

VPN 3000 Series Concentrator Reference Volume I: Configuration

Release 3.6
August 2002

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

Customer Order Number: DOC-7814741=
Text Part Number: 78-14741-01



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

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

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

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

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

CCIP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0206R)

VPN 3000 Series Concentrator Reference Volume I: Configuration

Copyright © 2002, Cisco Systems, Inc.

All rights reserved.



Preface ix

- Audience ix
- Prerequisites ix
- Organization x
- Related Documentation xii
- Conventions xiv
- Obtaining Documentation xvi
- Obtaining Technical Assistance xvii

CHAPTER 1

Using the VPN Concentrator Manager 1-1

- Browser Requirements 1-2
- Connecting to the VPN Concentrator Using HTTP 1-4
- Installing the SSL Certificate in Your Browser 1-5
- Connecting to the VPN Concentrator Using HTTPS 1-20
- Logging into the VPN Concentrator Manager 1-21
- Configuring HTTP, HTTPS, and SSL Parameters 1-22
- Organization of the VPN Concentrator Manager 1-22
- Navigating the VPN Concentrator Manager 1-23

CHAPTER 2

Configuration 2-1

- Configuration 2-1

CHAPTER 3

Interfaces 3-1

- Interfaces 3-2
- Interfaces | Power 3-6
- Interfaces | Ethernet 1 2 3 3-9
 - General Parameters Tab 3-10
 - RIP Parameters Tab 3-15
 - OSPF Parameters Tab 3-17
 - Bandwidth Parameters Tab 3-20

CHAPTER 4

System Configuration 4-1

System 4-1

CHAPTER 5

Servers 5-1

Servers 5-1

Servers | Authentication 5-2

Servers | Authentication | Add or Modify 5-5

Servers | Authentication | Delete 5-12

Servers | Authentication | Test 5-13

Servers | Accounting 5-16

Servers | Accounting | Add or Modify 5-18

Servers | DNS 5-20

Servers | DHCP 5-22

Servers | DHCP | Add or Modify 5-24

Servers | Firewall 5-25

Servers | NTP 5-26

Servers | NTP | Parameters 5-27

Servers | NTP | Hosts 5-28

Servers | NTP | Hosts | Add or Modify 5-29

CHAPTER 6

Address Management 6-1

Address Management 6-2

Address Management | Assignment 6-3

Address Management | Pools 6-5

Address Management | Pools | Add or Modify 6-6

CHAPTER 7

Tunneling Protocols 7-1

Tunneling Protocols 7-2

Tunneling Protocols | PPTP 7-3

Tunneling Protocols | L2TP 7-6

Tunneling Protocols | IPsec 7-9

Tunneling Protocols | IPsec | LAN-to-LAN 7-11

Tunneling Protocols | IPsec | LAN-to-LAN | No Public Interfaces 7-13

Tunneling Protocols | IPsec | LAN-to-LAN | Add or Modify 7-14

Tunneling Protocols | IPsec | LAN-to-LAN | Add | Local or Remote Network List 7-23

Tunneling Protocols | IPsec | LAN-to-LAN | Add | Done 7-25

Tunneling Protocols IPSec IKE Proposals	7-26
Tunneling Protocols IPSec IKE Proposals Add, Modify, or Copy	7-30
Tunneling Protocols IPSec NAT Transparency	7-34

CHAPTER 8**IP Routing 8-1**

IP Routing	8-2
IP Routing Static Routes	8-3
IP Routing Static Routes Add or Modify	8-5
IP Routing Default Gateways	8-7
IP Routing OSPF	8-9
IP Routing OSPF Areas	8-11
IP Routing OSPF Areas Add or Modify	8-12
IP Routing DHCP Parameters	8-14
IP Routing DHCP Relay	8-16
IP Routing Redundancy	8-18
IP Routing Reverse Route Injection	8-21

CHAPTER 9**Management Protocols 9-1**

Management Protocols	9-1
Management Protocols FTP	9-2
Management Protocols HTTP/HTTPS	9-4
Management Protocols TFTP	9-6
Management Protocols Telnet	9-8
Management Protocols SNMP	9-10
Management Protocols SNMP Communities	9-12
Management Protocols SNMP Communities Add or Modify	9-13
Management Protocols SSL	9-14
Management Protocols SSH	9-18
Management Protocols XML	9-20

CHAPTER 10**Events 10-1**

Event Class	10-1
Event Severity Level	10-4
Event Log	10-5
Event	10-6
Events General	10-7

- Events | FTP Backup 10-13
- Events | Classes 10-15
- Events | Classes | Add or Modify 10-17
- Events | Trap Destinations 10-20
- Events | Trap Destinations | Add or Modify 10-22
- Events | Syslog Servers 10-24
- Events | Syslog Servers | Add or Modify 10-25
- Events | SMTP Servers 10-27
- Events | SMTP Servers | Add or Modify 10-29
- Events | Email Recipients 10-30
- Events | Email Recipients | Add or Modify 10-32

CHAPTER 11

General 11-1

- General 11-1
- General | Identification 11-2
- General | Time and Date 11-3
- General | Sessions 11-5
- General | Global Authentication Parameters 11-6

CHAPTER 12

Client Update 12-1

- Client Update 12-2
- Client Update | Enable 12-3
- Client Update | Entries 12-4
- Client Update | Entries | Add or Modify 12-5

CHAPTER 13

Load Balancing Cisco VPN Clients 13-1

- Preliminary Steps 13-2
- Load Balancing 13-4

CHAPTER 14

User Management 14-1

- User Management 14-3
- User Management | Base Group 14-4
 - General Parameters Tab 14-4
 - IPSec Parameters Tab 14-9
 - Client Configuration Parameters Tab 14-16
 - Client FW Parameters Tab 14-24

HW Client Parameters Tab	14-29
PPTP/L2TP Parameters Tab	14-35
User Management Groups	14-41
User Management Groups Add or Modify (Internal)	14-43
Identity Parameters Tab	14-44
General Parameters Tab	14-46
IPSec Parameters Tab	14-51
Client Configuration Parameters Tab	14-57
Client FW Parameters Tab	14-63
HW Client Parameters Tab	14-68
PPTP/L2TP Parameters Tab	14-74
User Management Groups Modify (External)	14-80
User Management Groups Authentication Servers	14-82
User Management Groups Authentication Servers Add or Modify	14-84
User Management Groups Authentication Servers Test	14-91
User Management Groups Accounting Servers	14-94
User Management Groups Accounting Servers Add or Modify	14-96
User Management Groups Address Pools	14-98
User Management Groups Address Pools Add or Modify	14-99
User Management Groups Client Update	14-100
User Management Groups Client Update Add or Modify	14-101
User Management Groups Bandwidth Policy	14-103
User Management Groups Bandwidth Policy Interfaces	14-104
User Management Users	14-105
User Management Users Add or Modify	14-107
Identity Parameters Tab	14-108
General Parameters Tab	14-110
IPSec Parameters Tab	14-114
PPTP/L2TP Parameters Tab	14-116

CHAPTER 15**Policy Management 15-1**

Policy Management	15-2
Policy Management Access Hours	15-3
Policy Management Access Hours Add or Modify	15-4
Policy Management Traffic Management	15-6
Policy Management Traffic Management Network Lists	15-7
Policy Management Traffic Management Network Lists Add, Modify, or Copy	15-9

Policy Management | Traffic Management | Rules **15-11**

Policy Management | Traffic Management | Rules | Add, Modify, or Copy **15-15**

Policy Management | Traffic Management | Rules | Delete **15-23**

Policy Management | Traffic Management | Security Associations **15-24**

Policy Management | Traffic Management | Security Associations | Add or Modify **15-29**

Policy Management | Traffic Management | Security Associations | Delete **15-35**

Policy Management | Traffic Management | Filters **15-36**

Policy Management | Traffic Management | Filters | Add, Modify, or Copy **15-39**

Policy Management | Traffic Management | Assign Rules to Filter **15-42**

Policy Management | Traffic Management | Assign Rules to Filter | Add SA to Rule **15-45**

Policy Management | Traffic Management | Assign Rules to Filter | Change SA on Rule **15-47**

Policy Management | Traffic Management | NAT **15-49**

Policy Management | Traffic Management | NAT | Enable **15-50**

Policy Management | Traffic Management | NAT | Interface Rules **15-51**

Policy Management | Traffic Management | NAT | Rules | No Public Interfaces **15-53**

Policy Management | Traffic Management | NAT | Interface Rules | Add or Modify **15-54**

Policy Management | Traffic Management | NAT | LAN-to-LAN Rules **15-56**

Policy Management | Traffic Management | NAT | LAN-to-LAN Rules | Add or Modify **15-60**

Policy Management | Traffic Management | Bandwidth Policies **15-63**

Policy Management | Traffic Management | Bandwidth Policies | Add or Modify **15-64**

Policy Management | Certificate Group Matching **15-71**

Policy Management | Certificate Group Matching | Rules **15-72**

Policy Management | Certificate Group Matching | Rules | Add or Modify **15-74**

Policy Management | Certificate Group Matching | Policy **15-77**

Index

Index



Preface

The VPN Concentrator provides an HTML-based graphic interface, called the *VPN Concentrator Manager*, that allows you to configure, administer, and monitor your device easily. The VPN Concentrator Manager has three sets of screens that correspond to these tasks: Configuration screens, Administration screens, and Monitoring screens.

VPN 3000 Series Concentrator Reference Volume I: Configuration is the first in the two volume *VPN 3000 Series Concentrator Reference*. Together, both volumes document all the screens of the VPN Concentrator Manager.

- *VPN 3000 Series Concentrator Reference Volume I: Configuration* explains how to start and use the VPN Concentrator Manager. It details the Configuration screens and explains how to configure your device beyond the minimal parameters you set during quick configuration.
- *VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring* provides guidelines for administering and monitoring the VPN Concentrator. It explains and defines all functions available in the Administration and Monitoring screens of the VPN Concentrator Manager. Appendixes to this manual provide troubleshooting guidance and explain how to access and use the alternate command-line interface.

This manual contains only configuration information. It contains no information about administering or monitoring the VPN Concentrator. For administration or monitoring information, refer to *VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring*.

This manual also contains no information about installing the VPN Concentrator and initially configuring it. For information about set-up and initial configuration, refer to the *VPN 3000 Series Concentrator Getting Started*.

Audience

We also assume you are an experienced system administrator or network administrator with appropriate education and training, who knows how to install, configure, and manage internetworking systems. However, virtual private networks and VPN devices might be new to you. You should be familiar with Windows system configuration and management, and you should be familiar with Microsoft Internet Explorer or Netscape Navigator or Communicator browsers.

Prerequisites

We assume you have read the *VPN 3000 Series Concentrator Getting Started* manual, set up your VPN Concentrator, and followed the minimal configuration steps in quick configuration.

Organization

The chapters and sections of this guide correspond to the Configuration part of the VPN Concentrator Manager table of contents (the left frame of the Manager browser window) and are in the same order they appear there.

This guide is organized as follows:

Chapter	Title	Explains How To...
Chapter 1	Using the VPN Concentrator Manager	Log in, navigate, and use the VPN Concentrator Manager with a browser. It explains both HTTP and HTTPS browser connections, and how to install the SSL certificate for a secure (HTTPS) connection.
Chapter 2	Configuration	Access the Configuration screens.
Chapter 3	Interfaces	Configure the VPN Concentrator Ethernet interfaces, and how to configure the system power supply and voltage sensor alarms.
Chapter 4	System Configuration	Access the System Configuration screens.
Chapter 5	Servers	Configure the VPN Concentrator to communicate with and access servers for user authentication, user accounting, converting host names to IP addresses (DNS), assigning client IP addresses (DHCP), and network time synchronization (NTP).
Chapter 6	Address Management	Configure the client IP addresses available in your private network addressing scheme to let the client function as a VPN tunnel endpoint.
Chapter 7	Tunneling Protocols	Configure system-wide parameters for PPTP and L2TP, how to configure IPSec LAN-to-LAN connections, and how to configure IKE proposals for IPSec. These are the three most popular VPN tunneling protocols.
Chapter 8	IP Routing	Configure static routes, default gateways, and OSPF in the VPN Concentrator IP routing subsystem; how to configure DHCP global parameters; and how to configure redundant systems using VRRP.
Chapter 9	Management Protocols	Configure built-in VPN Concentrator servers that provide management functions: FTP, HTTP and HTTPS, TFTP, Telnet, SNMP, and SSL.
Chapter 10	Events	Configure how the system handles events such as alarms, traps, error conditions, network problems, task completion, or status changes. You can specify several ways to record and send event messages.
Chapter 11	General	Configure the system identification, date, time, and maximum session limit.

Chapter	Title	Explains How To...
Chapter 12	Client Update	Configure the VPN Concentrator to manage, from a central location, distribution of software and firmware updates to VPN 3002 hardware clients deployed in diverse locations.
Chapter 13	Load Balancing Cisco VPN Clients	Configure two or more VPN Concentrators to share their remote access session loads.
Chapter 14	User Management	Configure groups and users with attributes that determine their access to and use of the VPN. Configuring groups and users correctly is essential for managing the security of your VPN.
Chapter 15	Policy Management	Configure network lists, filters, rules, and Security Associations, all of which are policies that govern what data traffic can flow through the VPN. You should develop and configure policies first, since you apply them to groups, users, and interfaces. This chapter also describes NAT configuration.

**Note**

This guide is the first volume of the complete VPN Concentrator Manager reference. It documents only configuration tasks. For information on administering or monitoring your VPN Concentrator, refer to the *VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring*.

Related Documentation

Refer to the following documents for further information about Cisco VPN applications and products.

VPN 3000 Series Concentrator Documentation

The *VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring* provides guidelines for administering and monitoring the VPN Concentrator. It explains and defines all functions available in the Administration and Monitoring screens of the VPN Concentrator Manager. Appendixes to this manual provide troubleshooting guidance and explain how to access and use the alternate command-line interface.

The VPN Concentrator Manager also includes online help that you can access by clicking the **Help** icon on the toolbar in the Manager window.

The *VPN 3000 Series Concentrator Getting Started* manual takes you from unpacking and installing the VPN 3000 Series Concentrator, through configuring the minimal parameters to make it operational (called quick configuration).

VPN Client Documentation

The *VPN Client User Guide* explains how to install, configure, and use the VPN Client, which lets a remote client use the IPSec tunneling protocol for secure connection to a private network through the VPN Concentrator.

The *VPN Client Administrator Guide* tells how to configure a VPN 3000 Concentrator for remote user connections using the VPN Client, how to automate remote user profiles, how to use the VPN Client command-line interface, and how to get troubleshooting information.

VPN 3002 Hardware Client Documentation

The *VPN 3002 Hardware Client Reference* provides details on all the functions available in the VPN 3002 Hardware Client Manager. This manual is online only.

The *VPN 3002 Hardware Client Getting Started* manual provides information to take you from unpacking and installing the VPN 3002, through configuring the minimal parameters to make it operational (called Quick Configuration). This manual is available only online.

The *VPN 3002 Hardware Client Quick Start Card* summarizes the information for quick configuration. This quick reference card is provided with the VPN 3002 and is also available online.

The *VPN 3002 Hardware Client Basic Information* sticky label summarizes information for quick configuration. It is provided with the VPN 3002 and you can also print it from the online version; you can affix the label to the VPN 3002.

Documentation on VPN Software Distribution CDs

The VPN 3000 Series Concentrator and VPN 3002 Hardware Client documentation are provided on the VPN 3000 Concentrator software distribution CD-ROM in PDF format. The VPN Client documentation is included on the VPN Client software distribution CD-ROM, also in PDF format. To view the latest versions on the Cisco web site, click the **Support** icon on the toolbar at the top of the VPN Concentrator Manager, Hardware Client Manager, or Client window. To open the documentation, you need Acrobat Reader 3.0 or later; version 4.5 is included on the Cisco VPN 3000 Concentrator software distribution CD-ROM and on the VPN Client software distribution CD-ROM.

Other References

Other useful references include:

- Cisco Systems, *Dictionary of Internetworking Terms and Acronyms*. Cisco Press: 2001.
- *Virtual Private Networking: An Overview*. Microsoft Corporation: 1999. (Available from Microsoft website.)
- www.ietf.org for Internet Engineering Task Force (IETF) Working Group drafts on IP Security Protocol (IPSec).
- www.whatis.com, a web reference site with definitions for computer, networking, and data communication terms.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in boldface .
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> .
screen font	Terminal sessions and information the system displays are in screen font.
boldface screen font	Information you must enter is in boldface screen 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.

Notes use the following conventions:



Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Tips use the following conventions:



Tips

Means *the following are useful tips*.

Cautions use the following conventions:



Caution

Means *reader be careful*. Cautions alert you to actions or conditions that could result in equipment damage or loss of data.

Warnings use the following conventions:



Warning

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.

Data Formats

As you configure and manage the system, enter data in the following formats unless the instructions indicate otherwise:

Type of Data	Format
IP Addresses	IP addresses use 4-byte dotted decimal notation (for example, 192.168.12.34); as the example indicates, you can omit leading zeros in a byte position.
Subnet Masks and Wildcard Masks	Subnet masks use 4-byte dotted decimal notation (for example, 255.255.255.0). Wildcard masks use the same notation (for example, 0.0.0.255); as the example illustrates, you can omit leading zeros in a byte position.
MAC Addresses	MAC addresses use 6-byte hexadecimal notation (for example, 00.10.5A.1F.4F.07).
Host names	Host names use legitimate network host name or end-system name notation (for example, VPN01). Spaces are not allowed. A host name must uniquely identify a specific system on a network.
Text Strings	Text strings use upper- and lower-case alphanumeric characters. Most text strings are case-sensitive (for example, simon and Simon represent different usernames). In most cases, the maximum length of text strings is 48 characters.
Filenames	Filenames on the VPN Concentrator follow the DOS 8.3 naming convention: a maximum of eight characters for the name, plus a maximum of three characters for an extension. For example, LOG00007.TXT is a legitimate filename. The VPN Concentrator always stores filenames in uppercase.
Port Numbers	Port numbers use decimal numbers from 0 to 65535. No commas or spaces are permitted in a number.

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com>

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom of the page.

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

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems; Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

<http://www.cisco.com/register/>

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.



Using the VPN Concentrator Manager

The VPN Concentrator Manager (also known as the Manager) is an HTML-based interface that lets you configure, administer, monitor, and manage the VPN 3000 Series Concentrator with a standard web browser. To use it, you need only to connect to the VPN Concentrator using a PC and browser on the same private network as the VPN Concentrator.

The Manager uses the standard web client/server protocol, HTTP (Hypertext Transfer Protocol), which is a cleartext protocol. However, you can also use the Manager in a secure, encrypted HTTP connection over SSL (Secure Sockets Layer) protocol, which is known as HTTPS.

- To use a cleartext HTTP connection, see the [Connecting to the VPN Concentrator Using HTTP](#) section on [page 1-4](#).
- To use HTTP over SSL (HTTPS) with the Manager the first time, connect to the Manager using HTTP, and install an SSL certificate in the browser; see the [Installing the SSL Certificate in Your Browser](#) section on [page 1-5](#).
- Once the SSL certificate is installed, you can connect directly using HTTPS; see the [Connecting to the VPN Concentrator Using HTTPS](#) section on [page 1-20](#).

Browser Requirements

The VPN Concentrator Manager requires either Microsoft Internet Explorer version 4.0 or higher, or Netscape Navigator version 4.5-4.7 or 6.0. For best results, we recommend Internet Explorer. Whatever browser and version you use, install the latest patches and service packs for it.

JavaScript and Cookies

Be sure JavaScript and Cookies are enabled in the browser. Check these settings.

Browser	JavaScript	Cookies
Internet Explorer 4.0	<ol style="list-style-type: none"> 1. On the View menu, choose Internet Options. 2. On the Security tab, click Custom (for expert users) then click Settings. 3. In the Security Settings window, scroll down to Scripting. 4. Click Enable under Scripting of Java applets. 5. Click Enable under Active scripting. 	<ol style="list-style-type: none"> 1. On the View menu, choose Internet Options. 2. On the Advanced tab, scroll down to Security then Cookies. 3. Click Always accept cookies.
Internet Explorer 5.0	<ol style="list-style-type: none"> 1. On the Tools menu, choose Internet Options. 2. On the Security tab, click Custom Level. 3. In the Security Settings window, scroll down to Scripting. 4. Click Enable under Active scripting. 5. Click Enable under Scripting of Java applets. 	<ol style="list-style-type: none"> 1. On the Tools menu, choose Internet Options. 2. On the Security tab, click Custom Level. 3. In the Security Settings window, scroll down to Cookies. 4. Click Enable under Allow cookies that are stored on your computer. 5. Click Enable under Allow per-session cookies (not stored).
Netscape Navigator 4.5-4.7	<ol style="list-style-type: none"> 1. On the Edit menu, choose Preferences. 2. On the Advanced screen, check the Enable JavaScript check box. 	<ol style="list-style-type: none"> 1. On the Edit menu, choose Preferences. 2. On the Advanced screen, click one of the Accept... cookies choices, and <i>do not</i> check the Warn me before accepting a cookie check box.
Netscape Navigator 6.0	<ol style="list-style-type: none"> 1. On the Edit menu, choose Preferences. 2. On the Advanced screen, check the Enable JavaScript for Navigator check box. 	<ol style="list-style-type: none"> 1. On the Edit menu, choose Preferences. 2. Under the Advanced category, choose Cookies. 3. On the Cookies screen, choose Enable All Cookies. <i>Do not</i> check the Warn me before storing a cookie check box.

Navigation Toolbar

Do not use the *browser* navigation toolbar buttons Back, Forward, or Refresh/Reload with the VPN Concentrator Manager unless instructed to do so. To protect access security, clicking Refresh /Reload automatically logs out the Manager session. Clicking Back or Forward might result in outdated Manager screens with incorrect data or settings being displayed.

We recommend that you hide the browser navigation toolbar to prevent mistakes from occurring during use of the VPN Concentrator Manager.

Recommended PC Monitor/Display Settings

For easiest use, we recommend that you use the following settings on your monitor or display:

- Desktop area = 1024 x 768 pixels or greater. The minimum desktop area is 800 x 600 pixels.
- Color palette = 256 colors or more.

Netscape Navigator 4.x Browsers

If you are running the VPN Concentrator Manager in a Netscape Navigator 4.x browser, you might encounter the following problems:

- When you edit group or user attributes on the Configuration | User Management | Groups or Users screens, your changes might not be saved. The Inherit check box does not clear automatically, which causes your changes to revert to the inherited value of the group or Base Group. Therefore to save your changes, you must manually clear the Inherit check box.
- In some screens, when you resize your browser window, you see the Action buttons duplicated (one on top of the other).

For best results, use Internet Explorer instead of Netscape Navigator.

Connecting to the VPN Concentrator Using HTTP

When your system administration tasks and network permit a cleartext connection between the VPN Concentrator and your browser, you can use the standard HTTP protocol to connect to the system.

Even if you plan to use HTTPS, you must first use HTTP to install an SSL certificate in your browser.

-
- Step 1** Bring up the browser.
- Step 2** In the browser Address or Location field, enter the VPN Concentrator Ethernet 1 (Private) interface IP address, for example: 10.10.99.50. The browser automatically assumes and supplies an http:// prefix. The browser displays the VPN Concentrator Manager login screen. (See [Figure 1-1](#).)
-

Figure 1-1 VPN Concentrator Manager Login Screen



To continue using HTTP for the whole session, skip to [Logging into the VPN Concentrator Manager](#), page 1-21.

Installing the SSL Certificate in Your Browser

The VPN Concentrator Manager provides the option of using HTTP over SSL with the browser. SSL creates a secure session between your browser (client) and the VPN Concentrator (server). This protocol is known as HTTPS, and uses the `https://` prefix to connect to the server. The browser first authenticates the server, then encrypts all data passed during the session.

HTTPS is often confused with a similar protocol, S-HTTP (Secure HTTP), which encrypts only HTTP application-level data. SSL encrypts *all* data between client and server at the IP socket level, and is thus more secure.

SSL uses digital certificates for authentication. The VPN Concentrator creates a self-signed SSL server certificate when it boots, and this certificate must be installed in the browser. Once the certificate is installed, you can connect using HTTPS. You need to install the certificate from a given VPN Concentrator only once.

Managing the VPN Concentrator is the same with or without SSL. Manager screens might take slightly longer to load with SSL because of encryption/decryption processing. When connected via SSL, the browser shows a locked-padlock icon on its status bar. Both Microsoft Internet Explorer and Netscape Navigator support SSL.

Follow these steps to install and use the SSL certificate for the first time. We provide separate instructions for Internet Explorer and Netscape Navigator when they diverge.

Step 1 Connect to the VPN Concentrator using HTTP as noted in the preceding text.

Step 2 On the login screen, click the **Install SSL Certificate** link.

The Manager displays the Install SSL Certificate screen (see [Figure 1-2](#)) and automatically begins to download and install its SSL certificate in your browser.

Figure 1-2 Install SSL Certificate Screen

Install the SSL Certificate

Step 1: Download the SSL Certificate

The VPN 3000 Concentrator Series supports HTTP over SSL, also known as HTTPS. This requires the use of SSL digital certificates. A digital certificate has already been created for this VPN 3000 Concentrator Series. It will automatically download to your browser. **You should wait a few seconds for the certificate to be downloaded.**

**In a few seconds, a *File Download* dialog will appear for the SSL certificate.
Select *Open this file from its current location* to automatically install the SSL certificate.**

(If you chose **Save this file to disk**, double-clicking the file will install the certificate into Internet Explorer.)

The certificate only needs to be installed once per VPN 3000 Concentrator Series. If you installed a new SSL certificate onto the VPN 3000 Concentrator Series, you may already have this certificate in your browser. *If the certificate does not automatically download after one minute, [click here to install it](#).*

Step 2: Connect to the VPN 3000 Concentrator Series using SSL

To use SSL, use the protocol identifier **https:** rather than **http:** when accessing the VPN 3000 Concentrator Series (e.g. <https://10.10.147.2>). [After installing the SSL certificate, click here to connect to the VPN 3000 Concentrator Series using SSL.](#)

67283

At this point in the process, the installation sequence differs depending on the browser being used.

- For Internet Explorer, proceed to the next section, [Installing the SSL Certificate with Internet Explorer](#).
- For Netscape Navigator, see the [Installing the SSL Certificate with Netscape](#) section on [page 1-13](#).

Installing the SSL Certificate with Internet Explorer



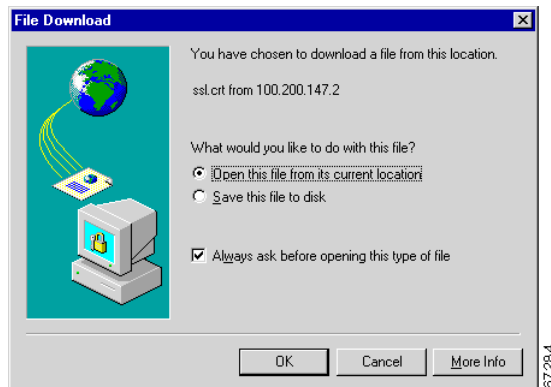
Note

This section describes SSL certificate installation using Microsoft Internet Explorer 5.0. With Internet Explorer 4.0, some dialog boxes might differ but the process is similar.

You need to install the SSL certificate from a given VPN Concentrator only once. If you do reinstall it, the browser repeats all these steps each time.

A few seconds after the VPN Concentrator Manager SSL screen appears, Internet Explorer displays a File Download dialog box that identifies the certificate filename and source, and asks whether to open or save the certificate. To immediately install the certificate in the browser, click the **Open this file from its current location** radio button. If you save the file, the browser prompts for a location; you must then double-click on the file to install it.

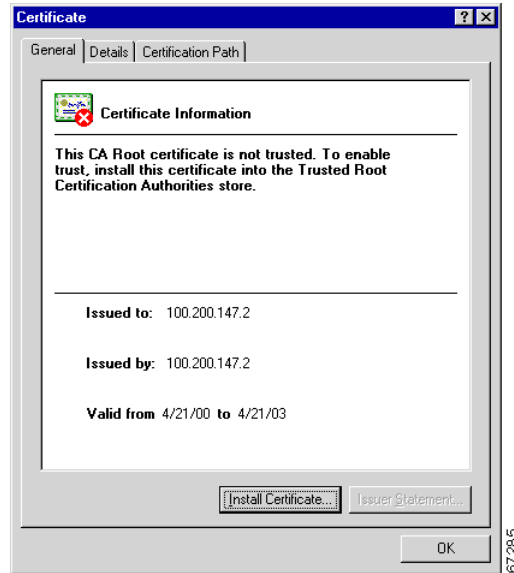
Figure 1-3 Internet Explorer File Download Dialog Box



Step 1 Click the **Open this file from its current location** radio button, then click **OK**.

The browser displays the Certificate dialog box with information about the certificate. (See [Figure 1-4](#).) You must now install the certificate.

Figure 1-4 Internet Explorer Certificate Dialog Box



Step 2 Click **Install Certificate**.

The browser starts a wizard to install the certificate. (See [Figure 1-5](#).) In Internet Explorer, these certificates are stored in the “certificates store.”

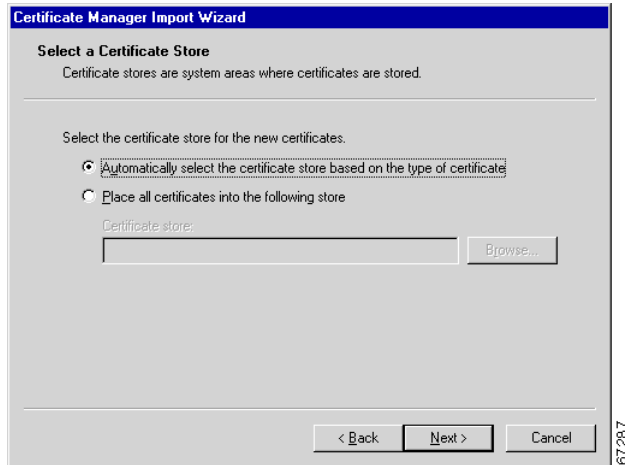
Figure 1-5 Internet Explorer Certificate Manager Import Wizard Dialog Box



Step 3 Click **Next** to continue.

The wizard opens the next dialog box; you are asked to choose a certificate store. (See [Figure 1-6](#).)

Figure 1-6 Internet Explorer Certificate Manager Import Wizard Dialog Box



Step 4 Click **Automatically select the certificate store**, then click **Next**.

The wizard opens a dialog box to complete the installation. (See [Figure 1-7](#).)

Figure 1-7 Internet Explorer Certificate Manager Import Wizard Dialog Box



Step 5 Click **Finish**.

The wizard opens the Root Certificate Store dialog box; you are asked to confirm the installation. (See [Figure 1-8](#).)

Figure 1-8 Internet Explorer Root Certificate Store Dialog Box

**Step 6** To install the certificate, click **Yes**. The dialog box then closes, and a final wizard confirmation dialog box opens. (See [Figure 1-9](#).)

Figure 1-9 Internet Explorer Certificate Manager Import Wizard Final Dialog Box

**Step 7** Click **OK** to close this dialog box, and click **OK** on the Certificate dialog box to close it. (See [Figure 1-4](#).)

You can now connect to the VPN Concentrator using HTTP over SSL (HTTPS).

Step 8 On the Manager SSL screen (see [Figure 1-2](#)), click the link that says, **After installing the SSL certificate, click here to connect to the VPN 3000 Concentrator Series using SSL**.

Depending on how your browser is configured, you might see a Security Alert dialog box. (See [Figure 1-10](#).)

