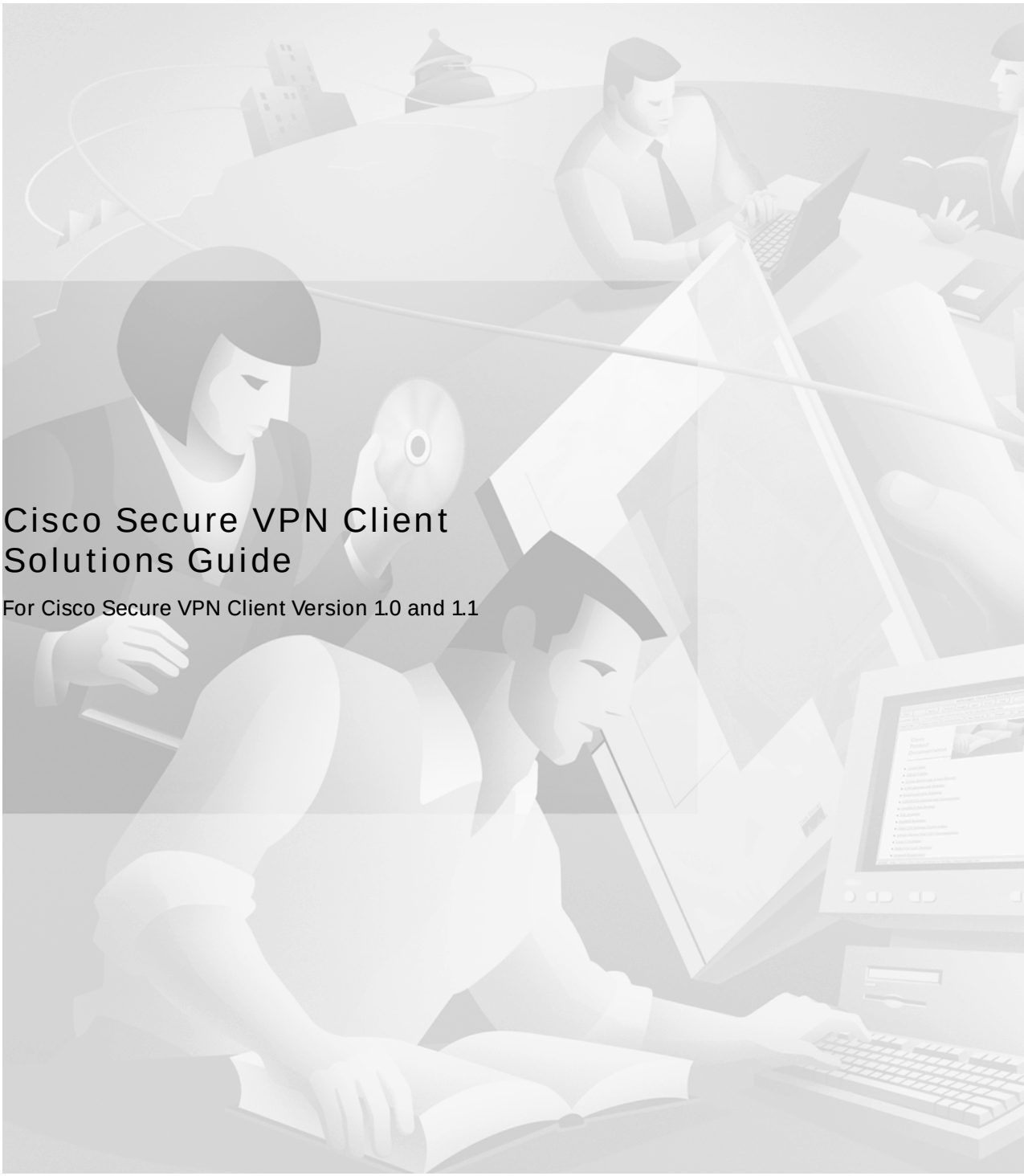
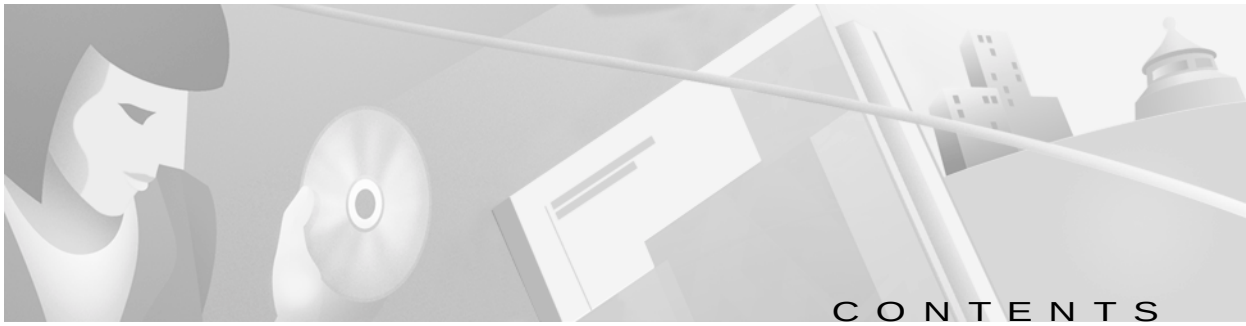


Cisco Secure VPN Client Solutions Guide

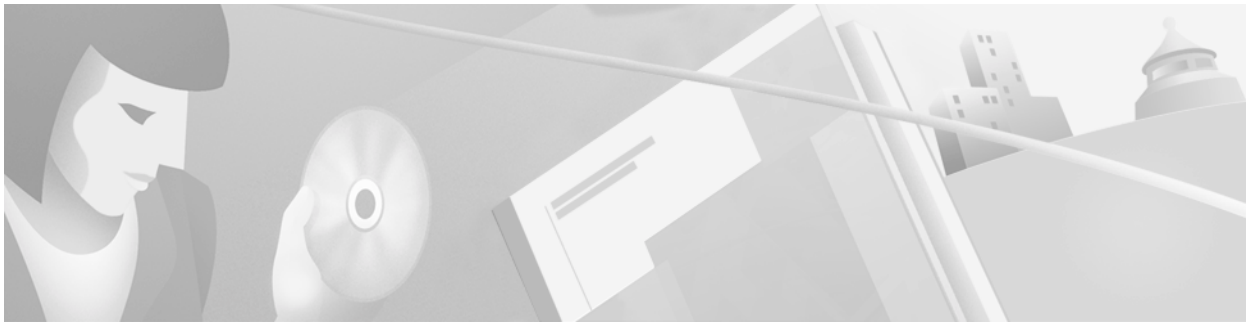
For Cisco Secure VPN Client Version 1.0 and 1.1

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-0259-02



CONTENTS



Preface

This guide describes Cisco-supported configurations for IP-based extranet Virtual Private Networks (VPNs) for an IP Security Protocol (IPSec) tunnel between a Cisco Secure VPN Client (VPN Client) and a Cisco IOS router or Cisco Secure PIX Firewall (gateway). The VPN Client acts as an IPSec peer that uses Internet Key Exchange (IKE) protocol and IPSec to negotiate, then establish an encrypted tunnel to another IPSec peer. Each configuration can consist of various Cisco IOS IPSec features including manual configuration, dynamic IP addressing, pre-shared keys, wildcard pre-shared keys, and digital certification.

This preface contains the following sections:

Scope

This guide does not cover every available feature for the Cisco Secure VPN Client; 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 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.

Audience

This solutions guide often refers to device-specific administrators, which can consist of any combination of the following audiences:

- Network administrators who are responsible for defining network security policies and distributing them to the end users within their 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

New and Changed Information

The following is new or changed information since the last release of the *Cisco Secure VPN Client* solutions guide:

- For the latest system requirements, feature and version specifications, sample VPN configurations, technical tips, and product bulletins for IPSec and the Cisco Secure VPN Client, this information will be maintained ongoing at the following URLs:
  - Sample configurations are available for non-registered users on CCO:

    http://www.cisco.com/warp/public/700/tech_configs.html#SECURITY

    or **Service & Support>Technical Assistance Center**>**Documents**>**Sample Configurations>Security**
  - Sample configurations and technical tips are available for registered users on CCO:

    http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Internetworking:IPSec&s=Implementation_and_Configuration#Samples_%26_Tips

    or **Service & Support>Technical Assistance Center**>**Technologies**>**IP Security (IPSec)**
  - Product literature is available for both non-registered and registered users on CCO:

    http://www.cisco.com/warp/public/cc/cisco/mkt/security/vpncli/prodlit/

    or **Products & Technologies**>**Cisco Secure**>**Security Products and Technologies**>**Cisco Secure VPN Client**>**Product Literature**
- A chapter titled “Case Study for Layer 3 Authentication and Encryption” has been added. This chapter provides a case study overview, a description of encryption and authentication features, site profile characteristics, and basic configuration tasks of IPSec tunneling between a VPN Client and a gateway.
- All chapters titled “Using...” have been changed to “Configuring...”
- All chapters previously documented as individual business cases are now configuring tasks, which can exist as standalone or combined tasks in the business case, “Case Study for Layer 3 Authentication and Encryption.”
- A chapter titled “Configuring Manual Configuration” has been added. This chapter describes how to configure a static IP address on your VPN Client.

- The chapter titled “Configuring Dynamic IP Addressing” has been modified to include illustrations of how this feature works, and protocol negotiation sequence.
- A chapter titled “Configuring a Pre-Shared Key or Wildcard Pre-Shared Key” has been added. This chapter describes how to configure a pre-shared key to authenticate a VPN Client or how to configure a wildcard pre-shared key to authenticate a pool of VPN Clients.
- The chapter on Entrust digital certificates has moved to the appendix titled Appendix A, “Configuring Entrust Digital Certificates.”
- An appendix titled Appendix B, “Configuring Microsoft Certificate Services” has been added.
- The chapter on VeriSign digital certificates has moved to the appendix titled Appendix C, “Configuring VeriSign Digital Certificates.”

Document Organization

The major elements of this guide are as follows:

Table 1 Document Organization

Chapter	Title	Description
Chapter 1	Access VPNs and IP Security Protocol Tunneling Technology Overview	Provides a physical overview of different types of VPNs, and VPN Client-specific details.
Chapter 2	Case Study for Layer 3 Authentication and Encryption	Provides a case study overview, site profile characteristics, and basic configuration tasks of IPSec tunneling between a VPN Client and a gateway.
Chapter 3	Configuring Manual Configuration	Shows how a static IP address is configured on a VPN Client for an IPSec tunnel between the VPN Client and a gateway.
Chapter 4	Configuring Dynamic IP Addressing	Shows how a static IP address is configured on a VPN Client for an IPSec tunnel between the VPN Client and a gateway.
Chapter 5	Configuring a Pre-Shared Key or Wildcard Pre-Shared Key	Shows how regular and wildcard pre-shared keys are generated for an IPSec tunnel between the VPN Client and a gateway.
Chapter 6	Configuring Digital Certification	Shows how digital certification is set up and maintained for an IPSec tunnel between the VPN Client and a gateway.
Appendix A	Configuring Entrust Digital Certificates	Shows how to request digital certification from the Entrust CA server and configure the CA server identity on your gateway.

Table 1 Document Organization (continued)

Chapter	Title	Description
Appendix B	Configuring Microsoft Certificate Services	Shows how to request digital certification using Microsoft Certificate Services and configure the CA server identity on your gateway.
Appendix C	Configuring VeriSign Digital Certificates	Shows how to request digital certification from the VeriSign CA server and configure the VeriSign CA identity on your gateway.
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.

Case Study Presented in This Solutions Guide

Most chapters in this solutions guide focus on configuring possible features within one business case, "Case Study for Layer 3 Authentication and Encryption." This business case explains the basic tasks for configuring an extranet VPN using a VPN Client to initiate an IPSec tunnel to the gateway of an enterprise network.

Related Documentation

The following sections describe the documentation available for the Cisco Secure VPN Client. Documentation is available as printed manuals and/or electronic documents.

Use this solutions guide with these documents:

- Product-Specific Documents
- Platform-Specific Documents
- Technology-Specific Documents
- Feature Modules
- Cisco IOS Software Documentation Set

Note 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 (Internet service provider VPN solutions), Cisco IOS software configuration, Cisco IOS router or access server installation and configuration.

Product-Specific Documents

Product-specific documents in this section include software that is a part of the Cisco Secure product family. These products include, but are not limited to, the following:

- Cisco Secure Policy Manager Documentation
- Cisco Secure VPN Client Documentation

Cisco Secure Policy Manager Documentation

These software documents are available for the Cisco Secure Policy Manager on CCO and the Documentation CD-ROM:

- On CCO: http://www.cisco.com/univercd/cc/td/doc/product/ismg/policy/index.htm

  or **Service & Support>Technical Documents>Documentation Home Page>Internet Services Management Group>Cisco Secure Policy Manager**
- On the Documentation CD-ROM: **Cisco Product Documentation>Internet Services Management Group>Cisco Secure Policy Manager**

Note Cisco Secure Policy Manager Version 2.0 is supported on the Cisco Secure VPN Client Version 1.0, but is not interoperable with Cisco Secure VPN Client Version 1.1. To avoid complications, make sure you have the compatible version of the Cisco Secure Policy Manager installed.

Table 2 Cisco Secure Policy Manager 2.0 Documentation

Document Titles	Chapter Topics	Customer Order Number
Configuring Cisco Secure Policy Manager	Getting Started Representing Your Network Populating the Network Topology Tree Configuring the Device-Specific Settings of Network Objects Configuring Monitoring and Reporting Working With Security Policies Generating, Verifying, and Publishing Command Sets Maintaining Cisco Secure Policy Manager	DOC-7810296
Installation Guide	Preface Planning Your Installation Installation Procedures Meeting the Prerequisites Working with Cisco Secure Policy Manager	DOC-786782
IPSec Tunnel Implementation	IPSec Tunnels Authentication Server Panel IPSec Tunnel Templates IPSec Tunnel Groups Configuring Policy Enforcement Points IPSec Tunnel Policy	OL-0426

Table 2 Cisco Secure Policy Manager 2.0 Documentation (continued)

Document Titles	Chapter Topics	Customer Order Number
Network Topology Definition	Understanding the Network Topology Tree Guidelines and Techniques for Defining Your Network Topology Representing Your Network Topology Populating the Network Topology Tree Configuring the Global Policy Override Settings for Policy Enforcement Points Configuring Administrative Control Communications Defining Traffic Flows and Shaping Rules	OL-0426
Upgrade Notes	Introduction System Requirements Upgrade the License Where To Go Next Related Documentation Obtaining Documentation Obtaining Technical Assistance	DOC-786808
Release Notes for Cisco Secure Policy Manager Version 2.0	Introduction Features and Functionality Changes System Requirements Installation Notes Limitations and Restrictions Caveats Related Documentation Obtaining Documentation Obtaining Technical Assistance	DOC-786781

Cisco Secure VPN Client Documentation

These software documents are available for the Cisco Secure VPN Client are on CCO and the Documentation CD-ROM:

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

  or **Service & Support>Technical Documents>Documentation Home Page>Internet Service Unit Documentation>Cisco Secure VPN Client**

- On the Documentation CD-ROM: **Cisco Product Documentation>Internet Service Unit Documentation>Cisco Secure VPN Client**

Table 3 Cisco Secure VPN Client Documentation

Document Titles	Chapter Topics	Customer Order Number
• *Cisco Secure VPN Client Version 1.0 Quick Start Guide* • *Cisco Secure VPN Client Version 1.1 Quick Start Guide*	Audience System Requirements Installing Cisco Secure VPN Client Roles in Cisco Secure VPN Client Operation Additional Information Configuring a Custom Installation Obtaining Documentation Ordering Documentation Obtaining Technical Assistance Documentation Feedback	DOC-786898 for Version 1.0 DOC-7810787 for Version 1.1
• *Release Notes for Cisco Secure VPN Client Version 1.0/1.0a* • *Release Notes for Cisco Secure VPN Client Version 1.1*	Introduction System Requirements Network Requirements Installation Notes Limitations and Restrictions Important Notes Caveats Related Documentation Cisco Connection Online Documentation CD-ROM	DOC-786929 for Versions 1.0/1.0a OL-0458 for Version 1.1
Cisco Secure VPN Client Solutions Guide	Preface Access VPNs and IP Security Protocol Tunneling Technology Overview Case Study for Layer 3 Authentication and Encryption Configuring Manual Configuration Configuring Dynamic IP Addressing Configuring Pre-shared Key or Wildcard Pre-shared Key Configuring Digital Certification Configuring Entrust Digital Certification Configuring Microsoft Certificate Services Configuring VeriSign Digital Certification Glossary	OL-0259

Platform-Specific Documents

Platform-specific documents include documents that are related to specific hardware platforms. A hardware platform is grouped as a set of models, or a series.

This section includes platform-specific documents, as follows:

- Cisco 1720 VPN Router Documentation
- Cisco 7100 VPN Router Documentation
- Cisco Secure PIX Firewall Documentation
- Access Router Documentation
- Access Server Documentation
- Core/High-End Router Documentation

Cisco 1720 VPN Router Documentation

These hardware and software documents are available for the Cisco 1720 VPN routers on CCO and the Documentation CD-ROM:

- On CCO: http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis1700/index.htm

  or **Service & Support>Technical Documents>Documentation Home Page>Access Servers and Access Routers>Modular Access Routers>Cisco 1720 Router**
- On the Documentation CD-ROM: **Cisco Product Documentation>Access Servers and Access Routers>Modular Access Routers>Cisco 1720 Router**

Table 4 Cisco 1720 VPN Router Documentation

Document Title	Chapter Topics	Customer Order Number
Cisco 1700 Series Quick Start Guide	Unpack the Box Install the Router Verify the Installation	DOC-785406
Cisco 1720 Router Release Notes, • Cisco IOS Release 12.0 T • Cisco IOS Released 12.1 T	Early Deployment Releases System Requirements New and Changed Information Limitations and Restrictions Important Notes Caveats Related Documentation Obtaining Documentation Obtaining Technical Assistance	DOC-786238 for Release 12.0 DOC-7810842 for Release 12.1 T
Cisco 1720 Router Hardware Installation Guide	About This Guide Overview of the Cisco 1700 Router Installing the Cisco 1700 Router Troubleshooting the Cisco 1700 Router Cisco 1700 Technical Specifications Cable Pinouts and Cabling Guidelines Installing and Upgrading Memory in the Cisco 1700 Router Ordering and Configuring an ISDN Line	DOC-785405

Table 4 Cisco 1720 VPN Router Documentation (continued)

Document Title	Chapter Topics	Customer Order Number
Cisco 1720 Software Configuration Guide	About This Guide Introduction to Configuring the Cisco 1700 Router Cisco IOS Software Skills Configuring a Leased Line Configuring Frame Relay Configuring ISDN Configuring Asynchronous Connections Configuring X.25 ROM Monitor Software Networking Concepts for the Cisco 1700 Router	DOC-785407
Regulatory Compliance and Safety Information for Cisco 1600 Routers and Cisco 1700 Routers	Electro-Magnetic Compatibility Compliance Operating Conditions for Canada Operating Conditions for the European Community Operating Conditions for the United Kingdom Agency Approvals Declaration of Conformity Conformit Europenne Marking Directive Translated Safety Warnings	DOC-786739
Cisco 1700 Series Configuration Notes	See CCO or Documentation CD-ROM	DOC-785977

Cisco 7100 VPN Router Documentation

These hardware and software documents are available for the Cisco 7100 series routers on CCO and the Documentation CD-ROM:

- On CCO: http://www.cisco.com/univercd/cc/td/doc/product/core/7100/index.htm

  or **Service & Support>Technical Documents>Documentation Home Page>Core/High-End Routers>Cisco 7100**
- On the Documentation CD-ROM: **Cisco Product Documentation>Core/High-End Routers>Cisco 7100**

Table 5 Cisco 7100 VPN Router Documentation

Document Title	Chapter Topics	Customer Order Number
Cisco 7100 Series Quick Start Guide	Prepare for Installation Rack-Mount the Router Connect the Router to the Network Connect the Power Start the System	DOC-786343
Cisco 7000 Family Routers Release Notes • Cisco IOS Release 12.0 T • Cisco IOS Release 12.1 T	System Requirements New and Changed Information Important Notes Caveats Related Documentation Service and Support Cisco Connection Online Documentation CD-ROM	DOC-786055 for Release 12.0 T DOC-7810811 for Release 12.1 T
Cisco 7100 Series Installation and Configuration Guide	Preface Cisco 7100 Series Product Overview Preparing for Installation Installing Cisco 7100 Series Routers Performing a Basic Startup Configuration Troubleshooting the Installation Modular Port Adapter Configuration Guidelines System Specifications Cable Specifications	DOC-786341
Cisco 7100 Series VPN Configuration Guide	Preface Using Cisco IOS Software Before You Begin Intranet and Extranet VPN Business Scenarios Remote Access VPN Business Scenario	DOC-786342

Table 5 Cisco 7100 VPN Router Documentation (continued)

Document Title	Chapter Topics	Customer Order Number
Regulatory Compliance and Safety Information for Cisco 7100 Series VPN Routers	If You Need More Information Cisco 7100 Series Overview Compliance with U.S. Export Laws and Regulations Regarding Encryption Standards Compliance Installation Requirements Safety Information Translated Safety Warnings Cisco Connection Online Documentation CD-ROM	DOC-786345
Port and Service Adapters	See CCO or Documentation CD-ROM	See CCO or Documentation CD-ROM
Field Replaceable Units	Using the Flash Disk Installing and Removing the Power Supply in Cisco 7100 Series Routers Installing Field-Replaceable Units Installing and Removing the Boot ROM in Cisco 7100 Using the Flash Disk	See CCO or Documentation CD-ROM

Cisco Secure PIX Firewall Documentation

These hardware and software documents are available for the Cisco Secure PIX Firewall on CCO and the Documentation CD-ROM:

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

  or **Technical Documents>Documentation Home Page>Internet Service Unit>Cisco Secure PIX Firewall**

- On the Documentation CD-ROM: **Cisco Product Documentation>Internet Service Unit>Cisco Secure PIX Firewall**

Note Cisco Secure PIX Firewall Version 5.0 is supported on the Cisco Secure VPN Client Version 1.0. Cisco Secure PIX Firewall Versions 5.1 and later are supported on the Cisco Secure VPN Client Version 1.1. To avoid complications, make sure you have the compatible version of the Cisco Secure PIX Firewall installed.

Table 6 Cisco Secure PIX Firewall Documentation

Document Title	Chapter Topics	Customer Order Number
• *Configuration Guide for the Cisco Secure PIX Firewall Version 5.1* • *Configuration Guide for the Cisco Secure PIX Firewall Version 5.0*	About This Manual Introduction Configuring the PIX Firewall Advanced Configurations Configuring IPSec Configuration Examples Command Reference PIX 515 Configuration Configuration Forms Acronyms and Abbreviations Configuring for MS-Exchange Use Subnet Masking and Addressing	DOC-7810392 DOC-787134
• *Release Notes for Cisco Secure PIX Firewall Version 5.1* • *Release Notes for Cisco Secure PIX Firewall Version 5.0*	System Requirements New and Changed Information Installation Notes Limitations and Restrictions Important Notes Caveats Related Documentation Cisco Connection Online Documentation CD-ROM	DOC-7810391 DOC-787133

Table 6 Cisco Secure PIX Firewall Documentation (continued)

Document Title	Chapter Topics	Customer Order Number
• *Installation Guide for the Cisco Secure PIX Firewall Version 5.1* • *Installation Guide for the Cisco Secure PIX Firewall Version 5.0*	About This Manual Introduction Installing a PIX Firewall Installing Failover Installing the PIX Firewall Syslog Server Opening a PIX Firewall Chassis Installing a Memory Upgrade Installing a Circuit Board Installing a DC Voltage Installing the PIX Firewall Setup Wizard	DOC-7810394 DOC-787135
• *Regulatory Compliance and Safety Information for the Cisco Secure PIX Firewall Version 5.1* • *Regulatory Compliance and Safety Information for the Cisco Secure PIX Firewall Version 5.0*	Agency Approvals Directives Compliance Safety Information Related Documentation Obtaining Documentation/Cisco Connection Online Obtaining Technical Assistance/Documentation CD-ROM	DOC-7810397
• *System Log Messages for the Cisco Secure PIX Firewall Version 5.1* • *System Log Messages for the Cisco Secure PIX Firewall Version 5.0*	About this Manual/About This Guide Introduction System Log Messages Messages Listed by Severity Level	OL-0249 See CCO or Documentation CD-ROM

Access Router Documentation

These hardware and software documents are available for modular access routers on CCO and the Documentation CD-ROM:

- On CCO: **Service & Support>Technical Documents>Documentation Home Page>Access Servers and Access Routers>Modular Access Routers**
- On the Documentation CD-ROM: **Cisco Product Documentation>Access Servers and Access Routers>Modular Access Routers**

Access Server Documentation

These hardware and software documents are available for access servers on CCO and the Documentation CD-ROM:

- On CCO: **Service & Support>Technical Documents>Documentation Home Page>Access Servers and Access Routers>Access Servers**
- On the Documentation CD-ROM: **Cisco Product Documentation>Access Servers and Access Routers>Access Servers**

Core/High-End Router Documentation

These hardware and software documents are available for core/high-end routers on CCO and the Documentation CD-ROM:

- On CCO: **Service & Support>Technical Documents>Documentation Home Page>Core/High-End Routers**
- On the Documentation CD-ROM: **Cisco Product Documentation>Core/High-End Routers**

Technology-Specific Documents

Technology-specific documents include internetworking solutions guides, data sheets, white papers, design implementation guides, technical tips, and product bulletins. The technology-specific documents in this section are specific to VPN. For additional technology-specific documents, refer to "Cisco IOS Software Documentation Set."

- A list of the available Cisco VPN documentation is available at the following site:

  http://www.cisco.com/warp/public/779/largeent/vpne/vpndocs/vpndoc.html

- Sample configurations and technical tips are available at the following site:

  http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Internetworking:IPSec&s=Implementation_and_Configuration#Samples_%26_Tips

- For additional information on configuring the VPN Client, refer to the following documents:
  - "Configuring IPSec" chapter in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.1*
  - "Configuration Examples" chapter in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.1*

Feature Modules

Feature modules describe new features and are an update to the Cisco IOS software documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. The feature module information is incorporated in the next printing of the Cisco IOS software documentation set.

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

  or **Technical Documents>Documentation Home Page>Internet Service Unit>Cisco Security Features**>**Cisco IOS Release-Specific Security Features** or **Cisco IOS Technology-Specific Security Features**

- On the Documentation CD-ROM: **Cisco Product Documentation>Internet Service Unit>Cisco Security Features**>**Cisco IOS Release-Specific Security Features** or **Cisco IOS Technology-Specific Security Features**

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents that are shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

Each module in the Cisco IOS software documentation set consists of two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. You can use each configuration guide in conjunction with its corresponding command reference.

On CCO and the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set.

