadas para abordar los retos esenciales de seguridad y conectividad necesarios para capacitar a los trabajadores.

La VPN para el acceso remoto proporciona poca visibilidad de las actividades relacionadas con las aplicaciones, tiene problemas de latencia y rendimiento debido al redireccionamiento del tráfico, y proporciona un amplio acceso a nivel de red a las aplicaciones de la red a usuarios autenticados, ampliando la superficie de ataque debido a los movimientos laterales sin restricciones. Además, los concentradores VPN con vulnerabilidades sin parchear actúan como importantes vectores de ataque para los ciberataques.

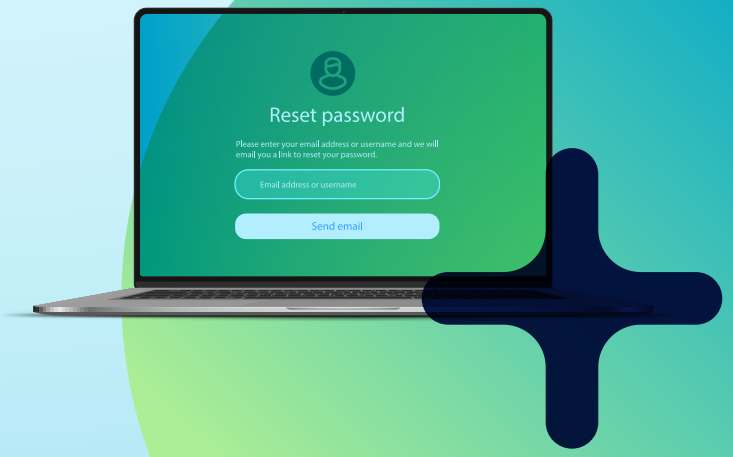
Al pasar de las soluciones VPN heredadas para el acceso remoto a una solución ZTNA como Netskope One Private Access, las organizaciones podrán hacer frente a los riesgos de seguridad relacionados con las VPN al permitir un acceso menos privilegiado a las aplicaciones privadas según la identidad y el contexto, minimizando al mismo tiempo los movimientos laterales no autorizados. Netskope One Private Access ofrece visibilidad en tiempo real del tráfico detallado de las aplicaciones y de las actividades de los usuarios, y permite una aplicación coherente de las políticas para los empleados que se conectan desde cualquier ubicación, ya sea remota o local. Además, la solución puede establecer una conectividad segura previa al inicio de sesión, facilitando la incorporación segura de nuevos dispositivos y el restablecimiento de contraseñas para los trabajadores remotos, y garantizando que solo los dispositivos autorizados tengan acceso a recursos internos críticos, como los servicios de directorio.

Los empleados pierden 11 horas al año restableciendo contraseñas[1]

CONSEJOS PARA LA IMPLEMENTACIÓN:

Un inventario de las implementaciones de VPN es una buena manera de empezar a actualizar su infraestructura. Este debe incluir:

- **Cuántas instancias de servicios VPN para el acceso remoto gestiona en la actualidad**
- **Qué tráfico de aplicaciones viaja a través de estas VPN de acceso remoto**
- **Usuarios designados con acceso mediante la VPN a estas aplicaciones**



[1]Business Reporter, «How much time does your organisation spend on managing passwords?», 7 de septiembre de 2022. https://www.independent.co.uk/news/business/business-reporter/time-organisation-managing-passwords-b2161856.html

2. Acelerar la migración a la nube

La transformación digital ha alcanzado un punto de inflexión: Cada vez más cargas de trabajo se alojan en nubes públicas en lugar de en centros de datos privados. Como resultado, la conectividad a IaaS, tanto para usuarios locales como remotos, ha sido una de las principales preocupaciones de las organizaciones a la hora de planificar su estrategia e implementación de la nube. En una infraestructura típica de VPN para el acceso remoto, el tráfico de usuario se enruta a través del centro de datos privado y luego se conecta a las nubes IaaS utilizando MPLS u otros túneles como AWS Direct Connect o Azure ExpressRoute. El redireccionamiento del tráfico no solo perjudica la experiencia del usuario y aumenta los gastos de infraestructura, sino que también requiere un enrutamiento complejo de la red.