Figure 1-10 Internet Explorer Security Alert Dialog Box

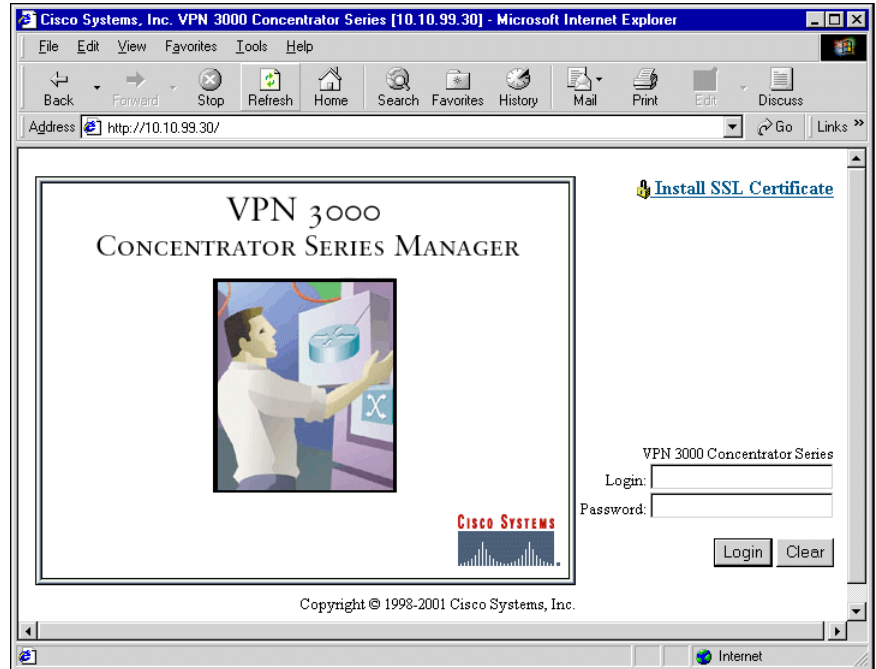


67291

Step 9 Click **OK**.

The VPN Concentrator displays the HTTPS version of the Manager login screen. (See [Figure 1-11](#).)

Figure 1-11 VPN Concentrator Manager Login Screen Using HTTPS (Internet Explorer)



The browser maintains the HTTPS state until you close the browser or access an insecure site; in the latter case you might see a Security Alert screen.

Step 10 Proceed to [Logging into the VPN Concentrator Manager, page 1-21](#) to log in as usual.

Viewing Certificates with Internet Explorer

Examine certificates stored in Internet Explorer using either of the following methods.

**Note**

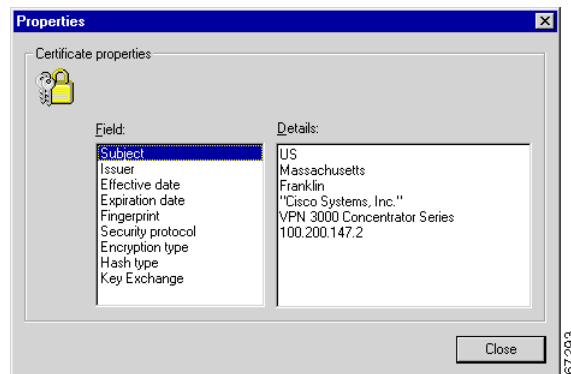
The VPN Concentrator SSL certificate name is its Ethernet 1 (Private) IP address.

To View Details of the Certificate in Use

Step 1 Note the padlock icon on the browser status bar (at the bottom of the browser) in [Figure 1-11](#). Double-click on the icon.

The browser opens a Properties screen showing details of the specific certificate in use. (See [Figure 1-12](#).)

Figure 1-12 Internet Explorer 4.0 Certificate Properties Screen



Step 2 Select any one of the Field items to see details.

Step 3 Click **Close** when finished.

To View All Stored Certificates (Internet Explorer 4.0 Only)



Note These steps apply only to Internet Explorer 4.0. If you are using Internet Explorer 5.0, skip to the next section.

- Step 1** Click the browser **View** menu. Choose **Internet Options**.
- Step 2** Click the **Content** tab, then click **Authorities** in the Certificates section.
The browser displays the Certificate Authorities screen. (See [Figure 1-13](#).)

Figure 1-13 Internet Explorer 4.0 Certificate Authorities Screen



- Step 3** Select a certificate. Click **View Certificate**.
The browser displays the Certificate Properties screen. (See [Figure 1-12](#).)

To View All Stored Certificates (Internet Explorer 5.0 Only)



Note These steps apply only to Internet Explorer 5.0. If you are using an earlier version of Internet Explorer, follow the steps in the previous section.

- Step 1** Click the browser **Tools** menu. Choose **Internet Options**.
The browser displays the Internet Options screen.
- Step 2** Click the **Content** tab. In the Certificates section, click **Certificates...**
The browser displays the Certificate Manager screen.
- Step 3** In the Certificate Manager screen, click the **Trusted Root Certification Authorities** tab. Select a certificate, then click **View Certificate**.
The browser displays the Certificate Properties screen. (See [Figure 1-12](#).)

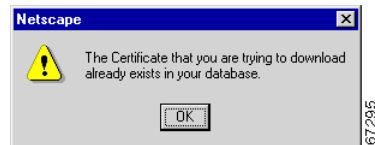
Installing the SSL Certificate with Netscape

This section describes SSL certificate installation using Netscape Navigator/Communicator 4.5.

Reinstallation

You need to install the SSL certificate from a given VPN Concentrator only once. If you attempt to reinstall it, Netscape displays the note shown in [Figure 1-14](#). Click **OK**, and connect to the VPN Concentrator using SSL (see [Step 8](#) on page 1-16).

Figure 1-14 Netscape Reinstallation Note



First-time Installation

The instructions below follow from [Step 2](#) on [page 1-5](#) and describe first-time certificate installation.

A few seconds after the VPN Concentrator Manager SSL screen appears, Netscape displays a New Certificate Authority screen. (See [Figure 1-15](#).)

Figure 1-15 Netscape New Certificate Authority Screen 1



Step 1 Click **Next>** to proceed.

Netscape displays the next New Certificate Authority screen, which further explains the process. (See [Figure 1-16](#).)

Figure 1-16 Netscape New Certificate Authority Screen 2



Step 2 Click **Next>** to proceed.

Netscape displays the next New Certificate Authority screen, which lets you examine details of the VPN Concentrator SSL certificate. (See [Figure 1-17](#).)

Figure 1-17 Netscape New Certificate Authority Screen 3



Step 3 Click **Next>** to proceed.

Netscape displays the next New Certificate Authority screen, with choices for using the certificate. No choices are checked by default. (See [Figure 1-18](#).)

Figure 1-18 Netscape New Certificate Authority Screen 4



Step 4 You must check at least the first box, **Accept this Certificate Authority for Certifying network sites**. Click **Next>** to proceed.

Netscape displays the next New Certificate Authority screen, which lets you choose to have the browser warn you about sending data to the VPN Concentrator. (See [Figure 1-19](#).)

Figure 1-19 Netscape New Certificate Authority Screen 5



Step 5 Checking the box is optional.



Note If the box is checked, you will get a warning whenever you apply settings on a Manager screen. It is probably less intrusive to manage the VPN Concentrator without those warnings.

Step 6 Click **Next>** to proceed.

Netscape displays the final New Certificate Authority screen, which asks you to provide a nickname for the certificate. (See [Figure 1-20](#).)

Figure 1-20 Netscape New Certificate Authority Screen 6



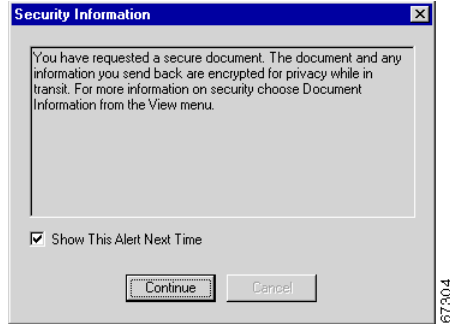
Step 7 In the Nickname field, enter a descriptive name for this certificate. “Nickname” is something of a misnomer. We suggest you use a clearly descriptive name such as Cisco VPN Concentrator 10.10.147.2. This name appears in the list of installed certificates; see the [Viewing Certificates with Netscape](#) section on [page 1-18](#).

Click **Finish**.

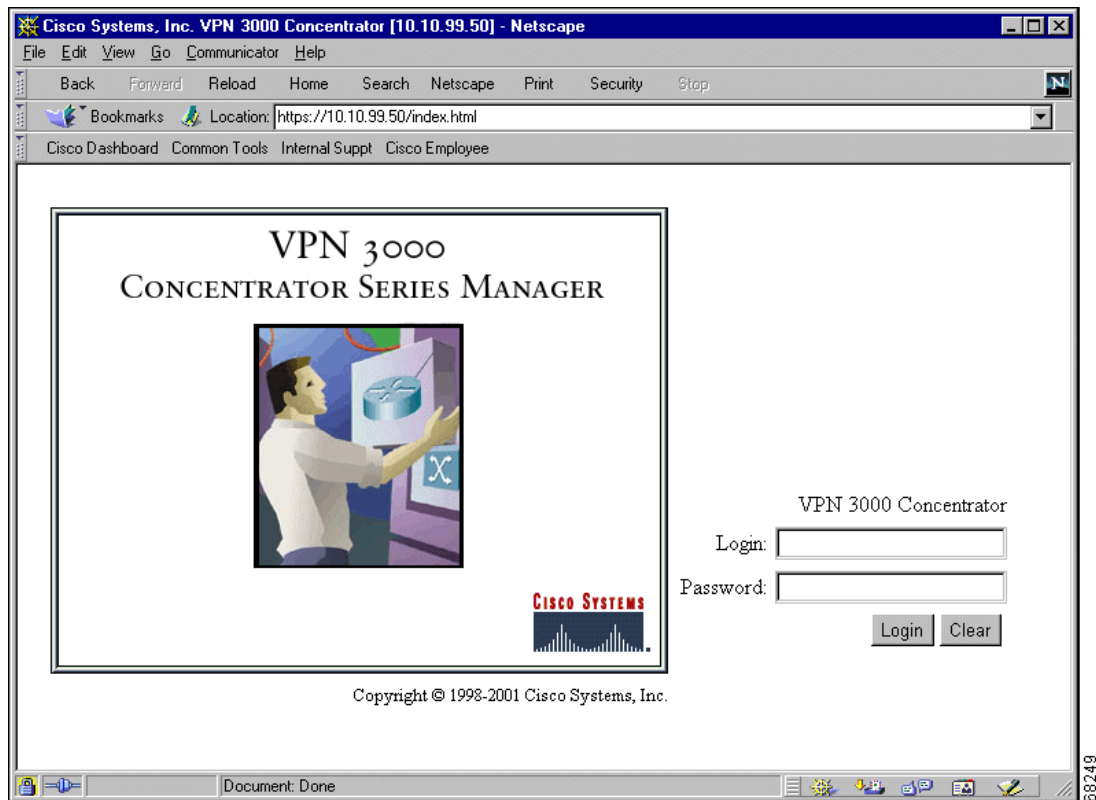
You can now connect to the VPN Concentrator using HTTP over SSL (HTTPS).

Step 8 On the Manager SSL screen (see [Figure 1-2](#)), click the link that says, **After installing the SSL certificate, click here to connect to the VPN Concentrator using SSL**.

Depending on how your browser is configured, you might see a Security Information Alert dialog box. (See [Figure 1-21](#).)

Figure 1-21 Netscape Security Information Alert Dialog Box**Step 9** Click **Continue**.

The VPN Concentrator displays the HTTPS version of the Manager login screen. (See [Figure 1-22](#).)

Figure 1-22 VPN Concentrator Manager Login Screen Using HTTPS (Netscape)

The browser maintains the HTTPS state until you close the browser or access an insecure site; in the latter case, you might see a Security Information Alert dialog box.

Proceed to [Logging into the VPN Concentrator Manager, page 1-21](#) to log in.

Viewing Certificates with Netscape

Examine certificates stored in Netscape Navigator/Communicator 4.5 using either of the following methods.

To View Details of the Certificate in Use

- Step 1** Note the locked-padlock icon on the bottom status bar in [Figure 1-22](#). If you click the icon, Netscape opens a Security Info window. (See [Figure 1-23](#).)



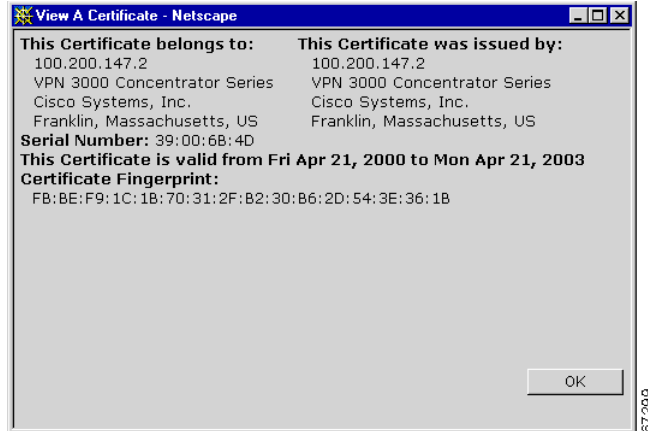
Note You can also open this window by clicking **Security** on the Navigator Toolbar at the top of the Netscape window.

Figure 1-23 Netscape Security Info Window



- Step 2** Click the **View Certificate** button to see details of the specific certificate in use. The View Certificates screen opens. (See [Figure 1-24](#).)

Figure 1-24 Netscape View Certificate Screen

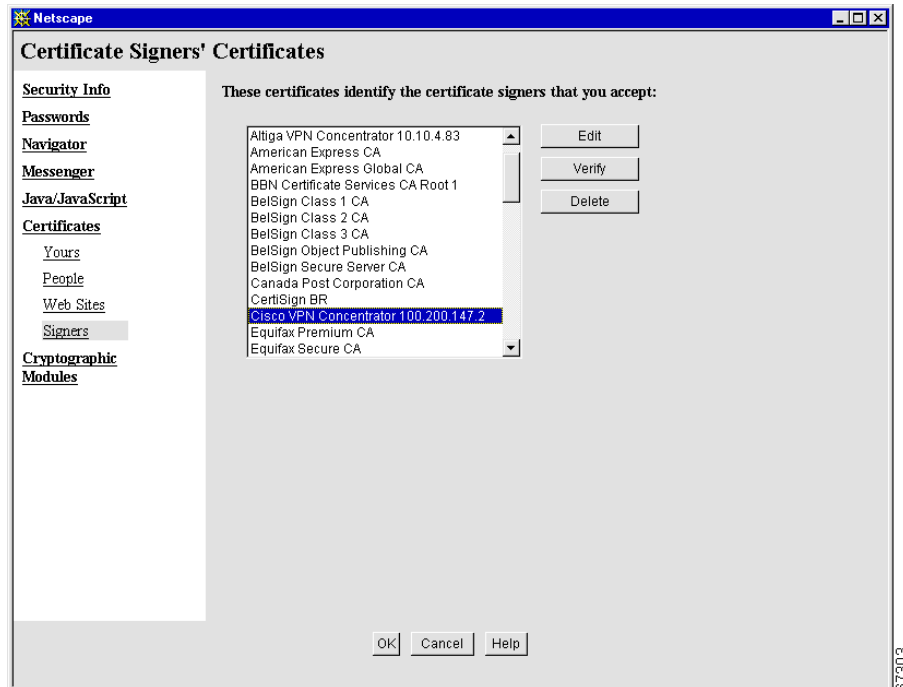


Step 3 Click **OK** when finished.

To View All Stored Certificates

Step 1 In the Security Info window (see Figure 1-25), select **Certificates**, then **Signers**. The “nickname” you entered in Step 7 on page 1-16 identifies the VPN Concentrator SSL certificate.

Figure 1-25 Netscape Certificates Signers List



Step 2 Select a certificate, then click **Edit**, **Verify**, or **Delete**. Click **OK** when finished.

Connecting to the VPN Concentrator Using HTTPS

Once you have installed the VPN Concentrator SSL certificate in the browser, you can connect directly using HTTPS:

- Step 1** Bring up the browser.
- Step 2** In the browser Address or Location field, enter `https://` plus the VPN Concentrator private interface IP address; for example, `https://10.10.147.2`.

The browser displays the VPN Concentrator Manager HTTPS login screen. (See [Figure 1-26](#).)

Figure 1-26 VPN Concentrator Manager HTTPS Login Screen



A locked-padlock icon on the browser status bar indicates an HTTPS session. This login screen does not include the Install SSL Certificate link.

Logging into the VPN Concentrator Manager

The procedure for logging into the VPN Concentrator Manager is the same for both types of connections, cleartext HTTP and secure HTTPS.

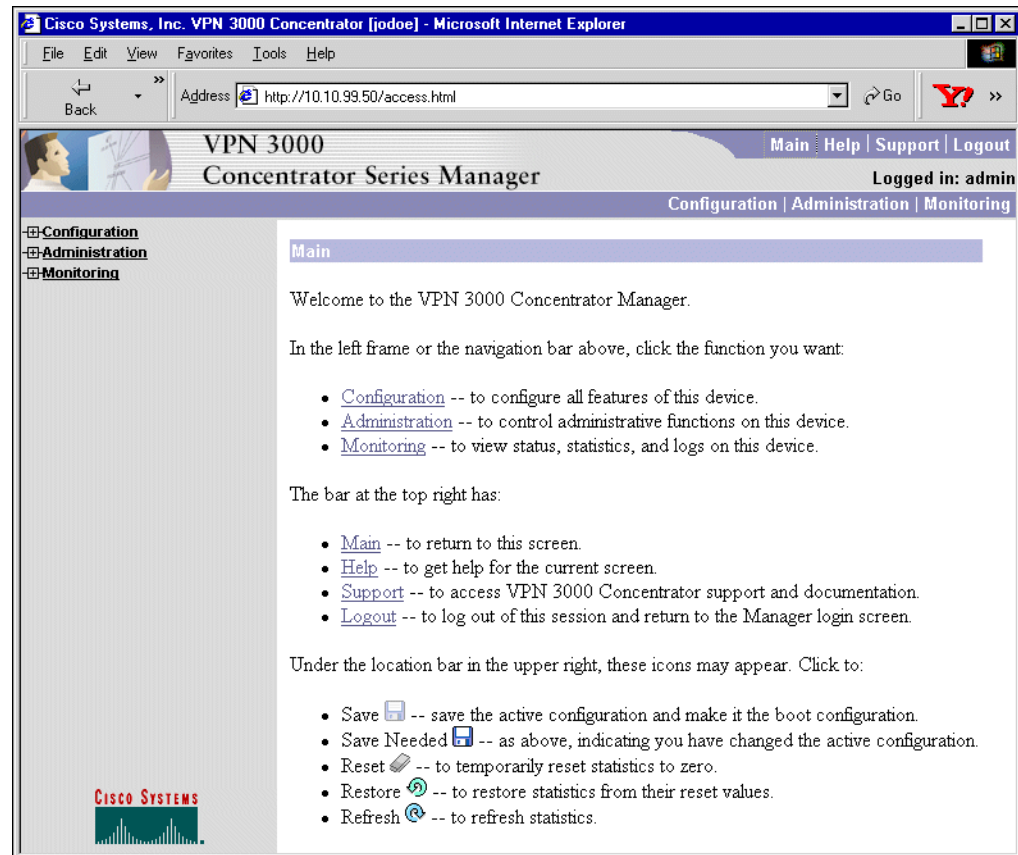
Entries are case-sensitive. With Microsoft Internet Explorer, you can select the Tab key to move from field to field; other browsers might work differently. If you make a mistake, click the **Clear** button and start over.

The following steps use the factory-supplied default entries. If you have changed them, use your entries.

- Step 1** Click in the **Login** field and type `admin`. (*Do not press Enter.*)
- Step 2** Click in the **Password** field and type `admin`. (The field shows `*****`.)
- Step 3** Click the **Login** button.

The VPN Concentrator Manager displays the main welcome screen. (See [Figure 1-27](#).)

Figure 1-27 Manager Main Welcome Screen



From here you can navigate the Manager using either the table of contents in the left frame, or the Manager toolbar in the top frame.

Configuring HTTP, HTTPS, and SSL Parameters

HTTP, HTTPS, and SSL are enabled by default on the VPN Concentrator, and they are configured with recommended parameters that should suit most administration tasks and security requirements.

To configure HTTP and HTTPS parameters, see the Configuration | System | Management Protocols | HTTP/HTTPS screen.

To configure SSL parameters, see the Configuration | System | Management Protocols | SSL screen.

For additional security, by default these parameters are only accessible from the private interface or through established VPN tunnels.

Organization of the VPN Concentrator Manager

The VPN Concentrator Manager consists of three major sections and many subsections:

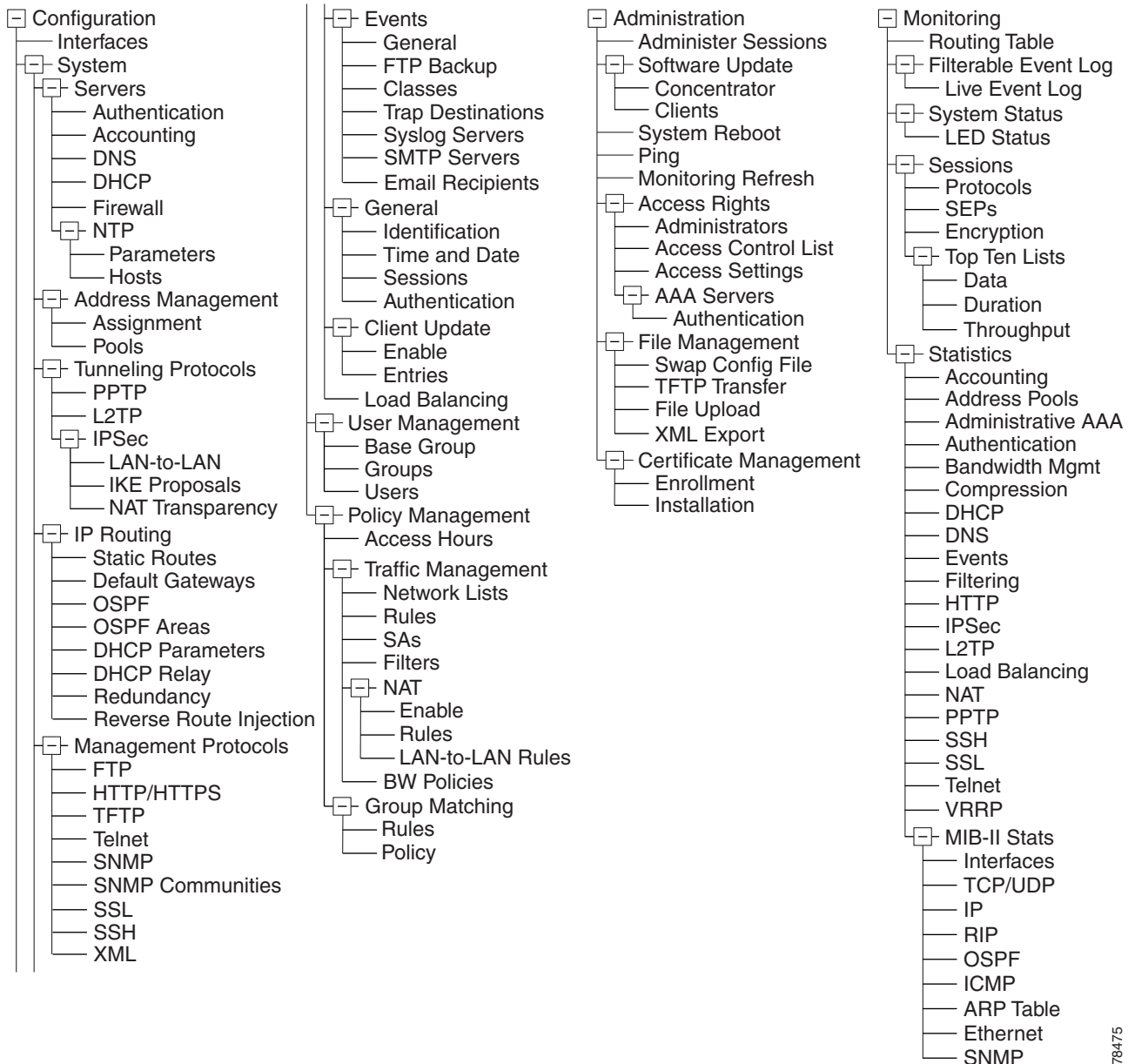
- **Configuration:** Setting all the parameters for the VPN Concentrator that govern its use and functionality as a VPN device:
 - **Interfaces:** Ethernet and power-supply interface parameters.
 - **System:** Parameters for system-wide functions such as server access, address management, tunneling protocols, IP routing, built-in management servers, event handling, and system identification.
 - **User Management:** Attributes for groups and users that determine their access to and use of the VPN.
 - **Policy Management:** Policies that control access times and data traffic through the VPN via filters, rules, and IPSec Security Associations.
- **Administration:** Managing higher-level functions that keep the VPN Concentrator operational and secure, such as who is allowed to configure the system, what software runs on it, and managing its digital certificates.
- **Monitoring:** Viewing routing tables, event logs, system LEDs and status, data on user sessions, and statistics for protocols and system functions.

This manual covers configuration. For information on administration or monitoring, refer to *VPN 3000 Concentrator Series Reference Volume II: Administration and Monitoring*. For Quick Configuration, refer to the *VPN 3000 Concentrator Series Getting Started* manual.

Navigating the VPN Concentrator Manager

Your primary tool for navigating the VPN Concentrator Manager is the table of contents in the left frame. [Figure 1-28](#) shows all its entries, fully expanded. (The figure shows the frame in multiple columns, but the actual frame is a single column. Use the scroll controls to move up and down the frame.)

Figure 1-28 Complete VPN Manager Table of Contents



78475



Configuration

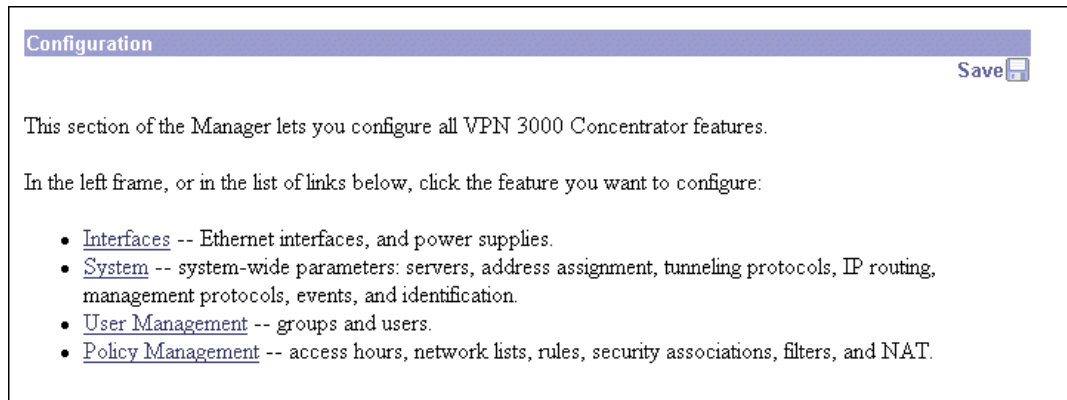
Configuring the VPN Concentrator means setting all the parameters that govern its use and functionality as a VPN device.

Cisco supplies default parameters that cover typical installations and uses; once you supply minimal parameters in Quick Configuration, the system is operational. To modify the system to meet your needs and to provide an appropriate level of system security, you should configure the system in detail.

Configuration

Step 1 In the Concentrator Manager table of contents, click **Configuration**. The Configuration screen opens.

Figure 2-1 Configuration Screen



The Configuration section of the Manager lets you configure all VPN Concentrator features and functions. For each section of the Manager, see the applicable chapter in this manual.

- **Interfaces:** Parameters specific to the Ethernet interfaces: public, private, and external. Power supply and voltage sensor alarms.
- **System:** Parameters for system-wide functions: server access, address assignment, tunneling protocols, IP routing, built-in management servers, system events, and system identification.
- **User Management:** Attributes for groups and users that determine their access to and use of the VPN.
- **Policy Management:** Policies that control data traffic through the VPN via filters, rules, and IPSec Security Associations; network lists; access times; and NAT.



Interfaces

The Interfaces section of the VPN 3000 Concentrator Series Manager applies primarily to Ethernet network interfaces. In this section, you configure functions that are interface-specific, rather than system-wide. There is also a screen to configure power-supply and voltage-sensor alarms.

Typically, you configure at least two network interfaces for the VPN Concentrator to operate as a VPN device: usually the Ethernet 1 (Private) and the Ethernet 2 (Public) interfaces. If you used Quick Configuration as described in the *VPN 3000 Series Concentrator Getting Started* manual, the system supplied many default parameters for the interfaces. In the Interfaces section, you can customize the configuration.

The VPN Concentrator uses filters to control, or govern, data traffic passing through the system (see Configuration | Policy Management | Traffic Management). You apply filters both to interfaces and to groups and users. Group and user filters govern tunneled group and user data traffic; interface filters govern all data traffic.

Network interfaces usually connect to a router that routes data traffic to other networks. The VPN Concentrator includes IP routing functions: static routes, RIP (Routing Information Protocol), and OSPF (Open Shortest Path First). You configure RIP and interface-specific OSPF in the Interfaces section. You configure static routes, the default gateway, and system-wide OSPF in the IP Router section (see the Configuration | System | IP Routing screens).

RIP and OSPF are routing protocols that routers use to send messages to other routers to determine network connectivity, status, and optimum paths for sending data traffic. The VPN Concentrator supports RIP versions 1 and 2, and OSPF version 2. You can enable both RIP and OSPF on an interface.

Filter settings override RIP and OSPF settings on an interface; therefore, be sure settings in filter rules are consistent with RIP and OSPF use. For example, if you intend to use RIP, be sure you apply a filter rule that forwards TCP/UDP packets with the RIP port configured.

Configuration | Interfaces

This section lets you configure the three VPN Concentrator Ethernet interface modules. You can also configure alarm thresholds for the power-supply modules.

Model 3005 comes with two Ethernet interfaces. Models 3015 through 3080 come with three Ethernet interfaces.

- Ethernet 1 (Private) is the interface to your private network (internal LAN).
- Ethernet 2 (Public) is the interface to the public network.
- Ethernet 3 (External) is the interface to an additional LAN (Models 3015 through 3080 only).

Configuring an Ethernet interface includes supplying an IP address, applying a traffic-management filter, setting the speed and transmission modes, and configuring RIP and OSPF routing protocols.



Note

Interface settings take effect as soon as you apply them. If the system is in active use, changes might affect tunnel traffic.

The table shows all installed interfaces and their status.

Figure 3-1 Configuration | Interfaces Screen (Model 3005)

Configuration | Interfaces
Monday, 01 October 2001 16:03:58


[Save](#) [Refresh](#)

This section lets you configure the VPN 3000 Concentrator's network interfaces.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	10.10.99.20	255.255.0.0	00.90.A4.08.00.1A	
Ethernet 2 (Public)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

- [Power Supply](#)



68231

Figure 3-2 Configuration | Interfaces Screen (Models 3015 through 3080)

Configuraton | Interfaces
Monday, 01 October 2001 16:20:11

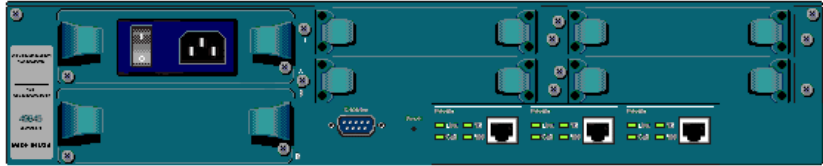
[Save](#) [Refresh](#)

This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	10.10.99.50	255.255.0.0	00.90.A4.00.25.A8	
Ethernet 2 (Public)	DOWN	10.10.99.99	255.0.0.0	00.90.A4.00.25.A9	
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

• [Power Supplies](#)



688230

To configure a module, either click the appropriate link in the status table; or use the mouse pointer to select the module on the back-panel image, and click anywhere in the highlighted area.

