netskope

5 signes qui montrent que votre VPN a atteint ses limites

Il y a quelques années, les VPN étaient considérés comme la technologie de référence, qui permettait aux collaborateurs à distance d'accéder de manière simple et sécurisée aux ressources internes de leur entreprise. Aujourd'hui, les VPN peinent à s'adapter au travail hybride et aux menaces modernes. Pendant trop longtemps, les entreprises se sont contentées de bricoler et de rafistoler leurs réseaux VPN, tout en subissant des problèmes de performance et des failles de sécurité, faute de solution durable. Il est temps de repenser notre dépendance à cette technologie obsolète. Voici cinq signes qui montrent que votre VPN a atteint ses limites et qu'il est urgent d'envisager d'autres solutions modernes comme l'accès réseau Zero Trust (ZTNA).

1 Il ralentit vos utilisateurs

Les configurations VPN traditionnelles redirigent le trafic des utilisateurs distants vers un datacenter centralisé, où une pile de sécurité entrante applique les stratégies de l'entreprise. Cette approche de la sécurité réseau, de type « castle-and-moat » (château encerclé par des douves), crée un goulot d'étranglement quand les applications sont hébergées dans le cloud ou les utilisateurs se trouvent loin du datacenter.

Votre réseau semble avoir atteint ses limites ? Le backhauling ajoute une latence importante et provoque des retards perceptibles qui nuisent directement à la productivité et à l'expérience des collaborateurs. Certains signes ne trompent pas. Ils pourraient indiquer qu'il est temps de réévaluer l'architecture du réseau de votre entreprise.

2 Vous êtes submergés par les bogues et les correctifs

Chaque mois apporte son lot de nouveaux avertissements de sécurité pour les VPN. La base de données CVE, accessible au public, recense près de 700 vulnérabilités liées à ces technologies. Souvent truffés de failles, les VPN représentent une aubaine pour les attaquants. Une seule faille de sécurité peut suffire pour compromettre l'intégralité du réseau d'une entreprise, et exposer celle-ci aux attaques par ransomware et au vol de ses données sensibles.

Un flux incessant de correctifs et un backlog qui ne cesse de croître sont des signes évidents que votre VPN a atteint ses limites. Cette situation devient rapidement accablante, surtout lorsque les ressources manquent pour suivre le rythme des mises à jour essentielles. Avec une surface d'attaque étendue, aussi bien sur le plan matériel que logiciel, les failles de sécurité passent trop facilement inaperçues. Chaque vulnérabilité non corrigée expose donc un peu plus vos systèmes aux menaces.

3 Sa gestion prend du temps et mobilise des ressources précieuses

Les administrateurs se trouvent confrontés à un choix délicat concernant la configuration de leurs VPN : faut-il privilégier une approche souple et permissive, quitte à fragiliser la sécurité du réseau, ou opter pour un contrôle rigoureux qui, certes protège mieux, mais complique la vie des utilisateurs et impose une gestion fastidieuse des autorisations ? Cette complexité s'accroît lorsque les entreprises déploient simultanément des règles de pare-feu avec leur VPN.

Lorsque la gestion des stratégies VPN devient un casse-tête et engloutit des ressources pour l'administration, la maintenance et l'audit, il est clair que la situation pose problème. Il est alors temps de rechercher d'autres solutions capables de concilier accessibilité et sécurité, sans exiger une surveillance constante pour ajuster les stratégies et traiter les demandes d'accès.

4 L'accès des tiers est hors de contrôle

Les entreprises accordent fréquemment aux collaborateurs externes un accès aux systèmes internes via des VPN, mais cette approche crée des défis spécifiques pour les équipes chargées de l'infrastructure et des opérations (I&O). La plupart des partenaires externes travaillent sur des appareils non managés, ce qui rend l'installation du client VPN de votre entreprise à la fois compliquée et peu souhaitable. En outre, ces utilisateurs n'ont généralement besoin d'accéder qu'à quelques applications spécifiques. Malgré cela, ils se retrouvent souvent avec des droits beaucoup trop étendus, ce qui expose davantage les systèmes aux risques de piratage et d'utilisation malveillante.

La gestion des accès externes s'avère délicate, particulièrement quand les appareils ne sont pas managés et que vos outils de contrôle ne sont pas très rigoureux. Savez-vous précisément quels utilisateurs externes se connectent à votre réseau et comment ils utilisent cet accès ? Éliminez ces risques en adoptant une solution sans agent, plus sécurisée et mieux adaptée à la gestion des accès d'utilisateurs externes.

5 Les plaintes concernant la VoIP se multiplient dans votre service d'assistance

Si les équipes de votre centre d'appels à distance rencontrent des problèmes de qualité avec la VoIP (appels saccadés, décalages ou interruptions), votre VPN pourrait bien en être la cause. Les solutions VoIP et UCaaS sont particulièrement sensibles aux conditions du réseau et nécessitent des connexions stables et continues pour garantir une qualité d'appel optimale. Le moindre incident peut entraîner une dégradation significative.

Le backhauling du trafic VoIP via un VPN jusqu'au datacenter de l'entreprise introduit souvent une perte de paquets, de la gigue et une latence, ce qui nuit à l'expérience utilisateur et réduit la productivité. Si cette situation vous semble familière, il est fort probable que votre VPN a atteint ses limites. Il est peut-être temps de repenser votre solution d'accès à distance et de rechercher d'autres solutions mieux adaptées, capables de réduire la charge de travail de votre

Il est temps de réagir si vous reconnaissez l'un de ces signes ! Découvrez les solutions proposées par Netskope

Netskope One Private Access

En savoir plus

netskope