



Cisco Secure VPN Client Solutions Guide

For Cisco Secure VPN Client Version 1.0 or Later

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-0259-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Access Registrar, AccessPath, Any to Any, AtmDirector, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, the Cisco Technologies logo, ConnectWay, Fast Step, FireRunner, GigaStack, IGX, Internet Quotient, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, Secure Script, ServiceWay, SlideCast, SMARTnet, *The Cell*, TrafficDirector, TransPath, ViewRunner, VisionWay, VlanDirector, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, GeoTel, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (9909R)

Cisco Secure VPN Client Solutions Guide

Copyright © 1999, Cisco Systems, Inc.

All rights reserved.



Preface vii

Audience	vii
Document Organization	viii
Business Cases Presented in This Solutions Guide	viii
New and Changed Information	ix
Related Documentation	ix
Conventions	xiii
Cisco Connection Online	xiv
Documentation CD-ROM	xv

CHAPTER 1

Overview of Virtual Private Networks and Cisco Secure VPN Client 1-1

What is a Virtual Private Network?	1-1
Types of Virtual Private Networks	1-2
Access VPNs	1-2
Intranet VPN	1-3
Extranet VPN	1-3
What is the Cisco Secure VPN Client?	1-4
Generating a Public/Private Key	1-5
Getting a Digital Certificate	1-5
Establishing a Security Policy	1-5
Interoperability with Cisco Routers	1-5
Recommended Cisco Routers	1-6
Cisco Routers with IP Security Protocol	1-6
Supported Configurations	1-7
Static or Dynamic Client IP Addresses with Pre-shared Keys	1-7
Static or Dynamic Client IP Addresses with Digital Certificates	1-7
Dynamic Client IP Addressing with IKE Mode Configuration	1-7
System Requirements	1-8
Client-side Requirements (Software)	1-8
Server-side Requirements (Hardware and Software)	1-8
Benefits	1-9
Client-initiated versus NAS-initiated Access VPNs	1-9

Pre-shared Keys versus Digital Certificates	1-9
Static versus Dynamic IP Addresses on the Client	1-11
Cisco Secure VPN Client versus Other VPN Solutions	1-11

CHAPTER 2

Using Pre-shared Keys: A Business Case 13

CHAPTER 3

Using Digital Certificates: Business Case Introduction 3-1

Benefits of Using Digital Certificates	3-1
Business Case Description	3-1
The Challenge	3-2
The Risk	3-2
The Solution	3-2
Supported Digital Certificates	3-6
Related Documentation	3-6

CHAPTER 4

Using Entrust Digital Certificates: A Business Case 4-1

Benefits of Using Entrust Digital Certificates	4-1
Configuring and Verifying	4-1
Configuring Entrust Digital Certifications	4-1
Configuring the Cisco Secure VPN Client	4-2
Task 1—Importing the Root CA Certificate	4-3
Task 2—Creating Public and Private Key Pair	4-5
Task 3—Requesting Client Certificate from Entrust CA Server	4-7
Task 4—Submitting the Certification Request to the Entrust Server	4-8
Task 5—Importing Your Signed Entrust Digital Certificate	4-14
Task 6—Configuring Other Connections for Security Policy	4-16
Task 7—Configuring A New Connection for Security Policy	4-18
Task 8—Specifying Identity Using RSA Signature	4-20
Task 9—Specifying Encryption and Authentication Methods for Authentication, Phase 1	4-22
Task 10—Specifying Encryption and Authentication Methods for Key Exchange, Phase 2	4-24
Task 11—Saving Your Configuration	4-25
Configuring the Cisco Router	4-26
Task 1—Configuring the Domain Name, Host Name, and Name Server	4-26
Task 2—Configuring ISAKMP Policy and Defining IPSec Transform Set	4-26
Task 3—Defining Crypto Dynamic Map and IKE Crypto Map to the Client	4-27

Task 4—Defining the CA, Enrolling Your Certificate, and Requesting Certificate Signature	4-28
Task 5—Applying the Crypto Map to the Interface	4-29
Verifying Entrust Digital Certifications	4-30
Task 1—Viewing and Verifying Using Certificate Manager	4-30
Task 2—Issuing Show Commands on Cisco Router	4-31
Related Documentation	4-32

CHAPTER 5

Using VeriSign Digital Certificates: A Business Case 5-1

Benefits of Using VeriSign Digital Certificates	5-1
Configuring, Verifying, and Troubleshooting	5-1
Configuring VeriSign Digital Certifications	5-1
Configuring the Cisco Secure VPN Client	5-2
Task 1—Importing the Root CA Certificate	5-3
Task 2—Creating Public and Private Key Pair	5-5
Task 3—Requesting Client Certificate from VeriSign CA Server	5-7
Task 4—Submitting the Certification Request to the VeriSign CA Server	5-8
Task 5—Importing Your Signed VeriSign Digital Certificate	5-12
Task 6—Configuring Other Connections for Security Policy	5-14
Task 7—Configuring A New Connection for Security Policy	5-16
Task 8—Specifying Identity Using RSA Signature	5-18
Task 9—Specifying Encryption and Authentication Methods for Authentication, Phase 1	5-20
Task 10—Specifying Encryption and Authentication Methods for Key Exchange, Phase 2	5-22
Task 11—Saving Your Configuration	5-23
Configuring the Cisco Router	5-24
Task 1—Configuring the Domain Name, Host Name, and Name Server	5-24
Task 2—Configuring ISAKMP Policy and Defining IPSec Transform Sets	5-24
Task 3—Defining Crypto Dynamic Map and IKE Crypto Map to the Client	5-25
Task 4—Defining the CA, Enrolling Your Certificate, and Requesting Certificate Signature	5-26
Task 5—Applying Crypto Map to the Interface	5-27
Verifying VeriSign Digital Certifications	5-28
Task 1—Viewing and Verifying Using Certificate Manager	5-28
Task 2—Issuing Show Commands on Cisco Router	5-29
Related Documentation	5-30

CHAPTER 6

Using Internet Key Exchange Mode Configuration: A Business Case 6-1

Benefit of Using Internet Key Exchange Mode Configuration 6-1

Business Case Description 6-1

The Challenge 6-2

The Risk 6-2

The Solution 6-2

Configuring and Verifying 6-3

Configuring Internet Key Exchange Mode Configuration 6-3

Configuring the Cisco Secure VPN Client 6-3

Configuring the Cisco Router 6-3

Task 1—Configuring the Domain Name, Host Name, and Name Server 6-3

Task 2—Defining the Pool of IP Addresses 6-4

Task 3—Defining the Crypto Maps That Attempt Client Configuration 6-4

Verifying IKE Mode Configuration 6-4

Related Documentation 6-5

GLOSSARY

INDEX



Preface

This guide describes Cisco-supported configurations for IP-based multi-service extranet Virtual Private Networks (VPNs) for an IP Security Protocol (IPSec) tunnel between a PC (with Cisco Secure VPN Client software installed) and a Cisco router.

This guide does not cover every available feature; it is not intended to be a comprehensive VPN configuration guide. Instead, this guide simply describes the Cisco-supported configurations for VPNs using the Cisco Secure VPN Client.

The extranet business scenarios introduced in this guide include specific tasks and configuration examples. The examples are the recommended methods for configuring the specified tasks. Although they are typically the easiest or the most straightforward method, they are not the only methods of configuring the tasks.

This preface contains the following sections:

- Audience
- Document Organization
- Business Cases Presented in This Solutions Guide
- New and Changed Information
- Related Documentation
- Conventions
- Cisco Connection Online
- Documentation CD-ROM

Audience

This solutions guide is intended primarily for the following audiences:

- Network administrators who are responsible for defining network security policies and distributing them to the end users within your organization
- System administrators who are responsible for installing and configuring internetworking equipment, are familiar with the fundamentals of router-based internetworking, and who are familiar with Cisco IOS software and Cisco products
- System administrators who are familiar with the fundamentals of router-based internetworking and who are responsible for installing and configuring internetworking equipment, but who might not be familiar with the specifics of Cisco products or the routing protocols supported by Cisco products
- Customers with technical networking background and experience

Document Organization

The major elements of this guide are as follows:

Chapter	Title	Description
Chapter 1	Overview of Virtual Private Networks and Cisco Secure VPN Client	Provides a physical overview of different types of VPNs, client-specific details, and related documentation.
Chapter 2	Using Pre-shared Keys: A Business Case	Shows how pre-shared keys are generated for a secure IPSec tunnel between the Cisco Secure VPN Client and a Cisco router.
Chapter 3	Using Digital Certificates: Business Case Introduction	Shows how a digital certificate is set up and maintained for a secure IPSec tunnel between the Cisco Secure VPN Client and a Cisco router.
Chapter 4	Using Entrust Digital Certificates: A Business Case	Shows how an Entrust digital certificate is set up and maintained for a secure IPSec tunnel between the Cisco Secure VPN Client and a Cisco router.
Chapter 5	Using VeriSign Digital Certificates: A Business Case	Shows how a VeriSign digital certificate is set up and maintained for a secure IPSec tunnel between the Cisco Secure VPN Client and a Cisco router.
Chapter 6	Using Internet Key Exchange Mode Configuration: A Business Case	Provides an example of setting up a secure IKE connection between a Cisco Secure VPN Client and a Cisco router with Cisco IOS IPSec support.
None	Glossary	Provides a list of terms and definitions related to the VPN configurations in this guide.
None	Index	Provides a list of terms found throughout this guide.

Business Cases Presented in This Solutions Guide

Each chapter in this solutions guide documents a business case. The *Cisco Secure VPN Client Solutions Guide* contains the following business cases:

- Using Pre-shared Keys: A Business Case
- Using Digital Certificates: Business Case Introduction
- Using Entrust Digital Certificates: A Business Case
- Using VeriSign Digital Certificates: A Business Case
- Using Internet Key Exchange Mode Configuration: A Business Case

New and Changed Information

Although the Cisco Secure VPN Client supports pre-shared keys, documentation for this configuration is not currently available in this guide. Documentation for pre-shared keys will be available in a later release.

Related Documentation

This document is not a comprehensive guide to all VPNs. The following aspects of VPN configuration are not covered in this guide:

- NAS-initiated VPNs
- Intranet VPNs
- Cisco router or access server installation and configuration

For more information on Cisco VPN products that are outside the scope of this document, refer to the following Cisco technical documents:

- For detailed information on configuring access VPNs using the L2F tunneling protocol, refer to the *Access VPN Solutions Using Tunneling Technology Solutions Guide*.
- For installation and VPN configuration information for the Cisco 7100 series routers, refer to the *Cisco 7100 Hardware Installation Guide* and the *Cisco 7100 VPN Configuration Guide*.
- For installation and configuration details for the Cisco 1700 series routers, refer to the *Cisco 1720 Router Hardware Installation Guide* and *Cisco 1700 Router Software Configuration Guide*.

For a listing of other Cisco technical documentation currently available on VPN networks, refer to the following table.

Document Title ¹	Customer Order Number	Path
Cisco Secure VPN Client Documentation		
Cisco Secure VPN Client <ul style="list-style-type: none"> Quick Start Guide Release Notes Solutions Guide 	<ul style="list-style-type: none"> DOC-786898 DOC-786929 OL-0259 	Hardware and Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Internet Service Unit Documentation>Cisco Secure VPN Client
Internetworking Solutions Guides Documentation		
<i>Access VPN Solutions Using Tunneling Technology</i>	<ul style="list-style-type: none"> OL-0293 	Hardware and Software Documentation: <ul style="list-style-type: none"> CCO²>Service & Support>Technical Documents>Documentation Home Page>Technology Information>Internetworking Solutions Guides>Access VPN Solutions Using Tunneling Technology
Cisco IOS Release 12.0 Documentation		
<i>Security Configuration Guide</i>	<ul style="list-style-type: none"> DOC-785843 	Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>Configuration Guide and Command References>Security Configuration Guide
<i>Security Command Reference</i>	<ul style="list-style-type: none"> DOC-785845 	Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>Configuration Guide and Command References>Security Command Reference
New Feature Documentation	<ul style="list-style-type: none"> See Path.³ 	Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>New Feature Documentation

Document Title ¹	Customer Order Number	Path
Cisco 1700 Series Routers		
Cisco 1720 Router <ul style="list-style-type: none"> Quick Start Guide Hardware Installation Guide Software Configuration Guide Release Notes Reg. Comp. and Safety Information Configuration Notes 	<ul style="list-style-type: none"> DOC-785406 DOC-785405 DOC-785407 See Path.³ DOC-783088 DOC-786739 DOC-785977 	Hardware and Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Access Servers and Access Routers>Modular Access Routers>Cisco 1720 Router Release Notes Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>Release Notes>Cisco 1700 Series Routers>Cisco 1720 Routers
Cisco 1750 Router <ul style="list-style-type: none"> VOIP Quick Start Guide Hardware Installation Guide VOIP Configuration Guide Release Notes Reg. Comp. and Safety Information 	<ul style="list-style-type: none"> DOC-786582 DOC-786169 OL-0139² See Path.³ DOC-783088 	Hardware and Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Access Servers and Access Routers>Modular Access Routers>Cisco 1750 Router Release Notes Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>Release Notes>Cisco 1700 Series Routers>Cisco 1750 Routers
Cisco 7000 Family Routers		
Cisco 7100 Router <ul style="list-style-type: none"> Quick Start Guide Installation and Configuration Guide VPN Configuration Guide Reg. Comp. and Safety Information Release Notes for Release 12.0 XE Port and Service Adapters Field Replaceable Units 	<ul style="list-style-type: none"> DOC-786343 DOC-786341 DOC-786342 DOC-786345 DOC-786019 See Path.³ See Path.³ 	Hardware and Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Core/High-End Routers>Cisco 7100 Release Notes Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>Release Notes>Cisco 7000 Family Routers>Cisco 7000 Family - Release Notes for Cisco Release 12.0 XE

Document Title ¹	Customer Order Number	Path
Cisco 2600 Series Routers		
Cisco 2600 Router <ul style="list-style-type: none"> Quick Start Guides Hardware Installation Guide Software Configuration Guide Network Module Hardware Installation Guide WAN Interface Cards Hardware Installation Guide Analog Modem Firmware Digital Modem Portware Reg. Comp. and Safety Information Configuration Notes International Regulatory Compliance Information for Telecommunications Equipment Release Notes for Release 12.0 T 	<ul style="list-style-type: none"> See Path.³ DOC-785037 DOC-785173 DOC-785047 DOC-785046 See Path.³ See Path.³ DOC-785148 See Path.³ DOC-786655 DOC-786136 	Hardware and Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Access Servers and Access Routers>Modular Access Routers>Cisco 2600 Series Release Notes Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>Release Notes>Cisco 2600 Series Routers>Cisco 2600 Series - Release Notes for Release 12.0 T
Cisco 3600 Series Routers		
Cisco 3600 Router <ul style="list-style-type: none"> Quick Start Guide Hardware Installation Guide Software Configuration Guide VOIP Software Configuration Guide Network Module Hardware Installation Guide WAN Interface Cards Hardware Installation Guide Analog Modem Firmware Digital Modem Portware Reg. Comp. and Safety Information Configuration Notes International Regulatory Compliance Information for Telecommunications Equipment Release Notes for Release 12.0 T 	<ul style="list-style-type: none"> DOC-786343 DOC-785921 DOC-785173 DOC-786046 DOC-785047 DOC-78-5046 See Path.³ See Path.³ DOC-783020 See Path.³ DOC-786655 DOC-786046 	Hardware and Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Access Servers and Access Routers>Modular Access Routers>Cisco 3600 Series Release Notes Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>Release Notes>Cisco 3600 Series Routers>Cisco 3600 Series - Release Notes for Release 12.0 T


Document Title ¹	Customer Order Number	Path
Cisco IOS Router Documentation		
<ul style="list-style-type: none"> Modular Access Routers Access Servers Core/High-End Routers 	<ul style="list-style-type: none"> See Path.³ See Path.³ See Path.³ 	<p>Modular Access Routers Documentation:</p> <p>CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Access Servers and Access Routers>Modular Access Routers</p> <p>Access Servers Documentation:</p> <p>CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Access Servers and Access Routers>Access Servers</p> <p>Core/High-End Routers Documentation:</p> <p>CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Core/High-End Routers></p>

1. If you are viewing this guide online, the hyperlinks in this column are subject to change without notice. If this occurs, refer to the Path column.
2. Cisco Connection Online (CCO) is located at <http://www.cisco.com>. For more information, see “Cisco Connection Online.”
3. In the Path column, refer to the CCO path for a listing of the available publications.

Conventions

Command descriptions use the following conventions:

Convention	Description
Click Screen1>Screen2>Screen3	Means use your mouse to navigate through a series of screens or menu items.
boldface font	Commands, keywords, menus, menu items, and options are in boldface .
<i>italic</i> font	Arguments for which you supply values are in <i>italics</i> .
[]	Elements in square brackets are optional.
{x y z}	Alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in screen font.

Convention	Description
boldface screen font	Information you must type is in boldface screen font .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.
 Note	Means <i>reader take note</i> . Notes contain helpful suggestions or references to material not covered in the publication.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: [cco.cisco.com](telnet://cco.cisco.com)
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

**Note**

If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.



Overview of Virtual Private Networks and Cisco Secure VPN Client

The Cisco Secure VPN Client is a software component in either an extranet Virtual Private Network (VPN) or a 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 client and a router using static or dynamic IP addresses.

This technology overview contains the following sections:

- What is a Virtual Private Network?
- Types of Virtual Private Networks
- What is the Cisco Secure VPN Client?
- Interoperability with Cisco Routers
- System Requirements
- Benefits

What is a Virtual Private Network?

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 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.

Types of Virtual Private Networks

The three basic types of VPNs, discussed in this section, are access VPNs, intranet VPNs, and extranet 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. For more information, refer to “Access VPNs.”
- **Intranet VPNs**—Connect corporate headquarters, remote offices, and branch offices over a shared infrastructure using dedicated connections. Businesses enjoy the same policies as a private network, including security, quality of service (QoS), manageability, and reliability. For more information, refer to “Intranet VPN.”
- **Extranet VPNs**—Link customers, suppliers, partners, or communities of interest to a corporate intranet over a shared infrastructure using dedicated connections. For more information, refer to “Extranet VPN.”

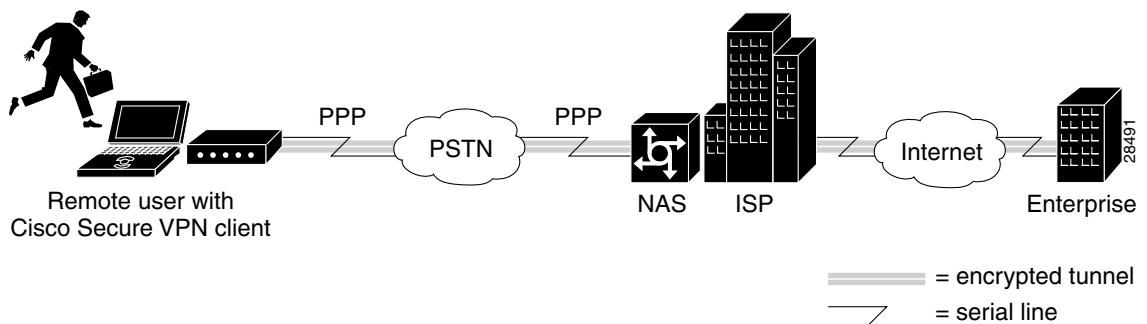
Access VPNs

There are two types of access VPNs, network access server (NAS)-initiated and client-initiated.

- **Client-initiated**—Remote users 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 VPNs over NAS-initiated VPNs is that they use encrypted tunneling to secure the connection between the client and the ISP over the PSTN.

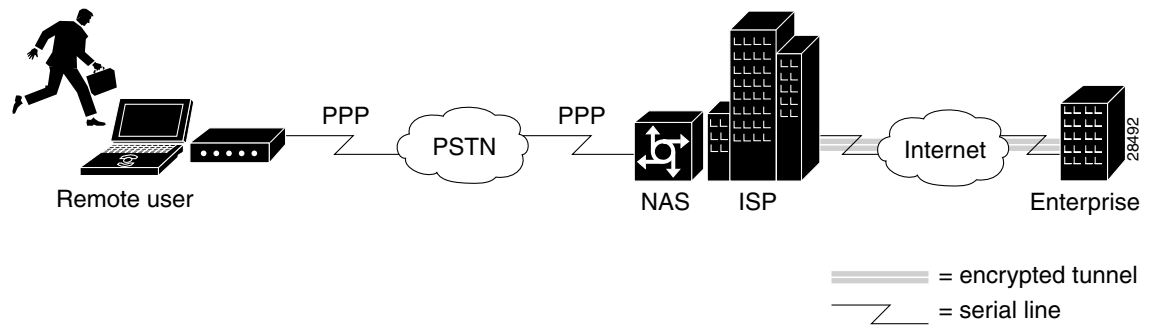
Figure 1-1 shows the Cisco Secure VPN Client in a client-initiated access VPN topology. The client establishes a PPP connection with the ISP's NAS, an IKE Mode Configuration session occurs, then an encrypted tunnel is established over the PSTN. Client-initiated access VPNs with the Cisco Secure VPN Client are covered in Chapter 6, “Using Internet Key Exchange Mode Configuration: A Business Case.”

Figure 1-1 Client-initiated Access VPN



- **NAS-initiated**—Remote users dial in to the ISP's NAS. The NAS establishes an encrypted tunnel to the enterprise's private network. NAS-initiated VPNs allow users to connect to multiple networks by using multiple tunnels, and do not require the client to maintain the tunnel-creating software. 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.

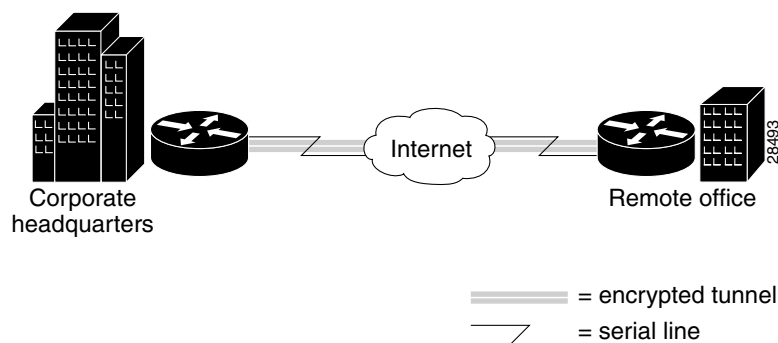
Figure 1-2 NAS-initiated Access VPN

Intranet VPN

An intranet is a network for business that is internal to a company. It delivers the most current information and services available to a company's networked employees. Intranets offer a common, platform-independent interface, which is less costly to implement than a client/server application. Intranets also increase employees' productivity by allowing for a reliable connection to consistent information. Intranet VPNs are used to allow the the same security and connectivity for a corporate headquarters, a remote office, and a branch office 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 router 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 routers—an IPSec tunnel will suffice. It is, however, possible for the client to negotiate a more strict transform set than the router-to-router 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 VPN

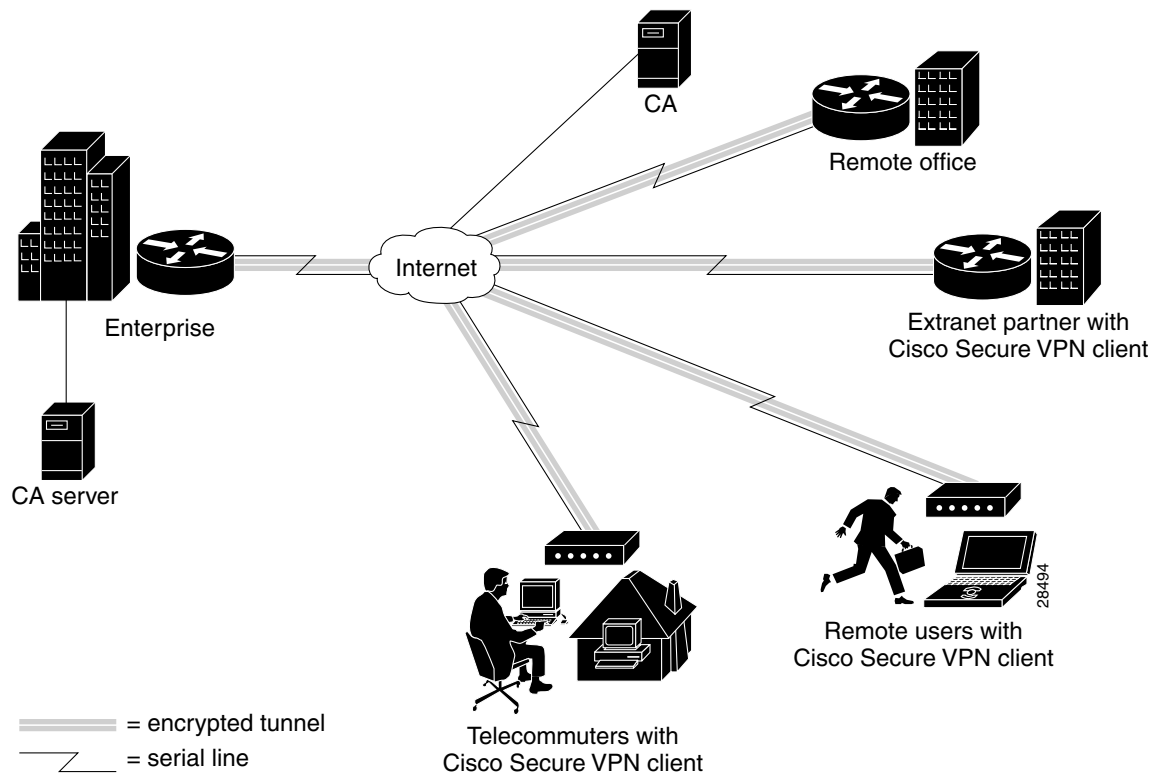
An extranet is an intranet that extends limited access to customers, suppliers, and partners. Extranets differ from intranets in that they allow access to users outside of the enterprise. By allowing greater access to the resources that are available to customers, suppliers, and partners, companies with extranet VPNs can actually 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. Telecommuters, remote users, extranet partners, and remote offices are checked for authentication, then authorized to access information relevant to their function. While the telecommuters might use static IP addresses, the remote users might use dynamic IP addresses. Extranet VPNs with the Cisco Secure VPN Client begin coverage in Chapter 3, “Using Digital Certificates: Business Case Introduction.”

**Note**

While this solutions guide uses digital certificates to describe an extranet VPN scenario, it is possible to use digital certificates for device authentication in all types of VPNs. Client-initiated access VPNs, intranet VPNs, and extranet VPNs all support digital certificates.

Figure 1-4 Extranet VPNs



What is the Cisco Secure VPN Client?

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 routers use IPSec to establish secure, encrypted tunnels between Cisco routers. 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

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 router acts as a server, while the Cisco Secure VPN Client performs tasks as a client.

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 Cisco Routers

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

This section contains the following topics:

- Recommended Cisco Routers
- Cisco Routers with IP Security Protocol
- Supported Configurations

Recommended Cisco Routers

For optimum interoperability, Cisco recommends using the following VPN-based routers when setting up a network with Cisco Secure VPN Client:

- Cisco 7100 VPN routers for large enterprises
- Cisco 2600 or Cisco 3600 series routers for medium-sized businesses
- Cisco 1720 VPN routers for small offices

Cisco Routers with IP Security Protocol

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

- Cisco 1600 series routers
- Cisco 1740 series routers
- Cisco 2500 series routers
- Cisco 2600 series routers
- Cisco 3600 series routers
- Cisco 4000 (Cisco 4000, 4000-M, 4500, 4500-M, 4700, 4700-M) series routers
- Cisco 7100 series routers
- Cisco 7200 series routers
- Cisco 7500 series routers
- Cisco AS5300 universal access servers

Supported Configurations

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

- Static or Dynamic Client IP Addresses with Pre-shared Keys
- Static or Dynamic Client IP Addresses with Digital Certificates
- Dynamic Client IP Addressing with IKE Mode Configuration

For a comparative listing of the advantages and disadvantages of using pre-shared keys and digital certificates for your configuration, see “Pre-shared Keys versus Digital Certificates.”

