

 SearchSecurity.com E-Book

Simple Steps to Securing Your SSL VPN

This expert E-book details a 5 point strategy for effectively securing remote access within your organization and features an expert article on how to successfully penetration test your company's VPN. This ebook concludes with a quiz that helps test your knowledge of IPsec vs. SSL VPNs and details additional resources that help you determine which technology best suits your company's needs.

Sponsored By:

 SONICWALL



Simple Steps to Securing Your SSL VPN

Table of Contents:

[A five-point strategy for secure remote access](#)

[Pen testing your VPN](#)

[Client-side security considerations for SSL VPNs](#)

[Quiz: IPsec vs. SSL VPNs](#)

[IPsec vs. SSL VPNs quiz answers](#)

[Resources from SonicWALL](#)

A five-point strategy for secure remote access

By George Wrenn

Managing secure remote access is a tough job. Because remote systems may directly connect to the Internet rather than through the corporate firewall, they pose an increased risk to your network environment. Virus and spyware protection, and a general VPN network policy isn't enough to keep these systems—and the network they connect to—safe. Here are five best practices for providing secure remote access.

1. Software controls policy

Create a policy that defines the exact security software controls that must exist on systems with remote access. For example, you may need to spell out that antivirus, anti-spyware and desktop firewalls must be installed and configured in a specific manner with the latest signatures, along with which vendors are acceptable. The best practice is to distribute the policy along with the connection setup or similar instructions for end users. Often a zero-tolerance policy is best for endpoint security. End users should meet a set of guidelines before connecting to the network. No AV, antispyware and desktop firewall? No remote access allowed. The policy should also spell out what ports and services may be exposed on the system.

2. Endpoint security management

Choose a vendor that offers comprehensive endpoint security management and policy enforcement as part of their VPN or remote access solution. It is best to mandate that all remote users use the enterprise sponsored VPN client. That's the only way you are going to get true policy compliance and assurance of endpoint security posture. Your chosen remote access solution should be able to refuse connections for endpoint systems that do not meet the policy compliance checks. Ideally, the solution should tell end users which items are out of compliance so they can remediate the situation prior to attempting to reconnect. This cuts down on help desk calls.

3. Enforce corporate policy compliance

Inform end users that corporate security policy extends to their remote desktop when connected to the enterprise network. For example, no file sharing and other disallowed use while connected to the corporate network.

4. Reporting features

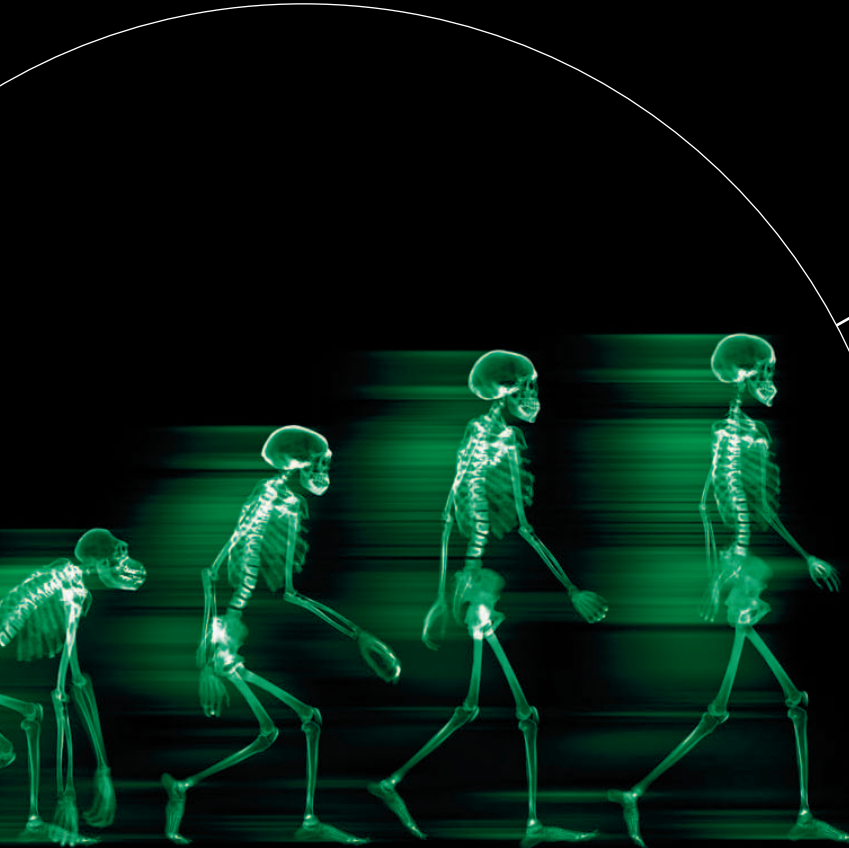
Reporting on end user compliance is critical. Most of the solutions mentioned above offer reporting capabilities to keep admins updated on the status of the connecting endpoints. Depending on the number of users you have to manage, it may be wise to set up alarms that e-mail admins when a machine that is significantly out of compliance tries to connect. In some cases administrative intervention may be warranted — especially when other access methods to the network may exist.

