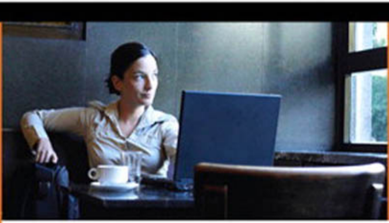
CISCO



SECURITY

SSL Remote Access VPNs

An introduction to designing and configuring
SSL virtual private networks

Jazib Frahim, CCIE® No. 5459
Qiang Huang, CCIE No. 4937

ciscopress.com

SSL Remote Access VPNs

Jazib Frahim, Qiang Huang

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America

First Printing June 2008

Library of Congress Catalog Card Number: 2005923483

ISBN-13: 978-1-58705-242-2

ISBN-10: 1-58705-242-3

Warning and Disclaimer

This book is designed to provide information about the Secure Socket Layer (SSL) Virtual Private Network (VPN) technology on Cisco products. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States, please contact: **International Sales** international@pearsoned.com

Introduction

This book provides a complete guide to the SSL VPN technology and discusses its implementation on Cisco SSL VPN–capable devices. Design guidance is provided to assist you in implementing SSL VPNs in an existing network infrastructure. This includes examining existing hardware and software to determine whether they are SSL VPN capable, providing design recommendations, and guiding you on setting up the Cisco SSL VPN devices.

Toward the end of Chapters 5 and 6, common deployment scenarios are covered to assist you in deploying an SSL VPN in your network.

Who Should Read This Book?

This book serves as a guide for network professionals who want to implement the Cisco SSL VPN remote access solution in their network to allow users to access the corporate resources easily and safely. The book systematically walks you through the product or solution architecture, installation, configuration, deployment, monitoring, and troubleshooting the SSL VPN solution. Any network professional should be able to use this book as a guide to successfully deploy SSL VPN remote access solutions in their network. Requirements include a basic knowledge of TCP/IP and networking, familiarity with Cisco routers/firewalls and their command-line interface (CLI), and a general understanding of the overall SSL VPN solution.

How This Book Is Organized

Part I of this book includes Chapters 1 and 2, which provide an overview of the remote access VPN technologies and introduce the SSL VPN technology. The remainder of the book is divided into two parts.

Part II encompasses Chapters 3 and 4 and introduces the Cisco SSL VPN product lines, with guidance on different design considerations.

Part III encompasses Chapters 5 through 7 and covers the installation, configuration, deployment, and troubleshooting of the individual components that make up the SSL VPN solution.

- Part I, "Introduction and Technology Overview," includes the following chapters:

  Chapter 1, "Introduction to Remote Access VPN Technologies": This chapter covers the remote access Virtual Private Network (VPN) technologies in detail. Protocols, such as the Point-to-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPsec), Layer 2 Forwarding (L2F), Layer 2 Tunneling Protocol (L2TP) over IPsec, and SSL VPN, are discussed to provide readers with an overview of the available remote access VPN technologies.

  Chapter 2, "SSL VPN Technology": This chapter provides a technology overview of the building blocks of SSL VPNs, including cryptographic algorithms, SSL and Transport Layer Security (TLS), and common SSL VPN technologies.

- Part II, “SSL VPN Design Considerations and Cisco Solution Overview,” includes the following chapters:

  Chapter 3, “SSL VPN Design Considerations”: This chapter discusses the common design best practices for planning and designing an SSL VPN solution.

  Chapter 4, “Cisco SSL VPN Family of Products”: This chapter discusses the SSL VPN functionality on Cisco Adaptive Security Appliance (ASA) and Cisco IOS routers and provides product specifications that are focused on SSL VPNs.

- Part III, “Deploying Cisco SSL VPN Solutions,” includes the following chapters:

  Chapter 5, “SSL VPNs on Cisco ASA”: This chapter provides details about the SSL VPN functionality in Cisco ASA. This chapter discusses clientless and full tunnel SSL VPN client implementations and focuses on Cisco Secure Desktop (CSD). This chapter also discusses the Host Scan feature that is used to collect posture information about end workstations. The dynamic access policy (DAP) feature, its usage, and detailed configuration examples are also provided. To reinforce learning, many different deployment scenarios are presented along with their configurations.

  Chapter 6, “SSL VPNs on Cisco IOS Routers”: This chapter provides details about the SSL VPN functionality in Cisco IOS routers. It begins by offering design guidance and then discusses the configuration of SSL VPNs in greater detail. The configurations of clientless, thin client, and AnyConnect Client modes are discussed. The second half of the chapter focuses on Cisco Secure Desktop (CSD) and offers guidance in setting up CSD features. To reinforce learning, two different deployment scenarios are presented along with their configurations. Toward the end of this chapter, SSL VPN monitoring through SDM is also discussed.

  Chapter 7, “Management of SSL VPNs”: This chapter discusses the central management of SSL VPN devices using Cisco Security Manager.

This chapter describes the following topics:

- SSL VPN resource access methods
- User authentication and access privilege management
- Security considerations
- Device placement and platform options
- Virtualization
- High availability
- Performance and scalability

CHAPTER 3

SSL VPN Design Considerations

This chapter discusses design issues you should consider when you build a Secure Socket Layer (SSL) Virtual Private Network (VPN) solution. Readers with experience managing a remote access solution, such as IP security (IPsec)–based remote access VPN, will recognize many common considerations that apply to SSL VPN-based remote access solutions. You will also encounter special considerations that pertain to the characteristics of SSL VPN technology.