Static or Dynamic Client IP Addresses with Pre-shared Keys

Using predefined, static IP addresses for the Cisco Secure VPN Client, you can generate pre-shared keys for a secure tunnel between the client and a Cisco router. Pre-shared keys are simple to implement, yet are not as scalable as digital certificates. For this reason, pre-shared keys are recommended for smaller networks (up to 10 clients).

For dynamic IP addressing for pre-shared keys, refer to “Dynamic Client IP Addressing with IKE Mode Configuration.”

Static or Dynamic Client IP Addresses with Digital Certificates

Using predefined IP addresses for the Cisco Secure VPN Client, you can request that a certification authority (CA) assign to you a digital certificate. Digital certificates offer more scalability than pre-shared keys, and are usually implemented on larger networks (more than 10 clients).

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

For dynamic IP addressing, refer to “Dynamic Client IP Addressing with IKE Mode Configuration.”

Dynamic Client IP Addressing with IKE Mode Configuration

IKE Mode Configuration occurs before an IPSec tunnel is established. This feature allows the Cisco router to dynamically assign an IP address to the client. After IKE Mode Configuration, either pre-shared keys or digital certificates can be used to authenticate the peer to establish an encrypted tunnel.

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)

These client-side requirements are needed to install and operate the Cisco Secure VPN Client:

- **PC-compatible Computer**—Pentium processor or equivalent
- **Operating System**—One of the following operating systems:
 - Microsoft Windows 98
 - Microsoft Windows 95
 - Microsoft Windows NT 4.0 (with Service Pack 3 or 4)
- **Minimum RAM**—Depending on your operating system:
 - 16 MB RAM for Windows 95
 - 32 MB RAM for Windows 98
 - 32 MB RAM for Windows NT 4.0
- **Available Hard Disk Space**—Approximately 9 MB
- **Software Installation**—CD-ROM drive
- **Interoperability Requirements**—Cisco IOS Release 12.0(4)XE and later releases
- **Communications Protocol**—Native Microsoft TCP/IP
- **Dial-up Connections**—Modem, internal or external, non-encrypting, or Native Microsoft PPP dialer
- **Network Connections**—Ethernet

Server-side Requirements (Hardware and Software)

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

- One of the following Cisco routers:
 - A Cisco 1700 series router (Recommended for small networks)
 - A Cisco 2600 or Cisco 3600 series router (Recommended for medium-sized networks)
 - A Cisco 7100 VPN router (Recommended for large networks)
 - Any Cisco IOS router (See “Cisco Routers with IP Security Protocol.”)
- Depending on the Cisco router selected, one of the following Cisco IOS IPsec software images:
 - For a Cisco 1700 series router or a Cisco 7100 VPN router, a supporting Cisco IOS IPsec software image from Cisco IOS Release 12.0(4)XE or later releases, including Release 12.0(5)T
 - For all other Cisco IOS routers, a supporting Cisco IOS IPsec software image from Cisco IOS Release 12.0(5)T or later releases

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
- Pre-shared Keys versus Digital Certificates
- Static versus Dynamic IP Addresses on the Client
- Cisco Secure VPN Client versus Other VPN Solutions

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.	Scalable to larger networks.	—
Client creates a VPN over PSTN and Internet using IPSec.	—	NAS creates a VPN over Internet using L2F.	PSTN is not secured.

Pre-shared Keys versus Digital Certificates

Table 1-2 outlines the advantages and disadvantages of pre-shared keys and digital certificates.

Table 1-2 Pre-shared Keys and Digital Certificates

Pre-shared Keys		Digital Certificates	
Pros	Cons	Pros	Cons
Pre-shared keys common in small networks of up to 10 clients.	Network is less scalable with pre-shared keys than with digital certificates. Router must be reconfigured with each additional client.	Network is more scalable with digital certificates than with pre-shared keys. You can configure unlimited clients.	Digital certificates can become complex.
There is no need to involve a CA for security.	—	Digital certificates allow for device authentication and overall more secure authentication.	Outside CA is required.

Static versus Dynamic IP Addresses on the Client

A static IP address is a unique IP address that is assigned to a client for an extended period of time, to be used by only that client. A dynamic IP address is an IP address that is temporarily assigned as part of a login session, to be returned to an IP pool at the end of the session. Use dynamic IP addresses to allocate your IP addresses. Do not use dynamic IP addresses if you have network address translation (NAT) or firewalling installed on the router into which the client dials. Remote users with dynamic IP addresses require dynamic crypto maps on the router at the enterprise.

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 and a router. Cisco Secure VPN Client is also scalable to large networks when used with digital certificates.



Using Pre-shared Keys: A Business Case

Documentation for pre-shared keys will be available in a later release of this guide. For more information, refer to “New and Changed Information” in the preface.





Using Digital Certificates: Business Case Introduction

This chapter describes how Cisco Secure VPN Client interoperates with a Cisco router using digital certificates. Using IPSec, digital certificates allow devices to be automatically authenticated to each other without the manual key exchanges required by Cisco Encryption Technology.

- Benefits of Using Digital Certificates
- Business Case Description
- Supported Digital Certificates
- Related Documentation



Note

Throughout this chapter, there are numerous configuration examples and sample configuration outputs that include unusable IP addresses. Be sure to use your own IP addresses when configuring your client and Cisco router.

Benefits of Using Digital Certificates

The benefits of digital certificates over pre-shared keys are as follows:

- Digital certificates are scaleable, which means that they can support a large enterprise network.
- Digital certificates authenticate devices.
- Digital certificates are more complex than pre-shared keys, but offer a more secure method of authentication.

Business Case Description

The following business scenario is an example of one case in which you might employ the Cisco Secure VPN Client with a Cisco router.

- The Challenge
- The Risk
- The Solution

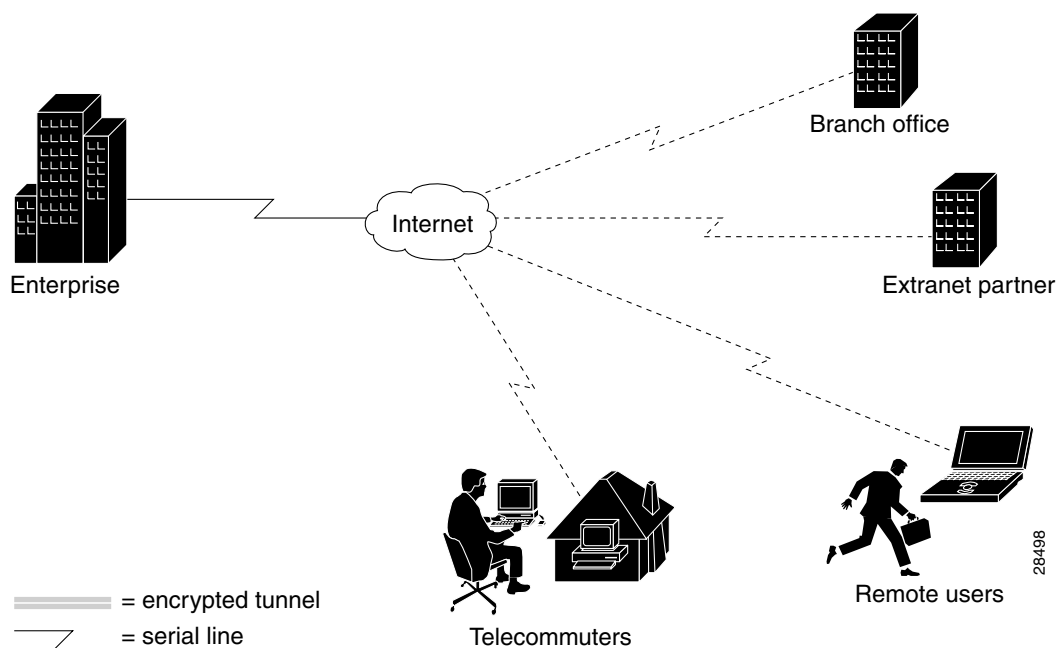
The Challenge

A large enterprise is represented by over 5,000 employees. Many of the sales employees alternate working environments between the main campus, small branch offices, and remote clients. The engineering development team works primarily at the main campus, and occasionally telecommute from home. The sales force works remotely giving product demonstration and information to customers, the engineering team adds new and improved functionality to the existing products. The sales force requires immediate access to the latest enhancements to the products. The sales force needs secure data transactions between their remote location and the main campus. Also, the telecommuting engineers require a secure connection between their home and the main campus.

The Risk

Figure 3-1 shows what happens when data that is secure within a large enterprise network gets transmitted over an insecure, public network such as the Internet. The data may remain secure (represented by the solid flow of data in the figure) inside the enterprise network; but once it is outside the firewall, the data is vulnerable to attack (as represented by the dashed flow of data). A third-party can intercept the data for the purpose of trading your company secrets for profit, replacing confidential documents with false data, or manipulating the existing data.

Figure 3-1 Security Risk of Transmitting Data over an Unprotected, Public Network



The Solution

Figure 3-2 shows what happens when data is transmitted using Cisco Secure VPN Client and a Cisco router to establish a secure, encrypted tunnel through which the data travels (as represented by the tunnel in the figure). From the enterprise network to the remote user, the data remains secure within the client-initiated encrypting tunnel. This solution demonstrates the Cisco Secure VPN Client and its interaction with a Cisco router to provide a secure, encrypted tunnel for data transmission.

Figure 3-2 Digital Certificates—Secure Data Transmission Using Cisco Secure VPN Client

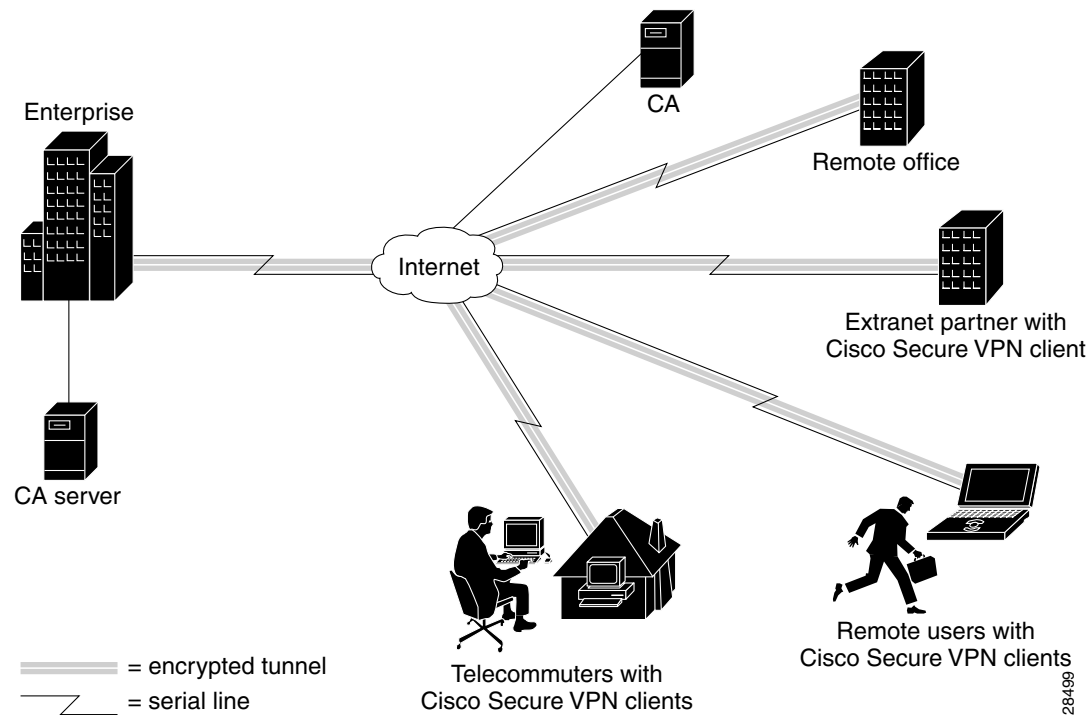
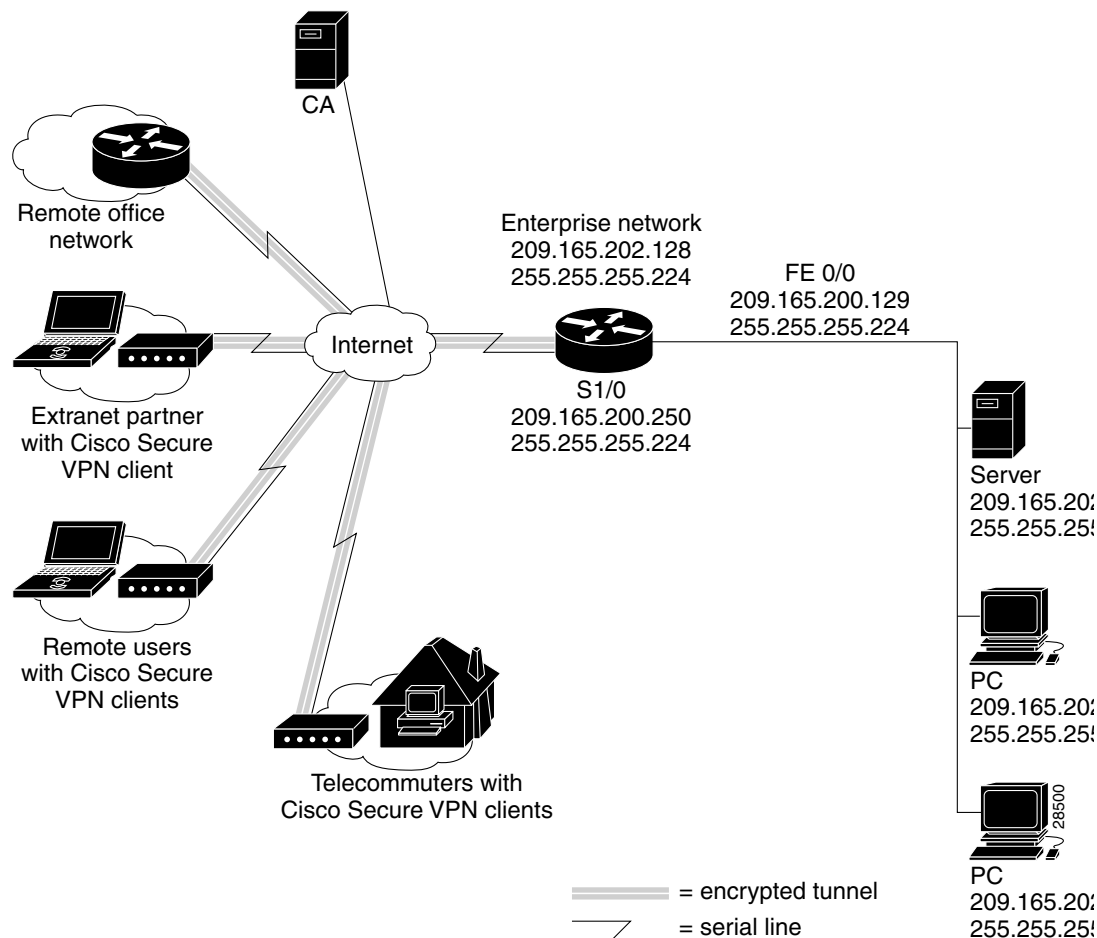


Figure 3-3 shows the physical elements of the scenario. The Internet is the main medium through which data communications occur.

Figure 3-3 Physical Elements—Digital Certificates with the Cisco Secure VPN Client



The telecommuters, remote users, and extranet partners have pre-configured Cisco Secure VPN Clients. For a more secure solution, the remote office might have nested tunnels configured on its client for more secure transform sets than a router-to-router transform set, although the client is not required for an Intranet-based VPN.

The large enterprise uses the Cisco 7140-2T3 as a gateway router. The Cisco 7140-2T3 router has two-high speed synchronous serial T3 interfaces, two Fast Ethernet 10/100BaseT autosensing interfaces.

Cisco 7000 family routers are supported in the following Cisco IOS Releases:

- Cisco IOS Release 12.0(4)XE and later releases
- Cisco IOS Release 12.0(5)T and later releases

These releases support the Cisco IOS Firewall feature set. The Cisco IOS Firewall feature set provides encryption services within the large enterprise.

**Note**

Any model of the Cisco 7100, with compatible interfaces and hardware modules, will work in this scenario. For Cisco 7100 documentation, see “Related Documentation.”

Also, any Cisco IOS router that supports IPSec will work instead of a Cisco 7100. For a list of supported routers, see the “System Requirements” section in Chapter 1 of this guide. For Cisco IOS router documentation, see “Related Documentation.”

The responsibilities of the different components of this VPN are as follows:

- Remote User, Telecommuter and Extranet Partner—Purchase digital certificates from the certification authority (CA). Configures clients with IP addresses set up by system administrator.
- System Administrator at Enterprise—Purchases, installs, and configures Cisco Secure VPN Client on remote users PCs. Assigns static or dynamic IP address on the clients or through the VPN router. Purchases and configures digital certificates for the enterprise Cisco router. Installs the server.
- CA Administrator at CA—Purchases, installs, and configures CA server. Generates digital certificates for clients on CA server. Provides system administrators with root CA certificate.
- ISP—Supplies clients with static IP addresses. Purchases, configures, and maintains the NAS. The NAS is the point-of-presence (POP) used to forward PPP sessions to the enterprise customer’s network. Supports and maintains in-house modem pools. Maintains an authentication, authorization, and accounting (AAA) server that authenticates the IP tunnel endpoint and domain name assigned to the enterprise customer’s gateway. Maintains an edge router that connects the ISP’s network to the enterprise customer’s network.

**Note**

This guide is not intended to provide ISP configuration as it is outside the scope of configuring a client-to-router connection. For information on how to secure tunnels between an ISP and an enterprise, refer to the *Access VPN Solutions Using Tunneling Technology Solutions Guide*.

Table 3-1 provides a functional description of the sequence of events that take place when establishing a client-initiated VPN using digital certificates.

Table 3-1 Protocol Negotiation and Security Association Sequence

Event	Description
1.	Either the ISP assigns an IP address to the client or the router that has been configured for IKE Mode Configuration may assign an IP address to the client.
2.	The remote user uses the client’s digital certificate to authenticate the Cisco router. Each router has its own digital certificate.
3.	The routers and clients digitally sign data and exchange certificate information using IKE. Negotiation is completed and IPSec security associations can be established.
4.	The client uses the tunnel encapsulation method to establish a secure connection to the router.

Supported Digital Certificates

This guide contains a separate chapter for each type of digital certificate supported by Cisco for use with the Cisco Secure VPN Client. You may configure a secure tunnel between the Cisco Secure VPN Client and a Cisco router by following the procedures in the following chapters:

- Chapter 4, “Using Entrust Digital Certificates: A Business Case”
- Chapter 5, “Using VeriSign Digital Certificates: A Business Case”



Note

Cisco Secure VPN Client may be interoperable with other digital certificates, however, Cisco does not currently support these and you would have to do your own troubleshooting. Cisco recommends using the Cisco-supported digital certificates, as they have been thoroughly tested and have been deemed deployable for customers.

Related Documentation

For more information on configuring the Cisco Secure VPN Client and digital certificates on a Cisco router, refer to Table 3-2.

Table 3-2 Related Documentation for Digital Certification

Document Title ¹	Customer Order Number	Path
Cisco Secure VPN Client Documentation		
Cisco Secure VPN Client <ul style="list-style-type: none"> • Quick Start Guide • Release Notes • Solutions Guide 	<ul style="list-style-type: none"> • DOC-786898 • DOC-786929 • OL-0259 	Hardware and Software Documentation: <ul style="list-style-type: none"> • CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Internet Service Unit Documentation>Cisco Secure VPN Client
Internetworking Solutions Guides Documentation		
<i>Access VPN Solutions Using Tunneling Technology</i>	<ul style="list-style-type: none"> • OL-0293 	Hardware and Software Documentation: <ul style="list-style-type: none"> • CCO²>Service & Support>Technical Documents>Documentation Home Page>Technology Information>Internetworking Solutions Guides>Access VPN Solutions Using Tunneling Technology

Table 3-2 Related Documentation for Digital Certification (continued)

Document Title ¹	Customer Order Number	Path
Cisco IOS Release 12.0 Documentation		
<i>Security Configuration Guide</i> <ul style="list-style-type: none"> “Configuring IPSec Network Security” “Configuring Certification Authority Interoperability” 	<ul style="list-style-type: none"> DOC-785843 See Path.³ See Path.³ 	Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>Configuration Guide and Command References>Security Configuration Guide
<i>Security Command Reference</i> <ul style="list-style-type: none"> “IPSec Network Security Commands” “Certification Authority Interoperability Commands” 	<ul style="list-style-type: none"> DOC-785845 See Path.³ See Path.³ 	Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>Configuration Guide and Command References>Security Command Reference
New Feature Documentation	<ul style="list-style-type: none"> See Path.³ 	Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>New Feature Documentation
Cisco 7000 Family Routers		
Cisco 7100 Router <ul style="list-style-type: none"> Quick Start Guide Installation and Configuration Guide VPN Configuration Guide Reg. Comp. and Safety Information Release Notes for Release 12.0 XE Port and Service Adapters Field Replaceable Units 	<ul style="list-style-type: none"> DOC-786343 DOC-786341 DOC-786342 DOC-786345 DOC-786019 See Path.³ See Path.³ 	Hardware and Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Core/High-End Routers>Cisco 7100 Release Notes Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>Release Notes>Cisco 7000 Family Routers>Cisco 7000 Family - Release Notes for Cisco Release 12.0 XE

Table 3-2 *Related Documentation for Digital Certification (continued)*

Document Title ¹	Customer Order Number	Path
Cisco IOS Router Documentation		
<ul style="list-style-type: none"> Modular Access Routers Access Servers Core/High-End Routers 	<ul style="list-style-type: none"> See Path.³ See Path.³ See Path.³ 	<p>Modular Access Routers Documentation:</p> <p>CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Access Servers and Access Routers>Modular Access Routers</p> <p>Access Servers Documentation:</p> <p>CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Access Servers and Access Routers>Access Servers</p> <p>Core/High-End Routers Documentation:</p> <p>CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Core/High-End Routers></p>

1. If you are viewing this guide online, the hyperlinks in this column are subject to change without notice. If this occurs, refer to the Path column.

2. Cisco Connection Online (CCO) is located at <http://www.cisco.com>. For more information, see “Cisco Connection Online.”

3. In the Path column, refer to the CCO path for a listing of the available publications.



Using Entrust Digital Certificates: A Business Case

This chapter describes how Cisco Secure VPN Client interoperates with a Cisco router using Entrust digital certificates. Using IPSec, digital certificates allow devices to be automatically authenticated to each other without the manual key exchanges required by Cisco Encryption Technology.

- Benefits of Using Entrust Digital Certificates
- Configuring and Verifying
- Related Documentation

Benefits of Using Entrust Digital Certificates

For of the benefits of using digital certificates, refer to the “Benefits of Using Digital Certificates” section in Chapter 3, “Using Digital Certificates: Business Case Introduction.”

Configuring and Verifying

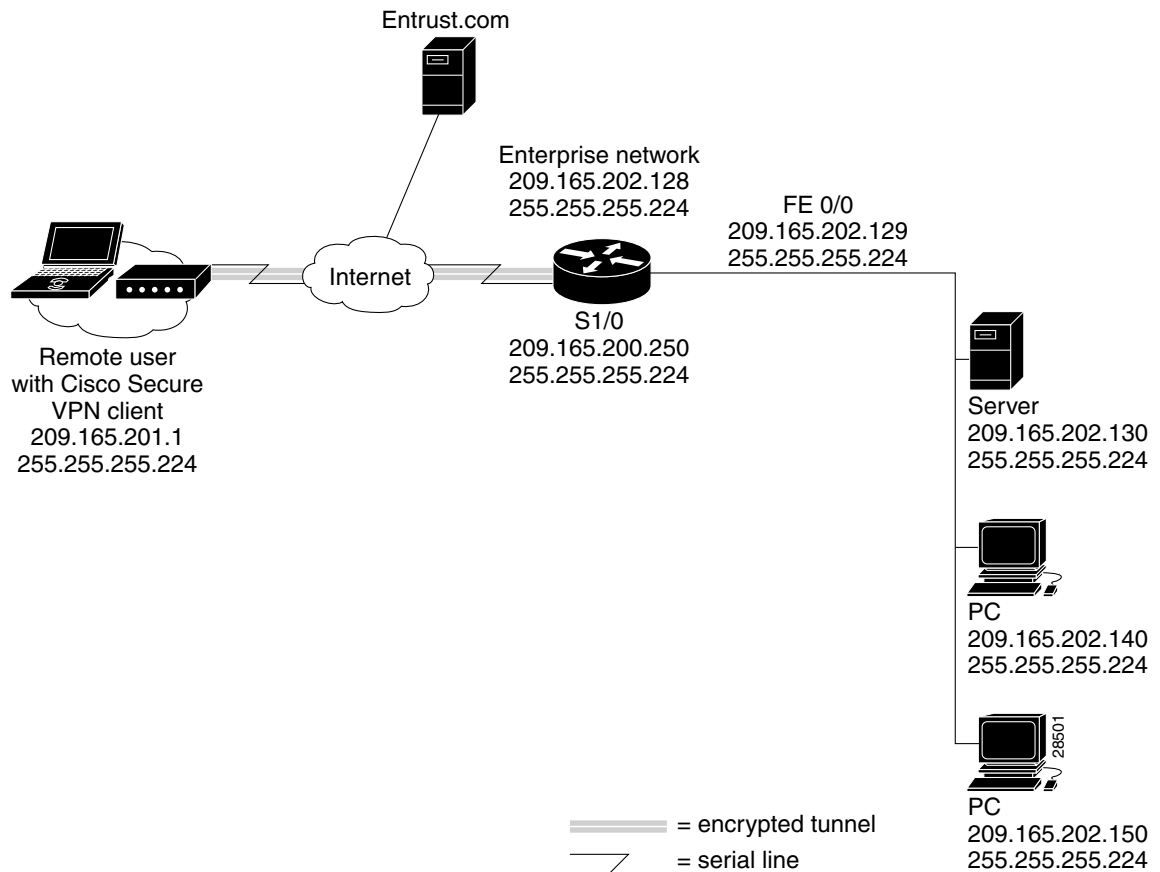
- Configuring Entrust Digital Certifications
- Verifying Entrust Digital Certifications

Configuring Entrust Digital Certifications

Configuring Entrust digital certificates for a secure IPSec tunnel between a remote client and a Cisco router involves the following tasks:

- Configuring the Cisco Secure VPN Client
- Configuring the Cisco Router

Figure 4-1 Physical Elements—Entrust Configuration Topology

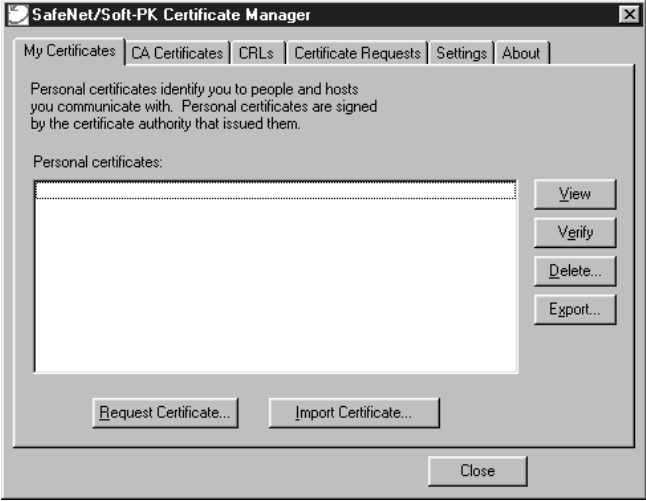
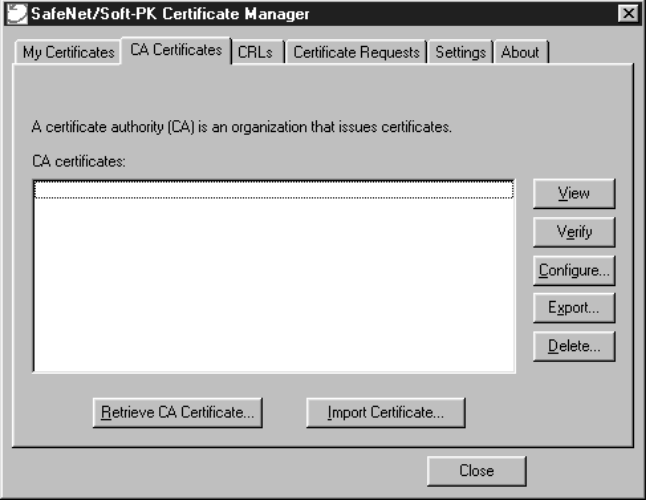


Configuring the Cisco Secure VPN Client

Configuring the Cisco Secure VPN Client requires the following tasks:

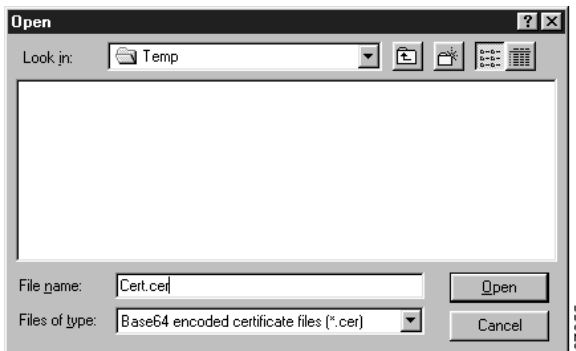
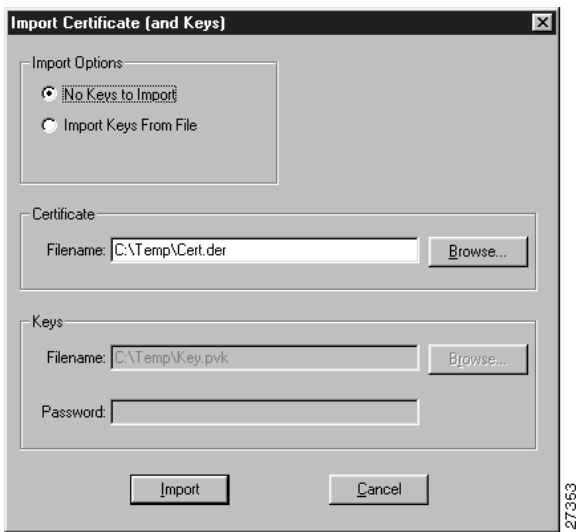
- Task 1—Importing the Root CA Certificate
- Task 2—Creating Public and Private Key Pair
- Task 3—Requesting Client Certificate from Entrust CA Server
- Task 4—Submitting the Certification Request to the Entrust Server
- Task 5—Importing Your Signed Entrust Digital Certificate
- Task 6—Configuring Other Connections for Security Policy
- Task 7—Configuring A New Connection for Security Policy
- Task 8—Specifying Identity Using RSA Signature
- Task 9—Specifying Encryption and Authentication Methods for Authentication, Phase 1
- Task 10—Specifying Encryption and Authentication Methods for Key Exchange, Phase 2
- Task 11—Saving Your Configuration

Task 1—Importing the Root CA Certificate

Task 1—Importing the Root CA Certificate		
Command	Purpose	
Step 1	Click Start>Programs>SafeNet/Soft-PK>Certificate Manager . The SafeNet/Soft-PK Certificate Manager dialog box appears.	Open the Certificate Manager . The Certificate Manager allows you to request, import, and store the digital certificates that you receive from the certification authority (CA).
		