5. Periodically review policy and reports

Every couple of months, review policies and reports to identify trends and patterns in access violations. This is important to ensure that the policy and technical controls are addressing your remote access security needs. If you find trends in access violations, add or modify policies accordingly.

About the author: *George Wrenn, CISSP, ISSEP, is a technical editor for our sister publication Information Security magazine and a security director at a financial services firm. He's also a graduate fellow at the Massachusetts Institute of Technology.*

A NEW CLASS OF NETWORK AND DATA PROTECTION FOR THE ENTERPRISE HAS EVOLVED.



SO MUCH FOR THE STATUS QUO.

Existing solutions can be technologically limited, notoriously expensive or painful to deploy and use. Step up to SonicWALL® E-Class – a new generation of enterprise-class network security, secure remote access, and email security solutions. The E-Class Network Security Appliance (NSA) is the first to use a 16-core microprocessor that can run deep packet inspection, gateway anti-virus, anti-spyware and intrusion prevention full throttle without compromising network speed. NSA appliances all have the enterprise features you'd expect including state sync, single sign-on, application firewall and the SonicWALL Global Management System to centrally manage thousands of appliances. E-Class Secure Remote Access provides ease of deployment and usage plus unsurpassed levels of granular control and connection to a wide range of leading end-point devices. E-Class Email Security stops spam and inspects every attachment for threats without sacrificing effectiveness. SonicWALL E-Class high performance protection – engineered to drive the cost and complexity out of running a secure network. Learn more at www.sonicwall.com/evolve or call 1.888.557.6642.



NETWORK SECURITY



SECURE REMOTE ACCESS



WEB AND E-MAIL SECURITY



BACKUP AND RECOVERY



POLICY AND MANAGEMENT

SONICWALL®

PROTECTION AT THE SPEED OF BUSINESS™

Pen testing your VPN

By Joel Dubin

A Virtual Private Network (VPN) is like a large sign, saying "Sensitive Data Here." Hackers know that when they've found a VPN, they've hit the jackpot, because it means somebody is trying to secure something confidential. Therefore, like any other gateway, your VPN needs to go through a thorough penetration test to check for vulnerabilities. It's easy to overlook VPNs when pen testing your network, as it's often assumed that they're the most secure part of it. But, they're not and they're a magnet for hackers.

Pen testing a VPN is straightforward, and there are some common tools for the job. It's not much different from the rest of your pen testing routine and should be part of it.

There are two types of VPNs: IPSec and SSL. Which VPN you are running will determine how you conduct the pen test. Regardless, there are three basic steps to pen testing your VPN:

1. Scout the terrain and plan the attack.
2. Exploit known vulnerabilities—then close or patch them.
3. Test for default user accounts—then shut them down.

