CHAPTER 1

Access VPNs and IP Security Protocol Tunneling Technology Overview

The Cisco Secure VPN Client is a software component in an extranet client-initiated access VPN. VPNs allow for private data to be encrypted and transmitted securely over a public network. With the Cisco Secure VPN Client, you can establish an encrypted tunnel between a VPN Client and a networking device using static or dynamic IP addresses.

This chapter contains the following sections:

- Virtual Private Networks Overview
- Cisco Secure VPN Client Overview
- Interoperability with Networking Devices
- System Requirements
- Benefits

Virtual Private Networks Overview

A Virtual Private Network (VPN) is a network that extends remote access to users over a shared infrastructure. VPNs maintain the same security, prioritizing, manageability, and reliability as a private network. They are the most cost-effective method of establishing a point-to-point protocol (PPP) connection between remote users and an enterprise customer's network. VPNs based on IP meet business customers' requirements to extend intranets to remote offices, mobile users, and telecommuters. Further, they can enable extranet links to business partners, suppliers, and key customers for greater customer satisfaction and reduced business costs.

The following sections describe the three basic types of VPNs:

- Access VPNs
- Intranet VPNs
- Extranet VPNs

Access VPNs

Access VPNs provide secure connections for remote access for individuals (for example, mobile users or telecommuters), a corporate intranet, or an extranet over a shared service provider network with the same policies as a private network.

The following sections describe the two types of access VPNs:

- Client-Initiated Access VPNs
- NAS-Initiated Access VPNs

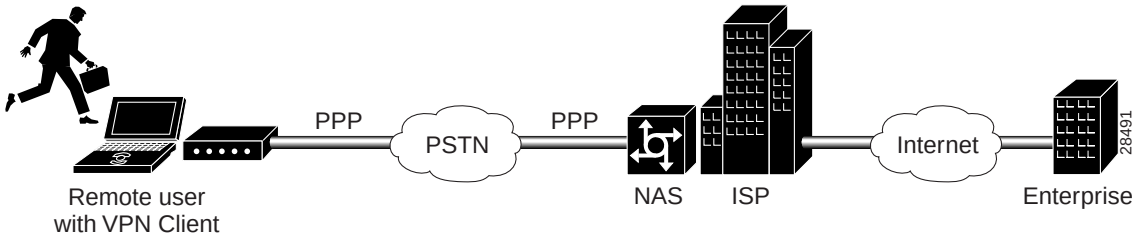
Client-Initiated Access VPNs

Client-initiated access VPNs allow for remote users to use clients to establish an encrypted IP tunnel across the Internet service provider's (ISP) shared network to the enterprise customer's network. The main advantage of client-initiated access VPNs over NAS-initiated access VPNs is that they use IPSec tunnel mode to secure the connection between the client and the ISP over the PSTN.

Figure 1-1 shows the Cisco Secure VPN Client in a client-initiated access VPN topology. The client establishes a secure PPP connection with the ISP's NAS, then an IPSec tunnel is established over the PSTN. All business cases in this solutions guide are client-initiated access VPNs in that the client always initiates the PPP connection with the ISP. VPN Clients may either use static IP addressing with manual configuration or dynamic IP addressing with IKE Mode Configuration.

Note Currently, IKE Mode Configuration is supported only as a gateway-initiated feature, however, before IKE Mode Configuration occurs the client must establish a PPP link with the ISP. Although IKE Mode Configuration is gateway-initiated, the entire negotiation sequence begins and ends as a client-initiated access VPN. Client-initiated IKE Mode Configuration will be available in a later release.