Refresh

To update the screen contents, click the **Refresh** button. The date and time above this reminder indicate when the screen was last updated.

Interface

The VPN Concentrator interface installed in the system. To configure an interface, click the appropriate link.

Ethernet 1 (Private), Ethernet 2 (Public), Ethernet 3 (External)

To configure Ethernet interface parameters, click the appropriate highlighted link in the table or click in a highlighted module on the back-panel image. See Configuration | Interfaces | Ethernet 1 2 3.

[Renew | Release]

This field appears under Ethernet 1, 2, or 3 if DHCP Client is enabled for that interface.

Renew: Renews the DHCP client lease for the interface.

Release: Releases the DHCP client lease for the interface.

DNS Server(s)

This field displays the IP addresses of up to three configured DNS servers.

To view or edit DNS server information, click **DNS Server**. The Configuration | System | Servers | DNS window appears.

DNS Domain Name

The registered domain in which the VPN Concentrator is located, for example: cisco.com.

To view or edit DNS Domain Name information, click **DNS Domain Name**. The Configuration | System | Servers | DNS window appears.

Status

The operational status of this interface.

- Up = (Green) Configured, enabled, and operational; ready to pass data traffic.
- Down = (Red) Configured but disabled or disconnected.
- Testing = In test mode; no regular data traffic can pass.
- Dormant = (Red) Configured and enabled but waiting for an external action, such as an incoming connection.
- Not Present = (Red) Missing hardware components.
- Lower Layer Down = (Red) Not operational because a lower-layer interface is down.
- Unknown = (Red) Not configured or not able to determine status.
- Not Configured = Present but not configured.
- Waiting for DHCP = DHCP is enabled, but the VPN Concentrator has not received an IP address.
- Lease expires in... (hh:mm:ss) = If DHCP Client is enabled on any interface, the amount of time remaining on the lease appears here. You can also view this information on the Configuration | Interfaces | Ethernet 1 2 3 screens.

IP Address

The IP address configured on this interface.

Subnet Mask

The subnet mask configured on this interface.

MAC Address

The unique hardware MAC (Medium Access Control) address for this interface, displayed in 6-byte hexadecimal notation.

Default Gateway

This field displays the IP address of the default gateway for the subnet associated with this interface.

To view or edit default gateway information, click **Default Gateway**. The Configuration | System | IP Routing | Default Gateways window displays.

When you are not using DHCP to obtain a default gateway, you configure a default gateway manually. If DHCP client on the Ethernet 2 (Public) interface is enabled, the default gateway is automatically entered in the routing table, and not in the Configuration | System | IP Routing | Default Gateways screen.

When you configure a default gateway manually, the system automatically removes the DHCP-obtained default gateway from the routing table. To reverse this operation, renew the DHCP lease for the Ethernet 2 (Public) interface.

Power Supplies

To configure alarm thresholds on system power supplies, click the appropriate highlighted link or click in a highlighted power-supply module in the back-panel image and see Configuration | Interfaces | Power.

Ethernet 1 (Private), Ethernet 2 (Public), Ethernet 3 (External) Module in Back-Panel Image

To configure Ethernet interface parameters, click the appropriate highlighted Ethernet module in the back-panel image and see Configuration | Interfaces | Ethernet 1 2 3.

Configuration | Interfaces | Power

This screen lets you configure alarm thresholds for voltages in the system power supplies, CPU, and main circuit board. You set high and low thresholds for the voltages. (For recommended thresholds, see [Table 3-1](#).) When the system detects a voltage outside a threshold value, it generates a HARDWAREMON (hardware monitoring) event. (See Configuration | System | Events.) If a power supply is faulty, the appropriate Power Supply LED on the front panel is amber.

Table 3-1 Recommended Power Thresholds

Thresholds Monitor	Minimum-Maximum Range (in Centivolts)	Tolerance
1.9V CPU	180-201 cV	±10 cV
2.5V CPU	241-260 cV	±10 cV
3.3V power supply	321-389 cV	±10% cV (+ 25 cV if redundant power supply)
5.0V power supply	471-577 cV	±10% cV (+ 25 cV if redundant power supply)
3.3V board	314-346 cV	±5%
5.0V board	474 - 524 cV	±5%



Warning

If a voltage generates an alarm, shut down the system in an orderly way and contact Cisco support. Operating the system with out-of-range voltages, especially if they exceed the high threshold, might cause permanent damage.

You can view system voltages and status on the Monitoring | System Status | Power screen.

Figure 3-3 Configuration | Interfaces | Power screen (Model 3005)

		CPU		Board	
		Low	High	Low	High
2.5V		241	260		
3.3V				314	346
5V				474	524

Voltages will be adjusted to conform to the hardware.

Apply Cancel

67109

Figure 3-4 Configuration | Interfaces | Power screen (Model 3015 through 3080)

		CPU		Power Supply A		Power Supply B		Board	
		Low	High	Low	High	Low	High	Low	High
1.9V		180	201						
3.3V				321	389	321	389	314	346
5V				471	577	471	577	474	524

Voltages will be adjusted to conform to the hardware.

Apply Cancel

67111

Alarm Thresholds

The fields show default values for alarm thresholds in centivolts, for example, 361 = 3.61 volts. Enter or edit these values as desired.

The hardware sets voltage thresholds in increments that might not match an entered value. The fields show the actual thresholds, and the values might differ from your entries.

CPU

High and low thresholds for the voltage sensors on the CPU chip. The value is system dependent, either 2.5 or 1.9 volts.

Power Supply A, B

High and low thresholds for the 3.3- and 5-volt outputs from the power supplies. You can enter values for the second power supply on Models 3015–3080 even if it is not installed.

Board

High and low thresholds for the 3.3- and 5-volt sensors on the main circuit board.

Apply / Cancel

To apply your settings to the system and include them in the active configuration, click **Apply**. The Manager returns to the Configuration | Interfaces screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | Interfaces screen.

Configuration | Interfaces | Ethernet 1 2 3

This screen lets you configure parameters for the Ethernet interface you selected. It displays the current parameters, if any.

Configuring an Ethernet interface includes supplying an IP address, identifying it as a public interface, applying a traffic-management filter, setting speed and transmission mode, and configuring RIP and OSPF routing protocols.

To apply a custom filter, you must configure the filter first; see Configuration | Policy Management | Traffic Management.

**Caution**

If you modify any parameters of the interface that you are currently using to connect to the VPN Concentrator, you will break the connection, and you will have to restart the Manager from the login screen.

Using the Tabs

This screen includes three tabbed sections. Click each tab to display its parameters. As you move from tab to tab, the Manager retains your settings. When you have finished setting parameters on all tabbed sections, click **Apply** or **Cancel**.

General Parameters Tab

This tab lets you configure general interface parameters: DHCP client, IP address, subnet mask, public interface status, filter, speed, transmission mode, maximum transmission unit, and IPSec fragmentation policy.

Figure 3-5 Configuration | Interfaces | Ethernet 1 2 3 Screen, General Tab

Configuration | Interfaces | Ethernet 1

Warning: You are modifying the interface you are using to connect to this device. If you make any changes, you will break the connection and you will have to restart from the login screen.

Configuring Ethernet Interface 1 (Private).

General RIP OSPF Bandwidth

General Parameters			
Sel	Attribute	Value	Description
<input type="radio"/>	Disabled		Select to disable this interface.
<input type="radio"/>	DHCP Client		Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.
<input checked="" type="radio"/>	Static IP Addressing		Select to configure the IP Address and Subnet Mask. Enter the IP Address and Subnet Mask for this interface.
	IP Address	10.10.99.50	
	Subnet Mask	255.255.0.0	
	Public Interface	<input type="checkbox"/>	Check to make this interface a "public" interface.
	MAC Address	00:90:A4:00:25:A8	The MAC address for this interface.
	Filter	---None---	Select the filter for this interface.
	Speed	10/100 auto	Select the speed for this interface.
	Duplex	Auto	Select the duplex mode for this interface.
	MTU	1500	Enter the Maximum Transmit Unit for this interface (68 - 1500).
	Public Interface IPSec Fragmentation Policy	<input checked="" type="radio"/> Do not fragment prior to IPSec encapsulation; fragment prior to interface transmission <input type="radio"/> Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP) <input type="radio"/> Fragment prior to IPSec encapsulation without Path MTU Discovery (Clear DF bit)	

Apply Cancel

79326

Disabled

To make the interface offline, click **Disabled**. This state lets you retain or change its configuration parameters

If the interface is configured but disabled (offline), the appropriate Ethernet Link Status LED blinks green on the VPN Concentrator front panel.

DHCP Client

Check the **DHCP Client** check box if you want to obtain the IP address, the subnet mask, and the default gateway for this interface via DHCP. If you check this box, do not make entries in the IP address and subnet mask fields that follow.

**Note**

Because some Internet service providers require that the host name be specified in DHCP requests, you might have to specify the system name when running the DHCP Client on the VPN Concentrator public interface. (Specify the system name on the Configuration | System | General | Identification screen.) The VPN Concentrator uses the system name as the host name in DHCP requests.

Static IP Addressing

IP Address

If you want to set a static IP address for this interface, enter the IP address here, using dotted decimal notation (for example, 192.168.12.34). Note that 0.0.0.0 is not allowed. Be sure no other device is using this address on the network.

Subnet Mask

Enter the subnet mask for this interface, using dotted decimal notation (for example, 255.255.255.0). The Manager automatically supplies a standard subnet mask appropriate for the IP address you just entered. For example, the IP address 192.168.12.34 is a Class C address, and the standard subnet mask is 255.255.255.0. You can accept this entry or change it. Note that 0.0.0.0 is not allowed.

Public Interface

To make this interface a public interface, check the **Public Interface** check box. A public interface is an interface to a public network, such as the Internet. You must configure a public interface before you can configure NAT and IPSec LAN-to-LAN, for example. You should designate only one VPN Concentrator interface as a public interface.

MAC Address

This is the unique hardware MAC (Medium Access Control) address for this interface, displayed in six byte hexadecimal notation. You cannot change this address.

Filter

The filter governs the handling of data packets through this interface: whether to forward or drop, in accordance with configured criteria. Cisco supplies three default filters that you can modify and use with the VPN Concentrator. You can configure filters on the Configuration | Policy Management | Traffic Management screens.

Click the drop-down menu button and choose the filter to apply to this interface:

- 1. Private (Default) = Allow all packets except source-routed IP packets. Cisco supplies this default filter for Ethernet 1, but it is not selected by default.
- 2. Public (Default) = Allow inbound and outbound tunneling protocols plus ICMP and VRRP. Allow fragmented IP packets. Drop everything else, including source-routed packets. Cisco supplies this default filter for Ethernet 2, and it is selected by default for Ethernet 2.
- 3. External (Default) = No rules applied to this filter. Drop all packets. Cisco supplies this default filter for Ethernet 3, but it is not selected by default.
- –None– = No filter applied to the interface, which means there are no restrictions on data packets. This is the default selection for Ethernet 1 and 3.

Other filters that you have configured also appear in this menu.

Speed

Click the **Speed** drop-down menu button and choose the interface speed:

- 10 Mbps = Fix the speed at 10 megabits per second (10Base-T networks).
- 100 Mbps = Fix the speed at 100 megabits per second (100Base-T networks).
- 10/100 auto = Let the VPN Concentrator automatically detect and set the appropriate speed, either 10 or 100 Mbps (default). Be sure that the port on the active network device (hub, switch, router, etc.) to which you connect this interface is also set to automatically negotiate the speed. Otherwise, choose the appropriate fixed speed.

Duplex

Click the **Duplex** drop-down menu button and choose the interface transmission mode:

- Auto = Let the VPN Concentrator automatically detect and set the appropriate transmission mode, either full or half duplex (default). Be sure that the port on the active network device (hub, switch, router, etc.) to which you connect this interface is also set to automatically negotiate the transmission mode. Otherwise, choose the appropriate fixed mode.
- Full-Duplex = Fix the transmission mode as full duplex: transmission in both directions at the same time.
- Half-Duplex = Fix the transmission mode as half duplex: transmission in only one direction at a time.

MTU

The MTU value specifies the maximum transmission unit (that is, packet size) in bytes for the interface. Valid values range from 68 through 1500. The default value, 1500, is the MTU for Ethernet.

IPSec Fragmentation

The IPSec fragmentation policy specifies how to treat packets that exceed the MTU setting when tunneling traffic through the public interface. This feature provides a way to handle cases where a router or NAT device between the VPN Concentrator and the client rejects or drops IP fragments. For example, suppose a client wants to FTP get from an FTP server behind a VPN Concentrator. The FTP server transmits packets that when encapsulated would exceed the VPN Concentrator's MTU size on the public interface. The following options determine how the VPN Concentrator processes these packets.

The fragmentation policy you set here applies to all traffic travelling out the VPN Concentrator public interface to clients running version 3.6 or later software. The second and third options described below may affect performance.

**Note**

Clients running software versions earlier than 3.6 or L2TP over IPSec clients can use only the first option, "Do not fragment prior to IPSec encapsulation; fragment prior to interface transmission."

The setting you configure applies to 3.6 clients only. The VPN Concentrator ignores the setting for clients running software versions earlier than 3.6 and protocols other than IPSec. For these clients the first option applies: "Do not fragment prior to IPSec encapsulation; fragment prior to interface transmission."

Do not fragment prior to IPSec encapsulation; fragment prior to interface transmission

The VPN Concentrator encapsulates all tunneled packets. After encapsulation, the VPN Concentrator fragments packets that exceed the MTU setting before transmitting them through the public interface. This is the default policy for the VPN Concentrator. This option works for situations where fragmented packets are allowed through the tunnel without hindrance. For the FTP example, large packets are encapsulated and then fragmented at the IP layer. Intermediate devices may drop fragments or just out-of-order fragments. Load-balancing devices can introduce out-of-order fragments.

Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP)

The VPN Concentrator fragments tunneled packets that would exceed the MTU setting during encapsulation. For this option, the VPN Concentrator drops large packets that have the Don't Fragment (DF) bit set, and sends an ICMP message "Packet needs to be fragmented but DF is set" to the packet's initiator. The ICMP message includes the maximum MTU size allowed. Path MTU Discovery means that an intermediate device (in this case the VPN Concentrator) informs the source of the MTU permitted to reach the destination.

If a large packet does not have the DF bit set, the VPN Concentrator fragments prior to encapsulating thus creating two independent non-fragmented IP packets and transmits them out the public interface. This is the default policy for the VPN 3002 hardware client.

For this example, the FTP server may use Path MTU Discovery to adjust the size of the packets it transmits to this destination.

Fragment prior to IPSec encapsulation without Path MTU Discovery (Clear DF bit)

The VPN Concentrator fragments tunneled packets that exceed the MTU setting before encapsulating them. If the DF bit on these packets is set, the VPN Concentrator clears the DF bit, fragments the packets, and then encapsulates them. This action creates two independent non-fragmented IP packets leaving the public interface and successfully transmits these packets to the peer site by turning the fragments into complete packets to be reassembled at the peer site.

In our example, the VPN Concentrator overrides the MTU and allows fragmentation by clearing the DF bit.

RIP Parameters Tab

RIP is a routing protocol that routers use for messages to other routers, to determine network connectivity, status, and optimum paths for sending data traffic. RIP uses distance-vector routing algorithms, and it is an older protocol that generates more network traffic than OSPF. The VPN Concentrator includes IP routing functions that support RIP versions 1 and 2. Many private networks with simple topologies still use RIPv1, although it lacks security features. RIPv2 is generally considered the preferred version; it includes functions for authenticating other routers, for example.

To use the Network Autodiscovery feature in IPsec LAN-to-LAN configuration, or to use the automatic list generation feature in Network Lists, you must enable Inbound RIPv2/v1 on Ethernet 1. (It is enabled by default.)

Figure 3-6 Configuration | Interfaces | Ethernet 1 2 3 screen, RIP Tab

Configuration | Interfaces | Ethernet 1

Warning: You are modifying the interface you are using to connect to this device. If you make any changes, you will break the connection and you will have to restart from the login screen.

Configuring Ethernet Interface 1 (Private).

General RIP OSPF Bandwidth

RIP Parameters		
Attribute	Value	Description
Inbound RIP	RIPv2/v1	Select the method of inbound RIP processing for this interface.
Outbound RIP	Disabled	Select the method of outbound RIP processing for this interface.

Apply Cancel

79327

Inbound RIP

This parameter applies to RIP messages coming into the VPN Concentrator. It configures the system to listen for RIP messages on this interface.

Click the **Inbound RIP** drop-down menu button and choose the inbound RIP function:

- Disabled = No inbound RIP functions. The system does not listen for any RIP messages on this interface (default for Ethernet 2 and 3).
- RIPv1 Only = Listen for and interpret only RIPv1 messages on this interface.
- RIPv2 Only = Listen for and interpret only RIPv2 messages on this interface.
- RIPv2/v1 = Listen for and interpret either RIPv1 or RIPv2 messages on this interface (default for Ethernet 1).

Outbound RIP

This parameter applies to RIP messages going out of the VPN Concentrator; that is, it configures the system to send RIP messages on this interface.

Click the **Outbound RIP** drop-down menu button and choose the outbound RIP function:

- Disabled = No outbound RIP functions. The system does not send any RIP messages on this interface (default).
- RIPv1 Only = Send only RIPv1 messages on this interface.
- RIPv2 Only = Send only RIPv2 messages on this interface.
- RIPv2/v1 compatible = Send RIPv2 messages that are compatible with RIPv1 on this interface.


OSPF Parameters Tab

OSPF is a routing protocol that routers use for messages to other routers, to determine network connectivity, status, and optimum paths for sending data traffic. OSPF uses link-state routing algorithms, and it is a newer protocol than RIP. It generates less network traffic and generally provides faster routing updates, but it requires more processing power than RIP. The VPN Concentrator includes IP routing functions that support OSPF version 2 (RFC 2328).

OSPF involves interface-specific parameters that you configure here, and system-wide parameters that you configure on the Configuration | System | IP Routing screens.

Figure 3-7 Configuration | Interfaces | Ethernet 1 2 3 Screen, OSPF Tab

Configuration | Interfaces | Ethernet 1

 You are modifying the interface you are using to connect to this device. If you make any changes, you will break the connection and you will have to restart from the login screen.

Configuring Ethernet Interface 1 (Private).

General
RIP
OSPF
Bandwidth

OSPF Parameters		
Attribute	Value	Description
OSPF Enabled	<input type="checkbox"/>	Check to enable OSPF on this interface.
OSPF Area ID	0.0.0.0	Enter the OSPF Area ID for this interface. The format is the same as an IP address.
OSPF Priority	1	Enter the OSPF Priority for this interface.
OSPF Metric	1	Enter the OSPF Metric for this interface.
OSPF Retransmit Interval	5	Enter the OSPF Retransmit Interval for this interface.
OSPF Hello Interval	10	Enter the OSPF Hello Interval for this interface.
OSPF Dead Interval	40	Enter the OSPF Dead Interval for this interface.
OSPF Transit Delay	1	Enter the OSPF Transit Delay for this interface.
OSPF Authentication	None	Select the OSPF Authentication method to use.
OSPF Password		Enter the OSPF Password when <i>Simple Password</i> or <i>MD5</i> is selected above.

Apply
Cancel

79328

OSPF Enabled

To enable OSPF routing on this interface, check the **OSPF Enabled** check box. (By default it is unchecked.)

To activate the OSPF system, you must also configure and enable OSPF on the Configuration | System | IP Routing | OSPF screen.

OSPF Area ID

The area ID identifies the subnet area within the OSPF Autonomous System or domain. Routers within an area have identical link-state databases. While its format is that of a dotted decimal IP address, the ID is only an identifier and not an address.

The 0.0.0.0 area ID identifies a special area, the backbone, that contains all area border routers, which are the routers connected to multiple areas.

Enter the area ID in the field, using IP address format in dotted decimal notation (for example, 10.10.0.0). The default entry is 0.0.0.0, the backbone. Your entry also appears in the OSPF Area list on the Configuration | System | IP Routing | OSPF Areas screen.

OSPF Priority

This entry assigns a priority to the OSPF router on this interface. OSPF routers on a network elect one to be the Designated Router, which has the master routing database and performs other administrative functions. In case of a tie, the router with the highest priority number wins. A 0 entry means this router is ineligible to become the Designated Router.

Enter the priority as a number from 0 to 255. The default is 1.

OSPF Metric

This entry is the metric, or cost, of the OSPF router on this interface. The cost determines preferred routing through the network, with the lowest cost being the most desirable.

Enter the metric as a number from 1 to 65535. The default is 1.

OSPF Retransmit Interval

This entry is the number of seconds between OSPF Link State Advertisements (LSAs) from this interface, which are messages that the router sends to describe its current state.

Enter the interval as a number from 0 to 3600 seconds. The default is 5 seconds, which is a typical value for LANs.

OSPF Hello Interval

This entry is the number of seconds between Hello packets that the router sends to announce its presence, join the OSPF routing area, and maintain neighbor relationships. This interval must be the same for all routers on a common network.

Enter the interval as a number from 1 to 65535 seconds. The default is 10 seconds, which is a typical value for LANs.

OSPF Dead Interval

This entry is the number of seconds for the OSPF router to wait before it declares that a neighboring router is out of service, after the router no longer sees the neighbor's Hello packets. This interval should be some multiple of the Hello Interval, and it must be the same for all routers on a common network.

Enter the interval as a number from 0 to 65535 seconds. The default is 40 seconds, which is a typical value for LANs.

OSPF Transit Delay

This entry is the estimated number of seconds it takes to transmit a link state update packet over this interface, and it should include both the transmission and propagation delays of the interface. This delay must be the same for all routers on a common network.

Enter the delay as a number from 0 to 3600 seconds. The default is 1 second, which is a typical value for LANs.

OSPF Authentication

This parameter sets the authentication method for OSPF protocol messages. OSPF messages can be authenticated so that only trusted routers can route messages within the domain. This authentication method must be the same for all routers on a common network.

Click the **OSPF Authentication** drop-down menu button and choose the authentication method:

- None = No authentication. OSPF messages are not authenticated (default).
- Simple Password = Use a clear-text password for authentication. This password must be the same for all routers on a common network. If you choose this method, enter the password in the OSPF Password field that follows.
- MD5 = Use the MD5 hashing algorithm with a shared key to generate an encrypted message digest for authentication. This key must be the same for all routers on a common network. If you choose this method, enter the key in the OSPF Password field that follows.

OSPF Password

If you chose Simple Password or MD5 for OSPF Authentication, enter the appropriate password or key in this field. Otherwise, leave the field blank.

- For Simple Password authentication, enter the common password. The maximum password length is 8 characters. The Manager displays your entry in clear text.
- For MD5 authentication, enter the shared key. The maximum shared key length is 8 characters. The Manager displays your entry in clear text.

Apply / Cancel

To apply your settings to this interface and include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | Interfaces screen.

Bandwidth Parameters Tab

The Bandwidth Parameters Tab lets you enable bandwidth management on the selected interface, define the link rate for the interface and assign a bandwidth management policy to be used on the interface. Before you do these steps, you must have already created a bandwidth management policy. To create a bandwidth management policy, use the Configuration | Policy Management | Traffic Management | Bandwidth Policies | Add screen.

For detailed information on the Bandwidth Management feature, see the Configuration | Policy Management | Traffic Management | Bandwidth Policies | Add or Modify section.

Figure 3-8 Configuration | Interfaces | Ethernet 1 2 3 Screen, Bandwidth Tab

Configuration | Interfaces | Ethernet 2

Configuring Ethernet Interface 2 (Public).

General | RIP | OSPF | **Bandwidth**

Bandwidth Management Parameters		
Attribute	Value	Description
Bandwidth Management	<input type="checkbox"/>	Check to enable bandwidth management.
Link Rate	1544 kbps	Set the link rate that will be applied to all tunneled traffic. The defined link rate must be based on available Internet bandwidth and not the physical LAN connection rate.
Bandwidth Policy	—None—	This policy is applied to all VPN tunnels that do not have a group based Bandwidth Management policy. Policies are configured at Configuration Policy Management Traffic Management Bandwidth Policies.

Apply Cancel

79487

Bandwidth Management

To enable bandwidth management on this interface, check the **Bandwidth Management** check box.

Link Rate

The link rate is the speed of the network connection through the Internet.



Note

The defined link rate is the available Internet bandwidth, not the physical LAN connection rate. If the router in front of the VPN Concentrator has a T1 connection to the Internet, set the link rate to 1544 kbps.

Enter a value for the speed of the network connection for this interface, and select a unit of measurement.

- bps—bits per second
- kbps—one thousand bits per second
- Mbps—one million bits per second

The default link rate is 1544 kbps.

Bandwidth Policy

Select a policy from the drop-down list. If there are no policies in this list, you must go to Configuration | Policy Management | Traffic Management | Bandwidth Policies and define one or more policies.

The policy you apply here is a default bandwidth policy for all users on this interface. This policy is applied to users who do not have a bandwidth management policy applied to their group.

Apply/Cancel

To apply this change to the configuration, click **Apply**. To cancel the action, click **Cancel**.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | Interfaces screen.




System Configuration

System configuration means configuring parameters for system-wide functions in the VPN Concentrator.

Configuration | System

Step 1 In the Configuration screen, click the **System** link. The System screen opens.

Figure 4-1 Configuration | System Screen

Configuration | System Save Needed 

This section of the VPN 3000 Concentrator Manager lets you configure system-wide parameters.

In the left frame, or in the list of links below, click the parameters you want to configure:

- [Servers](#) -- authentication, accounting, DNS, DHCP, and NTP.
- [Address Management](#) -- address assignment options and address pools.
- [Tunneling Protocols](#) -- PPTP, L2TP, IPSec LAN-to-LAN, IPSec IKE proposals, and IPSec over TCP.
- [IP Routing](#) -- static routes, default gateways, OSPF, global DHCP, and redundancy (VRRP).
- [Management Protocols](#) -- FTP, HTTP/HTTPS, TFTP, Telnet, SNMP, SSL, SSH and XML.
- [Events](#) -- defaults, classes, trap destinations, syslog and SMTP servers, and email.
- [General](#) -- system name, contact, location, time and date, maximum sessions, global authentication.
- [Client Update](#) -- enable, clients, URLs, revisions.
- [Load Balancing](#) -- cluster configuration, priority, enable, etc.

67-598

This section of the Manager lets you configure parameters for VPN Concentrator system-wide functions.

- **Servers:** Identifying servers for authentication, accounting, DNS, DHCP, firewall, and NTP.
- **Address Management:** Assigning addresses to clients as a tunnel is established.
- **Tunneling Protocols:** Configuring PPTP, L2TP, IPSec LAN-to-LAN connections, Internet Key Exchange (IKE) proposals, and NAT Transparency.
- **IP Routing:** Configuring static routes, default gateways, OSPF, global DHCP, DHCP Relay, redundancy (VRRP), and Reverse Route Injection (RRI).
- **Management Protocols:** Configuring and enabling built-in servers for FTP, HTTP/HTTPS, TFTP, Telnet, SNMP, SSL, SSH, and XML.
- **Events:** Handling system events via logs, FTP backup, SNMP traps, syslog, SMTP, and e-mail.
- **General:** Identifying the system, setting the time and date, changing the maximum session limit, and configuring global authentication parameters.
- **Client Update:** Automatically updates client software.
- **Load Balancing:** Configuring virtual clusters and individual devices within virtual clusters.

See the appropriate chapter in this manual or the online help for each section.



Servers

Configuring servers means identifying them to the VPN 3000 Concentrator so it can communicate with them correctly. These servers provide user authentication and accounting functions, convert host names to IP addresses, assign client IP addresses, and synchronize the system with network time. The VPN Concentrator functions as a client of these servers.

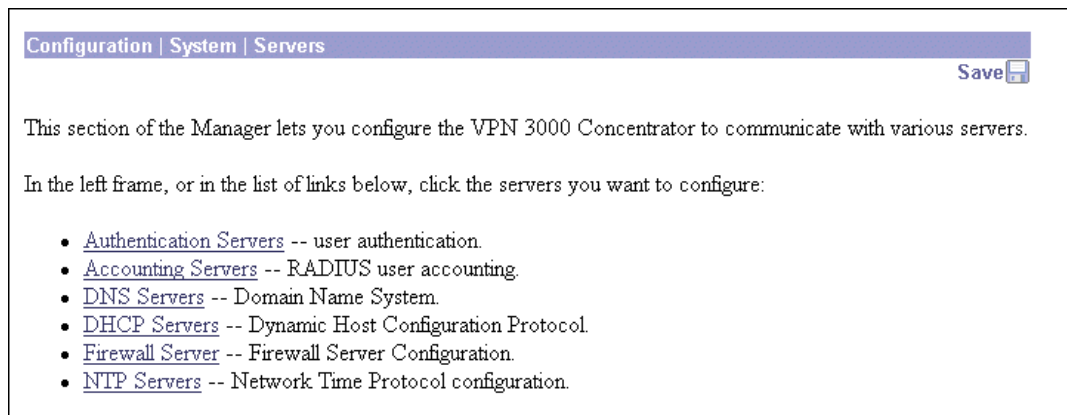
Configuration | System | Servers

This section of the Manager lets you configure the VPN Concentrator to communicate with servers for various functions.

- Authentication Servers: User authentication.
- Accounting Servers: RADIUS user accounting.
- DNS Servers: Domain Name System.
- DHCP Servers: Dynamic Host Configuration Protocol.
- Firewall Servers: Firewall enforcement by means of the Zone Labs Integrity Server.
- NTP Servers: Network Time Protocol.

You can also configure the VPN Concentrator internal authentication server here if you have not already done so during Quick Configuration.

Figure 5-1 Configuration | System | Servers Screen



68207

Configuration | System | Servers | Authentication

This section lets you configure the VPN Concentrator internal server and external RADIUS, NT Domain, and SDI servers for authenticating users. To create and use a VPN, you must configure at least one authentication server type; there must be at least one method of authenticating users.

If you check Use Address from Authentication Server on the Configuration | System | Address Management | Assignment screen, you must configure an authentication server here.

You must also configure servers here that correspond to the settings for Authentication method on the IPsec Parameters tab on the Configuration | User Management | Base Group and Group screens. For example, if you specify RADIUS authentication under IPsec for the base group, you must configure at least one RADIUS authentication server here. And in this example, the first RADIUS server is considered the primary server, the second RADIUS server is backup, etc.; any other server types are ignored.

Before you configure an external server here, be sure that the external server you reference is itself properly configured and that you know how to access it (IP address or host name, TCP/UDP port, secret/password, etc.). The VPN Concentrator functions as the client of these servers.

The Cisco VPN 3000 Series Concentrator software CD-ROM provides a link to an evaluation copy of the Cisco Secure ACS RADIUS Server software on the Cisco Web server.

After you have configured an external authentication server, you can also test it. Testing sends a username and password to the server to determine that the VPN Concentrator is communicating properly with it, and that the server properly authenticates valid users and rejects invalid users.

If you configure the internal authentication server, you can add users to the internal database by clicking the highlighted link, which takes you to the Configuration | User Management | Users screen. To configure the internal server, you just add at least one user or group to the internal database.