Step 2	<div>a. Click the CA Certificates tab.</div> <div>b. Click Import Certificate.</div>	Use the CA Certificates folder to retrieve, import, view, verify, configure, export, or delete the certificates you receive from the CA.
		

Task 1—Importing the Root CA Certificate

Command	Purpose
<p>Step 3 The Import Certificate (and Keys) dialog box appears.</p> <ol style="list-style-type: none"> In the Import Certificate (and Keys) dialog box, enter the following information: <ul style="list-style-type: none"> Under Import Options, select the No Keys to Import option. Obtain the root CA file from the system administrator, who should also supply you with the URL for IPSec CSR enrollment. The system administrator gets the root CA file and URL from the CA Administrator. Rename the root CA file with a “.cer” filename extension. Under Certificate, click Browse. 	<p>Import your CA root file certificate.</p> <p>There are three reasons to import a certificate rather than retrieving it:</p> <ul style="list-style-type: none"> You decide not to request a personal certificate online, and you need to reimport the certificate file your CA returned to you. You want to import a CA certificate that was downloaded directly from the CA’s web site. In the following events: <ul style="list-style-type: none"> Your computer crashes. Your files are corrupted. You need to copy your certificate from one computer to another. You are upgrading client software. You would need the certificate file you or your network administrator exported from My Certificates or CA Certificates as a backup.
<p>Step 4 The Open dialog box appears.</p> <ol style="list-style-type: none"> In the Files of Type list, click Base64 encoded certificate files. Locate the root CA file (the “.cer” file). Click Open. 	<p>Open the root CA file for importing to the CA Certificates folder.</p>



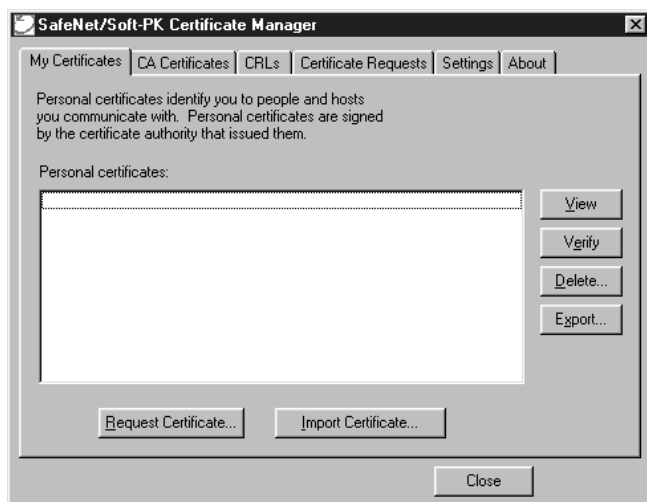
Task 1—Importing the Root CA Certificate

	Command	Purpose
Step 5	<p>The Import Certificate (and Keys) dialog box appears.</p> <ol style="list-style-type: none"> Click Import. Add the certificate to the Root Store. 	Add the CA root file to your list of CA Certificates.

Task 2—Creating Public and Private Key Pair

Task 2—Creating Public and Private Key Pair


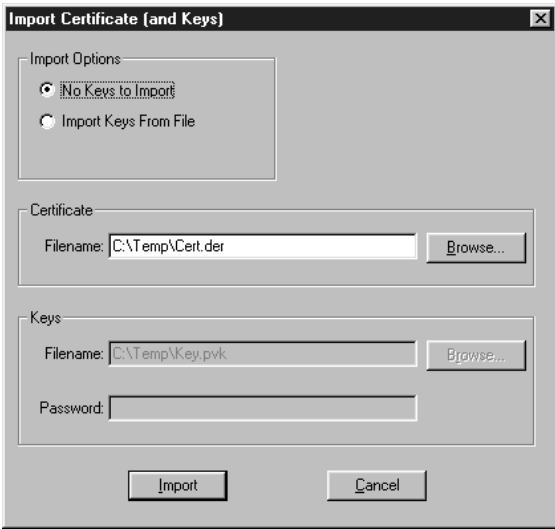
	Command	Purpose
Step 1	<ol style="list-style-type: none"> In the Certificate Manager dialog box, click the My Certificates tab. Click Request Certificate. 	Use the My Certificates folder to retrieve, import, view, verify, configure, export, or delete your personal certificate.



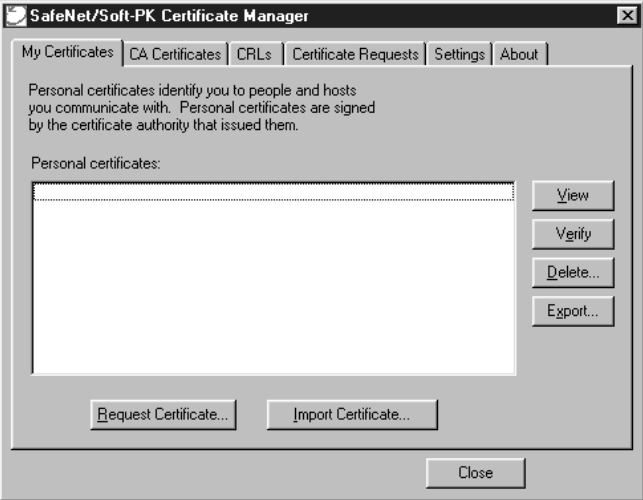
Note

You must have your root CA certificate before requesting a personal certificate. Otherwise, only a file-based request is possible.

Task 2—Creating Public and Private Key Pair

Command	Purpose
<p>Step 2 The Online Certificate Request dialog box appears.</p> <ol style="list-style-type: none"> In the Online Certificate Request dialog box, fill in the following section: <ul style="list-style-type: none"> Under Subject Information, fill in the following fields: <ul style="list-style-type: none"> In the Name field, enter the name of the certificate owner. In the Department field, enter the department for which this certificate will be configured. In the Company field, enter the company for which this certificate will be configured. In the State field, enter the state in which this certificate request was created. In the Country field, enter the country in which this certificate was created. In the Email field, enter the email account of the person associated with this certificate request. In the Domain Name field, enter the name of the domain for your business. In the IP Address field, do not enter anything. In the Request File section, perform the following tasks: <ul style="list-style-type: none"> In the Filename field, enter the filename of the certificate request or click Browse to locate the certificate request on your hard drive. <ol style="list-style-type: none"> Click OK. The client will generate public/private key pairs. 	<p>Enroll online for your personal certificate.</p> <p>You can configure a certificate request for online or file-based enrollment.</p> <ul style="list-style-type: none"> To configure an online enrollment, you must click the CA Certificate tab in the Certificate Manager dialog box, and retrieve a CA certificate first. <p> Note This information binds your identity to a public key that others will look for in a public key directory. Entering inaccurate or misleading information defeats the purpose of using public key.</p>
	

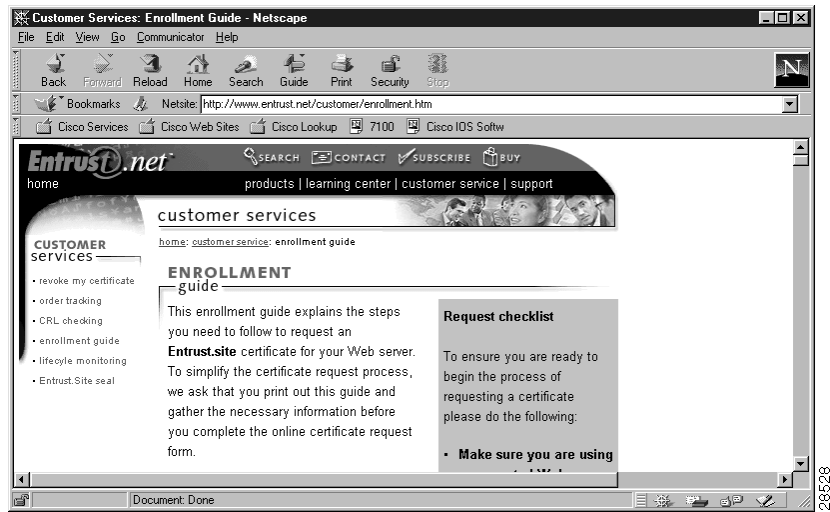
Task 3—Requesting Client Certificate from Entrust CA Server

Task 3—Requesting Client Certificate from Entrust CA Server	
Command	Purpose
<div>a. In the Certificate Manager dialog box, click the My Certificates tab.</div> <div>b. Click Request Certificate.</div> <div></div>	Request your personal certificate.

Task 4—Submitting the Certification Request to the Entrust Server

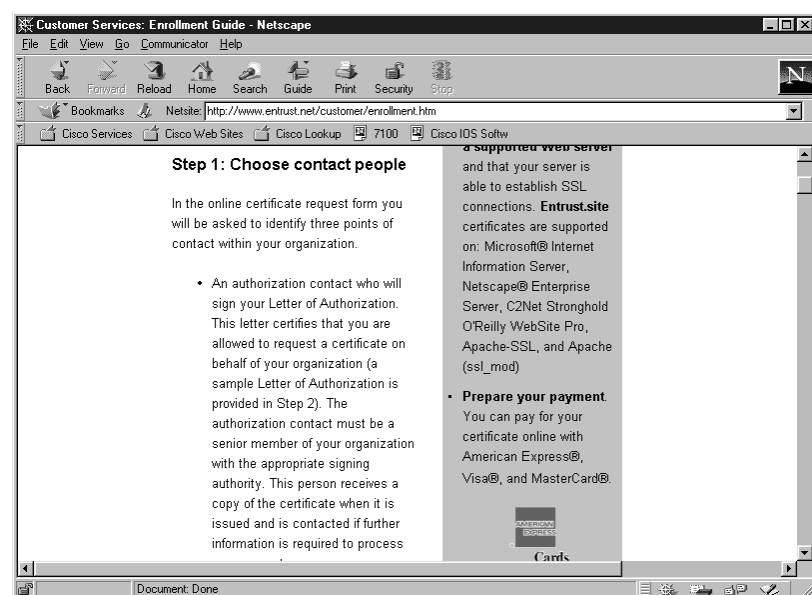
Task 4—Submitting the Certification Request to the Entrust Server

Command	Purpose
<p>Step 1</p> <p>a. Open your browser.</p> <p>b. Navigate to the Enrollment URL provided by your CA Administrator. For example:</p> <p>http://www.entrust.net/customer/enrollment.htm</p> <p>This web page consists of seven steps to securing an Entrust.site certificate.</p> <ul style="list-style-type: none"> • Choose Contact People • Print and Submit the Letter of Authentication • Confirm Proof of Right • Confirm Ownership of Domain Name • Submit CSR and Enter Server Information • Confirm Request Information • Make Payment 	<p>Print out and read the Enrollment Guide provided by Entrust before buying your digital certificate.</p>



Task 4—Submitting the Certification Request to the Entrust Server

Command	Purpose
Step 2 <ol style="list-style-type: none"> Choose an authorization contact to sign your Letter of Authorization. Be sure to include name, phone number, company, title, and email address. Choose a technical contact to receive the issued certificate and to be notified about certificate renewals and updates. Be sure to include name, phone number, company, title, and email address. Choose a security contact who understands security issues, to whom Entrust can send security-related information such as security news and Web security alerts. Be sure to include name, phone number, company, title, and email address. 	Establish authorization, technical, and security contacts.



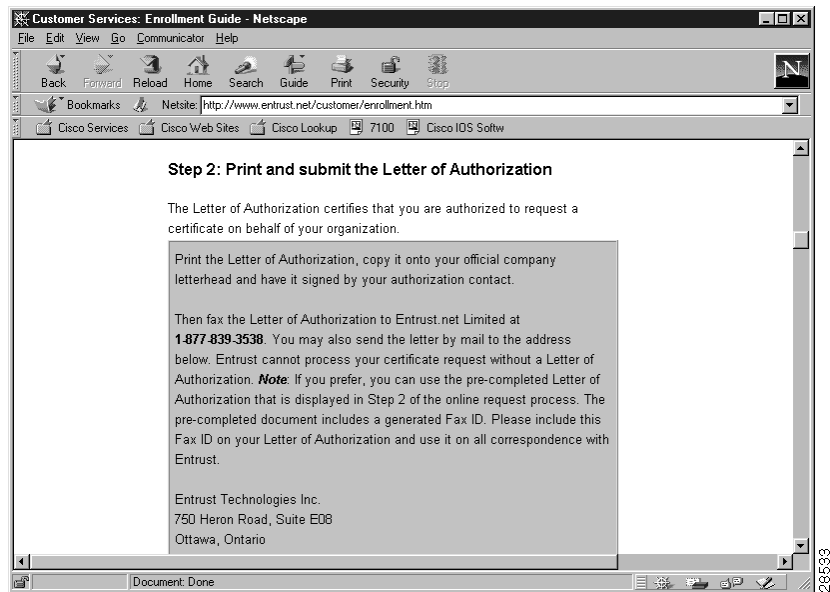
Task 4—Submitting the Certification Request to the Entrust Server

Command

Purpose

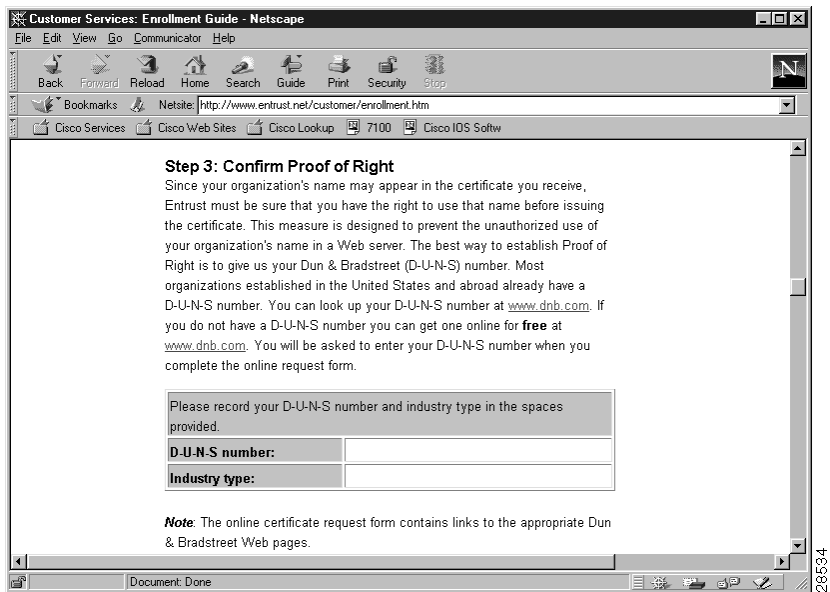
Step 3 Fill out the Letter of Authorization and submit it to the Entrust.net administrator.

The Letter of Authorization certifies that you are authorized to request a certificate on behalf of your organization.



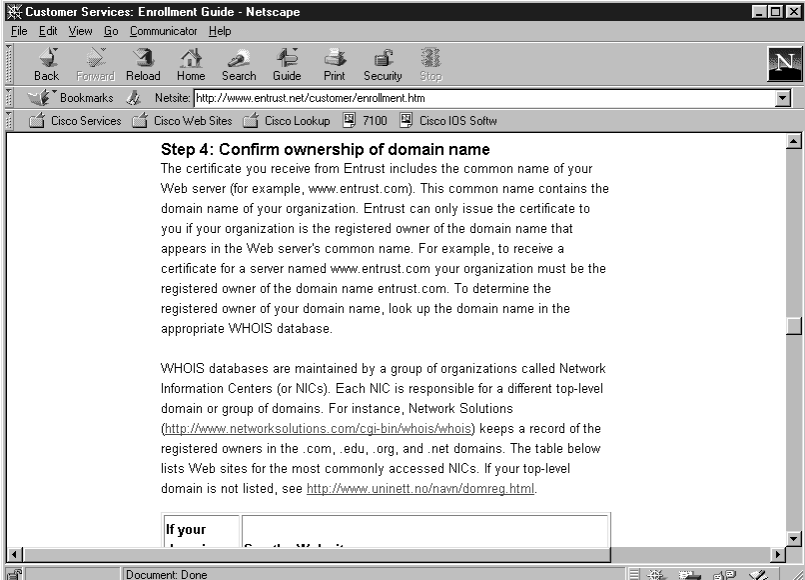
Step 4 Enter your Dun & Bradstreet (D-U-N-S) number for Proof of Right.

A D-U-N-S number is proof of right that you have the authority to use your organization's name before the the CA issues the certificate. This measure is designed to prevent the unauthorized use of your organization's name in a web server.



- If your organization is located in the United States, you may look up your D-U-N-S number at <https://www.dnb.com/product/eupdate/update.htm>.
- If your organization does not have a D-U-N-S number you can use, you may obtain one for free at <http://www.dnb.com/dunsno/whereduns.htm#own>.

Task 4—Submitting the Certification Request to the Entrust Server

Command	Purpose
Step 5 Enter your domain name and the registered owner of the domain. Be sure to include domain name, name of the owner, company name, and address.	<p>The certificate you receive from Entrust includes the common name of your web server (for example, www.entrust.com). This common name contains the domain name of your organization. Entrust can only issue the certificate to you if your organization is the registered owner of the domain name that appears in the web server's common name. For example, to receive a certificate for a server named www.entrust.com your organization must be the registered owner of the domain name www.entrust.com.</p>
 <p>Step 4: Confirm ownership of domain name</p> <p>The certificate you receive from Entrust includes the common name of your Web server (for example, www.entrust.com). This common name contains the domain name of your organization. Entrust can only issue the certificate to you if your organization is the registered owner of the domain name that appears in the Web server's common name. For example, to receive a certificate for a server named www.entrust.com your organization must be the registered owner of the domain name www.entrust.com. To determine the registered owner of your domain name, look up the domain name in the appropriate WHOIS database.</p> <p>WHOIS databases are maintained by a group of organizations called Network Information Centers (or NICs). Each NIC is responsible for a different top-level domain or group of domains. For instance, Network Solutions (http://www.networksolutions.com/cgi-bin/whois/whois) keeps a record of the registered owners in the .com, .edu, .org, and .net domains. The table below lists Web sites for the most commonly accessed NICs. If your top-level domain is not listed, see http://www.uninett.no/navn/domreg.html.</p> <p>If your</p>	28532

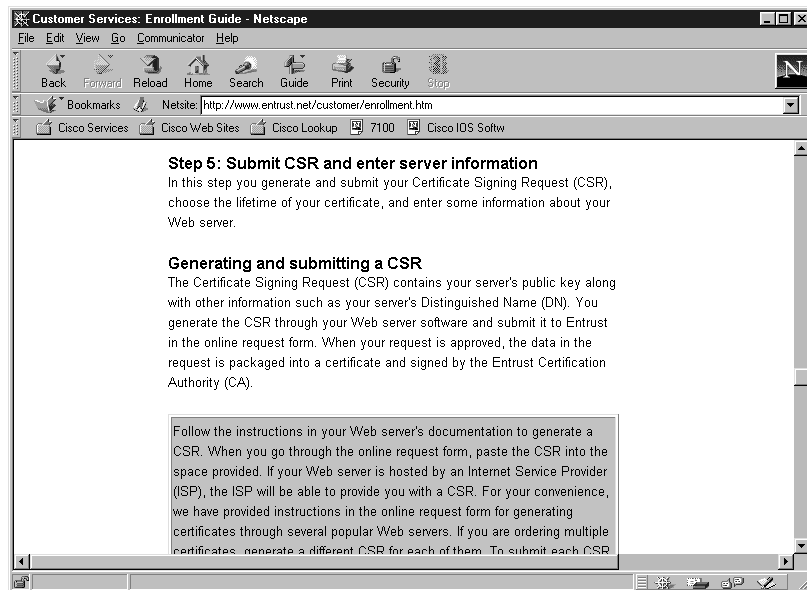
Task 4—Submitting the Certification Request to the Entrust Server

Command

Purpose

Step 6 Generate and submit your Certificate Signing Request (CSR), choose the lifetime of your certificate, and enter web server information.

The Certificate Signing Request (CSR) contains your server's public key along with other information such as your server's Distinguished Name (DN). You generate the CSR through your web server software and submit it to Entrust in the online request form. When your request is approved, the data in the request is packaged into a certificate and signed by the Entrust CA.



When you create a CSR a cryptographic key pair is generated. The public key is inserted into the CSR and subsequently signed by the Entrust CA. The private key remains on your computer. Be sure to securely back up the private key. If the private key is lost or becomes corrupt you will not be able to use your certificate.



Note

The private key is a very sensitive piece of information. Those with access to your private key could decrypt the SSL-protected data sent and received by your web server. Please take appropriate steps to ensure there is no unauthorized access to the private key.

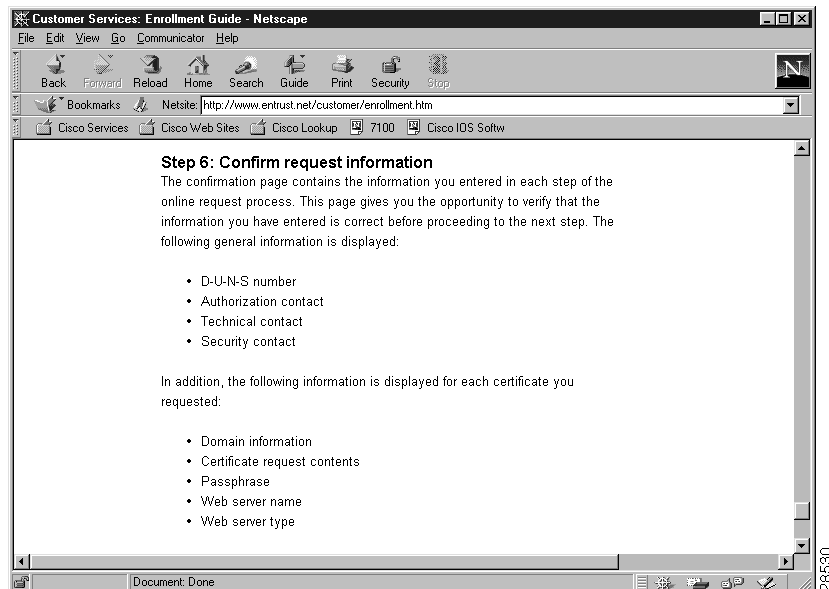
Task 4—Submitting the Certification Request to the Entrust Server

Command

Purpose

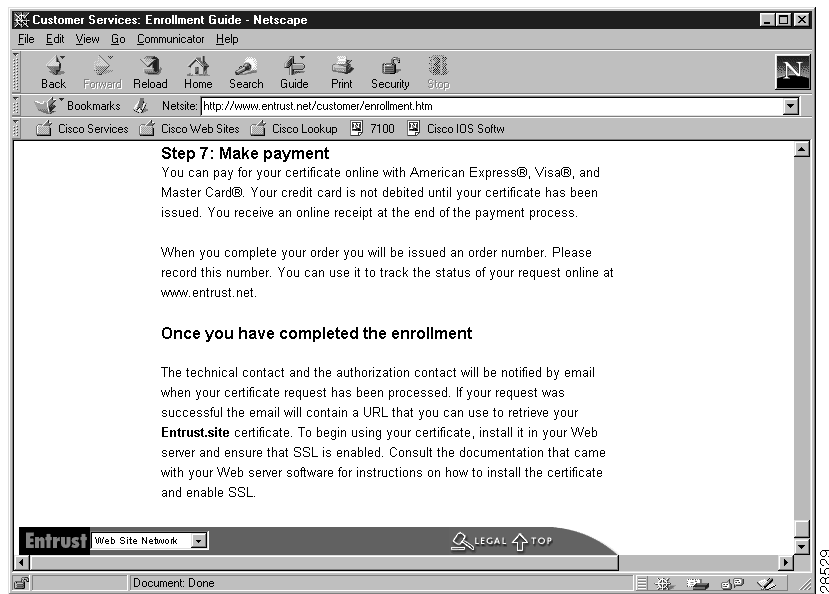
Step 7 Make sure the information that you entered appears correctly.

Verify that the information you have entered is correct before proceeding to the next step.

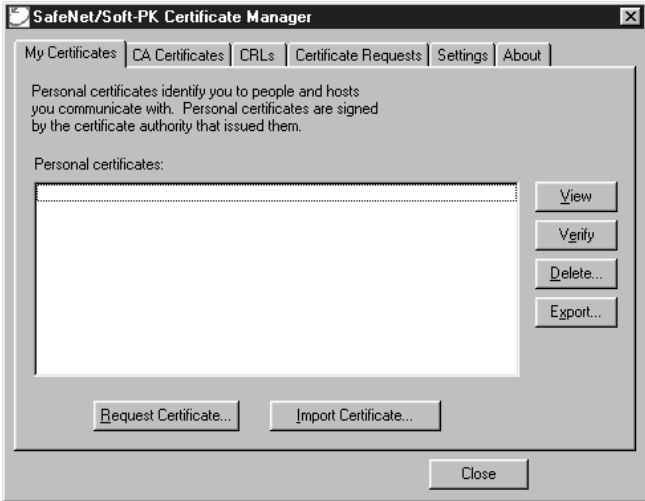


Step 8 Pay for your digital certificate.