To scout the terrain, run a simple port scan. This will reveal whether you are running an IPSec or SSL VPN. Even though you already know that, a port scan is a good defensive exercise that mirrors the steps of a potential intruder. Scan the network perimeter where the VPN may be located. The only caveat is to watch for bounced packets if the VPN is part of a combo with a firewall. If the scan shows that port 500 is open, the VPN is IPSec. Port 500 is the standard port for the Internet Key Exchange (IKE) protocol used for the key exchange required in IPSec. If the scan shows port 443 to be open, the standard port for SSL, then the VPN is obviously SSL. An SSL VPN uses the same port as any other SSL communication.

The exploit phase of the test must go in one of two directions. Testing an IPSec VPN is very different from testing an SSL VPN. The IPSec VPN is network-based, while the SSL VPN is Web-based. In fact, the SSL VPN is essentially a Web application and should be tested as such.

For IPSec VPNs, NTA Monitor has a tool called IKE-scan, which can fingerprint many VPN vendors and models. With that information, a hacker can search the Web for details of attacks against specific vendors. Exploits have been found and posted for Cisco, Nortel, Check Point and Watchguard devices. The tool can't fingerprint every VPN model, but it can reveal the type of authentication used in the VPN – useful information for a prowling cracker. Other tools, like IKEProbe and IKECrack, take advantage of weaknesses in the pre-shared key (PSK) authentication used in IPSec VPNs. The hashes captured by these tools can then be run through ordinary password crackers, such as Cain and Abel, to steal passwords for malicious access to the VPN and, of course, the corporate network.

For SSL VPNs, the same tools for scanning a Web application can be used. Tools can check for Web threats like cross-site scripting (XSS), SQL injection, buffer overflows, weak authentication and old-fashioned parameter manip-

ulation. The scan results can be followed by either automatic or manual tests to verify the vulnerabilities. Again, an SSL VPN is just a Web application. Test it like one.

Finally, IPSec VPNs, like any firewall or network device, have default user accounts. These accounts are used for initial installation and aren't needed after that. Either remove them or change their names, where possible. The same goes for any administrative accounts used for routine maintenance. Change default passwords.

A VPN isn't sacred. It's a network device like any other with flaws, blemishes and vulnerabilities. But, with proper pen testing, it can be hardened and secured, and effectively protect your network gateway.

About the author: *Joel Dubin, CISSP, is an independent computer security consultant in Chicago. He is a Microsoft MVP in security, and his expertise is in Web and application security. He is also the author of The Little Black Book of Computer Security available from Amazon.*

Client-side security considerations for SSL VPNs

By Lisa Phifer, Vice President, Core Competence, Inc.

Companies tired of VPN client software installation and configuration are being increasingly drawn to “clientless” solutions like SSL VPNs. However, using a browser-based VPN to go “clientless” still requires client-side vulnerability analysis and mitigation.

The lure of SSL VPNs

According to Frost and Sullivan, the SSL VPN market exploded in 2002, growing at a compound annual rate of 49% through 2010. The big draw? SSL VPNs leverage browsers present on nearly every desktop and handheld to avoid adding software. Security policy can be largely dictated by the VPN gateway, reducing remote configuration.

Circumventing these IT pain points should cut the cost of remote access.

What’s more, browser-based VPNs enable remote access from more locations. Travelers can use public PCs at business centers and Internet cafes. Teleworkers can use home PCs without IT oversight. Business partners can use PCs administered by other companies. Permitting remote access from these venues increases convenience, availability and productivity. But, there’s a catch: loss of IT control over the hosts used for remote access.

Leave nothing behind

Most public PCs contain traces of past user activity: Outlook inboxes filled with private e-mail, browser caches containing Webmail text and password-laced cookies, and file attachments saved to temp directories. Leaving this sensitive data behind on public PCs poses considerable risk, but relying on users to clean up after themselves is a very bad idea. Many have no idea what they leave behind; even those who know how to wipe their tracks clean make mistakes.