No design can fit every network, because everyone's policy and business requirements are different. This chapter provides a list of common design aspects that you need to consider when you design and deploy an SSL VPN solution and possible solutions that you can apply.

Not All Resource Access Methods Are Equal

As mentioned in Chapter 2, "SSL VPN Technology," SSL VPN employs a variety of techniques, each of which has its unique characteristics in terms of user experience, user privilege requirements, and levels of access to the network resources. This is one of the major differences between SSL VPN and traditional remote access solutions, such as IPsec-based remote access VPN.

When you design an SSL VPN network, it is important to understand that not all access methods are equal and different access methods can be deployed to achieve different goals. You should ask yourself several questions when you evaluate SSL VPN technology and before you deploy an SSL VPN access method:

- What level of access does it provide?
- What operating systems does it support, for example, Windows, Linux, Mac, and mobile devices?
- What user privileges does it require?
- What level of access control can you apply?

Table 3-1 provides answers to common questions about SSL VPN access methods.

Table 3-1 *SSL VPN Resource Access Methods*

	Client-Side Agent Required	User Privilege Required	Access Ubiquity	Level of Access	Granular Access Control
Reverse-proxy	No	No	Most ubiquitous	Limited to applications that can be adapted to the web	Very granular application-level control
Port forwarding	Yes; Java applet or ActiveX control	Standard user; administrative privilege sometimes required	Medium	Limited mostly to static server-based TCP applications	Medium; controls client/server application access
Integrated terminal services	Yes	Might require administrative privilege	Medium; mainly Windows systems	Windows Terminal service, Citrix, VNC	Medium; provide only terminal services
Tunnel client	Yes	Typically requires administrative privilege to install the client for the first time	Least ubiquitous; usually limited to corporate-owned/trusted systems	Network-layer access; supports almost all applications	Low

This table compares the special characteristics of an SSL VPN to the traditional remote access VPN solutions. The same network resources can be accessed by using several resource access methods, each of which gives the user different experiences and calls for different system requirements. When you design your SSL VPN solution, it is important to understand this and choose the right access method for the right purpose. Here are some general considerations:

- The reverse-proxy-based method is the most ubiquitous access method and is good for almost all users. It can be applied to support mobile users or business partners who need to access a specific application through web browsers. The applications supported in this case are normally web-based e-mail applications such as Microsoft OWA (Outlook Web Access) and iNotes or a web-based business application, such as salesforce and Oracle iProcurement.
- As mentioned in Chapter 2, the reverse-proxy mode supports only a limited number of applications that can be made suitable for web use.

- The port-forwarding clients can be used to support business partners or contractors who need to access a very limited number of client/server applications that cannot be adapted to the web. As described in Chapter 2, when users use the port-forwarding technology, they often need to reconfigure the application to point to the local loopback address. This can be inconvenient for the users. As tunnel client technology has matured, many companies go directly to using tunnel clients to support various applications.
- Tunnel clients can be used to support power users that need full resource access. Because of their requirement of user privilege and their nature of full network access, tunnel clients are normally deployed on corporate-owned user systems, such as work laptops. Strong security control should be deployed to ensure the proper security posture of the endpoints and the security protection of the corporate networks.
- Some vendors do not use true reverse-proxy to support web browser–based access. A small applet (for example, ActiveX control) is downloaded and installed on the user's computer after the user signs on to the SSL VPN portal. The applet then intercepts the user's web request and sends it off to the established SSL VPN connection. These applet transactions can take place in a manner that is fairly transparent to the end user so that the user does not even realize that he or she is dealing with a client. In this case, you need to understand the operating system, user privilege, and browser setting requirements of the client-side applet (for example, allow ActiveX download and execution) to make sure that they fit into your deployment requirements.

Later sections of this chapter discuss the security and performance considerations of different access methods.

User Authentication and Access Privilege Management

Effectively managing the VPN users and their access privileges is the core consideration in any remote access VPN design. There are mainly two aspects:

- A scalable and secure solution to authenticate users
- Decisions on what access privilege to grant to the users based on various user and security attributes

Many organizations migrate from the existing IPsec-based remote access VPN solutions to SSL VPN, whereas other organizations simply add SSL VPNs to their existing remote access VPN. The good news is that SSL VPNs fit well into the existing authentication infrastructure.

User Authentication

Although this section focuses on user authentication, first step back to have a quick look at the big picture. AAA stands for *authentication* (which defines who you are), *authorization* (which defines what you are allowed to do), and *accounting* (which provides a record of what you did). User authentication is a key step in an SSL VPN solution. Aside from validating users' credentials, user authentication allows an SSL VPN gateway to assign the user to a policy group. The assignment is made by using a user's organization group information, which is derived during the authentication phase, along with other attributes, such as endpoint security posture and time of day. The policy group defines the authorization privileges of the users.