- Release 12.0 Documentation Set
- Release 12.1 Documentation Set

Release 12.0 Documentation Set

Documentation modules for Cisco IOS Release 12.0 are located on CCO and the Documentation CD-ROM:

- On CCO: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/index.htm

  or **Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0>Configuration Guides and Command References**
- On the Documentation CD-ROM: **Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.0>Configuration Guides and Command References**

Table 7 Cisco IOS Release 12.0 Documentation Set

Document Title	Chapter Topics	Customer Order Number
• *Configuration Fundamentals Configuration Guide* • *Configuration Fundamentals Command Reference*	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management	DOC-785829 DOC-785830
• *Bridging and IBM Networking Configuration Guide* • *Bridging and IBM Networking Command Reference*	Transparent Bridging Source-Route Bridging Token Ring Inter-Switch Link Remote Source-Route Bridging DLSw+ STUN and BSTUN LLC2 and SDLC IBM Network Media Translation DSPU and SNA Service Point SNA Frame Relay Access Support APPN Cisco Database Connection NCIA Client/Server Topologies Cisco Mainframe Channel Connection Airline Product Set	DOC-785850 DOC-785851

Table 7 Cisco IOS Release 12.0 Documentation Set (continued)

Document Title	Chapter Topics	Customer Order Number
• *Dial Solutions Configuration Guide* • *Dial Solutions Command Reference*	X.25 over ISDN Appletalk Remote Access Asynchronous Callback, DDR, PPP, SLIP Bandwidth Allocation Control Protocol ISDN Basic Rate Service ISDN Caller ID Callback PPP Callback for DDR Channelized E1 & T1 Dial Backup for Dialer Profiles Dial Backup Using Dialer Watch Dial Backup for Serial Lines Peer-to-Peer DDR with Dialer Profiles DialOut Dial-In Terminal Services Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Dialup Networks Dial Business Solutions and Examples	DOC-785846 DOC-785847
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	Interface Configuration Overview LAN Interfaces Logical Interfaces Serial Interfaces	DOC-785905 DOC-785906
• *Network Protocols Configuration Guide, Part 1* • *Network Protocols Command Reference, Part 1*	IP Overview IP Addressing and Services IP Routing Protocols	DOC-785831 DOC-785834
• *Network Protocols Configuration Guide, Part 2* • *Network Protocols Command Reference, Part 2*	AppleTalk Novell IPX	DOC-785832 DOC-785835
• *Network Protocols Configuration Guide, Part 3* • *Network Protocols Command Reference, Part 3*	Network Protocols Overview Apollo Domain Banyan VINES DECnet ISO CLNS XNS	DOC-785833 DOC-785840
• *Security Configuration Guide* • *Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options	DOC-785843 DOC-785845

Table 7 Cisco IOS Release 12.0 Documentation Set (continued)

Document Title	Chapter Topics	Customer Order Number
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Switching Services Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing	DOC-785848 DOC-785849
• *Wide-Area Networking Configuration Guide* • *Wide-Area Networking Command Reference*	Wide-Area Network Overview ATM Frame Relay SMDS X.25 and LAPB	DOC-785838 DOC-785839
• *Voice, Video, and Home Applications Configuration Guide* • *Voice, Video, and Home Applications Command Reference*	Voice over IP Voice over Frame Relay Voice over ATM Voice over HDLC Frame Relay-ATM Internetworking Synchronized Clocks Video Support Universal Broadband Features	DOC-785854 DOC-785855
• *Quality of Service Solutions Configuration Guide* • *Quality of Service Solutions Command Reference*	Policy-Based Routing QoS Policy Propagation via BGP Committed Access Rate Weighted Fair Queueing Custom Queueing Priority Queueing Weighted Random Early Detection Scheduling Signaling RSVP Packet Drop Frame Relay Traffic Shaping Link Fragmentation RTP Header Compression	DOC-785852 DOC-785853
• *Cisco IOS Software Command Summary* • *Dial Solutions Quick Configuration Guide* • *System Error Messages* • *Debug Command Reference*		DOC-785859 DOC-785894 DOC-785860 DOC-785858

Release 12.1 Documentation Set

The Cisco IOS Release 12.1 software documentation set is located on CCO and the Documentation CD-ROM:

- On CCO: http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/index.htm

  or **Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.1**
- On the Documentation CD-ROM: **Cisco Product Documentation>Cisco IOS Software Configuration>Cisco IOS Release 12.1**

Table 8 Cisco IOS Release 12.1 Documentation Set

Document Title	Chapter Topics	Customer Order Number
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Configuration Fundamentals Overview Using the Command-Line Interface Using Configuration Tools Configuring Operating Characteristics Managing Connections, Menus, and System Banners Using the Cisco Web Browser Using the Cisco IOS File System Modifying, Downloading, and Maintaining Configuration Files Loading and Maintaining System Images Maintaining Router Memory Rebooting a Router Configuring Additional File Transfer Functions Monitoring the Router and Network Troubleshooting a Router Performing Basic System Management System Management Using System Controllers Web Scaling Using WCCP Managing Dial Shelves	DOC-7810222 DOC-7810223
• *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide* • *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference*	Overview of Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuring Apollo Domain Configuring Banyan VINES Configuring DECnet Configuring ISO CLNS Configuring XNS	DOC-7810241 DOC-7810245
• *Cisco IOS AppleTalk and Novell IPX Configuration Guide* • *Cisco IOS AppleTalk and Novell IPX Command Reference*	AppleTalk and Novel IPX Overview Configuring AppleTalk Configuring Novell IPX	DOC-7810240 DOC-7810267

Table 8 Cisco IOS Release 12.1 Documentation Set (continued)

Document Title	Chapter Topics	Customer Order Number
• *Cisco IOS Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume I* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume II*	Overview of SNA Internetworking Overview of Bridging Configuring Transparent Bridging Configuring Source-Route Bridging Configuring Token Ring Inter-Switch Link Configuring Token Ring Route Switch Module Overview of IBM Networking Configuring Remote Source-Route Bridging Configuring Data-Link Switching Plus+ Configuring Serial Tunnel and Block Serial Tunnel Configuring LLC2 and SDLC Parameters Configuring IBM Network Media Translation Configuring Frame Relay Access Support Configuring NCIA Server Configuring the Airline Product Set Configuring DSPU and SNA Service Point Support Configuring SNA Switching Services Configuring Cisco Transaction Connection Configuring Cisco Mainframe Channel Connection Adapters Configuring CLAW and TCP/IP Offload Support Configuring CMPC and CSNA Configuring CMPC+ Configuring the TN3270 Server	DOC-7810256 DOC-7810257 DOC-7810520

Table 8 Cisco IOS Release 12.1 Documentation Set (continued)

Document Title	Chapter Topics	Customer Order Number
• *Cisco IOS Dial Services Configuration Guide: Terminal Services* • *Cisco IOS Dial Services Configuration Guide: Network Services* • *Cisco IOS Dial Services Command Reference*	Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Networks X.25 on ISDN Solutions Telco Solutions Dial-Related Addressing Services Internetworking Dial Access Scenarios Preparing for Dial Access Modem Configuration and Management ISDN and Signalling Configuration PPP Configuration Dial-on-Demand Routing Configuration Dial-Backup Configuration Terminal Service Configuration	DOC-7810251 DOC-7810252 DOC-7810253
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Guide*	Interface Configuration Overview Configuring LAN Interfaces Configuring Serial Interfaces Configuring Logical Interfaces	DOC-7810224 DOC-7810238
• *Cisco IOS IP and IP Routing Configuration Guide* • *Cisco IOS IP and IP Routing Command Reference*	IP Overview Configuring IP Addressing Configuring DHCP Configuring IP Services Configuring Mobile IP Configuring On-Demand Routing Configuring RIP Configuring IGRP Configuring OSPF Configuring IP Enhanced IGRP Configuring Integrated IS-IS Configuring BGP Configuring Multicast BGP (MBGP) Configuring IP Routing Protocol-Independent Features Configuring IP Multicast Routing Configuring Multicast Source Discovery Protocol Configuring PGM Router Assist Configuring Unidirectional Link Routing Using IP Multicast Tools	DOC-7810592 DOC-7810239

Table 8 Cisco IOS Release 12.1 Documentation Set (continued)

Document Title	Chapter Topics	Customer Order Number
• *Cisco IOS Multiservice Applications Configuration Guide* • *Cisco IOS Multiservice Applications Command Reference*	Multiservice Applications Overview Configuring Voice over IP Configuring Gatekeepers (Multimedia Conference Manager) Configuring Voice over Frame Relay Configuring Voice over ATM Configuring Voice over HDLC Configuring Voice-Related Support Features Configuring PBX Signalling Configuring Store and Forward Fax Configuring Video Support Configuring Head-End Broadband Access Router Features Configuring Subscriber-End Broadband Access Router Features Configuring Synchronized Clocking	DOC-7810258 DOC-7810259

Table 8 Cisco IOS Release 12.1 Documentation Set (continued)

Document Title	Chapter Topics	Customer Order Number
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Quality of Service Overview Classification Overview Configuring Policy-Based Routing Configuring QoS Policy Propagation via Border Gateway Protocol Configuring Committed Access Rate Congestion Management Overview Configured Weighted Fair Queueing Configuring Custom Queueing Configuring Priority Queueing Congestion Avoidance Overview Configuring Weighted Random Early Detection Policing and Shaping Overview Configuring Generic Traffic Shaping Configuring Frame Relay and Frame Relay Traffic Shaping Signalling Overview Configuring RSVP Configuring Subnetwork Bandwidth Manager Configuring RSVP-ATM Quality of Service Interworking Link Efficiency Mechanisms Overview Configuring Link Fragmentation and Interleaving for Multilink PPP Configuring Compressed Real-Time Protocol IP to ATM CoS Overview Configuring IP to ATM CoS QoS Features for Voice Introduction	DOC-7810260 DOC-7810261

Table 8 Cisco IOS Release 12.1 Documentation Set (continued)

Document Title	Chapter Topics	Customer Order Number
• *Cisco IOS Security Configuration Guide* • *Cisco IOS Security Command Reference*	Security Overview AAA Overview Configuring Authentication Configuring Authorization Configuring Accounting Configuring RADIUS Configuring TACACS+ Configuring Kerberos RADIUS Commands TACACS+ Commands Access Control Lists: Overview and Guidelines Cisco Secure Integrated Software Firewall Overview Configuring Lock-and-Key Security (Dynamic Access Lists) Configuring IP Session Filtering (Reflexive Access Lists) Configuring TCP Intercept (Prevent Denial-of-Service Attacks) Configuring Context-Based Access Control Configuring Cisco Secure Integrated Software Intrusion Detection System Configuring Authentication Proxy Configuring Port to Application Mapping IP Security and Encryption Overview Configuring IPSec Network Security Configuring Certification Authority Interoperability Configuring Internet Key Exchange Security Protocol Configuring Passwords and Privileges Neighbor Router Authentication: Overview and Guidelines Configuring IP Security Options	DOC-7810248 DOC-7810249

Table 8 Cisco IOS Release 12.1 Documentation Set (continued)

Document Title	Chapter Topics	Customer Order Number
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Cisco IOS Switching Services Overview Switching Paths Overview Configuring Switching Paths Cisco Express Forwarding Overview Configuring Cisco Express Forwarding NetFlow Switching Overview Configuring NetFlow Switching MPLS Overview Configuring MPLS Configuring IP Multilayer Switching Configuring IP Multicast Multilayer Switching Configuring IPX Multilayer Switching Configuring Multicast Distributed Switching Routing Between VLANs Overview Configuring Routing Between VLANs with ISL Encapsulation Configuring Routing Between VLANs with IEEE 802.10 Encapsulation Configuring Routing Between VLANs with IEEE 802.1Q Encapsulation LAN Emulation Overview Configuring LAN Emulation Configuring Token Ring LANE MPOA Overview Configuring the MPOA Client Configuring the MPOA Server Configuring Token Ring LANE for MPOA	DOC-7810254 DOC-7810255
• *Cisco IOS Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	Wide-Area Networking Overview Configuring ATM Frame Relay Frame Relay-ATM Interworking Configuring SMDS Configuring X.25 and LAPB	DOC-7810246 DOC-7810247
• *Cisco IOS Configuration Guide Master Index* • *Cisco IOS Command Reference Master Index* • *Cisco IOS Command Summary* • *Cisco IOS Debug Command Reference* • *Cisco IOS Dial Services Quick Configuration Guide* • *Cisco IOS System Error Messages*		DOC-7810242 DOC-7810266 DOC-7810262 DOC-7810265 DOC-7810263

Conventions

Command Conventions

Command descriptions use the following conventions:

Convention	Description
Click **Window1>Window 2>Window3**	The > symbol represents a direction in which you are to navigate from one window to the next, using your mouse to click the windows in the order from first to last.
boldface font	Commands, keywords, menus, menu items, and options are in **boldface**.
italic font	Arguments or terms for which you supply values are in *italics*.
[ ]	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.
`boldface screen` font	Information you must type is in **`boldface screen`** font.Terminal sessions and console screens are in this font.
^	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 *reader take note*. Notes contain helpful suggestions or reference to material not contained in this manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss.

Document Conventions

Figure 1 Commonly Used Graphical User Interface Conventions

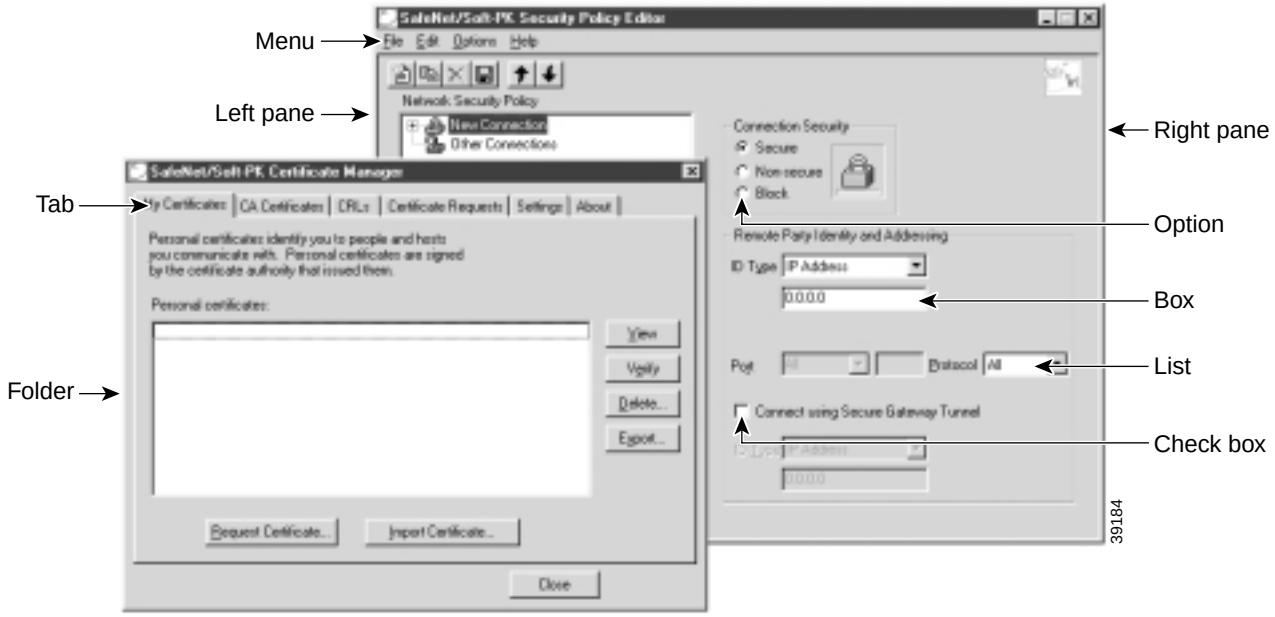
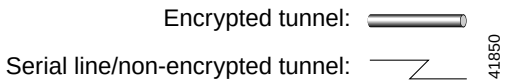


Figure 2 Commonly Used Images



Note Throughout this guide, there are numerous configuration examples that include unusable IP addresses, passwords, and public key examples. Be sure to use your own IP addresses, passwords, and public keys when configuring your VPN Clients and gateway.

Note The Cisco Secure VPN Client is also referenced as SafeNet/Soft-PK throughout this guide and in the software. Also, the SafeNet icon appears as the graphical user interface icon in the Windows taskbar. Unless the taskbar is changed, this icon appears in lower right corner of the screen.

Note For brevity, the Cisco Secure VPN Client is referred to as the generic term *VPN Client* throughout this guide. A Cisco IOS router or Cisco Secure PIX Firewall is referred to as the generic term *gateway* throughout this guide.

Note Throughout this guide, the standard pre-shared key authentication method is called *pre-shared keys*. Also, the wildcard pre-shared key authentication method is called *wildcard pre-shared key.* Unless otherwise specified, the single term *pre-shared keys* may apply to both pre-shared keys and wildcard pre-shared keys.

Note For a listing and description of the terms frequently used in this guide, refer to the "Glossary" at the end of this guide.

Obtaining Documentation

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.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 is updated monthly. Therefore, it is probably more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at http://www.cisco.com/cgi-bin/subcat/kaojump.cgi.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the web, e-mail, a self-addressed stamped response card included in many printed docs, or by sending mail to Cisco.

Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on CCO to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: www.cisco.com
- Telnet: cco.cisco.com
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
  - From North America, call 408 526-8070
  - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to cco-team@cisco.com.

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use www.cisco.com/techsupport.

To contact by e-mail, use one of the following:

Language	E-mail Address
English	tac@cisco.com
Hanzi (Chinese)	chinese-tac@cisco.com
Kanji (Japanese)	japan-tac@cisco.com
Hangul (Korean)	korea-tac@cisco.com
Spanish	tac@cisco.com
Thai	thai-tac@cisco.com

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml.

Documentation Feedback

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

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate and value your comments.

CHAPTER 1

Access VPNs and IP Security Protocol Tunneling Technology Overview

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

This chapter contains the following sections:

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

Virtual Private Networks Overview

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

The following sections describe the three basic types of VPNs:

- Access VPNs
- Intranet VPNs
- Extranet VPNs

Access VPNs

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

The following sections describe the two types of access VPNs:

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

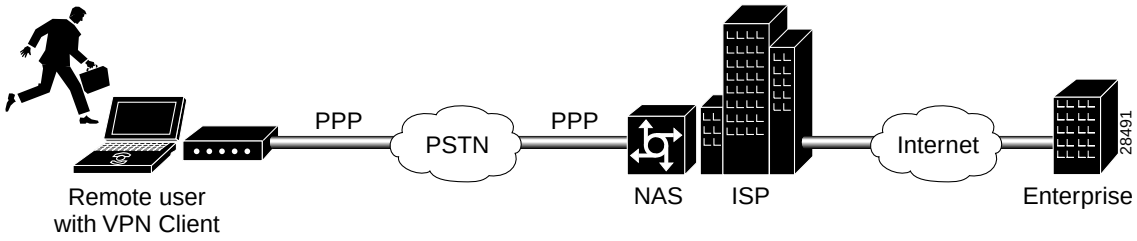
Client-Initiated Access VPNs

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

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

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

Figure 1-1 Client-Initiated Access VPN

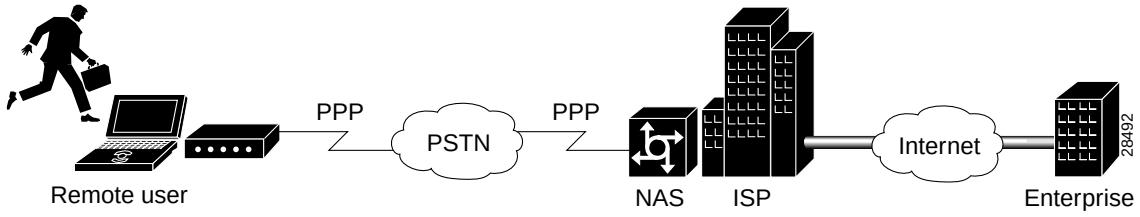


NAS-Initiated Access VPNs

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

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

Figure 1-2 NAS-Initiated Access VPN



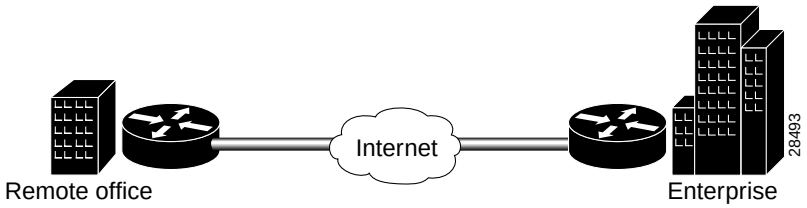
Intranet VPNs

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

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

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

Figure 1-3 Intranet VPN



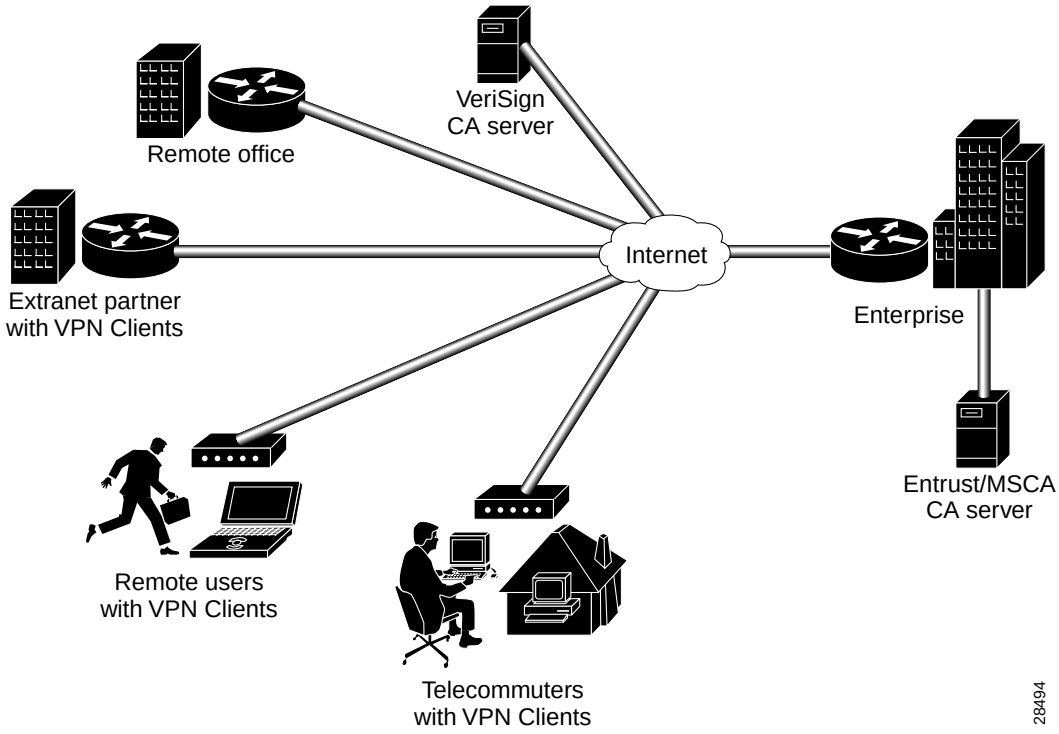
Extranet VPNs

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

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

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

Figure 1-4 Extranet VPNs



Cisco Secure VPN Client Overview

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

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

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

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

Generating a Public/Private Key

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

Getting a Digital Certificate

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

Establishing a Security Policy

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

Interoperability with Networking Devices

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

This section contains the following topics:

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

Recommended Networking Devices

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

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

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

Networking Devices with IP Security Protocol

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

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

Supported Configurations

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

- Using Pre-Shared Keys
- Using Digital Certification

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

Using Pre-Shared Keys

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

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

Using Digital Certification

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

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

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

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

System Requirements

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

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

Client-Side Requirements (Software)

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

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

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

Server-Side Requirements (Hardware and Software)

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

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

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

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

Benefits

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

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

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

Client-Initiated versus NAS-Initiated Access VPNs

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

Table 1-1 Client-Initiated versus NAS-Initiated

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

Cisco Secure VPN Client versus Other VPN Solutions

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

CHAPTER 2

Case Study for Layer 3 Authentication and Encryption

This chapter explains the basic tasks for configuring a multi-service, extranet Virtual Private Network (VPN) between a Cisco Secure VPN Client (VPN Client) and a Cisco IOS networking device (gateway). This case study describes IP Security Protocol (IPSec) tunnelling. This chapter includes the following sections:

- Case Study Overview
- Site Profile Characteristics

Note Throughout this chapter, there are numerous configuration examples that include unusable IP addresses, passwords, and public key examples. Be sure to use your own IP addresses, passwords, and public keys when configuring your VPN Clients and gateway.

Case Study Overview

This case study describes how an enterprise plans, designs, and implements remote access VPNs using IPSec tunneling protocol. IPSec tunneling protocol authenticates and encrypts point-to-point (PPP) sessions from one device to another across a shared network infrastructure. This case study describes how a VPN Client is authenticated and encrypts an IPSec tunnel to the corporate enterprise. This case study contains following topics:

- IPSec Tunneling Protocol
- Authentication and Encryption Features
- Building an Access VPN

IPSec Tunneling Protocol

This section includes the following topics:

- Description of IPSec Tunneling
- Function of IPSec Tunneling
- Benefits of IPSec Tunneling
- Roles in IPSec Tunneling

Description of IPSec Tunneling

IPSec tunneling protocol is based on the IPSec Security Protocol feature, which is framework of open standards developed by the Internet Engineering Task Force (IETF). IPSec 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.

Function of IPSec Tunneling

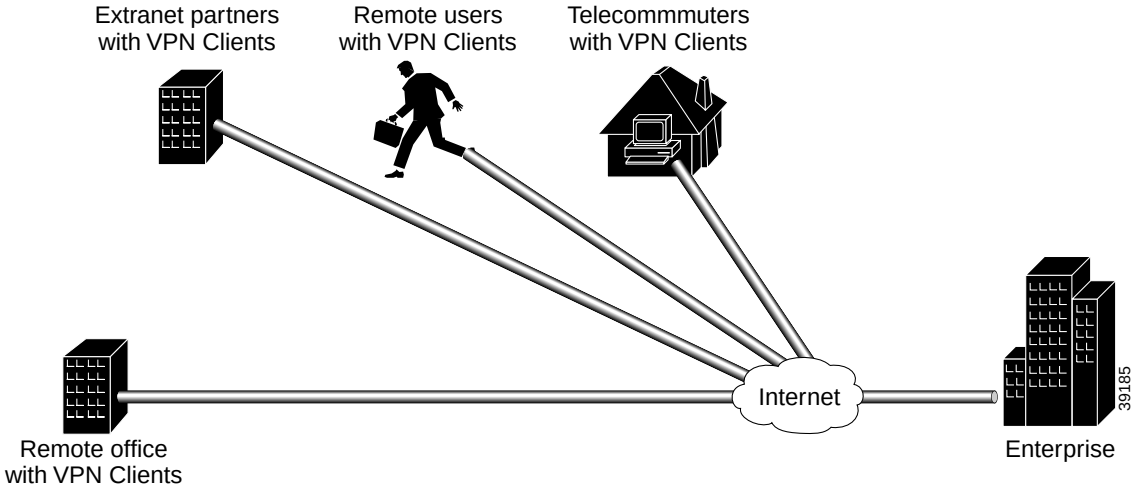
In IPSec tunnel mode, the remote users' VPN Clients encrypt the entire original IP datagrams. These encryptions become the payload in new IP packets. The VPN Clients initiate IPSec tunnels with a network device, such as a Cisco IOS router or a Cisco Secure PIX Firewall (gateway). The gateway acts as an IPSec proxy, performing encryption on behalf of all the hosts. The VPN Clients encrypt packets and forward them along the IPSec tunnel. The gateway decrypts the original IP datagrams and forwards them to their destination.

Benefits of IPSec Tunneling

The major advantage of IPSec tunnel mode is that the end systems do not need to be modified to receive the benefits of IPSec. IPSec tunnel mode also protects against traffic analysis; with IPSec tunnel mode an attacker can only determine the tunnel endpoints and not the true source and destination of the tunneled packets, even if they are the same as the tunnel endpoints.

Figure 2-1 shows an enterprise with a specific business objective. The enterprise must provide secured access to multiple remote users (such as telecommuters, travelling remote users, remote offices, and extranet partners). To do this, remote users use VPN Clients to authenticate a connection to the corporate internal network, then to encrypt tunnels for data to the corporate internal network using IPSec tunneling protocol.

Figure 2-1 End-to-End Client-Initiated Access VPN Scenario



Roles in IPSec Tunneling

- The extranet partner purchases, configures and maintains the PC and the VPN Client software.
- The remote users, telecommuters and remote offices all obtain equipment from the enterprise.
- The enterprise network administrator purchases, configures, and maintains the VPN Client software, the remote access PCs on which the VPN Client software is to be installed, the home gateway, a public web server, and the private corporate server.

Authentication and Encryption Features

For the enterprise, there are several business considerations when configuring Layer 3 Encryption:

- Will each remote user's VPN Client use manual pre-shared keys or scalable digital certificates for authentication?
- Will each remote user's VPN Client use its own pre-shared key for authentication or will a group of remote users' VPN Client share a wildcard pre-shared key for authentication?
- Will each remote user's VPN Client be manually configured for individual device authentication or will each group of remote users' VPN Clients be dynamically configured for authentication?

These considerations affect the overall VPN architecture of the enterprise network. Based on the features you choose to configure your VPN network, your network will be more or less secure and scalable. This section provides a brief introduction of the encryption features, their limitations and restrictions, and their role in a VPN solution. Depending on your network topology, one or more of the following encryption features may be a requirement in your VPN network.

- Manual Configuration (Static IP Addressing)
- IKE Mode Configuration (Dynamic IP Addressing)
- Pre-Shared Keys
- Wildcard Pre-Shared Keys
- Digital Certification

Note For information about which features are supported on a specific Cisco IOS software release or version of the VPN Client, refer to the release notes for your version of the VPN Client. For more details, refer to "Cisco Secure VPN Client Documentation" in the Preface.

Manual Configuration (Static IP Addressing)

This section includes the following topics:

- Description of Manual Configuration
- Function of Manual Configuration
- Benefits of Manual Configuration
- Limitations and Restrictions of Manual Configuration
- Alternatives to Manual Configuration

Description of Manual Configuration

The manual configuration feature addresses the enterprise requirement to allow for a more secure method of assigning IP addresses to a small number of VPN Clients by assigning static internal IP addresses. 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.

Function of Manual Configuration

Without the manual configuration feature, it is difficult for the gateway to authenticate a VPN Client with an IP address dynamically-assigned through an ISP. A local ISP assigns the VPN Client a routable IP address from its pool. The VPN Client creates an encrypted tunnel to the gateway. The tunnel source IP address, which is the IP address of the client as the IPSec peer, matches the original source IP address, which is the IP address assigned to the client by the ISP for communications with the ISP. Because both source IP addresses match, the gateway cannot determine which source IP address belongs to the trusted peer.

Benefits of Manual Configuration

For an enterprise with a small number of VPN Clients, manual configuration is a simple method of assigning internal corporate IP addresses to each remote VPN Client, making it easier to set up IPSec policy on each VPN Client. IKE Mode Configuration is the alternative to manually configuring internal IP addresses on each remote access VPN Client.

Limitations and Restrictions of Manual Configuration

For a large number of VPN Clients, manual configuration is not a very secure method. The IP address on the VPN Client is static, and remains configured on the VPN Client even when a remote user is not logged on. The static IP address or IKE security parameters on the VPN Client can be viewed, then used by an untrusting party. The untrusting party can masquerade as the remote user. For this reason, manual configuration is less secure than IKE Mode Configuration in that it is more sensitive to IP spoofing attacks. Should an attacker get access to the IKE security parameters on a VPN Client, that attacker can masquerade as the remote user authorized to connect to the corporate network.

For a large number of VPN Clients, manual configuration is also not very scalable because each VPN Client must be manually configured. Each time the network grows, configuring and maintaining additional VPN Clients can be time-consuming and complex. Each time the gateway is reconfigured to permit access to more VPN Clients, each VPN Client has to be reconfigured to match the new gateway configuration.

To prevent attacks, the following instructions should be a part of your enterprise security policy:

- The gateway administrator *must* manually configure each client. Each time a VPN Client is added to the network, the gateway administrator must configure another **access-list** global configuration command on the gateway to permit traffic from that static IP address on the VPN Client. Also, the gateway administrator must ensure all traffic destined for the VPN Clients' subnet is routed back to the gateway to be encrypted, using the **crypto map local-address** global configuration command with interface **loopback0**. A loopback interface is a virtual interface that is always up and allows routing protocols to stay up even if the physical interface is down.
- On the gateway, the gateway administrator *must* configure an access-list rule matching each VPN Client IP address because of the source proxy definitions—which are IP addresses instead of subnets—on the VPN Clients.
- The gateway administrator *must* ensure all traffic destined for the VPN Clients' IP address pool on the enterprise subnet is routed back to the gateway for encryption, because the gateway does not automatically route to the VPN Clients. To do this, the gateway administrator *must* define a static route between the gateway and all VPN Clients.

Alternatives to Manual Configuration

The alternative to static IP addressing with manual configuration is dynamic IP addressing with IKE Mode Configuration.

IKE Mode Configuration (Dynamic IP Addressing)

This section includes the following topics:

- Description of IKE Mode Configuration
- Function of IKE Mode Configuration
- Benefits of IKE Mode Configuration
- Alternatives to IKE Mode Configuration

Description of IKE Mode Configuration

The IKE Mode Configuration feature addresses the enterprise requirement to issue scalable, dynamic IP addresses to one or more clients by configuring scalable IPSec policy on the gateway. 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. IKE Mode Configuration is a gateway-initiated IKE negotiation that occurs between IKE phase 1 and IKE phase 2. The gateway assigns a dynamic IP address to the VPN Clients, replacing any current IP address configuration on the VPN Clients. IKE Mode Configuration secures the connection between the VPN Clients and ISPs with an IPSec tunnel, and allows for dynamic IP addressing of VPN Clients from the gateway. With IKE Mode Configuration, you can download IP addresses (and other network level configuration, such as your IPSec policy) to VPN Clients as part of an IKE negotiation. The gateway administrator can add VPN Clients to the network without having to reconfigure the gateway or the VPN clients.

Function of IKE Mode Configuration

Without the IKE Mode Configuration feature, it is difficult for the gateway to administer scalable IPSec policy on many VPN Clients. A new IPSec policy is required for each VPN Client because each has a dynamic IP address, each dynamic IP address is assigned by the VPN Client's local ISP, and each of these dynamic IP addresses will not be within the enterprise subnet's IP address range.