If you configure IPsec on the Quick Configuration | Protocols screen, the VPN Concentrator automatically configures the internal authentication server. The internal server is also the default selection on the Quick Configuration | Authentication screen.

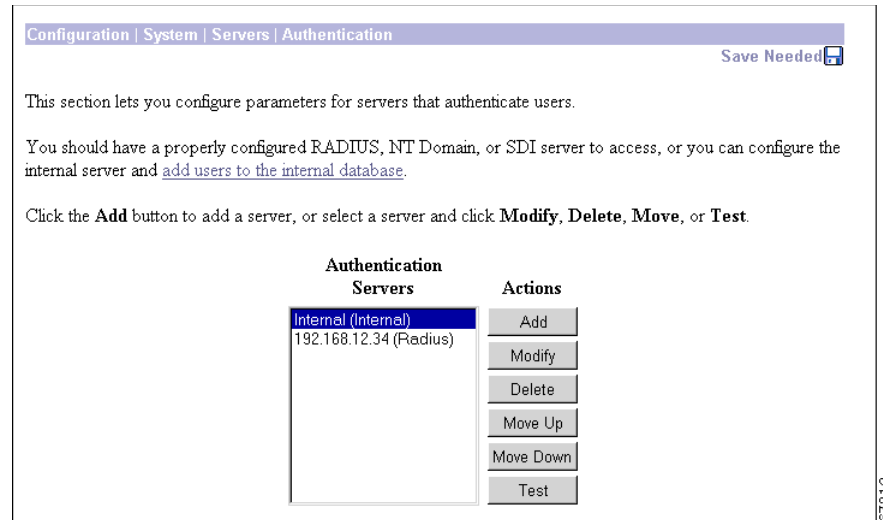
You can configure and prioritize up to 10 authentication servers here. The first server of a given type is the primary server for that type, and the rest are backup servers in case the primary is inoperative. After you configure authentication server(s), you assign them to groups and users; see [Chapter 14, “User Management,”](#) for information about configuring groups and users to use authentication servers.

Different Handling: PPTP Clients and Cisco VPN Clients

The VPN Concentrator handles authentication differently for PPTP clients and the Cisco VPN Client.

- For PPTP Clients: The VPN Concentrator authenticates the user first. If the user uses the RADIUS Server for authentication and the RADIUS server returns a group name in the Class attribute (#25), then the VPN Concentrator authenticates the group. The VPN Concentrator can authenticate the group either through the Internal database (Internal Authentication Server) or RADIUS (External Authentication Server).
- For the Cisco VPN Client: The VPN Concentrator authenticates the group first, either through the Internal Group database (Internal) or RADIUS (External). The VPN Concentrator then authenticates the user through the method selected in the group attributes for that user under the attribute Authentication Type (that is, RADIUS, SDI, Internal, etc.).

Figure 5-2 Configuration | System | Servers | Authentication Screen



Authentication Servers

The Authentication Servers list shows the configured servers, in priority order. Each entry shows the server identifier and type, for example: 192.168.12.34 (Radius). If no servers have been configured, the list shows --Empty--. The first server of each type is the primary, the rest are backup.

Add / Modify / Delete / Move / Test

To configure a new user-authentication server, click **Add**. The Manager opens the Configuration | System | Servers | Authentication | Add screen.

To modify a configured user authentication server, select the server from the list and click **Modify**. The Manager opens the Configuration | System | Servers | Authentication | Modify screen. The internal server has no configurable parameters, therefore there is no Modify screen. If you select the internal server and click **Modify**, the Manager displays an error message.

To remove a configured user authentication server, select the server from the list and click **Delete**.



Note

There is no confirmation or undo, except for the Internal Server (see the Configuration | System | Servers | Authentication | Delete screen).

The Manager refreshes the screen and shows the remaining entries in the Authentication Servers list.

**Note**

If you delete a server, users authenticated by that server will no longer be able to access the VPN unless another configured server can authenticate them.

To change the priority order for configured servers, select the entry from the list and click **Move [Up Arrow]** or **Move [Down Arrow]**. The Manager refreshes the screen and shows the reordered Authentication Servers list.

To test a configured external user authentication server, select the server from the list and click **Test**. The Manager opens the Configuration | System | Servers | Authentication | Test screen. There is no need to test the internal server, and trying to do so returns an error message.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | Servers | Authentication | Add or Modify

These screens let you:

- Add: Configure and add a new user authentication server.
- Modify: Modify parameters for a configured user authentication server.

Click the **Server Type** drop-down menu button and select the type of server. The screen and its configurable fields change depending on the server type. Choices are:

- RADIUS = An external Remote Authentication Dial-In User Service server (default).
- NT Domain = An external Windows NT Domain server.
- SDI = An external RSA Security Inc. SecurID server.
- Internal Server = The internal VPN Concentrator authentication server. With this server, you can configure a maximum of 100 groups and users (combined) in the internal database. See Configuration | User Management for details.

Find your selected server type:

Server Type = RADIUS

Configure these parameters for a RADIUS (Remote Authentication Dial-In User Service) authentication server.

RADIUS Authentication Information Specific to PPTP

Most RADIUS servers do not support MSCHAP Version 1 or 2 user authentication. If you plan to use a RADIUS server that does not support MSCHAP, you must configure the base group's PPTP Authentication Protocols to PAP and/or CHAP only. By doing this, you have no data encryption and possibly no password encryption.

CiscoSecure ACS for Windows Release 2.5 and higher supports MSCHAP V.1.

To use encryption with PPTP, your RADIUS server must support MSCHAP authentication and the return attribute MSCHAP-MPPE-Keys. Some examples of RADIUS servers that support MSCHAP-MPPE-Keys are:

- Funk Software's Steel-Belted RADIUS (MSCHAP V1 only)
- Microsoft's Internet Authentication Server, which comes with the NT 4.0 Server Options Pack
- Microsoft's Commercial Internet System (MCIS 2.0)
- Internet Authentication Server in Windows 2000 Server

Figure 5-3 Configuration | System | Servers | Authentication | Add or Modify RADIUS Screen

Configuration | System | Servers | Authentication | Add

Configure and add a user authentication server.

Server Type Selecting *Internal Server* will let you add users to the internal user database.

Authentication Server Enter IP address or hostname.

Server Port Enter 0 for default port (1645).

Timeout Enter the timeout for this server (seconds).

Retries Enter the number of retries for this server.

Server Secret Enter the RADIUS server secret.

Verify Re-enter the secret.

67308

Authentication Server

Enter the IP address or host name of the RADIUS authentication server, for example: 192.168.12.34. The maximum number of characters is 32. (If you have configured a DNS server, you can enter a host name in this field; otherwise, enter an IP address.)

Server Port

Enter the UDP port number by which you access the server. Enter **0** (the default) to have the system supply the default port number, 1645.



Note

The latest RFC states that RADIUS should be on UDP port number 1812, so you might need to change this default value to 1812.

Timeout

Enter the time in seconds to wait after sending a query to the server and receiving no response, before trying again. The minimum time is 1 second. The default time is 4 seconds. The maximum time is 30 seconds.

Retries

Enter the number of times to retry sending a query to the server after the timeout period. If there is still no response after this number of retries, the VPN Concentrator declares this server inoperative and uses the next RADIUS authentication server in the list. The minimum number of retries is 0. The default number is 2. The maximum number is 10.

Server Secret

Enter the RADIUS server secret (also called the shared secret), for example: C8z077f. The maximum field length is 64 characters. The field shows only asterisks.

Verify

Re-enter the RADIUS server secret to verify it. The field shows only asterisks.

Add or Apply / Cancel

To add the new server to the list of configured user authentication servers, click **Add**. Or to apply your changes to the configured server, click **Apply**. Both actions include your entries in the active configuration. The Manager returns to the Configuration | System | Servers | Authentication screen. Any new server appears at the bottom of the Authentication Servers list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | Servers | Authentication screen, and the Authentication Servers list is unchanged.

Server Type = NT Domain

Configure these parameters for a Windows NT Domain authentication server.

Figure 5-4 Configuration | System | Servers | Authentication | Add or Modify NT Domain Screen

Authentication Server Address

Enter the IP address of the NT Domain authentication server, for example: 192.168.12.34. Use dotted decimal notation.

Server Port

Enter the TCP port number by which you access the server. Enter 0 (the default) to have the system supply the default port number, 139.

Timeout

Enter the time in seconds to wait after sending a query to the server and receiving no response, before trying again. The minimum time is 1 second. The default time is 4 seconds. The maximum time is 30 seconds.

Retries

Enter the number of times to retry sending a query to the server after the timeout period. If there is still no response after this number of retries, the VPN Concentrator declares this server inoperative and uses the next NT Domain authentication server in the list. The minimum number of retries is 0. The default number of retries is 2. The maximum number of retries is 10.

Domain Controller Name

Enter the NT Primary Domain Controller host name for this server, for example: PDC01. The maximum host name length is 16 characters. You must enter this name, and it must be the correct host name for the server for which you entered the IP address in Authentication Server Address; if it is incorrect, authentication will fail.

Add or Apply / Cancel

To add the new server to the list of configured user authentication servers, click **Add**. Or to apply your changes to the configured server, click **Apply**. Both actions include your entries in the active configuration. The Manager returns to the Configuration | System | Servers | Authentication screen. Any new server appears at the bottom of the Authentication Servers list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | Servers | Authentication screen, and the Authentication Servers list is unchanged.

Server Type = SDI

Configure these parameters for an RSA Security Inc. SecurID authentication server.

VPN Concentrator software version 3.6 supports both version 5.0 and versions prior to SDI 5.0.

SDI Version pre-5.0

SDI versions prior to 5.0 use the concept of an SDI master and an SDI slave server which share a single node secret file (SECURID). On the VPN Concentrator you can configure one pre-5.0 SDI master server and one SDI slave server globally, and one SDI master and one SDI slave server per each group.

SDI Version 5.0

SDI version 5.0 uses the concepts of an SDI primary and SDI replica servers. A primary and its replicas share a single node secret file. On the VPN Concentrator you can configure one SDI 5.0 server globally, and one per each group.

A version 5.0 SDI server that you configure on the VPN Concentrator can be either the primary or any one of the replicas. See the section below, “[SDI Primary and Replica Servers](#)” for information about how the SDI agent selects servers to authenticate users.

You can have one SDI primary server, and up to 10 replicas; use the SDI documentation for configuration instructions. The primary and all the replicas can authenticate users. Each primary and its replicas share a single node secret file. The node secret file has its name based on the hexadecimal value of the ACE/Server IP address with .sdi appended. SDI servers that you configure here apply globally. You can also configure SDI servers on a group basis (see Configuration | User Management | Groups, and click **Add/Modify Auth Servers**).

Two-step Authentication Process

SDI version 5.0 uses a two-step process to prevent an intruder from capturing information from an RSA SecurID authentication request and using it to authenticate to another server. The Agent first sends a lock request to the SecurID server before sending the user authentication request. The server locks the username, preventing another (replica) server from accepting it. This means that the same user cannot authenticate to two VPN Concentrators using the same authentication servers simultaneously. After a successful username lock, the VPN Concentrator sends the passcode.

SDI Primary and Replica Servers

The VPN Concentrator obtains the server list when the first user authenticates to the configured server, which can be either a primary or a replica. The VPN Concentrator then assigns priorities to each of the servers on the list, and subsequent server selection derives at random from those assigned priorities. The highest priority servers have a higher likelihood of being selected.

Figure 5-5 Configuration | System | Servers | Authentication | Add or Modify SDI Screen

Configuration | System | Servers | Authentication | Add

Configure and add a user authentication server.

Server Type Selecting *Internal Server* will let you add users to the internal user database.

Authentication Server Enter IP address or hostname.

SDI Server Version Choose SDI Server Version.

Server Port Enter 0 for default port (5500).

Timeout Enter the timeout for this server (seconds).

Retries Enter the number of retries for this server.

79361

Authentication Server

Enter the IP address or host name of the SDI authentication server, for example: 192.168.12.34. The maximum host name length is 32 characters. (If you have configured a DNS server, you can enter a host name in this field; otherwise, enter an IP address.)

SDI Server Version

Use the drop-down menu to select the SDI server version you are using, pre-5.0 or 5.0.

Server Port

Enter the UDP port number by which you access the server. Enter **0** (the default) to have the system supply the default port number, 5500.

Timeout

Enter the time in seconds to wait after sending a query to the server and receiving no response, before trying again. The minimum value is 1 second. The default value is 4 seconds. The maximum value is 30 seconds.

Retries

Enter the number of times to retry sending a query to the server after the timeout period. If there is still no response after this number of retries, the VPN Concentrator declares this server inoperative and uses the next SDI authentication server in the list. The minimum number of retries is 0. The default number of retries is 2. The maximum number is 10.

Add or Apply / Cancel

To add the new server to the list of configured user authentication servers, click **Add**. Or to apply your changes to the configured server, click **Apply**. Both actions include your entries in the active configuration. The Manager returns to the Configuration | System | Servers | Authentication screen. Any new server appears at the bottom of the Authentication Servers list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | Servers | Authentication screen, and the Authentication Servers list is unchanged.

Server Type = Internal Server

The VPN Concentrator internal authentication server lets you enter a maximum of 100 groups and users (combined) in its database. To do so, see the Configuration | User Management screens, or click the highlighted link on the Configuration | System | Servers | Authentication screen.

The internal server has no configurable parameters, therefore there is no Modify screen. If you select the internal server and click **Modify** on the Configuration | System | Servers | Authentication screen, the Manager displays an error message.

You can configure only one instance of the internal server.

Figure 5-6 Configuration | System | Servers | Authentication | Add Internal Server Screen

Configuration | System | Servers | Authentication | Add

Configure and add a user authentication server.

Server Type Selecting *Internal Server* will let you add users to the internal user database.

67306

Add / Cancel

To add the internal server to the list of configured user authentication servers, and to include the entry in the active configuration, click **Add**. The Manager returns to the Configuration | System | Servers | Authentication screen. The new server appears at the bottom of the Authentication Servers list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entry, click **Cancel**. The Manager returns to the Configuration | System | Servers | Authentication screen, and the Authentication Servers list is unchanged.

Configuration | System | Servers | Authentication | Delete

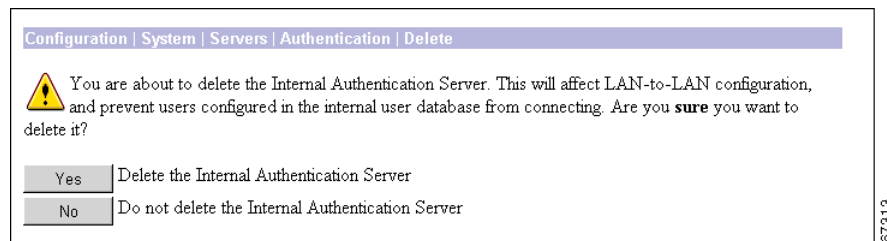
This screen asks you to confirm your decision to delete the internal authentication server. Deleting it prevents IPSec LAN-to-LAN connections, since they depend on internally configured groups for IPSec SA negotiations. Deleting it also prevents connections by all users that are configured in the internal user database.



Note

We strongly recommend that you *not* delete the internal authentication server.

Figure 5-7 Configuration | System | Servers | Authentication | Delete Screen



Yes / No

To delete the internal authentication server, click **Yes**.



Note

There is no undo.

The Manager returns to the Configuration | System | Servers | Authentication screen and shows the remaining entries in the Authentication Servers list.

To not delete the internal authentication server, click **No**. The Manager returns to the Configuration | System | Servers | Authentication screen, and the Authentication Servers list is unchanged.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | Servers | Authentication | Test

This screen lets you test a configured external user authentication server to determine that:

- The VPN Concentrator is communicating properly with the authentication server.
- The server correctly authenticates a valid user.
- The server correctly rejects an invalid user.

Figure 5-8 Configuration | System | Servers | Authentication | Test Screen

Configuration | System | Servers | Authentication | Test

Enter a username and password with which to test. Please wait for the operation to complete or timeout.

User Name

Password

OK Cancel

67314

User Name

To test connectivity and valid authentication, enter the username for a valid user who has been configured on the authentication server. The maximum username length is 32 characters. Entries are case-sensitive.

To test connectivity and authentication rejection, enter a username that is invalid on the authentication server.

Password

Enter the password for the username. Maximum 32 characters, case-sensitive. The field displays only asterisks.

OK / Cancel

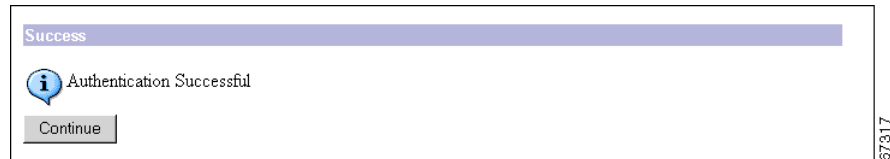
To send the username and password to the chosen authentication server, click **OK**. The authentication and response process takes a few seconds. The Manager displays a Success or Error screen.

To cancel the test and discard your entries, click **Cancel**. The Manager returns to the Configuration | System | Servers | Authentication screen.

Authentication Server Test: Success

If the VPN Concentrator communicates correctly with the authentication server, and the server correctly authenticates a valid user, the Manager displays a Success screen.

Figure 5-9 Authentication Server Test: Success Screen



Continue

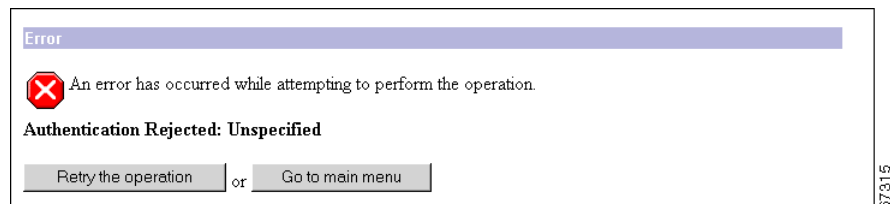
To return to the Configuration | System | Servers | Authentication | Test screen, click **Continue**. You can then test authentication for another username.

To return to the Configuration | System | Servers | Authentication screen, or any other screen, click the desired title in the left frame (Manager table of contents).

Authentication Server Test: Authentication Rejected Error

If the VPN Concentrator communicates correctly with the authentication server, and the server correctly rejects an invalid user, the Manager displays an Authentication Rejected Error screen.

Figure 5-10 Authentication Server Test: Authentication Rejected Error Screen



To return to the Configuration | System | Servers | Authentication | Test screen, click **Retry the operation**.

To go to the main VPN Concentrator Manager screen, click **Go to main menu**.

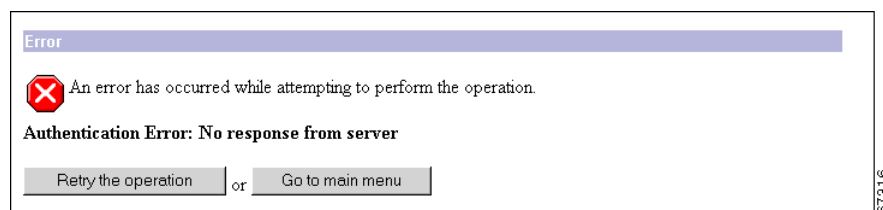
Authentication Server Test: Authentication Error

If the VPN Concentrator cannot communicate with the authentication server, the Manager displays an Authentication Error screen. Error messages include:

- No response from server = There is no response from the selected server within the configured timeout and retry periods.
- No active server found = The VPN Concentrator cannot find an active, configured server to test.

The server might be improperly configured or out of service, the network might be down or clogged, etc. Check the server configuration parameters, be sure the server is operating, check the network connections, etc.

Figure 5-11 Authentication Server Test: Authentication Error Screen



To return to the Configuration | System | Servers | Authentication | Test screen, click **Retry the operation**.

To go to the main VPN Concentrator Manager screen, click **Go to main menu**.

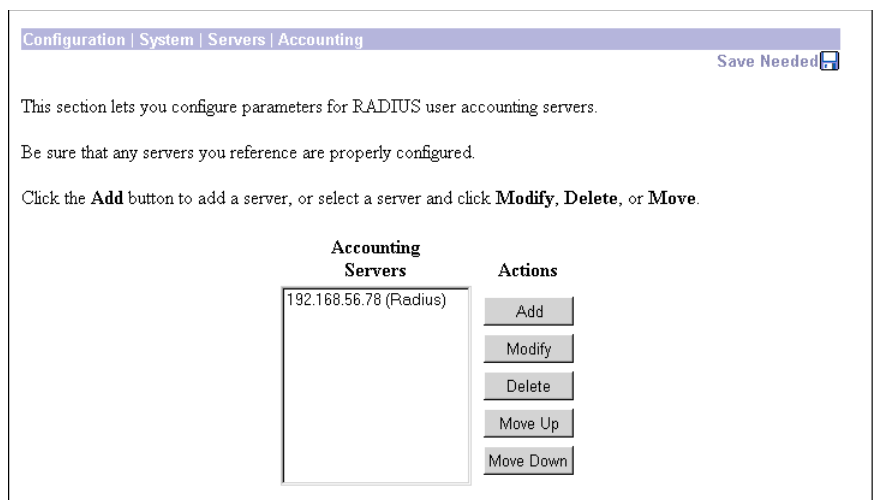
Configuration | System | Servers | Accounting

This section lets you configure external RADIUS user accounting servers, which collect data on user connect time, packets transmitted, etc., under the VPN tunneling protocols: PPTP, L2TP, and IPSec.

You can configure and prioritize up to ten accounting servers. The first server is the primary, and the rest are backup servers in case the primary is inoperative.

Before you configure an accounting server here, be sure that the server you reference is itself properly configured and that you know how to access it (IP address or host name, UDP port, server secret, etc.). The VPN Concentrator functions as the client of these servers.

Figure 5-12 Configuration | System | Servers | Accounting Screen



The VPN Concentrator communicates with RADIUS accounting servers per RFC 2139 and currently includes the attributes in [Table 5-1](#) in the accounting start and stop records. These attributes might change.

Table 5-1 RADIUS Accounting Record Attributes

Start Record	Stop Record
User Name	User Name
Acct Status Type	Acct Status Type
Class	Class
Service Type	Service Type
Framed Protocol	Framed Protocol
Framed IP Address	Framed IP Address
NAS Port	NAS Port
Acct Session ID	Session Time
Tunnel Client Endpoint Address	Input Octets
Authentic	Output Octets
Delay Time	Input Packets

Table 5-1 RADIUS Accounting Record Attributes (continued)

Start Record	Stop Record
NAS IP Address	Output Packets
NAS Port Type	Terminate Cause
Tunnel Type	Acct Session ID
	Tunnel Client Endpoint Address
	Authentic
	Delay Time
	NAS IP Address
	NAS Port Type
	Tunnel Type

Accounting Servers

The Accounting Servers list shows the configured servers, in priority order. Each entry shows the server identifier and type, for example: 192.168.12.34 (Radius). If no servers have been configured, the list shows --Empty--. The first server is the primary, the rest are backup.

Add / Modify / Delete / Move

To configure a new user accounting server, click **Add**. The Manager opens the Configuration | System | Servers | Accounting | Add screen.

To modify a configured user accounting server, select the server from the list and click **Modify**. The Manager opens the Configuration | System | Servers | Accounting | Modify screen.

To remove a configured user authentication server, select the server from the list and click **Delete**.



Note

There is no confirmation or undo.

The Manager refreshes the screen and shows the remaining entries in the Accounting Servers list.

To change the priority order for configured servers, select the entry from the list and click **Move [Up Arrow]** or **Move [Down Arrow]**. The Manager refreshes the screen and shows the reordered Accounting Servers list.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | Servers | Accounting | Add or Modify

These screens let you:

- Add: Configure and add a new RADIUS user accounting server.
- Modify: Modify parameters for a configured RADIUS user accounting server.

Figure 5-13 Configuration | System | Servers | Accounting | Add or Modify Screen

Accounting Server

Enter the IP address or host name of the RADIUS accounting server, for example: 192.168.12.34. (If you have configured a DNS server, you can enter a host name in this field; otherwise, enter an IP address.)

Server Port

Enter the UDP port number by which you access the accounting server. The default is 1646.



Note

The latest RFC states that RADIUS accounting servers should be on UDP port number 1813, so you might need to change this default value to 1813.

Timeout

Enter the time, in seconds, to wait after sending a query to the accounting server and receiving no response, before trying again. The minimum is time 1 second. The default time is 1 second. The maximum time is 30 seconds.

Retries

Enter the number of times to retry sending a query to the accounting server after the timeout period. If there is still no response after this number of retries, the system declares this server inoperative and uses the next accounting server in the list. The minimum number of retries is 0. The default number of retries is 3. The maximum number of retries is 10.

Server Secret

Enter the server secret (also called the shared secret), for example: C8z077f. The field shows only asterisks.

Verify

Re-enter the server secret to verify it. The field shows only asterisks.

Add or Apply / Cancel

To add this server to the list of configured user accounting servers, click **Add**. Or, to apply your changes to this user accounting server, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | System | Servers | Accounting screen. Any new server appears at the bottom of the Accounting Servers list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | Servers | Accounting screen, and the Accounting Servers list is unchanged.

Configuration | System | Servers | DNS

This screen lets you configure system-wide Domain Name System (DNS) servers. DNS servers convert domain names to IP addresses. Configuring DNS servers here lets you enter host names (for example, mail01.cisco.com) rather than IP addresses as you configure and manage the VPN Concentrator.

You can configure up to three DNS servers that the system queries in order.

Figure 5-14 Configuration | System | Servers | DNS Screen

Configuration | System | Servers | DNS

Configure system-wide DNS (Domain Name System) servers.

i Configuring DNS is optional, but it lets you use hostnames rather than IP addresses.

Enabled

Domain

Primary DNS Server

Secondary DNS Server

Tertiary DNS Server

Timeout Period seconds

Timeout Retries

Apply Cancel

67324

Enabled

To use DNS functions, check the **Enabled** check box (the default). To disable DNS, uncheck the box.

Domain

Enter the name of the registered domain in which the VPN Concentrator is located, for example: cisco.com. The maximum name length is 48 characters. This entry is sometimes called the domain name suffix or sub-domain. The DNS system within the VPN Concentrator automatically appends this domain name to host names before sending them to a DNS server for resolution.

Primary DNS Server

Enter the IP address of the primary DNS server, using dotted decimal notation, for example: 192.168.12.34. Be sure this entry is correct to avoid DNS resolution delays.

Secondary DNS Server

Enter the IP address of the secondary (first backup) DNS server, using dotted decimal notation. If the primary DNS server does not respond to a query within the Timeout Period specified, the system queries this server.

Tertiary DNS Server

Enter the IP address of the tertiary (second backup) DNS server, using dotted decimal notation. If the secondary DNS server does not respond to a query within the Timeout Period specified, the system queries this server.

Timeout Period

Enter the initial time in seconds to wait for a response to a DNS query before sending the query to the next server. The minimum time is 1 second. The default time is 2 seconds. The maximum time is 30 seconds. The time doubles with each retry cycle through the list of servers.

Timeout Retries

Enter the number of times to retry sending a DNS query to the configured servers, in order. In other words, this is the number of times to cycle through the list of servers before returning an error. The minimum number of retries is 0. The default number of retries is 2. The maximum number of retries is 10.

Apply / Cancel

To apply your settings for DNS servers and include the settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | Servers screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Servers screen.

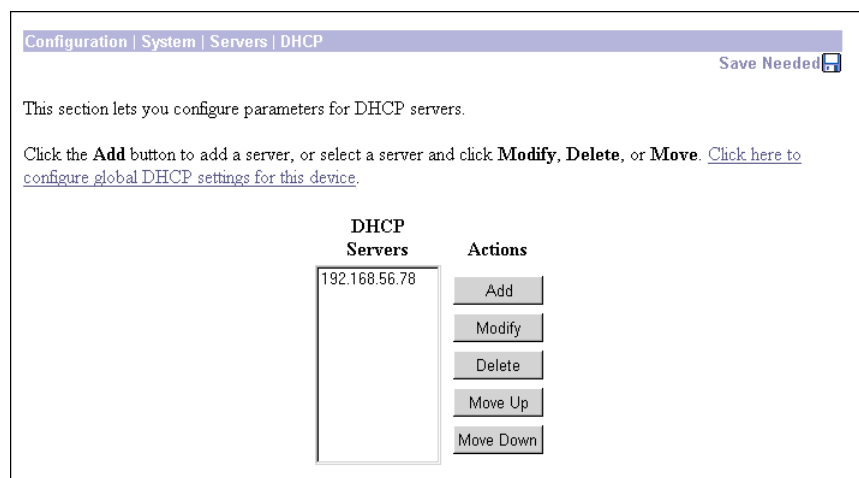
Configuration | System | Servers | DHCP

This section of the Manager lets you configure support for Dynamic Host Configuration Protocol (DHCP) servers that assign IP addresses to clients as a VPN tunnel is established.

If you check Use DHCP on the Configuration | System | Address Management | Assignment screen, you must configure at least one DHCP server here. You should also configure global DHCP parameters on the Configuration | System | IP Routing | DHCP screen; click the highlighted link to go there. The DHCP system within the VPN Concentrator is enabled by default on that screen.

You can configure and prioritize up to three DHCP servers. The first server is the primary, and the rest are backup servers in case the primary is inoperative.

Figure 5-15 Configuration | System | Servers | DHCP Screen



DHCP Servers

The DHCP Servers list shows the configured servers, in priority order. Each entry shows the server identifier, which can be an IP address or a host name, for example: 192.168.12.34. If no servers have been configured, the list shows --Empty--. The first server is the primary, the rest are backup.

Add / Modify / Delete / Move

To configure a new DHCP server, click **Add**. The Manager opens the Configuration | System | Servers | DHCP | Add screen.

To modify a configured DHCP server, select the server from the list and click **Modify**. The Manager opens the Configuration | System | Servers | DHCP | Modify screen.

To remove a configured DHCP server, select the server from the list and click **Delete**.

**Note**

There is no confirmation or undo.

The Manager refreshes the screen and shows the remaining entries in the DHCP Servers list.

**Note**

If you delete a DHCP server, any IP addresses obtained from that server will eventually time out, and the associated sessions will terminate.

To change the priority order for configured servers, select the entry from the list and click **Move [Up Arrow]** or **Move [Down Arrow]**. The Manager refreshes the screen and shows the reordered DHCP Servers list.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | Servers | DHCP | Add or Modify

These screens let you:

- Add: Configure and add a new DHCP server to the list of configured servers.
- Modify: Modify the parameters for a configured DHCP server.

Figure 5-16 Configuration | System | Servers | DHCP | Add or Modify Screen

Configuration | System | Servers | DHCP | Add

Configure and add a DHCP server.

DHCP Server Enter IP address or hostname.

Server Port

67310

DHCP Server

Enter the IP address or host name of the DHCP server, for example: 192.168.12.34. (If you have configured a DNS server, you can enter a host name in this field; otherwise, enter an IP address.)

Server Port

Enter the UDP port number by which you access the DHCP server. The default UDP port number is 67.

Add or Apply / Cancel

To add this server to the list of configured DHCP servers, click **Add**. Or, to apply your changes to this DHCP server, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | System | Servers | DHCP screen. Any new server appears at the bottom of the DHCP Servers list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | Servers | DHCP screen, and the DHCP Servers list is unchanged.

Configuration | System | Servers | Firewall

If any remote users in any of the groups configured on the VPN Concentrator are receiving their firewall policy from a Zone Labs Integrity Server, specify the host name or IP address of the server here. (See the “[Client FW Parameters Tab](#)” under Configuration | User Management | Base Group or Configuration | User Management | Groups | Add or Modify for more information on configuring groups to use a firewall server.) You can configure only one server.