Choice of Authentication Servers

You have a wide variety of identity technologies to choose from for authenticating users. The common choices are passwords, RADIUS, TACACS+, one-time password (OTP) systems, public-key infrastructure (PKI), smart cards, and so on. For remote access VPN authentication, a two-factor OTP system provides the strongest security and manageability combination. It is also common for small- to medium-sized companies to leverage existing user directory infrastructure such as Lightweight Directory Access Protocol (LDAP), Windows NTLM, or Windows XP/2000 Active Directory for VPN user authentication. To use this, you need to apply and enforce strong password policies because the strength of the security relies on those policies.

The design of the AAA system can vary depending on the size of your network and the disparity of access methods. For an SSL VPN device, the choices of authentication servers fall mainly into two categories:

- **A dedicated AAA server running RADIUS:** The AAA server is the interface between the SSL VPN appliance and the identity servers, such as corporate LDAP servers or OTP systems. Cisco Secure ACS is an example of this type of AAA server. The SSL VPN appliance communicates with the AAA server using the RADIUS protocol. Often, the AAA server sends a query to the external identity databases for identity authentication, and returns the authentication result to the SSL VPN appliance. The AAA server can speak different protocol languages with various identity databases such as LDAP, SecureID, and Windows Active Directory. An advanced AAA server, such as Cisco Secure ACS, can also retrieve additional user attributes from the external user identity servers, such as the users' roles in the organization or the users' password expiration information. All these user attributes can be used later in the authorization phase to determine the access privilege.
- **An SSL VPN appliance communicating directly with the identity server:** In this case, the SSL VPN appliance needs to be able to communicate with various types of identity servers, such as LDAP, OTP systems, or Windows domain controllers. This becomes fairly common because most current SSL VPN vendors support multiple

types of authentication servers. This mode is most common to small- to medium-sized companies that do not have disparate access methods, and hence have no need to have a central root AAA system.

When you choose to use this method, pay attention to what additional information the SSL VPN appliance can retrieve from the authentication servers, other than the results of the user authentication. For the later authorization phase, it is often useful for the SSL VPN appliance to also be able to get the users' organizational information. Enabling the SSL VPN appliance with this additional capability requires more integration between the SSL VPN appliance and the authentication server.

AAA Server Scalability and High Availability

The scalability and availability of the AAA server directly affect the availability of your VPN network and the user experience.

For a small- to medium-sized VPN network, it is relatively easy to address this design issue. Because the number of the VPN users is relatively small, the scalability of the AAA server is less of an issue. Also, because small to medium deployment normally does not have dispersed Internet VPN access, the AAA servers normally reside on a local network, and network delay and resiliency are not problematic. You should have a backup or secondary AAA server to provide local high availability. Most SSL VPN appliances support checking a secondary AAA server in case the primary server is not available.

For a medium to large enterprise network, the scalability and resiliency of the AAA systems are important and need to be carefully designed. For a remote access VPN deployment, you probably need to integrate your authentication requirements with the AAA infrastructure that is already in place to support other access methods.

Some good design guidelines for deploying a Cisco Secure Access Control Server (ACS) have been documented in the white paper "Guidelines for Placing ACS in the Network," which can be found at http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_white_paper09186a0080092567.shtml. In this white paper, the general design recommendations documented for scalability, resiliency, and device placement should apply to most AAA server deployments.

The following sections briefly highlight the important factors that need to be considered.

AAA Server Scalability

When you consider AAA server scalability, keep the following points in mind:

- The maximum number of users supported by the AAA server.
- The number of authentication requests per second the AAA server can handle.
- The type of database. For an internal user database on the AAA server itself, check its scalability to find out how many local users can be defined.

AAA Server High Availability and Resiliency

When you consider AAA server high availability (HA) and resiliency, keep the following points in mind:

- Consider a local secondary AAA server.
- For dispersed network access and VPN geographic HA design, consider placing a AAA server at each location that has business-critical impact.
- Incorporate a robust AAA server database synchronization mechanism.

Resource Access Privilege Management

After user authentication, the remote access VPN device should be able to authorize the user with resource access privileges based on the user's attributes. As described earlier, because of the ubiquity of the SSL VPN, its design needs to ensure the integrity of the endpoint. Hence the resource authorization also goes beyond the standard user attributes to include other security attributes. The following is a list of attributes that can be used to determine resource access privilege:

- **Sign-in URL:** For an SSL VPN device that offers different sign-in URLs to different groups of users, the sign-in URL can be used to decide the type of resource this group of users is entitled to.
- **User's digital certificate:** The organization information in the user's certificates can be used to map users to corresponding roles that allow different resource access.
- The result of endpoint security assessment: This point is discussed in more detail within the context of the security considerations. In essence, the posture of the endpoint can be used as a dynamic factor to decide users' access privilege to sensitive corporate resources.
- Time of day.
- Browser types.
- **User attributes:** These are the typical user attributes in the user identity database. For example, the marketing group in the LDAP database can be mapped to an internal marketing group in the SSL VPN.

Some of these attributes, such as endpoint security posture and users' IP addresses, are collected prior to user authentication. Some of the attributes, such as endpoint security posture, should be periodically reevaluated during the user session to dynamically determine the user's access privileges based on the most current situation.