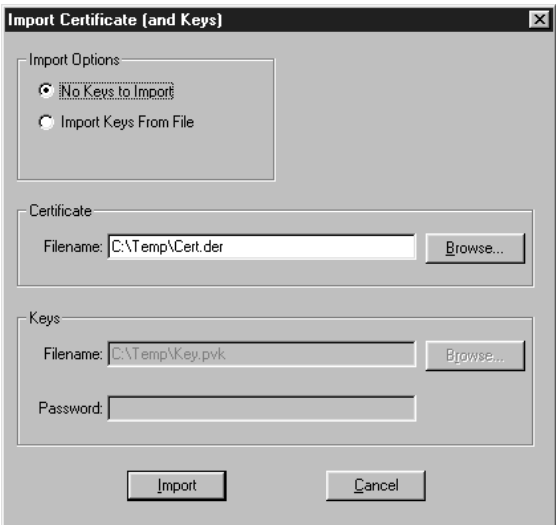
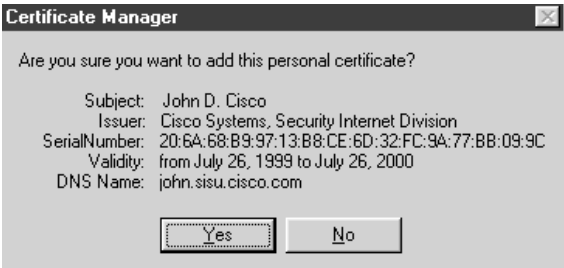
After submitting the request to the CA, you will be charged upon receipt of your digital certificate.



Task 5—Importing Your Signed Entrust Digital Certificate

Task 5—Importing Your Signed Entrust Digital Certificate		
	Command	Purpose
Step 1	<div><div>a. Click Start>Programs>SafeNet/Soft-PK>Certificate Manager.</div><div>b. Then, click the My Certificates tab.</div><div>c. Click Import Certificate.</div></div>	<div>The CA Administrator should have sent a signed digital certificate through email. This process will import your signed digital certificate.</div>
	<div><div></div><div>27342</div></div>	

Task 5—Importing Your Signed Entrust Digital Certificate

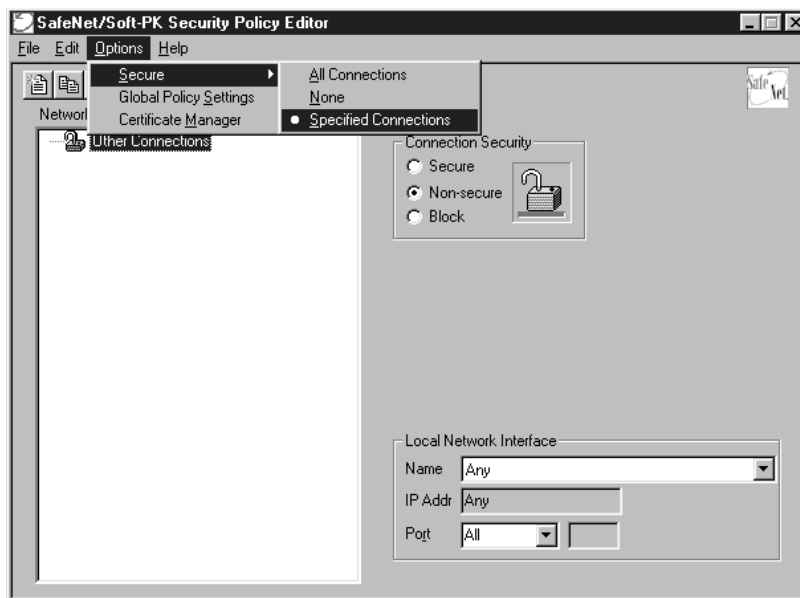
Command	Purpose
<p>Step 2 The Import Certificate (and Keys) dialog box appears.</p> <ol style="list-style-type: none"> In the Import Certificate (and Keys) dialog box, perform the following tasks: <ul style="list-style-type: none"> Under Import Options, click the No Keys to Import option. Under Certificate, click Browse. In the Files of Type list, click Base64 encoded certificate files. Add your signed digital certificate. Rename the file with a “.cer” filename extension. Under Keys, click Browse. Select your signed digital certificate. Click Import. 	<p>Import your signed digital certificate.</p> <p>There are three reasons to import a digital certificate rather than retrieving it:</p> <ul style="list-style-type: none"> You decide not to request a personal certificate online, and you need to reimport the certificate file your CA returned to you. You want to import a CA certificate that was downloaded directly from the CA's web site. In the following events: <ul style="list-style-type: none"> Your computer crashes. Your files are corrupted. You need to copy your certificate from one computer to another. You are upgrading client software. You would need the certificate file you or your network administrator exported from My Certificates or CA Certificates as a backup.
	<p>Step 3 The Certificate Manager confirmation dialog box appears. Click Yes to confirm.</p>
	<p>Your signed digital certificate will be imported once you confirm it is the correct one to add.</p>

Task 6—Configuring Other Connections for Security Policy

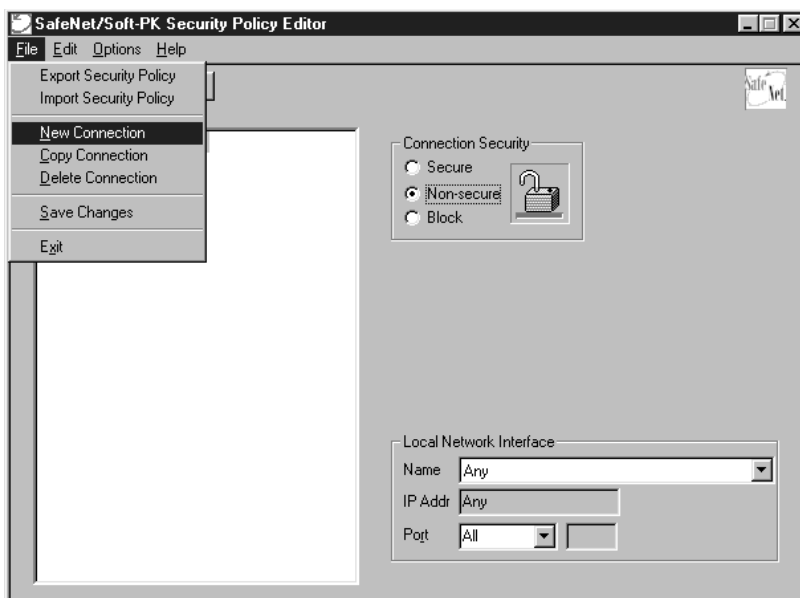
Task 6—Configuring Other Connections for Security Policy		
	Command	Purpose
Step 1	Click Start>Programs>SafeNet/Soft-PK>Security Policy Editor . The SafeNet/Soft-PK Security Policy Editor dialog box appears.	Use the Security Policy Editor to do the following: <ul style="list-style-type: none">• Establish connections and their associated proposals.• List connections in a hierarchical order that defines an IP data communications security policy.
<div><div><div>SafeNet/Soft-PK Security Policy Editor</div><div><div>File Edit Options Help</div><div><div><div>Network Security Policy</div><div>Other Connections</div></div><div><div>Connection Security</div><div><div><div><div>Secure</div><div>Non-secure</div><div>Block</div></div><div><div><div></div><div></div><div></div></div></div></div><div><div>Local Network Interface</div><div><div><div>Name</div><div>Any</div></div><div><div>IP Addr</div><div>Any</div></div><div><div>Port</div><div>All</div></div></div></div></div></div></div><div>27358</div></div></div></div>		

Task 6—Configuring Other Connections for Security Policy

Command	Purpose
Step 2 On the Options menu, click Secure>Specified Connections .	<p>Establish policies for individual connections using two main steps:</p> <ol style="list-style-type: none"> 1. Configuring “Other Connections” 2. Adding and configuring new connections <p>A new connection is a set of security parameters that pertain to an individual remote IP connection.</p> <p>You can create any number of new connections and name them. The system tests for a match between an incoming transmission and the proposed policies you have established, in the order in which they are listed in the Cisco Secure VPN Client Security Policy Editor dialog box. If you find that you need to reorder the sequence of policies, you can do so by moving them up or down within the Network Security Policy list. Remember that “Other Connections” is always the last rule in your list of security policies.</p>
Step 3 <ol style="list-style-type: none"> In the left pane, select Other Connections. In the right pane, under Connection Security, click the Non-Secure option. 	<p>Configure the default connection called Other Connections as the first step in establishing security policies for individual connections. For all IP communications that do not adhere to the security policies defined in the individual connections, Other Connections acts as a default.</p> <p>Click the Non-Secure radio button to allow IP communications for this connection to pass through unsecured. This will allow you to chance the settings under your Local Network Interface.</p>

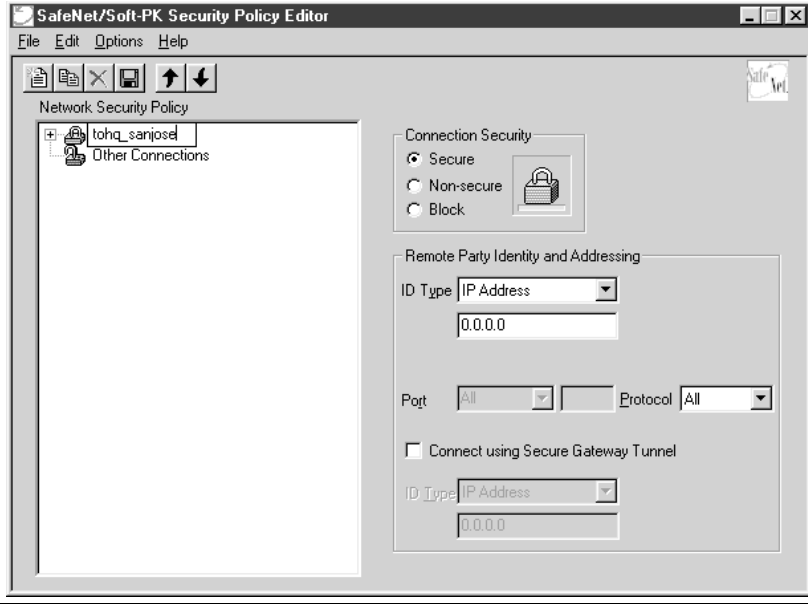


27363



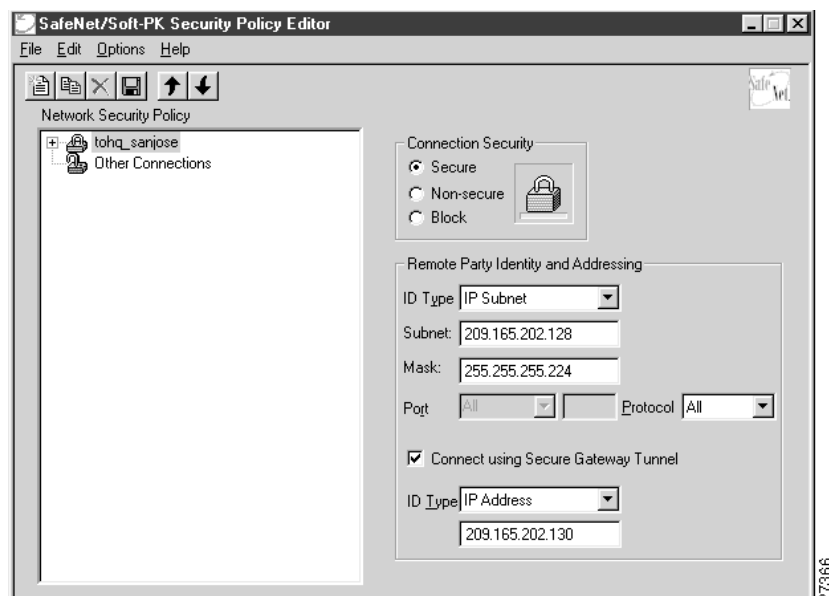
27364

Task 7—Configuring A New Connection for Security Policy

Task 7—Configuring A New Connection for Security Policy		
	Command	Purpose
Step 1	<ol style="list-style-type: none"> In the left pane, select the name of a connection (for instance, Other Connections). On the File menu, click New Connection. In the left pane, the default New Connection placeholder will appear. In its place, create a unique name for the connection to your router. For example, if your router name is <code>hq_sanjose</code>, you might rename the connection <code>tohq_sanjose</code>. 	<p>Create a new connection by contacting the other party for information, including the destination:</p> <ul style="list-style-type: none"> IP address Network IP address IPSec-compliant gateway device's IP address, if any) Domain name Email address IP subnet IP address range Subject's identity information <ul style="list-style-type: none"> Name Department Company State Country
		

Task 7—Configuring A New Connection for Security Policy

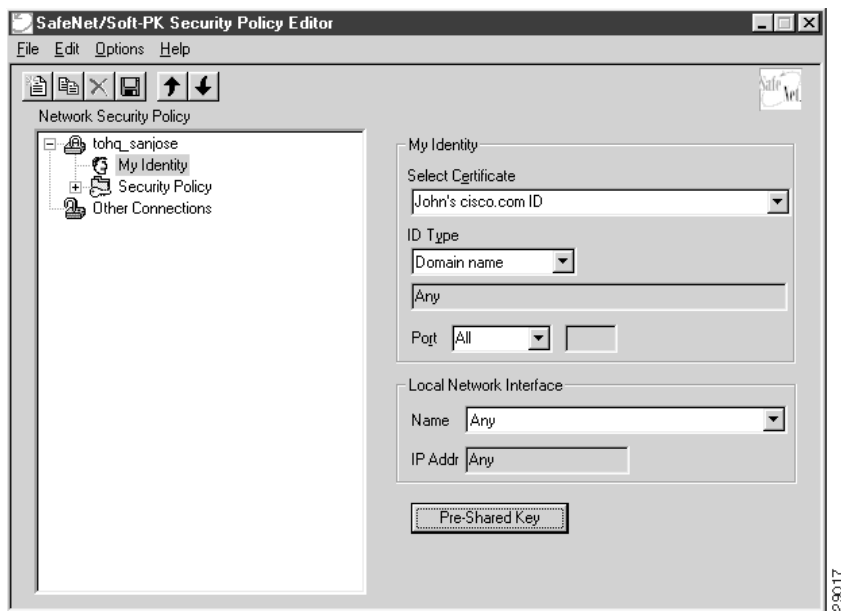
Command	Purpose
Step 2 <ol style="list-style-type: none"> In the left pane, click tohq_sanjose. In the right pane, configure the following parameters for tohq_sanjose: <ul style="list-style-type: none"> Under Connection Security, click the Secure option. Under Remote Party Identity and Addressing, select the following items: <ul style="list-style-type: none"> In the ID Type list, click IP Subnet. In the Subnet list, click 209.165.202.128 In the Mask list, click 255.255.255.224. All traffic (all protocols) destined for 209.165.202.128 will be encrypted and secure. The Port list and entry field are inactive as a default. In the Protocol list, click All. Select the Connect using Secure Gateway Tunnel check box. In the ID_Type list, click IP Address. In the ID_Type box, enter the IP address, 209.165.202.130. 	<p>Fill in the fields according to the information you received from the other party.</p> <ul style="list-style-type: none"> Secure option—Secures the IP communications for this connection. ID Type list—Lists type of identification of the other party. Subnet list—Enter the other party's subnet. Mask list—Enter the other party's subnet mask. Port list—A default of “All” secures all protocol ports. Connect using Secure Gateway Tunnel check box—Specify that the other party is protected by a secure IPSec-compliant gateway, such as a firewall, by selecting this check box. ID_Type list—Lists identification type of the gateway. ID_Type box—Enter the IP address of the gateway.



Task 8—Specifying Identity Using RSA Signature

Task 8—Specifying Identity Using RSA Signature

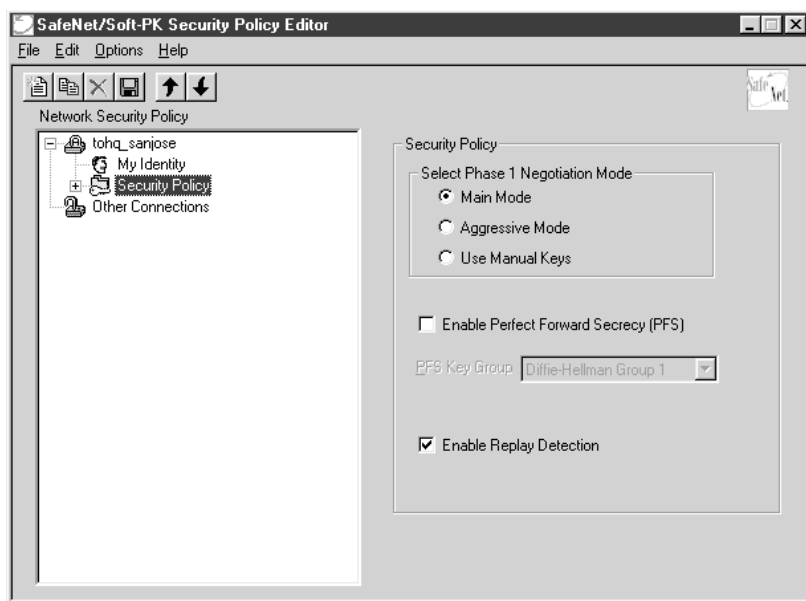
Command	Purpose
<p>Step 1</p> <ol style="list-style-type: none"> In the left pane, double-click tohq_sanjose. tohq_sanjose expands with My Identity and Security Policy. Click My Identity. The My Identity window appears. In the right pane, set the following parameters: <ul style="list-style-type: none"> Under My Identity, select the following items: <ul style="list-style-type: none"> In the Select Certificate list, click <i>your signed certificate</i>. In the ID_Type list, click IP Address. In the Port list, click All. Under Local Network Interface, select the following items: <ul style="list-style-type: none"> In the Name list, click Any. The IP Addr list is inactive as a default. 	<p>Select an identification that will allow the other party to identify you during the key exchange phase.</p> <ul style="list-style-type: none"> Select Certificate—Select your digital certificate. ID_Type—Select IP address. Port—A default of “All” secures all protocol ports.



29017

Task 8—Specifying Identity Using RSA Signature

Command	Purpose
<p>Step 2</p> <ol style="list-style-type: none"> In the left pane, under My Identity, double-click Security Policy. In the right pane, under Security Policy, specify the following items: <ul style="list-style-type: none"> Select Main Mode option. Select the Enable Replay Detection check box. 	<p>Click the Main Mode option, and select the Enable Replay Detection check box to set authentication requirements for your security policy.</p> <ul style="list-style-type: none"> Main Mode—Authentication method that protects identities by not revealing them until secure communications have been established. Enable Replay Detection—When selected, this counter determines whether or not a packet is unique. This prevents falsification of data.

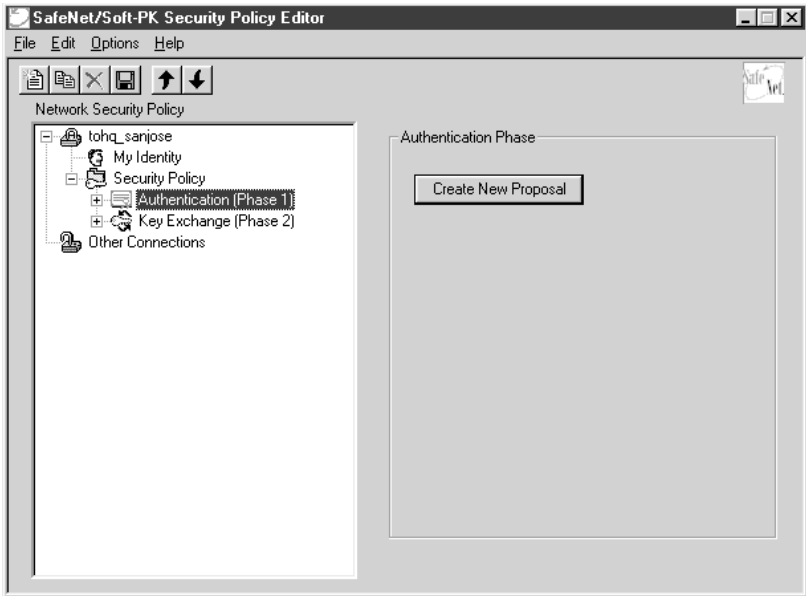


27389

Task 9—Specifying Encryption and Authentication Methods for Authentication, Phase 1

Task 9—Specifying Encryption and Authentication Methods for Authentication, Phase 1

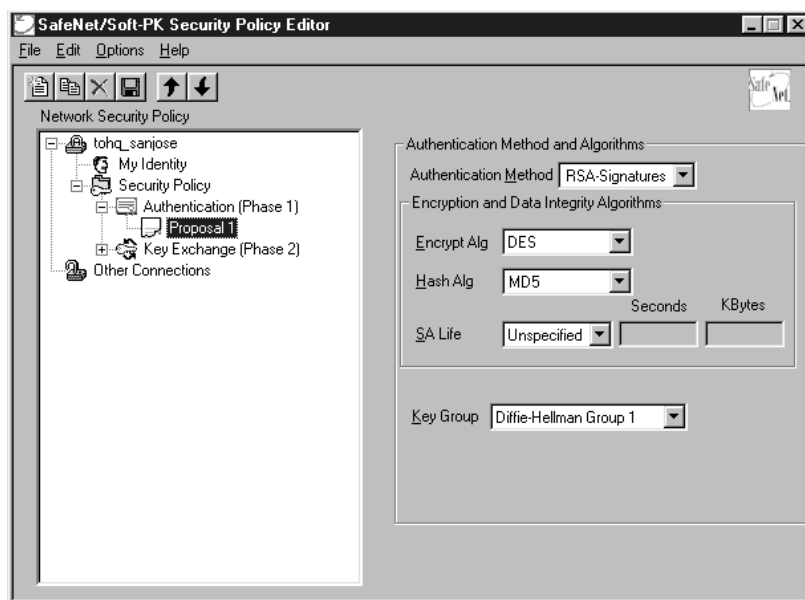
Command	Purpose
<p>Step 1</p> <ol style="list-style-type: none"> In the left pane, double-click Security Policy, then click Authentication (Phase 1). In the right pane, under Authentication Phase, perform the following task: <ul style="list-style-type: none"> Click Create New Proposal. 	<p>During Authentication (Phase 1), you and the trusted party will reveal your identities and negotiate how they will secure phase 2 communications.</p> <p>Before securing communications, the two parties involved negotiate the method they will use. Proposals are presented to the other party in the order in which they are sequenced in the Network Security Policy list. You can reorder the proposals after you create them.</p>



27370

Task 9—Specifying Encryption and Authentication Methods for Authentication, Phase 1

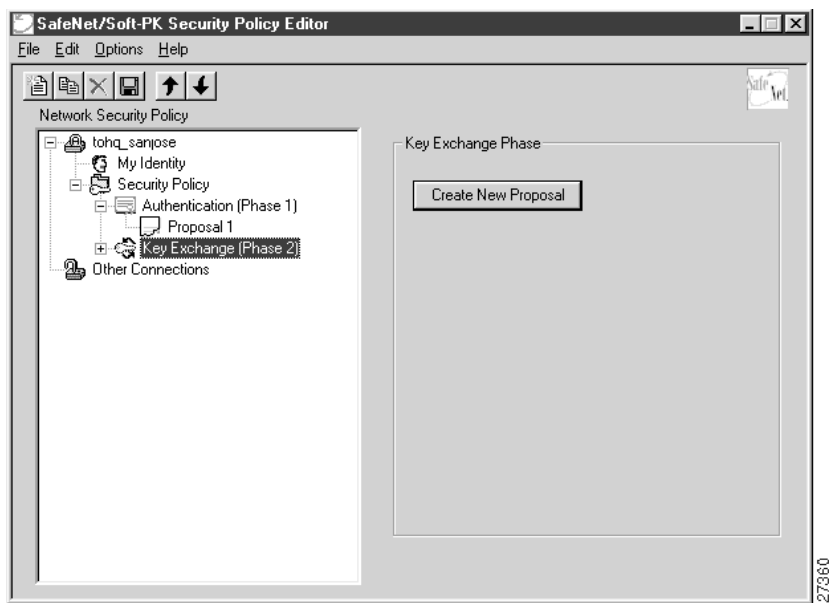
Command	Purpose
Step 2 <ol style="list-style-type: none"> In the left pane, under Authentication (Phase 1), a new Proposal appears called Proposal 1. In the right pane, under Authentication Method and Algorithms, perform the following tasks: <ul style="list-style-type: none"> In the Authentication Method list, click RSA-Signatures. Under Encryption and Data Integrity Algorithms, perform the following tasks: <ul style="list-style-type: none"> In the Encrypt Alg list, click DES. In the Hash Alg list, click MD5. In the SA Life list, click Unspecified. In the Key Group list, click Diffie-Hellman Group 1. 	Define the authentication method for the proposal. <ul style="list-style-type: none"> Authentication Method—Indicates the method of authentication. Encrypt Alg—Select DES for minimal security, Triple-DES for highest security, or Null for none at all. Depending on the IPSec image on your Cisco router, you will enter either DES or Triple-DES. Hash Alg—Select MD5 for minimal security, SHA-1 for highest security, or DES-MAC.



Note DES-MAC is currently not supported with Cisco IOS software.

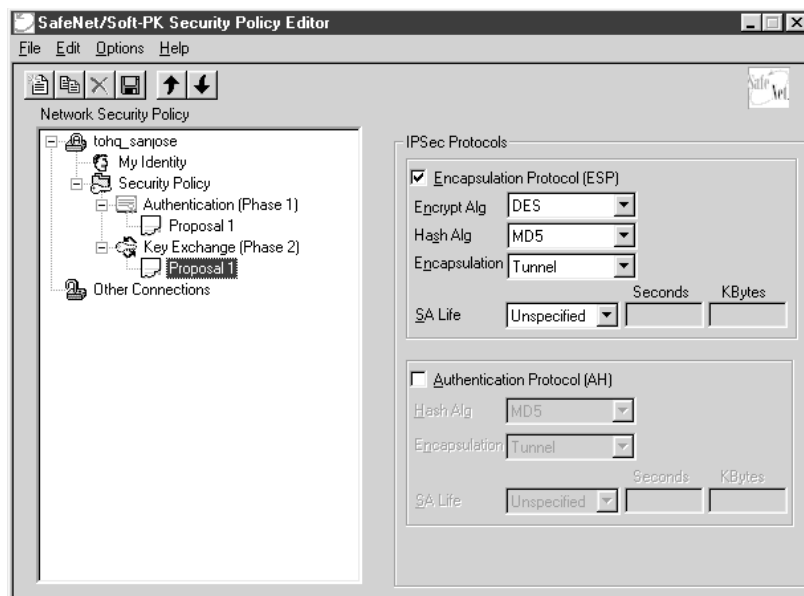
- SA Life**—Optionally, specify the period for which the key is valid.
- Key Group**—Allows you to select with Diffie-Hellman Group to use.