Figure 5-17 Configuration | System | Servers | Firewall Server Screen

Configuration | System | Servers | Firewall Server

Configure Zone Labs Integrity Server.

Zone Labs Integrity Server Enter the host name or IP address of the Zone Labs Integrity Server.

Server Port

Apply Cancel

79331

Zone Labs Integrity Server

Enter the host name or the IP address of the Zone Labs Integrity Server from which remote users on this VPN Concentrator derive their firewall policy.

Server Port

Assign a port for the VPN Concentrator to use to communicate with the firewall server. The default port is 5054.

Apply/Cancel

To include your entry in the active configuration, click **Apply**. The Manager returns to the Configuration | System | Server screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entry, click **Cancel**. The Manager returns to the Configuration | System | Server screen and the server configuration is unchanged.

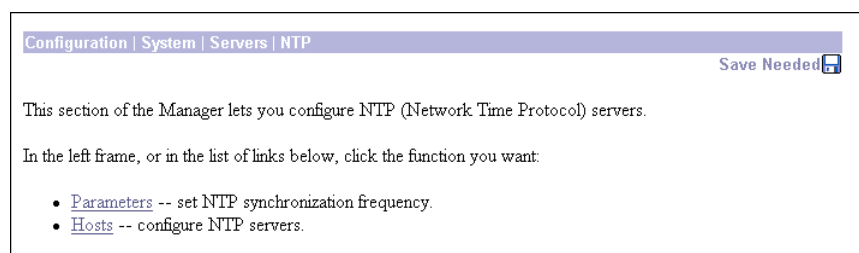
Configuration | System | Servers | NTP

This section of the Manager lets you configure NTP (Network Time Protocol) servers that the VPN Concentrator queries to synchronize with network time.

Clocks in many computers tend to drift a few seconds per day. Exact time synchronization is important for systems on a network so that protocol timestamps and events are accurate. Digital certificates, for example, carry a timestamp that determines a time frame for their validity. An inaccurate time or date could prevent connection.

To make the NTP function operational, you must configure at least one NTP server (host). You can configure up to 10 NTP servers. The VPN Concentrator queries all of them and synchronizes its system clock with the derived network time.

Figure 5-18 Configuration | System | Servers | NTP Screen



Configuration | System | Servers | NTP | Parameters

This Manager screen lets you configure the NTP synchronization frequency parameter. This parameter specifies how often the VPN Concentrator queries NTP servers to synchronize its clock with network time.

Figure 5-19 Configuration | System | Servers | NTP | Parameters Screen

Configuration | System | Servers | NTP | Parameters

Configure NTP synchronization frequency.

Sync Frequency (minutes) Enter the frequency to poll the NTP servers.

Apply Cancel

67330

Sync Frequency

Enter the synchronization frequency in minutes. The minimum is frequency is 0 minutes, which disables the NTP function. The default frequency is 60 minutes. The maximum frequency is 10080 minutes (1 week).

Apply / Cancel

To apply your NTP parameter setting and include the setting in the active configuration, click **Apply**. The Manager returns to the Configuration | System | Servers | NTP screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

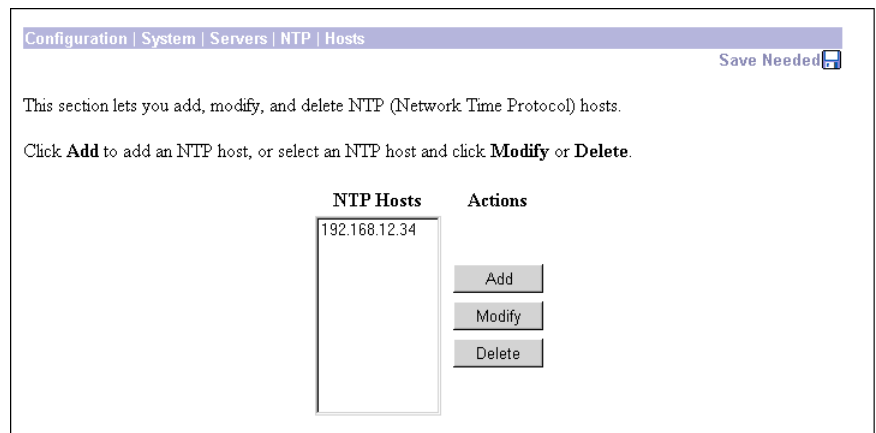
To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Servers | NTP screen.

Configuration | System | Servers | NTP | Hosts

This section of the Manager lets you add, modify, and delete NTP hosts (servers).

To make the NTP function operational, you must configure at least one NTP host. You can configure a maximum of 10 hosts. The VPN Concentrator queries all configured hosts and derives the correct network time from their responses.

Figure 5-20 Configuration | System | Servers | NTP | Hosts Screen



NTP Hosts

The NTP Hosts list shows the configured servers. Each entry shows the server identifier, which can be an IP address or a host name, for example: 192.168.12.34. If no servers have been configured, the list shows --Empty--.

Add / Modify / Delete

To configure a new NTP host (server), click **Add**. The Manager opens the Configuration | System | Servers | NTP | Hosts | Add screen.

To modify a configured NTP host, select the host from the list and click **Modify**. The Manager opens the Configuration | System | Servers | NTP | Hosts | Modify screen.

To remove a configured NTP host, select the host from the list and click **Delete**.



Note

There is no confirmation or undo.

The Manager refreshes the screen and shows the remaining entries in the NTP Hosts list.

Reminder:

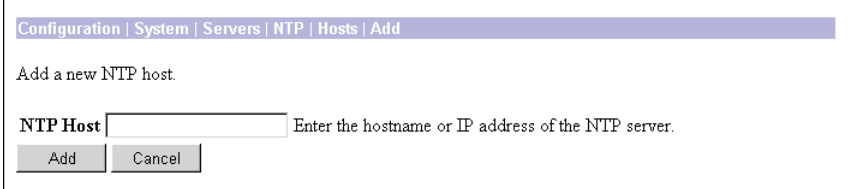
The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | Servers | NTP | Hosts | Add or Modify

These screens let you:

- Add a new NTP host to the list of configured hosts.
- Modify a configured NTP host.

Figure 5-21 Configuration | System | Servers | NTP | Hosts | Add or Modify Screen



Configuration | System | Servers | NTP | Hosts | Add

Add a new NTP host.

NTP Host Enter the hostname or IP address of the NTP server.

Add Cancel

67327

NTP Host

Enter the IP address or host name of the NTP host (server), for example: 192.168.12.34. (If you have configured a DNS server, you can enter a host name in this field; otherwise, enter an IP address.)

Add or Apply / Cancel

To add this host to the list of configured NTP hosts, click **Add**. Or, to apply your changes to a configured NTP host, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | System | Servers | NTP | Hosts screen. Any new host appears at the bottom of the NTP Hosts list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entry, click **Cancel**. The Manager returns to the Configuration | System | Servers | NTP | Hosts screen, and the NTP Hosts list is unchanged.



Address Management

IP addresses make internetwork connections possible. They are like telephone numbers: both the sender and receiver must have an assigned number in order to connect. But with VPNs, there are actually two sets of addresses: the first set connects client and server on the public network; and once that connection is made, the second set connects client and server through the VPN tunnel.

In VPN Concentrator address management, we are dealing with the second set of IP addresses: those private IP addresses that connect a client with a resource on the private network, through the tunnel, and let the client function as if it were directly connected to the private network. Furthermore, we are dealing only with the private IP addresses that get assigned to clients. The IP addresses assigned to other resources on your private network are part of your network administration responsibilities, not part of VPN Concentrator management.

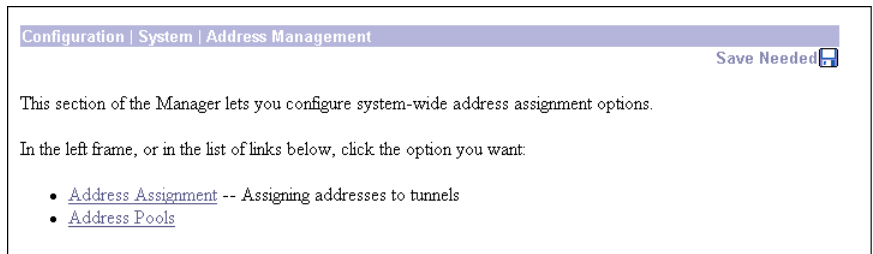
Therefore, when we discuss IP addresses here, we mean those IP addresses available in your private network addressing scheme, that let the client function as a tunnel endpoint.

Configuration | System | Address Management

This section of the VPN 3000 Concentrator Series Manager lets you configure options for assigning addresses to clients as a tunnel is established. A client must have an IP address to function as a tunnel endpoint.

- Assignment configures the prioritized methods for assigning IP addresses.
- Pools configures the internal address pools from which you can assign IP addresses.

Figure 6-1 Configuration | System | Address Management Screen



Configuration | System | Address Management | Assignment

This screen lets you select prioritized methods for assigning IP addresses to clients as a tunnel is established. The VPN Concentrator tries the selected methods in the order listed until it finds a valid IP address to assign. You must select at least one method; you can select any and all methods. There are no default methods.

If you assign addresses from a non-local subnet, you must add routes for those subnets pointing to the VPN Concentrator on your internal routers.

Figure 6-2 Configuration | System | Address Management | Assignment Screen

Configuration | System | Address Management | Assignment

This section presents Address Assignment options. Each of the following methods are tried, in order, until an address is found.

Use Client Address Check to use the IP address supplied by the client. This can be overridden by user/group configuration.

Use Address from Authentication Server Check to use an IP address retrieved from an authentication server for the client.

Use DHCP Check to use DHCP to obtain an IP address for the client.

Use Address Pools Check to use internal address pool configuration to obtain an IP address for the client.

Apply Cancel

67114

Use Client Address

Check the **Use Client Address** check box to let the client specify its own IP address. For maximum security, we recommend that you control IP address assignment and not use client-specified IP addresses. Do not check only this box if you are using IPSec, since IPSec does not allow client-specified IP addresses.

Make sure the setting here is consistent with the setting for Use Client Address on the PPTP/L2TP Parameters tab on the Configuration | User Management | Base Group screen. A different Use Client Address setting for specific groups and users overrides the setting here and on the base group screen. See the Configuration | User Management screens.

Use Address from Authentication Server

Check the **Use Address from Authentication Server** check box to assign IP addresses retrieved from an authentication server on a per-user basis. If you are using an authentication server (external or internal) that has IP addresses configured, we recommend using this method.

Check this box if you enter an IP Address and Subnet Mask on the Identity Parameters tab on the Configuration | User Management | Users | Add or Modify screens (which means you are using the internal authentication server).

Use DHCP

Check the **Use DHCP** check box to obtain IP addresses from a DHCP (Dynamic Host Configuration Protocol) server.

If you use DHCP, configure the server on the Configuration | System | Servers | DHCP and Configuration | System | IP Routing | DHCP screens.

Use Address Pools

Check the **Use Address Pools** check box to have the VPN Concentrator assign IP addresses from an internally configured pool. Internally configured address pools are the easiest method of address pool assignment to configure.

If you use this method, configure the IP address pools on the Configuration | System | Address Management | Pools screens.

Apply / Cancel

To include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | Address Management screen.

Reminder:

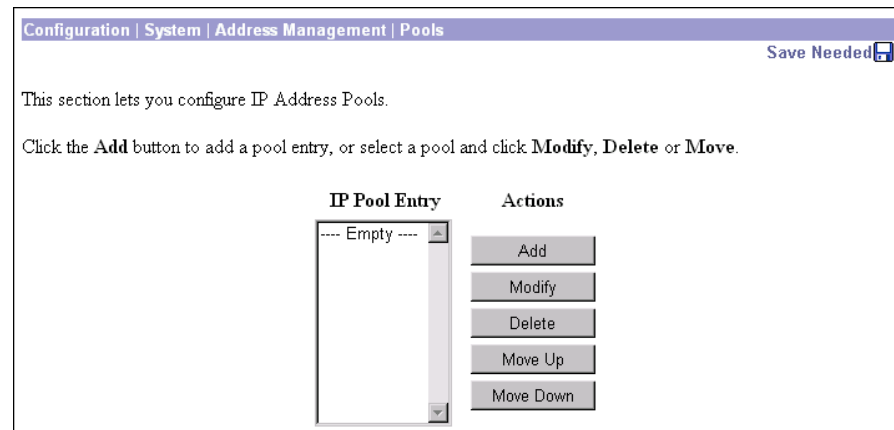
To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings or changes, click **Cancel**. The Manager returns to the Configuration | Address Management screen.

Configuration | System | Address Management | Pools

This section of the Manager lets you configure IP address pools from which the VPN Concentrator assigns addresses to clients. If you check Use Address Pools on the Configuration | System | Address Management | Assignment screen, you must configure at least one address pool. The IP addresses in the pools must not be assigned to other network resources.

Figure 6-3 Configuration | System | Address Management | Pools Screen



IP Pool Entry

The IP Pool Entry list shows each configured address pool as an address range, for example: 10.10.147.100 to 10.10.147.177. If no pools have been configured, the list shows --Empty--. The pools are listed in the order they are configured. The system uses these pools in the order listed: if all addresses in the first pool have been assigned, it uses the next pool, and so on.

If you assign addresses from a non-local subnet, we suggest that you add pools that fall on subnet boundaries in order to make adding routes for these networks easier.

Add / Modify / Delete

To configure a new IP address pool, click **Add**. The Manager opens the Configuration | System | Address Management | Pools | Add screen.

To modify an IP address pool that has been configured, select the pool from the list and click **Modify**. The Manager opens the Configuration | System | Address Management | Pools | Modify screen.

To delete an IP address pool that has been configured, select the pool from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining pools in the list.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | Address Management | Pools | Add or Modify

These screens let you:

- Add a new pool of IP addresses from which the VPN Concentrator assigns addresses to clients.
- Modify an IP address pool that you have previously configured.

The IP addresses in the pool range must not be assigned to other network resources.

Figure 6-4 Configuration | System | Address Management | Pools | Add or Modify Screen

Configuration | System | Address Management | Pools | Add

Add an address pool

Range Start Enter the start of the IP pool address range.

Range End Enter the end of the IP pool address range.

Add Cancel

Range Start

Enter the first IP address available in this pool. Use dotted decimal notation, for example: 10.10.147.100.

Range End

Enter the last IP address available in this pool. Use dotted decimal notation, for example: 10.10.147.177.

Add or Apply / Cancel

To add this IP address pool to the list of configured pools, click **Add**. Or to apply your changes to this IP address pool, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | System | Address Management | Pools screen. Any new pool appears at the end of the IP Pool Entry list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | Address Management | Pools screen, and the IP Pool Entry list is unchanged.



Tunneling Protocols

Tunneling protocols are the heart of virtual private networking. The tunnels make it possible to use a public TCP/IP network, such as the Internet, to create secure connections between remote users and a private corporate network.

The secure connection is called a tunnel, and the VPN 3000 Concentrator Series uses tunneling protocols to:

- Negotiate tunnel parameters.
- Establish tunnels.
- Authenticate users and data.
- Manage security keys.
- Encrypt and decrypt data.
- Manage data transfer across the tunnel.
- Manage data transfer inbound and outbound as a tunnel endpoint or router.

The VPN Concentrator functions as a bidirectional tunnel endpoint: it can receive plain packets from the private network, encapsulate them, create a tunnel, and send them to the other end of the tunnel where they are unencapsulated and sent to their final destination; or it can receive encapsulated packets from the public network, unencapsulate them, and send them to their final destination on the private network.

The VPN Concentrator supports the three most popular VPN tunneling protocols:

- PPTP: Point-to-Point Tunneling Protocol.
- L2TP: Layer 2 Tunneling Protocol.
- IPSec: IP Security Protocol.

It also supports L2TP over IPSec, which provides interoperability with the Windows 2000 VPN client. The VPN Concentrator is also interoperable with other clients that conform to L2TP/IPSec standards, but it does not formally support those clients.

This section explains how to configure the system-wide parameters for PPTP and L2TP, how to configure IPSec LAN-to-LAN connections, how to configure IKE proposals for IPSec Security Associations and LAN-to-LAN connections, and how to configure NAT Transparency, which includes IPSec over TCP and NAT Traversal (NAT-T).

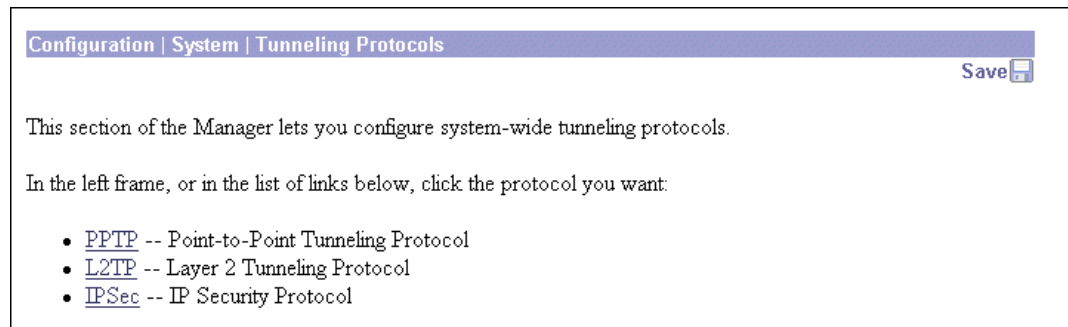
To configure L2TP over IPSec, see [Configuration | System | Tunneling Protocols | IPSec | IKE Proposals](#), and [Configuration | User Management](#).

Configuration | System | Tunneling Protocols

This section of the Manager lets you configure system-wide parameters for tunneling protocols.

- PPTP: Configure PPTP parameters.
- L2TP: Configure L2TP parameters.
- IPsec: Configure IPsec parameters and connections.
 - LAN-to-LAN: IPsec LAN-to-LAN connections between two VPN Concentrators (or between the VPN Concentrator and another secure gateway).
 - IKE Proposals: IKE proposals for IPsec Security Associations and LAN-to-LAN connections.
 - NAT Transparency: IPsec over TCP and IPsec over NAT-T

Figure 7-1 Configuration | System | Tunneling Protocols Screen



Configuration | System | Tunneling Protocols | PPTP

This screen lets you configure system-wide PPTP (Point-to-Point Tunneling Protocol) parameters.

The PPTP protocol defines mechanisms for establishing and controlling the tunnel, but uses Generic Routing Encapsulation (GRE) for data transfer.

PPTP is a client-server protocol. The VPN Concentrator always functions as a PPTP Network Server (PNS) and supports remote PC clients. The PPTP tunnel extends all the way from the PC to the VPN Concentrator.

PPTP is popular with Microsoft clients. Microsoft Dial-Up Networking (DUN) 1.2 and 1.3 under Windows 95/98 support it, as do versions of Windows NT 4.0, Windows 2000, and Windows XP. PPTP is typically used with Microsoft encryption (MPPE).

You can configure PPTP on rules in filters; see Configuration | Policy Management | Traffic Management. Groups and users also have PPTP parameters; see Configuration | User Management.

Figure 7-2 Configuration | System | Tunneling Protocols | PPTP Screen

Configuration | System | Tunneling Protocols | PPTP

This section lets you configure system-wide PPTP (Point-to-Point Tunneling Protocol) options.

Disabling PPTP will terminate any active PPTP sessions.

Enabled

Maximum Tunnel Idle Time seconds

Packet Window Size packets

Limit Transmit to Window Check to limit the transmitted packets based on the peer's receive window.

Max. Tunnels Enter 0 for unlimited tunnels.

Max. Sessions/Tunnel Enter 0 for unlimited sessions.

Packet Processing Delay 10^{ths} of seconds

Acknowledgement Delay milliseconds

Acknowledgement Timeout seconds

67343



Note

Cisco supplies default settings for PPTP parameters that ensure optimum performance for typical VPN use. We strongly recommend that you not change the defaults without advice from Cisco personnel.

Enabled

Check the **Enabled** check box to enable PPTP system-wide functions on the VPN Concentrator, or uncheck it to disable. The box is checked by default.



Caution

Disabling PPTP terminates any active PPTP sessions.

Maximum Tunnel Idle Time

Enter the time, in seconds, to wait before disconnecting an established PPTP tunnel with no active sessions. An open tunnel consumes system resources. Enter 0 to disconnect the tunnel immediately after the last session terminates (no idle time). The maximum idle time is 86400 seconds (24 hours). The default is 5 seconds.

Packet Window Size

Enter the maximum number of received but unacknowledged PPTP packets that the system can buffer. The system must queue unacknowledged PPTP packets until it can process them. The minimum number of packets is 0. The maximum number is 32. The default is 16 packets.

Limit Transmit to Window

Check the **Limit Transmit to Window** check box to limit the number of transmitted PPTP packets to the client's packet window size. Ignoring the window improves performance, provided that the client can ignore the window violation. The box is unchecked by default.

Max. Tunnels

Enter the maximum allowed number of simultaneously active PPTP tunnels. The minimum number of tunnels is 0. The maximum number of tunnels depends on the VPN Concentrator model, for example: model 3060 = 5000. Enter 0 for unlimited tunnels (the default).

Max. Sessions/Tunnel

Enter the maximum number of sessions allowed per PPTP tunnel. The minimum number of sessions is 0. The maximum number of sessions depends on the VPN Concentrator model, for example, model 3060 = 5000. Enter 0 for unlimited sessions (the default).

Packet Processing Delay

Enter the packet processing delay for PPTP flow control. This parameter is sent to the client in a PPTP control packet. Entries are in units of 100 milliseconds (0.1 second). The maximum delay is 65535; The default delay is 1 (0.1 second).

Acknowledgement Delay

Enter the number of milliseconds that the VPN Concentrator will wait to send an acknowledgement to the client when there is no data packet on which to piggyback an acknowledgement. Enter 0 to send an immediate acknowledgement. The minimum delay is 50 milliseconds. The maximum delay is 5000 milliseconds. The default delay is 500 milliseconds.

Acknowledgement Timeout

Enter the number of seconds to wait before determining that an acknowledgement has been lost, in other words, before resuming transmission to the client even though the transmit window is closed. The minimum is number of seconds is 1. The maximum number of seconds is 10. The default value is 3 seconds.

Apply / Cancel

To apply your PPTP settings and to include them in the active configuration, click **Apply**. The Manager returns to the Configuration | System | Tunneling Protocols screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Tunneling Protocols screen.

Configuration | System | Tunneling Protocols | L2TP

This screen lets you configure system-wide L2TP (Layer 2 Tunneling Protocol) parameters.

L2TP is a client-server protocol. It combines many features from PPTP and L2F (Layer 2 Forwarding), and is regarded as a successor to both. The L2TP protocol defines mechanisms both for establishing and controlling the tunnel and for transferring data.

The VPN Concentrator always functions as a L2TP Network Server (LNS) and supports remote PC clients. The L2TP tunnel extends all the way from the PC to the VPN Concentrator. When the client PC is running Windows 2000, the L2TP tunnel is typically layered over an IPSec transport connection.

You can configure L2TP on rules in filters; see Configuration | Policy Management | Traffic Management. Groups and users also have L2TP parameters; see Configuration | User Management.

Figure 7-3 Configuration | System | Tunneling Protocols | L2TP Screen

Configuration | System | Tunneling Protocols | L2TP

This section lets you configure system-wide L2TP (Layer 2 Tunneling Protocol) options.

Disabling L2TP will terminate any active L2TP sessions.

Enabled

Maximum Tunnel Idle Time seconds

Control Window Size packets

Control Retransmit Interval seconds

Control Retransmit Limit Enter the maximum number of times to retransmit control packets.

Max. Tunnels Enter 0 for unlimited tunnels.

Max. Sessions/Tunnel Enter 0 for unlimited sessions.

Hello Interval seconds

67841



Note

Cisco supplies default settings for L2TP parameters that ensure optimum performance for typical VPN use. We strongly recommend that you not change the defaults without advice from Cisco personnel.

Enabled

Check the **Enabled** check box to enable L2TP system-wide functions on the VPN Concentrator, or uncheck it to disable. The box is checked by default.



Caution

Disabling L2TP terminates any active L2TP sessions.

Maximum Tunnel Idle Time

Enter the time in seconds to wait before disconnecting an established L2TP tunnel with no active sessions. An open tunnel consumes system resources. Enter 0 to disconnect the tunnel immediately after the last session terminates (no idle time). Maximum is 86400 seconds (24 hours). The default is 60 seconds.

Control Window Size

Enter the maximum number of unacknowledged L2TP control channel packets that the system can receive and buffer. The minimum number of packets is 1. The maximum number is 16. The default number is 4.

Control Retransmit Interval

Enter the time in seconds to wait before retransmitting an unacknowledged L2TP tunnel control message to the remote client. Minimum is 1 (the default), and maximum is 10 seconds.

Control Retransmit Limit

Enter the number of times to retransmit L2TP tunnel control packets before assuming that the remote client is no longer responding. The minimum number of times is 1. The maximum number of times is 32. The default is 4 times.

Max. Tunnels

Enter the maximum allowed number of simultaneously active L2TP tunnels. The minimum value is 0 tunnels. The maximum value depends on the VPN Concentrator model; for example, model 3060 can have a maximum of 5000 tunnels. Enter **0** for unlimited tunnels. The default value is 0.

Max. Sessions/Tunnel

Enter the maximum number of sessions allowed per L2TP tunnel. The minimum number of sessions is 0. The maximum number depends on the VPN Concentrator model, for example: model 3060 = 5000. Enter 0 for unlimited sessions (the default).

Hello Interval

Enter the time in seconds to wait when the L2TP tunnel is idle (no control or payload packets received) before sending a Hello (or “keepalive”) packet to the remote client. The minimum wait time is 1 second. The maximum wait time is 3600 seconds. The default wait time is 60 seconds.

Apply / Cancel

To apply your L2TP settings and to include them in the active configuration, click **Apply**. The Manager returns to the Configuration | System | Tunneling Protocols screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Tunneling Protocols screen.

Configuration | System | Tunneling Protocols | IPSec

This section of the Manager lets you configure IPSec LAN-to-LAN connections, IKE (Internet Key Exchange) parameters for IPSec Security Associations and LAN-to-LAN connections, and NAT Transparency.

IPSec provides the most complete architecture for VPN tunnels, and it is perceived as the most secure protocol. Both LAN-to-LAN connections and client-to-LAN connections can use IPSec.

In IPSec terminology, a “peer” is a remote-access client or another secure gateway. During tunnel establishment under IPSec, the two peers negotiate Security Associations that govern authentication, encryption, encapsulation, key management, etc. These negotiations involve two phases: first, to establish the tunnel (the IKE SA); and second, to govern traffic within the tunnel (the IPSec SA).

In IPSec LAN-to-LAN connections, the VPN Concentrator can function as initiator or responder. In IPSec client-to-LAN connections, the VPN Concentrator functions only as responder. Initiators propose SAs; responders accept, reject, or make counter-proposals—all in accordance with configured SA parameters. To establish a connection, both entities must agree on the SAs.

The Cisco VPN Client complies with the IPSec protocol and is specifically designed to work with the VPN Concentrator. However, the VPN Concentrator can establish IPSec connections with many protocol-compliant clients. Likewise, the VPN Concentrator can establish LAN-to-LAN connections with other protocol-compliant VPN devices (often called “secure gateways”).

The Cisco VPN Client supports these IPSec attributes:

- Main mode for negotiating phase one ISAKMP Security Associations (SAs) when using digital certificates for authentication
- Aggressive mode for negotiating phase one ISAKMP Security Associations (SAs) when using preshared keys for authentication
- Authentication Algorithms:
 - ESP-MD5-HMAC-128
 - ESP-SHA1-HMAC-160
- Authentication Modes:
 - Preshared Keys
 - X.509 Digital Certificates
- Diffie-Hellman Groups 1, 2, and 5
- Encryption Algorithms:
 - AES-128, -192, and -256
 - DES-56
 - 3DES-168
 - ESP-NULL
- Extended Authentication (XAuth)
- Mode Configuration (also known as ISAKMP Configuration Method)
- Tunnel Encapsulation Mode
- IP compression (IPCOMP) using LZS

You configure IKE proposals (parameters for the IKE SA) here. You apply them to IPsec LAN-to-LAN connections in this section, and to IPsec SAs on the Configuration | Policy Management | Traffic Management | Security Associations screens. Therefore, you should configure IKE proposals before configuring other IPsec parameters. Cisco supplies default IKE proposals that you can use or modify.

Figure 7-4 Configuration | System | Tunneling Protocols | IPsec Screen

Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

General Parameters			
Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select the access hours assigned to this user.
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter the number of simultaneous logins for this user.
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) Enter the idle timeout for this user.
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this user.
Filter	-None-	<input checked="" type="checkbox"/>	Enter the filter assigned to this user.
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	<input checked="" type="checkbox"/>	Select the SEP cards this user can be assigned to.
Tunneling Protocols	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec	<input checked="" type="checkbox"/>	Select the tunneling protocols this user can connect with.

Add Cancel

67345

Configuration | System | Tunneling Protocols | IPSec | LAN-to-LAN

This section of the Manager lets you configure, add, modify, and delete IPSec LAN-to-LAN connections between two VPN Concentrators.

While the VPN Concentrator can establish LAN-to-LAN connections with other protocol-compliant VPN secure gateways, these instructions assume VPN Concentrators on both sides. And here, the “peer” is the other VPN Concentrator or secure gateway.

In a LAN-to-LAN connection, IPSec creates a tunnel between the public interfaces of two VPN Concentrators, which correspondingly route secure traffic to and from many hosts on their private LANs. There is no user configuration or authentication in a LAN-to-LAN connection; all hosts configured on the private networks can access hosts on the other side of the connection, at any time.

To fully configure a LAN-to-LAN connection, you must configure identical basic IPSec parameters on both VPN Concentrators, and configure mirror-image private network addresses or network lists.

The VPN Concentrator also provides a network autodiscovery feature that dynamically discovers and updates the private network addresses on each side of the LAN-to-LAN connection, so you do not have to explicitly configure them. This feature works only when both devices are VPN Concentrators and both VPN Concentrators have routing enabled on the private interface.

You must configure a public interface on the VPN Concentrator before you can configure an IPSec LAN-to-LAN connection. See the Configuration | Interfaces screens. You must also configure IKE proposals before configuring LAN-to-LAN connections. See the Configuration | System | Tunneling Protocols | IPSec | IKE Proposals screens.

You can configure only one LAN-to-LAN connection with each VPN Concentrator (or other secure gateway) peer.

Figure 7-5 Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN Screen

Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Attribute	Value	Description
Identity Parameters		
User Name	<input type="text"/>	Enter a unique user name.
Password	<input type="password"/>	Enter the user's password. The password must satisfy the group password requirements.
Verify	<input type="password"/>	Verify the user's password.
Group	<input type="text" value="-Base Group-"/>	Enter the group to which this user belongs.
IP Address	<input type="text"/>	Enter the IP address assigned to this user.
Subnet Mask	<input type="text"/>	Enter the subnet mask assigned to this user.

67346

LAN-to-LAN Connection

The LAN-to-LAN Connection list shows connections that have been configured. The connections are listed in the order you configure them, in the format *Name (Peer IP Address) on Interface*, for example: Branch 1 (192.168.34.56) on Ethernet 2 (Public). If no connections have been configured, the list shows --Empty--.

Add / Modify / Delete

To configure and add a new connection, click **Add**. See the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add screen. If you have not configured a public interface, the Manager displays the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | No Public Interfaces screen.