To clarify these concepts, we give an example of how an SSL VPN system can use some of these attributes to perform dynamic access privilege management. In this case study, a salesperson attempts to access corporate resources using an SSL VPN. Depending on the result of the endpoint assessment, the salesperson is granted different levels of resource access.

Scenario 1: Salesperson Accesses the VPN from a Kiosk Computer at a Sales Conference

Step 1 The salesperson initiates the VPN request by entering https://vpn.companyxyz.com into the browser.

Step 2 Upon receiving the access request, the SSL VPN appliance collects some user attributes and performs the endpoint security checking. The results are as follows:

IP address = Outside

Client digital certificate = Not present

Proper antivirus client installed and enabled = No

Step 3 Based on the results in Step 2, the SSL VPN chooses an authentication method for the user and performs user authentication:

Authentication method = Strong, OTP

Step 4 After successful user authentication, the SSL VPN appliance also retrieves the user's organization information through a separate authorization step:

User's organization group = Sales

Step 5 Based on the user attributes so far, the SSL VPN appliance maps the user to a VPN group or role:

VPN role = sales_insecure

Step 6 The sales_insecure role decides the user access privilege:

User privilege = Web access only

Session timeout = 30 minutes

Periodic security checking = Yes

Require secure desktop = Yes

Note: The secure desktop can be launched much earlier at the preauthentication phase based on the IP address attribute. This way, the user password entered into the client browser can be protected from software such as keystroke loggers.

Step 7 The salesperson logs in and starts to access the bookmarked web applications, such as OWA. More granular application-level access control can be applied at this phase.

Scenario 2: The Same Salesperson Accesses the VPN from a Corporate-Owned Laptop at Home

Step 1 The salesperson initiates the VPN request by entering https://vpn.companyxyz.com into the browser.

Step 2 Upon receiving the access request, the SSL VPN appliance collects some user attributes and performs the endpoint security checking. The results are as follows:

IP address = Outside

Client digital certificate = Yes

Proper antivirus client installed and enabled = Yes

Step 3 Based on the results in Step 2, the SSL VPN chooses an authentication method for the user and performs user authentication:

Authentication method = Strong, OTP

Step 4 After successful user authentication, the SSL VPN appliance also retrieves the user's organization information through a separate authorization step:

User's organization group = Sales

Step 5 Based on the user attributes so far, the SSL VPN maps the user to a VPN group or role:

VPN role = sales_secure

Step 6 The sales_secure role decides the user access privilege:

User privilege = Tunnel client

Session timeout = 12 hours

Periodic security checking = Yes

Require secure desktop = No

Step 7 The salesperson logs in and starts to access the corporate network using the tunnel client mode. Additional granular IP-based access control can be applied at this phase.

Security Considerations

A remote access VPN extends the perimeter of your network to the remote endpoints. An SSL VPN has been an entry point for security threats to enter the network. The ubiquity, versatility, and clientless nature of the SSL VPN provide significant business benefits and cost savings, but they also pose additional security challenges compared to traditional remote access VPNs.

The following sections first examine the security threats that need to be addressed in SSL VPN security design. The sections then cover some of the security design measures you can take that help to mitigate those threats.

Security Threats

The following sections look at the common security risks that are associated with SSL VPNs.

Lack of Security on Unmanaged Computers

As mentioned earlier, SSL VPNs can support users coming from any computer on the Internet, such as public domain machines (for example, kiosk PCs) that are not controlled by the corporate IT department. This department ensures that the machines have proper service packs and security software, such as antivirus software. This poses a major threat to security. If, for example, SSL VPN users sign in to the SSL VPN from a compromised or infected PC, they can become a source for spreading viruses, worms, network attacks, and Trojan horses into the corporate network.

Several other security risks mentioned in the sections that follow are also related to these security threats. In general, as you deal with uncontrolled endpoints, you face increased security risks.

Data Theft

Several types of security threats lead to data theft or password theft:

- **Sensitive data left in a browser's cache:** Web browsers cache the various web objects that users downloaded during browsing. This caching helps browsers to improve the browsing experience. The browser cache files are physically stored on the user's computer in predefined directories. For example, the Temporary Internet Files folder is used for Internet Explorer browsers. After users finish browsing and leave the computer, the browser cache is left on the computer and can be accessed by other users who later log on to the same computer. This can be a security risk in a kiosk scenario that uses SSL VPN clientless web access. In this case, a VPN user logs in to the SSL VPN portal from a kiosk machine to access corporate resources, such as e-mail or other business applications. During the session, the user can access sensitive documents through the web browser that caches the document on a local hard drive. After the user signs off and leaves, attackers can easily use the kiosk computer and collect the browser cache to retrieve the sensitive information.