When a remote user wants to connect to an corporate gateway, the remote user's VPN Client must first establish a point-to-point (PPP) connection to the ISP's NAS (network access server). The NAS authenticates the PPP connection. Then, the VPN Client initiates ISAKMP SA with the untrusted peer at the gateway. After the ISAKMP SA is created and authenticated, the gateway initiates IKE Mode Configuration with the VPN Client. After the VPN Client receives the dynamic IP address from the gateway, the VPN Client loads the IPSec SA from the gateway.

Benefits of IKE Mode Configuration

For corporations with large numbers of VPN Clients, IKE Mode Configuration is a scalable approach to assigning dynamic IP addresses and administering IPSec policy for VPNs between multiple remote access VPN clients and corporate networks. Gateway administrators do not have to manually configure each VPN Client, because no VPN Client configuration is required. With IKE Mode Configuration, the gateway can set up a scalable IPSec policy for a very large set of VPN Clients, replacing pre-existing IP addresses on VPN Clients with dynamic IP addresses within the IP range of the corporate subnet.

IKE Mode Configuration uses dynamic IP addressing, which is more secure than manual configuration with static IP addressing. The IPSec policy set up on the gateway uses dynamic crypto maps. With IKE Mode Configuration, each time a remote user forms a tunnel to the gateway using a VPN Client, a new IP address from within the corporate subnet's IP address pool is assigned to the VPN Client. Also, unlike manual configuration, IKE Mode Configuration does not rely on an access list because the gateway administrator can easily define the local address pool on the gateway. In addition, the gateway automatically defines a static route to the VPN Clients and inserts the static route into the routing table during IKE Mode Configuration. When all IKE and IPSec negotiations are completed, IKE Mode Configuration automatically removes the dynamic IP address, returns it to the corporate subnet's IP address pool, and removes the static route.

Alternatives to IKE Mode Configuration

The alternative to dynamic IP addressing with IKE Mode Configuration is static IP addressing with manual configuration.

Pre-Shared Keys

This section includes the following topics:

- Description of Pre-Shared Keys
- Function of Pre-Shared Keys
- Benefits of Pre-Shared Keys
- Limitations and Restrictions of Pre-Shared Keys
- Alternatives to Pre-Shared Keys

Description of Pre-Shared Keys

The pre-shared key feature addresses the enterprise requirement to allow for one or more clients to use individual shared secrets to authenticate encrypted tunnels to a gateway using IKE. The Diffie-Hellman key exchange combines public and private keys to create a shared secret to be used for authentication between IPSec peers. The shared secret can be shared between two or more peers. At each participating peer, you would specify a shared secret as part of an IKE policy. Distribution of this pre-shared key usually takes place through a secure out-of-band channel.

Note When using a pre-shared key, if one of the participating peers is not configured with the same pre-shared key, the IKE SA cannot be established. An IKE SA is a prerequisite to an IPSec SA. You *must* configure the pre-shared key at all peers.

Function of Pre-Shared Keys

The pre-shared key feature requires that each client has its own pre-shared key, which must match a pre-shared key configured on the gateway for authentication. Use pre-shared keys for VPN Clients with static or dynamic IP addresses.

Benefits of Pre-Shared Keys

Pre-shared keys are commonly used in small networks of up to 10 clients. With pre-shared keys, there is no need to involve a CA for security.

Limitations and Restrictions of Pre-Shared Keys

To prevent attacks, the following instructions should be a part of your security policy:

- The gateway administrated *must* initially configure each client with a separate and distinct key for secure authentication.
- Each time another client or remote user is added, the gateway administrator *must* configure that client with a new key, and reconfigure the gateway to permit that new key.
- Each time a client or remote user is removed, the gateway administrator *must* reconfigure the gateway to deny the key that client used.

Alternatives to Pre-Shared Keys

Without a method of client authentication, you cannot establish an encrypted tunnel between a client and gateway. Digital certification and wildcard pre-shared keys are alternatives to pre-shared keys. Both digital certification and wildcard pre-shared keys are more scalable than pre-shared keys.

Wildcard Pre-Shared Keys

This section includes the following topics:

- Description of Wildcard Pre-Shared Keys
- Function of Wildcard Pre-Shared Keys
- Benefits of Wildcard Pre-Shared Keys
- Limitations and Restrictions of Wildcard Pre-Shared Keys
- Alternatives to Wildcard Pre-Shared Keys

Description of Wildcard Pre-Shared Keys

The wildcard pre-shared key feature addresses the enterprise requirement to allow for one or more clients to use a shared secret key to authenticate encrypted tunnels to a gateway. With a wildcard pre-shared key configured on a router, any peer using the same pre-shared key is a valid peer to the router.

The key that you configure on one peer is identical to the values assigned to prospective peers. With wildcard pre-shared keys, a peer is no longer a static IP address, but a subnet that is dynamically assigned by the router.

Function of Wildcard Pre-Shared Keys

The wildcard pre-shared feature allows a group of clients with the same level of authentication to share a pre-shared key, which also must match a pre-shared key configured on the gateway for authentication. Use wildcard pre-shared keys for VPN Clients with static or dynamic IP addresses.

Benefits of Wildcard Pre-Shared Keys

Because a group of VPN Clients with the same level of authentication share a key, the wildcard pre-shared key method scales better than pre-shared keys. Each time another VPN Client is added, that client only needs to be configured with the group key—no gateway reconfiguration is required. Each time a client is removed, the gateway and all VPN Clients must be reconfigured with a new group key to prevent attacks. The *wildcard* aspect of wildcard pre-shared keys means that any IPSec peer with the pre-shared key can access the enterprise network, regardless of the IPSec peer's IP address assignment.

Limitations and Restrictions of Wildcard Pre-Shared Keys

The wildcard pre-shared key feature is vulnerable to IP spoofing, specifically the *man-in-the-middle* attack. An attacker can potentially redirect all traffic between the IPSec peers to go through an IKE proxy. If an attacker knows the pre-shared key and can redirect all traffic between the IPSec peers to go through an IKE proxy, the attacker can read and modify the IPSec-protected data without detection.

To prevent attacks to one or more parties using wildcard pre-shared key(s), the following instructions should be a part of your enterprise security policy:

- The gateway administrator *must* initially configure each client with the group key for secure authentication.
- For different groups of remote users requiring varying levels of authorization, the gateway administrator *must* use a distinctly different key for each peer. The gateway administrator *must* configure a key for each level of trust, and assign the correct keys to the correct parties.
- Each time another client or remote user is added to a group, the gateway administrator or remote user *must* configure that client with the pre-existing group key.

- Each time a client or remote user is removed from a group, the gateway administrator *must* reconfigure the gateway for a new group key. The remote user whose client is removed becomes an untrusted peer. The remaining trusted remote users *must* reconfigure their clients for a new key. The gateway administrator should distribute the new group key and instructions to remote users through a secure channel.

Alternatives to Wildcard Pre-Shared Keys

Without a method of client authentication, you cannot establish an encrypted tunnel between a client and gateway. Digital certification and pre-shared keys are alternatives to wildcard pre-shared keys.

Digital Certification

This section includes the following topics:

- Description of Digital Certification
- Function of Digital Certification
- Benefits of Digital Certification
- Limitations and Restrictions of Digital Certification
- Alternatives to Digital Certification

Description of Digital Certification

The digital certification feature addresses the enterprise requirement to allow one or more clients to use digital certificates to authenticate encrypted tunnels to a gateway. Digital certification is supported on the Cisco Secure VPN Client in certification authority (CA) and Registration Authority (RA) modes.

Simple Certificate Enrollment Protocol (SCEP) is a certificate enrollment protocol based on common and well understood PKCS #10/7 standards using HTTP transport methods. SCEP provides a standard way to enroll network devices with a CA, as well as to lookup and retrieve CRL information from LDAP or HTTP methods. Version 1.1 of the VPN Client supports the Registration Authority (RA) mode for SCEP enrollment. RA SCEP is currently supported by the Entrust and Microsoft CAs.

Note See to the latest release notes of your specific version of the VPN Client and networking devices for CA support.

Entrust VPN Connector or Microsoft Certificate Services

These CAs require that both IPSec peers transact with a Registration Authority (RA), which then forwards the requests through to the CA. Both the remote IPSec peer and the local IPSec peer must be configured with both the CA and RA public keys. The CA and RA public keys are signature and encryption key pairs, which must be generated and enrolled for authentication to occur.

- For more details, refer to Appendix A, “Configuring Entrust Digital Certificates.”
- For more details, refer to Appendix B, “Configuring Microsoft Certificate Services.”

VeriSign Onsite Management Service

This CA provides certificate processing, backup, key recovery, and customer support. The enterprise gateway administrator handles approval, enrollment, validation, issuance, and renewal of digital certificates.

For more details, refer to Appendix C, “Configuring VeriSign Digital Certificates.”

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.

Function of Digital Certification

The digital certification feature requires that each IPSec peer has its own digital certificate, which is issued and validated by the certification authority (CA). To authenticate itself to the gateway, the client sends a certificate that performs public key cryptography with the gateway. Each peer's certificate encapsulates that peer's public key, each certificate is authenticated by the CA, and all participating IPSec peers recognize the CA as an authenticating authority. This is called IKE with an RSA signature.

Essentially, the steps to signing on with a CA are as follows:

1. The VPN Client must generate a public/private key pair for the CA to sign. The VPN Client first signs outbound data with its private key. Then, the CA uses the VPN Client's public key to validate that this data was originated by the VPN Client.
2. The VPN Client requests the CA's public key. Only after the VPN Client has the CA's public key can the VPN Client validate data coming from the CA.
3. The VPN Client sends an enrollment request to the CA. The CA ties the VPN Client's personal certificate to its public key, then signs the personal certificate.
4. The VPN Client accepts the signed personal certificate. The VPN Client validates this certificate by decrypting the signed personal certificate with its private key.

Benefits of Digital Certification

Because each VPN Client and each router has its own digital certificate and authentication is handled by the CA, a network is more scalable and provides a more secure authentication with digital certificates than with pre-shared keys or wildcard pre-shared keys. With digital certification, you can configure unlimited numbers of VPN Clients without having to change the gateway configuration.

Limitations and Restrictions of Digital Certification

To prevent attacks to one or more parties using digital certification, the following instructions should be a part of your enterprise security policy:

- An IPSec peer can send its own certificate for multiple IPSec sessions with multiple IPSec peers.
- When an IPSec peer's certificate expires periodically, the gateway administrator *must* obtain new digital certificates from the CAs, and reconfigure the devices with these new digital certificates.
- The gateway administrator *must* ensure that all digital certificates obtained are interoperable with all the devices in the network.

Alternatives to Digital Certification

Without a method of client authentication, you cannot establish an encrypted tunnel between a client and gateway. Digital certification and pre-shared keys are the alternative to wildcard pre-shared keys.

Building an Access VPN

This section covers the following topics:

- Enterprise Network Equipment
- Enterprise Access VPN Description
- Protocol Negotiation Sequence

Enterprise Network Equipment

Figure 2-2 shows the specific network devices used by the enterprise to build the access VPN in this case study.

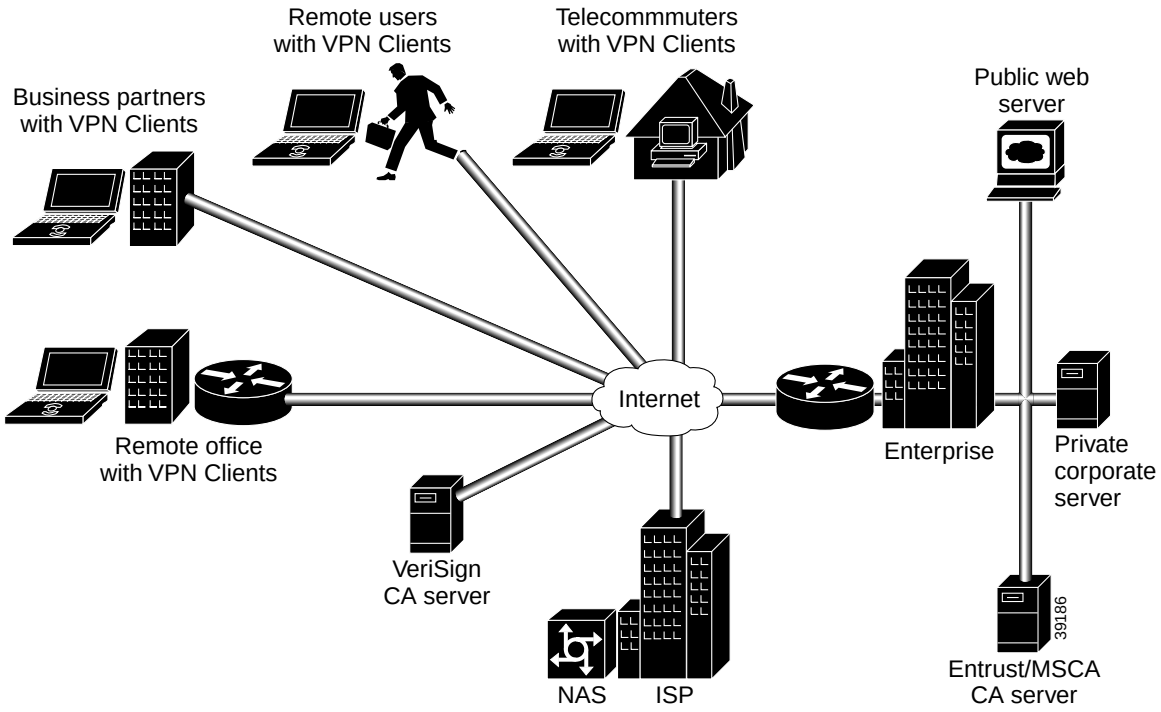
- The VPN Client software, which the network administrator may preconfigure with a one-time-only static IP address or set up to be configured on-the-fly with a dynamic IP address.
- A home gateway (such as a Cisco IOS router or a Cisco Secure PIX Firewall) configured with an IPSec software image from a supported Cisco IOS software release.
- A public web server and a private corporate server.

Enterprise Access VPN Description

The VPN Clients initiate the IPSec tunnels by requesting authentication with the IPSec peer, the home gateway. Once the home gateway authenticates the connection, the VPN Clients establish an encrypted tunnel to the home gateway. To route authorized traffic to its specified destination, an access-list is set up on the home gateway to permit or deny traffic into different subnets on the corporate network:

- For corporate employees, access to permitted for the private corporate server, where they may access confidential data remotely. Corporate employees may also view information on the public web server.
- For extranet partners, access is limited to a public web server, where they perform various IP-based network tasks, such as placing and managing product orders. Business partner access to all private internal corporate servers is denied.

Figure 2-2 Access VPN Case Study Network Topology



Protocol Negotiation Sequence

Figure 2-3 shows the protocol negotiation sequence between one VPN Client and a gateway. Table 2-1 describes the events displayed in this protocol negotiation sequence.

Note Although you may not have all encryption features configured for your VPN, Figure 2-3 shows the period during IKE negotiation during which each feature performs its task.

Figure 2-3 Protocol Negotiation Sequence—Client-Initiated Access VPN

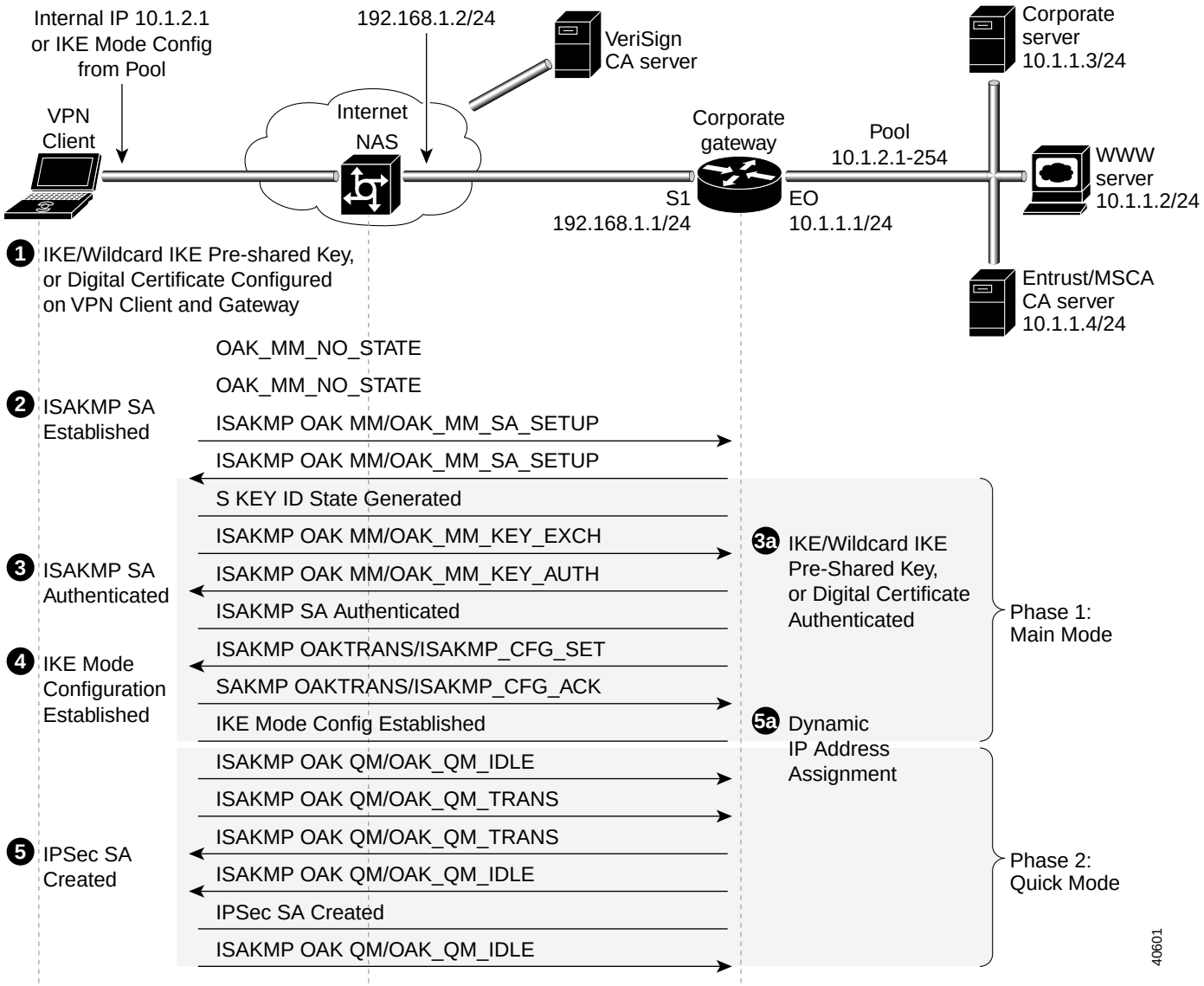


Table 2-1 Access VPN Events - Client-Initiated

Event	Description of Cisco Secure VPN Client	Description of NAS and Gateway
1.	To configure VPN access for remote corporate employees, the gateway administrator performs the following tasks: • Either configures a static IP address on the each VPN Client manually, or configures the home gateway to initiate IKE Mode Configuration with the VPN Clients. • Either configures pre-shared keys, wildcard pre-shared key, or digital certification for the VPN Clients' authentication method. Result: A method of assigning internal corporate IP addresses is assigned to each VPN Client.	To configure VPN access for remote corporate employees, the gateway administrator ensures the static IP address configured on the VPN Client is within the IP range of the corporate subnet. The gateway administrator also performs the following tasks: • Either configures a static IP address on the each VPN Client manually, or configures the home gateway to initiate IKE Mode Configuration with the VPN Clients. • Either selects pre-shared keys, wildcard pre-shared key, or digital certification for the VPN Clients' authentication method. Result: A method of assigning internal corporate IP addresses is assigned to each VPN Client.
2.	To start IKE negotiations, the VPN Client sends attributes including KE (Diffie-Hellman keys) and NON (non-repudiation) to the gateway during the first part of ISAKMP OAK MM state. **Note** Diffie-Hellman keys are shared with the gateway during the first part of ISAKMP OAK MM, and are exchanged during the second part of ISAKMP OAK MM state. Result: ISAKMP SA is created.	To start IKE negotiations, the VPN Client establishes ISAKMP SA with the gateway in the OAK_MM_SA_SETUP state. Setting up ISAKMP SA is the first part of Phase 1, Main Mode in IKE negotiation. Result: ISAKMP SA is created.
3.	To authenticate ISAKMP SA, the VPN Client sends attributes including predefined attributes and a CERT_REQ (certificate request) and VID (vendor identification of the certificate authority) to the gateway during the second part of ISAKMP OAK MM state. Result: ISAKMP SA is authenticated.	To authenticate ISAKMP SA, the VPN Client and the gateway participate in a Diffie-Hellman key exchange, OAK_MM_KEY_EXCH, to exchange public keys. Using either digital certificates or pre-shared keys, the gateway authenticates the VPN Client during the OAK_MM_KEY_AUTH state. Authentication of ISAKMP SA is the second part of Phase 1, Main Mode in IKE negotiation. Result: ISAKMP SA is authenticated.

Table 2-1 Access VPN Events - Client-Initiated (continued)

Event	Description of Cisco Secure VPN Client (continued)	Description of NAS and Gateway (continued)
4.	To get a dynamically-assigned IP address from the enterprise, the VPN Client receives the dynamic IP address from the pool of IP addresses on the gateway during the ISAKMP OAK TRANS state, which occurs during the ISAKMP OAK QM state. Result: IKE Mode Configuration occurs.	To get a dynamically-assigned IP address from the enterprise, the gateway transparently assigns the VPN Client a dynamic IP address from a pool of IP addresses during the ISAKMP_CFG_SET state. Then, the gateway receives an acknowledgement of having received the IP address from the VPN Client during the ISAKMP_CFG_ACK state. Result: IKE Mode Configuration occurs.
5.	To finish IKE negotiations, the VPN Client loads the IPSec SA from the gateway during the ISAKMP OAK QM state. Result: IPSec SA is established.	To finish IKE negotiations, the VPN Client establishes the idle Quick Mode state (OAK_QM_IDLE) with the gateway. The VPN Client's internal attributes define the IPSec SA to be transmitted to the gateway during the OAK_QM_TRANS state. The IPSec SA from the VPN Client is authenticated with the gateway and may be used for subsequent Quick Mode exchanges. Result: IPSec SA is established.

Site Profile Characteristics

Table 2-2 Hardware and Software Used in This Case Study

	Clients (Remote Access)	Gateway (Enterprise)
Chassis Type	*One* of the following computers, with Pentium processor or equivalent: • Desktop PC • Laptop	For hardware information on interoperable networking devices, see the following: • "Networking Devices with IP Security Protocol" section in Chapter 1, "Access VPNs and IP Security Protocol Tunneling Technology Overview." • "Platform-Specific Documents" section in the "Preface" of this guide. • For supported hardware version or Cisco IOS software release, see the related release notes in the "Cisco Secure VPN Client Documentation" section in the "Preface" of this guide.
Hardware	For required hardware on the computer, see the "Cisco Secure VPN Client Documentation" section in the "Preface" of this guide. **Note** This information is available in the "System Requirements" section of your VPN Client release notes.	**Note** This information is available in the "Network Requirements" section of your VPN Client release notes.

Table 2-2 Hardware and Software Used in This Case Study (continued)

	Clients (Remote Access) (continued)	Gateway (Enterprise) (continued)
Software	*One* of the following clients: • Cisco Secure VPN Client Version 1.0 • Cisco Secure VPN Client Version 1.1 For supported operating systems, see the "Cisco Secure VPN Client Documentation" section in the "Preface" of this guide. This information is available in the "System Requirements" section of the VPN Client release notes.	An IPSec software image from a supported Cisco IOS release. For supported Cisco IOS releases, see the related release notes in "Cisco Secure VPN Client Documentation" section in the "Preface" of this guide. This information is available in the "Network Requirements" section of the VPN Client release notes.
Memory	For memory requirements, see the "Cisco Secure VPN Client Documentation" section in the "Preface" of this guide. This information is available in the "System Requirements" section of the VPN Client release notes.	For memory on hardware devices, see "Platform-Specific Documents" section in the "Preface" of this guide. This information is usually available in the "Overview" chapter of the hardware installation guide for your hardware networking device.
Ethernet IP Address **Note** These sample IP addresses and keys are used throughout this guide. Be sure to use your own IP addresses and key when configuring your network.	Internal IP Address on VPN Client or IKE Mode Config Dynamically-Assigned Address: 10.1.2.1 255.255.255.0 Pre-shared Secret: cisco1234	Outside S/1 interface: 192.168.1.1 255.255.255.0 Inside E/0 interface: 10.1.1.1 255.255.255.0 Corporate Subnet: 10.1.1.0 255.255.255.0 Pre-shared secret: cisco1234
Protocol	Native Microsoft TCP/IP, IPSec Security Protocol	IPSec Security Protocol

CHAPTER 3

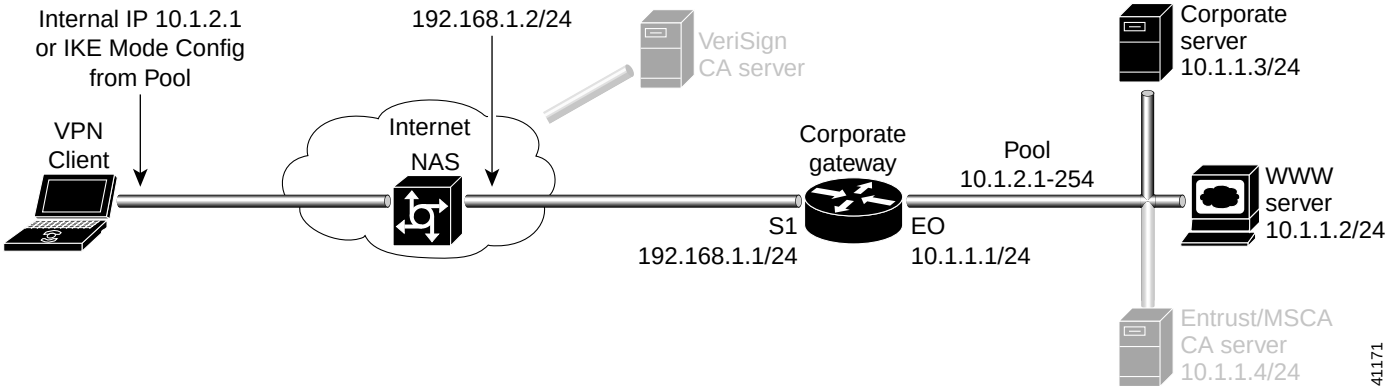
Configuring Manual Configuration

This chapter describes how to manually configure internal corporate IP addresses on a Cisco Secure VPN Client (VPN Client). With manual configuration, you can assign a static, internal IP address to a client, making it easier to administer IP Security Protocol (IPSec) policy from the Cisco router (gateway) to the VPN Client.This chapter includes the following sections:

- Task 1—Configuring Manual Configuration on the VPN Client
- Task 2—Configuring Manual Configuration on the Gateway
- Related Documentation

Note Throughout this chapter, there are numerous configuration examples that include unusable IP addresses, passwords, and public key examples. Be sure to use your own IP addresses, passwords, and public keys when configuring your VPN Clients and gateway.

Figure 3-1 Manual Configuration Topology



Task 1—Configuring Manual Configuration on the VPN Client

To configure manual configuration between a VPN Client and a Cisco router, perform the following tasks:

- Specifying an Internal Network Address on the VPN Client
- Configuring New Gateway for Security Policy
- Specifying the VPN Client's Identity

Specifying an Internal Network Address on the VPN Client

To specify an internal network address on a VPN Client, perform the following tasks:

- Open the Security Policy Editor
- Open and Define Global Policy Settings

To open the Security Policy Editor

Click **Start>Programs>Cisco Secure VPN Client>Security Policy Editor**.

The SafeNet/Soft-PK Security Policy Editor window appears, as shown in Figure 3-2. Table 3-2 describes the field descriptions for the SafeNet/Soft-PK Security Policy Editor.

Figure 3-2 SafeNet/Soft-PK Security Policy Editor

Table 3-1 SafeNet/Soft-PK Security Policy Editor Window Field Descriptions

Field	Description
Security Policy Editor	This window establishes connections and their associated proposals, and lists connections in a hierarchical order that defines an IP data communications security policy.
Other Connections	This object is a policy, or a default connection, and the first step in establishing security policies for individual connections.
Connection Security	Under Connection Security, you can define IP access for this connection using Secure, Non-secure, and Block options.
• Secure	• This option secures the IP communications for this connection.
• Non-secure	• This option allows for IP communications to occur without encryption, and allows you to change any settings under your Internet Interface. This is the default.
• Block	• This option denies all IP communications to the VPN Client.

To open and define Global Policy Settings

Step 1 On the **Options** menu, click **Global Policy Settings**.

The Global Policy Settings window appears, as shown in Figure 3-3. Table 3-2 describes the field descriptions for the Global Policy Settings window.

Step 2 Select the **Allow to Specify Internal Network Address** check box, and then click **OK**.

Figure 3-3 Global Policy Settings Window

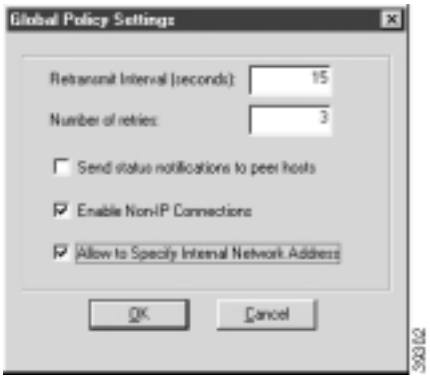


Table 3-2 Global Policy Settings Window Field Descriptions

Field	Description
Global Policy Settings	Using this window, set preferences for all transmissions.
Retransmit Interval (seconds)	In this box, specify the amount of time your computer waits before it retransmits a protocol packet to which a device has not responded. The default interval is 15 seconds.
Number of retries	In this box, specify the number of times your computer retransmits a protocol packet before abandoning the exchange. The default is 3 retries.
Send status notifications to peer hosts	If selected, this check box sends messages that inform communicating parties whether their security proposals have been accepted or rejected, and the timeout periods.
Enable Non-IP Connections	If selected, this option allows your computer to transmit non-IP data without security. As a default, the VPN Client secures IP data and discards all non-IP data.
Allow to Specify Internal Network Address	If selected, this option allows you to enter the exact IP address under My Identity. An internal network address is the actual IP address for the VPN Client behind a network firewall. Use this option to specify that you want to indicate an internal network address. This allows you to enter the IP address in the Network Security Policy window under My Identity in the Internal Network IP Address box.

Configuring New Gateway for Security Policy

To configure a new gateway for a security policy on a VPN Client, perform the following tasks:

- Create a New Connection
- Define the New Connection

To create a new connection

Step 1 In the left pane, click **Other Connections**.