Figure 1-1 Client-Initiated Access VPN

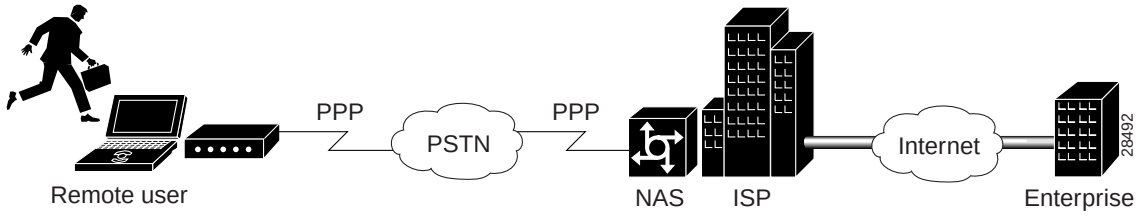


NAS-Initiated Access VPNs

NAS-initiated access VPNs allow for remote users to dial in to the ISP's NAS. The NAS establishes an encrypted tunnel to the enterprise's private network. NAS-initiated VPNs allow remote users to connect to multiple networks using multiple tunnels. NAS-initiated VPNs do not encrypt the connection between the client and the ISP, but rely on the security of the PSTN.

Figure 1-2 shows a NAS-initiated access VPN topology. Because the Cisco Secure VPN Client is not required for a NAS-initiated access VPN solution, it is not a component of this network. The disadvantage of NAS-initiated access VPNs is that the PSTN is not secured.

Figure 1-2 NAS-Initiated Access VPN



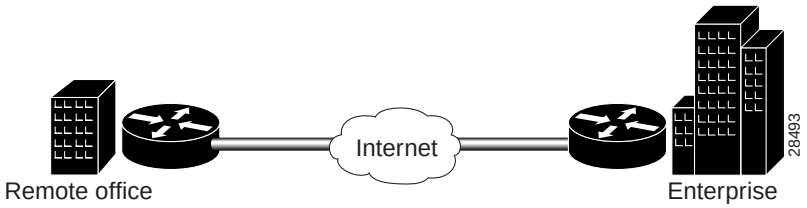
Intranet VPNs

Intranet VPNs connect corporate headquarters, remote offices, and branch offices over a shared infrastructure using dedicated connections. Intranets are networks for businesses that are internal to the companies. In intranets, a businesses benefits from the same policies as private networks, including security, quality of service (QoS), manageability, and reliability. Intranets deliver the most current information and services available to networked employees. Intranets also increase employees' productivity by allowing for a reliable connection to consistent information. With an intranet VPN, you get the same security and connectivity for a corporate headquarters, remote offices, and branch offices as you would have with a private network.

Figure 1-3 shows an intranet VPN topology. Because the Cisco Secure VPN Client acts as the client component in a client/server application, with the networking device functioning as a server, it is not commonly used in an intranet VPN scenario. Also, the Cisco Secure VPN Client is not necessary for secure encryption over an intranet between two networking devices–an IPSec tunnel will suffice. It is, however, possible for the client to negotiate a more strict transform set than the networking device-to-networking device transform set, depending on the level of security required between the host and destination.

For information on creating an intranet VPN, refer to the "Intranet VPN Scenario" chapter of the *Cisco 7100 VPN Configuration Guide.*