Task 10—Specifying Encryption and Authentication Methods for Key Exchange, Phase 2

Task 10—Specifying Encryption and Authentication Methods for Key Exchange, Phase 2		
Command		Purpose
<p>a. In the left pane, under Authentication (Phase 1), select Key Exchange (Phase 2).</p> <p>b. In the right pane, under Key Exchange Phase section, click Create New Proposal.</p>		<p>Negotiate which key exchange method of securing communications you and the other party will use by establishing a proposal.</p>
		

Task 10—Specifying Encryption and Authentication Methods for Key Exchange, Phase 2

Command	Purpose
<p>Step 2</p> <ol style="list-style-type: none"> In the left pane, under Key Exchange (Phase 2), a new proposal appears called Proposal 1. In the right pane, under IPsec Protocols, perform the following tasks: <ul style="list-style-type: none"> Select the Encapsulation Protocol check box. In the Encryption Alg list, click DES. In the Hash Alg list, click MD5. In the Encapsulation list, click Tunnel. 	<p>Define the key exchange method for the proposal.</p> <ul style="list-style-type: none"> Encapsulation Protocol—Indicates the method of authentication. Encryption Alg—Select DES for minimal security, Triple-DES for highest security, or Null for none at all. Depending on the IPsec image on your Cisco router, you will enter either DES or Triple-DES. Hash Alg—Select MD5 for minimal security, SHA-1 for highest security, or DES-MAC. <p>Note DES-MAC is currently not supported with Cisco IOS.</p> <ul style="list-style-type: none"> Encapsulation—Tunnel is the only method of encapsulation available for the Cisco Secure VPN Client. <p>Note Transport mode can be used only if the two end devices are both providing IPsec protection. Otherwise, you must use tunnel mode.</p>



Task 11—Saving Your Configuration

Task 11—Saving Your Configuration

Command	Purpose
<ol style="list-style-type: none"> On the File menu, click Save Changes to save the policies. When the Security Policy Editor dialog box appears, click OK. 	<p>Save your policies for implementation.</p>



Configuring the Cisco Router

Configuring the Cisco router requires the following tasks:

- Task 1—Configuring the Domain Name, Host Name, and Name Server
- Task 2—Configuring ISAKMP Policy and Defining IPSec Transform Set
- Task 3—Defining Crypto Dynamic Map and IKE Crypto Map to the Client
- Task 4—Defining the CA, Enrolling Your Certificate, and Requesting Certificate Signature
- Task 5—Applying the Crypto Map to the Interface

Task 1—Configuring the Domain Name, Host Name, and Name Server

Task 1—Configuring the Domain Name, Host Name, and Name Server		
	Command	Purpose
Step 1	router> enable	Enter privileged EXEC mode.
Step 2	router# configure terminal Enter configuration commands, one per line. End with CNTL/Z.	Enter global configuration mode.
Step 3	router(config)# ip domain-name sisu.cisco.com	Define the domain name. Enter your domain name.
Step 4	router(config)# hostname hq_sanjose hq_sanjose(config)#	Define the host name. Enter your host name
Step 5	hq_sanjose(config)# ip name-server 209.165.202.130	Define the name server. Enter the gateway IP address.

Task 2—Configuring ISAKMP Policy and Defining IPSec Transform Set

Task 2—Configuring ISAKMP Policy and Defining IPSec Transform Set		
	Command	Purpose
Step 1	hq_sanjose(config)# crypto isakmp policy 3 hq_sanjose(config-isakmp)# encryption des hq_sanjose(config-isakmp)# hash MD5 hq_sanjose(config-isakmp)# authentication rsa-sig hq_sanjose(config-isakmp)# exit	To define an IKE policy, use the crypto isakmp policy global configuration command. This command invokes the ISAKMP policy configuration (config-isakmp) command mode. IKE policies define a set of parameters to be used during the IKE negotiation.

Task 2—Configuring ISAKMP Policy and Defining IPsec Transform Set

	Command	Purpose
Step 2	<pre>hq_sanjose(config)# crypto ipsec transform-set ciscots esp-des esp-md5-hmac hq_sanjose(cfg-crypto-trans)# exit</pre>	<p>To define a transform set—an acceptable combination of security protocols and algorithms—use the crypto ipsec transform-set global configuration command. This command invokes the crypto transform configuration mode (cfg-crypto-trans).</p> <ul style="list-style-type: none"> • ciscots—Enter a unique name for this transform set. In this example, ciscots is used. • esp-des—ESP with the 56-bit DES encryption algorithm. • esp-md5-hmac—ESP with the MD5 (HMAC variant) authentication algorithm.

Task 3—Defining Crypto Dynamic Map and IKE Crypto Map to the Client**Task 3—Defining Crypto Dynamic Map and IKE Crypto Map to the Client**


	Command	Purpose
Step 1	<pre>hq_sanjose(config)# crypto dynamic-map ciscodm 4 hq_sanjose(cfg-crypto-dyn)# set transform-set ciscots hq_sanjose(cfg-crypto-dyn)# exit</pre>	<p>Associate the transform-set with a dynamic map. To create a dynamic crypto map entry, use the crypto dynamic-map global configuration command. Using this command puts you in dynamic crypto map configuration mode (cfg-crypto-dyn).</p> <ul style="list-style-type: none"> • ciscodm—Enter a unique name for this dynamic crypto map. In this example, ciscodm is used. • 4—Enter a number for this dynamic crypto map entry. <p>Apply the transform set to the crypto dynamic map. To specify which transform sets can be used with the crypto map entry, use the set transform-set crypto map configuration command.</p>
Step 2	<pre>hq_sanjose(config)# crypto map toclient 2 ipsec-isakmp dynamic ciscodm hq_sanjose(config-crypto-map)# exit</pre>	<p>Create a crypto map using IKE referencing the preexisting dynamic crypto map. To create or modify a crypto map entry and enter the crypto map configuration mode, use the crypto map global configuration command.</p> <ul style="list-style-type: none"> • toclient—Enter a unique name for this crypto map. In this example, toclient is used. • 2—Enter a number for this crypto map entry. • ipsec-isakmp—Indicates IKE will be used.

Task 4—Defining the CA, Enrolling Your Certificate, and Requesting Certificate Signature

Task 4—Defining the CA, Enrolling Your Certificate, and Requesting Certificate Signature

	Command	Purpose
Step 1	<pre>hq_sanjose(config)# crypto ca identity sisu.cisco.com hq_sanjose(cfg-ca-id)# enrollment mode ra hq_sanjose(cfg-ca-id)# enrollment url http://entrust-ca hq_sanjose(cfg-ca-id)# query url http://entrust-ca hq_sanjose(cfg-ca-id)# crl optional hq_sanjose(cfg-ca-id)# exit</pre>	Define Entrust enrollment commands. To declare the CA your router should use, use the crypto ca identity global configuration command. Using this command puts you into the ca-identity configuration mode, where you can specify characteristics for the CA.
Step 2	<pre>hq_sanjose(config)# crypto key generate rsa-usage mod 512 [signature key] mod 512 [encryption key]</pre>	<p>Generate the public and the private keys. The crypto key generate rsa-usage command creates two key-pairs for RSA:</p> <ul style="list-style-type: none"> • One key-pair for encryption • One key-pair for digital signatures <p>A key-pair refers to a public key and its corresponding secret key. If you do not specify “usage-keys” at the end of the command, the router will generate only one RSA key-pair and use it for both encryption and digital signatures.</p>
Step 3	<pre>hq_sanjose(config)# crypto ca authenticate sisu.cisco.com Certificate has the following attributes: Fingerprint: 103FXXXX 9D64XXXX 0AE7XXXX 626AXXXX % Do you accept this certificate? [yes/no]:yes</pre>	<p>Get the public key and CA server certificate. To authenticate the CA (by getting the CA's certificate), use the crypto ca authenticate global configuration command.</p> <p>At this point the router has a copy of the CA's certificate.</p> <p>Enter yes to accept the certificate.</p>
Step 4	<pre>hq_sanjose(config)# crypto ca enroll sisu.cisco.com</pre>	Send router's public key and get a signed certificate from the CA server. To obtain your router's certificate(s) from the CA, use the crypto ca enroll global configuration command.

Task 4—Defining the CA, Enrolling Your Certificate, and Requesting Certificate Signature

Command	Purpose
Step 5 Start certificate enrollment .. Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a proper note of it. Password: cisco1234 Re-enter password: cisco1234 % The subject name in the certificate will be: hq_sanjose.sisu.cisco.com % Include the router serial number in the subject name? [yes/no]: yes % The serial number in the certificate will be: 0431XXXX % Include an IP address in the subject name? [yes/no]: yes Interface: ethernet0 Request certificate from CA? [yes/no]: yes % Certificate request sent to Certificate Authority % The certificate request fingerprint will be displayed. % The 'show crypto ca certificate' command will also show the fingerprint. Fingerprint: C767XXXX 4721XXXX 0D1EXXXX C27EXXXX	 Note This is message text. Please read the message text, as might contain information about what to enter after it prompts you. At this point, the enrollment request is sent to the CA and is pending for the IPsec OnSite administrator's approval. The router will be polling every 2 minutes for the availability of the certificate. Wait until the router has retrieved the certificate. The router will display a message informing you that the certificate has been loaded.

Task 5—Applying the Crypto Map to the Interface**Task 5—Applying the Crypto Map to the Interface**

Command	Purpose
hq_sanjose(config)# interface ethernet0/0 hq_sanjose(config-if)# ip address 209.165.202.130 255.255.255.224 hq_sanjose(config-if)# crypto map toclient hq_sanjose(config-if)# exit	Apply the crypto map to the interface.

Verifying Entrust Digital Certifications

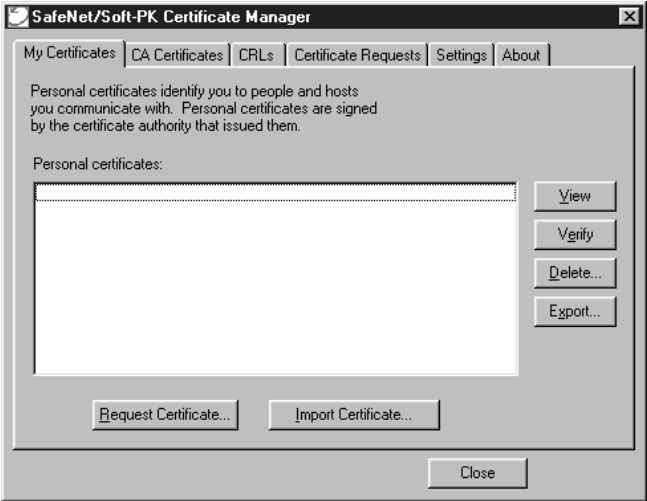
To verify that you have requested and your client has received your Entrust digital certification properly, monitor the status of your digital certificates in the Certificate Manager and issue **show** commands on your router. Verifying your digital certification includes the following tasks:

- Task 1—Viewing and Verifying Using Certificate Manager
- Task 2—Issuing Show Commands on Cisco Router

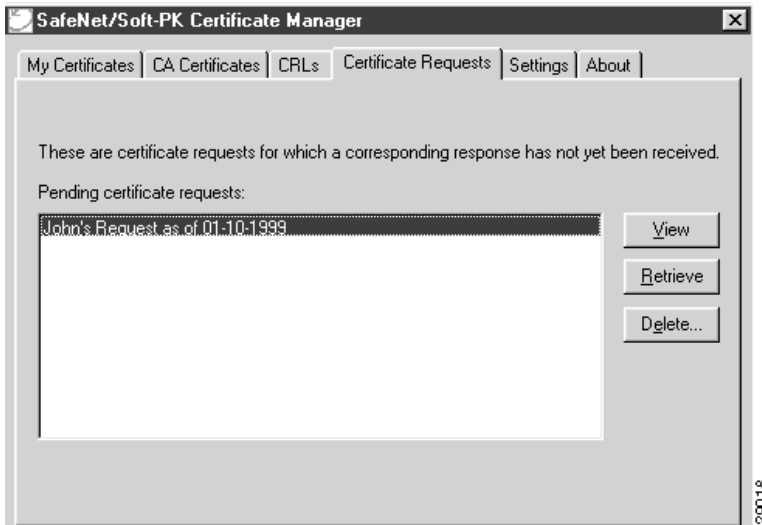
Task 1—Viewing and Verifying Using Certificate Manager

Task 1—Viewing and Verifying Using Certificate Manager

Command		Purpose
Step 1	In the Certificate Manager dialog box, click the My Certificates tab. Click View , then click Verify to confirm your digital certificate.	Your digital certification ID should appear under Personal Certificates. If your digital certificate does not appear here, go to the next step.



Task 1—Viewing and Verifying Using Certificate Manager

	Command	Purpose
Step 2	In the Certificate Manager dialog box, click the Certificate Requests tab. Check to see if you have sent in your request for the certificate.	Your certificate request should appear under Certificate Requests. If your certificate request does not appear here, go to the next step.
		
Step 3	Either you did not import the root CA file or you did not successfully import your personal digital certification from Entrust. See “Configuring the Cisco Secure VPN Client.”	Without the root CA file, you cannot import a digital certificate.

Task 2—Issuing Show Commands on Cisco Router**Task 2—Issuing Show Commands on Cisco Router**

	Command	Purpose
Step 1	show crypto key mypubkey rsa	View your router's RSA public keys.
Step 2	show crypto key pubkey-chain rsa	View a list of all the RSA public keys stored on your router. These include the public keys of peers who have sent your router their certificates during peer authentication for IPSec.

Task 2—Issuing Show Commands on Cisco Router

	Command	Purpose
Step 3	show crypto key pubkey-chain rsa [name <i>key-name</i> address <i>key-address</i>]	View details of a particular RSA public key stored on your router.
Step 4	show crypto ca certificates	View information about your certificate, the CA's certificate, and any RA certificates.

Related Documentation

For more information on configuring the Cisco Secure VPN Client and digital certificates on a Cisco router, refer to Table 4-1.

Table 4-1 Related Documentation for Digital Certification

Document Title ¹	Customer Order Number	Path
Cisco Secure VPN Client Documentation		
Cisco Secure VPN Client <ul style="list-style-type: none"> Quick Start Guide Release Notes Solutions Guide 	<ul style="list-style-type: none"> DOC-786898 DOC-786929 OL-0259 	Hardware and Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Internet Service Unit Documentation>Cisco Secure VPN Client
Internetworking Solutions Guides Documentation		
<i>Access VPN Solutions Using Tunneling Technology</i>	<ul style="list-style-type: none"> OL-0293 	Hardware and Software Documentation: <ul style="list-style-type: none"> CCO²>Service & Support>Technical Documents>Documentation Home Page>Technology Information>Internetworking Solutions Guides>Access VPN Solutions Using Tunneling Technology
Cisco IOS Release 12.0 Documentation		
<i>Security Configuration Guide</i> <ul style="list-style-type: none"> “Configuring IPsec Network Security” “Configuring Certification Authority Interoperability” 	<ul style="list-style-type: none"> DOC-785843 See Path.³ See Path.³ 	Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>Configuration Guide and Command References>Security Configuration Guide
<i>Security Command Reference</i> <ul style="list-style-type: none"> “IPsec Network Security Commands” “Certification Authority Interoperability Commands” 	<ul style="list-style-type: none"> DOC-785845 See Path.³ See Path.³ 	Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>Configuration Guide and Command References>Security Command Reference

Table 4-1 Related Documentation for Digital Certification (continued)

Document Title ¹	Customer Order Number	Path
New Feature Documentation	<ul style="list-style-type: none"> See Path.³ 	Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>New Feature Documentation
Cisco 7000 Family Routers		
Cisco 7100 Router <ul style="list-style-type: none"> Quick Start Guide Installation and Configuration Guide VPN Configuration Guide Reg. Comp. and Safety Information Release Notes for Release 12.0 XE Port and Service Adapters Field Replaceable Units 	<ul style="list-style-type: none"> DOC-786343 DOC-786341 DOC-786342 DOC-786345 DOC-786019 See Path.³ See Path.³ 	Hardware and Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Core/High-End Routers>Cisco 7100 Release Notes Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>Release Notes>Cisco 7000 Family Routers>Cisco 7000 Family - Release Notes for Cisco Release 12.0 XE

1. If you are viewing this guide online, the hyperlinks in this column are subject to change without notice. If this occurs, refer to the Path column.
2. Cisco Connection Online (CCO) is located at <http://www.cisco.com>. For more information, see “Cisco Connection Online.”
3. In the Path column, refer to the CCO path for a listing of the available publications.



Using VeriSign Digital Certificates: A Business Case

This chapter describes how Cisco Secure VPN Client interoperates with a Cisco router using VeriSign digital certificates. Using IPSec, digital certificates allow devices to be automatically authenticated to each other without the manual key exchanges required by Cisco Encryption Technology.

- Benefits of Using VeriSign Digital Certificates
- Configuring, Verifying, and Troubleshooting
- Related Documentation

Benefits of Using VeriSign Digital Certificates

For the benefits of using digital certificates, refer to the “Benefits of Using Digital Certificates” section in Chapter 3, “Using Digital Certificates: Business Case Introduction.”

Configuring, Verifying, and Troubleshooting

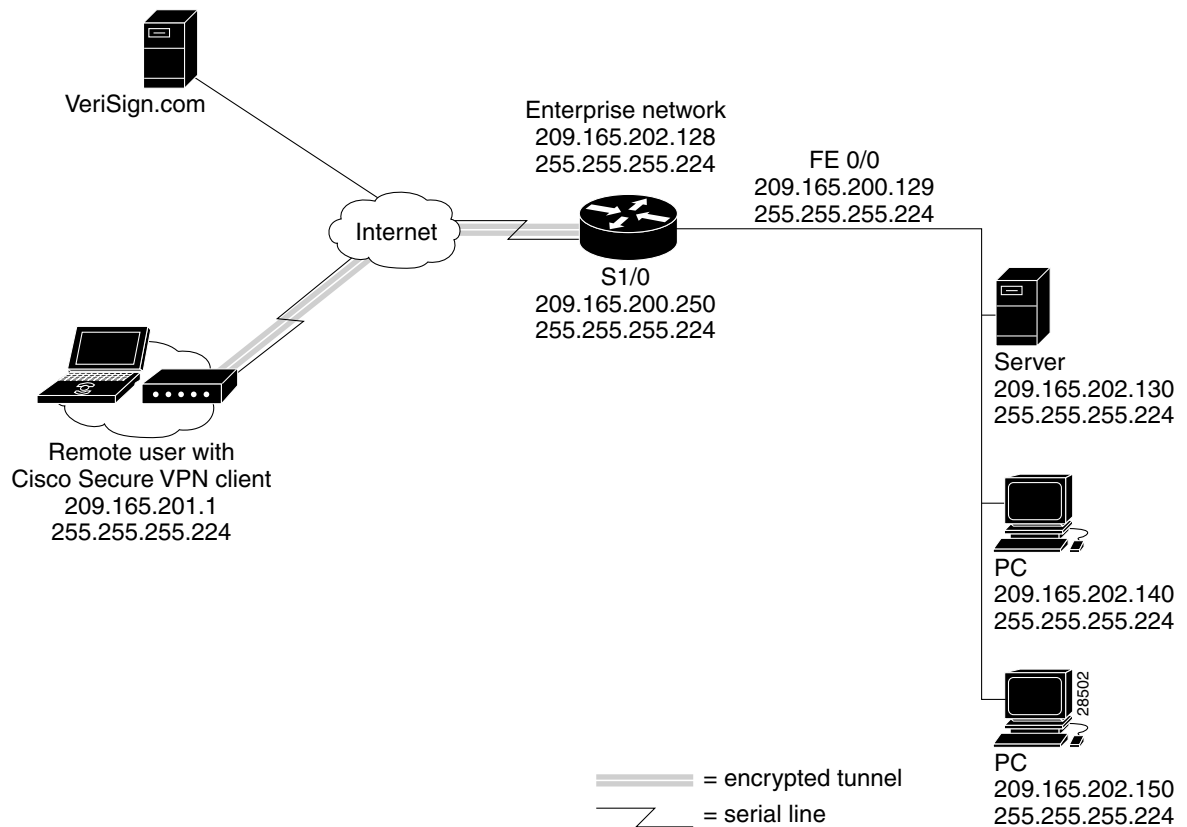
- Configuring VeriSign Digital Certifications
- Verifying VeriSign Digital Certifications

Configuring VeriSign Digital Certifications

Configuring VeriSign digital certificates for a secure IPSec tunnel between a remote client and a Cisco router involves the following tasks:

- Configuring the Cisco Secure VPN Client
- Configuring the Cisco Router

Figure 5-1 Physical Elements—VeriSign Configuration Topology



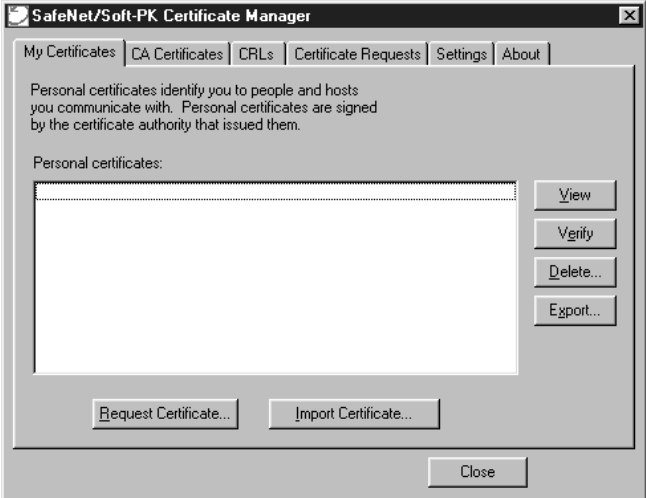
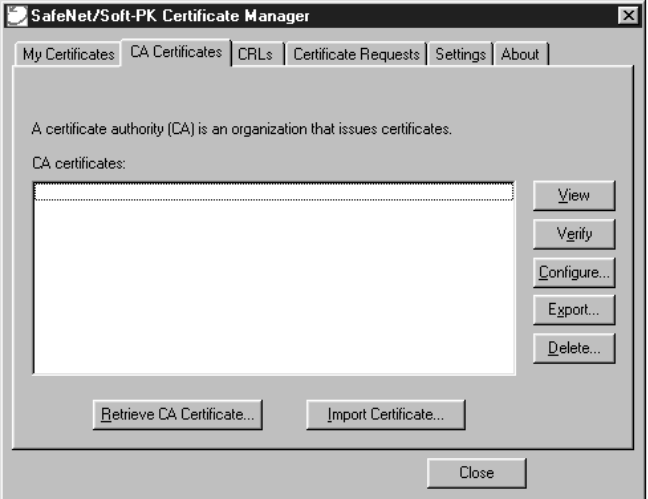
Configuring the Cisco Secure VPN Client

Configuring the Cisco Secure VPN Client requires the following tasks:

- Task 1—Importing the Root CA Certificate
- Task 2—Creating Public and Private Key Pair
- Task 3—Requesting Client Certificate from VeriSign CA Server
- Task 4—Submitting the Certification Request to the VeriSign CA Server
- Task 5—Importing Your Signed VeriSign Digital Certificate
- Task 6—Configuring Other Connections for Security Policy
- Task 7—Configuring A New Connection for Security Policy
- Task 8—Specifying Identity Using RSA Signature
- Task 9—Specifying Encryption and Authentication Methods for Authentication, Phase 1
- Task 10—Specifying Encryption and Authentication Methods for Key Exchange, Phase 2
- Task 11—Saving Your Configuration

Task 1—Importing the Root CA Certificate

Task 1—Importing the Root CA Certificate

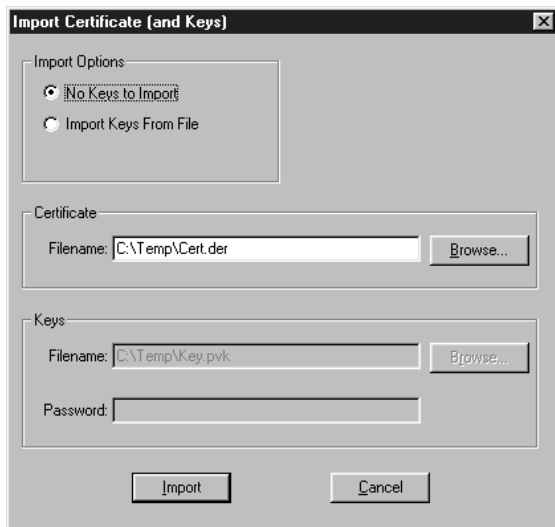
Command	Purpose
Step 1 Click Start>Programs>SafeNet/Soft-PK>Certificate Manager . The SafeNet/Soft-PK Certificate Manager dialog box appears.	Open the Certificate Manager . The Certificate Manager allows you to request, import, and store the digital certificates that you receive from the certification authority (CA).
	Step 2 a. Click the CA Certificates tab. b. Click Import Certificate . Go to the CA Certificates folder to retrieve, import, view, verify, configure, export, or delete the certificates you receive from the CA.
	

Task 1—Importing the Root CA Certificate

Command

Purpose

- Step 3** The Import Certificate (and Keys) dialog box appears.
- In the Import Certificate (and Keys) dialog box, enter the following information:
 - Under Import Options, select the **No Keys to Import** option.
 - Obtain the root CA file from the system administrator, who should also supply you with the URL for IPSec CSR enrollment. The system administrator gets the root CA file and URL from the CA Administrator.
 - Rename the root CA file with a “.cer” filename extension.
 - Under Certificate, click **Browse**.

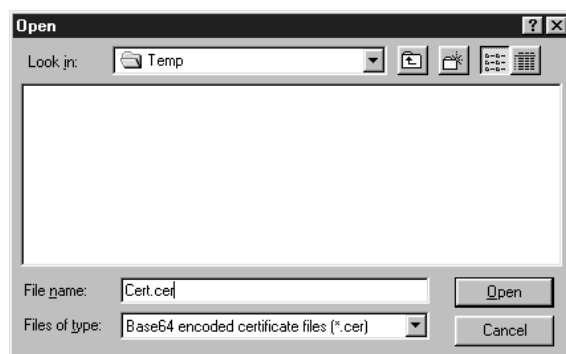


27353

- Import your root CA file certificate.
- There are three reasons to import a certificate rather than retrieving it:
- You decide not to request a personal certificate online, and you need to reimport the certificate file your CA returned to you.
 - You want to import a CA certificate that was downloaded directly from the CA's web site.
 - In the following events:
 - Your computer crashes.
 - Your files are corrupted.
 - You need to copy your certificate from one computer to another.
 - You are upgrading client software.

You would need the certificate file you or your network administrator exported from **My Certificates** or **CA Certificates** as a backup.

- Step 4** The Open dialog box appears.
- In the **Files of Type** list, click **Base64 encoded certificate files**.
 - Locate the root CA file (the “.cer” file).
 - Click **Open**.



27355


Open the root CA file for importing to the CA Certificates folder.

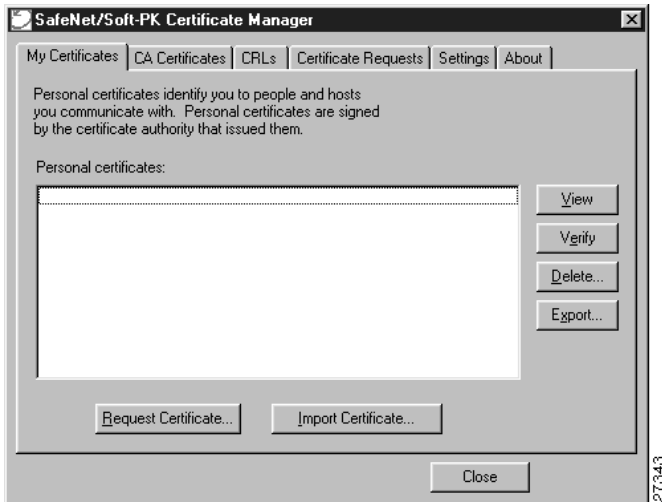
Task 1—Importing the Root CA Certificate

	Command	Purpose
Step 5	<p>The Import Certificate (and Keys) dialog box appears.</p> <ol style="list-style-type: none"> Click Import. Add the certificate to the Root Store. 	Add the CA root file to your list of CA Certificates.

Task 2—Creating Public and Private Key Pair

Task 2—Creating Public and Private Key Pair

	Command	Purpose
Step 1	<ol style="list-style-type: none"> In the Certificate Manager dialog box, click the My Certificates tab. Click Request Certificate. 	<p>Use the My Certificates folder to retrieve, import, view, verify, configure, export, or delete the certificates your personal certificate.</p> <p> Note You must have your root CA certificate before requesting a personal certificate. Otherwise, only a file-based request is possible.</p>



Task 2—Creating Public and Private Key Pair**Command****Purpose****Step 2**

The Online Certificate Request dialog box appears.