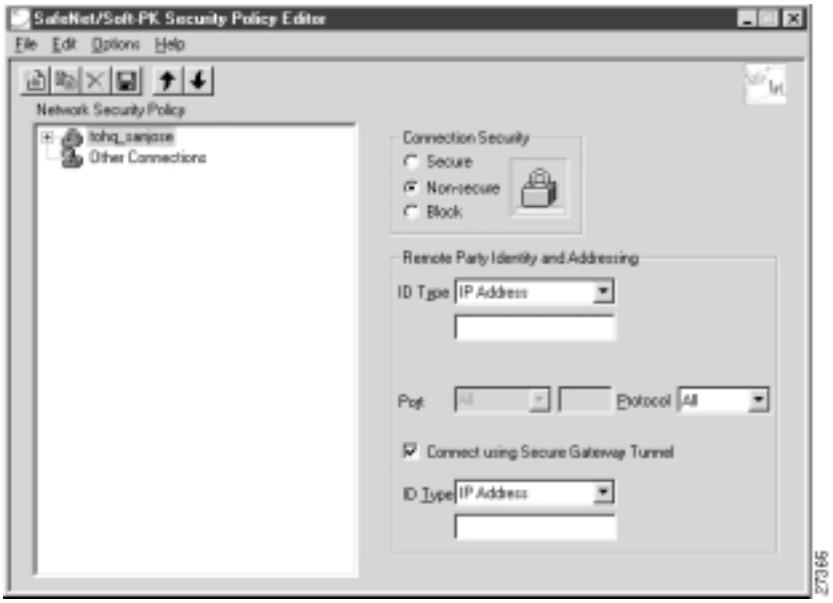
Step 2 On the **File** menu, click **New Connection**.

Step 3 In the left pane, the default **New Connection** placeholder appears for the New Connection pane.

Step 4 Select **New Connection**, and in its place, define a unique name for the connection to your gateway.

For example, if your router name is `hq_sanjose`, you might rename the connection **`tohq_sanjose`**, as shown in Figure 3-4. Table 3-3 describes the field descriptions for the New Connection pane.

Figure 3-4 Renaming a New Connection Pane



To define the new connection

Step 1 In the left pane, click your new connection. In this example, **tohq_sanjose** is clicked.

The new connection pane appears.

Step 2 In the right pane, under Connection Security, click **Secure**.

Step 3 In the right pane, under Remote Party Identity and Addressing, enter the following:

a. In the ID Type list, click **IP Subnet**.

b. In the Subnet box, enter the IP address of your corporate subnet. In this example, the IP address of the corporate subnet, **10.1.1.0** is entered.

c. In the Mask box, enter the subnet mask of the IP address of your corporate subnet. In this example, the subnet mask of the corporate subnet, **255.255.255.0** is entered.

d. The Port list and box are inactive as a default. In the Protocol list, click **All**.

e. Select the **Connect using Secure Gateway Tunnel** check box.

f. In the ID_Type list, click **IP Address**. In the ID_Type box, enter the IP address of the secure gateway. In this example the secure gateway, **192.168.1.1** is entered.

Figure 3-5 shows how this is displayed on the New Connection pane. Table 3-3 describes the field descriptions for the New Connection pane.

Figure 3-5 New Connection Pane

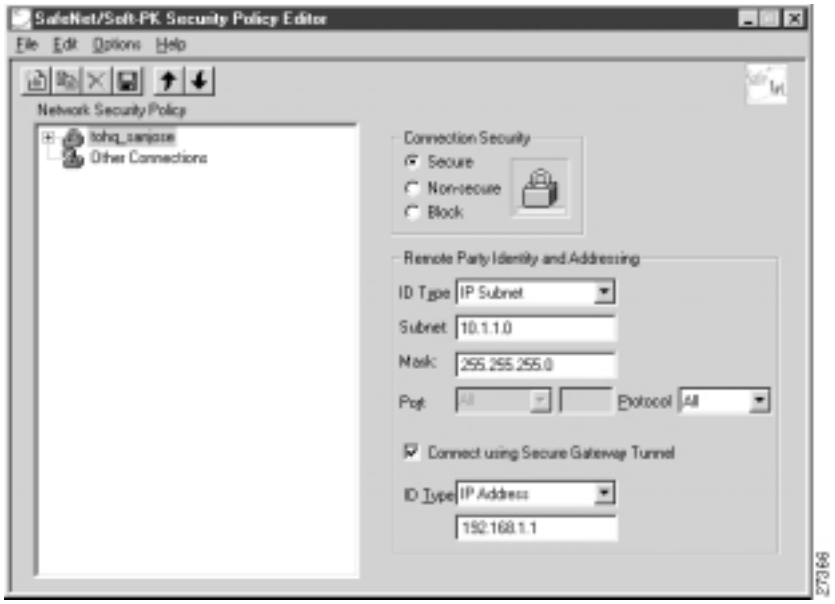


Table 3-3 New Connection Pane Field Descriptions

Field	Description
Network Security Policy	Under Network Security Policy, the proposals that will be used to negotiate the authentication and encryption methods are displayed.
• New Connection	• This object is a set of security parameters that pertain to an individual remote IP connection. *New Connection* is the default connection name.
• Other Connections	• This object is the default connection and 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. Other Connections is always the last rule among security policies.
Connection Security	Under Connection Security, you can define IP access for this connection.
• Secure	• This option secures the IP communications for this connection.
• Non-secure	• This option allows for IP communications to occur without encryption, and you to change any settings under your Internet Interface. This is the default.
• Block	• This option denies all IP communications to the VPN Client.
Remote Party Identity and Addressing	Under Remote Party Identity and Addressing, define the IPSec peer with which the VPN Client will establish a secure tunnel.

Table 3-3 New Connection Pane Field Descriptions (continued)

Field	Description
ID Type	This list displays options for defining the IPSec peer identity including IP address, domain name, email address, IP subnet, IP address range, and distinguished name. Depending on the option you choose, different values will appear in the right pane.
• IP Address	• This option allows a static IP address to be configured on the VPN Client. This is the default option.
– IP address value	– In this box, specify the IP address value.
• Domain Name	• This option enables the domain name value box and the IP Address box.
– Domain name value	– In this box, specify the domain name value.
– IP Address	– In this box, specify the IP address of the domain, the organizational IP address.
• Email Address	• This option allows you to indicate the email address of the peer.
– Email value	– In this box, specify the e-mail value.
– IP address value	– In this box, specify the peer's IP address.
• IP Subnet	• This option allows you to specify the IP subnet the client will be allowed to access using this peer.
– Subnet	– In this box, specify the subnet IP address.
– Mask	– In this box, specify the mask IP address.
• IP Address Range	• This option allows you to indicate the range of IP addresses to which this client will have access.
– From	– In this box, specify the beginning IP address.
– To	– In this box, specify the ending IP address.
• Distinguished Name	• This option allows you to specify the name, department, state, and country of the peer identity.
– Edit Name	– Using this button, specify the distinguished name settings.
– IP Address	– In this box, specify the peer's IP address.
Port	This list shows the IPSec peer's protocol ports. A default of *All* secures all protocol ports.
Connect using Secure Gateway Tunnel	If selected, this check box specifies that the IPSec peer is protected by a secure IPSec-compliant gateway, such as a firewall.

Table 3-3 New Connection Pane Field Descriptions (continued)

Field	Description
ID_Type	This list shows the identification type of the gateway including IP address, domain name, and distinguished name. Depending on the option you choose, different values will appear in the right pane.
• IP Address	• This option enables the IP address value box. This is the default.
– IP address value	– In this box, specify the IP address value.
• Domain Name	• This option enables the domain name value box and the IP Address box.
– Domain name value	– In this box, specify the domain name value.
– IP Address	– In this box, specify the IP address of the domain.
• Distinguished Name	• This option allows you to specify the name, department, state, and country of the gateway.
– Edit Name	– Using this button, specify the distinguished name settings.
– IP Address	– In this box, specify the gateway's IP address.

Specifying the VPN Client's Identity

To specify the remote party's identity on a VPN Client, perform the following tasks:

- Choose an Identity
- Specify Authentication

To choose an identity

Step 1 In the left pane, double-click the new connection. In this example, **tohq_sanjose** is double-clicked.

The new connection expands with My Identity and Security Policy.

Step 2 Click **My Identity**.

The My Identity pane appears in the right pane.

Step 3 In the right pane, under My Identity, enter the following:

a. If you are using digital certificates, select your digital certificate in the Select Certificate list. If you are not using digital certificates, then leave this field as-is.

b. In the ID_Type list, click **IP Address**.

c. In the Internal Network IP Address box enter VPN Client static IP address. In this example, **10.1.2.1** is entered.

d. In the Port list, click **All**.

e. In the Name list, click **Any**. The IP Addr list is inactive as a default.

f. If you are using pre-shared keys, click **Pre-shared**. Enter the key to be used during the Authentication Phase. Click **OK** when done. If you are not using pre-shared keys, then leave this field as-is.

Figure 3-6 shows how this is displayed on the My Identity pane. Table 3-4 describes the field descriptions for the My Identity pane.

Figure 3-6 My Identity Pane

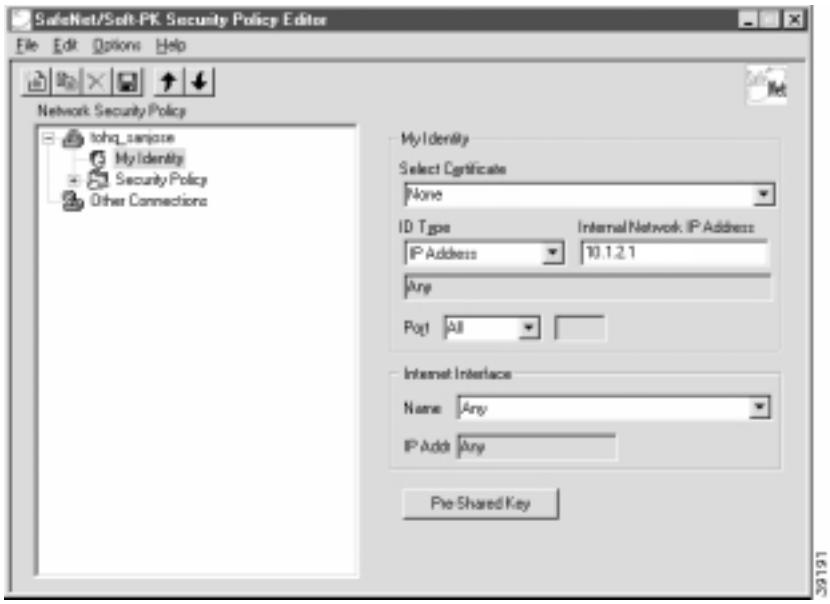


Table 3-4 My Identity Pane Field Descriptions

Field	Description
My Identity	This pane allows you to specify the identity of the VPN Client. Choose an identification that will allow the IPSec peer to identify you during the key exchange phase in the My Identity pane.
My Identity	Under My Identity, specify options for determining the identity of the VPN Client. These options include selecting certificate or pre-shared key, ID Type, and Port.
Select Certificate	If you are using digital certification, this list displays all the available digital certificates from which to choose. If you are not using digital certification, *None* is the default option.
ID_Type	This list indicates the IP address option for the VPN Client on the corporate subnet.
• IP Address – Internal Network IP Address	• This option enables the IP address value box. – In this box, specify the IP address of the VPN Client on the corporate subnet. This field only appears if you specify an internal IP address in the Global Policy Settings window.
Port	This list shows the VPN Client's protocol ports. A default of *All* secures all protocol ports.

Table 3-4 My Identity Pane Field Descriptions (continued)

Field	Description
Local Network Interface or Internet Interface	Under Local Network Interface or Internet Interface, the hardware interface on the PC or laptop through which the connection will be established.
Name	This list indicates the name of the hardware interface. A default of *Any* enables all hardware interfaces.
IP Addr	A default of *Any* enables all hardware interface IP addresses.
Pre-shared Key	The Pre-shared Key button enables the Pre-shared Key window. To specify a pre-shared key or a wildcard pre-shared key, enter the key to be used during the Authentication Phase in the Pre-shared Key window.

To specify authentication

- To configure authentication on a VPN Client using pre-shared key or wildcard pre-shared key, see "Task 2—Configuring a Pre-Shared Key or Wildcard Pre-Shared Key on the Gateway" in Chapter 5, "Configuring a Pre-Shared Key or Wildcard Pre-Shared Key."
- To configure authentication on a VPN Client using digital certification, see "Task 2—Configuring Digital Certification on the Gateway" in Chapter 6, "Configuring Digital Certification."

Task 2—Configuring Manual Configuration on the Gateway

To configure manual configuration on the gateway, perform the following tasks:

- Configuring the Gateway
- Defining an IPSec Transform Set
- Defining a Dynamic Crypto Map
- Defining a Static Crypto Map

Configuring the Gateway

To configure the gateway, perform the following tasks, as described in Table 3-5:

- Configure the Gateway
- Define a Host Name
- Define a Name Server

Table 3-5 Configuring the Gateway

Command	Purpose
`router> enable`	To enter privileged EXEC mode, enter the **enable** user EXEC command.

`router# configure terminal`
`Enter configuration commands, one per line.`
`End with CNTL/Z.`
	To enter global configuration mode, enter the **configure** privileged EXEC command. To configure the terminal attached at console port, enter the **terminal** keyword.

`router(config)# ip domain-name example.com`	To define a default domain name that the Cisco IOS software uses to complete unqualified host names, use the **ip domain-name** global configuration command. An unqualified host name is a host name without a dotted-decimal domain name. In this example, *example.com* is defined as the default domain name.
`router(config)# hostname hq_sanjose`	To specify or modify the host name for the network server, enter the **hostname** global configuration command. The host name is used in prompts and default configuration filenames. In this example, *hq_sanjose* is defined as the host name. The *hq_sanjose* host name replaces the default *router* host name.
`hq_sanjose(config)# ip name-server 192.168.1.1`	To specify the address of a name server to use for name and address resolution, enter the **ip name-server** global configuration command. In this example, the gateway is defined as the *IP name server.* The gateway's IP address is *192.168.1.1*.

Defining an IPSec Transform Set

To define an IPSec transform set on the gateway, perform the following tasks, as described in Table 3-6:

- Define IPSec Negotiation Security Associations
- Specify IPSec Encapsulation Method

Table 3-6 Defining an IPSec Transform Set

Command	Purpose
`hq-sanjose(config)# crypto ipsec transform-set vpn-transform esp-des ah-md5-hmac`	To define a combination of security associations to occur during IPSec negotiations, enter the **crypto ipsec transform-set** global configuration command. This command invokes the crypto transform (cfg-crypto-trans) configuration mode. In this example, the transform set named *vpn-transform* is defined with two security algorithm keywords: **esp-des** and **ah-md5-hmac**. **Note** There are complex rules defining which entries you can use for the transform arguments. These rules are explained in the command description for the **crypto ipsec transform-set** command. You can also use the **crypto ipsec transform-set** global configuration command to view the available transform arguments.
`hq-sanjose(cfg-crypto-trans)# mode tunnel`	To specify IPSec encapsulation between the gateway and the VPN Client, enter the **mode** crypto transform configuration command. The **mode** command is only applicable to traffic whose source and destination addresses are the IPSec peer addresses; it is ignored for all other traffic. (All other traffic is in tunnel mode only.) In this example, the **tunnel** mode is configured for *vpn-transform* for an IPSec encrypted tunnel.
`hq-sanjose(cfg-crypto-trans)# exit`	To exit crypto transform (cfg-crypto-trans) configuration mode, enter the **exit** crypto transform configuration command.

Defining a Dynamic Crypto Map

To define a dynamic crypto map, perform the following tasks, as described in Table 3-7:

- Define a Dynamic Crypto Map Entry
- Specify an IPSec Transform Set
- Define an Extended Access List
- Specify the IPSec Peer

Table 3-7 Defining a Dynamic Crypto Map

Command	Purpose
`hq_sanjose(config)# crypto dynamic-map vpn-dynamic 1`	To define a dynamic crypto map entry, enter the **crypto dynamic-map** command. This command invokes the crypto map (config-crypto-map) configuration mode. In this example, the dynamic map name is *vpn-dynamic*, and the sequence number (or priority) is *1*.
`hq_sanjose(config-crypto-map)# set transform-set vpn-transform`	To specify which transform sets are allowed for the crypto map entry, enter the **set transform-set** crypto map configuration command. In this example, the transform set previously defined in "Defining an IPSec Transform Set," *vpn-transform* is applied to the *vpn-dynamic* dynamic crypto map. **Note** You can list multiple transform sets in order of priority (highest priority first).
`hq_sanjose(config-crypto-map)# match address 101`	To specify an extended access list for a crypto map entry, enter the **match address** crypto map configuration command. This access list determines which traffic should or should not be protected by IPSec. If this is configured, the data flow identity proposed by the IPSec peer must fall within a permit statement for this crypto access list. If this is not configured, the router will accept any data flow identity proposed by the IPSec peer. However, if this is configured but the specified access list does not exist or is empty, the router will drop all packets.
`hq_sanjose(config-crypto-map)# exit`	To exit crypto map (config-crypto-map) configuration mode, enter the **exit** crypto map configuration command.

Defining a Static Crypto Map

To define a static crypto map, perform the following tasks, as described in Table 3-8:

- Define a Static Crypto Map Entry
- Add a Dynamic Crypto Map to the Static Crypto Map
- Define an Access List for VPN Client
- Apply the Crypto Map to the Gateway Interface

Table 3-8 Defining a Static Crypto Map

Command	Purpose
`hq_sanjose(config)# crypto map vpnclient 1 ipsec-isakmp vpn-dynamic`	To define a static crypto map and add a dynamic crypto map set to a static crypto map set, enter the **crypto map** global configuration command. In this example, the *vpn-dynamic* dynamic map (child) is applied to the *vpnclient* static crypto (parent) map.
`hq_sanjose(config)# access-list 101 permit ip 192.168.1.1 255.255.255.0 host 10.1.2.1`	To permit all IP traffic between the host and the gateway, use the extended version of the **access-list** global configuration command. **Note** An access-list must be configured for each VPN Client configured with static IP addresses on a corporate subnet. All IP traffic is permitted between the two IPSec peers.
`hq_sanjose(config)# crypto map vpn-dynamic local-address loopback0`	To specify and name an identifying interface to be used by the dynamic crypto map for IPSec traffic, use the **crypto map local-address** global configuration command. In this example, the address that the IPSec will use on the gateway interfaces is **loopback0**. The **loopback0** interface is specified as the local IP address for encryption on the gateway.

Related Documentation

For more information on manual configuration, refer to the “Manual Configuration (Static IP Addressing)” section in Chapter 2, “Case Study for Layer 3 Authentication and Encryption.”

For more information on configuring Cisco IOS software commands, refer to the “Cisco IOS Software Documentation Set” section in the “Preface.”

CHAPTER 4

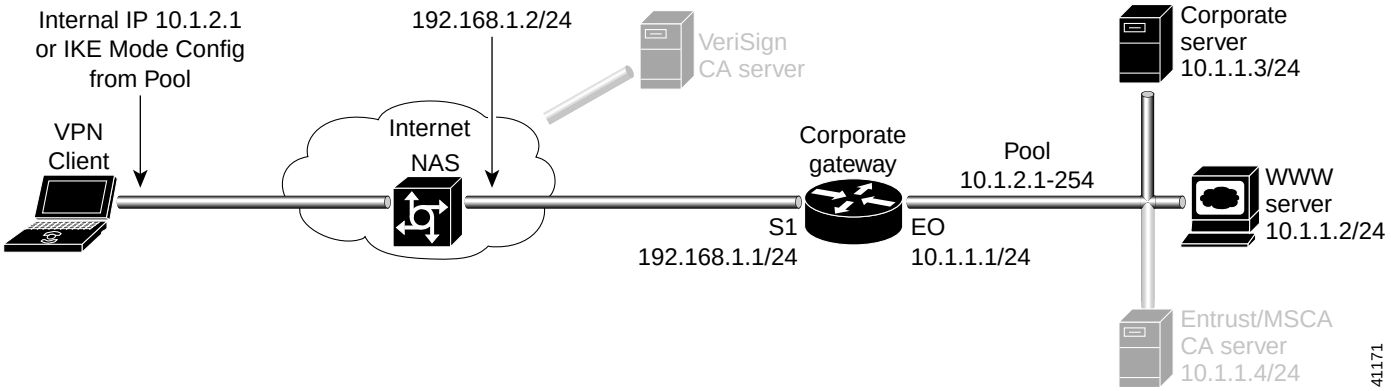
Configuring Dynamic IP Addressing

This chapter describes how to configure IP addresses on multiple remote Cisco Secure VPN Clients (VPN Clients) using Internet Key Exchange Mode Configration (IKE Mode Configuration). With IKE Mode Configuration, you can set up Virtual Private Networks (VPNs) with dynamic IP addressing from a Cisco router (gateway) to multiple VPN Clients for scalable IP Security Protocol (IPSec) policy. You can use IKE mode configuration to replace static or dynamic IP address on VPN Clients. This chapter contains the following sections:

- Task 1—Configuring Dynamic IP Addressing on the VPN Client
- Task 2—Configuring Dynamic IP Addressing on the Gateway
- Related Documentation

Note Throughout this chapter, there are numerous configuration examples that include unusable IP addresses, passwords, and public key examples. Be sure to use your own IP addresses, passwords, and public keys when configuring your VPN Clients and gateway.

Figure 4-1 Dynamic IP Addressing Topology



Task 1—Configuring Dynamic IP Addressing on the VPN Client

To configure IKE Mode Configuration on the VPN Client, you must specify an internal network address on the VPN Client. To do this, you must follow "Specifying an Internal Network Address on the VPN Client" in Chapter 3, "Configuring Manual Configuration."

IKE Mode configuration is enabled by default on the VPN Client.

Task 2—Configuring Dynamic IP Addressing on the Gateway

To configure the gateway, perform the following tasks:

- Configuring the Gateway
- Defining an IPSec Transform Set
- Defining a Dynamic Crypto Map
- Defining the VPN Clients' IP Address Pool
- Defining a Static Crypto Map

Configuring the Gateway

To configure the gateway, perform the following tasks, as described in Table 4-1:

- Configure the Gateway
- Define a Host Name
- Define the Name Server

Table 4-1 Configuring the Gateway

Command	Purpose
`router> enable`	To enter privileged EXEC mode, enter the **enable** user EXEC command.

`router# configure terminal`
`Enter configuration commands, one per line.`
`End with CNTL/Z.`
	To enter global configuration mode, enter the **configure** privileged EXEC command. To configure the terminal attached at console port, enter the **terminal** keyword.

`router(config)# ip domain-name example.com`	To define a default domain name that the Cisco IOS software uses to complete unqualified host names, use the **ip domain-name** global configuration command. An unqualified host name is a host name without a dotted-decimal domain name. In this example, *example.com* is defined as the default domain name.
`router(config)# hostname hq_sanjose`	To specify or modify the host name for the network server, enter the **hostname** global configuration command. The host name is used in prompts and default configuration filenames. In this example, *hq_sanjose* is defined as the host name. The *hq_sanjose* host name replaces the default *router* host name.

Defining an IPSec Transform Set

To define IPSec transform set on the gateway, perform the following tasks, as described in Table 4-2:

- Define IPSec Negotiation Security Associations
- Specify IPSec Encapsulation Method

Table 4-2 Defining an IPSec Transform Set

Command	Purpose
`hq-sanjose(config)# crypto ipsec transform-set vpn-transform esp-des ah-md5-hmac`	To define a combination of security associations to occur during IPSec negotiations and enter crypto transform configuration mode, enter the **crypto ipsec transform-set** global configuration command. In this example, the transform set named *vpn-transform* is defined with two security algorithms: **esp-des** and **ah-md5-hmac**. **Note** There are complex rules defining which entries you can use for the transform arguments. These rules are explained in the command description for the **crypto ipsec transform-set** command. You can also use the **crypto ipsec transform-set** global configuration command to view the available transform arguments.
`hq-sanjose(cfg-crypto-trans)# mode tunnel`	To specify IPSec encapsulation between the gateway and the VPN Client, enter the **mode** crypto transform configuration command. The **mode** command is only applicable to traffic whose source and destination addresses are the IPSec peer addresses; it is ignored for all other traffic. (All other traffic is in tunnel mode only.) In this example, *tunnel* mode is configured for *vpn-transform* for an IPSec encrypted tunnel.
`hq-sanjose(cfg-crypto-trans)# exit`	To exit crypto map configuration mode, enter the **exit** crypto transform configuration command.

Defining a Dynamic Crypto Map

To define a dynamic crypto map, perform the following tasks, as described in Table 4-3:

- Define a Dynamic Crypto Map Entry
- Specify an IPSec Transform Set
- Define an Extended Access List
- Specify the IPSec Peer

Table 4-3 Defining a Dynamic Crypto Map

Command	Purpose
`hq_sanjose(config)# crypto dynamic-map vpn-dynamic 1`	To define a dynamic crypto map entry and enter the crypto map configuration mode, enter the **crypto dynamic-map** command. In this example, the dynamic map name is *vpn-dynamic*, and the sequence number (or priority) is *1*.
`hq_sanjose(config-crypto-map)# set transform-set vpn-transform`	To specify which transform sets are allowed for the crypto map entry, enter the **set transform-set** crypto map configuration command. In this example, the transform set previously defined in Defining an IPSec Transform Set, *vpn-transform* is applied to the *vpn-dynamic* dynamic crypto map. **Note** You can list multiple transform sets in order of priority (highest priority first).
`hq_sanjose(config-crypto-map)# match address 101`	To specify an extended access list for a crypto map entry, enter the **match address** crypto map configuration command. This access list determines which traffic should be protected by IPSec and which traffic should not be protected by IPSec. If this is configured, the data flow identity proposed by the IPSec peer must fall within a permit statement for this crypto access list. If this is not configured, the router will accept any data flow identity proposed by the IPSec peer. However, if this is configured but the specified access list does not exist or is empty, the router will drop all packets.
`hq_sanjose(config-crypto-map)# exit`	To exit crypto map configuration mode, enter the **exit** crypto map configuration command.

Defining the VPN Clients' IP Address Pool

To define the VPN Clients' IP address pool, perform the following tasks, as described in Table 4-4:

- Define the VPN Client's Local IP Address Pool
- Reference the Local IP Address Pool to Reference IKE
- Specify Gateway-initiated IKE Mode Configuration

Table 4-4 Defining the VPN Clients' IP Address Pool

Command	Purpose
`hq_sanjose(config)# ip local pool vpn-pool 10.1.2.1-10.1.2.254`	To define a local IP address pool for VPN Clients, enter the **ip local pool** command. You can use existing local address pools to define a set of addresses. The IP address pool must be within the IP range of the corporate subnet. In this example, the pool name is *vpn-pool*. This IP address pool has a range from *10.1.2.1—10.1.2.254*. The local address pool for VPN Clients is defined.
`hq_sanjose(config)# crypto isakmp client configuration address-pool local vpn-pool`	To configure the local IP address pool for VPN Clients to reference IKE on your router, use the **crypto isakmp client configuration address-pool local** global configuration command. In this example, the pool name is *vpn-pool*. The IP address pool for VPN Clients is set to reference IKE on your router.
`hq_sanjose(config)# crypto map vpnclient client configuration address initiate`	To configure IKE Mode Configuration on the static crypto map, use the **crypto map client configuration address** global configuration command. In this example, the crypto map is *vpnclient*. To indicate that IKE Mode Configuration is to be gateway-initiated, use the **initiate** keyword. **Note** Cisco supports gateway-initiated IKE Mode Configuration only. Client-initiated IKE Mode Configuration is not currently supported. A crypto map is defined for gateway-initiated IKE Mode Configuration.
`hq_sanjose(config)# exit`	To exit global configuration mode, enter the **exit** global configuration command.

Defining a Static Crypto Map

To define a static crypto map, perform the following tasks, as described in Table 4-5:

- Defining a Static Crypto Map
- Add a Dynamic Crypto Map to the Static Crypto Map
- Define an Access List for VPN Client
- Apply the Crypto Map to the Gateway Interface

Table 4-5 Defining a Static Crypto Map

Command	Purpose
`hq_sanjose(config)# crypto map vpnclient 1 ipsec-isakmp vpn-dynamic`	To define a static crypto map and add a dynamic crypto map set to a static crypto map set, enter the **crypto map** global configuration command. In this example, the *vpn-dynamic* dynamic map (child) is applied to the *vpnclient* static crypto (parent) map.
`hq_sanjose(config)# access-list 101 permit ip 192.168.1.1 255.255.255.0 host 10.1.2.1`	(Optional) To permit all IP traffic between the host and the gateway when using static IP addressing on the VPN Client, use the extended version of the **access-list** global configuration command. **Note** An access-list must be configured for each VPN Client configured with static IP addresses on a corporate subnet. In this example, all IP traffic is permitted between the two IPSec peers.
`hq_sanjose(config)# interface ethernet0/0`	To configure an interface, enter the **interface** global configuration command. This command invokes the interface (config-if) configuration mode.
`hq_sanjose(config-if)# ip address 10.1.1.1 255.255.255.0`	To indicate an IP address to the interface, enter the **ip address** interface configuration command. In this example, *10.1.1.1* is specified as the IP address of the Ethernet 0/0 interface.
`hq_sanjose(config-if)# crypto map vpnclient`	To apply a previously defined crypto map set to an interface, enter the **crypto map** interface configuration command. In this example, crypto map *vpnclient* is applied to outbound packets from Ethernet interface 0/0.

Related Documentation

For more information on IKE Mode Configuration, refer to the "IKE Mode Configuration (Dynamic IP Addressing)" section in Chapter 2, "Case Study for Layer 3 Authentication and Encryption."

For more information on configuring Cisco IOS software commands, refer to the "Cisco IOS Software Documentation Set" section in the "Preface."