Como alternativa moderna a las VPN heredadas para el acceso remoto, Netskope permite una conectividad eficaz a la nube pública sin necesidad de hacer un giro de «horquilla». La conexión es segura, flexible y altamente ampliable. Netskope One Private Access ayuda a proteger los datos y recursos con un control de acceso a nivel de aplicación basado en la identidad del usuario y la postura de seguridad del dispositivo. Al utilizar la conectividad lógica en lugar de la basada en IP, se agilizan drásticamente las operaciones de la nube y la red, permitiendo la automatización al mismo tiempo que se elimina el redireccionamiento del tráfico.

CONSEJOS PARA LA IMPLEMENTACIÓN:

Las organizaciones que busquen sustituir las VPN para el acceso remoto también deberían buscar instancias de VPN en la nube, como AWS Client VPN o Azure VPN Gateway. Deben aprovechar las herramientas de automatización, como los módulos Terraform, para automatizar la implementación, la configuración y la ampliación de los editores de Netskope One Private Access que se ejecutan en EC2 y otros entornos de nube.

3. Facilitar el acceso a los dispositivos no gestionados (cuando tenga sentido)

Las organizaciones necesitan conceder a los contratistas externos, proveedores de servicios y socios un acceso seguro a los recursos corporativos. Al mismo tiempo, los empleados también exigen un acceso fluido a los recursos privados a través de sus dispositivos personales. Esto lleva al reto de facilitar el acceso de dispositivos no gestionados sin el riesgo de exponer los recursos en la Internet pública o la DMZ. Exigir un software cliente especial puede no ser factible, ya que los usuarios pueden ser reacios a instalar software en sus dispositivos personales. Conceder acceso mediante la VPN a dispositivos no gestionados puede dar lugar a un acceso excesivo.

Puede proporcionar de forma segura acceso a dispositivos no gestionados para usuarios externos y BYOD de empleados sin los riesgos asociados a la VPN, la DMZ o la exposición de recursos a la Internet pública. Netskope One Private Access admite la implementación sin cliente para dispositivos no gestionados, proporcionando un acceso seguro Zero Trust a aplicaciones privadas, alojadas en las instalaciones o en la nube.

La implementación de ZTNA sin cliente permite un acceso sin fricciones basado en navegador a través de una arquitectura de proxy inverso que se integra con proveedores de identidad (IdP) para autenticar a los usuarios que intentan acceder a aplicaciones privadas. Aprovechando los mismos controles DLP de la plataforma Netskope One SSE, las organizaciones pueden mantener una visibilidad granular y una política de protección de datos coherente en todos los dispositivos, gestionados y no gestionados.

Por término medio, un empleado utiliza **2,5 dispositivos en el trabajo**, lo que incluye dispositivos no corporativos, como ordenadores portátiles personales, teléfonos inteligentes y tabletas.[2]

[2]Zippia. «26 Surprising BYOD Statistics [2023]: BYOD Trends In The Workplace» Zippia.com. 17 de octubre de 2022. https://www.zippia.com/advice/byod-statistics/