- **Browser histories:** Similar to the browser cache, browser histories are stored by the browser to enhance the user experience. The browser histories reveal the user activities and internal web server structure. Similar to the browser cache, browser histories saved on unmanaged computers are vulnerable to data theft.
- **Browser cookies:** A cookie is a text-only string sent by a web server to a web browser. The cookie can reside in the browser's memory or be stored on a local hard drive. A cookie is often used for purposes such as authentication, tracking, and personalization, such as site preference. Depending on their usage and content, cookies could contain sensitive information about users. Similar to a browser cache, cookies saved on unmanaged computers are vulnerable to data theft.
- **Brower-saved forms and user passwords:** Similarly, browser-saved forms and user passwords are vulnerable to data theft and password theft.
- **Documents on unmanaged computers:** More generally, documents and other types of sensitive data left on the unmanaged computers are vulnerable to data theft. For example, it is common for a VPN user to temporarily download a sensitive document to the local computer for reading or editing and later forget to delete the sensitive document before logging off. Furthermore, even if the user deletes the files before the VPN logoff, it is fairly easy for attackers to recover the deleted files by using common file-recovery utilities that are readily available on the Internet.
- **Data theft and password theft using keystroke loggers or other Trojan horse programs:** In the SSL VPN web-based clientless mode, users can access corporate resources from an already compromised computer that contains malware. For example, loggers that are preinstalled by the attackers can capture user input, such as e-mail IDs and passwords, and take screen shots of the e-mails.

Man-in-the-Middle Attacks

There have been known man-in-the-middle (MITM) attacks to the SSL protocol, and this is how they can work. The attacker first launches an Address Resolution Protocol (ARP) spoofing attack or Domain Name System (DNS) spoofing attack to the SSL VPN user. The success of the attack will redirect the SSL traffic to the attack host that is configured with SSL proxy software. The attack host then acts as the destination web server by establishing an SSL connection with the user on one side and another SSL connection with the true destination web server on the other side, proxying the traffic back and forth. Because the attack host serves as the endpoint of the two SSL tunnels, it has the proper keys to decrypt the SSL traffic. In this attack, the attack host would need to present a spoofed digital certificate to the end users. In most cases, the web browser prompts the end user with a security alert. However, users often simply ignore the warning and proceed.

Web Application Attack

SSL and SSL VPNs do not have built-in mechanisms to detect application attacks such as SQL injections, buffer overflow attacks of web applications, directory traversal attacks, or cross-site scripting.

Spread of Viruses, Worms, and Trojans from Remote Computers to the Internal Network

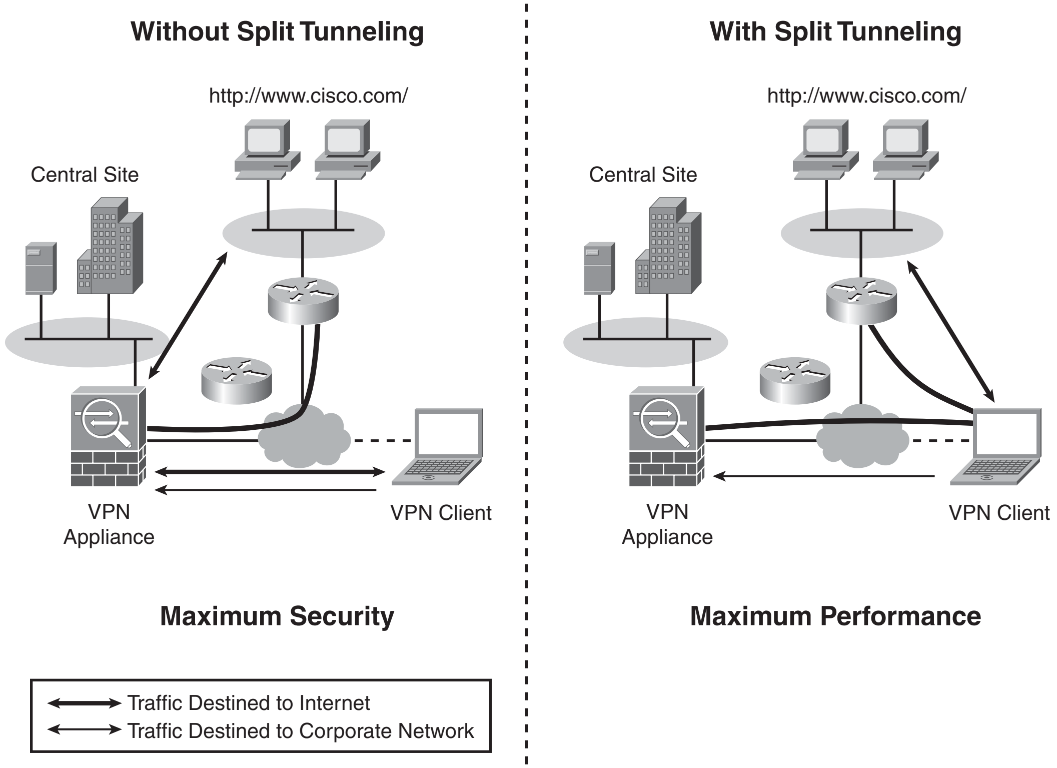
Corporate networks are vulnerable to the spread of viruses, worms, and Trojans when the SSL VPN users connect using the tunnel client mode. With the tunnel client mode, the endpoints are directly connected to the corporate network with full network-layer access. Endpoints might not be compliant with corporate security policy, which can require, for example, a proper Windows patching level or up-to-date antivirus DAT files. In this case, a high possibility exists that the endpoints will forward their infection to the internal network.

