10 tips to secure client VPNs

www.computerworld.com/s/article/9003779/10_tips_to_secure_client_VPNs

Computerworld | Oct 2, 2006 1:00 AM PT

If you have given your trusted employees and key contractors remote access to your network via a client virtual private network (VPN), congratulations! By now, you have seen the productivity and cost benefits from allowing collaboration that surmounts geographical separation.

You may also have discovered that keeping your network secure is now even trickier than it was, because each uncontrolled remote computer potentially creates another avenue of access to the network for attackers. Here are 10 tips to help secure your network while ensuring the benefits of your VPN.

1. Use the strongest possible authentication method for VPN access. Exactly what this is will depend on your network infrastructure, and you should check your VPN or operating system documentation to determine your options.

For example, on a network with Microsoft servers, the most secure authentication is provided by Extensible Authentication Protocol-Transport Level Security (EAP-TLS) used with smart cards. These require a public key infrastructure (PKI) and incur the overhead of encoding and distributing smart cards securely. On these networks, Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAP v2) and Extensible Authentication Protocol (EAP) provide the next best authentication security.

Password Authentication Protocol (PAP), Shiva Password Authentication Protocol (SPAP) and Challenge Handshake Authentication Protocol (CHAP) are too weak to be allowed.

2. Use the strongest possible encryption method for VPN access. On a network with Microsoft servers, this is Layer Two Tunneling Protocol (L2TP) over Internet Protocol security (IPsec). Point-to-Point Tunneling Protocol (PPTP) is too weak to be allowed, unless your client passwords are guaranteed to be strong (see tip No. 6). OpenVPN, a Secure Socket Layer (SSL) VPN, can be run with TLS-based session authentication, Blowfish or AES-256 encryption, and SHA1 authentication of tunnel data.

3. Limit VPN access to those with a valid business reason, and only when necessary. A VPN connection is a door to your LAN, and should only be open when it needs to be. Remote employees should be discouraged from connecting to the VPN all day to check e-mail (see tip No. 5). Remote employees and contractors should also be discouraged from connecting to the VPN to download commonly needed files (see tip No. 4).

4. Provide access to selected files through intranets or extranets rather than VPNs. A secure HTTP Secure (HTTPS) Web site with safe password authentication (not basic authentication) exposes only selected files on a single server, not your whole network, and scales better than a VPN.

5. Enable e-mail access without requiring VPN access. On Microsoft Exchange servers, set up an Exchange proxy server to allow Outlook to access Exchange via remote procedure call (RPC) protocol over HTTP, protected by SSL encryption.

On other mail servers, enable Post Office Protocol 3 (POP3) and/or Internet Message Access Protocol (IMAP) mail receipt and Simple Mail Transfer Protocol (SMTP) mail sending. Require secure password authentication (SPA) and SSL encryption to improve the security of these mail systems. Secure Web mail is another viable option for remote employees, especially when they are traveling and need to use other people's computers.

6. Implement and enforce a strong password policy. In the absence of two-factor authentication using smart cards or biometrics (see tip No. 1), your network is only as secure as the weakest password in use.

No one should be allowed to keep a password permanently, use a word found in a dictionary for a password, use a number related to their telephone or social security number, or use the name of a family member or pet.

Passwords should be unguessable even by family members, and long enough with a large enough character set to be prohibitively hard for a password-guessing program to find. This goes double for administrators.

7. Provide strong antivirus, antispam and personal firewall protection to your remote users, and require that they use it. Every computer fully connected to the VPN (see tip No. 8) can spread infections throughout the network, potentially bringing company business to a halt.

8. Quarantine users from the time to they connect to the VPN until their computer has been verified as safe. When a client computer starts a VPN session, it should not have full access to the network until it has been checked for compliance with network policies. This should include checking for current antivirus and antispam signatures, an operating system fully patched against critical security flaws and no active remote-control software, key loggers or Trojans.

The downside of doing a thorough scan at login is that it can delay the user from doing useful work for several minutes. You can improve the experience for frequent VPN users by having the server remember each client computer's scan history and reduce the scan level for several days after each successful scan.

9. Forbid the use of other VPNs and remote-control software while connected to your VPN. The last thing you need is for your network to be exposed to other networks. Most VPN software sets the client's routing to use the network's default gateway after connection by default, but this is usually optional.

Very remote employees may find that work-related Internet browsing becomes prohibitively slow if all their traffic is routed through the network, and they will want to turn this option off, but that will also defeat any protection against hostile sites that you have established at your proxy or gateway.

A personal firewall and a client for your proxy firewall can allow employees to have safe remote network access without slowing down their Internet connection. You can also establish a clear, written policy about what constitutes acceptable Internet usage while connected to the VPN.

10. Secure remote wireless networks. Employees working from home often use laptops connected to a cable or DSL modem through their own wireless access point.

Unfortunately, many wireless routers are never configured for security: they are merely connected and turned on. Teach employees how to configure their wireless routers and computers for WPA with a pre-shared key, how to configure their personal firewalls (see tip No. 7), and why it is important to keep their home networks secure.

Maintaining network security requires constant vigilance, and maintaining VPN security even more vigilance. If you adhere to these 10 tips, however, you'll be much less likely to encounter VPN-related security breaches.

Martin Heller develops software and Web sites, and writes from Andover, Mass. You can contact him at cw@mheller.com.

Martin Heller — Contributing Editor

Martin Heller is a contributing editor and reviewer for InfoWorld. Formerly a web and Windows programming consultant, he developed databases, software, and websites from 1986 to 2010. More recently, he has served as VP of technology and education at Alpha Software and chairman and CEO at Tubifi.