SSL VPN Security - Cisco

SSL VPN Security

Introduction

In recent years, various virtual private network (VPN) technologies have been widely used to provide secure site-to-site connectivity and remote access. There are many reasons for such overwhelming adoption and business success; two major factors are total ownership cost savings and productivity enhancements. The total ownership cost can be considered as the initial deployment cost plus the cost of user training, support, and facility maintenance over time. Productivity enhancements can be measured in terms of tool effectiveness, user time savings, usability improvements, and user satisfaction.

Secure Sockets Layer (SSL) VPN is an emerging technology that provides remote-access VPN capability, using the SSL function that is already built into a modern web browser. SSL VPN allows users from any Internet-enabled location to launch a web browser to establish remote-access VPN connections, thus promising productivity enhancements and improved availability, as well as further IT cost reduction for VPN client software and support.

Additional VPN background information is widely available. This paper addresses security issues and challenges associated with SSL VPN, including general VPN security and specific SSL VPN security, as well as endpoint device security and information protection. Security mechanisms that can be used for risk mitigation are also discussed.

Advantages of SSL VPN

SSL VPN has some unique features when compared with other existing VPN technologies. Most noticeably, SSL VPN uses SSL protocol and its successor, Transport Layer Security (TLS), to provide a secure connection between remote users and internal network resources. Today, this SSL/TLS function exists ubiquitously in modern web browsers. Unlike traditional IP Security (IPSec) remote-access VPN technology, which requires installation of IPSec client software on a client machine before a connection can be established, users typically do not need to install client software in order to use SSL VPN. As a result, SSL VPN is also known as “clientless VPN” or “Web VPN”.

Another SSL VPN advantage over IPSec VPN is its ease of use for end users. Different IPSec VPN vendors may have different implementation and configuration requirements. SSL VPN, on the other hand, requires only a modern web browser. End users may even choose their favorite web browsers without being restricted by the operating system.

One SSL VPN advantage for end users is in the area of outbound connection security. In most environments, outbound Secure HTTP (HTTPS) traffic, which is also based on SSL, is not blocked. This means that even if a particular local environment does not permit outbound IPSec VPN sessions (such restriction is not unusual), SSL VPN is likely free of such restriction.

There is a difference between a full VPN tunnel and an SSL-enabled proxy server. The latter is an application gateway that supports a certain type of applications. A complete SSL VPN, on the other hand, is a VPN that provides all VPN characteristics and local LAN user experience (in terms of network access). If application access requirements are modest, SSL VPN does not require additional client software to be installed on the endpoint device. For broader application access, a dynamically downloadable tunneling client is typically delivered when needed to the client machine to support such full SSL VPN capabilities.

Security Risks

While providing significant business benefits and cost savings, VPN technologies (SSL VPN included) come with their own security issues. These issues must be dealt with appropriately to ensure the confidentiality and integrity of data and information, as well as overall corporate network security. The following discussion first addresses the general security risks associated with using computers via VPN to access a company's internal network, then addresses SSL VPN security risks.

General Security Risks

User-credential-related risks
VPNs provide easy access from the Internet into a corporate network and its internal resources. VPN security is only as strong as the methods used to authenticate the users (and the devices) at the remote end of the VPN connection. Simple authentication methods based on static passwords are subject to password "cracking" attacks, eavesdropping, or even social engineering attacks. Two-factor authentication, which consists of something you know and something you have, is a minimum requirement for providing secure remote access to the corporate network. In some cases, three-factor authentication may be necessary; this form of authentication adds one more requirement—something you are (a biometric such as fingerprint or iris scan, for example).

Spread of viruses, worms, and Trojans from remote computers to the internal network
Remote access is a major threat vector to network security. Every remote computer that does not meet corporate security requirements may potentially forward an "infection" from its local network environment to an organization's internal network. Up-to-date antivirus software on the remote computer is required to mitigate this type of risk.

Split tunneling
Split tunneling takes place when a computer on the remote end of a VPN tunnel simultaneously exchanges network traffic with both the shared (public) network and the internal (private) network without first placing all of the network traffic inside the VPN tunnel. This provides an opportunity for attackers on the shared network to compromise the remote computer and use it to gain network access to the internal network. A host-based firewall is an effective way to defend against network-based attacks. Furthermore, many organizations have chosen to disallow split tunneling.