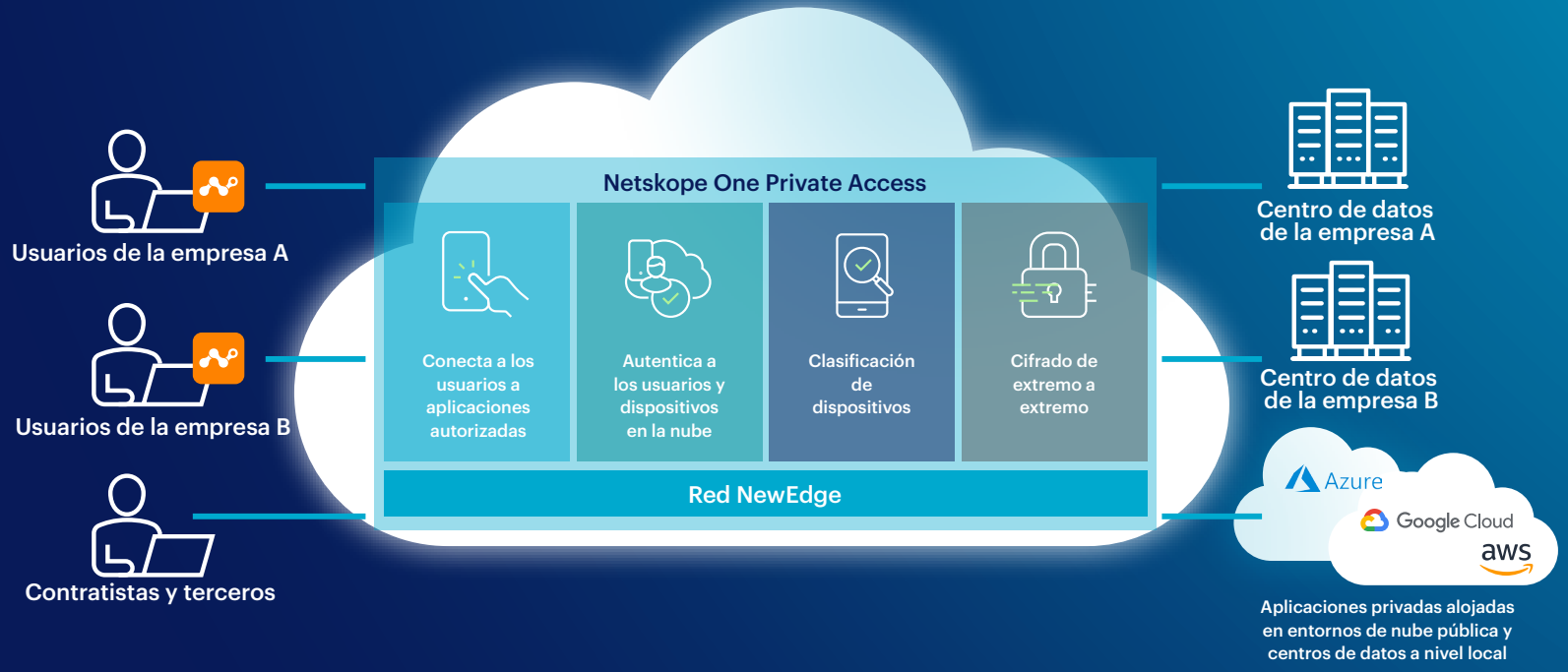
4. Acelerar la integración de FyA

Las actividades de fusiones y adquisiciones (FyA) son acontecimientos de ritmo rápido en los que hay mucho en juego, y el tiempo apremia. Para los equipos de TI, redes y seguridad, las FyA presentan un conjunto único de desafíos. El éxito de las FyA depende de la rapidez con que pueda completarse la integración de las dos empresas.

Los equipos de TI se enfrentan al reto de ofrecer acceso desde el primer día, conectando a usuarios de ambas entidades a aplicaciones internas de misión crítica y garantizando al mismo tiempo la seguridad de los datos sensibles. Los métodos tradicionales de fusión de dos redes son un proceso costoso, largo y complejo que a menudo provoca conflictos de IP y exige renumerar las direcciones. A menudo, las reglas del cortafuegos no pueden ofrecer un control de acceso granular, lo que hace que ambas redes sean vulnerables.

Netskope One Private Access, que se ofrece como una única solución, integra las funciones ZTNA/SD-WAN en un único cliente de punto de conexión ligero, lo que permite la retirada completa –y no solo la sustitución parcial– de las VPN para el acceso remoto para todos los casos de uso relacionados con el acceso a aplicaciones relevantes. Un cliente SASE unificado dirige automáticamente el tráfico de los usuarios a sus destinos, ya sean aplicaciones en la nube, aplicaciones privadas, IaaS o web. Netskope One Private Access permite a las organizaciones captar rápidamente valor empresarial durante las actividades de FyA conectando a empleados, contratistas y asesores a recursos esenciales desde el primer día, incluso para las aplicaciones heredadas. Esta solución elimina la necesidad de configurar la VPN y fusionar las redes, lo que permite a las empresas iniciar inmediatamente la integración de forma segura. El acceso se concede en función de criterios de confianza adaptativos, teniendo en cuenta la identidad del usuario, la seguridad del dispositivo y otros factores contextuales. Al proporcionar acceso selectivo a las aplicaciones y los datos,

Netskope One Private Access reduce el riesgo de movimientos laterales y la exposición de información confidencial.



