Ten tips to protect the client virtual private network

Virtual private networks (VPNs) are increasingly asserting profit advantages in their performance and prices. You can provide remote network access to trusted employees or solution bidders via a virtual private network. Geographical distance now & oci

Virtual private networks (VPNs) are increasingly asserting profit advantages in their performance and prices. You can provide remote network access to trusted employees or solution bidders via a virtual private network. Geographical distance is no longer a problem.

Along with the steps of expanding, network security requires more sophisticated and clever methods. Just a remote machine that loses control can create an attractive and dangerous penetration path for attackers.

Here are 10 tips we would like to provide to help you keep your security safe while ensuring the profit factor from VPNs.

1. Use the strongest VPN access authentication method.

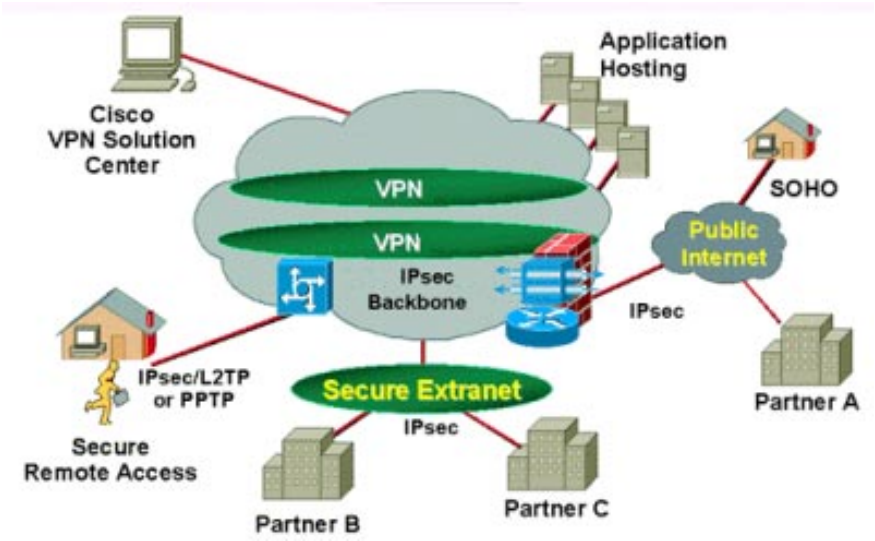
Exactly which method depends on the network infrastructure. You should check the documentation in the VPN or operating system to determine the most appropriate method.

If the network uses Microsoft servers, the safest authentication method is the Extensible Authentication Protocol and Transport Level Security, also known as EAP-TLS. They are used with smart cards. This method requires a common key infrastructure (PKI), which can securely encrypt and distribute smart cards. The Microsoft Handshake Challenge Authentication Protocol Version 2 (MS-CHAP v2) and Extensible Authentication Protocol (EAP) protocols are the best choice for next security authentication methods.

You should not choose the Password Authentication Protocol (PAP) - password authentication protocol, Shiva Password Authentication Protocol (SPAP) - Shiva password authentication protocol and Handshake Challenge authentication protocol (CHAP), they are too weak, not secure for your network.

2. Use the strongest method of encrypting VPN access.

For a network using a Microsoft server, you should use Layer Two Tunneling Protocol (L2TP) with Internet Protocol security (IPsec). Point-to-Point Tunneling (PPTP) is too weak, unless your client's password is strong enough (see tip 6). OpenVPN, a single sockert virtual private network (SSL) can run with TLS session authentication, Blowfish or AES-256 encryption program and SHA1 authentication of tunnel data.



3. Limiting VPN access with reasonable commercial reasons and only when necessary.

VPN connection is the door to the LAN, it should only be opened when needed. You should limit remote employees to connect to VPN all day to check e-mail (see tip 5). For bidders, it is also recommended to prevent connecting to VPNs to download necessary files normally (see tip 4).

4. Provide access to selected files via Intranet or Extranet instead of VPN.

A secure HTTP Secure (HTTPS) website with secure password authentication only puts selected files on a single server, not the entire network, and has a better elasticity than VPN.

5. Allow e-mail access without access to VPN.

On a Microsoft Exchange server, you should install an Exchange proxy server to allow Outlook to access Exchange via remote procedure call (RPC) protocol in HTTP. This component is protected by SSL encryption protocol.

With other e-mail services, you can use the Post Office Protocol (POP3) protocol with the Internet Message Access Protocol (IMAP) or Simple Mail Transfer Protocol (SMTP) mailing protocol. You should also use password security authentication (SPA) and SSL encryption program to demonstrate the security of these mail systems. Secure Web mail is another option for remote employees, especially when they are traveling or using someone else's computer.

6. Enforce and force employees to implement a secure password policy.

If you're missing a two-factor authentication program (smart card and biometrics), your network will only be secure with the weakest password level.

You should not keep a password for too long, but change it often, at least once every 3 months. Do not use a word found in the dictionary or some phone-related numbers, social security numbers, family members' names, pet names for passwords.

Password should be hard to understand, difficult to guess even for family members. It should not be too short.

Creating a secure element in a password is an important step.

7. Provide anti-virus, anti-spam and personal firewall programs for remote users and ask them to use them.

Every computer that is fully connected to the VPN (see tip 8) can spread malicious programs over the network, potentially threatening to disrupt a company's commercial transaction. So you should provide personal antivirus, antispam, firewall programs to your employees and require them to use them.

8. Quarantine users to verify their computer's security level before allowing connection to the VPN network.

When a client computer starts the VPN session, it will not have full access to the network until it has been tested for security. The test part can be current antivirus and antispam traces; check full operating system patches, fix serious security errors; remote control software does not work; keyloggers or Trojans.

The downside of this method is that users will be late for a few minutes when they want to do certain things. You can overcome by remembering the scan schedule in your computer and reducing the scanning frequency by a few days compared to the previous scan.

9. Prohibit using virtual private network or other remote control software when connecting to your network.

The last thing needed for your network is to distinguish it from other networks. Most VPN software sets the orientation for customers to use the default gateway, after the default connection. But often that is optional, not required.

When all Internet browser work-related traffic is routed through the network, the transfer rate becomes so slow that it is extremely annoying. Often, remote employees only want to turn off this option. But that also means eliminating the protection program against malicious websites that have been set up at the proxy or gateway.

A personal firewall and a client proxy firewall allow employees to have secure remote network access without slowing down their Internet connection. You can also set up a clear policy on how to use the Internet when connecting to a VPN for security.

10. Secure remote wireless network.

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 to be safe. They are merely connected and turned on. Teach your staff how to configure your wireless router, WPA computers with a 'pre-shared' key, how to configure your personal firewall and explain to them the importance of home network security.

Maintaining network security requires a certain amount of vigilance. Maintaining virtual private network security is even more vigilant. But based on the 10 tips above you may be less likely to face VPN related issues much more.

similar articles on tips and guides. Thank you for reading and for following us regularly.