SSL VPN Risks

Security risks more specific to SSL VPN are discussed below. Many of these risks are related to the fact that SSL VPN can be used on public machines.

Lack of required host security software on public machines
SSL VPN makes it easy and convenient to connect from anywhere on the Internet to a corporate internal network. However, public machines used for SSL VPN may not have the required antivirus software installed and properly maintained; also, they typically do not have a host-based firewall installed and enabled. These public machines cause a major threat when used for SSL VPN. They may spread viruses, worms, and Trojan horses—and may even become a back door for malicious attackers. Even strong user authentication will fail to protect the network if a remote computer has been compromised, because an attacker can "piggyback" onto a live session via the Trojan and target the internal resources.

Physical access to shared machines
If a remote computer has an established network connection to your internal network, and the user leaves the session open, your internal network is now exposed to people who have physical access to the machine. Unauthorized personnel may use this computer to explore and attack your internal resources. SSL VPN significantly increases this type of risk—a connection can be started from any Internet-based machine. The physical access nature of shared machines adds numerous risks besides providing unauthorized network connection to the corporate internal network; these are discussed later in this paper.

Keystroke loggers
SSL VPN client machines may be more vulnerable to keystroke loggers because publicly accessible

computers (at kiosks, for example) may be involved. These computers may not meet your organization's security policies and standards. When these machines are compromised, keystroke loggers may allow interception of user credentials and other confidential information. It is possible to install malicious software or even hardware-based keystroke loggers to gather sensitive information.

Endpoints—loss of sensitive information and intellectual property
Sensitive information covers a wide range of items, including user credentials (account name/password), sales forecasts, internal personnel information, and customer information. Intellectual property includes source code, company, and even third-party (under NDA) design and technology information. Critical information may be left on a remote computer if the computer is not properly protected—this is especially important when the remote computer is shared with the public. Endpoint protection is key to addressing this type of risk. User awareness and education also play critical roles.

Man-in-the-middle attacks
In a man-in-the-middle attack, the attacker intercepts user traffic to capture credentials and other relevant information. The attacker then uses this information to access the actual destination network. During the process, the attacker typically serves as a proxy/gateway that presents a false SSL VPN site to the user; this proxy/gateway passes whatever authentication the user enters on to the real destination site. Depending on the sophistication of the malicious proxy/gateway, many actions may be taken once access to the internal network is gained. Some information may be sent back to the user, or the user may be terminated with a fake "service not available" message.

This attack typically works when a user does not properly verify that he or she is communicating with the real SSL VPN headend website. The general corporate user typically does not have sufficient knowledge to read and to verify that an SSL certificate belongs to an appropriate party before connecting; often, the user clicks "yes" and accepts a certificate permanently. And in some kiosks, the public machines might have their web browser security settings so low that no warning is issued when an SSL certificate appears suspicious.

Hardware limitation
Certain two-factor authentication mechanisms like smart cards do not work with certain public machines. For example, some kiosk machines might not have the necessary hardware (USB ports, for example) available to plug in the card reader.

Risk Mitigation

While many vendors and products are available in the market today, they may not all provide sufficient risk mitigation mechanisms and capabilities. A thorough planning and comparison process can help you identify what is most appropriate and effective to protect your organization. Below is a detailed analysis of the security measures that should be applied when implementing SSL VPN.

Security policies and secure access through strong user authentication
SSL VPN deployment and users of SSL VPN should comply with the remote access and VPN security policies in your organization. Strong user authentication is a top priority; several choices are available to achieve this purpose. Typically, one starts by implementing two-factor authentication techniques. Examples include hardware tokens, digital certificates (as a form of user authentication), and smart cards. In addition, your organization should also clearly state what types of host security requirements must be met (such as personal firewall, antivirus, hot fixes, or security patches). Other decisions should include whether your organization permits split tunneling.

Host identity verification
There is a difference between trusting a user (after passing strong user authentication) and trusting that user's computer. While the former has traditionally been emphasized, only recently has the latter been given sufficient attention (see Trusted Platform Module - TPM). As discussed earlier, a Trojan-laden computer defeats strong user authentication. But a "company computer", which is typically supported and managed according to corporate security policies, typically deserves more trust than a "non-company computer". A secure SSL VPN infrastructure should allow you to verify a remote host's identity by checking on predefined end device parameters. Examples include registry entries, special files in a specified location, or digital certificates (as a form of device authentication). The host identity information can be used to make your access permission decisions.