Proporcione acceso desde el primer día a los recursos internos sin la complejidad de combinar las redes, configurar la VPN de un centro a otro y las reglas de cortafuegos.

5. Compatibilidad con los centros de contacto remotos

Hay **1,8 millones** de empleados de centros de llamadas en todo el mundo y solo en los Estados Unidos el 52"% de estos centros emplean agentes remotos.[3] Estos agentes son representantes del servicio de atención al cliente, agentes de reservas de viajes, asesores sanitarios y otras funciones. Aunque muchos centros de llamadas se están actualizando a las comunicaciones unificadas como servicio (UCaaS) basadas en la nube, muchas organizaciones siguen utilizando VoIP alojada en las instalaciones y, a menudo, enrutan las llamadas a través de VPN de acceso remoto. Para los empleados de los centros de llamadas remotos, la calidad de la VoIP puede ser impredecible si se confía en las VPN. Suelen estar saturados, lo que contribuye a aumentar la fluctuación y latencia de las llamadas VoIP, que pueden resultar frustrantes para las personas a ambos lados de la línea.

Hasta la fecha, la mayoría de los ZTNA en la nube no son compatibles con los sistemas VoIP alojados en las instalaciones, lo que obliga a las organizaciones a mantener tanto la infraestructura ZTNA como la VPN.

El 52%
de los centros de llamadas solo en EE. UU. emplean agentes remotos

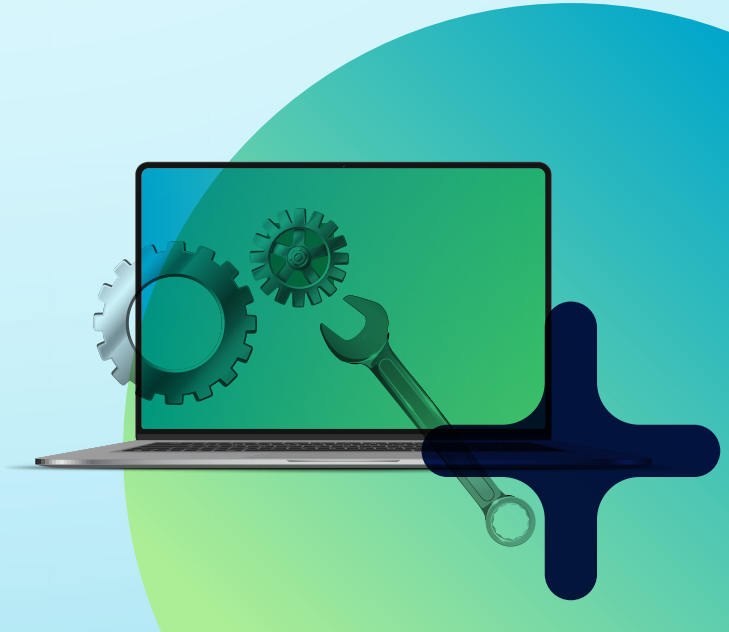
Netskope One Private Access ofrece funciones convergentes de ZTNA y SD-WAN en una única solución. Gracias a la dirección dinámica del tráfico y a la calidad de servicio basada en el contexto, se mejora la productividad de los empleados de los centros de llamadas remotos con una experiencia de aplicación de voz y vídeo garantizada, al tiempo que se mejora la postura de seguridad con un acceso Zero Trust a todos los recursos internos.

[3]Fuente: «Estadísticas de los centros de llamadas - 2023» Truelist.com. 1 de enero de 2023. https://truelist.co/blog/call-center-statistics/#:~:text=The%20number%20of%20people%20working,million%20currently%20to%201.8%20million

6. Adaptarse a las aplicaciones heredadas

Comprobar la compatibilidad es un paso fundamental en la actualización tecnológica. Las organizaciones que están implementando el ZTNA también necesitan probar la compatibilidad de las aplicaciones. Durante este proceso, es probable que las organizaciones descubran algunas aplicaciones heredadas que son incompatibles con la mayoría de las soluciones ZTNA actuales. Por ejemplo, las aplicaciones heredadas que requieren tráfico iniciado por el servidor no funcionan bien con la «conectividad de dentro hacia afuera» de una solución ZTNA moderna, que requiere que el tráfico sea iniciado en el punto de conexión. Estos sistemas heredados suelen ser exclusivos y requieren tiempo, recursos y una cuidadosa planificación para ser rediseñados y modernizados (y a menudo esto significa migrar a entornos IaaS alojados en la nube).