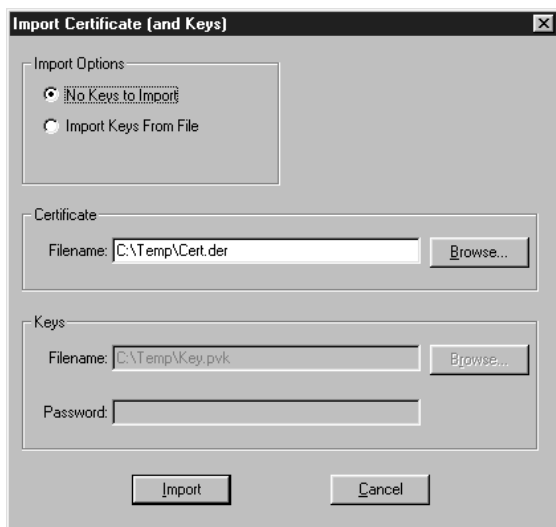
- a. In the Online Certificate Request dialog box, fill in the following section:
 - Under Subject Information, fill in the following fields:
 - In the **Name** field, enter the name of the certificate owner.
 - In the **Department** field, enter the department for which this certificate will be configured.
 - In the **Company** field, enter the company for which this certificate will be configured.
 - In the **State** field, enter the state in which this certificate request was created.
 - In the **Country** field, enter the country in which this certificate was created.
 - In the **Email** field, enter the email account of the person associated with this certificate request.
 - In the **Domain Name** field, enter the name of the domain for your business.
 - In the **IP Address** field, do not enter anything.
 - Under Request File, perform the following tasks:
 - In the **Filename** field, enter the filename of the certificate request or click **Browse** to locate the certificate request on your hard drive.
- b. Click **OK**. The client will generate public/private key pairs.

You can configure a certificate request for online or file-based enrollment.

- To configure an online enrollment, you must click the **CA Certificate** tab in the Certificate Manager dialog box, and retrieve a CA certificate.


**Note**

This information binds your identity to a public key that others will look for in a public key directory. Entering inaccurate or misleading information defeats the purpose of using public key.



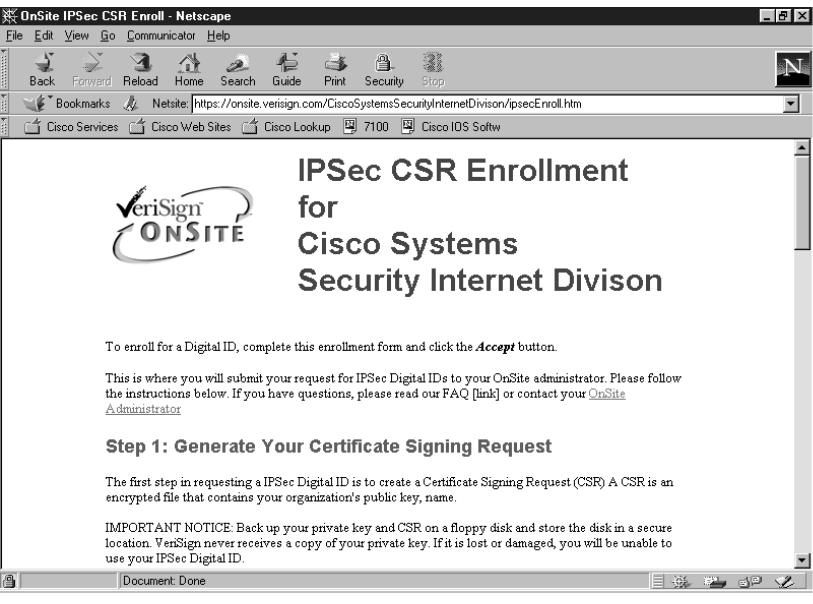
Task 3—Requesting Client Certificate from VeriSign CA Server

Task 3—Requesting Client Certificate from VeriSign CA Server

Command	Purpose
<ol style="list-style-type: none"> In the Certificate Manager dialog box, click the My Certificates tab. Click Request Certificate. 	Request your personal certificate.
	

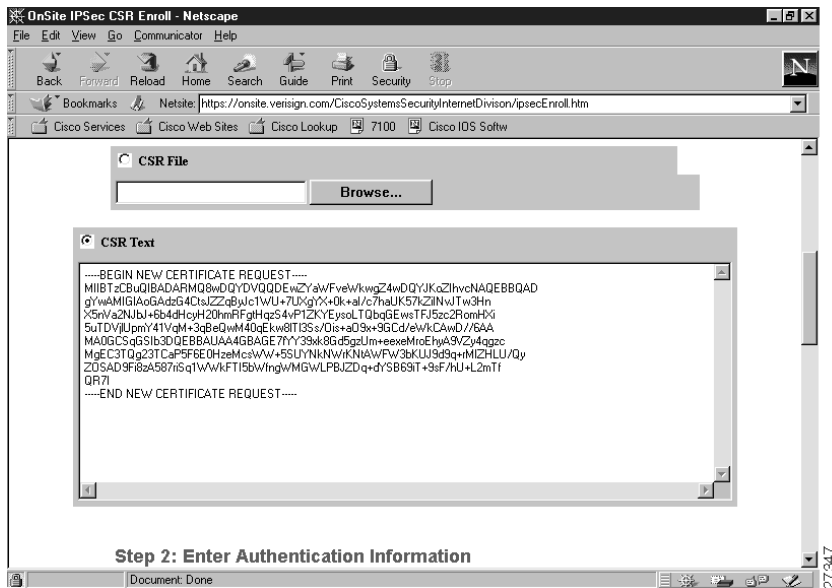
Task 4—Submitting the Certification Request to the VeriSign CA Server

Task 4—Submitting the Certification Request to the VeriSign CA Server

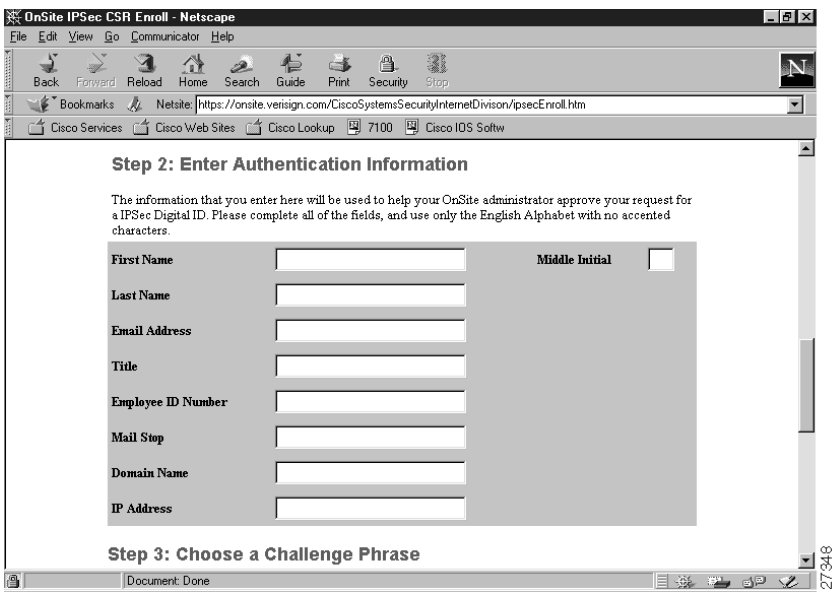
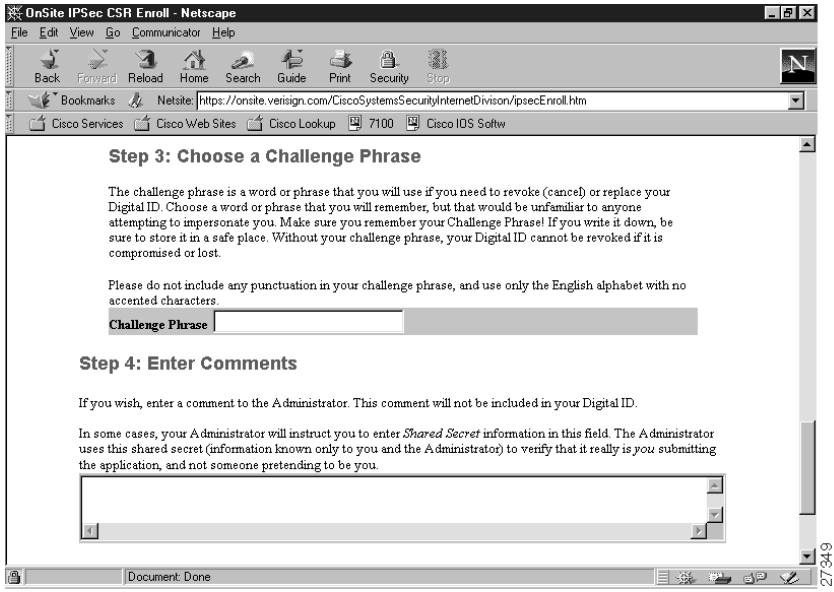
Command	Purpose
<p>Step 1</p> <ol style="list-style-type: none"> Open your browser. Navigate to the URL for IPsec CSR Enrollment using the URL provided by your CA Administrator. For example: http://onsite.Verisign.com/ This web page consists of five steps to securing a CSR: <ul style="list-style-type: none"> Generate Your Certificate Signing Request Enter Authentication Information Choose a Challenge Phrase Enter Comments Submit Request 	<p>Request for your certificate to be signed by the CA Administrator.</p>
	

Task 4—Submitting the Certification Request to the VeriSign CA Server

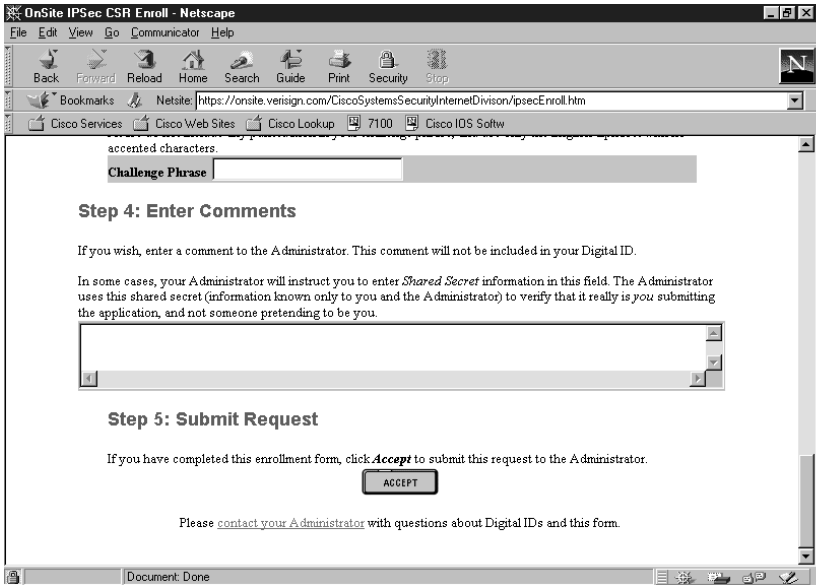
Command	Purpose
Step 2 Click the CSR Text option. Generate and submit your Certificate Signing Request (CSR).	<p>The Certificate Signing Request (CSR) contains your server's public key along with other information such as your server's Distinguished Name (DN). You generate the CSR through your web server software and submit it to VeriSign in the online request form. When your request is approved, the data in the request is packaged into a certificate and signed by the VeriSign CA.</p> <p>When you create a CSR a cryptographic key pair is generated. The public key is inserted into the CSR and subsequently signed by the VeriSign CA. The private key remains on your computer. Be sure to securely back up the private key. If the private key is lost or becomes corrupt you will not be able to use your certificate.</p> <hr/> <p>Note The private key is a very sensitive piece of information. Those with access to your private key could decrypt the SSL-protected data sent and received by your web server. Please take appropriate steps to ensure there is no unauthorized access to the private key.</p>



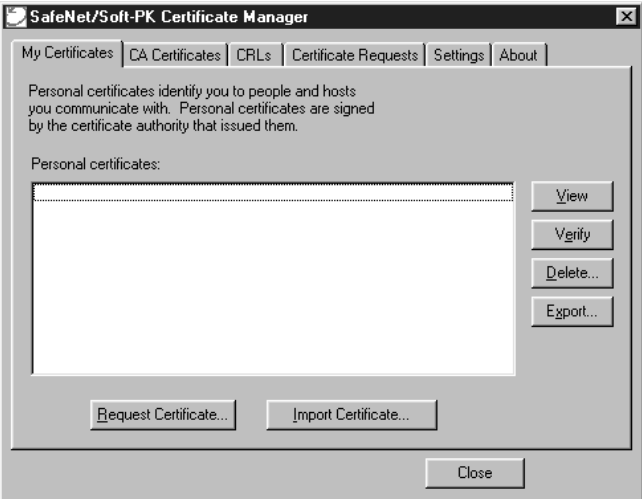
Task 4—Submitting the Certification Request to the VeriSign CA Server

Command	Purpose
<p>Step 3 Enter at minimum your First Name, Last Name, and Email Address.</p> 	<p>Enter the authentication information. This information will allow the CA administrator to identify you.</p>
<p>Step 4 Choose a Challenge Phrase, and enter it in the empty field.</p> 	<p>A Challenge Phrase should be unique and will be used to identify you in the event you lose or misplace your digital certificate.</p>

Task 4—Submitting the Certification Request to the VeriSign CA Server

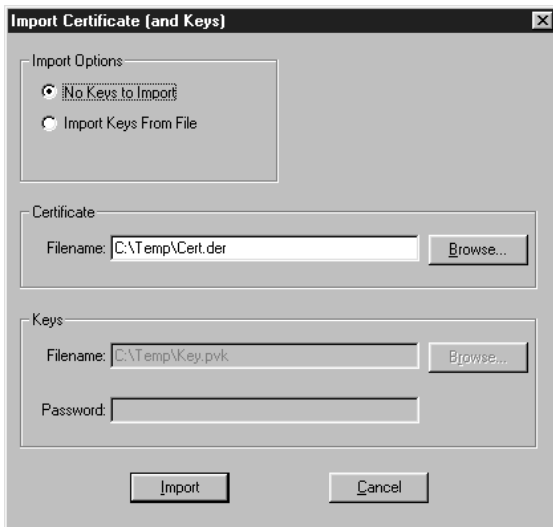
Command	Purpose
<p>Step 5 Enter any comments you may have for the CA administrator.</p> 	<p>Enter any comments for the CA administrator.</p>
<p>Step 6</p> <ol style="list-style-type: none"> Click Accept to submit the request to the CA administrator. Call the CA administrator to inform her or him about your pending request. After your CA administrator approves the request, you should receive your certificate through email. 	<p>Submit your request for a digital certificate to the CA.</p>

Task 5—Importing Your Signed VeriSign Digital Certificate

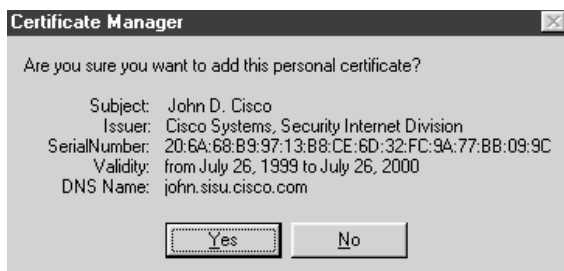
Task 5—Importing Your Signed VeriSign Digital Certificate		
	Command	Purpose
Step 1	<div>a. Click Start>Programs>SafeNet/Soft-PK>Certificate Manager.</div> <div>b. Then, click the My Certificates tab.</div> <div>c. Click Import Certificate.</div>	The CA administrator should have sent a digital certificate through email. This process will import your signed digital certificate.
	<div></div>	

Task 5—Importing Your Signed VeriSign Digital Certificate

Command	Purpose
<p>Step 2 The Import Certificate (and Keys) dialog box appears.</p> <ol style="list-style-type: none"> In the Import Certificate (and Keys) dialog box, perform the following tasks: <ul style="list-style-type: none"> Under Import Options, click the No Keys to Import option. Under Certificate, click Browse. In the Files of Type list, click Base64 encoded certificate files. Add your signed digital certificate. Rename the file with a “.cer” filename extension. Under Keys, click Browse. Select your signed digital certificate. Click Import. 	<p>Import your signed digital certificate.</p> <p>There are three reasons to import a digital certificate rather than retrieving it:</p> <ul style="list-style-type: none"> You decide not to request a personal certificate online, and you need to reimport the certificate file your CA returned to you. You want to import a CA certificate that was downloaded directly from the CA's web site. In the following events: <ul style="list-style-type: none"> Your computer crashes. Your files are corrupted. You need to copy your certificate from one computer to another. You are upgrading client software. You would need the certificate file you or your network administrator exported from My Certificates or CA Certificates as a backup.
<p>Step 3 The Certificate Manager confirmation dialog box appears. Click Yes to confirm.</p>	<p>Your signed digital certificate will be imported once you confirm it is the correct one to add.</p>

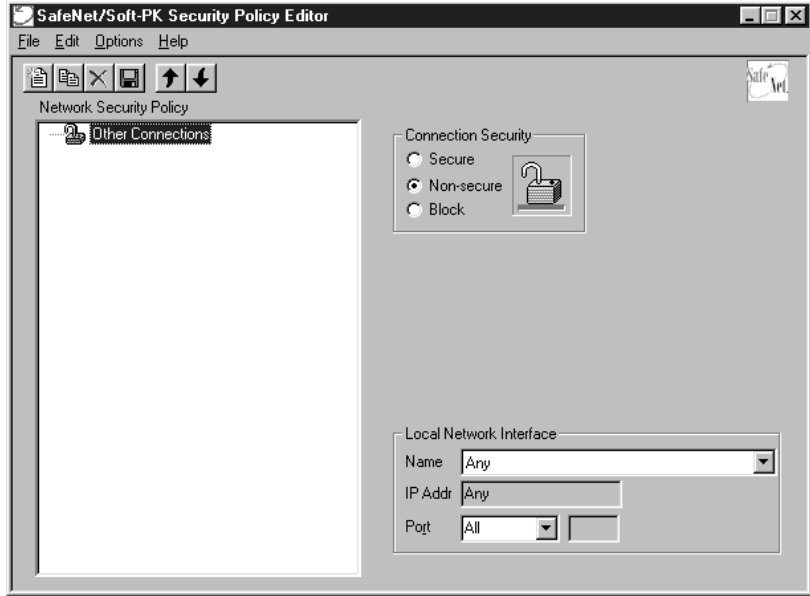


27363



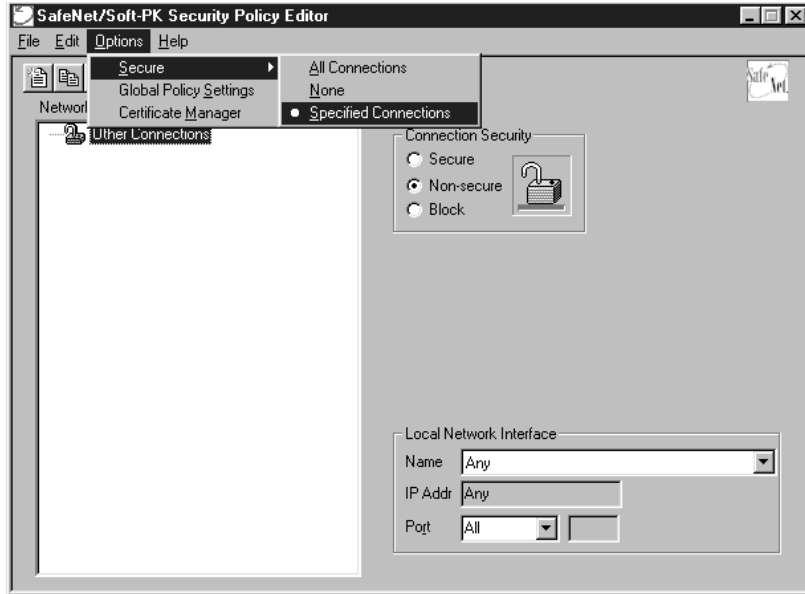
29019

Task 6—Configuring Other Connections for Security Policy

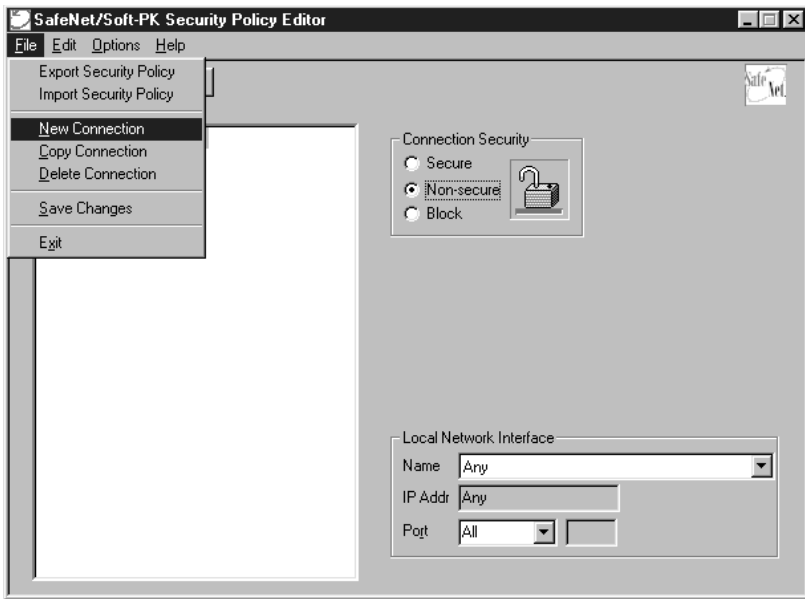
Task 6—Configuring Other Connections for Security Policy		
Command		Purpose
Step 1	<p>Click Start>Programs>SafeNet/Soft-PK>Security Policy Editor. The SafeNet/Soft-PK Security Policy Editor dialog box appears.</p> 	<p>Use the Security Policy Editor to do the following:</p> <ul style="list-style-type: none">• Establish connections and their associated proposals.• List connections in a hierarchical order that defines an IP data communications security policy.

Task 6—Configuring Other Connections for Security Policy

Command	Purpose
Step 2 On the Options menu, click Secure>Specified Connections .	<p>Establish policies for individual connections using two main steps:</p> <ol style="list-style-type: none"> 1. Configuring “Other Connections” 2. Adding and configuring new connections <p>A new connection is a set of security parameters that pertain to an individual remote IP connection.</p> <p>You can create any number of new connections and name them. The system tests for a match between an incoming transmission and the proposed policies you have established, in the order in which they are listed in the SafeNet/Soft-PK Security Policy Editor dialog box. If you find that you need to reorder the sequence of policies, you can do so by moving them up or down within the Network Security Policy list.</p> <p>Remember that “Other Connections” is always the last rule in your list of security policies.</p>
Step 3 <ol style="list-style-type: none"> a. In the left pane, select Other Connections. b. In the right pane, under Connection Security, click the Non-Secure option. 	<p>Configure the default connection called Other Connections as the first step in establishing security policies for individual connections. For all IP communications that do not adhere to the security policies defined in the individual connections, Other Connections acts as a default.</p> <p>Click the Non-Secure option to allow IP communications for this connection to pass through unsecured. This will allow you to change the settings under your Local Network Interface.</p>

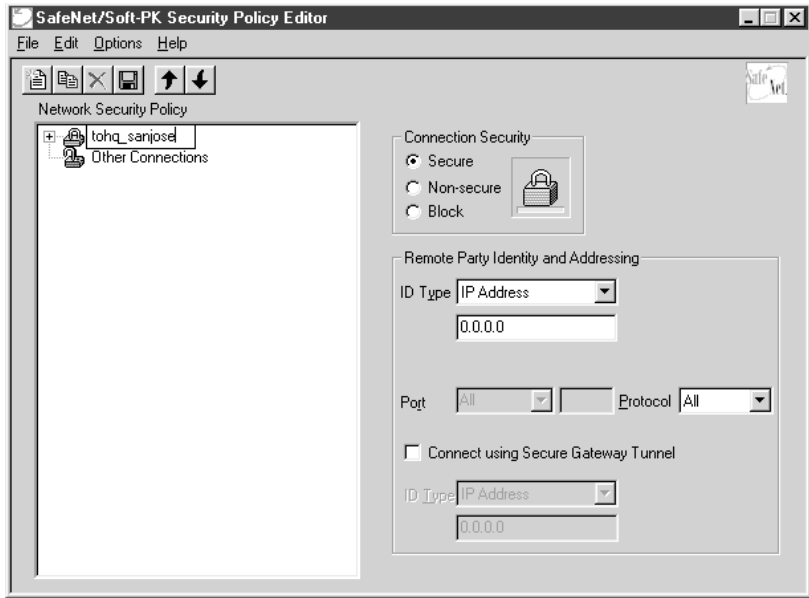


27363



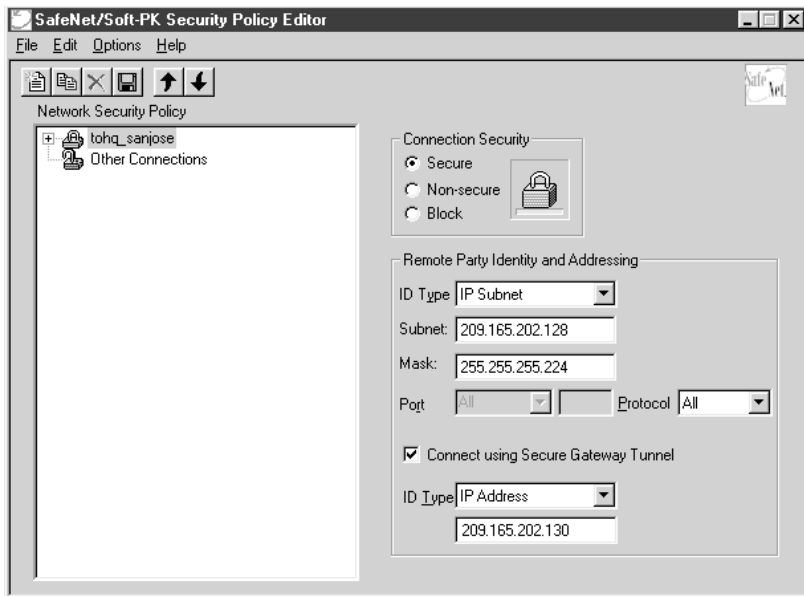
27364

Task 7—Configuring A New Connection for Security Policy

Task 7—Configuring A New Connection for Security Policy		
	Command	Purpose
Step 1	<ol style="list-style-type: none"> In the left pane, select the name of a connection (for instance, Other Connections). On the File menu, click New Connection. In the left pane, the default New Connection placeholder will appear. In its place, create a unique name for the connection to your router. For example, if your router name is <code>hq_sanjose</code>, you might rename the connection <code>tohq_sanjose</code>. 	<p>Create a new connection by contacting the other party for information, including the destination:</p> <ul style="list-style-type: none"> IP address Network IP address IPSec-compliant gateway device's IP address, if any Domain name Email address IP subnet IP address range Subject's identity information <ul style="list-style-type: none"> Name Department Company State Country
		

Task 7—Configuring A New Connection for Security Policy

Command	Purpose
<p>Step 2</p> <p>a. In the left pane, click tohq_sanjose.</p> <p>b. In the right pane, configure the following parameters for tohq_sanjose:</p> <ul style="list-style-type: none"> Under Connection Security, click the Secure option. Under Remote Party Identity and Addressing, select the following items: <ul style="list-style-type: none"> In the ID Type list, click IP Subnet. In the Subnet list, click 209.165.202.128 In the Mask list, click 255.255.255.224. All traffic (all protocols) destined for 209.165.202.128 will be encrypted and secure. The Port list and entry field are inactive as a default. In the Protocol list, click All. Select the Connect using Secure Gateway Tunnel check box. In the ID_Type list, click IP Address. In the ID_Type box, enter the IP address, 209.165.202.130. 	<p>Fill in the fields according to the information you received from the other party.</p> <ul style="list-style-type: none"> Secure option—Secures the IP communications for this connection. ID Type list—Lists type of identification of the other party. Subnet list—Enter the other party's subnet. Mask list—Enter the other party's subnet mask. Port list—A default of “All” secures all protocol ports. Connect using Secure Gateway Tunnel check box—Specify that the other party is protected by a secure IPSec-compliant gateway, such as a firewall, by selecting this check box. ID_Type list—Lists identification type of the gateway. ID_Type box—Enter the IP address of the gateway.

