VPN Drop-Issue Diagnostic Checklist

Use this quick-reference guide to identify and resolve common causes of VPN instability.

Brought to you by Fusion Connect — your partner in connectivity, managed network, and dedicated internet access.

Step 1: Confirm the Scope

Goal: Determine whether it's local or widespread.

- ☐ Test VPN connection from multiple locations or users.
- ☐ Disconnect VPN and test basic internet access (ping, traceroute, or speed test).
- ☐ Check provider or ISP status page for known outages.
- ☐ If multiple branches share the same provider, note whether they're all affected.

Step 2: Assess Bandwidth & Performance

Goal: Identify congestion or instability in the underlying link.

- ☐ Run consistent speed tests during VPN use (upload/download/latency).
- ☐ Monitor packet loss or jitter (even 2–3 % can break tunnels).
- ☐ Compare with baseline performance from other times or locations.
- ☐ If you're on consumer-grade broadband, consider business-class or dedicated internet access.

Contact us:
+1 888-301-1721
info@fusionconnect.com
www.fusionconnect.com

See Terms and Conditions

Step 3: Check Firewall & Routing Rules
Goal: Ensure security policies aren't killing the tunnel.

- [ ] Review recent firewall firmware updates or rule changes.
- [ ] Confirm VPN traffic ports (UDP 500/4500, TCP 443 for SSL, etc.) are open both directions.
- [ ] Verify NAT session timeout values—extend them if idle tunnels drop.
- [ ] Enable or confirm "keep-alive" or "dead-peer-detection" settings.

Step 4: Verify DNS & IP Configuration
Goal: Prevent address or name conflicts that cause handshake failures.

- [ ] Confirm unique IP subnets for each site (no duplicates like "192.168.1.0/24").
- [ ] Clear local DNS cache and confirm endpoint hostname resolves correctly.
- [ ] Check internal split-tunnel DNS settings—ensure internal lookups go to the right DNS servers.
- [ ] Test VPN connection by IP address instead of hostname to isolate DNS errors.

Step 5: Inspect VPN Client or Edge Device
Goal: Rule out outdated or misconfigured software.

- [ ] Confirm VPN client version is current and supported by vendor.
- [ ] Review release notes for stability fixes or OS compatibility issues.
- [ ] Reinstall or repair client if configuration corruption is suspected.
- [ ] Verify that firmware on edge appliances or routers is up-to-date.

Step 6: Document & Escalate Efficiently
Goal: Capture data to share with provider or managed-service partner.

- [ ] Record time/date and frequency of disconnects.
- [ ] Capture screenshots or logs of error messages.
- [ ] Note ISP circuit ID or public IP at affected location.
- [ ] If using Fusion Connect Managed Network Services, open a support ticket with this info for faster resolution.

fusion connect

PRO-TIP

If VPN drops happen often across sites, consider Managed Network Services or SD-WAN solutions that proactively monitor and route around congestion. Fusion Connect's dedicated internet access and managed connectivity options provide that resiliency and visibility from the same partner who supports your network edge.

Visit **www.fusionconnect.com** to learn more.
Or, contact a Fusion Connect Business Consultant today at 888-301-1721.