Sin embargo, Netskope One Private Access resuelve todos estos ejemplos de las aplicaciones heredadas al proporcionar un acceso seguro y optimizado a todas las aplicaciones privadas desde un único cliente integrado. De este modo, las organizaciones pueden prolongar la longevidad de las aplicaciones heredadas, reducir los costes de gestión de múltiples soluciones de acceso remoto y proporcionar un acceso rápido y fiable a las aplicaciones, independientemente de dónde estén alojadas.



Conclusión

Mientras que en su día fueron una tecnología de vanguardia, las VPN heredadas de acceso remoto suponen ahora un reto para los equipos de seguridad, para los que son una fuente de gran vulnerabilidad ante las amenazas, y para los equipos de infraestructura y operaciones, ya que afectan al rendimiento de la red y, como resultado, degradan la experiencia general del usuario.

Pero la mayoría de las soluciones ZTNA actuales no son una panacea; si no resuelven todos los casos de uso relevantes, las organizaciones se encuentran con que solo pueden realizar una sustitución parcial de la VPN, lo que les deja con una mezcla de infraestructura (VPN tradicional más «algo» de ZTNA) que puede ser incluso más complicada que antes.

Netskope One Private Access está diseñado para ayudar a las organizaciones a acelerar su adopción de Zero Trust con ZTNA mediante una solución totalmente integrada que cataliza la sustitución satisfactoria de toda la infraestructura de la VPN. Proporciona un camino claro hacia la sustitución completa de las VPN de acceso remoto para todos los casos de uso de acceso a aplicaciones, reduciendo la superficie de ataque digital, mejorando la postura de seguridad con principios Zero Trust e impulsando la productividad de los trabajadores remotos con una experiencia de acceso a las aplicaciones optimizada y sin problemas.

Acerca de Netskope One Private Access

Netskope One Private Access aporta capacidades SD-WAN al ZTNA para permitir una conectividad segura y optimizada a todas las aplicaciones privadas, incluyendo VoIP alojada en las instalaciones, vídeo y asistencia remota. De este modo, las organizaciones pueden:

- Modernizar la conectividad y aumentar la seguridad.
- Mejorar la experiencia del usuario.
- Garantizar un acceso altamente fiable y optimizado a las aplicaciones de voz y vídeo.
- Reducir la complejidad y los costes operativos.
- Acelerar los planes para retirar la infraestructura de VPN heredada de acceso remoto, eliminando la necesidad de mantener herramientas de acceso remoto independientes.
- Conseguir una visibilidad y un control sin precedentes del tráfico de las aplicaciones.

Netskope One Private Access permite la retirada completa–no solo la sustitución parcial– de la VPN de acceso remoto para todos los casos de uso de acceso a aplicaciones relevantes, a la vez que mejora la postura de seguridad y ofrece un acceso a las aplicaciones optimizado y sin interrupciones.

Acerca de Netskope

Netskope, líder mundial en SASE, ayuda a las organizaciones a aplicar los principios de Zero Trust y las innovaciones de IA/AA para proteger los datos y defenderse frente a las ciberamenazas. Rápida y fácil de usar, la plataforma Netskope One y su motor patentado Zero Trust proporciona acceso optimizado y seguridad en tiempo real a personas, dispositivos y datos en cualquier lugar. Miles de clientes confían en Netskope y en su potente red NewEdge para reducir riesgos y obtener una visibilidad inigualable de cualquier actividad en la nube, la web y las aplicaciones privadas, ofreciendo siempre seguridad y acelerando el rendimiento sin concesiones. Más información en **netskope.com**.

¿Le gustaría obtener más información?

Solicite una demostración

netskope