CHAPTER 5

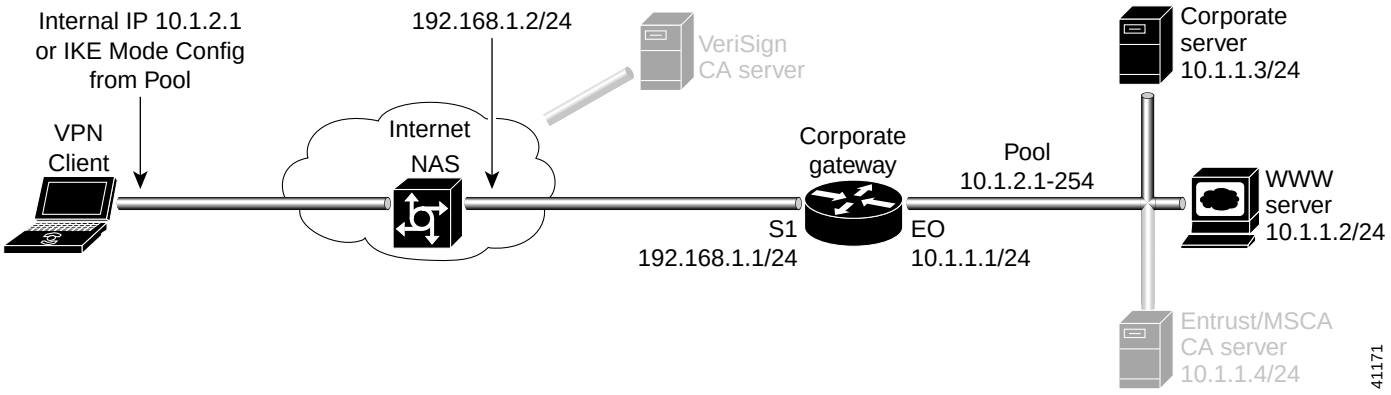
Configuring a Pre-Shared Key or Wildcard Pre-Shared Key

This chapter describes how a Cisco Secure VPN Client (VPN Client) interoperates with a Cisco gateway using a pre-shared key or wildcard pre-shared key for Internet Key Exchange (IKE) authentication. With a pre-shared key, you can allow for one or more clients to use individual shared secret keys to authenticate encrypted tunnels to a gateway.With a wildcard pre-shared key, you can allow for one or more clients to use a shared secret key to authenticate encrypted tunnels to a gateway.

- Task 1—Configuring a Pre-Shared Key or Wildcard Pre-Shared Key on the VPN Client
- Task 2—Configuring a Pre-Shared Key or Wildcard Pre-Shared Key on the Gateway
- Related Documentation

Note Throughout this chapter, there are numerous configuration examples that include unusable IP addresses, passwords, and public key examples. Be sure to use your own IP addresses, passwords, and public keys when configuring your VPN Clients and gateway.

Figure 5-1 Pre-Shared Key Topology



Task 1—Configuring a Pre-Shared Key or Wildcard Pre-Shared Key on the VPN Client

- Configuring a New Gateway for Security Policy
- Specifying a VPN Client's Identity
- Configuring Authentication on the VPN Client

Configuring a New Gateway for Security Policy

To configure a new gateway for a security policy on a VPN Client, perform the following tasks:

- Open the Security Policy Editor
- Configure Other Connections
- Create a New Connection
- Define the New Connection

To open the Security Policy Editor

Click **Start**>**Programs**>**Cisco Secure VPN Client**>**Security Policy Editor**.

The SafeNet/Soft-PK Security Policy Editor window appears, as shown in Figure 5-2. Table 5-1 describes the field descriptions for the SafeNet/Soft-PK Security Policy Editor.

Figure 5-2 SafeNet/Soft-PK Security Policy Editor

Table 5-1 SafeNet/Soft-PK Security Policy Editor Window Field Descriptions

Field	Description
Security Policy Editor	This window establishes connections and their associated proposals, and lists connections in a hierarchical order that defines an IP data communications security policy.
Other Connections	This object is a policy, or a default connection, and the first step in establishing security policies for individual connections.
Connection Security	Under Connection Security, you can define IP access for this connection using Secure, Non-secure, and Block options.
• Secure	• This option secures the IP communications for this connection.
• Non-secure	• This option allows for IP communications to occur without encryption, and allows you to change any settings under your Internet Interface or Local Network Interface.
• Block	• This option denies all IP communications to the VPN Client.

To configure other connections

Step 1 On the **Options** menu, click **Secure**>**Specified Connections**.

In the left pane, **Other Connections** appears.

The Other Connections pane appears in the right pane. Use the Other Connections as the default for your security policy.

Step 2 In the right pane, under Connection Security, click the **Non-Secure** option. Leave all other fields as-is.

Figure 5-2 shows how this is displayed on the Other Connections pane. Table 5-2 describes the field descriptions for the Other Connections pane.

Note If you do not specify the Non-Secure option for the Other Connections pane, you *will not* be able to modify the Internet Interface or Local Network Interface to add the pre-shared key.

To create a new connection

Step 1 In the left pane, click **Other Connections**.

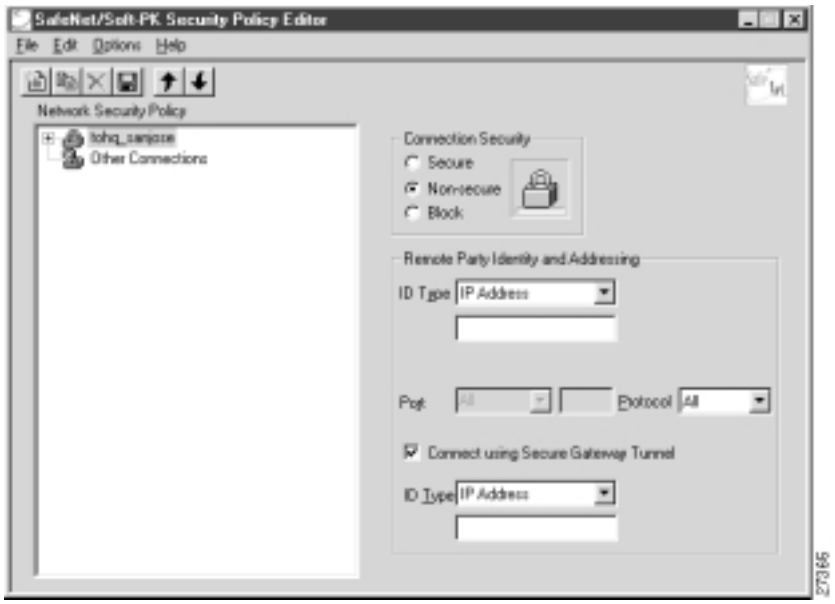
Step 2 On the **File** menu, click **New Connection**.

In the left pane, the default **New Connection** placeholder appears for the New Connection pane.

Step 3 Select **New Connection**, and in its place, define a unique name for the connection to your gateway.

For example, if your router name is `hq_sanjose`, you might rename the connection **`tohq_sanjose`**, as shown in Figure 5-3. Table 5-2 describes the field descriptions for the New Connection pane.

Figure 5-3 Renaming a New Connection



To define the new connection

Step 1 In the left pane, click your new connection. In this example, **tohq_sanjose** is clicked.

The New Connection pane appears.

Step 2 In the right pane, click the **Secure** option.

Step 3 Either define the connection using a pre-shared key or wildcard pre-shared key.

To define the connection for the VPN Client with a pre-shared key

In the right pane, under Remote Party IP Addressing, enter the following parameters:

Step 1 In the ID Type list, click **IP Subnet**.

Step 2 In the Subnet box, enter your corporate subnet. In this example, the IP address of the corporate subnet, **10.1.1.0** is entered.

Step 3 In the Mask box, enter the subnet mask of the IP address of your corporate subnet. In this example, the subnet mask of the corporate subnet, **255.255.255.0** is entered.

Step 4 The Port list and box are inactive as a default. In the Protocol list, click **All**.

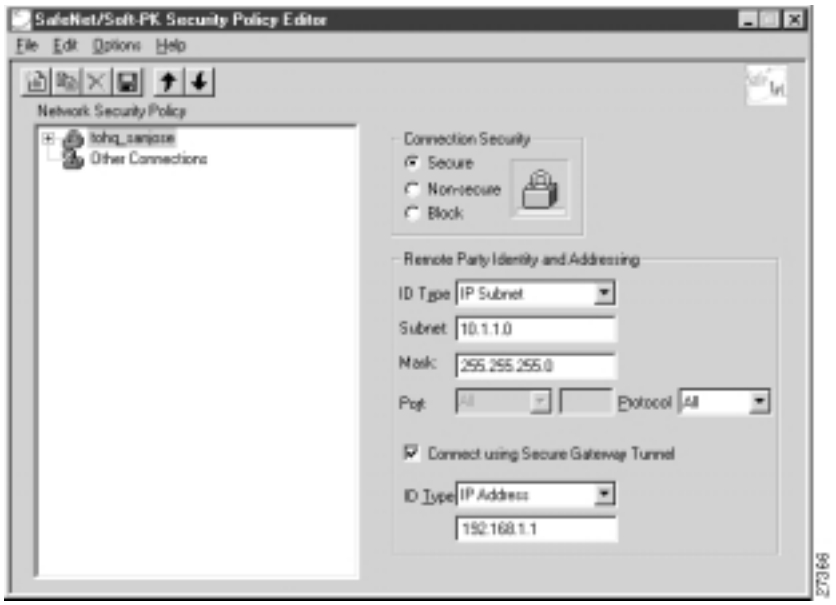
Step 5 Select the **Connect using Secure Gateway Tunnel** check box.

Step 6 In the ID_Type list, click **IP Address**.

Step 7 In the ID_Type box, enter the IP address of the secure gateway. In this example, the secure gateway, **192.168.1.1** is entered.

Figure 5-4 shows how this is displayed on the New Connection pane for pre-shared key. Table 5-2 describes the field descriptions for the New Connection pane.

Figure 5-4 Defining a New Connection for Pre-Shared Key



To define the connection for the VPN Client for a wildcard pre-shared key

In the right pane, under Remote Party IP Addressing, enter the following parameters:

Step 1 In the ID Type list, click **IP Address**.

Step 2 In the IP address value box, enter the wildcard IP address, **0.0.0.0**.

Step 3 The Port list and box are inactive as a default. In the Protocol list, click **All**. Leave all other fields as-is.

Figure 5-5 shows how this is displayed on the New Connection pane for wildcard pre-shared key. Table 5-2 describes the field descriptions for the New Connection pane.

Figure 5-5 Defining a New Connection for Wildcard Pre-Shared Key

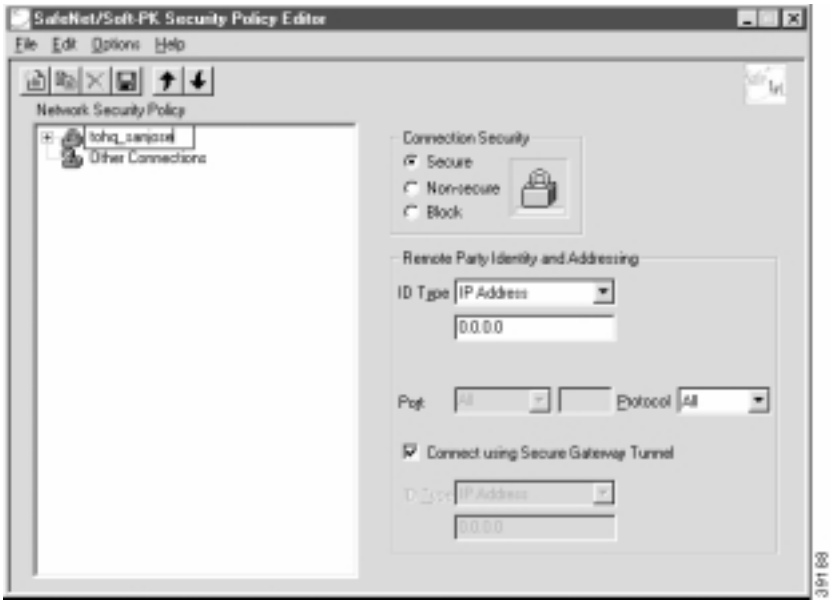


Table 5-2 New Connection Pane Field Descriptions

Field	Description
Network Security Policy	Under Network Security Policy, the proposals that will be used to negotiate the authentication and encryption methods are displayed.
• New Connection	• This object is a set of security parameters that pertain to an individual remote IP connection. *New Connection* is the default connection name.
• Other Connections	• This object is a policy, or a default connection, and 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. Other Connections is always the last rule among security policies.
Connection Security	Under Connection Security, you can define IP access for this connection using Secure, Non-secure, and Block options.
• Secure	• This option secures the IP communications for this connection.
• Non-secure	• This option allows for IP communications to occur without encryption, and you to change any settings under your Internet Interface or Local Network Interface.
• Block	• This option denies all IP communications to the VPN Client.
Remote Party Identity and Addressing	Under Remote Party Identity and Addressing, define the IPSec peer with which the VPN Client will establish a secure tunnel.
ID Type	This list displays options for defining the IPSec peer identity including IP address, domain name, email address, IP subnet, IP address range, and distinguished name. Depending on the option you choose, different values will appear in the right pane.
• IP Address	• This option allows a static IP address to be configured on the VPN Client. This is the default option.
– IP address value	– In this box, specify the IP address value.
• Domain Name	• This option enables the domain name value box and the IP Address box.
– Domain name value	– In this box, specify the domain name value.
– IP Address	– In this box, specify the IP address of the domain, the organizational IP address.
• Email Address	• This option allows you to indicate the email address of the peer.
– Email value	– In this box, specify the e-mail value.
– IP address value	– In this box, specify the peer's IP address.
• IP Subnet	• This option allows you to specify the IP subnet the client will be allowed to access using this peer.
– Subnet	– In this box, specify the subnet IP address.
– Mask	– In this box, specify the mask IP address.

Table 5-2 New Connection Pane Field Descriptions (continued)

Field	Description
• IP Address Range – From – To	• This option allows you to indicate the range of IP addresses to which this client will have access. – In this box, specify the beginning IP address. – In this box, specify the ending IP address.
• Distinguished Name – Edit Name – IP Address	• This option allows you to specify the name, department, state, and country of the peer identity. – When clicked, this button allows you to specify distiguished name settings. – In this box, specify the peer's IP address.
Port	This list shows the IPSec peer's protocol ports. A default of *All* secures all protocol ports.
Connect using Secure Gateway Tunnel	If selected, this check box specifies that the IPSec peer is protected by a secure IPSec-compliant gateway, such as a firewall.
ID_Type	This list shows the identification type of the gateway including IP address, domain name, and distinguished name. Depending on the option you choose, different values will appear in the right pane.
• IP Address – IP address value	• This option enables the IP address value box. This is the default option. – In this box, specify the IP address value.
• Domain Name – Domain name value – IP Address	• This option enables the domain name value box and the IP Address box. – In this box, specify the domain name value. – In this box, specify the IP Address of the domain.
• Distinguished Name – Edit Name – IP Address	• This option allows you to specify the name, department, state, and country of the gateway. – When clicked, this button allows you to specify the distiguished name settings. – In this box, specify the gateway's IP address.

Specifying a VPN Client's Identity

To specify the VPN Client's identity, perform the following tasks:

- Choose an Identity
- Enter the Pre-Shared Key

To choose an identity

Step 1 In the left pane, double-click the new connection. In this example, **tohq_sanjose** is double-clicked.

The new connection expands with My Identity and Security Policy.

Step 2 Click **My Identity**.

The My Identity pane appears in the right pane.

Step 3 In the right pane, under My Identity, enter the following:

a. In the ID_Type list, click **IP Address**.

b. In the Port list, click **All**.

Step 4 In the right pane, under Internet Interface (or Local Network Interface), enter the following:

a. In the Name list, click **Any**. The IP Addr list is inactive as a default.

Step 5 Click **Pre-Shared Key**.

The Pre-Shared Key window appears.

Figure 5-6 shows how this is displayed on the My Identity pane for pre-shared key. Table 5-3 describes the field descriptions for the My Identity pane.

Figure 5-6 My Identity Pane

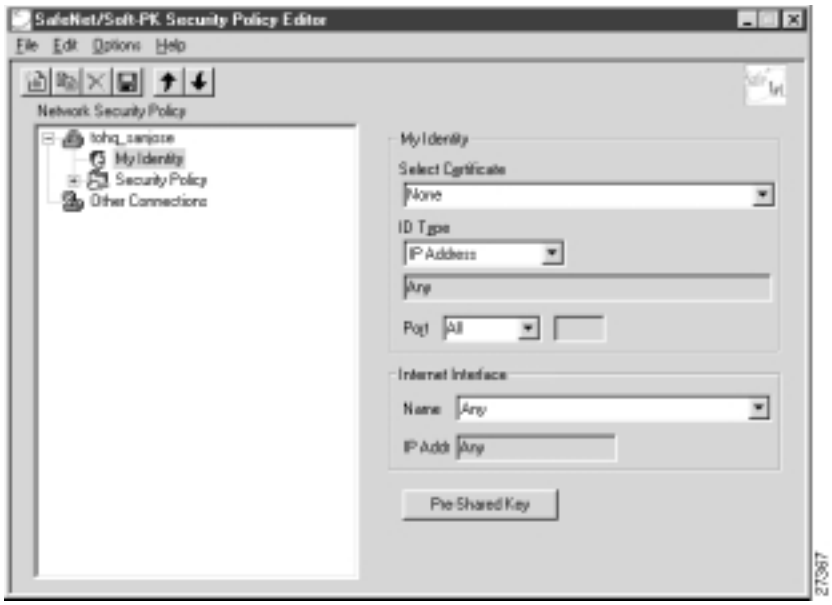


Table 5-3 My Identity Pane Field Descriptions

Field	Description
Network Security Policy	Under Network Security Policy, the proposals that will be used to negotiate the authentication and encryption methods are displayed.
• New Connection>My Identity	• This pane allows you to specify the identity of the VPN Client. This identity will allow the other peer to identify the device during the key exchange phase.

Table 5-3 My Identity Pane Field Descriptions (continued)

Field	Description
My Identity	Under My Identity, specify options for determining the identity of the VPN Client. These options include Select Certificate, ID Type, and Port.
Select Certificate	If you are using digital certification, this list displays all the available digital certificates from which to choose. If you are not using digital certification, *None* is the default option.
ID_Type • IP Address	This list indicates the IP address option for the VPN Client on the corporate subnet. • This field indicates that the VPN Client will be identified by the gateway using the VPN Client's statically or dynamically-assigned IP address.
Port	This list shows the VPN Client's protocol ports. A default of *All* secures all protocol ports.
Local Network Interface: Version 1.0 *or* Internet Interface: Version 1.1	Under Local Network Interface or Internet Interface, specify the hardware interface on the PC or laptop through which the connection will be established. These options include Name and IP Addr options.
Name	This list indicates the names of the hardware interfaces on the PC or laptop. A default of *Any* enables all hardware interfaces.
IP Addr	This list indicates the IP addresses of the hardware interfaces on the PC or laptop. A default of *Any* enables all hardware interface IP addresses.
• Pre-Shared Key	• This button enables the Pre-Shared Key dialog box.

To enter the pre-shared key

Step 1 In the Pre-Shared Key dialog box, under Enter Pre-Shared Key, enter the pre-shared keystring.

The minimum keystring is 8 characters, and the maximum keystring is 128 characters. In this example, *cisco1234* is entered.

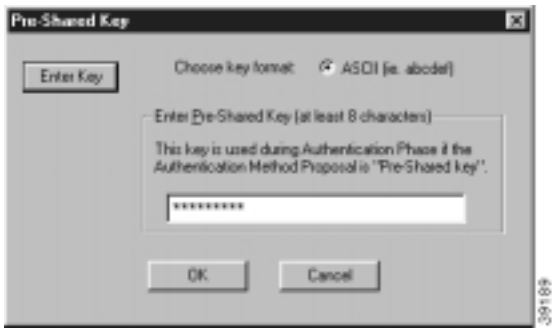
To start the key exchange, both the VPN Client and the gateway must use the same public key.

Step 2 Click **OK**.

Figure 5-7 shows how this is displayed in the Pre-Shared Key dialog box.

Note In the Cisco Secure VPN Client Version 1.0, the pre-shared keystring is visible from the Pre-Shared Key dialog box. In Cisco Secure VPN Client Version 1.1, the pre-shared keystring is hidden.

Figure 5-7 Pre-Shared Key Dialog Box



Configuring Authentication on the VPN Client

To configure authentication on the VPN Client for a pre-shared key or wildcard-preshared key, perform the following steps:

- Specify Authentication Security Policy
- Specify Authentication for Phase 1 IKE
- Specify Authentication for Phase 2 IKE

To specify authentication security policy

Step 1 In the left pane, under My Identity, double-click **Security Policy**.

The Security Policy pane appears in the right pane.

Step 2 In the right pane, under Security Policy, click **Main Mode**.

Step 3 Select the **Enable Replay Detection** check box.

Figure 5-8 shows how this is displayed on the Security Policy pane. Table 5-4 describes the field descriptions for the Security Policy pane.

Figure 5-8 Security Policy Pane

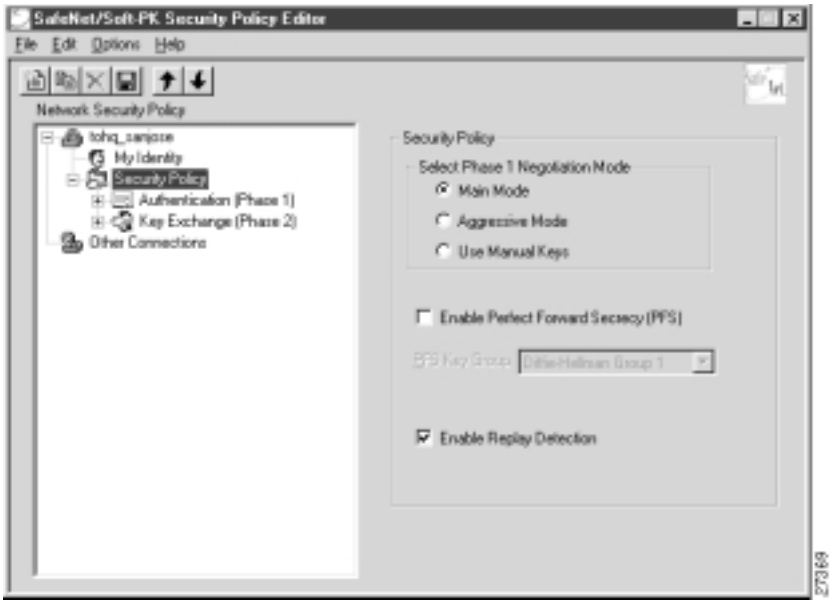


Table 5-4 Security Policy Pane Field Descriptions

Field	Description
Network Security Policy • New Connection>Security Policy	Under Network Security Policy, the proposals that will be used to negotiate the authentication and encryption methods are displayed. • This pane allows you to specify authentication and data integrity.
Security Policy	Under Security Policy, define the Select Phase 1 Negotiation Mode, Enable Perfect Forward Secrecy, or Replay Detection options.
Select Phase 1 Negotiation Mode • Main Mode • Aggressive Mode • Use Manual Keys	Under Select Phase 1 Negotiation Mode, select the mode for authenticating ISAKMP SAs using Main Mode, Aggressive Mode, or Use Manual Key options. • This option allows identities to not be revealed until all secure communications have been established, which requires a longer processing time. • This option allows identities to viewed while secure communications are taking place, which makes for a faster processing time. • This option is available for troubleshooting purposes only.
Enable Perfect Forward Secrecy	When selected, this check box triggers an authentication method, which protects against repeat compromises of a shared secret key.
Enable Replay Detection	When selected, this check box sets a counter that determines whether or not a packet is unique to prevent data from being falsified.

To specify authentication for phase 1 IKE

Step 1 In the left pane, double-click **Security Policy**, and then double-click **Authentication (Phase 1)**. Under Authentication (Phase 1).

A new proposal appears called *Proposal 1*.

The Proposal 1 pane appears in the right pane.

In the right pane, under Authentication Method and Algorithms, in the Authentication Method list, **Pre-Shared key** appears. Because you have already specified a pre-shared key, you cannot make a selection here.

Step 2 In the right pane, under Authentication Method and Algorithms, select the following:

a. In the Encrypt Alg list, click **DES**.

b. In the Hash Alg list, click **MD5**.

c. In the SA Life list, click **Unspecified**.

d. In the Key Group list, click **Diffie-Hellman Group 1**.

Figure 5-9 shows how this is displayed on the Authentication (Phase 1)—Proposal 1 pane for pre-shared key. Table 5-5 describes the field descriptions for the Authentication (Phase 1)—Proposal 1 pane for pre-shared key.

Figure 5-9 Authentication (Phase 1)—Proposal 1 Pane

Table 5-5 Authentication (Phase 1)—Proposal 1 Pane Field Descriptions

Field	Description
Network Security Policy • New Connection>Security Policy>Authentication (Phase 1)>Proposal 1	Under Network Security Policy, the proposals that will be used to negotiate the authentication and encryption methods are displayed. • This pane allows you to specify authentication methods for Authentication Phase 1. During Authentication (Phase 1), you and your peer will reveal your identities and negotiate how they will secure Phase 2 communications. Before securing communications, the two peers involved negotiate the method they will use. Proposals are presented to the other peer in the order in which they are sequenced in the Network Security Policy list. You can reorder the proposals after you create them.
Authentication Method and Algorithms	Under Authentication Method and Algorithms, define the authentication method used and authentication and encryption algoritms.
Authentication Method • Pre-Shared Key • RSA Signatures	This list defines the authentication method being used, either Pre-Shared Key or RSA Signatures. The default is the method of authentication selected under My Identity. • This option appears if the method of authentication selected under My Identity is pre-shared key. • This option appears if the method of authentication selected under My Identity is digital certification.
Encryption and Data Integrity Algorithms	Under Encryption and Data Integrity Algorithms, define the algorithms to be used during Phase 1 negotiation including Encrypt Alg, Hash Alg, SA Life, and Key Group.
Encrypt Alg • DES • Triple-DES	This list allows you to specify encryption with DES or Triple DES options. • This option provides minimal security with 56-bit data encryption standard, which uses less processing time than does Triple-DES. • This option allows for maximum security with 168-bit data encryption standard, which uses more processing time than does DES. **Note** Triple DES is only supported within the U.S. domestic versions of both the Cisco IOS software and the VPN Client.

Table 5-5 Authentication (Phase 1)—Proposal 1 Pane Field Descriptions (continued)

Field	Description
Hash Alg • MD5 • SHA-1	This list allows you to specify authentication with MD5 and SHA-1 options. • This option provides minimal authentication with 128-bit digest, which uses less processing time than does SHA. • This option allows for maximum authentication with 160-bit digest, which uses more processing time than does MD5. **Note** Cisco IOS software does not currently support the DES-MAC Hash Algorithm option.
SA Life	(Optional) This list allows you to specify the period for which the IKE SA is valid using Unspecified, Seconds, Kbytes, or Both options. **Note** When the VPN Client and gateway participate in IKE Phases 1 and 2 negotiation, the lowest SA life value offered by either device will be used as the agreed-upon value.
• Unspecified	• This option allows the other IPSec peer to indicate when IKE SA expires.
• Seconds	• This option allows you to specify SA life in seconds.
• Kbytes	• This option allows you to specify SA life in kilobytes.
• Both	• This option allows you to specify both seconds and kilobytes, whichever comes first, before an SA life expires.
Key Group	This list allows you to specify the Diffie-Hellman key exchange using Diffie-Hellman Group 1 or Diffie-Hellman Group 2 options. **Note** Cisco IOS software does not currently support Diffie-Hellman Group 5.
• Diffie-Hellman Group 1	• This option enables 768-bit encryption, which requires less processing time than does Diffie-Hellman Group 2.
• Diffie-Hellman Group 2	• This option enables 1024-bit encryption, which is more secure than Diffie-Hellman Group 1.

To specify authentication for phase 2 IKE

Step 1 In the left pane, under Authentication (Phase 1), double-click **Key Exchange (Phase 2)**.

In the left pane, under Key Exchange (Phase 2), a new proposal appears called *Proposal 1*.

Step 2 In the right pane, under IPSec Protocols, select the following:

a. In the **SA Life** list, click **Unspecified**.

b. Select the **Encapsulation Protocol (ESP)** check box.

c. In the Encrypt Alg list, click **DES**.

d. In the Hash Alg list, click **MD5**.

e. In the Encapsulation list, click **Tunnel**.

Figure 5-10 shows how this is displayed on the Authentication (Phase 2)—Proposal 1 pane for pre-shared key. Table 5-6 describes the field descriptions for the Authentication (Phase 2)—Proposal 1 pane for pre-shared key.

Figure 5-10 Authentication (Phase 2)—Proposal 1 Pane

Table 5-6 Authentication (Phase 2)—Proposal 1 Pane Field Descriptions

Field	Description
Network Security Policy • New Connection>Security Policy>Key Exchange (Phase 2)>Proposal 1	Under Network Security Policy, the proposals that will be used to negotiate the authentication and encryption methods are displayed. • This pane allows you to specify authentication methods for Key Exchange (Phase 2). Set authentication requirements in the Security Policy pane. Negotiate which key exchange method of securing communications you and the other IPSec peer will use by establishing a proposal.

Table 5-6 Authentication (Phase 2)—Proposal 1 Pane Field Descriptions (continued)

Field	Description
IPSec Protocols	Under IPSec Protocols, define the algorithms to be used during Phase 2 key exchange, including SA Life, Encrypt Alg, Hash Alg, and Encapsulation options.
SA Life	This list allows you to specify the period for which the IKE SA is valid using Unspecified, Seconds, Kbytes, or Both options. **Note** When the VPN Client and gateway participate in IKE phases 1 and 2 negotiation, the lowest SA life value offered by either device will be used as the agreed-upon value.
• Unspecified	• This option allows the other IPSec peer to indicate when IKE SA expires.
• Seconds	• This option allows you to specify SA life in seconds.
• Kbytes	• This option allows you to specify SA life in kilobytes.
• Both	• This option allows you to specify both seconds and kilobytes, whichever comes first, before an SA life expires.
Encapsulation Protocol	If selected, this check box indicates that encryption and authentication will be selected for this proposal.
Encrypt Alg	This list allows you to specify encryption with DES or Triple DES options.
• DES	• This option provides minimal security with 56-bit data encryption standard, which uses less processing time than does Triple-DES.
• Triple-DES	• This option allows for maximum security with 168-bit data encryption standard, which uses more processing time than does DES. **Note** Triple DES is only supported within the U.S. domestic versions of both the Cisco IOS software and the VPN Client.
Hash Alg	This list allows you to specify authentication with MD5 or SHA-1 options.
• MD5	• This option provides minimal authentication with 128-bit digest, which uses less processing time than does SHA. **Note** Cisco IOS software does not currently support the DES-MAC Hash Algorithm option.
• SHA-1	• This option allows for maximum authentication with 160-bit digest, which uses more processing time than does MD5.

Table 5-6 Authentication (Phase 2)—Proposal 1 Pane Field Descriptions (continued)

Field	Description
Encapsulation	This list allows you to specify encapsulation method with Tunnel or Transport options.
• Tunnel	• This option is the only method of secure encapsulation available for the Cisco Secure VPN Client.
• Transport	• This option allows non-IPSec protected encapsulation (when both peers are not using IPSec.) Otherwise, you *must* use the Tunnel option for maximum security.

To save your policy

Step 1 On the **File** menu, click **Save Changes** to save the policy.

The Security Policy Editor dialog box appears. Before your policy is implemented, you must save your policy settings.

Step 2 Click **OK**.

Figure 5-11 shows how this is displayed in the Security Policy Editor dialog box.