Figure 1-3 Intranet VPN



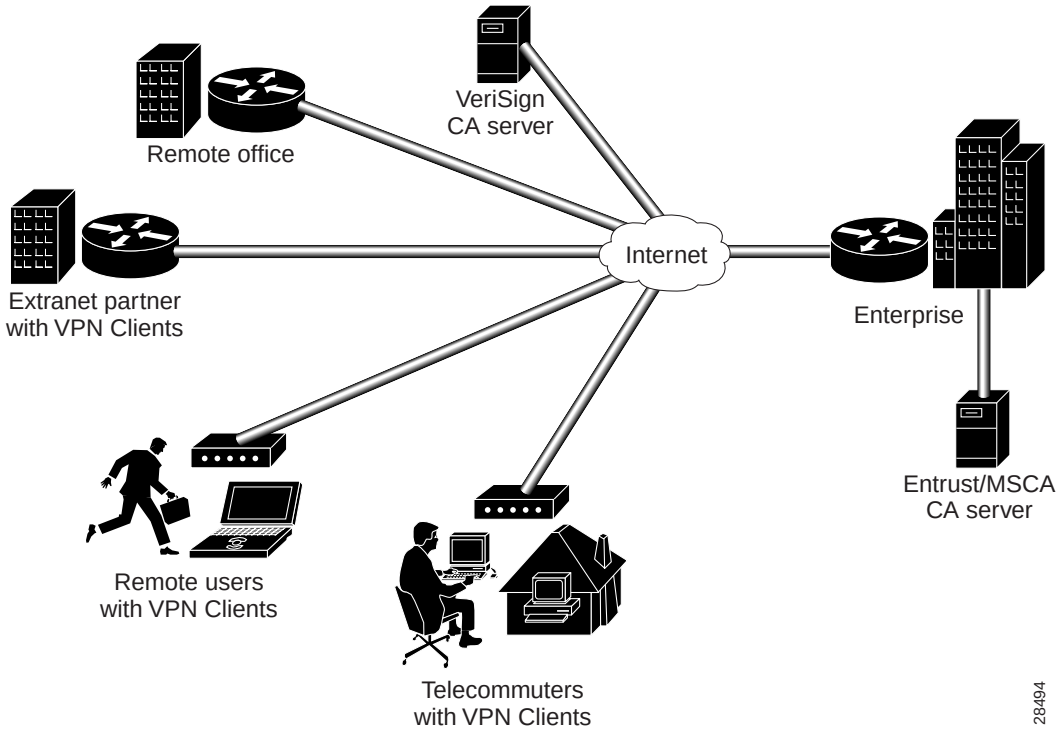
Extranet VPNs

Extranet VPNs link customers, suppliers, partners, or communities of interest to a corporate intranet over a shared infrastructure using dedicated connections. Extranets are intranets that extend limited access to customers, suppliers, and partners; while providing authorized access for telecommuters and remote offices. Extranets differ from intranets in that they allow access to remote users outside of the enterprise. By allowing greater access to the resources that are available to customers, suppliers, and partners; companies with extranet VPNs improve their customer satisfaction and reduce business costs at the same time.

Figure 1-4 shows the Cisco Secure VPN Client in an extranet VPN topology. Using digital certificates, clients establish a secure tunnel over the Internet to the enterprise. A certification authority (CA) issues a digital certificate to each client for device authentication. VPN Clients may either use static IP addressing with manual configuration or dynamic IP addressing with IKE Mode Configuration. The CA server checks the identity of remote users, then authorizes remote users to access information relevant to their function. Extranet VPNs with the Cisco Secure VPN Client are addressed in Chapter 6, "Configuring Digital Certification." Static and dynamic IP addressing is addressed in Chapter 4, "Configuring Dynamic IP Addressing."

Note While Figure 1-4 uses digital certificates to describe an extranet VPN scenario, you may opt to use pre-shared keys instead of digital certificates. You can use either digital certificates or pre-shared keys for authentication in all types of VPNs.

Figure 1-4 Extranet VPNs



Cisco Secure VPN Client Overview

Cisco Secure VPN Client is a software component that allows a desktop user to create an encrypted tunnel using IPSec and/or IKE to a remote site for an end-to-end, extranet VPN solution. IP Security Protocol (IPSec) encryption technology is an IETF-based effort that is accepted industry-wide. Internet Key Exchange (IKE) is a hybrid protocol which implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.) IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. Cisco IOS networking devices use IPSec to establish secure, encrypted tunnels between Cisco networking devices. This creates a secure client-to-server

communication over a Layer 3 IP network, such as the Internet. In this solutions guide, the Cisco IOS IPSec-enabled networking device acts as a server, while the Cisco Secure VPN Client performs tasks as a client.

The Cisco Secure VPN Client software allows you to perform the following tasks directly from your desktop:

- Generating a Public/Private Key
- Getting a Digital Certificate
- Establishing a Security Policy

Generating a Public/Private Key

Using IKE, you can configure the Cisco Secure VPN Client to use the public/private key system for encryption. The public/private key system is a method of encrypting and decrypting Internet traffic for a secure connection without prior notification. Public/private key technology uses an encryption algorithm (such as DES) and an encryption key, which two parties—a recipient and a sender—use to pass data between one another. The recipient holds the private key, while the public key belongs to the certification authority (CA) or directory server for distribution.

