Devolutions

10 Ways to Increase VPN Security

VPNS USE ENCRYPTION TO CREATE A SECURE CONNECTION OVER UNSECURED INTERNET INFRASTRUCTURE

Here is a question I get a lot: "Do virtual private networks provide effective security for businesses?" The short answer is: Yes! Now, here is the longer answer:

VPNs use encryption to create a secure connection over unsecured internet infrastructure. However, while VPNs provide strong security and anonymity, they aren't bulletproof. Just like passwords, VPNs can be hacked. However, there are some things that all organizations should do to increase their protection. These include:

1. Implement 2FA/MFA

If a password is compromised, or if VPN client certificates and authentication cookies are used to bypass authentication, then enforcing 2FA/MFA on your VPN can be your last, best line of defense. Of course it goes without saying (but I'll mention it just in case) that implementing a strong password policy in your organization is essential.

2. Use the OpenVPN Protocol

VPNs support different protocols that provide varying levels of security. The three most common protocols are PPTP, L2TP and OpenVPN:

- PPTP is the weakest protocol. It uses 128-bit encryption, and the authentication and connection process can be intercepted by hackers — which would result in data being decrypted and compromised. On the plus side, because it has the lowest encryption, PPTP is also one of the fastest protocols.
- The L2TP protocol is more secure than PPTP, but it's quite slow and can significantly increase operating costs.
- OpenVPN offers the highest level of security and privacy. It's also relatively fast, and recoveries from lost connections are rapid. We strongly recommend that organizations only use a VPN solution that supports OpenVPN.

3. Stop DNS Leaks

A DNS leak is a security flaw that enables DNS requests to be revealed to ISP DNS servers, even though the VPN service attempts to conceal them. If this happens in your organization, then contact your VPN vendor and see if they offer DNS leak protection. If not, it is probably necessary to start shopping for another solution.

4. Use a Kill Switch

In the unlikely event that your VPN connection drops, you will be at risk of using a regular unprotected connection managed by your ISP. A kill switch prevents this by shutting down apps and preventing access to websites as soon as the connection is lost.

5. Use Network Lock

If your Wi-Fi network gets interrupted, a network lock automatically blocks your computer from accessing the internet. This keeps information secure and protected while the VPN reconfigures.

6. Stop IPv6 Leaks

IPv6 is a version of the Internet Protocol that allows you to access more internet addresses than IPv4. The issue with IPv6 is that it operates outside the VPN territory, and a hacker could use it to see who you are. I recommend running a quick test here to verify if you're safe. If not, then you can disable IPv6 manually by running the following command on Windows: netsh interface teredo set state disabled

7. Stop WebRTC Leaks

WebRTC (Web Real-Time Communication) is an open-source project that allows two devices to communicate with each other by broadcasting each other's IP addresses. It is used by most browsers (e.g., Chrome, Firefox, Safari, Edge, and mobile browsers for Android and iOS) for various voice and video chat apps (e.g., Google Hangouts, Skype for Web, Discord, etc.).

What's the problem here? It's this: whenever a user connects to a site that has WebRTC enabled, WebRTC can transmit data outside a VPN's encrypted tunnel. This in turn exposes the user's real IP address and location. How can you tell if this is happening? Run this test: turn off your VPN and connect to a site that uses WebRTC. Look at your connection information and note the IP address. Then, launch your VPN. If your IP address changes to the VPN's or disappears, then you don't have a WebRTC leak. But if your IP address remains the same, then you do.

In this case, the simplest and best solution is to choose a different VPN service that blocks WebRTC traffic from being transmitted outside the encrypted VPN tunnel. If changing VPNs is not practical or financially feasible at this time, then you can block them manually in your browser. For steps and screenshots on how to do this, I recommend this excellent article at Comparitech.com.

8. Limit VPN Access

Limit VPN access to specific authorized users, and only for the required amount of time. Remember that a VPN connection is a door to your LAN.

9. Use an Intranet or Extranet Instead of a VPN

It may be prudent to enable users to access certain files through a secure HTTPS website with 2FA or MFA authentication, rather than through a VPN. In this configuration, a breach will only expose selected files on a single server vs. the whole network.

10. Secure Remote Wireless Networks

VPNs are used to secure unsecure wireless routers that are surprisingly insecure by default, these vulnerabilities can sometimes undermine VPNs. There are many things end users can do, or that can be done on their behalf by IT staff. Rather than listing them all here, I encourage you to read and share our article, "9 Tips to Make Your Home Wireless Network More Secure" (and of course the advice applies to securing corporate wireless networks as well).

The Bottom Line

Will implementing all of the tips above absolutely, categorially, unequivocally make your VPN impenetrable? Unfortunately, no. However, it will greatly improve data security and significantly reduce both the likelihood and severity of a breach. As such, I strongly urge you to make this a top priority.

If you are not satisfied with your current VPN or want to explore what is available in the marketplace, then I invite you to check out our comparison of 8 popular VPNs. And if you have any additional tips or advice for securing VPNs, please comment below so that we can all benefit from your knowledge and experience.