Figure 5-11 Security Policy Editor

Task 2—Configuring a Pre-Shared Key or Wildcard Pre-Shared Key on the Gateway

To configure a pre-shared key or wildcard pre-shared key on the gateway, perform the following steps:

- Configuring the Gateway
- Configuring ISAKMP
- Configuring IPSec
- Defining a Dynamic Crypto Map
- Defining a Static Crypto Map

Configuring the Gateway

To configure the gateway, perform the following tasks, as described in Table 5-7:

- Configure the Gateway
- Define the Host Name
- Define the Name Server

Table 5-7 Configuring the Gateway

Command	Purpose
`router> enable`	To enter privileged EXEC mode, enter the **enable** user EXEC command.

`router# configure terminal`
`Enter configuration commands, one per line.`
`End with CNTL/Z.`
	To enter global configuration mode, enter the **configure** privileged EXEC command. To configure the terminal attached at console port, enter the **terminal** keyword.

`router(config)# ip domain-name example.com`	To define a default domain name that the Cisco IOS software uses to complete unqualified host names, use the **ip domain-name** global configuration command. An unqualified host name is a host name without a dotted-decimal domain name. In this example, *example.com* is defined as the default domain name.
`router(config)# hostname hq_sanjose`	To specify or modify the host name for the network server, enter the **hostname** global configuration command. The host name is used in prompts and default configuration filenames. In this example, *hq_sanjose* is defined as the host name. The *hq_sanjose* host name replaces the default *router* host name.
`hq_sanjose(config)# ip name-server 192.168.1.1`	To specify the address of a name server to use for name and address resolution, enter the **ip name-server** global configuration command. In this example, the gateway is defined as the *IP name server*. The gateway's IP address is *192.168.1.1*.

Configuring ISAKMP

To configure ISAKMP on the gateway, perform the following tasks, as described in Table 5-8:

- Configure ISAKMP Policy
- Configure Pre-Shared Key

Table 5-8 Configuring ISAKMP

Command	Purpose
`hq_sanjose(config)# crypto isakmp policy 3`	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. In this example, the ISAKMP policy is assigned a priority of *3*.
`hq_sanjose(config-isakmp)# encryption des`	(Optional) To specify the encryption algorithm, use the **encryption (IKE policy)** ISAKMP policy configuration command. The options for encryption are the **des** and **3des** keywords. DES is configured by default for minimum security and fastest processing.
`hq_sanjose(config-isakmp)# hash sha`	(Optional) To specify the hash algorithm, use the **hash (IKE policy)** ISAKMP policy configuration command. IKE policies define a set of parameters to be used during IKE negotiation. The options for hashing are the **sha** and **md5** keywords. SHA is configured by default for maximum authentication with slower processing than MD5.
`hq_sanjose(config-isakmp)# authentication pre-share`	To specify the authentication method, use the **authentication (IKE policy**) ISAKMP policy configuration command. The options for authentication method are the **rsa-sig**, **rsa-encr**, and **pre-share** keywords. To specify pre-shared key as the authentication method, enter the **pre-share** keyword.
`hq_sanjose(config-isakmp)# group 1`	(Optional) To specify the Diffie-Hellman group identifier, use the group ISAKMP policy configuration command. The options for Diffie-Hellman group are the **1** and **2** keywords. Diffie-Hellman Group 1 is configured by default for minimum security with the fastest processing time.

Table 5-8 Configuring ISAKMP (continued)

Command	Purpose
`hq_sanjose(config-isakmp)# lifetime 86400`	(Optional) To specify the lifetime of an IKE SA before it expires, use the **lifetime** ISAKMP policy configuration command. The lifetime can be using an integer from *60* to *86,400* seconds. A day (86,400 seconds) is configured by default.
`hq_sanjose(config-isakmp)# exit`	To exit ISAKMP policy configuration (config-isakmp) command mode, enter the **exit** ISAKMP policy configuration command.

`hq_sanjose(config)# crypto isakmp key cisco1234 address 10.1.2.1`
or
`hq_sanjose(config)# crypto isakmp key cisco1234 address 0.0.0.0`
	To configure a pre-shared authentication key, use the **crypto isakmp key** global configuration command. You must configure this key whenever you specify pre-shared key in an IKE policy. Use any combination of alphanumeric characters between 8 and 128 bytes. This pre-shared key must be identical at both peers.
	The VPN Client pre-shared key and IP address are specified as follows:
	• If configuring pre-shared key, specify a separate pre-shared key and static IP address for each VPN Client.
	In the first example, one VPN Client is configured with *cisco1234* as the pre-shared key and *10.1.2.1* as static IP address of the VPN Client. The **address** keyword indicates an IP address will be used for authentication.
	• If configuring wildcard pre-shared key, specify one pre-shared key for each group of VPN Clients at the same level of authorization. Then, specify the wildcard IP address, *0.0.0.0*, for dynamic IP addressing. The **address** keyword indicates an IP address will be used for authentication.
	In the second example, one or more VPN Client(s) is/are configured with *cisco1234* as the pre-shared key and *0.0.0.0* as wildcard IP address of the VPN Client.

Caution For security purposes, you *must* distribute the pre-shared key (pre-shared key or wildcard pre-shared key) to remote users through a secure out-of-band channel. For more details, see "Authentication and Encryption Features" in Chapter 2, "Case Study for Layer 3 Authentication and Encryption."

Configuring IPSec

To configure IPSec on the gateway, perform the following tasks, as described in Table 5-9:

- Configure IPSec Transform Set
- Configure IPSec Encapsulation

Table 5-9 Configuring IPSec

Command	Purpose
`hq_sanjose(config)# crypto ipsec transform-set vpn-transform esp-des esp-md5-hmac`	To define a combination of security associations to occur during IPSec negotiations, enter the **crypto ipsec transform-set** global configuration command. This command invokes the crypto transform (cfg-crypto-trans) configuration mode. In this example, the transform set named *vpn-transform* is defined with two security algorithm keywords: **esp-des** and **ah-md5-hmac**. This is the recommended combination for minimum encryption and authentication. **Note** There are complex rules defining which entries you can use for the transform arguments. These rules are explained in the command description for the **crypto ipsec transform-set** command. You can also use the **crypto ipsec transform-set** global configuration command to view the available transform arguments.
`hq_sanjose(cfg-crypto-trans)# mode tunnel`	(Optional) To specify encapsulation between the gateway and the VPN Client, enter the **mode** crypto transform configuration command. The **mode** command is only applicable to traffic whose source and destination addresses are the IPSec peer addresses; it is ignored for all other traffic. (All other traffic is in tunnel mode only.) The options for encapsulation are **tunnel** and **transport** keywords. Tunnel is configured by default for IPSec encapsulation.
`hq_sanjose(cfg-crypto-trans)# exit`	To exit crypto transform (cfg-crypto-trans) configuration mode, enter the **exit** crypto transform configuration command.

Defining a Dynamic Crypto Map

To define a dynamic crypto map, perform the following tasks, as described in Table 5-10:

- Define a Dynamic Crypto Map Entry
- Add a Dynamic Crypto Map to the Static Crypto Map

Table 5-10 Defining a Dynamic Crypto Map

Command	Purpose
`hq_sanjose(config)# crypto dynamic-map vpn-dynamic 1`	To define a dynamic crypto map entry, use the **crypto dynamic-map** command. This command invokes the crypto map (config-crypto-map) configuration mode. The dynamic map entry will reference the static crypto map entry. In this example, the dynamic map name is *vpn-dynamic*, and the sequence number (or priority) is *1*.
`hq_sanjose(config-crypto-map)# set transform-set vpn-transform`	To specify which transform sets are allowed for the crypto map entry, enter the **set transform-set** crypto map configuration command. In this example, the transform set previously defined in Configuring IPSec, *vpn-transform*, is applied to the *vpn-dynamic* dynamic crypto map. **Note** You can list multiple transform sets in order of priority (highest priority first).
`hq_sanjose(config-crypto-map)# set security-association lifetime seconds 2700`	(Optional) If you want the security associations for this crypto map to be negotiated using shorter IPSec SA lifetimes than the globally specified lifetimes, specify a key lifetime for the crypto map entry. Specify the IPSec lifetimes using one of the following keywords: **seconds** or **kilobytes**. The crypto map's security associations are negotiated according to the global lifetimes. In this example, the SA lifetime is *2700* seconds.
`hq_sanjose(config-crypto-map)# exit`	To exit crypto map (config-crypto-map) configuration mode, enter the **exit** crypto map configuration command.

Defining a Static Crypto Map

To define a static crypto map, perform the following tasks, as described in Table 5-11:

- Define a Static Crypto Map Entry
- Add a Dynamic Crypto Map to a Static Crypto Map
- Define an Access List for the VPN Client
- Apply the Crypto Map to the Gateway Interface

Table 5-11 Defining Static Crypto Map

Command	Purpose
`hq_sanjose(config)# crypto map vpnclient 1 ipsec-isakmp vpn-dynamic`	To define a static crypto map and add a dynamic crypto map set to a static crypto map set, enter the **crypto map** global configuration command. In this example, the *vpn-dynamic* dynamic map (child) is applied to the *vpnclient* static crypto map (parent).
`hq_sanjose(config)# access-list 101 permit ip 192.168.1.1 255.255.255.224 host 10.1.2.1`	(Optional) To permit all IP traffic between the host and the gateway when using static IP addressing on the VPN Client, use the extended version of the **access-list** global configuration command. **Note** An access-list must be configured for each VPN Client configured with static IP addresses on a corporate subnet. In this example, all IP traffic is permitted between the two IPSec peers.
`hq_sanjose(config)# interface ethernet0/0`	To configure an interface, enter the **interface** global configuration command. This command invokes the interface (config-if) configuration mode.
`hq_sanjose(config-if)# ip address 10.1.1.1 255.255.255.0`	To indicate an IP address to the interface, enter the **ip address** interface configuration command. In this example, *10.1.1.1* is specified as the IP address of the Ethernet 0/0 interface.
`hq_sanjose(config-if)# crypto map vpnclient`	To apply a previously defined crypto map set to an interface, enter the **crypto map** interface configuration command. In this example, crypto map *vpnclient* is applied to outbound packets from Ethernet interface 0/0.

Related Documentation

For more information on pre-shared key and wildcard pre-shared key, refer to the “Pre-Shared Keys” section or “Wildcard Pre-Shared Keys” section in Chapter 2, “Case Study for Layer 3 Authentication and Encryption.”

For more information on configuring Cisco IOS software commands, refer to the “Cisco IOS Software Documentation Set” section in the “Preface.”

CHAPTER 6

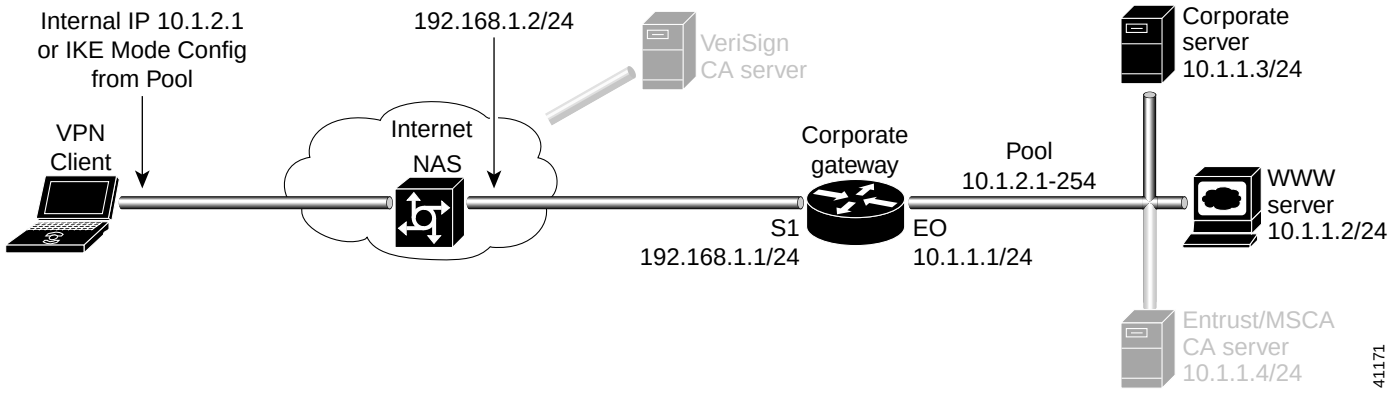
Configuring Digital Certification

This chapter describes how Cisco Secure VPN Client interoperates with Cisco networking devices using digital certificates in certification authority (CA) and Registration Authority (RA) modes with file-based enrollment and Simple Certificate Enrollment Protocol (SCEP). Using IPSec, digital certificates allow devices to be automatically authenticated to each other without manual key exchanges. This chapter includes the following sections:

- Task 1—Configuring Digital Certifications on the VPN Client
- Task 2—Configuring Digital Certification on the Gateway

Note Throughout this chapter, there are numerous configuration examples that include unusable IP addresses, passwords, and public key examples. Be sure to use your own IP addresses, passwords, and public keys when configuring your VPN Clients and gateway.

Figure 6-1 Digital Certificate Topology



Task 1—Configuring Digital Certifications on the VPN Client

- Importing the Root CA Certificate
- Creating a Public and Private Key Pair
- Sending the Certification Request to the CA Server
- Importing Your Signed Digital Certificate
- Configuring a New Gateway for a Security Policy
- Specifying the VPN Client's Identity
- Configuring Authentication on the VPN Client

Note Before configuring digital certification, it is recommended you configure pre-shared key authentication to establish VPN connectivity for debugging purposes. Once you have successfully established the VPN, then you can implement digital certification.

For details on configuring pre-shared keys, refer to Chapter 5, "Configuring a Pre-Shared Key or Wildcard Pre-Shared Key."

Importing the Root CA Certificate

To import the root CA certificate on the VPN Client, perform the following steps:

- Open the My Certificates Folder
- Open the CA Certificates Folder
- Import the Root CA Certificate
- Locate the Root CA File

To open the My Certificates folder

Click **Start**>**Programs**>**Cisco Secure VPN Client**>**Certificate Manager**.

The SafeNet/Soft-PK Certificate Manager dialog box appears with the My Certificates folder as a default, as shown in Figure 6-2. Table 6-1 describes the field descriptions for the My Certificates folder.

Figure 6-2 My Certificates Folder

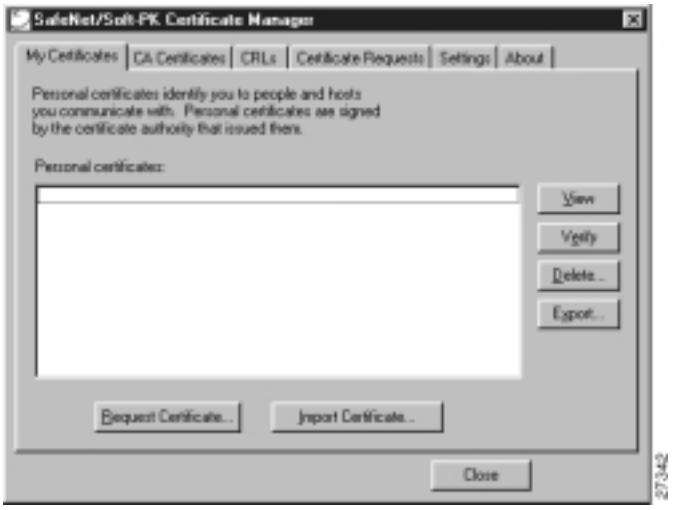


Table 6-1 My Certificates Folder Field Descriptions

Field	Description
Certificate Manager	This folder allows you to request, import, and store the digital certificates that you receive from the certification authority (CA). There are two types of digital certificates: root CA certificates and personal certificates.
My Certificates	This folder shows the available personal certificates and provides options for certificate management.
Personal certificates	This box lists the personal digital certificates available for this VPN Client. You must have your own personal digital certificate from a CA, which verifies your identity to the IPSec peers with which you will communicate. **Note** You must have a root CA certificate before you can request a personal certificate.
• View	• When clicked, this button allows you to view the contents of your digital certificate issued by the CA.
• Verify	• When clicked, this button prompts the VPN Client to check the validity dates and to check the digital certificate against its revocation list. An information window returns the current status of the certificate along with its content.
• Delete	• When clicked, this button allows you to delete a digital certificate.
• Export	• When clicked, this button allows you to export or copy a digital certificate.
• Request Certificate	• When clicked, this button allows you to request a certificate from a specified CA on the Internet.
• Import Certificate	• When clicked, this button allows you to import a certificate.

To open the CA Certificates folder

Click the **CA Certificates** tab.

The CA Certificates Folder appears as shown in Figure 6-3. Table 6-2 describes the field descriptions for the CA Certificates folder.

Figure 6-3 CA Certificates Folder

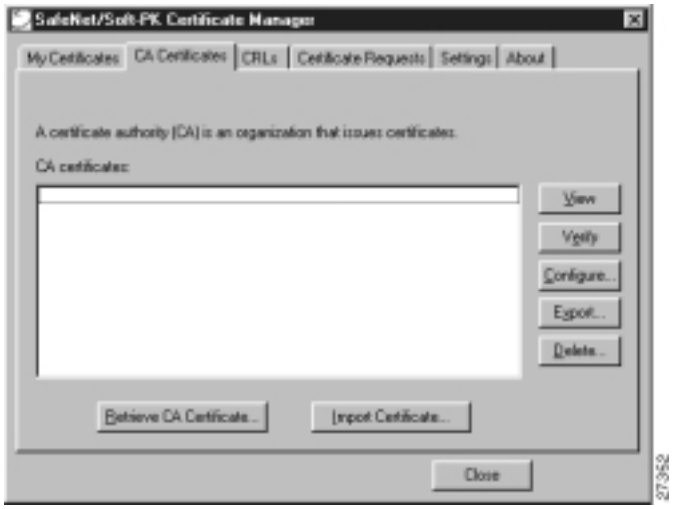


Table 6-2 CA Certificates Folder Field Descriptions

Field	Description
CA Certificates	This folder allows you to retrieve, import, view, verify, configure, export, or delete the certificates you receive from the CA.
CA certificates	This box lists the root CA digital certificates available for this VPN Client. Each CA you contact must provide you with its own root CA digital certificate, which verifies its identity. **Note** You must have a root CA certificate before you can request a personal certificate.

Table 6-2 CA Certificates Folder Field Descriptions (continued)

Field	Description
• View	• When clicked, this button allows you to view the contents of your digital certificate issued by the CA.
• Verify	• When clicked, this button prompts the VPN Client to check the validity dates and to check the digital certificate against its revocation list. An information window returns the current status of the certificate along with its content.
• Delete	• When clicked, this button allows you to delete a digital certificate.
• Export	• When clicked, this button allows you to export or copy a digital certificate.
• Request Certificate	• When clicked, this button allows you to request a certificate from a specified CA on the Internet.
• Import Certificate	• When clicked, this button allows you to import a certificate.

To import the Root CA certificate

Step 1 In the CA Certificates Folder, click **Import Certificate**.

The Import Certificate (and Keys) dialog box appears as shown in Figure 6-4. Table 6-3 describes the field descriptions for the Import Certificate (and Keys) dialog box.

Step 2 Under Import Options, click the **No Keys to Import** option.

Step 3 Under Certificate, click **Browse**.

Figure 6-4 Import Certificate (and Keys) Dialog Box

Table 6-3 Import Certificate (and Keys) Dialog Box Field Descriptions

Field	Description
Import Certificate (and Keys)	This dialog box allows you to import a previously exported digital certificate or to import a recently downloaded digital certificate. Use this dialog box to obtain the root CA file from the system administrator, who should also supply you with the URL for IPSec CSR enrollment. The system administrator receives the root CA file and URL from the CA Administrator.
Import Options	Under Import Options, specify whether or not you want to import your keys by indicating either the No Keys to Import option or the Import Keys From File option.
• No Keys to Import	• This option indicates that you downloaded the CA certificate, or the CA sent a personal certificate to you in an e-mail, directed you to copy it from a server, or gave it to you on a floppy disk because you chose not to request one online. No keys require importing because the keys should be in the same file as the certificate.
• Import Keys From File	• This option indicates that you are importing a certificate file that you or your network administrator exported from the Certificate Manager window under My Identity. The keys for this personal certificate would have been copied to this file when you or your network administrator exported it.
Certificate	Under Certificate, specify the location of the certificate file using the Filename box.
• Filename	This box allows you to enter the certificate file's drive, directory, and filename, or use Browse to find it.
Keys	Under Keys, you can specify the location of the certificate file with keys.
• Filename	• This box is activated when you click the Import Keys From File option. Enter the filename to import a certificate file, or click Browse to find it.
• Password	• This box is activated when you click the Import Keys From File option. Enter the password to import a certificate file.
• Import	• When clicked, this button allows you to either import the digital certificate specified.

To locate the Root CA file

Step 1 From the CA Certificates Folder, click **Import**.

The Open dialog box appears, as shown in Figure 6-5. Use the Open dialog box to locate the root CA file on your hard drive. Open the root CA file for importing to the CA Certificates folder.

Step 2 In the Files of Type list, click **Base64 encoded certificate files**.

Step 3 Locate the root CA file (the *.cer* file), and then click **Open**.

The Import Certificate (and Keys) dialog box reappears, as shown in Figure 6-4.

Step 4 To add the certificate to the root store, click **Import.**

Figure 6-5 Open Dialog Box

Creating a Public and Private Key Pair

To create a public and private key pair, perform the following tasks:

- Open My Certificates Folder
- Specify Online Certificate Request

To open the My Certificates folder

Click **Start**>**Programs**>**Cisco Secure VPN Client**>**Certificate Manager**.

The SafeNet/Soft-PK Certificate Manager dialog box appears with the My Certificates folder as a default, as shown in Figure 6-2. Table 6-1 describes the field descriptions for the My Certificates folder.

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

To specify On-line Certificate Request

Step 1 In the SafeNet/Soft-PK Certificate Manager, click **Request Certificate**.

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

The Online Certificate Request dialog box appears. Figure 6-6 shows the Online Certificate Request window. Table 6-4 describes the field descriptions for the Online Certificate Request window.

Step 2 In the Online Certificate Request dialog box, fill in the sections based on the identity of the owner of the certificate, and then click **OK**.

Figure 6-6 shows how these sections can be specified. Be sure to use your own identity specifications.

The client will generate public/private key pairs.

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.

Figure 6-6 Online Certificate Request

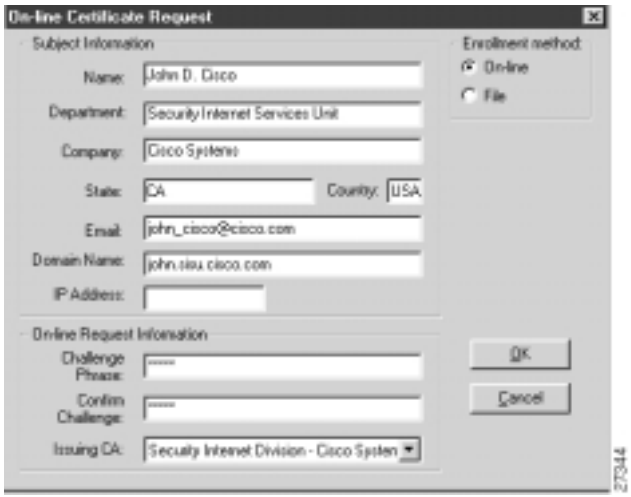


Table 6-4 Online Certificate Request

Field	Description
On-line Certificate Request	This dialog box allows you to specify public and private key pairs and enroll your personal certificate online. You can configure a certificate request for online or file-based enrollment.
Subject Information	Under Subject Information, specify the identity of the certificate owner, including Name, Department, Company, State, Email, Domain Name, and IP Address options.
• Name	• This box allows you to enter the certificate owner's name.
• Department	• This box allows you to enter the certificate owner's department.
• Company	• This box allows you to enter the certificate owner's company.
• State	• This box allows you to enter the state where the company headquarters is located.
• Email	• This box allows you to enter the certificate owner's email address.
• Domain Name	• This box allows you to enter the domain of the company.
• IP Address	• This box allows you to specify an IP address, but you need not enter anything here.

Table 6-4 Online Certificate Request (continued)

Field	Description
Online Request Information	Under Online Request Information, fill in the Challenge Phrase, Confirm Challenge, and Issuing CA box.
• Challenge Phrase	• This box allows you to enter a challenge phrase to be used to identify you in the event you choose to cancel or replace your digital certificate. You must remember this phrase.
• Confirm Challenge	• This box allows you to confirm your phrase.
• Issuing CA	• This box allows you to select a CA server issuing the certificate.

Sending the Certification Request to the CA Server

- To configure Entrust digital certificates, see Appendix A, "Configuring Entrust Digital Certificates."
- To configure Microsoft digital certificates, see Appendix B, "Configuring Microsoft Certificate Services."
- To configure VeriSign digital certificates, see Appendix C, "Configuring VeriSign Digital Certificates."

Importing Your Signed Digital Certificate

To import the signed digital certificate on the VPN Client, perform the following steps:

- Open the My Certificates Folder
- Import the Signed Digital Certificate
- Locate the Signed Digital Certificate
- Confirm Signed Digital Certificate

To open the My Certificates folder

Click **Start**>**Programs**>**Cisco Secure VPN Client**>**Certificate Manager**.

The SafeNet/Soft-PK Certificate Manager dialog box appears with the My Certificates folder as a default, as shown in Figure 6-2. Table 6-1 describes the field descriptions for the My Certificates folder.

To import the signed digital certificate

Step 1 In the My Certificates Folder, click **Import Certificate**.

Note The CA Administrator should have sent you a signed digital certificate through email.

The Import Certificate (and Keys) dialog box appears, as shown in Figure 6-4. Table 6-3 describes the field descriptions for the Import Certificate (and Keys) dialog box.

Step 2 In the Import Certificate (and Keys) dialog box, select the **No Keys to Import** option.

Step 3 Under Certificate, click **Browse**.

To locate and import the signed digital certificate

Step 1 From the My Certificates Folder, click **Import**.

The Open dialog box appears, as shown in Figure 6-5.

Step 2 In the Files of Type list, click **Base64 encoded certificate files**.

Step 3 Add your signed digital certificate, and then rename the file with a "**.cer**" filename extension.

Step 4 Select your signed digital certificate, and then, click **Open**.

The Import Certificate (and Keys) dialog box reappears.

Step 5 Click **Import**.

Figure 6-7 Open Dialog Box

To confirm signed digital certificate

After clicking Import, the Certificate Manager dialog box appears displaying the personal certificate to be added, as shown in Figure 6-8. To confirm that you want to add this personal certificate, click **Yes**.

Figure 6-8 Certificate Manager Dialog Box

Configuring a New Gateway for a Security Policy

To configure a new gateway for a security policy on a VPN Client, perform the following tasks:

- Open the Security Policy Editor
- Configure Other Connections
- Create a New Connection
- Define the New Connection

To open the Security Policy Editor

Click **Start**>**Programs**>**Cisco Secure VPN Client**>**Security Policy Editor**.

The SafeNet/Soft-PK Security Policy Editor dialog box appears, as shown in Figure 6-9. Table 6-5 describes the field descriptions for the SafeNet/Soft-PK Security Policy Editor.

Figure 6-9 SafeNet/Soft-PK Security Policy Editor

Table 6-5 SafeNet/Soft-PK Security Policy Editor Window Field Descriptions

Field	Description
Security Policy Editor	This window establishes connections and their associated proposals, and lists connections in a hierarchical order that defines an IP data communications security policy.
Other Connections	This object is a policy, or a default connection, and the first step in establishing security policies for individual connections.

Table 6-5 SafeNet/Soft-PK Security Policy Editor Window Field Descriptions (continued)

Field	Description
Connection Security	Under Connection Security, you can define IP access for this connection using Secure, Non-secure, and Block options.
• Secure	• This option secures the IP communications for this connection.
• Non-secure	• This option allows for IP communications to occur without encryption, and allows you to change any settings under your Internet Interface or Local Network Interface.
• Block	• This option denies all IP communications to the VPN Client.

To configure other connections

Step 1 From the **Options** menu, click **Secure**>**Specified Connections**.

In the left pane, **Other Connections** appears.

The Other Connections pane appears in the right pane. Use the Other Connections as the default for your security policy.

Step 2 In the right pane, under Connection Security, click the **Non-Secure** option. Leave all other fields as-is.

Figure 6-9 shows how this is displayed on the Other Connections pane. Table 6-6 describes the field descriptions for the Other Connections pane.

To create a new connection

Step 1 In the left pane, click **Other Connections**.

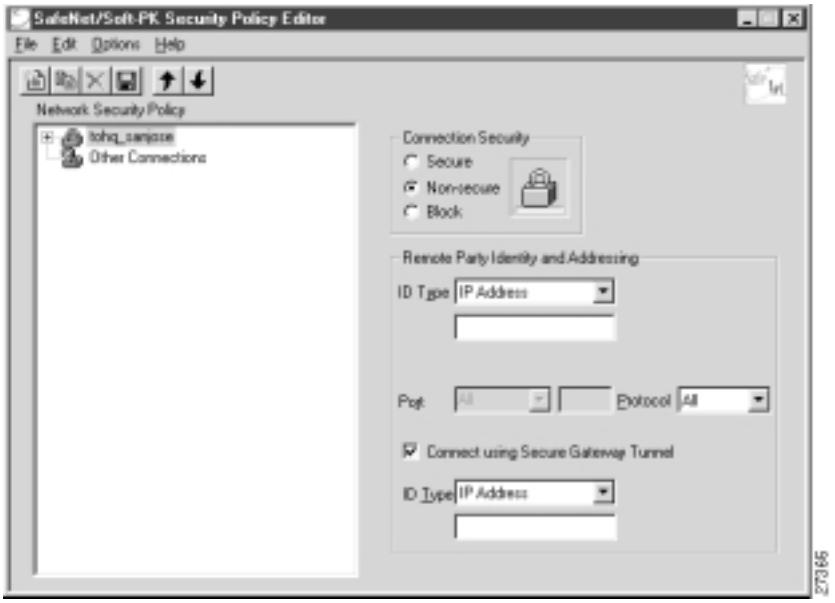
Step 2 On the **File** menu, click **New Connection**.

In the left pane, the default **New Connection** placeholder appears for the New Connection pane.

Step 3 Select **New Connection**, and in its place, define a unique name for the connection to your gateway.

For example, if your router name is `hq_sanjose`, you might rename the connection **`tohq_sanjose`**, as shown in Figure 6-10. Table 6-6 describes the field descriptions for the New Connection pane.

Figure 6-10 Renaming a New Connection



To define the new connection

Step 1 In the left pane, click your new connection. In this example, **tohq_sanjose** is clicked.

The New Connection pane appears in the right pane.

Step 2 In the right pane, under Connection Security, click the **Secure** option.