Getting a Digital Certificate

With IPSec, you can configure the Cisco Secure VPN Client to use digital certificates for authentication. To verify a sender's identity, the CA issues a digital certificate, an electronic file that the CA approves by signing once the sender's identity is verified. Once the sender has the issuing CA's digital certificate (as well as the sender's digital certificate), the sender should establish a security policy.

Establishing a Security Policy

A security policy provides information about how to verify a user's identity, ensure integrity to prevent tampering with data, and actively auditing for intrusion detection. Every corporate network should have a security policy that determines how the network is maintained for authenticated users and monitored for unauthorized access.

Interoperability with Networking Devices

This guide covers the current Cisco-supported configurations between the Cisco Secure VPN Client and Cisco networking devices. For the configurations in this guide, Cisco recommends using VPN-based networking devices; however, Cisco Secure VPN Client is interoperable with all Cisco networking devices that support IPSec.

This section contains the following topics:

- Recommended Networking Devices
- Networking Devices with IP Security Protocol
- Supported Configurations

Recommended Networking Devices

For optimum interoperability, Cisco recommends using the following networking devices when setting up a network with Cisco Secure VPN Client:

- Cisco Secure PIX Firewall
- Cisco 7100 VPN router
- Cisco 1720 VPN router

For documentation on these networking devices and information on supported versions, refer to "Platform-Specific Documents" in the Preface.

Networking Devices with IP Security Protocol

All Cisco networking devices that support Cisco IOS IPSec are interoperable with Cisco Secure VPN Client. These Cisco networking devices are as follows:

- Cisco 800 series router
- Cisco 1400 series router
- Cisco 1600 series router
- Cisco 1700 series router (Cisco 1720 VPN, 1750 Voice)
- Cisco 2500 series router
- Cisco 2600 series router
- Cisco 3600 series router
- Cisco 4000 series router (Cisco 4000, 4000-M, 4500, 4500-M, 4700, 4700-M)
- Cisco 7100 VPN series router
- Cisco 7200 series router
- Cisco 7500 series router
- Cisco 12000 series router
- Cisco AS5300 series universal access server
- Cisco MC3810 multiservice access concentrator
- Cisco Secure PIX Firewall

Supported Configurations

Currently, Cisco supports usage of the Cisco Secure VPN Client with IPSec and IKE. For interoperability between the Cisco Secure VPN Client and Cisco networking devices, Cisco supports the following configurations:

- Using Pre-Shared Keys
- Using Digital Certification

Note For a comparative listing of the encryption features including manual configuration, dynamic IP addressing, pre-shared keys, wildcard pre-shared keys, and digital certification, see the "Authentication and Encryption Features" section in Chapter 2, "Case Study for Layer 3 Authentication and Encryption."

Using Pre-Shared Keys

You can generate pre-shared keys for user authentication between a VPN Client and a gateway. Pre-shared keys are simple to implement.

- For more information on static IP addressing, refer to the "Manual Configuration (Static IP Addressing)" section in Chapter 2, "Case Study for Layer 3 Authentication and Encryption."
- For more information on dynamic IP addressing, refer to the "IKE Mode Configuration (Dynamic IP Addressing)" section in Chapter 2, "Case Study for Layer 3 Authentication and Encryption."
- For more information on pre-shared keys, refer to the "Pre-Shared Keys" section in Chapter 2, "Case Study for Layer 3 Authentication and Encryption."
- For more information on wildcard pre-shared keys, refer to the "Wildcard Pre-Shared Keys" section in Chapter 2, "Case Study for Layer 3 Authentication and Encryption."

Using Digital Certification

You can request that a certification authority (CA) assign a digital certificate to each VPN Client for device authentication. Digital certificates offer more scalability than pre-shared keys, and are usually implemented on larger networks (more than 10 clients).

Note VeriSign digital certification is not supported on Cisco Secure PIX Firewall Version 5.1. For more details, see the "Cisco Secure PIX Firewall Documentation" section in the Preface.