To modify the parameters of a configured connection, select the connection from the list and click **Modify**. See the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Modify screen.

To delete a configured connection, select the connection from the list and click **Delete**.



Note

There is no confirmation or undo.

The Manager deletes the connection, its LAN-to-LAN filter rules, SAs, and group. The Manager then refreshes the screen and shows the remaining connections in the list.



Caution

Deleting a connection immediately deletes any tunnels (and user sessions) using that connection.

Reminder:

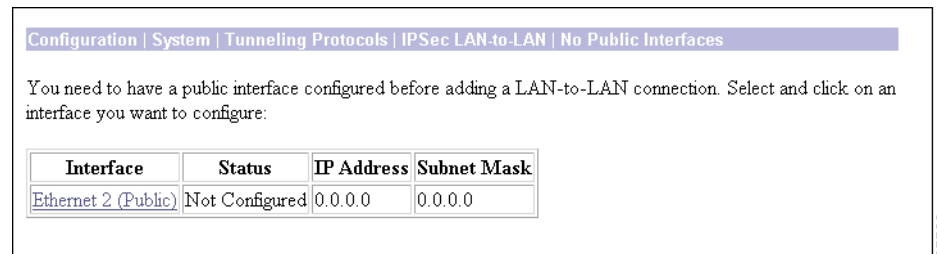
The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | Tunneling Protocols | IPSec | LAN-to-LAN | No Public Interfaces

The Manager displays this screen if you have not configured a public interface on the VPN Concentrator and you try to add an IPSec LAN-to-LAN connection. The public interface need not be enabled, but it must be configured with an IP address and the Public Interface parameter enabled.

You should designate only one VPN Concentrator interface as a public interface.

Figure 7-6 Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | No Public Interfaces Screen



Click the highlighted link to configure the desired public interface. The Manager opens the appropriate Configuration | Interfaces screen.

Configuration | System | Tunneling Protocols | IPSec | LAN-to-LAN | Add or Modify

These screens let you:

- Add: Configure and add a new IPSec LAN-to-LAN connection.
- Modify: Modify parameters of a configured IPSec LAN-to-LAN connection.

You must configure a public interface on the VPN Concentrator before you can configure an IPSec LAN-to-LAN connection. See the Configuration | Interfaces screens.

You can configure only one LAN-to-LAN connection with each VPN Concentrator (or other secure gateway) peer.

The maximum number of LAN-to-LAN connections supported is determined by the hardware and is model-dependent.

Table 7-1 Maximum LAN-to-LAN Connections for Each VPN Concentrator Model

VPN Concentrator Model	Maximum Number of Sessions
3005 & 3015	100
3030	500
3060 & 3080	1000

Figure 7-7 Configuration | System | Tunneling Protocols | IPsec LAN-to-LAN | Add or Modify Screen

Configuration | System | Tunneling Protocols | IPsec LAN-to-LAN | Add

Add a new IPsec LAN-to-LAN connection.

Name	<input type="text"/>	Enter the name for this LAN-to-LAN connection.
Interface	Ethernet 2 (Public) (0.0.0.0)	Select the interface for this LAN-to-LAN connection.
Peer	<input type="text"/>	Enter the IP address of the remote peer for this LAN-to-LAN connection.
Digital Certificate	None (Use Preshared Keys)	Select the digital certificate to use.
Certificate Transmission	<input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only	Choose how to send the digital certificate to the IKE peer.
Preshared Key	<input type="text"/>	Enter the preshared key for this LAN-to-LAN connection.
Authentication	ESP/MD5/HMAC-128	Specify the packet authentication mechanism to use.
Encryption	3DES-168	Specify the encryption mechanism to use.
IKE Proposal	IKE-3DES-MD5	Select the IKE Proposal to use for this LAN-to-LAN connection.
Filter	--None--	Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.
IPsec NAT-T	<input type="checkbox"/>	Check to let NAT-T compatible IPsec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPsec over NAT-T under NAT Transparency.
Bandwidth Policy	---None---	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
Reserved Bandwidth	0 bps	Enter the reserved bandwidth for this LAN-to-LAN connection.
Routing	None	Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.

Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.

Network List	Use IP Address/Wildcard-mask below	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address	<input type="text"/>	Note: Enter a <i>wildcard mask</i>, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask	<input type="text"/>	

Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.

Network List	Use IP Address/Wildcard-mask below	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address	<input type="text"/>	Note: Enter a <i>wildcard mask</i>, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask	<input type="text"/>	

78464

When you Add or Modify a connection on these screens, the VPN Concentrator automatically:

- Creates or modifies two filter rules with the Apply IPsec action: one inbound, one outbound, named L2L:<Name> In and L2L:<Name> Out.
- Creates or modifies an IPsec Security Association named L2L:<Name>.
- Applies these rules to the filter on the public interface and applies the SA to the rules. If the public interface does not have a filter, it applies the Public (default) filter with the preceding rules.
- Creates or modifies a group named with the Peer IP address. If the VPN Concentrator internal authentication server has not been configured, it does so, and adds the group to the database.

All of the rules, SAs, filters, and group have default parameters or those specified on this screen. You can modify the rules and SA on the Configuration | Policy Management | Traffic Management screens, the group on the Configuration | User Management | Groups screens, and the interface on the Configuration | Interfaces screens. However, we recommend that you keep the configured defaults. You cannot delete these rules, SAs, or group individually; the system automatically deletes them when you delete the LAN-to-LAN connection.

To fully configure a LAN-to-LAN connection, you must configure identical IPsec LAN-to-LAN parameters on both VPN Concentrators, and configure mirror-image local and remote private network addresses. For example:

Configure	On this VPN Concentrator	On Peer VPN Concentrator
Local Network	10.10.0.0/0.0.255.255	11.0.0.0/0.255.255.255
Remote Network	11.0.0.0/0.255.255.255	10.10.0.0/0.0.255.255

If you use network lists, you must also configure and apply them as mirror images on the two VPN Concentrators. If you use network autodiscovery, you must use it on both VPN Concentrators.



Caution

On the **Modify** screen, any changes take effect as soon as you click **Apply**. If client sessions are using this connection, changes delete the tunnel (and the sessions) without warning.

Name

Enter a unique descriptive name for this connection. The maximum name length is 32 characters. Since the created rules and SA use this name, we recommend that you keep it short.

Interface

Add screen:

- Click the **Interface** drop-down menu button and select the configured public interface on this VPN Concentrator for this end of the LAN-to-LAN connection. The list shows all interfaces that have the Public Interface parameter enabled. See Configuration | Interfaces.

Modify screen:

- The screen shows the configured public interface on this VPN Concentrator for this end of the LAN-to-LAN connection. You cannot change the interface. To move the connection to another interface, you must delete this connection and add a new one for the other interface.

Peer

Enter the IP address of the remote peer in the LAN-to-LAN connection. This must be the IP address of the public interface on the peer VPN Concentrator. Use dotted decimal notation, for example: 192.168.34.56.

Digital Certificate

This parameter specifies whether to use preshared keys or a PKI (Public Key Infrastructure) digital identity certificate to authenticate the peer during Phase 1 IKE negotiations. See the discussion under Administration | Certificate Management.

Click the **Digital Certificate** drop-down menu button and choose the option. The list shows any digital certificates that have been installed, plus:

- None (Use Preshared Keys) = Use only preshared keys to authenticate the peer during Phase 1 IKE negotiations. This is the default choice.

Certificate Transmission

If you configured authentication using digital certificates, choose the type of certificate transmission.

- Entire certificate chain = Send the peer the identity certificate and all issuing certificates. Issuing certificates include the root certificate and any subordinate CA certificates.
- Identity certificate only = Send the peer only the identity certificate.

Preshared Key

Enter a preshared key for this connection. Use a minimum of 4, a maximum of 32, alphanumeric characters, for example: sZ9s14ep7. The system displays your entry in clear text.

This key becomes the password for the IPSec LAN-to-LAN group that is created, and you must enter the same key on the peer VPN Concentrator. (This is *not* a manual encryption or authentication key. The system automatically generates those session keys.)

Authentication

This parameter specifies the data, or packet, authentication algorithm. Packet authentication proves that data comes from whom you think it comes from; it is often referred to as “data integrity” in VPN literature. The IPSec ESP (Encapsulating Security Payload) protocol provides both encryption and authentication.

Click the **Authentication** drop-down menu button and choose the algorithm:

- None = No data authentication.
- ESP/MD5/HMAC-128 = ESP protocol using HMAC (Hashed Message Authentication Coding) with the MD5 hash function using a 128-bit key. This is the default choice.
- ESP/SHA/HMAC-160 = ESP protocol using HMAC with the SHA-1 hash function using a 160-bit key. This choice is more secure but requires more processing overhead.

Encryption

This parameter specifies the data, or packet, encryption algorithm. Data encryption makes the data unreadable if intercepted.

Click the **Encryption** drop-down menu button and choose the algorithm:

- Null = Use ESP without encryption; no packet encryption.
- DES-56 = Use DES encryption with a 56-bit key.
- 3DES-168 = Use Triple-DES encryption with a 168-bit key. This is the default.
- AES-128 = Advanced Encryption Standard (AES) encryption with a 128-bit key. AES provides greater security than DES and is computationally more efficient than triple DES.
- AES-192 = AES encryption with a 192-bit key.
- AES-256 = AES encryption with a 256-bit key.

IKE Proposal

This parameter specifies the set of attributes for Phase 1 IPsec negotiations, which are known as IKE proposals. See the Configuration | System | Tunneling Protocols | IPsec | IKE Proposals screen. You must configure, activate, and prioritize IKE proposals before configuring LAN-to-LAN connections.

Click the **IKE Proposal** drop-down menu button and choose the IKE proposal. The list shows only active IKE proposals in priority order. Cisco-supplied default active proposals are:

- CiscoVPNClient-3DES-MD5 = Use preshared keys (XAUTH) and MD5/HMAC-128 for authentication. Use 3DES-168 encryption. Use D-H Group 2 to generate SA keys. This choice allows XAUTH user-based authentication and is the default.
- IKE-3DES-MD5 = Use preshared keys and MD5/HMAC-128 for authentication. Use 3DES-168 encryption. Use D-H Group 2 to generate SA keys.
- IKE-3DES-MD5-DH1 = Use preshared keys and MD5/HMAC-128 for authentication. Use 3DES-168 encryption. Use D-H Group 1 to generate SA keys. This choice is compatible with the Cisco VPN 3000 Client.
- IKE-DES-MD5 = Use preshared keys and MD5/HMAC-128 for authentication. Use DES-56 encryption. Use D-H Group 1 to generate SA keys. This choice is compatible with the Cisco VPN 3000 Client.
- IKE-3DES-MD5-DH7 = Use preshared keys and MD5/HMAC-128 for authentication. Use 3DES-168 encryption. Use D-H Group 7 (ECC) to generate SA keys. This IKE proposal is intended for use with the movianVPN client; it can also be used with any peer that supports ECC groups for D-H.
- IKE-3DES-MD5-RSA = Use RSA digital certificate and MD5/HMAC-128 for authentication. Use 3DES-168 encryption. Use D-H Group 2 to generate SA keys.
- IKE-AES128-SHA = Use Preshared keys and SHA/HMAC-160 for authentication. Use AES-128 for encryption. Use D-H Group 2 or Group 5 to generate SA keys.

Filter

Filters consist of rules that determine whether to allow or reject tunneled data packets coming through the VPN Concentrator, based on criteria such as source address, destination address, and protocol. Cisco supplies three default filters, which you can modify. To configure filters and rules, see the Configuration | Policy Management | Traffic Management screens.

Click the **Filter** drop-down menu button and select the filter:

- --None-- = No filter applied, which means there are no restrictions on tunneled data traffic. This is the default selection.
- Private (Default) = Allow all packets except source-routed IP packets. (This is the default filter for the private Ethernet interface.)
- Public (Default) = Allow inbound and outbound tunneling protocols plus ICMP and VRRP. Allow fragmented IP packets. Drop everything else, including source-routed packets. (This is the default filter for the public Ethernet interface.)
- External (Default) = No rules applied to this filter. Drop all packets. (This is the default filter for the external Ethernet interface.)

Additional filters that you have configured also appear on the list.

IPSec NAT-T

NAT-T (NAT Traversal) lets IPSec peers establish a LAN-to-LAN connection through a NAT device. It does this by encapsulating IPSec traffic in UDP datagrams, using port 4500, thereby providing NAT devices with port information. NAT-T auto-detects any NAT devices, and only encapsulates IPSec traffic when necessary.

The VPN Concentrator implementation of NAT-T supports IPSec peers behind a single NAT/PAT device as follows:

- One Microsoft L2TP/IPSec client (can support other remote access clients and one L2TP/IPSec client).
- One LAN-to-LAN connection.
- Either a LAN-to-LAN connection or multiple remote access clients, but not a mixture of both.

To use NAT-T you must:

- Open port 4500 on any firewall you have configured in front of a VPN Concentrator.
- Reconfigure previous IPSec/UDP settings using port 4500 to a different port.
- Enable IPSec over NAT-T globally in the Configuration | System | Tunneling Protocols | IPSec | NAT Transparency screen.
- Select the second or third option for the Fragmentation Policy parameter in the Configuration | Interfaces | Ethernet screen. These options let traffic travel across NAT devices that do not support IP fragmentation; they do not impede the operation of NAT devices that do support IP fragmentation.

Check the box to enable NAT-T for this LAN-to-LAN connection.

Bandwidth Policy

Select a bandwidth policy to apply to this IPSec LAN-to-LAN connection from the drop-down list. If there are no policies in this list, you must go to Configuration | Policy Management | Traffic Management | Bandwidth Policies and define one or more policies. If you do not want to select a policy here, then select **None**. For more information on the Bandwidth Management feature, see the Configuration | Policy Management | Traffic Management | Bandwidth Policies | Add or Modify screen.

Routing

The VPN Concentrator provides two ways to advertise static LAN-to-LAN routes.

- Reverse Route Injection = The local VPN Concentrator adds the addresses of one or more remote networks to its routing table and advertises these entries to specified networks on the local LAN. If you choose this option, specify the Local and Remote Network parameters that follow. Then, enable RIP or OSPF on the private interface.
- Network Autodiscovery = This feature dynamically discovers and continuously updates the private network addresses on each side of the LAN-to-LAN connection. This feature uses RIP. You must enable Inbound RIP IPv2/v1 on the Ethernet 1 (Private) interface of both VPN Concentrators. (See the “[Configuration | Interfaces](#)” section.) If you choose this option, skip the Local and Remote Network parameters; they are ignored.
- None = Do not advertise static LAN-to-LAN routes.

Local Network

These entries identify the private network on this VPN Concentrator, the hosts of which can use the LAN-to-LAN connection.

- These entries must match those in the Remote Network section on the peer VPN Concentrator.
- If you are using a LAN-to-LAN NAT rule, this is the translated network address.

Network List

Click the **Network List** drop-down menu button and choose the configured network list that specifies the local network addresses. A network list is a list of network addresses that are treated as a single object. See the Configuration | Policy Management | Traffic Management | Network Lists screens. Otherwise, you can choose:

- Use IP Address/Wildcard-mask below, which lets you enter a network address.
- Create new Network List (on Add screen only), which lets you create a network list of local network addresses. The Manager automatically opens the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Local Network List screen when you click Add; see description below.

If you choose a configured network list, the Manager ignores entries in the IP Address and Wildcard Mask fields.

**Note**

An IP address is used with a wildcard mask to provide the desired granularity. A wildcard mask is the reverse of a subnet mask. In other words, the wildcard mask has ones in bit positions to ignore, zeros in bit positions to match. For example:

0.0.0.0/255.255.255.255 = any address

10.10.1.35/0.0.0.0 = only 10.10.1.35

10.10.1.35/0.0.0.255 = all 10.10.1.nnn addresses

IP Address

Enter the IP address of the private local network on this VPN Concentrator. Use dotted decimal notation, for example: 10.10.0.0.

Wildcard Mask

Enter the wildcard mask for the private local network. Use dotted decimal notation, for example: 0.0.255.255. The system supplies a default wildcard mask appropriate to the IP address class.

Remote Network

These entries identify the private network on the remote peer VPN Concentrator whose hosts can use the LAN-to-LAN connection.

- These entries must match those in the Local Network section on the peer VPN Concentrator.
- If you are using a LAN-to-LAN NAT rule, this is the remote network address.

Network List

Click the **Network List** drop-down menu button and choose the configured network list that specifies the remote network addresses. A network list is a list of network addresses that are treated as a single object. See the Configuration | Policy Management | Traffic Management | Network Lists screens. Otherwise, you can choose:

- Use IP Address/Wildcard-mask, which lets you enter a network address.
- Create new Network List (on Add screen only), which lets you create a network list of remote network addresses. The Manager automatically opens the Configuration | System | Tunneling Protocols | IPsec LAN-to-LAN | Add | Remote Network List screen when you click Add; see description below.

If you choose a configured network list, the Manager ignores entries in the IP Address and Wildcard-mask fields.

See the preceding *wildcard mask* note.

IP Address

Enter the IP address of the private network on the remote peer VPN Concentrator. Use dotted decimal notation, for example: 11.0.0.1.

Wildcard Mask

Enter the wildcard mask for the private remote network. Use dotted decimal notation, for example: 0.255.255.255. The system supplies a default wildcard mask appropriate to the IP address class.

Add or Apply / Cancel

- **Add screen:** To add this connection to the list of configured LAN-to-LAN connections, click **Add**. If you are creating new network lists, the Manager automatically displays the appropriate Local or Remote Network List screens. Otherwise, the Manager displays the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done screen.
- **Modify screen:** To apply your changes to this LAN-to-LAN connection, click **Apply**. The Manager returns to the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN screen.



Caution

Any changes take effect as soon as you click Apply. If client sessions are using this connection, changes delete the tunnel (and the sessions) without warning.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN screen, and the LAN-to-LAN Connection list is unchanged.

Configuration | System | Tunneling Protocols | IPSec | LAN-to-LAN | Add | Local or Remote Network List

These screens let you configure and add network lists for the Local Network or Remote Network of a new IPSec LAN-to-LAN connection. The Manager automatically opens these screens if you choose Create new Network List under Network List on the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add screen.

A network list is a list of network addresses that are treated as a single object. See the Configuration | Policy Management | Traffic Management | Network Lists screens also.

On the Local Network List screen, the Manager can automatically generate a network list using the valid network routes in the routing table for the Ethernet 1 (Private) interface of this VPN Concentrator. (See Monitoring | Routing Table.)

A single network list can contain a maximum of 10 network entries.

Figure 7-8 Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Local or Remote Network List Screen

Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Local Network List

Configure and add a new Network List for the Local end of an IPSec LAN-to-LAN connection. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name

Network List

Name of the Network List you are adding. The name must be unique.

- Enter the Networks and Wildcard masks using the following format: **n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

67334

List Name

The Manager supplies a default name that identifies the list as a LAN-to-LAN local or remote list, which we recommend you keep. Otherwise, enter a unique name for this network list. The maximum name length is 48 characters. Entries are case-sensitive. Spaces are allowed.

If you use the Generate Local List feature on the Local Network List screen, edit this name *after* the system generates the network list.

Network List

Enter the networks in this network list. Enter each network on a single line using the format *n.n.n.n/w.w.w.w*, where *n.n.n.n* is the network IP address and *w.w.w.w* is the wildcard mask.

**Note**

Enter a *wildcard mask*, which is the reverse of a subnet mask. A wildcard mask has ones in bit positions to ignore, zeros in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.

If you omit the wildcard mask, the Manager supplies the default wildcard mask for the class of the network address. For example, 192.168.12.0 is a Class C address, and default wildcard mask is 0.0.0.255.

You can enter a maximum of 200 networks in a single network list.

Generate Local List

On the Local Network List screen, click the **Generate Local List** button to have the Manager automatically generate a network list using the first 200 valid network routes in the routing table for the Ethernet 1 (Private) interface of this VPN Concentrator. (See Monitoring | Routing Table.) The Manager refreshes the screen after it generates the list, and you can then edit the Network List and the List Name.

Add

To add this network list to the configured network lists, click **Add**. The Manager displays either the Remote Network List screen or the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done screen.

Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done

The Manager displays this screen when you have finished configuring all parameters for a new IPSec LAN-to-LAN connection. It documents the added configuration entities.

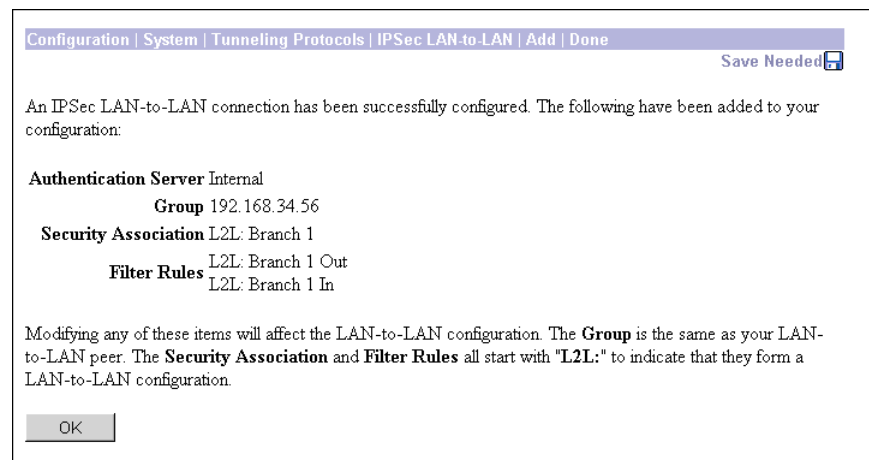
The Manager displays this screen only once. We suggest you print a copy of the screen to save it for your records.

To examine or modify an entity, see the appropriate screen:

- **Group:** See Configuration | User Management | Groups.
- **Security Association:** See Configuration | Policy Management | Traffic Management | Security Associations.
- **Filter Rules:** See Configuration | Policy Management | Traffic Management | Rules.

You cannot delete the group, SA, or rules individually, nor can you remove the rules from their filter. The system automatically deletes them when you delete the LAN-to-LAN connection.

Figure 7-9 Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done Screen



OK

To close this screen and return to the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN screen, click **OK**. The LAN-to-LAN Connection list shows the new connection, and the Manager includes all the new settings in the active configuration.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | Tunneling Protocols | IPSec | IKE Proposals

This section of the Manager lets you configure, add, modify, activate, deactivate, delete, and prioritize IKE proposals, which are sets of parameters for Phase 1 IPSec negotiations. During Phase 1, the two peers establish a secure tunnel within which they then negotiate the Phase 2 parameters.

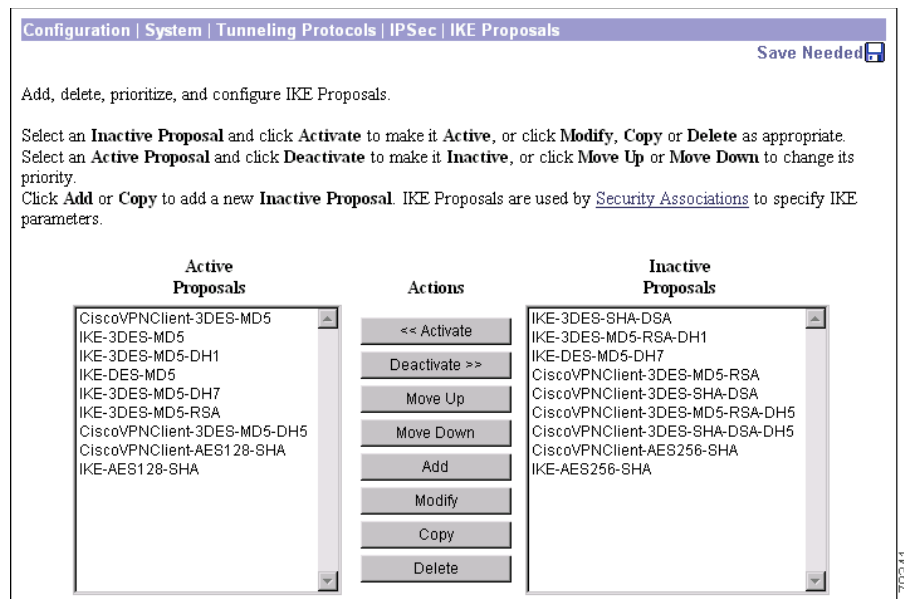
The VPN Concentrator uses IKE proposals both as initiator and responder in IPSec negotiations. In LAN-to-LAN connections, the VPN Concentrator can function as initiator or responder. In client-to-LAN connections, the VPN Concentrator functions only as responder.

You must configure, activate, and prioritize IKE proposals before you configure IPSec Security Associations. See Configuration | Policy Management | Traffic Management | Security Associations, or click the **Security Associations** link on this screen.

You must also configure and activate IKE proposals before configuring IPSec LAN-to-LAN connections. See Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN.

You can configure a maximum of 150 IKE proposals total (active and inactive).

Figure 7-10 Configuration | System | Tunneling Protocols | IPSec | IKE Proposals Screen



Cisco supplies default IKE proposals that you can use or modify; see [Table 7-2](#). The documentation for the Cisco VPN Client and for the VPN 3002 Hardware Client each include a table of all valid IKE proposals for remote access connections. See Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add for explanations of the parameters.

Table 7-2 Cisco-Supplied Default IKE Proposals: Proposals Active by Default

Proposal Name	Authentication Mode	Authentication Algorithm	Encryption Algorithm	Diffie-Hellman Group	Lifetime Measurements	Data Lifetime	Time Lifetime
CiscoVPNClient-3DES-MD5	Preshared Keys (XAUTH)	MD5/HMAC-128	3DES-168	Group 2 (1024-bits)	Time	10000 KB	86400 sec
IKE-3DES-MD5	Preshared Keys	MD5/HMAC-128	3DES-168	Group 2 (1024-bits)	Time	10000 KB	86400 sec
IKE-3DES-MD5-DH1	Preshared Keys	MD5/HMAC-128	3DES-168	Group 1 (768-bits)	Time	10000 KB	86400 sec
IKE-DES-MD5	Preshared Keys	MD5/HMAC-128	DES-56	Group 1 (768-bits)	Time	10000 KB	86400 sec
IKE-3DES-MD5-DH7	Preshared Keys	MD5/HMAC-128	3DES-168	Group 7 (ECC) (163-bits)	Time	10000 KB	86400 sec
IKE-3DES-MD5-RSA	RSA Digital Certificate	MD5/HMAC-128	3DES-168	Group 2 (1024-bits)	Time	10000 KB	86400 sec
IKE-AES128-SHA	Preshared Keys	SHA/HMAC-160	AES-128	Group 2 (1024-bits)	Time	10000 KB	86400 sec
CiscoVPNClient-AES128-SHA	Preshared Keys	SHA/HMAC-160	AES-128	Group 2 (1024-bits)	Time	10000 KB	86400 sec
CiscoVPNClient-3DES-MD5-DH5		MD5/HMAC-128	3DES-168	Group 5 (1536-bits)	Time	10000 KB	86400 sec

Table 7-3 Cisco-Supplied Default IKE Proposals: Proposals Inactive by Default

Proposal Name	Authen. Mode	Authen. Algorithm	Encryption Algorithm	Diffie-Hellman Group	Lifetime Measurements	Data Lifetime	Time Lifetime
IKE-3DES-SHA-DSA	RSA Digital Certificate	SHA/HMAC-160	3DES-168	Group 2 (1024-bits)	Time	10000 KB	86400 sec
IKE-3DES-MD5-RSA-DH1	RSA Digital Certificate	MD5/HMAC-128	3DES-168	Group 1 (768-bits)	Time	10000 KB	86400 sec
IKE-DES-MD5-DH7	Preshared Keys	MD5/HMAC-128	DES-56	Group 7 (ECC) (163-bits)	Time	10000 KB	86400 sec
CiscoVPNClient-3DES-MD5-RSA	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	3DES-168	Group 2 (1024-bits)	Time	10000 KB	86400 sec
CiscoVPNClient-3DES-SHA-DSA	DSA Digital Certificate (XAUTH)	SHA/HMAC-160	3DES-168	Group 2 (1024-bits)	Time	10000 KB	86400 sec
CiscoVPNClient-AES256-SHA	Preshared Keys	SHA/HMAC-160	AES-256	Group 2 (1024-bits)	Time	10000 KB	86400 sec
IKE-AES256-SHA	Preshared Keys	SHA/HMAC-160	AES-256	Group 2 (1024-bits)	Time	10000 KB	86400 sec

Active Proposals

The field shows the names of IKE proposals that have been configured, activated, and prioritized. As an IPsec responder, the VPN Concentrator checks these proposals in priority order, to see if it can find one that agrees with parameters in the initiator's proposed SA.

Activating a proposal also makes it available for use wherever the Manager displays an IKE Proposal list, and the first active proposal appears as the default selection.

Inactive Proposals

The field shows the names of IKE proposals that have been configured but are inactive. New proposals appear in this list when you first configure and add them. The VPN Concentrator does not use these proposals in any IPsec negotiations, nor do they appear in IKE Proposal lists.



Note

To configure L2TP over IPsec, you must activate IKE-3DES-MD5-RSA. Also see the Configuration | User Management screens.

<< Activate

To activate an inactive IKE proposal, select it from the Inactive Proposals list and click the <<Activate button. The Manager moves the proposal to the Active Proposals list and refreshes the screen.

>> Deactivate

To deactivate an active IKE proposal, select it from the Active Proposals list and click the >>**Deactivate** button. If the active proposal is configured on a Security Association, the Manager displays an error message; and you must remove it from the SA before you can deactivate it. Otherwise, the Manager moves the proposal to the Inactive Proposals list and refreshes the screen.

Move Up / Move Down

To change the priority order of an active IKE proposal, select it from the Active Proposals list and click **Move Up** or **Move Down**. The Manager refreshes the screen and shows the reordered Active Proposals list. These actions move the proposal up or down one position.

Add

To configure and add a new IKE proposal to the list of Inactive Proposals, click the **Add** button. See Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add.

Modify

To modify a configured IKE proposal, select it from either Active Proposals or Inactive Proposals and click the **Modify** button. See Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Modify. Modifying an active proposal does not affect connections currently using it, but changes do affect subsequent connections.

Copy

To use a configured IKE proposal as the basis for configuring and adding a new one, select it from either Active Proposals or Inactive Proposals and click the **Copy** button. See Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Copy. The new proposal appears in the Inactive Proposals list.

Delete

To delete a configured IKE proposal, select it from either Active Proposals or Inactive Proposals and click the **Delete** button. If an active proposal is configured on a Security Association, the Manager displays an error message; and you must remove it from the SA before you can delete it. *Otherwise, there is no confirmation or undo.* The Manager refreshes the screen and shows the remaining IKE proposals in the list.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | Tunneling Protocols | IPsec | IKE Proposals | Add, Modify, or Copy

These screens let you:

- Add: Configure and add a new inactive IKE proposal.
- Modify: Modify a previously configured IKE proposal.
- Copy: Copy a configured IKE proposal, modify its parameters, save it with a new name, and add it to the configured inactive IKE proposals.

You can configure a maximum of 150 IKE proposals total (active and inactive), and you can make any number of them active.

Figure 7-11 Configuration | System | Tunneling Protocols | IPsec | IKE Proposals | Add, Modify, or Copy Screen

Configuration | System | Tunneling Protocols | IPsec | IKE Proposals | Add

Configure and add a new IKE Proposal

Proposal Name	<input type="text"/>	Specify the name of this IKE Proposal
Authentication Mode	<input type="text" value="Preshared Keys"/>	Select the authentication mode to use.
Authentication Algorithm	<input type="text" value="MD5/HMAC-128"/>	Select the packet authentication algorithm to use.
Encryption Algorithm	<input type="text" value="3DES-168"/>	Select the encryption algorithm to use.
Diffie-Hellman Group	<input type="text" value="Group 2 (1024-bits)"/>	Select the Diffie Hellman Group to use.
Lifetime Measurement	<input type="text" value="Time"/>	Select the lifetime measurement of the IKE keys.
Data Lifetime	<input type="text" value="10000"/>	Specify the data lifetime in kilobytes (KB).
Time Lifetime	<input type="text" value="86400"/>	Specify the time lifetime in seconds.