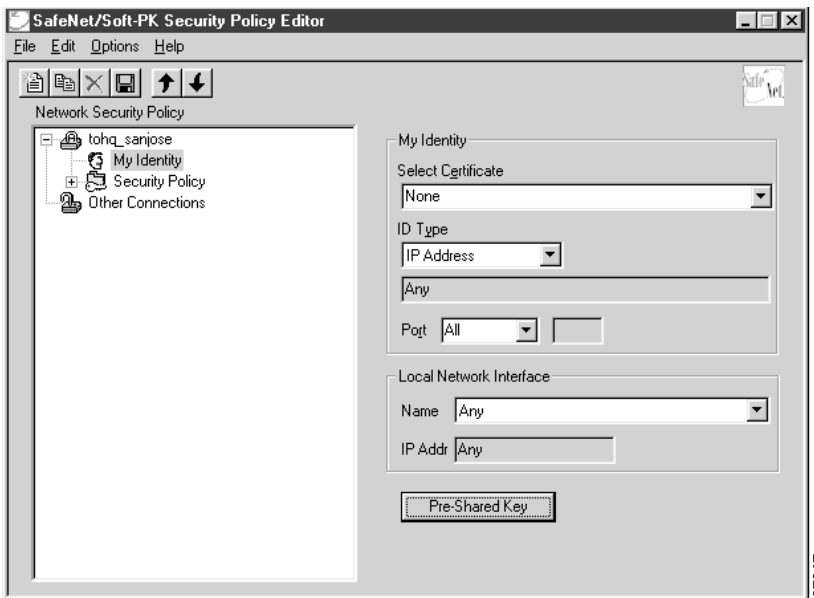


27366

Task 8—Specifying Identity Using RSA Signature

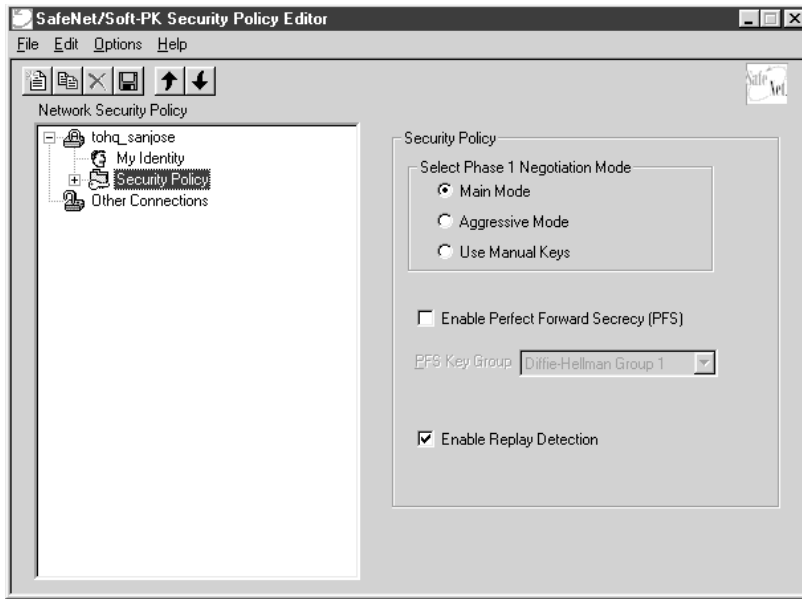
Task 8—Specifying Identity Using RSA Signature

Command	Purpose
<p>Step 1</p> <ol style="list-style-type: none"> In the left pane, double-click tohq_sanjose. tohq_sanjose expands with My Identity and Security Policy. Click My Identity. The My Identity window appears. In the right pane, set the following parameters: <ul style="list-style-type: none"> Under My Identity, select the following items: <ul style="list-style-type: none"> In the Select Certificate list, click <i>your signed certificate</i>. In the ID_Type list, click IP Address. In the Port list, click All. Under Local Network Interface, select the following items: <ul style="list-style-type: none"> In the Name list, click Any. The IP Addr list is inactive as a default. 	<p>Select an identification that will allow the other party to identify you during the key exchange phase.</p> <ul style="list-style-type: none"> Select Certificate—Select your digital certificate. ID_Type—Select IP address. Port—A default of “All” secures all protocol ports.



Task 8—Specifying Identity Using RSA Signature

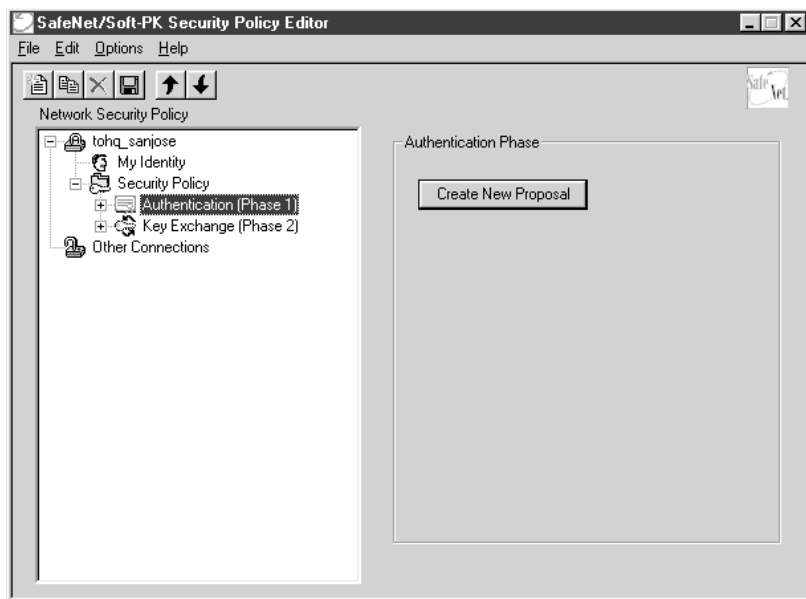
Command	Purpose
<p>Step 2</p> <ol style="list-style-type: none"> In the left pane, under My Identity, double-click Security Policy. In the right pane, under Security Policy, specify the following items: <ul style="list-style-type: none"> Select Main Mode option. Select the Enable Replay Detection check box. 	<p>Select the Main Mode and Enable Replay Detection check boxes to set authentication requirements for your security policy.</p> <ul style="list-style-type: none"> Main Mode—Authentication method that protects identities by not revealing them until secure communications have been established. Enable Replay Detection—When selected, this counter determines whether or not a packet is unique. This prevents falsification of data.



Task 9—Specifying Encryption and Authentication Methods for Authentication, Phase 1

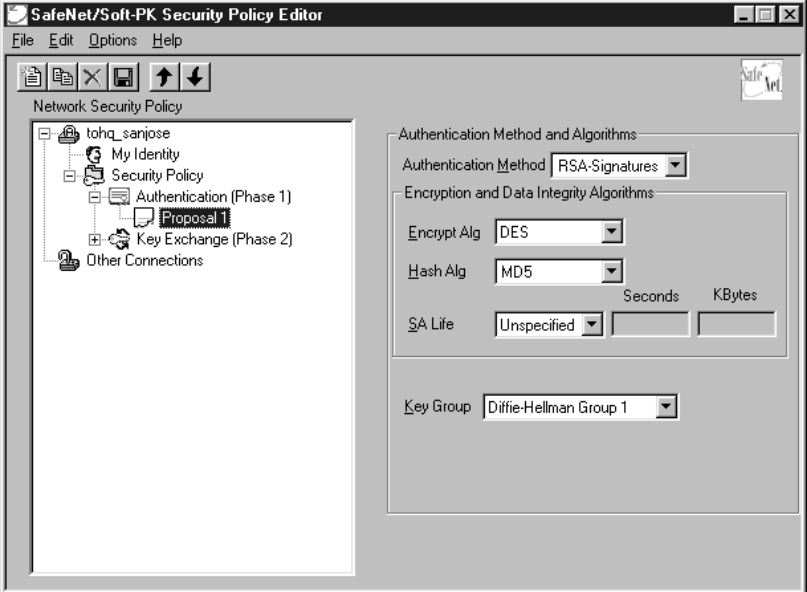
Task 9—Specifying Encryption and Authentication Methods for Authentication, Phase 1

Command	Purpose
<p>Step 1</p> <ol style="list-style-type: none"> In the left pane, double-click Security Policy, then click Authentication (Phase 1). In the right pane, under Authentication Phase, perform the following task: <ul style="list-style-type: none"> Click Create New Proposal. 	<p>During Authentication (Phase 1), you and the trusted party will reveal your identities and negotiate how they will secure phase 2 communications.</p> <p>Before securing communications, the two parties involved negotiate the method they will use. Each method is called a “proposal.” Proposals are presented to the other party in the order in which they are sequenced in the Network Security Policy list. You can reorder the proposals after you create them.</p>

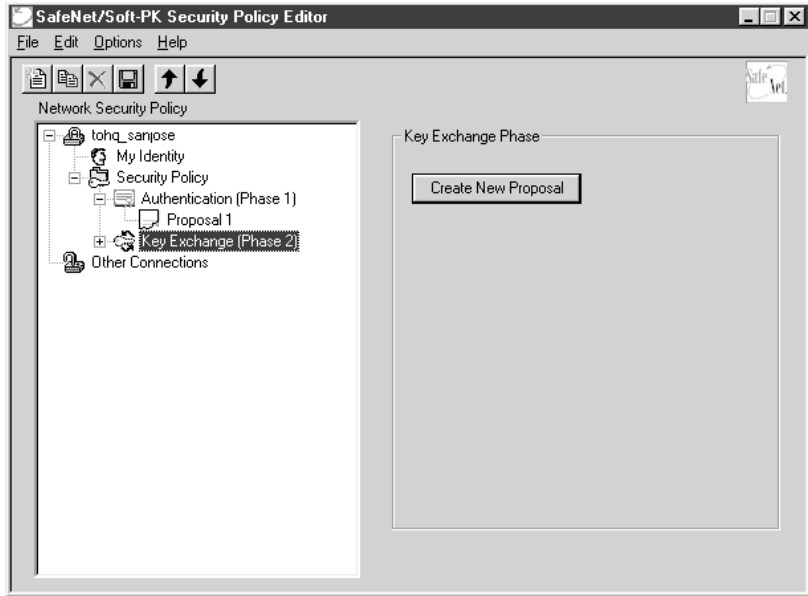


27370

Task 9—Specifying Encryption and Authentication Methods for Authentication, Phase 1

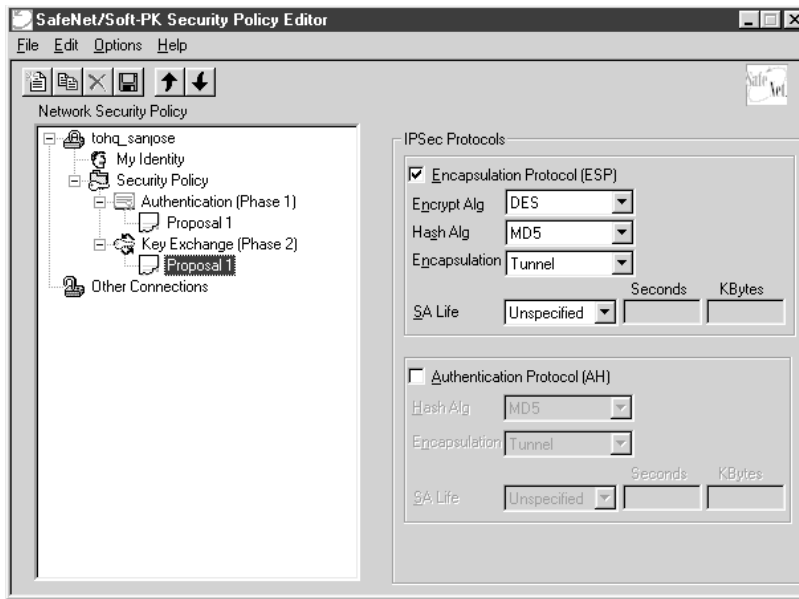
Command	Purpose
<p>Step 2</p> <ol style="list-style-type: none"> In the left pane, under Authentication (Phase 1), a new Proposal appears called Proposal 1. In the right pane, under Authentication Method and Algorithms, perform the following tasks: <ul style="list-style-type: none"> In the Authentication Method list, click RSA-Signatures. Under Encryption and Data Integrity Algorithms, perform the following tasks: <ul style="list-style-type: none"> In the Encrypt Alg list, click DES. In the Hash Alg list, click MD5. In the SA Life list, click Unspecified. In the Key Group list, click Diffie-Hellman Group 1. 	<p>Define the authentication method for the proposal.</p> <ul style="list-style-type: none"> Authentication Method—Indicates the method of authentication. Encrypt Alg—Select DES for minimal security, Triple-DES for highest security, or Null for none at all. Depending on the IPSec image on your Cisco router, you will enter either DES or Triple-DES. Hash Alg—Select MD5 for minimal security, SHA-1 for highest security, or DES-MAC.
	<p>Note DES-MAC is currently not supported with Cisco IOS software.</p> <ul style="list-style-type: none"> SA Life—Optionally, specify the period for which the key is valid. Key Group—Allows you to select with Diffie-Hellman Group to use.

Task 10—Specifying Encryption and Authentication Methods for Key Exchange, Phase 2

Task 10—Specifying Encryption and Authentication Methods for Key Exchange, Phase 2		
Command		Purpose
<p>a. In the left pane, under Authentication (Phase 1), select Key Exchange (Phase 2).</p> <p>b. In the right pane, under Key Exchange Phase section, click Create New Proposal.</p>		<p>Negotiate which key exchange method of securing communications you and the other party will use by establishing a proposal.</p>
		

Task 10—Specifying Encryption and Authentication Methods for Key Exchange, Phase 2

Command	Purpose
<p>Step 2</p> <ol style="list-style-type: none"> In the left pane, under Key Exchange (Phase 2), a new proposal appears called Proposal 1. In the right pane, under IPsec Protocols, perform the following tasks: <ul style="list-style-type: none"> Select the Encapsulation Protocol check box. In the Encryption Alg list, click DES. In the Hash Alg list, click MD5. In the Encapsulation list, click Tunnel. 	<p>Define the key exchange method for the proposal.</p> <ul style="list-style-type: none"> Encapsulation Protocol—Indicates the method of authentication. Encryption Alg—Select DES for minimal security, Triple-DES for highest security, or Null for none at all. Depending on the IPsec image on your Cisco router, you will enter either DES or Triple-DES. Hash Alg—Select MD5 for minimal security, SHA-1 for highest security, or DES-MAC. <p>Note DES-MAC is currently not supported with Cisco IOS software.</p> <ul style="list-style-type: none"> Encapsulation—Tunnel is the only method of encapsulation available for the Cisco Secure VPN Client. <p>Note Transport mode can be used only if the two end devices are both providing IPsec protection. Otherwise, you must use tunnel mode.</p>

**Task 11—Saving Your Configuration****Task 11—Saving Your Configuration**

Command	Purpose
<ol style="list-style-type: none"> On the File menu, click Save Changes to save the policies. When the Security Policy Editor dialog box appears, click OK. 	Save your policies for implementation.



Configuring the Cisco Router

Configuring the Cisco router requires the following tasks:

- Task 1—Configuring the Domain Name, Host Name, and Name Server
- Task 2—Configuring ISAKMP Policy and Defining IPSec Transform Sets
- Task 3—Defining Crypto Dynamic Map and IKE Crypto Map to the Client
- Task 4—Defining the CA, Enrolling Your Certificate, and Requesting Certificate Signature
- Task 5—Applying Crypto Map to the Interface

Task 1—Configuring the Domain Name, Host Name, and Name Server

Task 1—Configuring the Domain Name, Host Name, and Name Server		
	Command	Purpose
Step 1	router> enable	Enter privileged EXEC mode.
Step 2	router# configure terminal Enter configuration commands, one per line. End with CNTL/Z.	Enter global configuration mode.
Step 3	router(config)# ip domain-name sisu.cisco.com	Define the domain name. Enter your domain name.
Step 4	router(config)# hostname hq_sanjose hq_sanjose(config)#	Define the host name. Enter your host name
Step 5	hq_sanjose(config)# ip name-server 209.165.202.130	Define the name server. Enter the gateway IP address.

Task 2—Configuring ISAKMP Policy and Defining IPSec Transform Sets

Task 2—Configuring ISAKMP Policy and Defining IPSec Transform Sets		
	Command	Purpose
Step 1	hq_sanjose(config)# crypto isakmp policy 3 hq_sanjose(config-isakmp)# encryption des hq_sanjose(config-isakmp)# hash MD5 hq_sanjose(config-isakmp)# authentication rsa-sig hq_sanjose(config-isakmp)# exit	To define an IKE policy, use the crypto isakmp policy global configuration command. This command invokes the ISAKMP policy configuration (config-isakmp) command mode. IKE policies define a set of parameters to be used during the IKE negotiation.

Task 2—Configuring ISAKMP Policy and Defining IPsec Transform Sets

	Command	Purpose
Step 2	<pre>hq_sanjose(config)# crypto ipsec transform-set ciscots esp-des esp-md5-hmac hq_sanjose(cfg-crypto-trans)# exit</pre>	<p>To define a transform set—an acceptable combination of security protocols and algorithms—use the crypto ipsec transform-set global configuration command. This command invokes the crypto transform configuration mode (cfg-crypto-trans).</p> <ul style="list-style-type: none"> • ciscots—Enter a unique name for this transform set. In this example, ciscots is used. • esp-des—ESP with the 56-bit DES encryption algorithm. • esp-md5-hmac—ESP with the MD5 (HMAC variant) authentication algorithm.

Task 3—Defining Crypto Dynamic Map and IKE Crypto Map to the Client**Task 3—Defining Crypto Dynamic Map and IKE Crypto Map to the Client**


	Command	Purpose
Step 1	<pre>hq_sanjose(config)# crypto dynamic-map ciscodm 4 hq_sanjose(cfg-crypto-dyn)# set transform-set ciscots hq_sanjose(cfg-crypto-dyn)# exit</pre>	<p>Associate the transform-set with a dynamic map. To create a dynamic crypto map entry, use the crypto dynamic-map global configuration command. Using this command puts you into dynamic crypto map configuration mode (cfg-crypto-dyn).</p> <ul style="list-style-type: none"> • ciscodm—Enter a unique name for this dynamic crypto map. In this example, ciscodm is used. • 4—Enter a number for this dynamic crypto map entry. <p>Apply the transform set to the crypto dynamic map. To specify which transform sets can be used with the crypto map entry, use the set transform-set crypto map configuration command.</p>
Step 2	<pre>hq_sanjose(config)# crypto map toclient 2 ipsec-isakmp dynamic ciscodm hq_sanjose(config-crypto-map)# exit</pre>	<p>Create a crypto map using IKE referencing the preexisting dynamic crypto map. To create or modify a crypto map entry and enter the crypto map configuration mode, use the crypto map global configuration command.</p> <ul style="list-style-type: none"> • toclient—Enter a unique name for this crypto map. In this example, toclient is used. • 2—Enter a number for this crypto map entry. • ipsec-isakmp—Indicates IKE will be used.

Task 4—Defining the CA, Enrolling Your Certificate, and Requesting Certificate Signature

Task 4—Defining the CA, Enrolling Your Certificate, and Requesting Certificate Signature

	Command	Purpose
Step 1	<pre>hq_sanjose(config)# crypto ca identity sisu.cisco.com hq_sanjose(cfg-ca-id)# enrollment url http://onsiteipsec.Verisign.com hq_sanjose(cfg-ca-id)# enrollment retry count 100 hq_sanjose(cfg-ca-id)# enrollment retry period 2 hq_sanjose(cfg-ca-id)# crl optional hq_sanjose(cfg-ca-id)# exit</pre>	<p>Define VeriSign related enrollment commands. To declare the CA your router should use, use the crypto ca identity global configuration command. Using this command puts you into the ca-identity configuration mode, where you can specify characteristics for the CA.</p>
Step 2	<pre>hq_sanjose(config)# crypto key generate rsa The name for the keys will be: hq_sanjose.sisu.cisco.com Choose a 512 bit or smaller key modulus for your General Purpose Keys. How many bits in the modulus [512]: Generating RSA keys [OK]</pre>	<p>Generate the public and the private keys. The crypto key generate rsa-usage command creates two key-pairs for RSA:</p> <ul style="list-style-type: none"> • One key-pair for encryption • One key-pair for digital signatures <p>A key-pair refers to a public key and its corresponding secret key. If you do not specify “usage-keys” at the end of the command, the router will generate only one RSA key-pair and use it for both encryption and digital signatures.</p>
Step 3	<pre>hq_sanjose(config)# crypto ca authenticate sisu.cisco.com Certificate has the following attributes: Fingerprint: 103FXXXX 9D64XXXX 0AE7XXXX 626AXXXX % Do you accept this certificate? [yes/no]:yes</pre>	<p>Get the public key and CA Server certificate. To authenticate the CA (by getting the CA's certificate), use the crypto ca authenticate global configuration command.</p> <p>At this point the router has a copy of the CA's certificate.</p> <p>Enter yes to accept the certificate.</p>
Step 4	<pre>hq_sanjose(config)# crypto ca enroll sisu.cisco.com</pre>	<p>Send router's public key and get a signed certificate from CA Server. To obtain your router's certificate(s) from the CA, use the crypto ca enroll global configuration command.</p>

Task 4—Defining the CA, Enrolling Your Certificate, and Requesting Certificate Signature

Command	Purpose
Step 5 Start certificate enrollment .. Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a proper note of it. Password: cisco1234 Re-enter password: cisco1234 % The subject name in the certificate will be: hq_sanjose.sisu.cisco.com % Include the router serial number in the subject name? [yes/no]: yes % The serial number in the certificate will be: 0431XXXX % Include an IP address in the subject name? [yes/no]: yes Interface: ethernet0 Request certificate from CA? [yes/no]: yes % Certificate request sent to Certificate Authority % The certificate request fingerprint will be displayed. % The 'show crypto ca certificate' command will also show the fingerprint. Fingerprint: C767XXXX 4721XXXX 0D1EXXXX C27EXXXX	 Note This is message text. Please read the message text, as might contain information about what to enter after it prompts you. At this point, the enrollment request is sent to the CA and is pending for the IPsec OnSite administrator's approval. The router will be polling every 2 minutes for the availability of the certificate. Wait until the router has retrieved the certificate. The router will display a message informing you that the certificate has been loaded.

Task 5—Applying Crypto Map to the Interface**Task 5—Applying Crypto Map to the Interface**

Command	Purpose
hq_sanjose(config)# interface ethernet0/0 hq_sanjose(config-if)# ip address ip address 209.165.202.130 255.255.255.224 hq_sanjose(config-if)# crypto map toclient hq_sanjose(config-if)# exit	Apply the crypto map to the interface.

Verifying VeriSign Digital Certifications

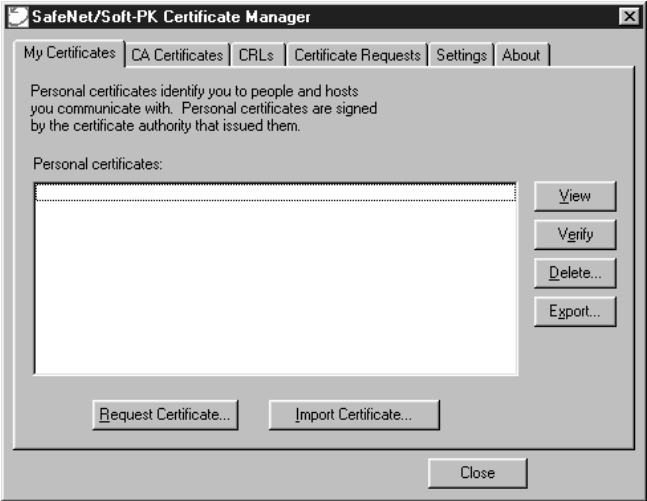
To verify that you have requested and your client has received your VeriSign digital certification properly, monitor the status of your digital certificates in the Certificate Manager and issue **show** commands on your router. Verifying your digital certification includes the following tasks:

- Task 1—Viewing and Verifying Using Certificate Manager
- Task 2—Issuing Show Commands on Cisco Router

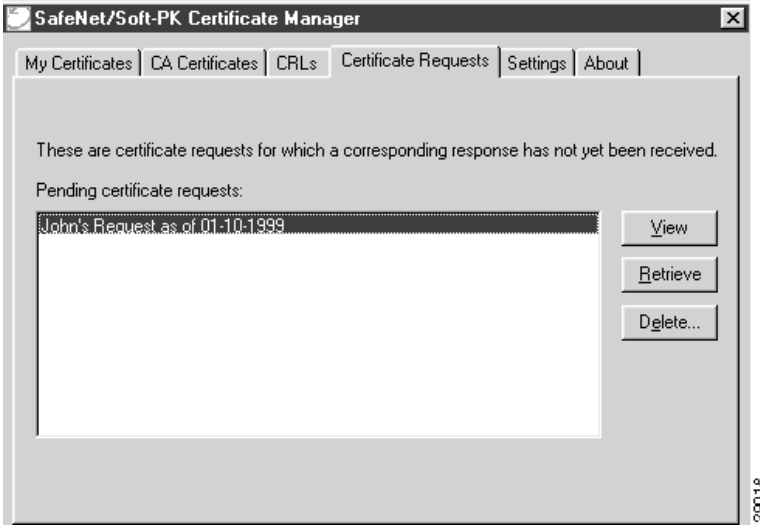
Task 1—Viewing and Verifying Using Certificate Manager

Task 1—Viewing and Verifying Using Certificate Manager

Command		Purpose
Step 1	In the Certificate Manager dialog box, click the My Certificates tab. Click View , then click Verify to confirm your digital certificate.	Your digital certification ID should appear under Personal Certificates. If your digital certificate does not appear here, go to the next step.



Task 1—Viewing and Verifying Using Certificate Manager

	Command	Purpose
Step 2	In the Certificate Manager dialog box, click the Certificate Requests tab. Check to see if you have sent in your request for the certificate.	Your certificate request should appear under Certificate Requests. If your certificate request does not appear here, go to the next step.
		
Step 3	Either you did not import the root CA file or you did not successfully import your personal digital certification from VeriSign. See “Configuring the Cisco Secure VPN Client.”	Without the root CA file, you cannot import a digital certificate.

Task 2—Issuing Show Commands on Cisco Router**Task 2—Issuing Show Commands on Cisco Router**

	Command	Purpose
Step 1	show crypto key mypubkey rsa	View your router's RSA public keys.
Step 2	show crypto key pubkey-chain rsa	View a list of all the RSA public keys stored on your router. These include the public keys of peers who have sent your router their certificates during peer authentication for IPSec.

Task 2—Issuing Show Commands on Cisco Router

	Command	Purpose
Step 3	show crypto key pubkey-chain rsa [name <i>key-name</i> address <i>key-address</i>]	View details of a particular RSA public key stored on your router.
Step 4	show crypto ca certificates	View information about your certificate, the CA's certificate, and any RA certificates.

Related Documentation

For more information on configuring the Cisco Secure VPN Client and digital certificates on a Cisco router, refer to Table 5-1.

