netskope

5 señales de que su VPN está en apuros

Hubo un tiempo en que las redes privadas virtuales (VPN) se consideraban la vanguardia de la tecnología, ya que ofrecían una forma sencilla y segura de que los usuarios remotos accedieran a los recursos protegidos de las redes corporativas. En la actualidad, las redes privadas virtuales (VPN) luchan por mantenerse al día con el trabajo híbrido y las amenazas de hoy en día. Durante demasiado tiempo, las empresas han estado ampliando y parcheando su infraestructura VPN existente, tolerando los consiguientes problemas de rendimiento de la red y vulnerabilidades de seguridad. Es hora de replantearnos nuestra dependencia de esta tecnología heredada. He aquí cinco señales reveladoras de que su VPN está en apuros, lo que indica la necesidad de explorar alternativas de acceso más modernas como el acceso Zero Trust (confianza cero) a la red.

1 Está ralentizando a los usuarios

Las configuraciones tradicionales de VPN transportan el tráfico de usuarios remotos a un centro de datos centralizado y a través de una pila de seguridad para aplicar las políticas corporativas. Este enfoque de seguridad de la red, a menudo denominado modelo de castillo y foso, se convierte en un cuello de botella cuando las aplicaciones residen en la nube o los usuarios están lejos del centro de datos.

¿Siente que su red está en apuros? Redirigir el tráfico provoca una latencia añadida significativa, causando retrasos notables que afectan directamente a la productividad y satisfacción de los empleados. Esté atento a estas señales; podrían ser la llamada de atención que su organización necesita para reevaluar su arquitectura de red.

2 Se está ahogando en fallos y parches

Cada mes parecen llegar nuevas advertencias de seguridad para las VPN. La base de datos CVE, de acceso público, enumera casi 700 vulnerabilidades relacionadas con las VPN. Conocidas por sus fallos, las VPN son una mina de oro para los atacantes. Una sola vulnerabilidad exitosa puede proporcionar acceso sin restricciones a todo el sistema de su red corporativa, convirtiéndose en una puerta de entrada para ataques de ransomware y robo de datos.

Si tiene un flujo interminable de parches además de retrasos cada vez mayores, sabe que su VPN está en apuros. Puede ser abrumador, especialmente cuando carece de los recursos necesarios para estar al tanto de todas las actualizaciones que deben aplicarse a las VPN. Dada la amplia superficie de ataque de hardware y software que hay que cubrir, es muy fácil que los riesgos se cuelen por las grietas, dejando los sistemas expuestos y vulnerables.

3 Le cuesta tiempo y recursos gestionarlo

Los administradores tienen una difícil elección a la hora de establecer políticas de VPN: optar por políticas amplias y abiertas y enfrentarse a posibles riesgos de seguridad e imponer políticas restrictivas, bloquear usuarios y atascarse manualmente proporcionando o corrigiendo el acceso. Para complicar aún más las cosas, muchas empresas implementarán reglas de cortafuegos junto con sus VPN.

Cuando la gestión de las políticas de VPN se convierte en una fuente de complejidad y en un desgaste de recursos que hay que gestionar, mantener y auditar, está claro que se encuentra en un aprieto en relación con las políticas. Considere la posibilidad de buscar alternativas que puedan equilibrar la accesibilidad con la seguridad sin necesidad de supervisión manual para gestionar las políticas y las solicitudes de acceso.

4 El acceso de terceros está desbocado

Las organizaciones suelen proporcionar a los colaboradores externos acceso a los sistemas internos a través de VPN, pero esto plantea retos únicos a los equipos de infraestructura y operaciones de TI. La mayoría de los terceros operan en terminales no gestionados, lo que hace que la implementación del cliente VPN de su empresa no solo sea poco práctica, sino en gran medida, inoportuna. Además, estos usuarios normalmente solo necesitan acceder a una serie de aplicaciones, pero a menudo obtienen permisos excesivamente amplios, lo que aumenta el riesgo de uso indebido y el peligro.

Gestionar el acceso de terceros no es fácil cuando se trata de dispositivos no gestionados y se carece de las herramientas granulares adecuadas. ¿Tiene visibilidad de los usuarios externos que se conectan a su red y lo que hacen con ese acceso? Evite este problema de acceso de terceros con una alternativa sin agente.

5 Las quejas sobre VoIP llegan a su servicio de asistencia al usuario

Si los equipos de su centro de llamadas remoto tienen problemas con llamadas VoIP entrecortadas, lentas o interrumpidas, la culpa puede ser de la VPN. VoIP y UCaaS son extremadamente sensibles a las condiciones de la red y requieren conexiones estables e ininterrumpidas para mantener la calidad de las llamadas; incluso el más mínimo contratiempo puede provocar una degradación importante.

El redireccionamiento del tráfico VoIP a través de una VPN al centro de datos de la empresa puede general la pérdida de paquetes, fluctuación y latencia, lo que afecta a la experiencia de usuario y a la productividad en general. Si todo esto le resulta familiar, es un signo revelador de que su VPN le ha metido en problemas. Tal vez sea el momento de reconsiderar su solución de acceso remoto y explorar alternativas más fáciles de usar para aliviar la carga del servicio de asistencia al usuario.

Si reconoce alguna de estas señales, ¡es hora de cambiar! Explore otras posibilidades con Netskope

Netskope One Private Access

Más información

netskope