To address this risk, most SSL VPNs take steps to automatically clean up after each remote access session, no matter who owns the remote PC. Features to look for when considering SSL VPN products include:

- **Secure logout**—Forced session disconnection and browser window close, typically based on centrally defined inactivity or duration timeouts.
- **Credential scrubbing**—Deleting cached credentials at session end or preventing them from being cached on the client in the first place.
- **Temp file clean up**—Deleting files created during the session or blocking their creation, including cached pages, offline content and downloaded programs.
- **Cookie blocking**—Removing cookies at session end, or better yet, no personally identifiable or reusable information written to cookies during sessions.
- **Auto forms completion disabling**—Avoiding client storage of data entered in private Web page forms that might otherwise be visible to subsequent users.

- **Personal information profile disabling**—Preventing access to, and use of, user data commonly integrated with browsers, like Outlook Address Book entries.
- **Browser history removal**—Stopping VPN URLs from being used as a launch point for common Web server attacks (e.g., password-guessing, DoS floods, script injection).

Prevent tunnel compromise

Post-session clean up is essential, but it doesn't go far enough. PCs available for public use in cafes, airports and conference centers are readily accessible to strangers 24/7, greatly increasing the risk of compromise. Attackers can install packet-capture tools, keystroke loggers and even desktop session recorders to obtain usernames, passwords and private data. Spyware, remote access Trojans and denial-of-service zombies can be implanted to probe or attack corporate resources during active VPN sessions.

To prevent IPsec/L2TP/PPTP VPN tunnel compromise on company laptops, most companies mandate client-side personal firewalls, antivirus software and up-to-date security patches. These measures are typically part of the "remote access bundle" that IT installs and configures on every host, either directly or by supplying software and instructions to employees. For "clientless" access, this may not be practical or possible.

Some argue that SSL VPNs pose less risk because network VPNs use secure tunnels to connect remote hosts to private networks, while SSL VPNs typically connect individual client applications to private servers. A narrower window of opportunity can eliminate some vulnerabilities—for example, preventing Trojan access to other systems and ports. However, this really depends upon the product and policy granularity.

To implement more granular policies, look for products that can define access rights based not just on application, but also on individual commands (e.g., permit read but not write or delete) and user/group-specific URLs and objects (e.g., folders, accounts). Granularity is a double-edged sword: Look for incremental or hierarchical grouping features, and design your policies with both maintenance and performance in mind.

These are just some of the steps you can take to address client-side security concerns for network-level and browser-based VPNs. Keep in mind that all VPNs pose some risk; effective VPN deployment requires understanding and managing inherent vulnerabilities. Going "clientless" with an SSL VPN may avoid new client-side software, but it still requires client-side vulnerability analysis and mitigation.

About the author: *As owner of consulting firm Core Competence, Lisa Phifer advises companies regarding security needs, product assessment and the use of emerging technologies and best practices. She has been involved in the design, implementation and evaluation of security and network management products for more than 20 years.*

Quiz: IPsec vs. SSL VPNs

Test your knowledge of IPsec and SSL VPNs with this quiz, and click through to our additional resources to help you determine which technology best suits your organization's needs.

- 1.) Which type of VPN encryption sets up a secure, encrypted link between two points, but does not encrypt the headers of the data packets?**
 - a. Transport encryption
 - b. Tunneling encryption

- 2.) Which of the following is a basic requirement of an SSL VPN?**
 - a. Proxy access and protocol conversion
 - b. Remote-access orientation
 - c. Extranet support
 - d. Highly granular access controls
 - e. All of the above

- 3.) In which scenario is an IPsec VPN generally considered a better solution than an SSL VPN for remote access?**
 - a. Telecommuters coming from fixed sites, using managed corporate devices and terminating in a secure, private network on either side.
 - b. Telecommuters without fixed access who want to come in from a variety of sites.