Table 5-1 Related Documentation for Digital Certification

Document Title ¹	Customer Order Number	Path
Cisco Secure VPN Client Documentation		
Cisco Secure VPN Client <ul style="list-style-type: none"> Quick Start Guide Release Notes Solutions Guide 	<ul style="list-style-type: none"> DOC-786898 DOC-786929 OL-0259 	Hardware and Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Internet Service Unit Documentation>Cisco Secure VPN Client
Internetworking Solutions Guides Documentation		
<i>Access VPN Solutions Using Tunneling Technology</i>	<ul style="list-style-type: none"> OL-0293 	Hardware and Software Documentation: <ul style="list-style-type: none"> CCO²>Service & Support>Technical Documents>Documentation Home Page>Technology Information>Internetworking Solutions Guides>Access VPN Solutions Using Tunneling Technology
Cisco IOS Release 12.0 Documentation		
<i>Security Configuration Guide</i> <ul style="list-style-type: none"> “Configuring IPsec Network Security” “Configuring Certification Authority Interoperability” 	<ul style="list-style-type: none"> DOC-785843 See Path.³ See Path.³ 	Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>Configuration Guide and Command References>Security Configuration Guide
<i>Security Command Reference</i> <ul style="list-style-type: none"> “IPsec Network Security Commands” “Certification Authority Interoperability Commands” 	<ul style="list-style-type: none"> DOC-785845 See Path.³ See Path.³ 	Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>Configuration Guide and Command References>Security Command Reference

Table 5-1 Related Documentation for Digital Certification (continued)

Document Title ¹	Customer Order Number	Path
New Feature Documentation	<ul style="list-style-type: none"> See Path.³ 	Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>New Feature Documentation
Cisco 7000 Family Routers		
Cisco 7100 Router <ul style="list-style-type: none"> Quick Start Guide Installation and Configuration Guide VPN Configuration Guide Reg. Comp. and Safety Information Release Notes for Release 12.0 XE Port and Service Adapters Field Replaceable Units 	<ul style="list-style-type: none"> DOC-786343 DOC-786341 DOC-786342 DOC-786345 DOC-786019 See Path.³ See Path.³ 	Hardware and Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Core/High-End Routers>Cisco 7100 Release Notes Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>Release Notes>Cisco 7000 Family Routers>Cisco 7000 Family - Release Notes for Cisco Release 12.0 XE

1. If you are viewing this guide online, the hyperlinks in this column are subject to change without notice. If this occurs, refer to the Path column.
2. Cisco Connection Online (CCO) is located at <http://www.cisco.com>. For more information, see “Cisco Connection Online.”
3. In the Path column, refer to the CCO path for a listing of the available publications.



Using Internet Key Exchange Mode Configuration: A Business Case

This chapter describes how Cisco Secure VPN Client interoperates with a Cisco router configured for Internet Key Exchange (IKE) Mode Configuration. IKE Mode Configuration allows a gateway to download an IP address (and other network level configuration) to the client as part of an IKE negotiation. Using this exchange, the gateway gives IP addresses to the IKE client to be used as an “inner” IP address encapsulated under IPSec. This provides a known IP address for the client which can be matched against the IP Security Protocol (IPSec) policy. This chapter contains the following sections:

- Benefit of Using Internet Key Exchange Mode Configuration
- Business Case Description
- Configuring and Verifying
- Related Documentation

Benefit of Using Internet Key Exchange Mode Configuration

To implement IPSec Virtual Private Networks (VPNs) between remote access clients with dynamic IP addresses and a corporate gateway, you have to dynamically administer scalable IPSec policy on the gateway once each client is authenticated. With IKE Mode Configuration, the gateway can set up scalable policy for a very large set of clients irrespective of the IP addresses of those clients. IKE Mode Configuration allows for dynamic IP addressing instead of static IP addressing on the client.

Business Case Description

The following business scenario is an example of one case in which you might employ the Cisco Secure VPN Client with a Cisco router.

- The Challenge
- The Risk
- The Solution

The Challenge

For large networks, a scalable IPsec policy must be set up between the clients and gateway, irrespective of the static IP addressing of the clients.

The Risk

As a network grows, configuring and maintaining additional clients can be time-consuming and complex. Each time the gateway is reconfigured to permit access to more clients, each client has to be reconfigured to match the gateway configuration.

The Solution

Use IKE Mode Configuration to begin your IKE negotiation. This secures the connection between the client and ISP with an IPsec tunnel, and allows for dynamic IP addressing of clients. Additional clients may be added to the network without having to reconfigure the gateway. Figure 6-1 shows the physical elements of an IKE Mode Configuration.

Figure 6-1 Physical Elements—IKE Mode Configuration Topology

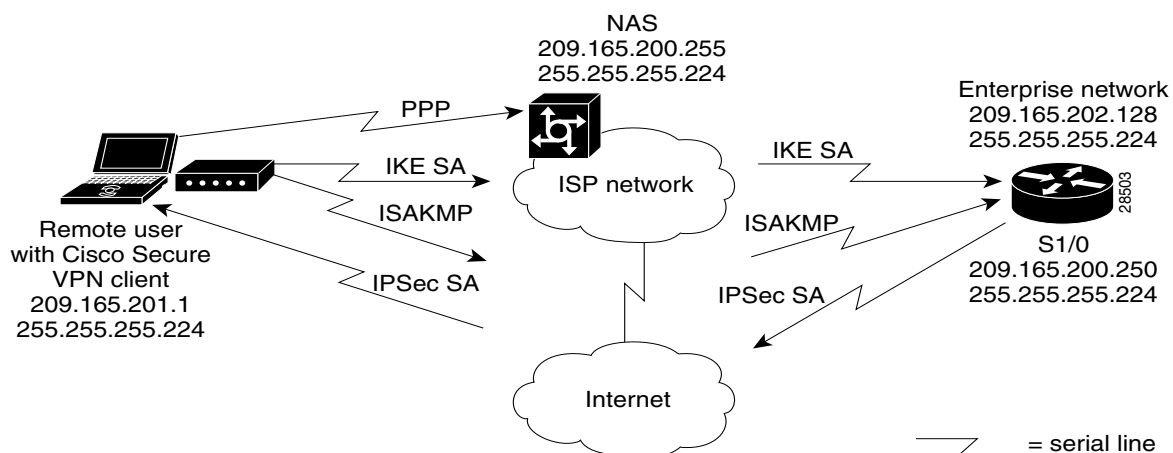


Table 6-1 IKE Mode Configuration Events - Client-initiated

Event	Description
1.	The client dials into the ISP through a modem using PPP.
2.	The client establishes IKE SA with the gateway.
3.	The gateway sends ISAKMP_CFG_SET to the client.
4.	The client sends ISAKMP_CFG_ACK to the gateway.
5.	The client uses internal attributes to establish IPsec SA.

Configuring and Verifying

This section covers the following information:

- Configuring Internet Key Exchange Mode Configuration
- Verifying IKE Mode Configuration

Configuring Internet Key Exchange Mode Configuration

Configuring IKE Mode Configuration for a secure tunnel between a remote client and a Cisco router involves the following tasks:

- Configuring the Cisco Secure VPN Client
- Configuring the Cisco Router

Configuring the Cisco Secure VPN Client

Because IKE Mode Configuration allows the Cisco Secure VPN Client to dynamically receive its IP address from the router, no client configuration is required. If a static IP address for the client preexists before enabling IKE Mode Configuration on the router, enabling IKE Mode Configuration will release the static IP address and renew the IP configuration with its own dynamic IP address for the client.

Configuring the Cisco Router

To configure the Cisco router, perform the following tasks:

- Task 1—Configuring the Domain Name, Host Name, and Name Server
- Task 2—Defining the Pool of IP Addresses
- Task 3—Defining the Crypto Maps That Attempt Client Configuration

Task 1—Configuring the Domain Name, Host Name, and Name Server

Task 1—Configuring the Domain Name, Host Name, and Name Server		
	Command	Purpose
Step 1	router> enable	Enter privileged EXEC mode.
Step 2	router# configure terminal Enter configuration commands, one per line. End with CNTL/Z.	Enter global configuration mode.
Step 3	router(config)# ip domain-name sisu.cisco.com	Define the domain name. Enter your domain name.
Step 4	router(config)# hostname hq_sanjose hq_sanjose(config)#	Define the host name. Enter your host name
Step 5	hq_sanjose(config)# ip name-server 200.165.200.225	Define the name server. Enter the gateway IP address.

Task 2—Defining the Pool of IP Addresses

Task 2—Defining the Pool of IP Addresses		
	Command	Purpose
Step 1	router(config)# ip local pool <pool-name> <start-addr> <end-addr>	Existing local address pools are used to define a set of addresses. To define a local address pool, use the existing ip local pool command. For more information on the ip local pool command, refer to the <i>Security Command Reference</i> , Cisco IOS Release 12.0.
Step 2	router(config)# crypto isakmp client configuration address-pool local <pool-name>	The local pool references the IKE configuration. To reference this local address pool in the IKE configuration, use the new crypto isakmp client configuration address-pool local command. For more information on the crypto isakmp client configuration address-pool local command, refer to the <i>Security Command Reference</i> , Cisco IOS Release 12.0.

Task 3—Defining the Crypto Maps That Attempt Client Configuration

Task 3—Defining the Crypto Maps That Attempt Client Configuration		
	Command	Purpose
	router(config)# crypto map <tag> client configuration address < initiate respond >	To configure IKE Mode Configuration in global crypto map configuration mode, use the new crypto map client configuration address command. For more information on the crypto map client configuration address command, refer to the <i>Security Command Reference</i> , Cisco IOS Release 12.0.

Verifying IKE Mode Configuration

To verify IKE Mode Configuration is configured, you must check the router's running configuration. Enter the **show running-config** command on the router in global configuration mode.

Related Documentation

For more information on configuring the Cisco Secure VPN Client using IKE Mode Configuration on a Cisco router, refer to Table 6-2.

Table 6-2 Related Documentation for IKE Mode Configuration

Cisco IOS Release 12.0 Documentation		
<i>Security Configuration Guide</i> <ul style="list-style-type: none"> “Configuring Internet Key Exchange Security Protocol” 	<ul style="list-style-type: none"> DOC-785843 See Path.¹ 	Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>Configuration Guide and Command References>Security Configuration Guide>Configuring Internet Key Exchange Security Protocol
<i>Security Command Reference</i> <ul style="list-style-type: none"> “Internet Key Exchange Security Protocol Commands” 	<ul style="list-style-type: none"> DOC-785845 See Path.¹ 	Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>Configuration Guide and Command References>Security Command Reference>Internet Key Exchange Security Protocol Commands
New Feature Documentation <ul style="list-style-type: none"> Internet Key Exchange Mode Configuration 	<ul style="list-style-type: none"> See Path.¹ See Path.¹ 	Software Documentation: <ul style="list-style-type: none"> CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>New Feature Documentation CCO>Service & Support>Technical Documents>Documentation Home Page>Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>New Feature Documentation>New Features in 12.0-Based Limited Lifetime Releases>New Features in Release 12.0 XE>New Features in Release 12.0(4)XE>Internet Key Exchange Mode Configuration

1. In the Path column, refer to the CCO path for a listing of the available publications.



A

Access Virtual Private Network

See Access VPN.

Access VPN

Access Virtual Private Network. A virtual private network (VPN) that provides remote access to a corporate intranet or extranet over a shared infrastructure with the same policies as a private network. Access VPNs encompass analog, dial, ISDN, Digital Subscriber Line (DSL), mobile IP, and cable technologies to securely connect mobile users, telecommuters, or branch offices.

AH

Authentication Header. A security protocol which provides data authentication and optional anti-replay services. AH is embedded in the data to be protected (a full IP datagram).

Both the older RFC1828 AH and the updated AH protocol are implemented.

RFC 1828 specifies the HMAC variant algorithm; it does not provide anti-replay services.

The updated AH protocol is per the latest version of the “IP Authentication Header” Internet Draft (draft-ietf-ipsec-auth-header-xx.txt). The updated AH protocol allows for the use of various authentication algorithms; Cisco IOS has implemented the mandatory MD5 and SHA (HMAC variants) authentication algorithms. The updated AH protocol provides anti-replay services.

anti-replay

A security service where the receiver can reject old or duplicate packets to protect itself against replay attacks. IPSec provides this optional service by use of a sequence number combined with the use of data authentication. This service is not available for manually established security associations (that is, security associations established by manual configuration and not by IKE).

authentication

The method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol you select, encryption. Authentication establishes data integrity and ensures no one tampers with the data in transit. It also provides data origin authentication.

Authentication Header

See AH.

C

CA	certification authority. A service responsible for managing certificate requests and issuing certificates to participating IPsec network devices. This service is explicitly entrusted by the receiver to validate identities and to create digital certificates. This service provides centralized key management for the participating devices.
CBC	Cipher Block Chaining. A component that requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPsec packet.
certification authority	See CA.
Certificate Manager	A dialog box in Cisco Secure VPN Client that allows you to request, import, and store the digital certificates you receive from certification authorities (CAs).
Certificate Signing Request	See CSR.
Cipher Block Chaining	See CBC.
client	A node or software program (front-end device) that requests services from a server.
Client-initiated Virtual Private Network	See Client-initiated VPN.
Client-initiated VPN	Client-initiated Virtual Private Network. A virtual private network (VPN) in which users establish an encrypted IP tunnel across the internet service provider (ISP)'s shared network to the enterprise customer's network. The enterprise customer manages the client software that initiates the tunnel.
crypto map	A command that filters traffic to be protected and defines the policy to be applied to that traffic.
CSR	Certificate Signing Request. An electronic request you send to the certification authority for a digital certificate signature. A digital certificate must be verified and signed by a certification authority to be valid.

D

D&B D-U-N-S number	Dun & Bradstreet Data Universal Numbering System. The certification authorityD&B D-U-N-S number is D&B's distinctive nine-digit identification sequence, which links to a many quality information products and services originating from D&B. The D&B D-U-N-S Number is an internationally recognized common company identifier in EDI and global electronic commerce transactions.
data confidentiality	<p>The ability to encrypt packets before transmitting them across a network. With confidentiality, the designated recipient can decrypt and read data, while those without authorization cannot decrypt and read this data. It is provided by encryption algorithms such as Data Encryption Standard (DES).</p> <p>Method where protected data is manipulated so that no attacker can read it. This is commonly provided by data encryption and keys that are only available to the parties involved in the communication.</p>

D (continued)

Data Encryption Standard	See DES.
data integrity	Verification for the recipient that data has not been modified during transmission. This is provided by secret-key, public-key, and hashing algorithms.
data origin authentication	A security service where the receiver can verify that protected data could have originated only from the sender. This service requires a data integrity service plus a key distribution mechanism, where a secret key is shared only between the sender and receiver. Also, see authentication.
DES	Data Encryption Standard. A standard that encrypts packet data. IKE implements the 56-bit DES-CBC with Explicit IV standard.
DH	A public key cryptography protocol which allows two parties to establish a shared secret over an insecure communications channel. Diffie-Hellman is used within Internet Key Exchange (IKE) to establish session keys. Diffie-Hellman is a component of Oakley key exchange. Cisco IOS software supports 768-bit and 1024-bit Diffie-Hellman groups.
Diffie-Hellman	See DH.
digital certificate	A digital certificate contains information to identify a user or device, such as the name, serial number, company, department or IP address. It also contains a copy of the entity's public key. The certificate is signed by a certification authority (CA).
digital signature	A digital signature is enabled by public key cryptography. It provides a means to digitally authenticate devices and individual users. A signature is formed when data is encrypted with a user's private key. A digital certificate receives its signature when it is signed by a certification authority (CA).
Dun & Bradstreet Data Universal Numbering System	See D&B D-U-N-S number.
dynamic IP address	A dynamic IP address is an IP address that is temporarily assigned as part of a login session, to be returned to an IP pool at the end of the session

E

Encapsulating Security Payload See ESP.

encapsulation The tunneling of data in a particular protocol header. For example, Ethernet data is tunneled in a specific Ethernet header before network transit. Also, when bridging dissimilar networks, the entire frame from one network is simply placed in the header used by the data link layer protocol of the other network.

encryption The application of a specific algorithm to data to scramble its appearance, making the data incomprehensible to those who are not authorized to see the information.

ESP Encapsulating Security Payload. A security protocol which provides data confidentiality and protection services, optional data authentication, and anti-replay services. ESP encapsulates the data to be protected. ESP can be used either by itself or in conjunction with AH.

Both the older RFC 1829 ESP and the updated ESP protocol are implemented.

RFC 1829 specifies DES-CBC as the encryption algorithm; it does not provide data authentication or anti-replay services.

The updated ESP protocol is per the latest version of the “IP Encapsulating Security Payload” Internet Draft (draft-ietf-ipsec-esp-v2-xx.txt). The updated ESP protocol allows for the use of various cipher algorithms and (optionally) various authentication algorithms. Cisco IOS implements the mandatory 56-bit DES-CBC with Explicit IV as the encryption algorithm, and MD5 or SHA (HMAC variants) as the authentication algorithms. The updated ESP protocol provides anti-replay services.

esp-des encryption algorithm Encapsulation Security Protocol (ESP) with the 56-bit Data Encryption Standard (DES) encryption algorithm. This is an ESP encryption transform. ESP is a security protocol which provides packet encryption and optional data authentication, and anti-replay services. ESP encapsulates the protected data. Data Encryption Standard (DES) is used to encrypt packet data.

esp-md5-hmac encryption algorithm ESP with the MD5 (HMAC variant) encryption algorithm. ESP is a security protocol which provides packet encryption and optional data authentication, and anti-replay services. ESP encapsulates the protected data. Message Digest 5 (MD5) is a hash algorithm used to authenticate packet data. HMAC is a keyed hash variant which provides an additional level of hashing.

Extranet Virtual Private Network See Extranet VPN.

Extranet VPN Extranet Virtual Private Network. A private communications channel between two or more separate entities that may involve data traversing the Internet or some other Wide Area Network (WAN). An extranet VPN links customers, suppliers, partners, or communities of interest to a corporate intranet over a shared infrastructure using dedicated connections.

G

gateway A device that performs an application layer conversion from one protocol stack to another.

H

hash algorithm	A mechanism for data authentication and maintenance of data integrity as packets are transmitted. This one way function takes an input message of arbitrary length and produces a fixed length digest. Cisco uses both Secure Hash Algorithm (SHA) and Message Digest 5 (MD5) hashes in the implementation of the IPSec framework. See HMAC variant.
HMAC variant	Keyed-Hashing for Message Authentication. A mechanism for message authentication using cryptographic hashes such as SHA and MD5. See RFC 2104.
Keyed-Hashing for Message Authentication	See HMAC variant.

I

IKE	<p>Internet Key Exchange. A hybrid protocol that implements Oakley key exchange and Skeme key exchange inside the ISAKMP framework. While IKE can be used with other protocols, its initial implementation is with the IPSec protocol. IKE provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations.</p> <p>IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require keys. Before any IPSec traffic can be passed, each router/firewall/host must be able to verify the identity of its peer. This can be done by manually entering pre-shared keys into both hosts or by a CA service.</p> <p>This is the protocol formerly known as ISAKMP/Oakley, and is defined in The Internet Key Exchange (IKE). A potential point of confusion is that the acronyms “ISAKMP” and “IKE” are both used in Cisco IOS software to refer to the same thing. These two items are somewhat different.</p>
Internet Engineering Task Force	Task force consisting of over 80 working groups responsible for developing Internet standards.
Internet Key Exchange	See IKE.
Internet Security Association and Key Management Protocol	See ISAKMP.
Internet Virtual Private Network	See Internet VPN.
Internet VPN	Internet Virtual Private Network. A private communications channel over the public access Internet that connects remote offices across the Internet and remote dial users to their home gateway via an ISP.
Intranet Virtual Private Network	See Intranet VPN.

I (continued)

Intranet VPN	Intranet Virtual Private Network. A private communications channel within an enterprise or organization that may or may not involve traffic traversing a Wide Area Network (WAN). An intranet VPN links corporate headquarters, remote offices, and branch offices over a shared infrastructure using dedicated connections.
IP Security Protocol	See IPSec.
IPSec	IP Security Protocol. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer; it uses IKE to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.
ISAKMP	Internet Security Association and Key Management Protocol. A protocol framework which defines payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of an SA.

M

MD5	<p>Message Digest Hash. One way hash that combines a shared secret and the message (the header and payload) to produce a 128-bit value. The recipient of the message runs the same hash of the message and compares it with the inserted hash value to yield the same result, which indicates that nothing in the packet has been changed in transit.</p> <p>SHA is more secure than MD4 and MD5. Cisco uses hashes for authentication within the IPSec framework.</p>
Message Digest 5	See MD5.

N

NAS	network access server. Cisco platform (or collection of platforms such as an AccessPath system which interfaces between the packet world (for, example) the Internet) and the circuit world (for example, the PSTN).
NAS-Initiated VPN	network access server-initiated Virtual Private Network. Users dial in to the ISP's network access server, which establishes an encrypted tunnel to the enterprise's private network.
network access server	See NAS.
network access server-initiated Virtual Private Network	See NAS-Initiated VPN.
non-repudiation	<p>A quality where a third party can prove that a communication between two other parties took place. Non-repudiation is desirable if you want to be able to trace your communications and prove that they occurred.</p> <p>See also repudiation.</p>

O

Oakley key exchange	A key exchange protocol that defines how to acquire authenticated keying material. The basic mechanism for Oakley is the Diffie-Hellman key exchange algorithm (DH).
----------------------------	--

P

peer	A router or device that participates as an endpoint in IPSec and IKE.
peer authentication methods	Methods required to authenticate the data flows between peers. Also used to generate a shared secret key to protect the IKE channel via DES-CBC. This shared secret key is also used as a basis for creating the IPSec shared secret encryption key by combining it with a random value.
Plain Old Telephone System	See PSTN.
POTS	See PSTN.
pre-shared keys	An authentication method in a policy. A given pre-shared key is shared between two peers.
PSTN	General term referring to the variety of telephone networks and services in place worldwide. Sometimes called Plain Old Telephone System (POTS).
public key cryptography	Each user has a key-pair containing both a public and a private key. The keys act as complements, and anything encrypted with one of the keys can be decrypted with the other. Public key cryptography is the same as public/private key system.

P (continued)

Public Switched Telephone Network See PSTN.

public/private key system See public key cryptography.

Q

- QoS** quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.
- quality of service** See QoS.

R

- replay-detection** A security service where the receiver can reject old or duplicate packets in order to defeat replay attacks (replay attacks rely on the attacker sending out older or duplicate packets to the receiver and the receiver thinking that the bogus traffic is legitimate). Replay-detection is done by using sequence numbers combined with authentication, and is a standard feature of IPSec.
- repudiation** A quality that prevents a third party from being able to prove that a communication between two other parties ever took place. This is a desirable quality if you do not want your communications to be traceable.
- See also non-repudiation.
- Rivest, Shamir and Adleman** See RSA.
- RSA** Rivest, Shamir and Adleman algorithm. A public key cryptographic algorithm (named after its inventors, Rivest, Shamir and Adleman) with a variable key length. Cisco's IKE implementation uses a Diffie-Hellman (DH) exchange to get the secret keys. This exchange can be authenticated with RSA (or pre-shared keys). With the Diffie-Hellman exchange, the DES key never crosses the network (not even in encrypted form), which is not the case with the RSA encrypt and sign technique. RSA is not public domain, and must be licensed from RSA Data Security.

S

- SA** Security Association. An instance of security policy and keying material applied to a data flow. Both IKE and IPSec use SAs, although SAs are independent of one another. IPSec SAs are unidirectional and they are unique in each security protocol. An IKE SA is used by IKE only, and unlike the IPSec SA, it is bi-directional. IKE negotiates and establishes SAs on behalf of IPSec. A user can also establish IPSec SAs manually.
- A set of SAs are needed for a protected data pipe, one per direction per protocol. For example, if you have a pipe that supports ESP between peers, one ESP SA is required for each direction. SAs are uniquely identified by destination (IPSec endpoint) address, security protocol (AH or ESP), and security parameter index (SPI).
- Secure Hash Algorithm** See SHA.
- Security Association** See SA.

S (continued)

Security Parameter Index See SPI.

security policy The means to configure the Policy Enforcement Points (PEPs) to accept or deny network traffic. These rules allow a network service to originate from a specific source.

Security Policy Editor A dialog box in Cisco Secure VPN Client that allows you to establish connections and associated authentication and key exchange proposals, then list them in hierarchical order for defining an IP data communications security policy.

SHA A one way hash put forth by NIST. SHA is closely modeled after MD4 and produces a 160-bit digest. Because SHA produces a 160-bit digest, it is more resistant to attacks than 128-bit hashes (such as MD5), but it is slower.

Skeme key exchange A key exchange protocol which defines how to derive authenticated keying material, with rapid key refreshment.

SPI Security Parameter Index. This is a number which, together with a destination IP address and security protocol, uniquely identifies a particular security association. When using IKE to establish the security associations, the SPI for each security association is a pseudo-randomly derived number. Without IKE, the SPI is manually specified for each security association.

static IP address A static IP address is a unique IP address that is assigned to a client for an extended period of time, to be used by only that client

T

3DES	A variant of the DES, which iterates three times with three separate keys, effectively doubling the strength of DES.
transform	A transform describes a security protocol (AH or ESP) with its corresponding algorithms. For example, ESP with the DES cipher algorithm and HMAC variant-SHA for authentication.
transform set	A grouping of IPSec algorithms to negotiate with IKE. A transform set specifies one or two IPSec security protocols (either ESP or AH or both) and specifies which algorithms to use with the selected security protocol.
transport mode	A mode in which the IP payload is encrypted, and the original IP headers are left intact. It adds only a few bytes to each packet and allows devices on the public network to see the final source and destination of the packet. This capability allows one to enable special processing (for example, quality of service) in the intermediate network based on the information on the IP header. However, the Layer 4 header will be encrypted, limiting the examination of the packet. The opposite of transport mode is tunnel mode.
Triple DES	See 3DES.
tunnel	A secure communication path between two peers, such as a client and a router.
tunnel mode	Encapsulation in which the entire original IP datagram is encrypted, and it becomes the payload in a new IP packet. This mode allows a network device, such as a router, to act as an IPSec proxy. The router performs encryption on behalf of the hosts. The source's router encrypts packets and forwards them along the IPSec tunnel. The destination's router decrypts the original IP datagram and forwards it on to the destination system.

V

Virtual Private Network	See VPN.
VPN	Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses tunnels to encrypt all information at the IP level.



INDEX

A

access VPNs **1-2**
Authentication Method
 option **4-23, 5-21**

B

benefits **1-9**

C

CA Certificates
 option **4-3**
certificate enrollment, configuring
 online **4-6**
Certificate Manager
 description **4-3, 5-3**
Certificate Signing Request **4-12, 5-9**
Cisco Secure VPN Client
 Certificate Manager
 description **4-3, 5-3**
 description **1-4**
 My Certificates option **4-5**
 Security Policy Editor **4-16, 5-14**
client-initiated VPNs **1-2**
connection
 description **4-17, 4-18, 5-15**
Connect using Secure Gateway Tunnel
 option **4-19, 5-17**
CSR
 See Certificate Signing Request

D

digital certificate **1-5**
 benefits **3-1**
 Certificate Signing Request **4-12, 5-9**
 description **3-1**
digital certificates
 importing **4-4**
D-U-N-S
 D&B numbering **4-10**

E

Enable Replay Detection
 description
 option **4-21, 5-19**
Encapsulation
 option **4-25, 5-23**
Encapsulation Protocol
 option **4-25, 5-23**
Encrypt Alg
 option **4-23, 5-21**
Encryption Alg
 option **4-25, 5-23**
extranet VPNs **1-2, 1-3**

H

Hash Alg
 option **4-23, 4-25, 5-21, 5-23**

I

ID Type

option **4-19, 4-20, 5-17, 5-18**

IKE

description **1-4**

IKE Mode Configuration

Internet Key Exchange Mode Configuration **6-1**

Internet Key Exchange

description **1-4**

intranet VPNs **1-2, 1-3**

IP Network Security

description **1-4**

IPSec

description **1-4**

IP Type

option **4-19, 5-17**

K

Key Group

option **4-23, 5-21**

M

Main Mode

description

option **4-21, 5-19**

Mask

option **4-19, 5-17**

NNAS-initiated VPNs **1-2**

new connection

See connection

P

Port

option **4-19, 4-20, 5-17, 5-18**

public/private key system **1-5**

R

root CA file **4-4, 5-4**

root certificate authority file **4-4, 5-4**

S

SA Life

option **4-23, 5-21**

Secure

option **4-19, 5-17**

security policy **1-5**

Security Policy Editor

description **4-16, 5-14**

Select Certificate

option **4-20, 5-18**

Subnet

option **4-19, 5-17**

system requirements **1-8**

V

VPN

description **1-1**

type

access **1-2**

client-initiated **1-2**

NAS-initiated **1-2**

extranet **1-2, 1-3**

intranet **1-2, 1-3**