Split Tunneling

In a remote access VPN deployment, split tunneling gives the user direct access to a public network and VPN access to a private network simultaneously. The end user's computer becomes an extended Internet entry point to the corporate network. If no proper security measures are in place on the end user's computer, attackers have opportunities to compromise the computer from the Internet and gain access to the internal network through the VPN tunnel. For this reason, many organizations choose to disable split tunneling in their remote access VPN deployment. Figure 3-1 illustrates the split tunneling topology.

When split tunneling is disabled, one common issue is that users can no longer access the local LAN for tasks such as printing. The solution is to disable split tunneling but enable local LAN access. This way, the local LAN traffic will not be tunneled to the head-end SSL VPN gateway.

Figure 3-1 *Split Tunneling*



Password Attacks

The password attack is one of the most effective attacks. Common practices such as weak passwords and simple authentication methods such as static passwords are vulnerable to various attacks through password cracking or eavesdropping.

Security Risk Mitigation

The following sections detail the design considerations and security measures that you should consider when implementing an SSL VPN deployment.

Strong User Authentication and Password Policy

Using a strong user authentication mechanism is critical to the security of a remote access VPN. If possible, consider using two-factor authentication techniques, such as hardware tokens and smart cards. If static passwords are used, enforce strong password policy.

Choose Strong Cryptographic Algorithms

The SSL VPN device normally allows you to choose SSL/TLS protocol versions and cipher suites. Consider enforcing SSLv3 or Transport Layer Security (TLS) rather than SSL version 2. Also, choose strong cipher suites for data encryption and integrity. For example, choose Triple DES (3DES) or AES instead of RC4.

Session Timeout and Persistent Sessions

On the SSL VPN device, configure a short session timeout to prevent potential piggybacking unauthorized access to your internal network through a public computer.

Some vendors support persistent sessions that keep the SSL VPN session even after the user closes the browser without signing off. End users might think that closure of the browser is equal to termination of the session. This could lead to unauthorized access to the internal network from a public computer.

Endpoint Security Posture Assessment and Validation

A thorough preconnect security assessment is necessary. As discussed earlier, this helps prevent viruses, worms, and Trojan horses from spreading into the internal network and helps administrators make intelligent decisions on what access privilege to grant to the VPN users based on the endpoint security posture. The preconnect security posture validation can include the following aspects:

- **Location checking:** Using information such as IP address, Windows registries, or even PC screen banners, the SSL VPN device can figure out whether the user is coming from the Internet or from a corporate LAN, using corporate-owned PCs or a kiosk PC.
- **Security posture checking:** This refers to a checklist that can be used to determine whether the endpoint has proper antivirus protection, a personal firewall, or other required security agents that are installed and enabled with up-to-date policies.
- **Malware scans:** A malware scan can detect items such as keystroke loggers, spyware, and other Trojan horse programs on the endpoints.

VPN Session Data Protection

Although SSL VPNs provide secure communication, the session data is not encrypted on the endpoints and can be vulnerable to various malicious programs already on the compromised endpoints, such as a compromised kiosk computer. To protect the VPN session data, consider deploying secure desktop technology. 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, might not be able to access the content stored on the secure desktop. This type of implementation also helps ensure that data will be erased in a secure manner at the end of the session. Later chapters describe the Cisco Secure Desktop in more detail.

Techniques to Prevent Data Theft

To prevent the previously mentioned data theft, consider the following techniques:

- **Cookie management:** Many SSL VPN vendors support cookie management so that user cookies are not passed down to the endpoint.
- **Browser cache control:** HTTP (RFC 2616) offers several cache-control headers that can be used to control the caching behavior of the browser.
- **Cache cleaner:** Many SSL VPN vendors offer a cache cleaner that cleans the browser cache at the end of the session when users log off. The cache cleaner can delete the browser cache and browser histories. When deploying a cache cleaner, consider the following:
    - — Which folders does the cache cleaner clean? Some applications leave the cache in a different folder from the standard browser cache folder. Make sure that the cache cleaner can clean those locations. For example, the popular web-based e-mail application iNotes leaves its cache in a different folder than the standard browser cache folder. In this situation, the cache cleaner could miss the cache.
    - — Which operating systems does the cache cleaner support?
    - — Does the cache cleaner perform secure data sanitization? As mentioned earlier, a simple file delete is not secure. The secure cache cleaner complies to higher data sanitization standards than simple file delete to ensure that the deleted files can not be recovered later.
- **Secure desktop:** Because the secure desktop provides a sandbox that traps all the session data, deletion of the secure desktop at the end of the session provides a thorough data cleanup. This method is more thorough than the cache cleaner, which cleans only specific locations.

- **User education and security awareness:** These are also important aspects of the company security efforts. For SSL VPN security, focus on the following:
  - — Educate users on the potential security risks associated with accessing corporate resources from a public system.
  - — Encourage users to exercise security precautions when they use an SSL VPN on a public computer. This includes terminating the VPN session before leaving the computers, not leaving sensitive documents on the local hard drive of the public computer, and carefully examining certificate messages to guard against MITM attacks.