- 4.) Which layer of the network does an IPsec VPN operate on?**
 - a. Layer 3
 - b. Layer 4
 - c. Layers 4 through 7
 - d. None of the above

- 5.) Which of the following operational modes is the simplest and most usable, as well as the most supported by SSL VPNs?**
 - a. Application translation
 - b. Port forwarding
 - c. Proxy
 - d. Network extension

6.) Which of the following describes an IPsec VPN?

- a. Requires host-based clients and hardware at a central location. Users have full office functionality, but there's very little granularity in access control.
- b. Does not require a client download. Remote connections made via a Web browser or a downloadable Java or ActiveX agent. Role-based access can be assigned for each user, and application and client administration is eliminated.

7.) True or False: SSL VPNs are inherently less secure than IPsec VPNs.

- a. True
- b. False

8.) Encapsulating Security Payload (ESP) allows for...

- a. Authentication of the sender of data
- b. Encryption of the data
- c. Both authentication of the sender and encryption of the data
- d. None of the above

9.) Which of the following features of SSL VPNs help avoid the risk of leaving sensitive information on public PCs used to access a corporate network?

- a. Secure logout
- b. Credential scrubbing
- c. Auto forms completion disabling
- d. All of the above

10.) What is the transmission of data through a public network in such a way that the routing nodes in the public network are unaware that the transmission is part of a private network?

- a. Tunneling
- b. Virtual private network
- c. Output feedback
- d. Promiscuous mode

[Click here for answers.](#)

IPsec vs. SSL VPNs quiz answers

1.) The correct answer is: **a. Transport encryption**

From Crypto basics: VPNs:

VPNs are capable of encrypting two different ways: transport and tunneling. The transport encryption sets up a secure, encrypted link across the Internet wires, and it encrypts the data (payload) you are sending to the other end. This is the equivalent of the delivery truck carrying a package via the underground passageway. (I'm not using the word tunnel here because I don't want to confuse you!) The encryption is invisible to the user—other than passwords, passphrases, or a special card to plug into the computer, the user doesn't have to press a button that says "encrypt" or "decrypt." All the data in transit is protected from sight. The only drawback to transport encryption is the fact that the headers on the data are sent in the clear. In effect, that's like disguising the package and then putting a label on it that says what's inside. Maybe not the smartest thing to do considering that intruders may occasionally gain access.

2.) The correct answer is: **e. All of the above**

From IPsec and SSL VPNs: Solving remote access problems:

Six Basic Requirements of an SSL VPN

- Proxy access and protocol conversion
 - o End user HTTPS to proxy; proxy HTTP[S] to resources
 - o Application translation (e.g., HTTPS to SMB/CIFS)
- Clientless (sic) Access
 - o Works within the browser
 - o No thick/thin client required
- Remote-access Orientation
 - o No site-to-site
 - o Designed with simplicity and ease-of-use over security
- Extranet Support
 - o End-user has only a casual connection to resource
- Highly Granular Access Controls
 - o Primarily a security appliance, not an access method
- SSL Transport

3.) The correct answer is: **a. Telecommuters coming from fixed sites, using managed corporate devices and terminating in a secure, private network on either side.**

From Letting telecommuters in—Your VPN alternatives:

The most secure VPN is the traditional arrangement with the telecommuter coming from a fixed site, ideally using a managed, corporate device and terminating in a secure, private network on either side. Quite a bit of effort can go into setting up this arrangement; you need to see that hardware, software and settings, as well as authentication, are set up perfectly and maintained on both ends, despite user changes to software, firmware and hardware, but the security can be worth the trouble. Let's throw out some protocols—literally.

There are three or four at this end of the pool. Only one from this group is secure enough to take seriously: IPsec, especially in conjunction with L2TP.

IPsec is the standard to buy; it encrypts at the packet level. PPTP has weak encryption keys, weak password hashing and unauthenticated control traffic. L2TP traffic can be read by network sniffers. However, when combined with IPsec for encryption, L2TP becomes unreadable and offers IPsec authenticated access for multiple protocols. Just be sure the device you buy supports the combined IPsec and L2TP standard.