Step 3 In the right pane, under Remote Party Identity and Addressing, enter the following:

a. From the ID Type list, click **IP Subnet**. In this example, the IP address of the corporate subnet, **10.1.1.0** is entered.

b. In the Mask list, enter the subnet mask of the IP address of your corporate subnet. In this example, the subnet mask of the corporate subnet, **255.255.255.0** is entered.

c. The Port list and box are inactive as a default.

d. In the Protocol list, click **All**.

e. Select the **Connect using Secure Gateway Tunnel** check box.

f. In the ID_Type list, click **IP Address**.

g. In the ID_Type box, enter the IP address of the secure gateway. In this example the secure gateway, **192.168.1.1** is entered.

Figure 6-11 shows how this is displayed on the New Connection pane for digital certificates. Table 6-6 describes the field descriptions for the New Connection pane.

Figure 6-11 Defining a New Connection for Digital Certificates

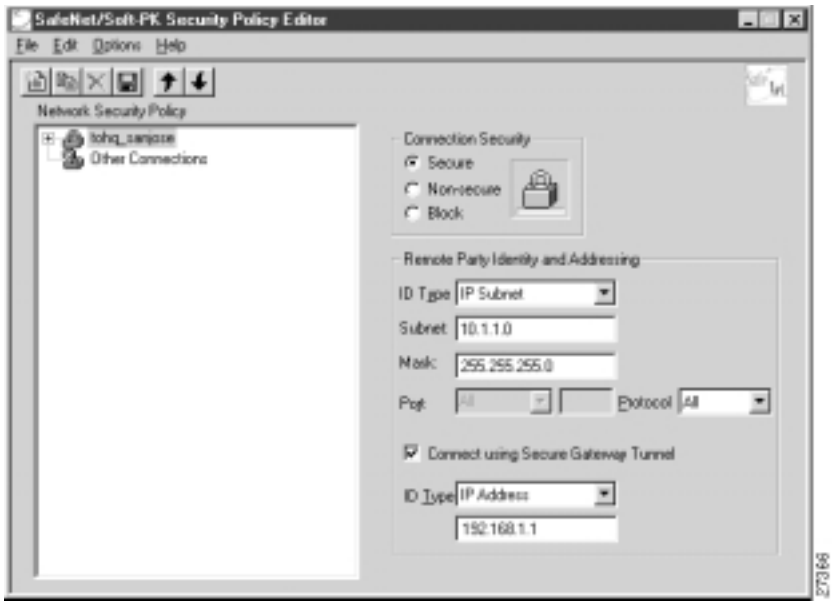


Table 6-6 New Connection Pane Field Descriptions

Field	Description
Network Security Policy	Under Network Security Policy, the proposals that will be used to negotiate the authentication and encryption methods are displayed.
• New Connection	• This object is a set of security parameters that pertain to an individual remote IP connection. *New Connection* is the default connection name.
• Other Connections	• This object is a policy, or a default connection, and 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. Other Connections is always the last rule among security policies.
Connection Security	Under Connection Security, you can define IP access for this connection using Secure, Non-secure, and Block options.
• Secure	• This option secures the IP communications for this connection.
• Non-secure	• This option allows for IP communications to occur without encryption, and allows you to change any settings under your Internet Interface or Local Network Interface.
• Block	• This option denies all IP communications to the VPN Client.
Remote Party Identity and Addressing	Under Remote Party Identity and Addressing, define the IPSec peer with which the VPN Client will establish a secure tunnel.

Table 6-6 New Connection Pane Field Descriptions (continued)

Field	Description
ID Type	This list displays options for defining the IPSec peer identity including IP address, domain name, email address, IP subnet, IP address range, and distinguished name. IP subnet is the default option. Depending on the option you choose, different values will appear in the right pane.
• IP Address	• This option allows a static IP address to be configured on the VPN Client.
– IP address value	– In this box, specify the IP address value.
• Domain Name	• This option enables the domain name value box and the IP Address box.
– Domain name value	– In this box, specify the domain name value.
– IP Address	– In this box, specify the IP address of the domain, the organizational IP address.
• Email Address	• This option allows you to indicate the email address of the peer.
– Email value	– In this box, specify the e-mail value.
– IP address value	– In this box, specify the peer's IP address.
• IP Subnet	• This option allows you to specify the IP subnet the client will be allowed to access using this peer.
– Subnet	– In this box, specify the subnet IP address.
– Mask	– In this box, specify the mask IP address.
• IP Address Range	• This option allows you to indicate the range of IP addresses to which this client will have access.
– From	– In this box, specify the beginning IP address.
– To	– In this box, specify the ending IP address.
• Distinguished Name	• This option allows you to specify the name, department, state, and country of the peer identity.
– Edit Name	– When clicked, this button allows you to specify the distinguished name settings.
– IP Address	– In this box, specify the peer's IP address.
Port	This list shows the IPSec peer's protocol ports. A default of *All* secures all protocol ports.
Connect using Secure Gateway Tunnel	If selected, this check box specifies that the IPSec peer is protected by a secure IPSec-compliant gateway, such as a firewall.

Table 6-6 New Connection Pane Field Descriptions (continued)

Field	Description
ID_Type	This list shows the identification type of the gateway including IP address, domain name, and distinguished name. IP Address is the default option. Depending on the option you choose, different values will appear in the right pane.
• IP Address	• This option enables the IP address value box.
– IP address value	– In this box, specify the IP address value.
– Domain Name	– This option enables the domain name value box and the IP Address box.
– Domain name value	– In this box, specify the domain name value.
– IP Address	– In this box, specify the IP Address of the domain.
• Distinguished Name	• This option allows you to specify the name, department, state, and country of the gateway.
– Edit Name	– When clicked, this button allows you to specify the distinguished name settings.
– IP Address	– In this box, specify the gateway's IP address.

Specifying the VPN Client's Identity

To specify the remote party's identity on a VPN Client, you must choose an identity, as follows:

To choose an identity

Step 1 In the left pane, double-click your new connection. In this example, **tohq_sanjose** is clicked.

The new connection expands with My Identity and Security Policy.

Step 2 Click **My Identity**.

The My Identity pane appears in the right pane. Figure 6-12 shows how this is displayed on the My Identity pane. Table 6-6 describes the field descriptions for the My Identity pane.

Step 3 In the right pane, Under My Identity, select the following:

a. From the Select Certificate list, click your digital certificate. In this example, **John's example.com ID** is selected.

b. In the ID_Type list, click **Domain name**.

c. In the Port list, click **All**.

d. In the Name list, click **Any**. The IP Addr list is inactive as a default.

Figure 6-12 My Identity Pane

Table 6-7 My Identity Pane Field Descriptions

Field	Description
Network Security Policy • New Connection>My Identity	Under Network Security Policy, the proposals that will be used to negotiate the authentication and encryption methods are displayed. • This pane allows you to specify the identity of the VPN Client. Choose an identification that will allow the other party to identify you during the key exchange phase.
My Identity	Under My Identity, specify options for determining the identity of the VPN Client. These options include Select Certificate, ID Type, Port and Name lists.
Select Certificate	If you are using digital certification, this list displays all the available digital certificates from which to choose. If you are not using digital certification, *None* is the default option.
ID_Type	This list indicates the IP address option for the VPN Client on the corporate subnet.
• Domain Name	• This box indicates that the VPN Client will be identified by the gateway using the domain name of the certificate identity. This is the default.
Port	This list shows the VPN Client's protocol ports. A default of *All* secures all protocol ports.

Table 6-7 My Identity Pane Field Descriptions (continued)

Field	Description
Local Network Interface	Under Local Network Interface, the hardware interface on the PC or laptop through which the connection will be established.
Name	This list indicates the names of the hardware interfaces on the PC or laptop. A default of *Any* enables all hardware interfaces.
IP Addr	This list indicates the IP addresses of the hardware interfaces on the PC or laptop. A default of *Any* enables all hardware interface IP addresses.
• Pre-Shared Key	• When clicked, this button enables the Pre-Shared Key dialog box. This button is not used while configuring digital certificates.

Configuring Authentication on the VPN Client

To configure authentication on the VPN Client, perform the following tasks:

- Specify Authentication Security Policy
- Specify Authentication for Phase 1 IKE
- Specify Authentication for Phase 2 IKE

To specify authentication security policy

Step 1 In the left pane, under My Identity, double-click **Security Policy**.

The Security Policy pane appears in the right pane.

Step 2 In the right pane, under Security Policy, select the following:

a. Click **Main Mode**.

b. Select the **Enable Replay Detection** check box.

Figure 6-13 shows how this is displayed on the Security Policy pane. Table 6-8 describes the field descriptions for the Security Policy pane.

Figure 6-13 Security Policy Pane

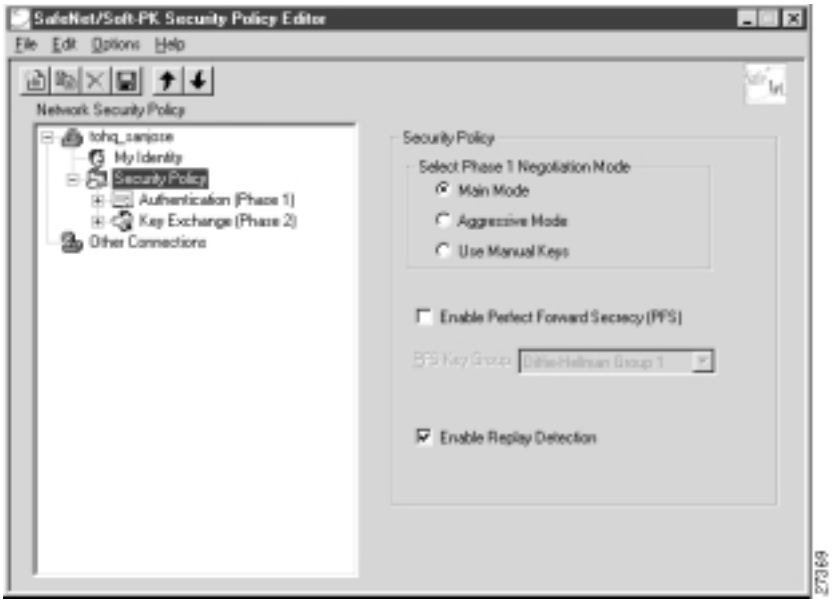


Table 6-8 Security Policy Pane Field Descriptions

Field	Description
Network Security Policy • New Connection>Security Policy	Under Network Security Policy, the proposals that will be used to negotiate the authentication and encryption methods are displayed. • This pane allows you to specify authentication and data integrity.
Security Policy	Under Security Policy, define the Select Phase 1 Negotiation Mode, Enable Perfect Forward Secrecy, or Replay Detection options.
Select Phase 1 Negotiation Mode • Main Mode • Aggressive Mode • Use Manual Keys	Under Select Phase 1 Negotiation Mode, select the mode for authenticating ISAKMP SAs using Main Mode, Aggressive Mode, or Use Manual Key options. • This option allows identities to not be revealed until all secure communications have been established, which requires a longer processing time. • This option allows identities to viewed while secure communications are taking place, which makes for a faster processing time. • This option is available for troubleshooting purposes only.
Enable Perfect Forward Secrecy	When selected, this check box triggers an authentication method protects against repeat compromises of a shared secret key.
Enable Replay Detection	When selected, this check box sets a counter, which determines whether or not a packet is unique to prevent data from being falsified.

To specify authentication for Phase 1 IKE

Step 1 In the left pane, double-click **Security Policy**, and then double-click **Authentication (Phase 1)**. Under Authentication (Phase 1).

A new proposal appears called *Proposal 1*.

Step 2 The Proposal 1 pane appears in the right pane.

In the right pane, under Authentication Method and Algorithms, from the Authentication Method list, **RSA-Signatures** displays.

Step 3 In the right pane, under Authentication Method and Algorithms, select the following:

a. In the Encrypt Alg list, click **DES**.

b. In the Hash Alg list, click **MD5**.

c. In the SA Life list, click **Unspecified**.

d. In the Key Group list, click **Diffie-Hellman Group 1**.

Figure 6-14 shows how this is displayed on the Authentication Phase—Proposal 1 pane for pre-shared key. Table 6-9 describes the field descriptions for the Authentication Phase—Proposal 1 pane for pre-shared key.

Figure 6-14 Authentication (Phase 1)—Proposal 1 Pane

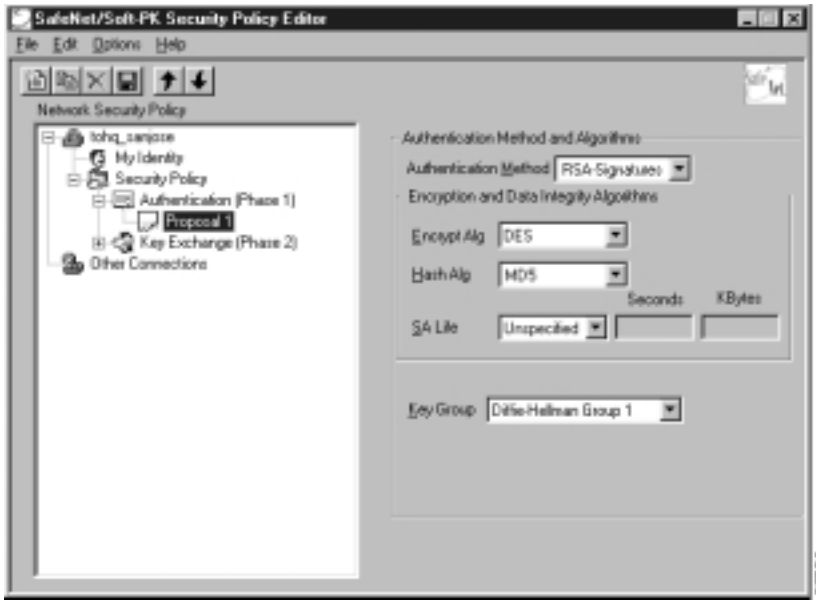


Table 6-9 Authentication (Phase 1)—Proposal 1 Pane Field Descriptions

Field	Description
Network Security Policy • New Connection>Security Policy>Authentication (Phase 1)>Proposal 1	Under Network Security Policy, the proposals that will be used to negotiate the authentication and encryption methods are displayed. • This pane allows you to specify authentication methods for Authentication Phase 1. During Authentication (Phase 1), you and your peer will reveal your identities and negotiate how they will secure Phase 2 communications. Before securing communications, the two peers involved negotiate the method they will use. Proposals are presented to the other peer in the order in which they are sequenced in the Network Security Policy list. You can reorder the proposals after you create them.
Authentication Method and Algorithms	Under Authentication Method and Algorithms, define the authentication method used and authentication and encryption algorithms.
Authentication Method • Pre-Shared Key • RSA Signatures	This list defines the authentication method being used, either Pre-Shared Key or RSA Signatures. The default is the method of authentication selected under My Identity. • This option appears if the method of authentication selected under My Identity is pre-shared key. • This option appears if the method of authentication selected under My Identity is digital certification.
Encryption and Data Integrity Algorithms	Under Encryption and Data Integrity Algorithms, define the algorithms to be used during Phase 1 negotiation including Encrypt Alg, Hash Alg, SA Life, and Key Group.
Encrypt Alg • DES • Triple-DES	This list allows you to specify encryption with DES or Triple DES options. • This option provides minimal security with 56-bit data encryption standard, which uses less processing time than does Triple-DES. • This option allows for maximum security with 168-bit data encryption standard, which uses more processing time than does DES. **Note** Triple DES is only supported within the U.S. domestic versions of both the Cisco IOS software and the VPN Client.

Table 6-9 Authentication (Phase 1)—Proposal 1 Pane Field Descriptions (continued)

Field	Description
Hash Alg • MD5 • SHA-1	This list allows you to specify authentication with MD5 and SHA-1 options. • This option provides minimal authentication with 128-bit digest, which uses less processing time than does SHA. • This option allows for maximum authentication with 160-bit digest, which uses more processing time than does MD5. **Note** Cisco IOS software does not currently support the DES-MAC Hash Algorithm option.
SA Life • Unspecified • Seconds • Kbytes • Both	(Optional) This list allows you to specify the period for which the IKE SA is valid using Unspecified, Seconds, Kbytes, or Both options. **Note** When the VPN Client and gateway participate in IKE Phases 1 and 2 negotiation, the lowest SA life value offered by either device will be used as the agreed-upon value. • This option allows the other IPSec peer to indicate when IKE SA expires. • This option allows you to specify SA life in seconds. • This option allows you to specify SA life in kilobytes. • This option allows you to specify both seconds and kilobytes, whichever comes first, before an SA life expires.
Key Group • Diffie-Hellman Group 1 • Diffie-Hellman Group 2	This list allows you to specify the Diffie-Hellman key exchange using Diffie-Hellman Group 1 or Diffie-Hellman Group 2 options. **Note** Cisco IOS software does not currently support Diffie-Hellman Group 5. • This option enables 768-bit encryption, which requires less processing time than does Diffie-Hellman Group 2. • This option enables 1024-bit encryption, which is more secure than Diffie-Hellman Group 1.

To specify authentication for phase 2 IKE

Step 1 In the left pane, under Authentication (Phase 1), double-click **Key Exchange (Phase 2)**.

In the left pane, under Key Exchange (Phase 2), a new proposal appears called *Proposal 1*.

Step 2 In the right pane, under IPSec Protocols, select the following:

a. In the **SA Life** list, click **Unspecified**.

b. Select the **Encapsulation Protocol (ESP)** check box.

c. In the Encrypt Alg list, click **DES**.

d. In the Hash Alg list, click **MD5**.

e. In the Encapsulation list, click **Tunnel**.

Figure 6-15 Authentication (Phase 2)—Proposal 1 Pane

Table 6-10 Authentication (Phase 2)—Proposal 1 Pane Field Descriptions

Field	Description
Network Security Policy • New Connection>Security Policy>Key Exchange (Phase 2)>Proposal 1	Under Network Security Policy, the proposals that will be used to negotiate the authentication and encryption methods are displayed. • This pane allows you to specify authentication methods for Key Exchange (Phase 2). Set authentication requirements in the Security Policy pane. Negotiate which key exchange method of securing communications you and the other IPSec peer will use by establishing a proposal.
IPSec Protocols	Under IPSec Protocols, define the algorithms to be used during Phase 2 key exchange, including SA Life, Encrypt Alg, Hash Alg, and Encapsulation options.

Table 6-10 Authentication (Phase 2)—Proposal 1 Pane Field Descriptions (continued)

Field	Description
SA Life	This list allows you to specify the period for which the IKE SA is valid using Unspecified, Seconds, Kbytes, or Both options. **Note** When the VPN Client and gateway participate in IKE Phases 1 and 2 negotiation, the lowest SA life value offered by either device will be used as the agreed-upon value.
• Unspecified	• This option allows the other IPSec peer to indicate when IKE SA expires.
• Seconds	• This option allows you to specify SA life in seconds.
• Kbytes	• This option allows you to specify SA life in kilobytes.
• Both	• This option allows you to specify both seconds and kilobytes, whichever comes first, before an SA life expires.
Encapsulation Protocol	If selected, this check box indicates that encryption and authentication will be selected for this proposal.
Encrypt Alg	This list allows you to specify encryption with DES or Triple DES options.
• DES	• This option provides minimal security with 56-bit data encryption standard, which uses less processing time than does Triple-DES.
• Triple-DES	• This option allows for maximum security with 168-bit data encryption standard, which uses more processing time than does DES. **Note** Triple DES is only supported within the U.S. domestic versions of both the Cisco IOS software and the VPN Client.
Hash Alg	This list allows you to specify authentication with MD5 or SHA-1 options.
• MD5	• This option provides minimal authentication with 128-bit digest, which uses less processing time than does SHA. **Note** Cisco IOS software does not currently support the DES-MAC Hash Algorithm option.
• SHA-1	• This option allows for maximum authentication with 160-bit digest, which uses more processing time than does MD5.

Table 6-10 Authentication (Phase 2)—Proposal 1 Pane Field Descriptions (continued)

Field	Description
Encapsulation	This list allows you to specify encapsulation method with Tunnel or Transport options.
• Tunnel	• This option is the only method of secure encapsulation available for the Cisco Secure VPN Client.
• Transport	• This option allows non-IPSec protected encapsulation (when both peers are not using IPSec.) Otherwise, you *must* use the Tunnel option for maximum security.

To save your policy

Step 1 On the **File** menu, click **Save Changes** to save the policy.

The Security Policy Editor dialog box appears. Before your policy is implemented, you must save your policy settings.

Step 2 Click **OK**.

Figure 6-16 shows how this is displayed in the Security Policy Editor dialog box.

Figure 6-16 Security Policy Editor

Task 2—Configuring Digital Certification on the Gateway

To configure digital certification on the gateway, perform the following steps:

- Configuring the Gateway
- Configuring ISAKMP
- Configuring IPSec
- Defining a Dynamic Crypto Map
- Declaring the CA
- Specifying a Public and Private Key

Configuring the Gateway

To configure the gateway, perform the following tasks, as described in Table 6-11:

- Configure the Gateway
- Define a Host Name
- Define a Name Server

Table 6-11 Configuring the Gateway

Command	Purpose
`router> enable`	To enter privileged EXEC mode, enter the **enable** user EXEC command.

`router# configure terminal`
`Enter configuration commands, one per line.`
`End with CNTL/Z.`
	To enter global configuration mode, enter the **configure** privileged EXEC command. To configure the terminal attached at console port, enter the **terminal** keyword.

`router(config)# ip domain-name example.com`	To define a default domain name that the Cisco IOS software uses to complete unqualified host names, use the **ip domain-name** global configuration command. An unqualified host name is a host name without a dotted-decimal domain name. In this example, *example.com* is defined as the default domain name.
`router(config)# hostname hq_sanjose`	To specify or modify the host name for the network server, enter the **hostname** global configuration command. The host name is used in prompts and default configuration filenames. In this example, *hq_sanjose* is defined as the host name. The *hq_sanjose* host name replaces the default *router* host name.
`hq_sanjose(config)# ip name-server 192.168.1.1`	To specify the address of a name server to use for name and address resolution, enter the **ip name-server** global configuration command. In this example, the gateway is defined as the *IP name server*. The gateway's IP address is *192.168.1.1*.

Configuring ISAKMP

To configure ISAKMP on the gateway, perform the following tasks, as described in Table 6-12:

- Configure ISAKMP Policy
- Configure IKE RSA Signatures

Table 6-12 Configuring ISAKMP

Command	Purpose
`hq_sanjose(config)# crypto isakmp policy 3`	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. In this example, the ISAKMP policy is assigned a priority of *3*.
`hq_sanjose(config-isakmp)# encryption des`	To specify the encryption algorithm, use the **encryption (IKE policy)** ISAKMP policy configuration command. The options for encryption are the **des** and **3des** keywords. DES is configured by default for minimum security and fastest processing.
`hq_sanjose(config-isakmp)# hash sha`	To specify the hash algorithm, use the **hash (IKE policy)** ISAKMP policy configuration command. IKE policies define a set of parameters to be used during IKE negotiation. The options for hashing are **sha** and **md5** keywords. SHA is configured by default for maximum authentication with slower processing than MD5.
`hq_sanjose(config-isakmp)# authentication rsa-sig`	To specify the authentication method, use the **authentication (IKE policy**) ISAKMP policy configuration command. The options for authentication method are **rsa-sig**, **rsa-encr**, and **pre-share** keywords. To specify digital certificates as the authentication method, enter the **rsa-sig** keyword.
`hq_sanjose(config-isakmp)# exit`	To exit ISAKMP policy configuration (config-isakmp) command mode, enter the **exit** crypto transform configuration command.

Configuring IPSec

To configure IPSec on the gateway, perform the following tasks, as described in Table 6-13:

- Configure IPSec Transform Set
- Configure IPSec Encapsulation

Table 6-13 Configuring IPSec

Command	Purpose
`hq_sanjose(config)# crypto ipsec transform-set vpn-transform esp-des esp-md5-hmac`	To define a combination of security associations to occur during IPSec negotiations, enter the **crypto ipsec transform-set** global configuration command. This command invokes the crypto transform (cfg-crypto-trans) configuration mode. In this example, the transform set named *vpn-transform* is defined with two security algorithm keywords: **esp-des** and **esp-md5-hmac**. **Note** There are complex rules defining which entries you can use for the transform arguments. These rules are explained in the command description for the **crypto ipsec transform-set** command. You can also use the **crypto ipsec transform-set** global configuration command to view the available transform arguments.
`hq_sanjose(cfg-crypto-trans)# mode tunnel`	(Optional) To specify encapsulation between the gateway and the VPN Client, enter the **mode** crypto transform configuration command. The **mode** command is only applicable to traffic whose source and destination addresses are the IPSec peer addresses; it is ignored for all other traffic. (All other traffic is in tunnel mode only.) The options for encapsulation are **tunnel** and **transport** keywords. Tunnel is configured by default for IPSec encapsulation.
`hq_sanjose(cfg-crypto-trans)# exit`	To exit crypto transform (cfg-crypto-trans) configuration mode, enter the **exit** crypto transform configuration command.

Defining a Dynamic Crypto Map

To define a dynamic crypto map, perform the following tasks, as described in Table 6-14:

- Define a Dynamic Crypto Map Entry
- Add a Dynamic Crypto Map to the Static Crypto Map
- Apply the Crypto Map to the Gateway Interface

Table 6-14 Defining a Dynamic Crypto Map

Command	Purpose
`hq_sanjose(config)# crypto dynamic-map vpn-dynamic 1`	To define a dynamic crypto map entry, enter the **crypto dynamic-map** command. This command invokes the crypto map (config-crypto-map) configuration mode. In this example, the dynamic map name is *vpn-dynamic*, and the sequence number (or priority) is *1*.
`hq_sanjose(config-crypto-map)# set transform-set vpn-transform`	To specify which transform sets are allowed for the crypto map entry, enter the **set transform-set** crypto map configuration command. In this example, the transform set previously defined in Configuring IPSec, *vpn-transform* is applied to the *vpn-dynamic* dynamic crypto map. **Note** You can list multiple transform sets in order of priority (highest priority first).
`hq_sanjose(config-crypto-map)# set security-association lifetime seconds 2700`	(Optional) If you want the security associations for this crypto map to be negotiated using shorter IPSec SA lifetimes than the globally specified lifetimes, specify a key lifetime for the crypto map entry. Specify the IPSec lifetimes using one of the following keywords: **seconds** or **kilobytes**. In this example, the SA lifetime is *2700* seconds.
`hq_sanjose(config-crypto-map)# exit`	To exit crypto map (config-crypto-map) configuration mode, enter the **exit** crypto map configuration command.

Table 6-14 Defining a Dynamic Crypto Map (continued)

Command	Purpose
`hq_sanjose(config)# crypto map vpnclient 1 ipsec-isakmp vpn-dynamic`	To add a dynamic crypto map set to a static crypto map set, use the **crypto map** global configuration command. The crypto map entry references the dynamic crypto map sets. Set the crypto map entries referencing dynamic maps to be the lowest priority entries in a crypto map set (that is, have the highest sequence numbers). In this example, the dynamic map *vpn-dynamic* is added to the crypto map *vpnclient*. The **ipsec-isakmp** keyword indicates IPSec and IKE negotiations are being configured. The crypto map *vpnclient* references the dynamic map *vpn-dynamic* and has a priority of *1* because this is the only crypto map used for this security policy. Otherwise, a higher priority number would have been assigned to this crypto map.
`hq_sanjose(config)# interface ethernet0/0`	To configure an interface, enter the **interface** global configuration command. This command invokes the interface (config-if) configuration mode.
`hq_sanjose(config-if)# ip address 10.1.1.1 255.255.255.0`	To indicate an IP address to the interface, enter the **ip address** interface configuration command. In this example, *10.1.1.1* is specified as the IP address of the Ethernet 0/0 interface.
`hq_sanjose(config-if)# crypto map vpnclient`	To apply a previously defined crypto map set to an interface, enter the **crypto map** interface configuration command. In this example, crypto map *vpnclient* is applied to outbound packets from Ethernet interface 0/0.
`hq_sanjose(config-if)# exit`	To exit interface (config-if) configuration mode, enter the **exit** interface configuration command.

Declaring the CA

To enroll your certificate with a CA, perform the following tasks, as described in Table 6-15:

- Specify the CA
- Specify Compatibility with CA's RA
- Specify CA's Enrollment URL
- Specify LDAP Support
- Specify CRL Option

Table 6-15 Declare the CA

Command	Purpose
`hq_sanjose(config)# crypto ca identity example.com`	To declare the CA your router should use, enter the **crypto ca identity** global configuration command. This command invokes the ca-identity (cfg-ca-id) configuration mode. In this example, *example.com* is defined as the domain name for which this certificate is requested.
`hq_sanjose(cfg-ca-id)# enrollment mode ra`	To indicate compatibility with the CA's Registration Authority (RA) system, enter the **enrollment mode ra** ca-identity configuration command.
`hq_sanjose(cfg-ca-id)# enrollment url http://ca-server`	To specify the CA's location where your router should send certificate requests by indicating the CA's enrollment URL, enter the **enrollment url** ca-identity configuration command. In this example, *http://ca-server* is specified as the CA server.
`hq_sanjose(cfg-ca-id)# query url http://ca-server`	To specify Lightweight Directory Access Protocol (LDAP) support, enter the **query url** ca-identity configuration command. This command is required if your CA supports both RA and LDAP. LDAP is a query protocol used when the router retrieves certificates and CRLs. The default query protocol is Certificate Enrollment Protocol (CEP). In this example, *http://ca-server* is specified as the LDAP server.
`hq_sanjose(cfg-ca-id)# crl optional`	To allow other peers' certificates to still be accepted by your router even if the appropriate Certificate Revocation List (CRL) is not accessible to your router, use the **crl optional** ca-identity configuration command.
`hq_sanjose(cfg-ca-id)# exit`	To exit ca-identity (cfg-ca-id) configuration mode, enter the **exit** ca-identity configuration command.

Specifying a Public and Private Key

To specify a public and private key, perform the following tasks, as described in Table 6-16:

- Generate the Public and Private Key on the Gateway
- Receive the CA Public Key and CA Server Certificate
- Send the Gateway Public Key
- Receive the Signed Gateway Certificate
- Enroll the Gateway Certificate with the CA

Table 6-16 Specify a Public and Private Key

Command	Purpose

`hq_sanjose(config)# crypto key generate rsa usage-keys`
`mod 512 [signature key]`
`mod 512 [encryption key]`
	To generate the public and the private keys, enter the **crypto key generate rsa** global configuration command. This command creates two key-pairs for RSA:
	• One key-pair for digital signatures
	• One key-pair for encryption
	A key-pair refers to a public key and its corresponding secret key. If you do not specify the **usage-keys** keyword at the end of the command, the router will generate only one RSA key-pair and use it for both digital signatures and encryption.