Web Application Firewalls, Intrusion Prevention Systems, and Antivirus and Network Admission Control Technologies

As mentioned earlier, the SSL protocol does not have a built-in mechanism to defend against web application attacks, and the SSL VPN tunnel client mode makes it easier for viruses and worms to spread into the Internet network from infected endpoints. Consider integrating threat defense technologies and security compliance technologies with your SSL VPN solution to mitigate these security risks:

- **Web application firewalls:** These are OSI Layer 7 firewalls that can understand and analyze HTTP application traffic to detect protocol conformance violations and attacks. They normally use a combination of protocol conformance enforcement and attack signature pattern-matching techniques to either prevent application anomalies or look for specific attack patterns.
- **Intrusion prevention systems (IPS) and gateway-level antivirus systems:** These systems offer a broader level of threat prevention. They help to prevent network attacks, viruses, worms, Trojan horses, spyware, and other security threats from entering the internal networks.
- **Network Admission Control (NAC):** This is an emerging technology that addresses security compliance enforcement issues. The basic idea is to make sure that the endpoints are compliant with corporate security policies, such as having proper antivirus software and Windows patching level, before the network devices grant users access to network resources. The endpoint security integrity checking that we just discussed is a form of Network Admission Control, and it can be integrated with the overall NAC framework to provide a consistent security validation for all types of network access methods.

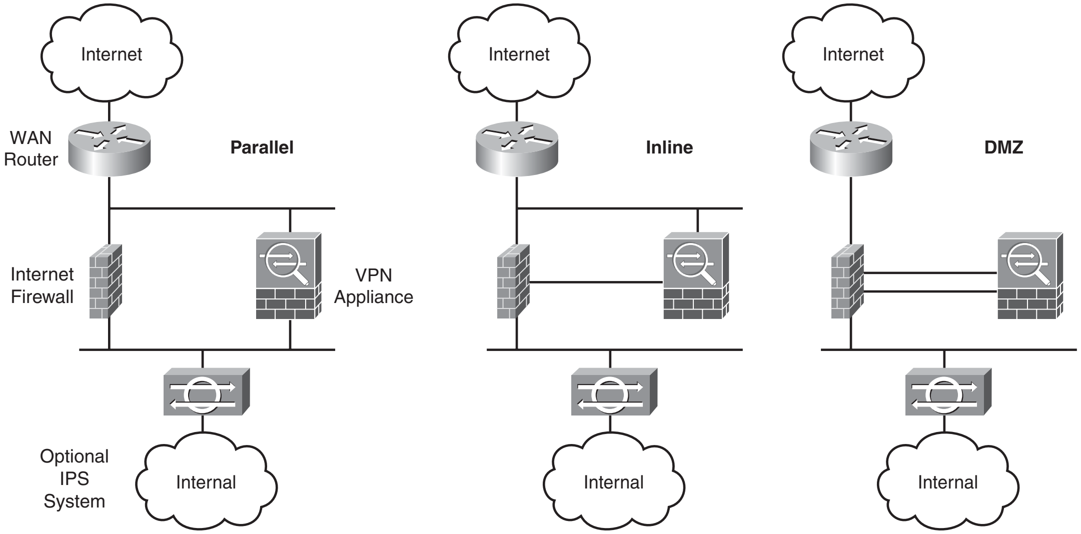
Device Placement

SSL VPN appliances are normally placed at the Internet edge of the corporate network. At the Internet edge of the network, other security devices are often deployed to protect the internal network from attacks. This section discusses the device placement issues you should consider when placing the SSL VPN devices among other security services at the edge.

For companies that already have an IPsec-based remote access VPN solution deployed, the device placement considerations should also apply to SSL VPN deployment.

Figure 3-2 shows three common designs for placing the SSL VPN appliances in a medium-sized network.

Figure 3-2 *SSL VPN Device Placement*



The device placement relationship between the SSL VPN appliance and Internet firewall is mainly based on the following two considerations:

- Do you trust the VPN traffic? In parallel mode, the VPN traffic is trusted and thus sent directly into the internal network after decryption. A high level of security risk is associated with this design. In the other two modes shown in Figure 3-2, VPN traffic is semitrusted and goes through a stateful firewall for access control and access logging.
- Do you need a firewall to protect the SSL VPN appliance? In parallel and inline mode, apply access control lists (ACL) on the WAN router to allow only the SSL VPN traffic to the SSL VPN appliance. In the DMZ mode, you can put that access control on the

Internet firewall and configure more advanced session control to guard against denial of service (DoS) attacks. Because the traffic is encrypted, the firewall will not be able to inspect much SSL traffic. Also, with this design, the firewall sees the VPN traffic twice: once before decryption and once after decryption. Hence, higher performance is required of the firewall.

In all cases, an optional IPS is placed after the VPN decryption to inspect the traffic for attacks. Depending on your security policy and requirements, the IPS can operate in an inline mode or promiscuous mode.

Platform Options

SSL VPNs are evolving in a manner similar to IPsec technology. This technology started as dedicated VPN concentrators and slowly became integrated with other network and security services. Two types of SSL VPN solutions are on the market: the pure-play SSL VPN appliances and the solutions that integrate SSL VPN functionalities with other network devices such as routers and firewalls. The emerging Unified Threat Management (UTM) market provides enterprises with options to deploy a single security device that offers multiple security services such as a firewall, a VPN, an IPS, antivirus and antispam software, and other content security services. Each solution has its merits and deployment benefits. Cisco offers the integrated solution with Cisco routers and Adaptive Security Appliances (ASA). A UTM appliance, the Cisco ASA appliances allows security administrators to deploy additional security services to the SSL VPN traffic.