Add Cancel

67031

Proposal Name

Enter a unique name for this IKE proposal. The maximum name length is 48 characters. Entries are case-sensitive. Spaces are allowed.

Authentication Mode

This parameter specifies how to authenticate the remote client or peer. Authentication proves that the connecting entity is the one you think it is. If you select one of the digital certificate modes, an appropriate digital certificate must be installed on this VPN Concentrator and the remote client or peer. See the discussion under Administration | Certificate Management.

Click the **Authentication Mode** drop-down menu button and choose the method:

- Preshared Keys = Use preshared keys (the default). The keys are derived from the password of the user's or peer's group.
- RSA Digital Certificate = Use a digital certificate with keys generated by the RSA algorithm.
- DSA Digital Certificate = Use a digital certificate with keys generated by the DSA algorithm.
- Preshared Keys (XAUTH) = Use preshared keys (the default). The keys are derived from the password of the user's or peer's group. Require user-based authentication via XAUTH.
- RSA Digital Certificate (XAUTH) = Use a digital certificate with keys generated by the RSA algorithm. Require user-based authentication via XAUTH.
- DSA Digital Certificate (XAUTH) = Use a digital certificate with keys generated by the DSA algorithm. Require user-based authentication via XAUTH.

Authentication Algorithm

This parameter specifies the data, or packet, authentication algorithm. Packet authentication proves that data comes from the source you think it comes from.

Click the **Authentication Algorithm** drop-down menu button and choose one of the following algorithms:

- MD5/HMAC-128 = HMAC (Hashed Message Authentication Coding) with the MD5 hash function using a 128-bit key. This is the default choice.
- SHA/HMAC-160 = HMAC with the SHA-1 hash function using a 160-bit key. This choice is more secure but requires more processing overhead.

Encryption Algorithm

This parameter specifies the data, or packet, encryption algorithm. Data encryption makes the data unreadable if intercepted.

Click the **Encryption Algorithm** drop-down menu button and choose the algorithm:

- DES-56 = Data Encryption Standard (DES) encryption with a 56-bit key.
- 3DES-168 = Triple-DES encryption with a 168-bit key. This is the default.
- AES-128 = Advanced Encryption Standard (AES) encryption with a 128-bit key. AES provides greater security than DES and is computationally more efficient than triple DES.
- AES-192 = AES encryption with a 192-bit key.
- AES-256 = AES encryption with a 256-bit key.

When you select an encryption algorithm, the Manager selects and displays the default Diffie-Hellman group for that encryption algorithm. You can

Diffie-Hellman Group

This parameter specifies the Diffie-Hellman group used to generate IPsec SA keys. The Diffie-Hellman technique generates keys using prime numbers and “generator” numbers in a mathematical relationship. When you choose an encryption algorithm, the Manager automatically selects the default Diffie-Hellman group for that algorithm; you can change the group here if you want, subject to the constraints noted below.



Note

For the VPN 3002 Hardware Client: In order to use Groups 1 or 5, you must be using digital certificates. Otherwise, only Group 2 is available. To use Groups 1, or 5, make sure there is a digital certificate installed on the VPN 3002; and on the VPN Concentrator, choose one of the digital certificate authentication options under Authentication Mode.

Click the **Diffie-Hellman Group** drop-down menu button and choose the group:

- Group 1 (768-bits) = Use Diffie-Hellman Group 1 to generate IPsec SA keys, where the prime and generator numbers are 768 bits. Choose this option if you select DES-56 under Encryption Algorithm.
- Group 2 (1024-bits) = Use Diffie-Hellman Group 2 to generate IPsec SA keys, where the prime and generator numbers are 1024 bits. This is the default choice for use with the 3DES-168 Encryption Algorithm.
- Group 5 (1536-bits) = Use Diffie-Hellman Group 5 to generate IPsec SA keys, where the prime and generator numbers are 1536 bits. This is the default choice for use with the AES encryption algorithms. It works only for LAN-to-LAN connections, and for clients using certificates.
- Group 7 (ECC) = Use Diffie-Hellman Group 7 to generate IPsec SA keys, where the elliptical curve field size is 163 bits. You can use this option with any encryption algorithm. This option is intended for use with the movianVPN client, but you can use it with any peers that support Group 7 (ECC).

Lifetime Measurement

This parameter specifies how to measure the lifetime of the IKE SA keys, which is how long the IKE SA lasts until it expires and must be renegotiated with new keys. It is used with the Data Lifetime or Time Lifetime parameters.



Note

If the peer proposes a shorter lifetime measurement, the VPN Concentrator uses that lifetime measurement instead.

Click the **Lifetime Measurement** drop-down menu button and choose the measurement method:

- Time = Use time (seconds) to measure the lifetime of the SA (the default). Configure the Time Lifetime parameter below.
- Data = Use data (number of kilobytes) to measure the lifetime of the SA. Configure the Data Lifetime parameter below.
- Both = Use both time and data, whichever occurs first, to measure the lifetime. Configure both Time Lifetime and Data Lifetime parameters.
- None = No lifetime measurement. The SA lasts until terminated for other reasons. It lasts a maximum of 86400 seconds (24 hours).

Data Lifetime

If you choose Data or Both under Lifetime Measurement, enter the number of kilobytes of payload data after which the IKE SA expires. The minimum number is 10 KB. The default number is 10000 KB. The maximum number is 2147483647 KB.

Time Lifetime

If you choose Time or Both under Lifetime Measurement, enter the number of seconds after which the IKE SA expires. The minimum number is 60 seconds. The default number is 86400 seconds (24 hours). The maximum number is 2147483647 seconds (about 68 years).

Add or Apply / Cancel

Add or Copy screen:

- To add this IKE proposal to the list of Inactive Proposals, click **Add** or **Apply**. The Manager returns to the Configuration | System | Tunneling Protocols | IPSec | IKE Proposals screen. To use the new proposal, you must activate and prioritize it as explained for that screen.

Modify screen:

- To apply your changes to this IKE proposal, click **Apply**. The Manager returns to the Configuration | System | Tunneling Protocols | IPSec | IKE Proposals screen. If you modify an active proposal, changes do not affect connections currently using it, but they do affect subsequent connections.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Tunneling Protocols | IPSec | IKE Proposals screen, and the IKE proposals lists are unchanged.

Configuration | System | Tunneling Protocols | IPSec | NAT Transparency

This screen lets you configure NAT Transparency, which consists of IPSec over TCP and IPSec over NAT Traversal (NAT-T).

Figure 7-12 Configuration | System | Tunneling Protocols | IPSec | NAT Transparency Screen

Configuration | System | Tunneling Protocols | IPSec | NAT Transparency Save Needed

This section lets you configure system-wide IPSec NAT Transparency.

IPSec over TCP Check to enable IPSec over TCP.

TCP Port(s) Enter up to 10 comma-separated TCP ports (1 - 65535).

IPSec over NAT-T Check to enable IPSec over NAT-T, which detects the need for UDP encapsulation in NAT/PAT environments, using UDP port 4500.

79366

IPSec over TCP

IPSec over TCP enables a VPN client to operate in an environment in which standard Encapsulating Security Protocol (ESP, Protocol 50) or Internet Key Exchange (IKE, UDP 500) cannot function, or can function only with modification to existing firewall rules. IPSec over TCP encapsulates both the IKE and IPSec protocols within a TCP packet, and enables secure tunneling through both NAT and PAT devices and firewalls.



Note

This feature does not work with proxy-based firewalls.

IPSec over TCP works with both the VPN software client and the VPN 3002 hardware client. It works only on the public interface. It is a client to Concentrator feature only. It does not work for LAN-to-LAN connections.

- The VPN Concentrator can simultaneously support standard IPSec, IPSec over TCP, NAT-Traversal, and IPSec over UDP, depending on the client with which it is exchanging data.
- The VPN 3002 hardware client, which supports one tunnel at a time, can connect using standard IPSec, IPSec over TCP, NAT-Traversal, or IPSec over UDP.
- When enabled, IPSec over TCP takes precedence over all other methods.
- When both NAT-T and IPSec over UDP are enabled, NAT-T takes precedence.

To use IPSec over TCP, both the VPN Concentrator and the client must:

- Be running version 3.5 or later software.
- Enable IPSec over TCP.
- Configure the same port for IPSec over TCP on both the Concentrator and the client.

You enable IPSec over TCP on both the Concentrator and the client to which it connects. For software clients, refer to the *VPN Client User Guide* for configuration instructions. For the VPN 3002 hardware client, refer to the *VPN 3002 Hardware Client Getting Started* guide, and to the *VPN 3002 Hardware Client Reference*.

If you enter a well-known port, for example port 80 (HTTP) or port 443 (HTTPS), the system displays a warning that the protocol associated with that port will no longer work on the public interface. The consequence is that you can no longer use a browser to manage the VPN Concentrator through the public interface. To solve this problem, reconfigure the HTTP/HTTPS management to different ports.

You must configure TCP port(s) on the client as well as on the VPN Concentrator. The client configuration must include at least one of the ports you set for the VPN Concentrator here.

Check the box to enable IPSec over TCP.

TCP Port(s)

Enter up to 10 ports, using a comma to separate the ports. You do not need to use spaces. The default port is 10,000. The range is 1 to 65,635.

IPSec over NAT-T

NAT-T (NAT Traversal) lets IPSec peers establish a connection through a NAT device. It does this by encapsulating IPSec traffic in UDP datagrams, using port 4500, thereby providing NAT devices with port information. NAT-T auto-detects any NAT devices, and only encapsulates IPSec traffic when necessary.

Both the VPN Client and the VPN 3002 hardware client support NAT-T in software version 3.6 and later.

- To enable NAT-T on the VPN Client, see the *VPN Client Administrator Guide*.
- The VPN 3002 uses NAT-T by default, and requires no configuration.

Remote access clients that support both NAT-T and IPSec/UDP methods first attempt NAT-T, and then IPSec/UDP (if enabled) if a NAT device is not auto-detected, allowing IPSec traffic to pass through firewalls that disallow IPSec.

The VPN Concentrator implementation of NAT-T supports IPSec peers behind a single NAT/PAT device as follows:

- One Microsoft L2TP/IPSec client.
- One LAN-to-LAN connection.
- Either a LAN-to-LAN connection or multiple remote access clients, but not a mixture of both.

To use NAT-T you must:

- Open port 4500 on any firewall you have configured in front of a VPN Concentrator.
- Reconfigure previous IPSec/UDP configurations using port 4500 to a different port.
- Select the second or third options for the Fragmentation Policy parameter in the Configuration | Interfaces | Ethernet screen. These options let traffic travel across NAT devices that do not support IP fragmentation; they do not impede the operation of NAT devices that do support IP fragmentation.
- Check the box in this screen to Enable IPSec over NAT-T.

Check the box to enable IPSec over NAT Traversal.



IP Routing

In a typical installation, the VPN Concentrator is connected to the public network through an external router, which routes data traffic between networks, and it might also be connected to the private network through a router.

The VPN Concentrator itself includes an IP routing subsystem with static routing, RIP (Routing Information Protocol), and OSPF (Open Shortest Path First) functions. RIP and OSPF are routing protocols that routers use for messages to other routers within an internal or private network, to determine network connectivity, status, and optimum paths for sending data traffic.

After the IP routing subsystem establishes the data paths, the routing itself occurs at wire speed. The subsystem looks at the destination IP address in all packets coming through the VPN Concentrator, even tunneled ones, to determine where to send them. If the packets are encrypted, it sends them to the appropriate tunneling protocol subsystem (PPTP, L2TP, IPsec) for processing and subsequent routing. If the packets are not encrypted, it routes them in accordance with the configured IP routing parameters.

To route packets, the subsystem uses learned routes first (learned from RIP and OSPF), then static routes, then uses the default gateway. If you do not configure the default gateway, the subsystem drops packets that it cannot otherwise route. The VPN Concentrator also provides a tunnel default gateway, which is a separate default gateway for tunneled traffic only.

You configure static routes, the default gateways, and system-wide OSPF parameters in this section. This section also includes the system-wide DHCP (Dynamic Host Configuration Protocol) parameters. You configure RIP and interface-specific OSPF parameters on the network interfaces; see Configuration | Interfaces.

This section of the Manager also lets you configure VPN Concentrator redundancy using VRRP (Virtual Router Redundancy Protocol). This feature applies to installations of two or more VPN Concentrators in a parallel, redundant configuration. It provides automatic switchover to a backup system in case the primary system is out of service, thus ensuring user access to the VPN. This feature supports user access via IPsec LAN-to-LAN connections, IPsec client (single-user remote-access) connections, and PPTP client connections.

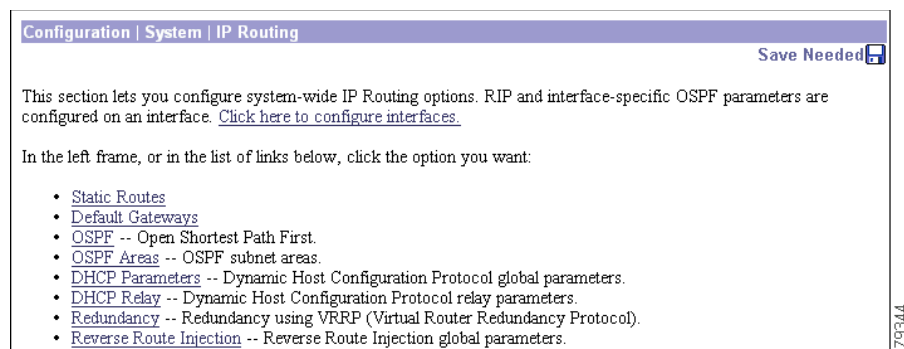
Configuration | System | IP Routing

This section of the Manager lets you configure system-wide IP routing parameters:

- **Static Routes:** Manually configured routing tables.
- **Default Gateways:** Routes for otherwise unrouted traffic.
- **OSPF:** Open Shortest Path First routing protocol.
- **OSPF Areas:** Subnet areas within the OSPF domain.
- **DHCP:** Dynamic Host Configuration Protocol global parameters for DHCP Proxy and DHCP relay.
- **Redundancy:** Virtual Router Redundancy Protocol parameters.
- **Reverse Route Injection:** Reverse Route Injection global parameters.

You configure RIP and interface-specific OSPF parameters on the network interfaces; click the highlighted link to go to the Configuration | Interfaces screen.

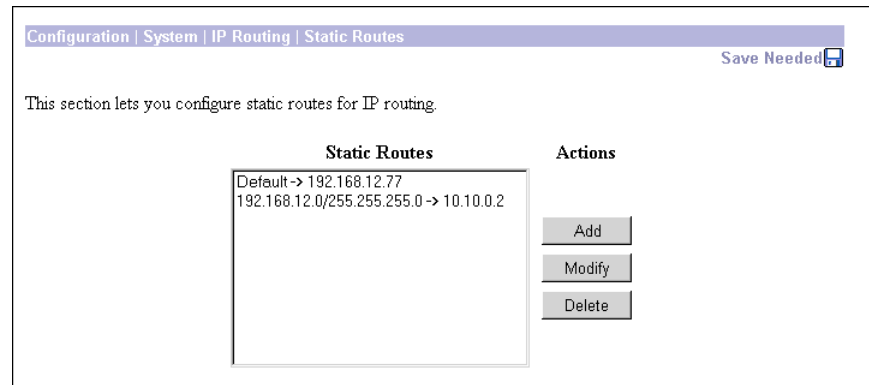
Figure 8-1 Configuration | System | IP Routing Screen



Configuration | System | IP Routing | Static Routes

This section of the Manager lets you configure static routes for IP routing. You usually configure static routes for private networks that cannot be learned via RIP or OSPF.

Figure 8-2 Configuration | System | IP Routing | Static Routes Screen



Static Routes

The Static Routes list shows manual IP routes that have been configured. The format is *[destination network address/subnet mask -> outbound destination]*, for example: 192.168.12.0/255.255.255.0 -> 10.10.0.2. If you have configured the default gateway, it appears first in the list as Default -> default router address. If no static routes have been configured, the list shows --Empty--.



Note

The following static routing table limitations exist on the various platforms. The ability to populate all routes will depend on having sufficient system memory.

3002 - 50 routes

3005 - 200 routes

30XX - 10,240 routes

When the routing table is full, the following message will appear in the log:

```
12539 08/30/2001 22:07:55.270 SEV=2 IP/26 RPT=12
```

```
Routing Table Full, add new route failed.
```

Add / Modify / Delete

To configure and add a new static route, click **Add**. The Manager opens the Configuration | System | IP Routing | Static Routes | Add screen.

To modify a configured static route, select the route from the list and click **Modify**. The Manager opens the Configuration | System | IP Routing | Static Routes | Modify screen. If you select the default gateway, the Manager opens the Configuration | System | IP Routing | Default Gateways screen.

To delete a configured static route, select the route from the list and click **Delete**.



Note

There is no confirmation and no undo.

The Manager refreshes the screen and shows the remaining static routes in the list. You cannot delete the default gateways here; to do so, see the Configuration | System | IP Routing | Default Gateways screen.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | IP Routing | Static Routes | Add or Modify

These Manager screens let you:

- Add: Configure and add a new static, or manual, route to the IP routing table.
- Modify: Modify the parameters for a configured static route.

Figure 8-3 Configuration | System | IP Routing | Static Routes | Add or Modify Screen

Configuration | System | IP Routing | Static Routes | Add

Configure and add a static route.

Network Address Enter the network address.

Subnet Mask Enter the subnet mask.

Metric Enter the numeric metric for this route (1 through 16).

Destination

Router Address Enter the router/gateway IP address.

Interface Ethernet 1 (Private) (10.10.99.30) Select the interface to route to.

Add Cancel

67103

Network Address

Enter the destination network IP address to which this static route applies. Packets with this destination address will be sent to the destination you enter. Used dotted decimal notation, for example: 192.168.12.0.

Subnet Mask

Enter the subnet mask for the destination network IP address. Use dotted decimal notation, for example: 255.255.255.0. The subnet mask indicates which part of the IP address represents the network and which part represents hosts. The router subsystem looks at only the network part.

The Manager automatically supplies a standard subnet mask appropriate for the IP address you just entered. For example, the IP address 192.168.12.0 is a Class C address, and the standard subnet mask is 255.255.255.0. You can accept this entry or change it. Note that 0.0.0.0 is not allowed here, since that would resolve to the equivalent of a default gateway.

Metric

Enter the metric, or cost, for this route. Use a number from 1 to 16, where 1 is the lowest cost. The routing subsystem always tries to use the least costly route. For example, if a route uses a low-speed line, you might assign a high metric so the system will use it only if all high-speed routes are unavailable.

Destination

Click a radio button to choose the outbound destination for these packets. You can choose only one destination: either a specific router/gateway, or a VPN Concentrator interface.

Router Address

Enter the IP address of the specific router or gateway to which to route these packets; that is, the IP address of the next hop between the VPN Concentrator and the ultimate destination of the packet. Use dotted decimal notation, for example: 10.10.0.2.

Interface

Click the **Interface** drop-down menu button and choose a configured VPN Concentrator interface as the outbound destination. The menu lists all interfaces that have been configured. The default interface for a static route is the Ethernet 2 (Public) interface.

For example, in a LAN-to-LAN configuration where remote-access clients are assigned IP addresses that are not on the private network, you could configure a static route with those addresses outbound to the Ethernet 1 (Private) interface. The clients could then access the peer VPN Concentrator and its networks.

Add or Apply / Cancel

To add a new static route to the list of configured routes, click **Add**. Or to apply your changes to a static route, click **Apply**. Both actions include your entries in the active configuration. The Manager returns to the Configuration | System | IP Routing | Static Routes screen. Any new route appears at the bottom of the Static Routes list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | IP Routing | Static Routes screen, and the Static Routes list is unchanged.

Configuration | System | IP Routing | Default Gateways

This screen lets you configure the default gateway for IP routing, and configure the tunnel default gateway for tunneled traffic. You use this same screen both to initially configure and to change default gateways. You can also configure the default gateway on the Configuration | Quick | System Info screen.

The IP routing subsystem routes data packets first using learned routes, then static routes, then the default gateway. If you do not specify a default gateway, the system drops packets it cannot otherwise route.

For tunneled data, if the system does not know a destination address, it tries to route the packet to the tunnel default gateway first. If that route is not configured, it uses the regular default gateway.

Figure 8-4 Configuration | System | IP Routing | Default Gateways Screen

Configuration | System | IP Routing | Default Gateways

Configure the default gateways for your system.

Default Gateway Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.

Metric Enter the metric, from 1 to 16.

Tunnel Default Gateway Enter the IP address of the default gateway or router for tunnels. Enter 0.0.0.0 for no default router.

Override Default Gateway Check to allow learned default gateways to override the configured default gateway.

67198

Default Gateway

Enter the IP address of the default gateway or router. Use dotted decimal notation, for example: 192.168.12.77. This address must *not* be the same as the IP address configured on any VPN Concentrator interface. If you do not use a default gateway, enter 0.0.0.0 (the default entry).

To delete a configured default gateway, enter 0.0.0.0.

The default gateway must be reachable from a VPN Concentrator interface, and it is usually on the public network. The Manager displays a warning screen if you enter an IP address that is not on one of its interface networks, and it displays a dialog box if you enter an IP address that is not on the public network.

Metric

Enter the metric, or cost, for the route to the default gateway. Use a number from 1 to 16, where 1 is the lowest cost. The routing subsystem always tries to use the least costly route. For example, if this route uses a low-speed line, you might assign a high metric so the system will use it only if all high-speed routes are unavailable.

Tunnel Default Gateway

Enter the IP address of the default gateway for tunneled data. Use dotted decimal notation, for example: 10.10.0.2. If you do not use a tunnel default gateway, enter 0.0.0.0 (the default entry).

To delete a configured tunnel default gateway, enter 0.0.0.0.

This gateway is often a firewall in parallel with the VPN Concentrator and between the public and private networks. The tunnel default gateway applies to all tunneled traffic, including IPsec LAN-to-LAN traffic.

**Note**

If you use an external device instead of the VPN Concentrator for NAT (Network Address Translation), you must configure the tunnel default gateway.

Override Default Gateway

To allow default gateways learned via RIP or OSPF to override the configured default gateway, check the **Override Default Gateway** check box (the default). To always use the configured default gateway, uncheck the box.

Apply / Cancel

To apply the settings for default gateways, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | IP Routing screen. If you configure a Default Gateway, it also appears in the Static Routes list on the Configuration | System | IP Routing | Static Routes screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | IP Routing screen.

Configuration | System | IP Routing | OSPF

This screen lets you configure system-wide parameters for the OSPF (Open Shortest Path First) routing protocol. You must also configure interface-specific OSPF parameters on the Configuration | Interfaces screens.

OSPF is a protocol that the IP routing subsystem uses for messages to other OSPF routers within an internal or private network, to determine network connectivity, status, and optimum paths for sending data traffic. The VPN Concentrator supports OSPF version 2 (RFC 2328).

The complete private network is called an OSPF Autonomous System (AS), or domain. The subnets within the AS are called areas. You configure OSPF areas on the Configuration | System | IP Routing | OSPF Areas screens.

Figure 8-5 Configuration | System | IP Routing | OSPF Screen

Enabled

To enable the VPN Concentrator OSPF router, check the **Enabled** check box. (By default it is unchecked.) You must also enter a Router ID. You must check this box for OSPF to work on any interface that uses it.

To change a configured Router ID, you must disable OSPF here.

To enable OSPF routing on an interface, you must also configure and enable OSPF on the appropriate Configuration | Interfaces screen.

Router ID

The router ID uniquely identifies the VPN Concentrator OSPF router to other OSPF routers in its domain. While the format is that of an IP address, it functions only as an identifier and not an address. By convention, however, this identifier is the same as the IP address of the interface that is connected to the OSPF router network.

Enter the router ID in the field. Use dotted decimal IP address format, for example: 10.10.4.6. The default entry is 0.0.0.0 (no router configured). If you enable the OSPF router, you must enter an ID.

**Note**

Once you configure and apply a router ID, you must disable OSPF before you can change it. You cannot change the ID back to 0.0.0.0.

Autonomous System

An OSPF Autonomous System (AS), or domain, is a complete internal network. An AS boundary router exchanges routing information with routers belonging to other Autonomous Systems, and advertises external AS routing information throughout its AS. If you are using reverse route injection (RRI) with OSPF, you must enable Autonomous System.

Check the **Autonomous System** check box to indicate that the VPN Concentrator OSPF router is the boundary router for an Autonomous System. If you check this box, the VPN Concentrator also redistributes RIP and static routes into the OSPF areas. By default, the box is unchecked.

Apply / Cancel

To apply your OSPF settings, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | IP Routing screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

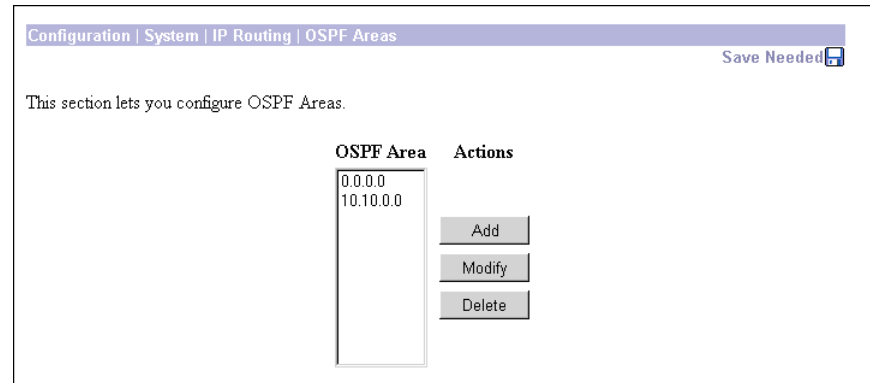
To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | IP Routing screen.

Configuration | System | IP Routing | OSPF Areas

This section of the Manager lets you configure OSPF areas, which are the subnets within an OSPF Autonomous System or domain. You should configure entries for all areas connected to this VPN Concentrator OSPF router.

You can also identify an OSPF area on a VPN Concentrator network interface (see Configuration | Interfaces). Those area identifiers appear in the OSPF Area list on this screen.

Figure 8-6 Configuration | System | IP Routing | OSPF Areas Screen



OSPF Area

The OSPF Area list shows identifiers for all areas that are connected to this VPN Concentrator OSPF router. The format is the same as a dotted decimal IP address, for example: 10.10.0.0. The default entry is 0.0.0.0. This entry identifies a special area known as the backbone that contains all area border routers, which are the routers connected to multiple areas.

Add / Modify / Delete

To configure and add a new OSPF area, click **Add**. The Manager opens the Configuration | System | IP Routing | OSPF Areas | Add screen.

To modify a configured OSPF area, select the area from the list and click **Modify**. The Manager opens the Configuration | System | IP Routing | OSPF Areas | Modify screen.

To delete a configured OSPF area, select the area from the list and click **Delete**.



Note

There is no confirmation or undo.

The Manager refreshes the screen and shows the remaining entries in the OSPF Area list.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | IP Routing | OSPF Areas | Add or Modify

These Manager screens let you:

- Add: Configure and add an OSPF area.
- Modify: Modify parameters for a configured OSPF area.



Note

Once you have configured an OSPF Area, you cannot modify its ID. To change an area ID, delete the existing area and add a new one.

Figure 8-7 Configuration | System | IP Routing | OSPF Areas | Add or Modify Screen

Area ID

- Add: Enter the area ID in the field. Use IP address dotted decimal notation, for example: 10.10.0.0. The default entry is 0.0.0.0, the backbone.
- Modify: Once you have configured an area ID, you cannot change it. See preceding note.

The Area ID identifies the subnet area within the OSPF Autonomous System or domain. While its format is the same as an IP address, it functions only as an identifier and not an address. The 0.0.0.0 area ID identifies a special area—the backbone—that contains all area border routers.

Area Summary

Check the **Area Summary** check box to have the OSPF router generate and propagate summary LSAs (Link-State Advertisements) into OSPF stub areas. LSAs describe the state of the router's interfaces and routing paths. Stub areas contain only final-destination hosts and do not pass traffic through to other areas. Sending LSAs to them is usually not necessary. By default this box is unchecked.

External LSA Import

Click the **External LSA Import** drop-down menu button and choose whether to bring in LSAs from neighboring Autonomous Systems. LSAs describe the state of the AS router's interfaces and routing paths. Importing those LSAs builds a more complete link-state database, but it requires more processing. The choices are:

- External = Yes, import LSAs from neighboring ASs (the default).
- No External = No, do not import external LSAs.

Add or Apply / Cancel

To add this OSPF area to the list of configured areas, click **Add**. Or to apply your changes to this OSPF area, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | System | IP Routing | OSPF Areas screen. Any new entry appears at the bottom of the OSPF Area list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | IP Routing | OSPF Areas screen, and the OSPF Area list is unchanged.

Configuration | System | IP Routing | DHCP Parameters

This screen lets you configure DHCP (Dynamic Host Configuration Protocol) Proxy parameters that apply to DHCP functions within the VPN Concentrator. You can use external DHCP servers to assign IP addresses to the VPN tunnel as it is established.

If you check the Use DHCP check box on the Configuration | System | Address Management | Assignment screen, you must configure at least one DHCP server on the Configuration | System | Servers | DHCP screens. You configure global DHCP parameters here.

Figure 8-8 Configuration | System | IP Routing | DHCP Parameters Screen

Configuration | System | IP Routing | DHCP Parameters

Configure system-wide DHCP (Dynamic Host Configuration Protocol) parameters.

Enabled Check to enable support for DHCP services (Proxy and Client on interfaces).

Lease Timeout minutes

Listen Port *We recommend that you not change this default.*

Timeout Period seconds

Apply Cancel

79323

Enabled

Check the **Enabled** check box to enable DHCP Proxy, which allows the VPN tunnel to get its IP address from a DHCP server. The box is checked by default.

Lease Timeout

Enter the timeout in minutes for addresses that are obtained from a DHCP server. The minimum timeout is 5 minutes. The default is 120 minutes. The maximum is 500000 minutes. DHCP servers “lease” IP addresses for this period of time. Before the lease expires, the VPN Concentrator asks to renew it on behalf of the client. If for some reason the lease is not renewed, the connection terminates when the lease expires. The DHCP server’s lease period takes precedence over this setting.

Listen Port

Enter the UDP port number on which DHCP server response messages are accepted. The default is 67, which is the well-known port. *To ensure proper communication with DHCP servers, we strongly recommend that you not change this default.*

Timeout Period

Enter the initial time in seconds to wait for a response to a DHCP request before sending the request to the next configured DHCP server. The minimum time is 1 second. The default time is 2 seconds. The maximum time is 30 seconds. This time doubles with each cycle through the list of configured DHCP servers.

Apply / Cancel

To apply the settings for DHCP parameters, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | IP Routing screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | IP Routing screen.

Configuration | System | IP Routing | DHCP Relay

DHCP relay lets VPN clients, particularly wireless clients, obtain a network configuration from a DHCP server on the VPN Concentrator's private network before creating a VPN tunnel. The client sends a DHCP request to the public or external network. The VPN Concentrator receives the DHCP request on its public or external interface, and forwards the request. To respond with a DHCP offer, one or more DHCP servers on the corporate network must have an IP address scope for the public network. When the DHCP server does respond with a DHCP offer, the VPN client and the DHCP server then proceed with DHCP negotiations, with the VPN Concentrator acting as a router, relaying DHCP messages between them.