Host security posture validation
Once a remote computer is allowed access to the VPN, it becomes an extension of your organization's network. Host security to protect this endpoint device is vital to protect both the data residing on the host and the connection to your internal network. Your SSL VPN infrastructure should be able to validate host security posture by examining version of antivirus software, personal firewall, service updates, security patch levels, and possibly additional customized scripts and files. This validation is critical to ensure compliancy with your corporate security policies and standards.

Secure desktop
What do you do if a remote computer does not meet your rigorous corporate security policies and standards? A major SSL VPN business benefit is to allow users to "VPN in" from any Internet-based computer. Many of them are non-company assets that typically would not meet your security policies and standards. To solve this dilemma, some recent SSL VPN products provide the ability to create a safe "sandbox" or "secure desktop" on the remote computer. This secure desktop is typically protected from other processes on the computer and has an "on-the-fly" encrypted file system. Malicious codes, even if they are present on the computer, are not able to access the content stored in the secure desktop. This type of implementation also helps ensures that data will be erased in a secure manner at the end of the session.

Cache cleaning
To further protect confidential information and intellectual properties, advanced SSL VPN implementation should allow deletion of all traces of session data from locations such as browser history, Internet temporary files, and cookies. The cache cleaning feature mitigates the risk of leaving sensitive information behind.

Keystroke logger detection
Ideally, malicious codes such as keystroke loggers can be detected before a user starts a VPN session. Recent SSL VPN products offer such security features. They allow keystroke logger detection before a user login session is performed. Be aware, however, that different vendors may offer varying degrees of success and effectiveness—and most are powerless in dealing with hardware-based keystroke loggers.

Configuration consideration
Check your intended SSL VPN products to see if they allow you to configure the following:
- Session timeouts—A short timeout (typically set to 10 minutes or less) reduces the opportunity for unauthorized personnel to gain access to your internal network via a public computer.
- SSL version verification—The SSL server function of the VPN concentrator must be configured to reject SSL 2.0 connections. SSL version 2.0 contained many security flaws, which have been fixed in SSL version 3.
- Server certificate support—To create the SSL/TLS tunnel and to prevent server spoofing (man-in-the-middle attacks), the VPN concentrator should install a server certificate chained to your corporate root certificate authority. Alternatively, you should use a server certificate issued by a trusted certificate authority.

To further reduce the risks caused by remote computers, you may consider imposing additional security restrictions. One option (based on the remote computer's host security parameters) is to require SSL VPN sessions to start from certain pre-approved source IP addresses and to restrict access to a limited list of resources only, if the remote computer does not meet your existing host security requirements. Another option (based on the remote computer's device identify) is to severely restrict access to a minimum number of applications/resources only, if the remote computer cannot be verified to be a "company asset". The choice of these restricted applications/resources should be such that they provide basic user needs without exposing sensitive information.

User education and security awareness
User education and security awareness is an integral component of an organization's overall security effort. SSL VPN user security awareness campaigns may focus on the following:
- Awareness information on why VPN in general and SSL VPN in particular present security risks to your organization
- Discouraging use at public terminals that do not meet your corporate security policies and standards
- Encouraging users to exercise security precautions, such as terminating VPN sessions and clearing documents/information before leaving a public computer

- Tips that remind users to pay attention to URL details and to examine the server certificate (via the little gold padlock in the corner of the web browser, for example) to guard against man-in-the-middle attacks.

Conclusion

SSL VPN promises to provide more productivity enhancements, improved availability, and further IT cost savings. SSL VPN security offers yet additional information security challenges. Successful SSL VPN deployment and operations involve managing security risks while supporting business needs. The security risk analysis and risk mitigation mechanisms discussed in this paper should help you deploy and secure SSL VPN in your organization.

Acknowledgements

The author Steven Song is a Security Architect for Corporate Security Programs Organization at Cisco Systems Inc. and specializes in network security.

References

Transport Layer Security (TLS):
http://www.faqs.org/rfcs/rfc2246.html

Trusted Platform Module (TPM):
https://www.trustedcomputinggroup.org/downloads/specifications/tpm/tpm

Security problems fixed in SSL version 3:
http://www.eucybervote.org/Reports/MSI-WP2-D7V1-V1.0-02.htm