Virtualization

The concept of virtualization is becoming more and more popular among enterprise customers. For SSL VPNs, the need for virtualization is natural. Enterprises like to provide different remote access VPN presences to different user groups, such as partners and different departments of employees. The following are some basic capabilities you should consider for a "virtualized" SSL VPN deployment:

- Provides a customized SSL VPN presence for individual user groups. For example, each business partner has its own SSL VPN sign-in page with a customized user interface.
- Provides customized authentication methods and VPN group policies for different user groups.
- Provides management roles for running each VPN separately.
- Has total separation of different VPNs in terms of system resources, routing tables, user databases, and policy management interfaces.

Some SSL VPN vendors supply the first three capabilities in the previous list without having to provide a full virtualized implementation. For each VPN user group, the SSL

VPN provides a dedicated sign-in URL. For example, partner A has a sign-in URL of https://www.companyxyz.com/vpn_for_partnerA, and partner B has a different sign-in URL of https://www.companyxzy.com/vpn_for_partnerB. Each sign-in URL has a customized user interface, such as a logo, page layout, and resource bookmarks. Each sign-in URL is associated with a different set of authentication methods and policy flows that are also specifically designed to meet different user group requirements. To the end user, the experience is "virtualized." However, from the SSL VPN system perspective, it is not virtualized.

The fourth capability in the previous list calls for a true virtualization, not only at the user level but also at the system resource level and policy management level. This is normally a requirement for service providers who provide managed remote access VPN services to multiple customers. These customers often demand total traffic and resource and management separation from other VPN customers. This can also be a requirement for large enterprises that have remote access VPNs for different trade partners.

High Availability

The high availability (HA) consideration for a remote access VPN deployment has two parts: local and geographic HA.

Local HA methods include the following:

- **Hot standby failover:** The two SSL VPN appliances are in an active-passive failover session. Common failover protocols include Virtual Router Redundancy Protocol (VRRP) and Hot Standby Routing Protocol (HSRP). A stateful failover synchronizes the SSL VPN session information between the two units to ensure minimum user disruption during the failover.
- **Active-active failover:** Both units are active and handle traffic during the normal state. Some administrators like to oversubscribe the resource and have both units working in full or higher than 50 percent capacity. This could lead to a domino effect. For example, when failure occurs, the failover unit will be overwhelmed by the aggregated user requests.
- **Multiunit clustering:** This is similar to active-active failover but with more than two units. The clustering is mainly used to improve scalability, but it can also provide high availability.

Geographic HA extends the VPN resiliency beyond local network availability. The VPN appliances are placed in multiple locations to serve the local users and also work as backup appliances for other locations.

Performance and Scalability

Performance considerations for an SSL VPN design are a bit different from those of the IPsec-based VPN because of the multiple technologies that the SSL VPN features. When you try to determine the performance of an SSL VPN appliance, you need to be clear about which resource access method you have in mind. The performance of different access methods varies greatly. The following list outlines the performance characteristics of the two most popular access methods:

- **Reverse-proxy-based web access method:** This access method challenges performance and resources more than any other. The SSL VPN appliance needs to perform content rewriting for each web application page and object. This involves resource-consuming pattern searching and matching. The complexity of the web page, which includes the number of URLs and Java scripts, directly affects the performance of the system. Resources permitting, a performance testing using the web pages from your web application can give you a good estimate of real-world performance. Light Reading Lab published a test methodology for clientless performance measurement. It is posted at http://networktest.com/ssl03/ssl03meth.html.

  Consider enabling the server-side caching feature if it is available on your SSL VPN system. With caching enabled, the frequently accessed web content will be cached by the SSL VPN appliance after it is rewritten the first time.

- **Tunnel client mode:** This mode is less complicated than the clientless mode and has higher performance. Instead of having to be inspected and rewritten, the web content goes through the simple encryption process, which can be easily hardware accelerated.

Chapter 2 covers the potential performance challenge that occurs when SSL or TLS supports applications that use real-time protocols. You need to consider this when you need to support applications such as IP telephony.

The scalability of the SSL VPN network is normally addressed by clustering multiple units together. For example, Cisco Adaptive Security Appliances (ASA) support pay-as-you-grow clustering techniques. Enterprises can start with a small cluster, and as the company grows, VPN administrators can easily add more units to the cluster to support more users.

Summary

This chapter discussed some of the important design considerations in an SSL VPN deployment. The areas covered include the characteristics of various SSL VPN resource access methods, user authentication and access privilege management, security, device placement, platform options, virtualization, high availability, performance, and scalability. The remainder of this book discusses in detail how to configure the Cisco SSL VPN product to implement these design considerations.

References

SSL VPN security white paper at http://www.cisco.com, Steven Song, http://www.cisco.com/web/about/security/intelligence/05_08_SSL-VPN-Security.html.

Cisco SAFE VPN IPSec Virtual Private Networks in Depth, Jason Halpern, et al., http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a00801dca2d.shtml#wp48088.

Networkers 2006 presentation SEC-2010, Deploying Remote Access IPSec and SSL VPNs, Pete Davis.

INDEX