As of this publication, the Cisco Secure VPN Client is supported with Cisco networking devices using Entrust, Microsoft, and VeriSign digital certificates.

- For more information on static IP addressing, refer to the "Manual Configuration (Static IP Addressing)" section in Chapter 2, "Case Study for Layer 3 Authentication and Encryption."
- For more information on dynamic IP addressing, refer to the "IKE Mode Configuration (Dynamic IP Addressing)" section in Chapter 2, "Case Study for Layer 3 Authentication and Encryption."
- For more information on digital certification, refer to the "Digital Certification" section in Chapter 2, "Case Study for Layer 3 Authentication and Encryption."

System Requirements

To perform the tasks outlined in this solutions guide, you will require the following materials:

- Client-Side Requirements (Software)
- Server-Side Requirements (Hardware and Software)

Client-Side Requirements (Software)

For the client-side requirements, refer to the "System Requirements" section in the release notes for your version of the VPN Client:

- On CCO: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csvpnc/csvpnrn/index.htm

  or **Service & Support** > **Technical Documents** > **Documentation Home Page** > **Internet Service Unit Documentation** > **Cisco Secure VPN Client** > **Cisco Secure VPN Client Release Notes**
- On the Documentation CD-ROM: **Cisco Product Documentation** > **Internet Service Unit Documentation** > **Cisco Secure VPN Client** > **Cisco Secure VPN Client Release Notes**

Server-Side Requirements (Hardware and Software)

These server-side requirements are needed to install and operate the Cisco networking device for interoperability with a Cisco Secure VPN Client:

- One of the networking devices listed under "Networking Devices with IP Security Protocol."
- An IPSec software image loaded onto the networking device from a supported Cisco IOS software release.

  For the supported Cisco IOS software release, refer to the "Network Requirements" section in the release notes for your version of the VPN Client.
  - On CCO: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csvpnc/csvpnrn/index.htm,

    or **Service & Support** > **Technical Documents** > **Documentation Home Page** > **Internet Service Unit Documentation** > **Cisco Secure VPN Client** > **Cisco Secure VPN Client Release Notes**
  - On the Documentation CD-ROM: **Cisco Product Documentation** > **Internet Service Unit Documentation** > **Cisco Secure VPN Client** > **Cisco Secure VPN Client Release Notes**

Benefits

Choosing a VPN network design that best fits the needs of your business is essential. This section lists the following benefits:

- Client-Initiated versus NAS-Initiated Access VPNs
- Cisco Secure VPN Client versus Other VPN Solutions

For information on the Layer 3 Encryption feature benefits, see the "Authentication and Encryption Features" section in Chapter 2, "Case Study for Layer 3 Authentication and Encryption."

Client-Initiated versus NAS-Initiated Access VPNs

Table 1-1 outlines the advantages and disadvantages of the two access VPNs, client-initiated and NAS-initiated.

Table 1-1 Client-Initiated versus NAS-Initiated

Client-Initiated		NAS-Initiated	
Pros	**Cons**	**Pros**	**Cons**
Encryption guarantees a secure tunnel between client and server.	Some client maintenance is required.	No client maintenance is required.	No encryption occurs over the PSTN.
Network is more scalable with digital certificates than with pre-shared keys. You can configure unlimited clients.	Network is less scalable with pre-shared keys than with digital certificates. Router must be reconfigured with each additional client. One workaround is to use wildcard pre-shared key.	Scalable to larger networks.	Third-party CA required for PKI.
Client creates a VPN over PSTN and Internet using IPSec.	None.	NAS creates a VPN over Internet using L2F.	PSTN is not secured.

Cisco Secure VPN Client versus Other VPN Solutions

The Cisco Secure VPN Client is preferable over access VPNs with tunneling protocol such as L2F because of its ability to secure transmissions over the PSTN. When using pre-shared keys, it is the simplest method of security for encrypted tunneling between a remote user's VPN Client and a networking device. Cisco Secure VPN Client is also scalable to large networks when used with digital certificates.