4.) The correct answer is: **a. Layer 3**

From Is IPsec on borrowed time?:

IPsec VPN is a layer 3 technology that provides a secure tunnel between a remote location and the corporate network.

5.) The correct answer is: **c. Proxy**

From IPsec and SSL VPNs: Solving remote access problems:

Listed in order of simplicity and usability: From simplest and most usable to most complex and difficult

Not every SSL VPN product supports all four modes. Listed in order of support (most supported to least)

- Proxy
- Application Translation
- Port Forwarding
- Network Extension

6.) The correct answer is: **a. Requires host-based clients and hardware at a central location. Users have full office functionality, but there's very little granularity in access control.**

From Is IPsec on borrowed time?:

IPsec VPN is a layer 3 technology that provides a secure tunnel between a remote location and the corporate network. It requires host-based clients and expensive hardware at a central location; ongoing configuration maintenance and account administration are heavy burdens. Users have full office functionality using IPsec VPNs, but there's very little granularity in access control. Access is generally permit or deny with most shared network resources available to any user.

7.) The correct answer is: **b. False**

From VPN fast facts: True or false?:

While they differ architecturally, both VPNs can be deployed securely—or poorly. Security builds upon standards and products that implement them, but ultimately depends upon appropriate deployment and sound policy definition.

8.) The correct answer is: **c. Both authentication of the sender and encryption of the data**

From the SearchSecurity.com Glossary:

IPsec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well.

9.) The correct answer is: **d. All of the above**

From Client-side security considerations for SSL VPNs:

Most SSL VPNs take steps to automatically clean up after each remote access session, no matter who owns the remote PC. Features to look for when considering SSL VPN products include:

- Secure logout—Forced session disconnection and browser window close, typically based on centrally defined inactivity or duration timeouts.
- Credential scrubbing—Deleting cached credentials at session end or preventing them from being cached on the client in the first place.
- Temp file clean up—Deleting files created during the session or blocking their creation, including cached pages, offline content and downloaded programs.
- Cookie blocking—Removing cookies at session end, or better yet, no personally identifiable or reusable information written to cookies during sessions.
- Auto forms completion disabling—Avoiding client storage of data entered in private Web page forms that might otherwise be visible to subsequent users.
- Personal information profile disabling—Preventing access to, and use of, user data commonly integrated with browsers, like Outlook Address Book entries.
- Browser history removal—Stopping VPN URLs from being used as a launch point for common Web server attacks (e.g., password-guessing, DoS floods, script injection).

10.) The correct answer is: **a. Tunneling**

From the SearchSecurity.com glossary:

Tunneling, also known as "port forwarding," is the transmission of data intended for use only within a private, usually corporate network through a public network in such a way that the routing nodes in the public network are unaware that the transmission is part of a private network. Tunneling is generally done by encapsulating the private network data and protocol information within the public network transmission units so that the private network protocol information appears to the public network as data. Tunneling allows the use of the Internet, which is a public network, to convey data on behalf of a private network.

How'd you score?

9-10 correct: VPN virtuoso

6-8 correct: VPN savvy

3-5 correct: VPN novice

Resources from SonicWALL



[Stratecast: An SSL VPN Selection Framework - One Size Does Not Fit All](#)

[Best Practices for Secure Remote Access - A Guide to the Future](#)

[IPSec vs. SSL VPN: Transition Criteria and Methodology](#)

About SonicWALL

SonicWALL® is a recognized global leader in secure networking infrastructure and data protection. The company designs, develops and manufactures solutions that provide comprehensive network and data protection including network security, secure remote access, Web and e-mail security, and backup and recovery. With appliance-based solutions—as well as value-added subscription services—SonicWALL's rich portfolio of solutions delivers the comprehensive enterprise-class Internet and data protection necessary to safeguard organizations of all sizes. In July of 2007 SonicWALL acquired Aventail Corporation, a leading SSL VPN solution provider. For more information, go to www.sonicwall.com.