Tip Sheet

AVIATRIX®

5 Tips to Avoid VPN Outages in the Multicloud Era

Reduce downtime. Improve visibility. Protect your business.

Why It Matters

VPN downtime isn't just frustrating—it's a threat to availability, compliance, and trust. Without real-time visibility and AI-assisted diagnostics, simple misconfigurations can lead to hours of investigation and lost productivity. In a zero trust world, unmonitored VPN traffic creates blind spots attackers can exploit. Organizations need a platform-native solution that bridges security and connectivity with embedded intelligence.

And the stakes are high:

- **$5,600–$9,000** lost per minute of downtime
- **44%** of enterprises say an hour of downtime costs over **$1M**
- Security and compliance **risks multiply** when VPN traffic goes unmonitored

5 Expert Tips to Stay Ahead of VPN Issues

1. Monitor Continuously, Not Just When Something Breaks

Most teams only spot VPN problems after users report them. Implement continuous diagnostics to catch misconfigurations and failures before they cascade to resolve outages in minutes and strengthen cloud security.

2. Validate Credentials and Certificates Proactively

Many outages stem from expired certificates or invalid logins. Establish alerts for expiring credentials and enforce consistent certificate hygiene across all environments.

3. Visualize Network Behavior Across Clouds

Cloud-native VPNs span regions, vendors, and topologies. Use tools that give unified visibility across single, multicloud, hybrid, or on-prem environments to identify anomalies faster.

4. Automate Root Cause Analysis with AI

Troubleshooting manually is slow and can be error-prone. Offload initial diagnosis to AI tools that can spot protocol mismatches, policy conflicts, or tunnel instabilities in seconds.

5. Empower Your Junior Engineers with Smart Workflows

Downtime is expensive, and bottlenecks form when only a few experts can solve VPN issues. Guided, AI-powered workflows can help your whole team respond faster–with confidence.

Ready to Take Action?

The Secure Network Supervisor Agent by Aviatrix turns these best practices into action–automating VPN diagnostics and surfacing real-time insights through Microsoft Security Copilot.

As part of the **Aviatrix Cloud Native Security Fabric**, it brings embedded enforcement, multicloud visibility, and intelligent troubleshooting to your cloud network–without needing bolt-on tools. The agent integrates infrastructure-level telemetry with AI-assisted SOC workflows to reduce mean time to resolution, prevent misconfigurations, and improve zero trust posture.

It's the first AI-powered network agent purpose-built for Security Copilot–making NetOps and SecOps faster, smarter, and more aligned.

Request a demo to see how Aviatrix helps you stop VPN outages before they start.

Request a Demo

About Aviatrix

Aviatrix® is the cloud network security company trusted by more than 500 of the world's leading enterprises. As cloud infrastructures become more complex and costly, the Aviatrix Cloud Network Security platform gives companies back the power, control, security, and simplicity they need to modernize their cloud strategies. Aviatrix is the only secure networking solution built specifically for the cloud, that ensures companies are ready for AI and what's next. Combined with the Aviatrix Certified Engineer (ACE) Program, the industry's leading secure multicloud networking certification, Aviatrix unifies cloud, networking, and security teams and unlocks greater potential across any cloud.