netskope

5 Telltale Signs Your VPN Is in a Pickle

Once upon a time, virtual private networks (VPNs) were considered the cutting edge of technology, offering a simple and secure way for remote users to access protected resources on corporate networks. Fast forward to the present, and VPNs are struggling to keep up with hybrid work and modern-day threats. Businesses, for too long, have been stretching and patching up their existing VPN infrastructure, tolerating the consequential network performance issues and security vulnerabilities. It's time to rethink our continued reliance on this legacy technology. Here are five telltale signs that your VPN is in a pickle, signaling the need to explore more modern access alternatives like Zero Trust Network Access (ZTNA).

1 It's slowing your users down

Traditional VPN setups backhaul remote user traffic to a centralized data center and through an inbound security stack to enforce corporate policies. This network security approach, often called the castle-and-moat model, becomes a bottleneck when applications reside in the cloud or users are far from the data center.

Feeling like your network is in a pickle? Backhauling results in significant added latency, causing noticeable delays that directly impact employee productivity and satisfaction. Keep an eye out for these signs; they might just be the wake-up call your organization needs to reevaluate its network architecture.

2 You're drowning in bugs and patches

Every month seems to bring new security warnings for VPNs. The publicly available CVE database lists nearly 700 vulnerabilities linked to VPNs. Notorious for being buggy, VPNs are a goldmine for attackers. A single successful exploit can provide unfettered, system-wide access to your corporate network, becoming a gateway for ransomware attacks and data theft.

If you have an endless stream of patches coupled with a growing backlog, you know you're in a VPN pickle. It can be overwhelming, especially when you lack the resources to stay on top of all the updates that need to be applied to your VPNs. Given the expansive hardware and software attack surface you have to cover, it's all too easy for risks to slip through the cracks, leaving your systems exposed and vulnerable.

3 It’s costing you time and resources to manage

Administrators have a tough choice when it comes to setting VPN policies: opt for broad, open policies and face potential security risks, or impose restrictive policies, block users, and get bogged down manually providing or fixing access. Further complicating matters, many companies will deploy firewall rules alongside their VPN.

When VPN policy management becomes a source of complexity and a drain on resources to manage, maintain, and audit, you’re unmistakably in a policy pickle. Consider seeking alternatives that can balance accessibility with security without requiring manual oversight to manage policies and access requests.

4 Third-party access is running amok

Organizations commonly provide external collaborators access to internal systems through VPNs, but it poses unique challenges for I&O teams. Most third parties operate on unmanaged endpoints, making the deployment of your company’s VPN client not only impractical but largely unwelcome. Moreover, these users usually only require access to a handful of applications, but often amass overly broad permissions, increasing the risk of misuse and compromise.

Managing third-party access isn’t easy when you’re dealing with unmanaged devices and a lack of appropriate, granular tools. Do you have visibility into external users connecting to your network and what they are doing with that access? Steer clear of this third-party access pickle with an agentless alternative.

5 VoIP complaints are hitting your help desk

If your remote call center teams are struggling with choppy, laggy, or dropped VoIP calls, your VPN might be to blame. VoIP and UCaaS are extremely sensitive to network conditions and require stable, uninterrupted connections to maintain call quality—even the slightest hiccup can lead to significant degradation.

Backhauling VoIP traffic through a VPN to the corporate data center can introduce packet loss, jitter, and latency, impacting user experience and overall productivity. If this sounds all too familiar, it’s a telltale sign that your VPN has landed you in a pickle. Perhaps it’s time to reconsider your remote access solution and explore more user-friendly alternatives to ease the strain on your help desk.

If you recognize any of these signs, it’s high time for a switch! Explore the possibilities with Netskope

ZTNA next

Learn more

netskope