`hq_sanjose(config)# crypto ca authenticate example.com`
`Certificate has the following attributes:`
`Fingerprint: 103FXXXX 9D64XXXX 0AE7XXXX 626AXXXX`
`% Do you accept this certificate? [yes/no]:yes`
	To receive the public key and CA server certificate and authenticate the CA (by receiving the CA's certificate), use the **crypto ca authenticate** global configuration command.
	In this example, *example.com* is defined as the domain name for which this certificate is authenticated.
	At this point the router has a copy of the CA's certificate.
	In this example, *yes* is entered to accept the certificate.

Table 6-16 Specify a Public and Private Key (continued)

Command	Purpose
hq_sanjose(config)# **crypto ca enroll example.com** 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.example.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: **ethernet0/0** 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	To send the gateway's public key and receive a signed certificate from the CA server, enter the **crypto ca enroll** global configuration command. In this example, *example.com* is defined as the domain name for which this certificate is received. **Note** This is message text. This text 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 CA administrator's approval. The router will be polling every 2 minutes for the availability of the certificate. In this example, *cisco1234* is entered as the challenge password. Should you choose to revoke your certificate, the CA must be provided with this challenge password. In this example, *hq_sanjose.example.com* is entered as the name server and domain name to which this digital certificate applies. In this example, *yes* is entered to indicate the router serial number is to be included in the subject name. The serial number is not used by IPSec or IKE but may be used by the CA to either authenticate certificates or to later associate a certificate with a particular router In this example, *yes* is entered to indicate the IP address is to be included in the subject name. Normally, you would not include the IP address because the IP address binds the certificate more tightly to a specific entity. Also, if the router is moved, you would need to issue a new certificate. Finally, a router has multiple IP addresses, any of which might be used with IPSec. In this example, the *ethernet 0/0* interface for the IP address specified is entered. This interface should correspond to the interface to which you apply your crypto map set. In this example, *yes* is entered to request the certificate. Wait until the router has retrieved the certificate. The router will display a message informing you that the certificate has been loaded.

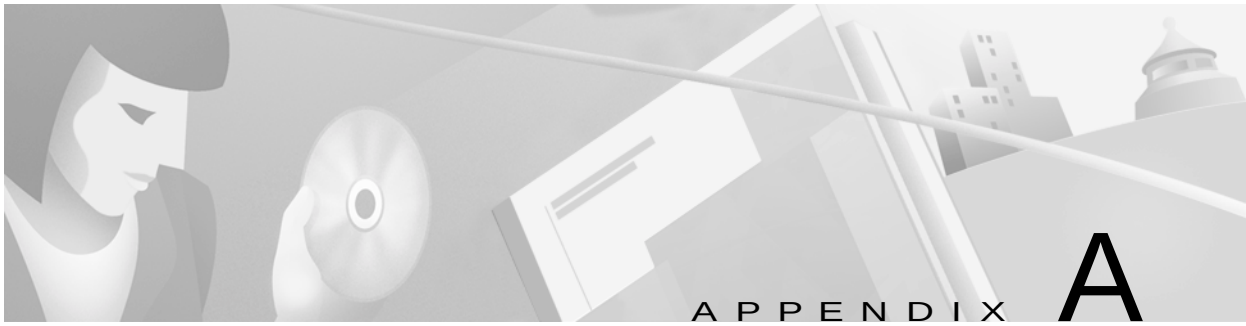
Related Documentation

For more information on digital certification, refer to the “Digital Certification” section in Chapter 2, “Case Study for Layer 3 Authentication and Encryption.”

For more information on configuring Cisco IOS software commands, refer to the “Cisco IOS Software Documentation Set” section in the “Preface.”

For more information SCEP, refer to the following URL:

http://www.cisco.com/warp/public/cc/cisco/mkt/security/tech/scep_wp.htm



Configuring Entrust Digital Certificates

This appendix provides additional information on requesting digital certification from the Entrust CA server and configuring ca-identity configuration commands on your gateway. Use this appendix with Chapter 6, “Configuring Digital Certification,” and the enrollment procedures on the Entrust web site.

Entrust Certificate Authority

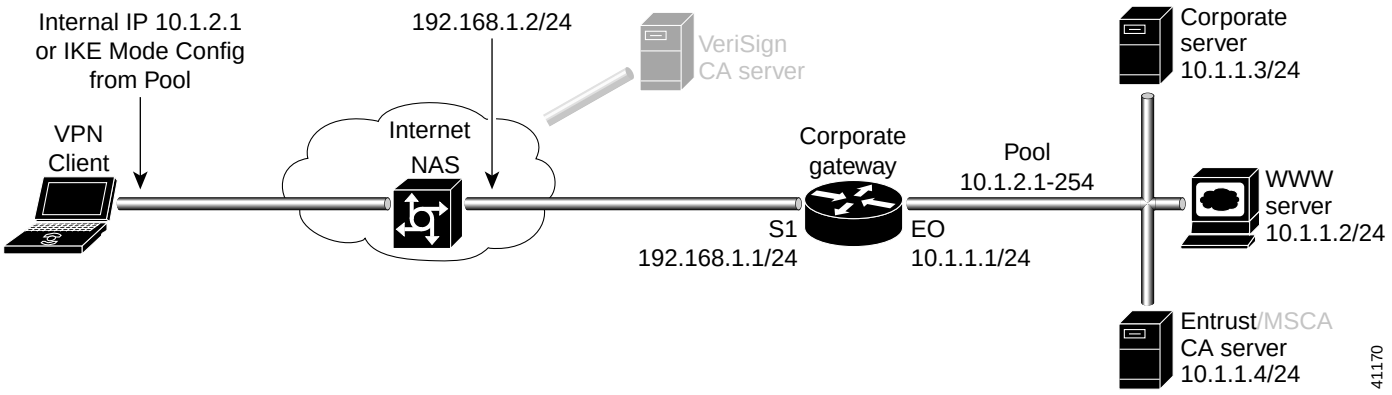
This CA requires that both IPSec peers transact with a Registration Authority (RA), which then forwards the requests through to the CA. Both the remote IPSec peer and the local IPSec peer must be configured with the both the CA and RA public keys. The CA and RA public keys are signature and encryption key pairs, which must be generated and enrolled for authentication to occur.

For information on configuring Entrust CA, see the following URLs:

- On configuring Entrust/VPN Connector:
  http://www.entrust.com/entrust/vpnconnect/
- On configuring Certificate Enrollment Protocol and Entrust:
  http://freecerts.entrust.com/vpncerts/cep.htm
- On Configuring a Networking Device with Entrust/VPN Connector:
  http://freecerts.entrust.com/vpncerts/cep_config.htm

Note While Cisco Secure VPN Client supports Entrust, the Entrust enrollment method is subject to change over time. Please see the Entrust web site at http://www.entrust.com for the current enrollment method.

Figure A-1 Entrust CA Server Topology



Configuring Entrust CA Identity on the Gateway

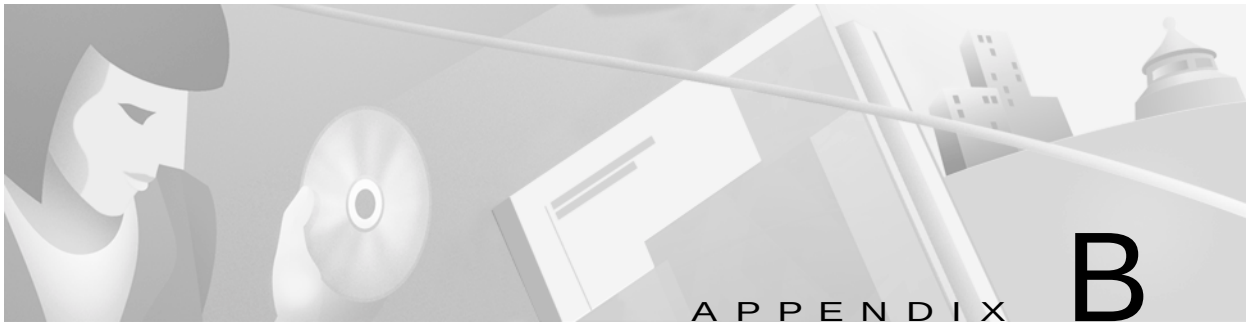
This step corresponds to the "Declaring the CA" section in Chapter 6, "Configuring Digital Certification."

To enroll your certificate with a CA, perform the following tasks, as described in Table A-1:

- Specify the CA
- Specify Compatibility with CA's RA
- Specify CA's Enrollment URL
- Specify LDAP Support
- Specify CRL Option

Table A-1 Declare the CA

Command	Purpose
`hq_sanjose(config)# crypto ca identity example.com`	To declare the CA your router should use, enter the **crypto ca identity** global configuration command. This command invokes the ca-identity (cfg-ca-id) configuration mode. In this example, *example.com* is defined as the domain name for which this certificate is requested.
`hq_sanjose(cfg-ca-id)# enrollment mode ra`	To indicate compatibility with the CA's Registration Authority (RA) system, enter the **enrollment mode ra** ca-identity configuration command.
`hq_sanjose(cfg-ca-id)# enrollment url http://entrust-ca`	To specify the CA's location where your router should send certificate requests by indicating the CA's enrollment URL, enter the **enrollment url** ca-identity configuration command. In this example, *http://entrust-ca* is specified as the CA server.
`hq_sanjose(cfg-ca-id)# query url http://entrust-ca`	To specify Lightweight Directory Access Protocol (LDAP) support, enter the **query url** ca-identity configuration command. This command is required if your CA supports both RA and LDAP. LDAP is a query protocol used when the router retrieves certificates and CRLs. The default query protocol is Certificate Enrollment Protocol (CEP). In this example, *http://entrust-ca* is specified as the LDAP server.
`hq_sanjose(cfg-ca-id)# crl optional`	To allow other peers' certificates to still be accepted by your router even if the appropriate Certificate Revocation List (CRL) is not accessible to your router, use the **crl optional** ca-identity configuration command.
`hq_sanjose(cfg-ca-id)# exit`	To exit ca-identity (cfg-ca-id) configuration mode, enter the **exit** ca-identity configuration command.



APPENDIX B

Configuring Microsoft Certificate Services

This appendix provides additional information on requesting digital certification from the Microsoft CA server and configuring ca-identity configuration commands on your gateway. Use this appendix with Chapter 6, “Configuring Digital Certification.”

Microsoft Certificate Services

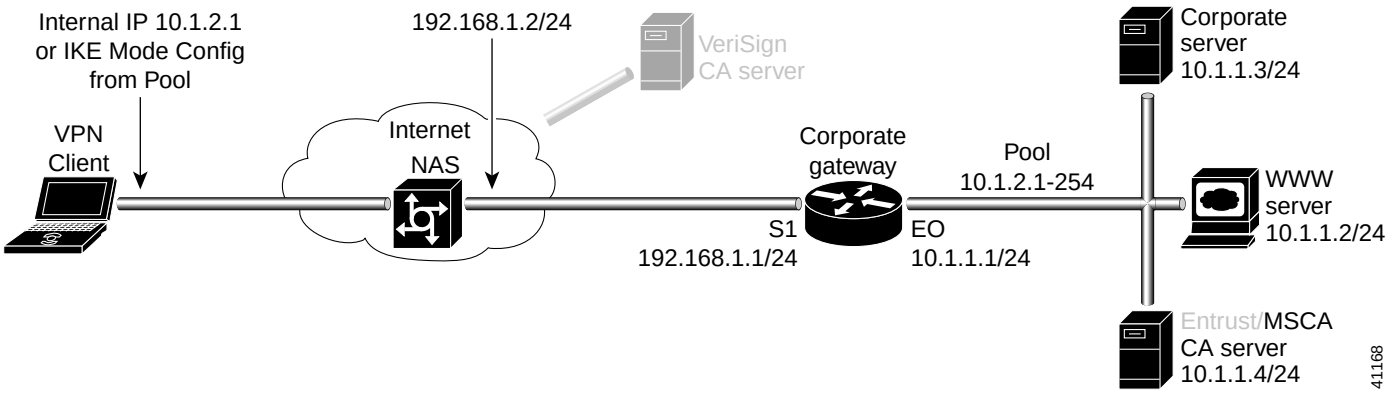
This CA requires that both IPSec peers transact with a Registration Authority (RA), which then forwards the requests through to the CA. Both the remote IPSec peer and the local IPSec peer must be configured with the both the CA and RA public keys. The CA and RA public keys are signature and encryption key pairs, which must be generated and enrolled for authentication to occur.

For information on configuring Microsoft Certificate Services, see the following URLs:

- On Setting up a Certificate Authority:
  http://www.microsoft.com/windows2000/library/planning/security/casetupsteps.asp
- On Microsoft Certificate Services Web Pages:
  http://www.microsoft.com/windows2000/library/planning/security/cawebsteps.asp
- On Administering Microsoft Certificate Services:
  http://www.microsoft.com/windows2000/library/planning/security/adminca.asp

Note While Cisco Secure VPN Client supports Microsoft Certificate Services, these enrollment methods are subject to change over time. Please see the Microsoft web site at http://www.microsoft.com for the current enrollment method.

Figure B-1 Microsoft CA Server Topology



Configuring Microsoft CA Identity on Gateway

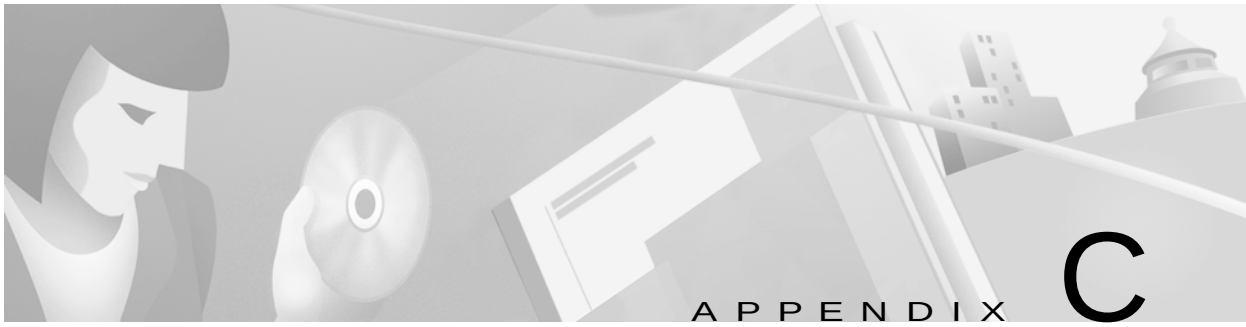
This step corresponds to "Declaring the CA" in Chapter 6, "Configuring Digital Certification."

To enroll your certificate with a Microsoft CA, perform the following tasks, as described in Table B-1:

- Specify the CA
- Specify Compatibility with CA's RA
- Specify CA's Enrollment URL
- Specify LDAP Support
- Specify CRL Option

Table B-1 Declare the CA

Command	Purpose
`hq_sanjose(config)# crypto ca identity example.com`	To declare the CA your router should use, enter the **crypto ca identity** global configuration command. This command invokes the ca-identity (cfg-ca-id) configuration mode. In this example, *example.com* is defined as the domain name for which this certificate is requested.
`hq_sanjose(cfg-ca-id)# enrollment mode ra`	To indicate compatibility with the CA's Registration Authority (RA) system, enter the **enrollment mode ra** ca-identity configuration command.
`hq_sanjose(cfg-ca-id)# enrollment url http://microsoft-ca`	To specify the CA's location where your router should send certificate requests by indicating the CA's enrollment URL, enter the **enrollment url** ca-identity configuration command. In this example, *http://microsoft-ca* is specified as the CA server.
`hq_sanjose(cfg-ca-id)# query url http://microsoft-ca`	To specify Lightweight Directory Access Protocol (LDAP) support, enter the **query url** ca-identity configuration command. This command is required if your CA supports both RA and LDAP. LDAP is a query protocol used when the router retrieves certificates and CRLs. The default query protocol is Certificate Enrollment Protocol (CEP). In this example, *http://microsoft-ca* is specified as the LDAP server.
`hq_sanjose(cfg-ca-id)# crl optional`	To allow other peers' certificates to still be accepted by your router even if the appropriate Certificate Revocation List (CRL) is not accessible to your router, use the **crl optional** ca-identity configuration command.
`hq_sanjose(cfg-ca-id)# exit`	To exit ca-identity (cfg-ca-id) configuration mode, enter the **exit** ca-identity configuration command.



APPENDIX C

Configuring VeriSign Digital Certificates

This appendix provides additional information on requesting digital certification from the VeriSign CA server and configuring ca-identity configuration commands on your gateway. Use this appendix with Chapter 6, "Configuring Digital Certification," and the enrollment guide on the VeriSign web site.

VeriSign Certificate Authority

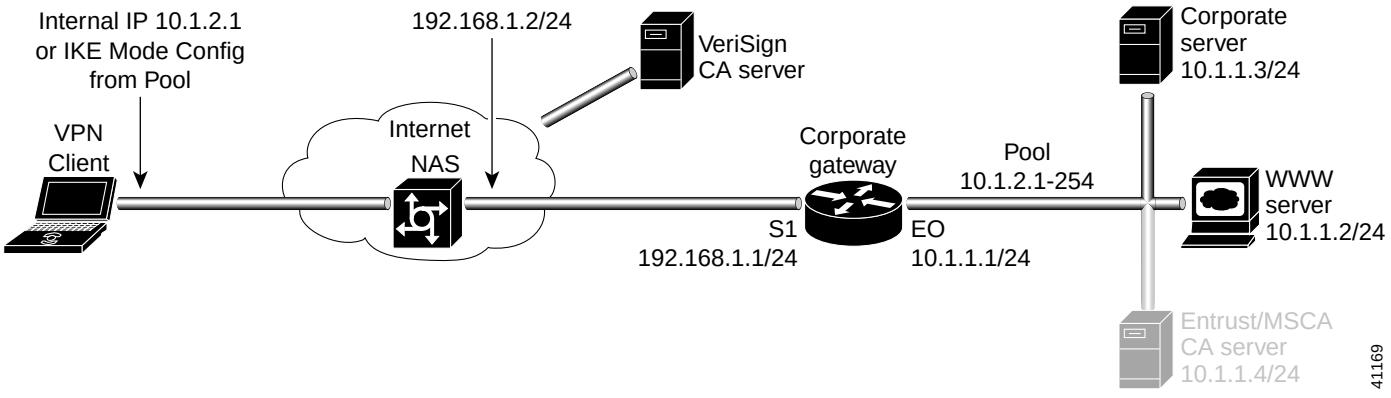
This CA provides certificate processing, backup, key recovery, and customer support. The gateway administrator handles approval, enrollment, validation, issuance, and renewal of digital certificates.

This section includes the following topics:

- Sending Certification Request to VeriSign CA Server
- Configuring VeriSign CA Identity on Gateway

Note While Cisco Secure VPN Client supports VeriSign, the VeriSign enrollment method is subject to change over time. Please see the Verisign web site at http://www.verisign.com for the current enrollment method.

Figure C-1 VeriSign CA Server Topology



Sending Certification Request to VeriSign CA Server

This step corresponds to "Sending the Certification Request to the CA Server" in Chapter 6, "Configuring Digital Certification." For details on submitting a VeriSign certificate request to the Verisign CA, see the following URL: http://www.verisign.com/onsite/ipsec/ciscoIntro.html

Configuring VeriSign CA Identity on Gateway

This step corresponds to "Declaring the CA" in Chapter 6, "Configuring Digital Certification."

To enroll your certificate with a VeriSign CA, perform the following tasks as described in Table C-1:

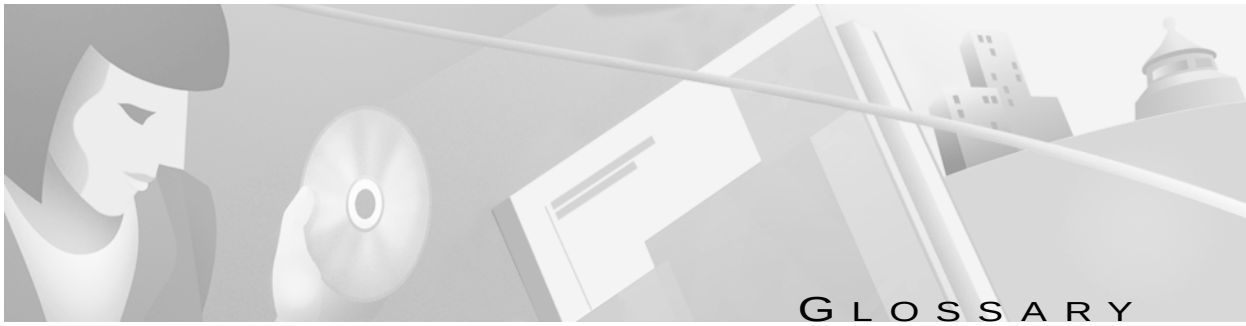
- Specify the CA
- Specify Compatibility with CA's RA
- Specify CA's Enrollment URL
- Specify LDAP Support
- Specify CRL Option

Table C-1 Declare the CA

Command	Purpose
`hq_sanjose(config)# crypto ca identity example.com`	To declare the CA your router should use, enter the **crypto ca identity** global configuration command. This command invokes the ca-identity (cfg-ca-id) configuration mode. In this example, *example.com* is defined as the domain name for which this certificate is requested.
`hq_sanjose(cfg-ca-id)# enrollment mode ra`	To indicate compatibility with the CA's Registration Authority (RA) system, enter the **enrollment mode ra** ca-identity configuration command.
`hq_sanjose(cfg-ca-id)# enrollment url http://onsiteipsec.VeriSign.com`	To specify the CA's location where your router should send certificate requests by indicating the CA's enrollment URL, enter the **enrollment url** ca-identity configuration command. In this example, *http://onsiteipsec.VeriSign.com* is specified as the CA server.
`hq_sanjose(cfg-ca-id)# query url http://onsiteipsec.VeriSign.com`	To specify Lightweight Directory Access Protocol (LDAP) support, enter the **query url** ca-identity configuration command. This command is required if your CA supports both RA and LDAP. LDAP is a query protocol used when the router retrieves certificates and CRLs. The default query protocol is Certificate Enrollment Protocol (CEP). In this example, *http://onsiteipsec.VeriSign.com* is specified as the LDAP server.

Table C-1 Declare the CA (continued)

Command	Purpose
`hq_sanjose(cfg-ca-id)# crl optional`	To allow other peers' certificates to still be accepted by your router even if the appropriate Certificate Revocation List (CRL) is not accessible to your router, use the **crl optional** ca-identity configuration command.
`hq_sanjose(cfg-ca-id)# exit`	To exit ca-identity (cfg-ca-id) configuration mode, enter the **exit** ca-identity configuration command.



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, data integrity, and optional anti-replay services. AH is embedded in the data to be protected (a full IP datagram).

AH does not provide confidentiality. AH does not provide encryption, only authentication.

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.
RFC 2402 is the latest version of AH.

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 software has implemented the mandatory MD5 and SHA (HMAC variants) authentication algorithms.

The updated AH protocol provides anti-replay services.

AH (HMAC-MD5) AH (HMAC-MD5). Authentication Header (Keyed-Hashing for Message Authentication-Message Digest 5). See AH.

MD5 provides source authentication for each network packet using the HMAC-MD5 hash algorithm. Also, provides optional anti-replay services, in which a receiving peer can protect itself against replay attacks by denying old or duplicate packets.

MD5 performs faster and provides less secure authentication than does SHA.

RFC 2402 is the latest version of AH.
RFC 2403 is the latest version of MD5.

A (continued)

AH (HMAC-SHA) AH (HMAC-SHA). Authentication Header (Keyed-Hashing for Message Authentication-Secure Hash Algorithm). See AH.

Provides source authentication for each network packet using the HMAC-SHA hash algorithm. Also, provides optional anti-replay services, in which a receiving peer can protect itself against replay attacks by denying old or duplicate packets.

SHA provides more secure authentication and performs slower than does MD5.

RFC 2402 is the latest version of AH.
RFC 2404 is the latest version of SHA.

Aggressive Mode This mode during IKE negotiation is quicker than Main Mode because it eliminates several steps when the communicating parties are negotiating authentication (Phase 1).

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 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 D&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.

DNS Domain Name System. System used in the Internet for translating names of network nodes into addresses.

D (continued)

data confidentiality 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).

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.

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.

With Diffie- Hellman key exchange, a public and private key can be combined to create a shared secret between two peers. Using Diffie-Hellman, you can establish session keys for IKE negotiation. Valid values for this setting are as follows:

Diffie-Hellman Group 1 enables 768-bit encryption, which requires less processing time than does Diffie-Hellman Group 2.

Diffie-Hellman Group 2 enables 1024-bit encryption, which is more secure than Diffie-Hellman Group 1.

You should choose either option based on compatibility, available processing power, and security concerns. Not all vendors support Diffie-Hellman group 2. Diffie-Hellman group 2 is also significantly more CPU intensive than Diffie-Hellman group 1; therefore, you would not want to use Diffie-Hellman group 2 on low-end devices. Diffie-Hellman group 2 is more secure than Diffie-Hellman group 1.

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).

Domain Name System See DNS.

D (continued)

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. Dynamic addresses are obtained by devices when they attach to a network, by means of some protocol-specific process. A device using a dynamic address often has a different address each time it connects to the network.

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, data integrity, and protection services, optional data origin authentication, and anti-replay services. ESP encapsulates the data to be protected. ESP can be used either by itself or in conjunction with AH. ESP can be configured with DES or Triple DES.

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.
RFC 2406 documents the latest version of ESP.

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 software 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-CBC) ESP (DES-CBC). Encapsulation (Data Encryption Standard-Cipher Block Chaining) encryption algorithm. See ESP.

DES-CBC provides 56-bit basic encryption with the updated ESP protocol, anti-replay services, and can be used with various cipher and authentication algorithms.

DES performs faster and provides less secure encryption than does Triple DES.

Supported combined with HMAC-MD5 or HMAC-SHA.

RFC 2406 documents the latest version of ESP.
RFC 2405 documents the latest version of ESP CBC.

E (continued)

ESP (HMAC-MD5) ESP (HMAC-MD5). Encapsulation with Authentication Header (Keyed-Hashing for Message Authentication-Message Digest 5) encryption and authentication algorithm. See ESP and AH.

HMAC-MD5 provides source authentication for each network packet using the HMAC-MD5 hash algorithm. Also, provides optional anti-replay services, in which a receiving peer can protect itself against replay attacks by denying old or duplicate packets.

MD5 performs faster and provides less secure authentication than does SHA.

Supported combined with DES-CBC.

RFC 2406 documents the latest version of ESP.
RFC 2403 documents the latest version of MD5.

ESP (HMAC-SHA) ESP(HMAC-SHA). Encapsulation with Authentication Header (Keyed-Hashing for Message Authentication-Secure Hash Algorithm) encryption and authentication algorithm. See ESP and AH.

SHA provides source authentication for each network packet using the HMAC-SHA hash algorithm. Also, provides optional anti-replay services, in which a receiving peer can protect itself against replay attacks by denying old or duplicate packets.

SHA provides more secure authentication and performs slower than does MD5.

Supported combined with DES-CBC and Triple-DES.

RFC 2406 documents the latest version of ESP.
RFC 2404 documents the latest version of SHA.

ESP (Triple DES) ESP (Triple DES). Encapsulation (Triple Data Encryption Standard) encryption algorithm. See ESP.

Triple DES provides 168-bit encryption and processes each cipher block three times with three different keys to increase encryption strength.

Triple DES provides more secure encryption and performs slower than does DES-CBC.

Supported combined with HMAC-MD5 or HMAC-SHA.

RFC 2406 documents the latest version of ESP.

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.

SHA produces a 160-bit digest, which is more resistant to brute-force attacks than MD5. It is recommended that you use SHA for a more secure authentication.

MD5 produces a 128-bit digest, which uses less processing time than does SHA. It is recommended that you use SHA for a more secure authentication.

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 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.

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.

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.

I (continued)

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.

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.

RFC 2401 documents IP Security Architecture.

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 Message Digest 5. 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.

SHA is more secure than MD4 and MD5. Cisco uses hashes for authentication within the IPSec framework.

RFC 2403 documents the latest version of MD5.

Main Mode This mode ensures the highest level of security when the communicating parties are negotiating authentication (phase 1).

Manual Keys This mode requires no negotiations; it is available for troubleshooting only.

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 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.

See also repudiation.

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.

Perfect Forward Secrecy Perfect forward secrecy (PFS) is a cryptographic characteristic associated with a derived shared secret value. With PFS, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys.

PKI Public Key Infrastructure. Software, encryption and authentication technologies, and services that allows secure communications for enterprises over the Internet. Consists of

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. Pre-shared keys are simpler to configure, but less scalable than digital certification.

P (continued)

PSTN Public Switched Telephone Network. 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.

public key infrastructure See PKI.

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

RA Registration Authority. A server that acts as a proxy for the CA so that CA functions can continue when the CA is offline.

Registration Authority See RA.

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).

SCEP Simple Certificate Enrollment Protocol. A PKI communication protocol which leverages existing technology by using PKCS #7 and PKCS #10.

Secure Hash Algorithm See SHA.

Security Association See SA.

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.

RFC 2404 documents the latest version of SHA.

Simple Certificate Enrollment Protocol See SCEP.

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. SPI has a 32-bit value.

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. Static addresses are assigned by a network administrator according to a preconceived Internetwork addressing plan. A static address does not change until the network administrator manually changes it.

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. Transport mode is typically used in a host-to-host connection.

Triple DES See 3DES.

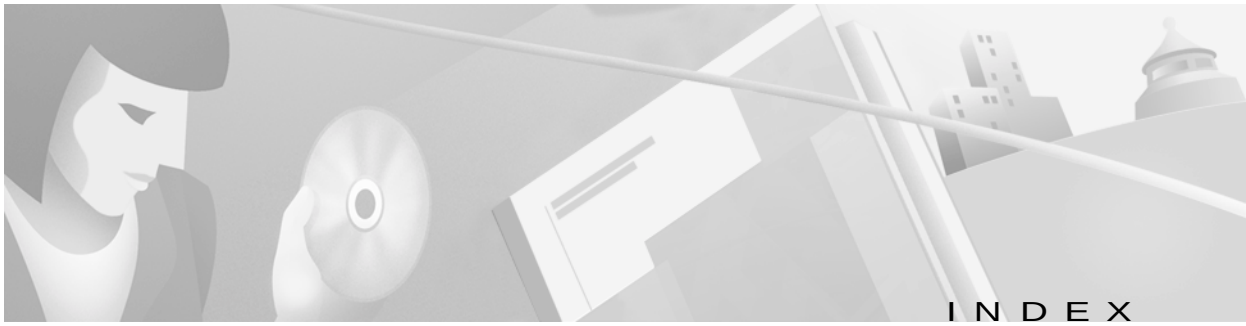
tunnel A secure communication path between two peers, such as a client and a router.

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. Tunnel mode is typically used in a gateway-to-gateway connection.

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.



L

M

N

P

S

T

U

V

W