The primary benefit of DHCP relay is that you do not have to maintain a separate DHCP server for VPN clients. For DHCP relay to work, however, the VPN Concentrator allows unauthenticated DHCP traffic through the VPN Concentrator. This poses a potential security risk, for example, vulnerability to denial of service attacks by requesting all available DHCP addresses, or by exhausting CPU and/or network bandwidth. You should be aware of these security issues.



Note

To enable DHCP relay, you must also assign the DHCP In and DHCP Out rules to the interface filter in the Configuration | Policy Management | Traffic Management | Filters screen.

Configuration | System | IP Routing | DHCP Relay

Configure DHCP Relay (Dynamic Host Configuration Protocol) parameters.

To enable DHCP Relay, you must also assign proper rules to filters in the **Configuration | Policy Management | Traffic Management | Filters** screen.

Enabled Check to enable DHCP Relay.

DHCP Info Transmission Broadcast to all interfaces.

Forward to Enter the network/host address.

Enter the subnet mask.

79524

Enabled

Check the **Enabled** check box to enable DHCP relay on the VPN Concentrator.

DHCP Info Transmission

This parameter determines how the VPN Concentrator transmits DHCP requests. Select one of these options:

- Broadcast to all interfaces = DHCP requests that come in the public interface are broadcast out the private and external interfaces. DHCP requests that come in the external interface are broadcast out the private interface.
- Forward to a specific network/host address, including the subnet mask=DHCP requests are sent to a specific network or host. Enter the IP address and subnet mask for the network or host. Remember that the subnet mask for a specific host is 255.255.255.255.

Apply / Cancel

To apply the settings for DHCP relay parameters, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | IP Routing screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | IP Routing | Redundancy

This screen lets you configure parameters for Virtual Router Redundancy Protocol (VRRP), which manages automatic switch over from one VPN Concentrator to another in a redundant installation. Automatic switchover provides user access to the VPN even if the primary VPN Concentrator is out of service.

These functions apply only to installations where two or more VPN Concentrators are in parallel. One VPN Concentrator is the master system, and the other(s) are backup systems. A backup system acts as a virtual master system when a switchover occurs.

**Note**

If VRRP is configured on a VPN Concentrator, you cannot also enable load balancing. In a VRRP configuration, the backup device remains idle unless the active VPN Concentrator fails. Load balancing does not permit idle devices.

This feature supports user access via IPsec LAN-to-LAN connections, IPsec client (single-user remote-access) connections, and PPTP client connections.

- For IPsec LAN-to-LAN connections, switchover is fully automatic. Users do not need to do anything. Switchover typically occurs within 3 to 10 seconds.
- For single-user IPsec and PPTP connections, users are disconnected from the failing system but they can reconnect without changing any connection parameters.

Before configuring or enabling VRRP on this screen, you must configure all Ethernet interfaces that apply to your installation, on all redundant VPN Concentrators. See the Configuration | Interfaces screens.

You must also configure *identical* IPsec LAN-to-LAN parameters on the redundant VPN Concentrators. See the Configuration | System | Tunneling Protocols | IPsec LAN-to-LAN screens.

**Note**

VRRP cannot be used when DHCP is enabled on the VPN Concentrator's interfaces. Use static IP addressing when VRRP is enabled.

In a VRRP configuration, if the public or private interface of the master system goes down, the other interfaces shut down automatically and the backup VPN device takes over. The backup VPN device takes over only when it stops receiving VRRP messages on *both* the public and private interfaces.

Some failure cases are not detected by VRRP. If a forwarding device (router or switch) fails on a network connecting the VRRP master and backup devices, the master might not detect the failure at the link level. For example, if you have a Cisco Catalyst switch between the master and backup devices and you shut that switch port down, this shutdown does not bring down the link layer. As long as the link layer is up, the VPN Concentrator does not detect the interface as "DOWN" (appearing on the Configuration | Interfaces screen), and therefore it does not stop sending messages to the backup device on all its interfaces. In this case, because the backup device is still receiving VRRP messages on at least one interface, it does not take over as the master.

Also, when a Cisco Catalyst switch in a VRRP scenario uses Spanning-Tree Protocol (STP), the inherent delays with STP cause a delay in recognizing that a backup VPN Concentrator has taken over as the master. To reduce this delay to 15 seconds, enable Portfast on switches that use STP. To configure Portfast on Cisco switches, refer to the document:

<http://www.cisco.com/warp/public/473/12.html>

Figure 8-9 Configuration | System | IP Routing | Redundancy Screen

Configuration | System | IP Routing | Redundancy

Configure the Virtual Router Redundancy Protocol (VRRP) for your system. All interfaces that you want to configure VRRP on should already be configured. If you later configure an additional interface, you need to revisit this screen.

Enable VRRP Check to enable VRRP.

Group ID Enter the Group ID for this set of redundant routers.

Group Password Enter the shared group password, or leave blank for no password.

Role Select the Role for this system within the group.

Advertisement Interval Enter the Advertisement interval (seconds).

Group Shared Addresses

1 (Private)

2 (Public)

3 (External)

79365

Enable VRRP

Check the **Enable VRRP** check box to enable VRRP functions. The box is unchecked by default.

Group ID

Enter a number that uniquely identifies this group of redundant VPN Concentrators. This number must be the same on all systems in this group. Use a number from 1 (default) to 255. Since there is rarely more than one virtual group on a LAN, we suggest you accept the default.

Group Password

Enter a password for additional security in identifying this group of redundant VPN Concentrators. The maximum password length is 8 characters. The Manager shows your entry in clear text, and VRRP advertisements contain this password in clear text. This password must be the same on all systems in this group. Leave this field blank to use no password.

Role

Click the **Role** drop-down menu button and choose the role of this VPN Concentrator in this redundant group.

- Master = This is the Master system in this group (the default choice). Be sure to configure only one Master system in a group with a given Group ID.
- Backup 1 through Backup 5 = This is a Backup system in this group.

Advertisement Interval

Enter the time interval in seconds between VRRP advertisements to other systems in this group. Only the Master system sends advertisements; this field is ignored on Backup systems while they remain Backup. The minimum interval is 1 second. The default interval is 1 second. The maximum is 255 seconds. Since a Backup system can become a Master system, we suggest you accept the default for all systems.

Group Shared Addresses

Enter the IP addresses that are treated as configured router addresses by all virtual routers in this group. The Manager displays fields only for the Ethernet interfaces that have been configured.

On the Master system, these entries are the IP addresses configured on its Ethernet interfaces, and the Manager supplies them by default.

On a Backup system, the fields are empty by default, and you must enter the same IP addresses as those on the *Master* system.

1 (Private)

The IP address for the Ethernet 1 (Private) interface shared by the virtual routers in this group.

2 (Public)

The IP address for the Ethernet 2 (Public) interface shared by the virtual routers in this group.

3 (External)

The IP address for the Ethernet 3 (External) interface shared by the virtual routers in this group.

Apply / Cancel

To apply the settings for VRRP, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | IP Routing screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | IP Routing screen.

Configuration | System | IP Routing | Reverse Route Injection

The VPN Concentrator can automatically add static routes to the routing table and announce these routes to its private network or border routers using OSPF or RIP. This feature is called *reverse route injection (RRI)*. The RRI options that you can configure vary with the type of connection:

- Remote software clients or VPN 3002 Hardware Clients using Client (PAT) mode:
 - For individual remote clients, enable the Client Reverse Route Injection option.
 - For a group of remote clients, enter an address pool in the Address Pool Hold Down Routes field.
- Remote VPN 3002 Hardware Clients using Network Extension Mode (NEM): enable the Network Extension Reverse Route Injection option.
- LAN-to-LAN connections: see the Routing option on the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add or Modify screen.

To add routes to the routing table of the VPN Concentrator without advertising them to the private network, disable routing on the private interface.

To advertise the routes, enable OSPF or RIP on the VPN Concentrator's private interface. (See the Configuration | Interfaces | Ethernet 1 2 3 screen, RIP or OSPF tabs.)

Figure 8-10 Configuration | System | IP Routing | Reverse Route Injection Screen

Configuration | System | IP Routing | Reverse Route Injection

Configure system-wide *Reverse Route Injection* parameters. This feature adds specific routes to the routing table for distribution via RIP or OSPF to neighbouring routers for path discovery. Click on **Generate Hold Down Routes** to generate hold down routes based on configured address pools.

Client Reverse Route Injection

Network Extension Reverse Route Injection

Address Pool Hold Down Routes

Check to add non-local (to the private interface) client host routes to the routing table.

Check to add hardware client network extension connection routes to the routing table.

- Add or modify network address and subnet mask using the following standard format: **n.n.n.n/n.n.n.n** (e.g. 192.168.90.64/255.255.255.192).
- Enter each network address and subnet mask pair on a single line.
- If you are using the natural subnet mask, you may omit the subnet mask.

Apply
Cancel
Generate Hold Down Routes

66205

Client Reverse Route Injection

**Note**

This option applies to all remote software clients and VPN 3002 Hardware Clients using Client (PAT) Mode.

Check the **Client Reverse Route Injection** check box to add host routes for each remote client to the VPN Concentrator routing table. The VPN Concentrator adds a host route when the client connects and deletes it when the client disconnects.

This option adds individual clients; to add address pools, use the Address Pool Hold Down Routes option.

This box is unchecked by default.

Network Extension Reverse Route Injection

**Note**

This option applies only to VPN 3002 Hardware Clients using Network Extension Mode.

Check the **Network Extension Reverse Route Injection** check box to add a network route for each network behind a VPN 3002 Hardware Client to the routing table on the VPN Concentrator. The VPN Concentrator adds the route when the VPN 3002 connects and deletes the route when it disconnects.

This box is unchecked by default.

Address Pool Hold Down Routes

**Note**

This option applies to all remote software clients and VPN 3002 Hardware Clients using Client (PAT) Mode.

In the **Address Pool Hold Down Routes** field, enter any hold down routes to add to the VPN Concentrator routing table. You can either enter routes automatically or manually:

- To automatically generate a list of hold down routes based on currently configured address pools, click the **Generate Hold Down Routes** button. You can then edit this list, if you want.
- If you are entering routes manually, use the following format: *n.n.n.n/n.n.n.n*; for example, 192.168.90.64/255.255.255.192. Enter each network address/subnet mask pair on a single line.

If you configure both the Client Reverse Route Injection and the Address Pool Hold Down Routes fields, when a remote client connects to the VPN Concentrator, the VPN Concentrator checks first to see if the client address falls under any of the address pool routes listed here. If not, it adds the client's route to the routing table.

Generate Hold Down Routes

**Note**

If you have typed any entries into the Address Pool Hold Down Routes window, clicking this button will erase them. If you want to keep these previous entries, copy them to a file or clipboard and paste them back in after clicking the Generate Hold Down Routes button.

Click the **Generate Hold Down Routes** button to automatically display hold down routes based on configured address pools in the Address Pool Hold Down Routes window.

Apply / Cancel

To apply the settings for Reverse Route Injection, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | IP Routing screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | IP Routing screen.



Management Protocols

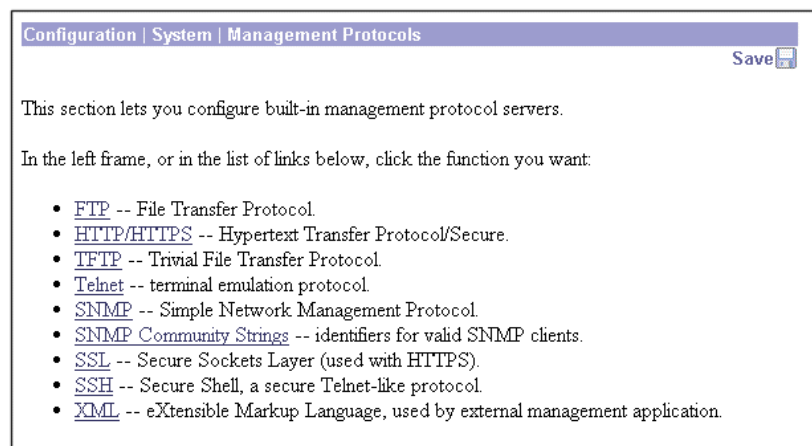
The VPN 3000 Concentrator Series includes various built-in servers, using various protocols, that let you perform typical network and system management functions. This section explains how you configure and enable those servers.

Configuration | System | Management Protocols

This section of the Manager lets you configure and enable built-in VPN Concentrator servers that provide management functions using:

- FTP: File Transfer Protocol.
- HTTP/HTTPS: Hypertext Transfer Protocol, and HTTP over SSL (Secure Sockets Layer) protocol.
- TFTP: Trivial File Transfer Protocol.
- Telnet: Terminal emulation protocol, and Telnet over SSL.
- SNMP: Simple Network Management Protocol.
- SNMP Community Strings: Identifiers for valid SNMP clients.
- SSL: Secure Sockets Layer protocol.
- SSH: Secure Shell.
- XML: Extensible Markup Language.

Figure 9-1 Configuration | System | Management Protocols Screen



Configuration | System | Management Protocols | FTP

This screen lets you configure and enable the VPN Concentrator's FTP (File Transfer Protocol) server. When the server is enabled, you can use an FTP client to upload and download files in VPN Concentrator Flash memory.

FTP server login usernames and passwords are the same as those enabled and configured on the Administration | Access Rights | Administrators screens. To protect security, the VPN Concentrator does not allow anonymous FTP login.

The settings here have no effect on FTP backup of event log files. (See Configuration | System | Events | General and FTP Backup.) For those operations, the VPN Concentrator acts as an FTP client.

Figure 9-2 Configuration | System | Management Protocols | FTP Screen

Configuration | System | Management Protocols | FTP

Configure the FTP server.

Enable Disabling will provide additional security.

Port The default port is 21. Changing the port will provide additional security.

Maximum Connections Enter the maximum number of concurrent control connections (sessions).

Apply Cancel

67246

Enable

Check the **Enable** check box to enable the FTP server. The box is checked by default. Disabling the FTP server provides additional security.

Port

Enter the port number that the FTP server uses. The default value is 21.

Maximum Connections

Enter the maximum number of concurrent control connections (sessions) that the FTP server allows. (FTP uses separate connections for control and data transfer during a session.) The minimum number is 1. The default is 5. The maximum is 20.

Apply / Cancel

To apply your FTP server settings, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | Management Protocols screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Management Protocols screen.

Configuration | System | Management Protocols | HTTP/HTTPS

This screen lets you configure and enable the VPN Concentrator's HTTP/HTTPS server: Hypertext Transfer Protocol and HTTP over SSL (Secure Sockets Layer) protocol. When the server is enabled, you can use a web browser to communicate with the VPN Concentrator. HTTPS lets you use a web browser over a secure, encrypted connection.



Note

The VPN Concentrator Manager requires the HTTP/HTTPS server. *If you click Apply, even if you have made no changes on this screen, you will break your HTTP/HTTPS connection and you must restart the Manager session from the login screen.*

If you disable *either* HTTP or HTTPS, and that is the protocol you are currently using, you can reconnect with the other protocol if it is enabled and configured.

If you disable *both* HTTP and HTTPS, you cannot use a web browser to connect to the VPN Concentrator. Use the Cisco Command Line Interface from the console or a Telnet session.


Related information:

- For information on installing the SSL digital certificate in your browser and connecting via HTTPS, see "[Using the VPN Concentrator Manager.](#)"
- To configure SSL parameters, see the Configuration | System | Management Protocols | SSL screen.
- To install, generate, view, or delete the SSL certificate on the VPN Concentrator, see the Administration | Certificate Management screens.

Figure 9-3 Configuration | System | Management Protocols | HTTP/HTTPS Screen

Configuration | System | Management Protocols | HTTP/HTTPS

Configure the HTTP/HTTPS server.

 If you click **Apply**, you will break your HTTP/HTTPS connection to this device, and you will have to restart from the login screen.

Enable HTTP Disabling will provide additional security.

Enable HTTPS HTTPS uses SSL encryption to provide security.

HTTP Port The default port is 80. Changing the port will provide additional security.

HTTPS Port The default port is 443. Changing the port will provide additional security.

Maximum Sessions Enter the maximum number of concurrent HTTP/HTTPS server users.

67247

Enable HTTP

Check the **Enable HTTP** check box to enable the HTTP server. The box is checked by default. You must enable HTTP to install the SSL certificate in the browser initially, so you can thereafter use HTTPS. Disabling the HTTP server provides additional security, but makes system management less convenient. See the preceding notes.

Enable HTTPS

Check the **Enable HTTPS** check box to enable the HTTPS server. The box is checked by default. HTTPS—also known as HTTP over SSL—lets you use the VPN Concentrator Manager over an encrypted connection.

HTTP Port

Enter the port number that the HTTP server uses. The default value is 80.

HTTPS Port

Enter the port number that the HTTPS server uses. The default value is 443.

Maximum Sessions

Enter the maximum number of concurrent, combined HTTP and HTTPS sessions (users) that the server allows. The minimum number of sessions is 1. The default number is 4. The maximum number is 10.

Apply / Cancel

To apply your HTTP/HTTPS server settings, to include your settings in the active configuration, *and to break the current HTTP/HTTPS connection*, click **Apply**. If HTTP or HTTPS is still enabled, the Manager returns to the main login screen. If both HTTP and HTTPS are disabled, you can no longer use the Manager.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Management Protocols screen.

Configuration | System | Management Protocols | TFTP

This screen lets you configure and enable the VPN Concentrator's TFTP (Trivial File Transfer Protocol) server. When the server is enabled, you can use a TFTP client to upload and download files in VPN Concentrator Flash memory.

TFTP is similar to FTP, but it has no login procedure and no user interface commands. It allows only file transfers. The lack of a login procedure makes it relatively insecure.

The settings here have no effect on TFTP file transfer from the Administration | File Management | TFTP Transfer screen. For those operations, the VPN Concentrator acts as a TFTP client.

Figure 9-4 Configuration | System | Management Protocols | TFTP Screen

Enable

Check the **Enable** check box to enable the TFTP server. The box is unchecked by default. Disabling the TFTP server provides additional security.

Port

Enter the port number that the TFTP server uses. The default port number is 69.

Maximum Connections

Enter the maximum number of simultaneous connections that the TFTP server allows. The minimum number is 1. The default number is 5. The maximum number is 20.

Timeout

Enter the timeout in seconds for inactive TFTP connections. The minimum timeout is 1 second. The default is 10 seconds. The maximum is 30 seconds. Change the default value only if you have problems with TFTP transfers.

Apply / Cancel

To apply your TFTP settings, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | Management Protocols screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Management Protocols screen.

Configuration | System | Management Protocols | Telnet

This screen lets you configure and enable the VPN Concentrator's Telnet terminal emulation server, and Telnet over SSL (Secure Sockets Layer protocol). When the server is enabled, you can use a Telnet client to communicate with the VPN Concentrator. You can fully manage and administer the VPN Concentrator using the Cisco Command Line Interface via Telnet.

Telnet server login usernames and passwords are the same as those enabled and configured on the Administration | Access Rights | Administrators screens.

Telnet/SSL uses a secure, encrypted connection. Although we are not aware of commercial Telnet/SSL clients, there are some working shareware applications. For example, see <ftp://ftp.gbn.net/pub/security/Crypto/SSLapps> for `ssltel02.zip`, an "SSL Telnet for Windows" shareware application. *(Please note that this application is mentioned for information only and that Cisco Systems does not supply, support, or endorse it in any way.)*

See the Configuration | System | Management Protocols | SSL screen to configure SSL parameters. See the Administration | Certificate Management | Certificates screen to manage the SSL digital certificate.

Figure 9-5 Configuration | System | Management Protocols | Telnet Screen

Configuration | System | Management Protocols | Telnet

Configure the Telnet server.

Enable Telnet	<input checked="" type="checkbox"/>	Disabling will provide additional security.
Enable Telnet/SSL	<input checked="" type="checkbox"/>	Telnet/SSL uses SSL encryption to provide security.
Telnet Port	<input type="text" value="23"/>	The default port is 23. Changing the port will provide additional security.
Telnet/SSL Port	<input type="text" value="992"/>	The default port is 992. Changing the port will provide additional security.
Maximum Connections	<input type="text" value="5"/>	Enter the maximum number of concurrent connections.

Apply Cancel

67252

Enable Telnet

Check the **Enable Telnet** check box to enable the Telnet server. The box is checked by default. Disabling the Telnet server provides additional security, but doing so prevents using the Cisco Command-Line Interface via Telnet.

Enable Telnet/SSL

Check the **Enable Telnet/SSL** check box to enable Telnet over SSL. The box is checked by default. Telnet/SSL uses Telnet over a secure, encrypted connection.

Telnet Port

Enter the port number that the Telnet server uses. The default value is 23.

Telnet/SSL Port

Enter the port number that Telnet over SSL uses. The default value is 992.

Maximum Connections

Enter the maximum number of concurrent, combined Telnet and Telnet/SSL connections that the server allows. The minimum number is 1. The default number is 5. The maximum number is 10.

Apply / Cancel

To apply your Telnet settings, and to include the settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | Management Protocols screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Management Protocols screen.

Configuration | System | Management Protocols | SNMP

This screen lets you configure and enable the VPN Concentrator's SNMP (Simple Network Management Protocol) server. When the server is enabled, you can use an SNMP client to collect information from the VPN Concentrator but not to configure it.

To use the SNMP server, you must also configure an SNMP Community on the Configuration | System | Management Protocols | SNMP Communities screen.

The settings on this screen have no effect on sending system events to SNMP trap destinations (see Configuration | System | Events | General and Trap Destinations). For those functions, the VPN Concentrator acts as an SNMP client.

Figure 9-6 Configuration | System | Management Protocols | SNMP Screen

Configuration | System | Management Protocols | SNMP

Configure the SNMP server.

Enable Disabling will provide additional security. You can use third-party SNMP managers only for viewing statistics, not for configuring this device.

Port The default port is 161. Changing the port will provide additional security.

Maximum Queued Requests Enter the maximum number of outstanding queued requests.

Apply Cancel

67249

Enable

Check the **Enable** check box to enable the SNMP server. The box is checked by default. Disabling the SNMP server provides additional security.

Port

Enter the port number that the SNMP server uses. The default value is 161.

Maximum Queued Requests

Enter the maximum number of outstanding queued requests that the SNMP server allows. The minimum number is 1. The default number is 4. The maximum number is 200.

Apply / Cancel

To apply your SNMP settings, and to include the settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | Management Protocols screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

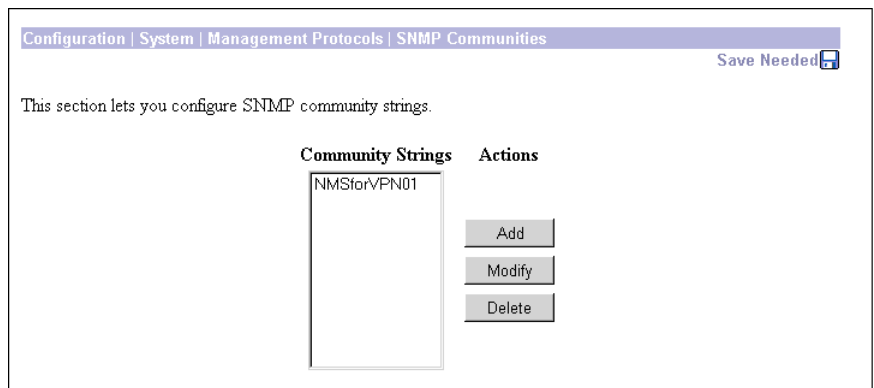
To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Management Protocols screen.

Configuration | System | Management Protocols | SNMP Communities

This section of the Manager lets you configure and manage SNMP community strings, which identify valid communities from which the SNMP server will accept requests. A community string is like a password: it validates messages between an SNMP client and the server.

To use the VPN Concentrator SNMP server, you must configure and add at least one community string. You can configure a maximum of 10 community strings. To protect security, the SNMP server does *not* include the usual default public community string, and we recommend that you not configure it.

Figure 9-7 Configuration | System | Management Protocols | SNMP Communities Screen



Community Strings

The Community Strings list shows SNMP community strings that have been configured. If no strings have been configured, the list shows --Empty--.

Add / Modify / Delete

To configure and add a new community string, click **Add**. The Manager opens the Configuration | System | Management Protocols | SNMP Communities | Add screen.

To modify a configured community string, select the string from the list and click **Modify**. The Manager opens the Configuration | System | Management Protocols | SNMP Communities | Modify screen.

To delete a configured community string, select the string from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the list.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | Management Protocols | SNMP Communities | Add or Modify

These Manager screens let you:

- Add: Configure and add a new SNMP community string.
- Modify: Modify a configured SNMP community string.

Figure 9-8 Configuration | System | Management Protocols | SNMP Communities | Add or Modify Screen

Configuration | System | Management Protocols | SNMP Communities | Add

Add an SNMP Community string.

Community String Enter the community string.

Add Cancel

67244

Community String

Enter the SNMP community string. Maximum 31 characters, case-sensitive.

Add or Apply / Cancel

To add this entry to the list of configured community strings, click **Add**. Or to apply your changes to this community string, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | System | Management Protocols | SNMP Communities screen; a new entry appears at the bottom of the Community Strings list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entry or changes, click **Cancel**. The Manager returns to the Configuration | System | Management Protocols | SNMP Communities screen, and the Community Strings list is unchanged.

Configuration | System | Management Protocols | SSL

This screen lets you configure the VPN Concentrator SSL (Secure Sockets Layer) protocol server. These settings apply to both HTTPS and Telnet over SSL. HTTPS lets you use a web browser over a secure, encrypted connection to manage the VPN Concentrator.

SSL creates a secure session between the client and the VPN Concentrator server. The client first authenticates the server, they negotiate session security parameters, and then they encrypt all data passed during the session. If, during negotiation, the server and client cannot agree on security parameters, the session terminates.

SSL uses digital certificates for authentication. The VPN Concentrator creates a self-signed SSL server certificate when it boots; or you can install in the VPN Concentrator an SSL certificate that has been issued in a PKI context. This certificate must then be installed in the client (for HTTPS; Telnet does not usually require it). You need to install the certificate from a given VPN Concentrator only once.

The default SSL settings should suit most administration tasks and network security requirements. *We recommend that you not change them unless advised to do so.*

**Note**

To ensure the security of your connection to the VPN Concentrator Manager, if you click **Apply** on this screen—even if you have made no changes—you will break your connection to the Manager and you must restart the Manager session from the login screen.

Related information:

- For information on installing the SSL digital certificate in your browser and connecting via HTTPS, see [Chapter 1, “Using the VPN Concentrator Manager”](#).
- To configure HTTPS parameters, see the Configuration | System | Management Protocols | HTTP/HTTPS screen.
- To configure Telnet/SSL parameters, see the Configuration | System | Management Protocols | Telnet screen.
- To manage SSL digital certificates, see the Administration | Certificate Management screens.

Figure 9-9 Configuration | System | Management Protocols | SSL Screen

Configuration | System | Management Protocols | SSL

Configure SSL.

Warning: If you click **Apply**, you will break your HTTP/HTTPS connection to this device, and you will have to restart from the login screen.

Encryption Protocols

- RC4-128/MD5
- 3DES-168/SHA
- DES-56/SHA
- RC4-40/MD5 Export
- DES-40/SHA Export

Check the encryption algorithms to enable. Unchecking them all disables SSL.

Client Authentication

Check to enable client authentication. Client authentication requires an installed Certificate Authority and a personal certificate installed in your browser.

SSL Version

Select the SSL version to use. Using a SSL V2 Hello provides compatibility with most browsers.

Generated Certificate Key Size

Select the key size used in the generated certificate.

67251

Encryption Protocols

Check the **Encryption Protocols** check boxes for the encryption algorithms that the VPN Concentrator SSL server can negotiate with a client and use for session encryption. All are checked by default. You must check at least one algorithm to enable SSL. *Unchecking all algorithms disables SSL.*

The algorithms are negotiated in the order shown. You cannot change the order, but you can enable or disable selected algorithms.

- RC4-128/MD5 = RC4 encryption with a 128-bit key and the MD5 hash function. This option is available in most SSL clients.
- 3DES-168/SHA = Triple-DES encryption with a 168-bit key and the SHA-1 hash function. This is the strongest (most secure) option.
- DES-56/SHA = DES encryption with a 56-bit key and the SHA-1 hash function.
- RC4-40/MD5 Export = RC4 encryption with a 128-bit key—40 bits of which are private—and the MD5 hash function. This option is available in the export (non-U.S.) versions of many SSL clients.
- DES-40/SHA Export = DES encryption with a 56-bit key—40 bits of which are private—and the SHA-1 hash function. This option is available in the export (non-U.S.) versions of many SSL clients.

Client Authentication

This parameter applies to HTTPS only; it is ignored for Telnet/SSL.

Check the **Client Authentication** check box to enable SSL client authentication. The box is unchecked by default. In the most common SSL connection, the client authenticates the server, not vice-versa. Client authentication requires personal certificates installed in the browser, and trusted certificates installed in the server. Specifically, the VPN Concentrator must have a root CA certificate installed; and a certificate signed by one of the VPN Concentrator's trusted CAs must be installed in the web browser. See Administration | Certificate Management.

SSL Version

Click the drop-down menu button and choose the SSL version to use. SSL Version 3 has more security options than Version 2, and TLS (Transport Layer Security) Version 1 has more security options than SSL Version 3. Some clients that send an SSL Version 2 "Hello" (initial negotiation), can actually use a more secure version during the session. Telnet/SSL clients usually can use only SSL Version 2.

Choices are:

- Negotiate SSL V2/V3 = The server tries to use SSL Version 3 but accepts Version 2 if the client cannot use Version 3. This is the default choice. It works with most browsers and Telnet/SSL clients.
- SSL V3 with SSL V2 Hello = The server insists on SSL Version 3 but accepts an initial Version 2 "Hello."
- SSL V3 Only = The server insists on SSL Version 3 only.
- SSL V2 Only = The server insists on SSL Version 2 only. This selection works with most Telnet/SSL clients.
- TLS V1 Only = The server insists on TLS Version 1 only. At present, only Microsoft Internet Explorer 5.0 supports this option.
- TLS V1 with SSL V2 Hello = The server insists on TLS Version 1 but accepts an initial SSL Version 2 "Hello." At present, only Microsoft Internet Explorer 5.0 supports this option.

Generated Certificate Key Size

Click the drop-down menu button and choose the size of the RSA key that the VPN Concentrator uses in its self-signed (generated) SSL server certificate. A larger key size increases security, but it also increases the processing necessary for all transactions over SSL. The increases vary, depending on the type of transaction (encryption or decryption).

Choices are:

- 512-bit RSA Key = This key size provides sufficient security. It is the most common, and requires the least processing.
- 768-bit RSA Key = This key size provides normal security. It requires approximately 2 to 4 times more processing than the 512-bit key.
- 1024-bit RSA Key = This key size provides high security and is the default choice. It requires approximately 4 to 8 times more processing than the 512-bit key.

Apply / Cancel

To apply your SSL settings, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | Management Protocols screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Management Protocols screen.

Configuration | System | Management Protocols | SSH

This screen lets you configure the VPN Concentrator SSH (Secure Shell) protocol server. SSH is a secure Telnet-like terminal emulator protocol that you can use to manage the VPN Concentrator, using the Command Line Interface, over a remote connection. The VPN Concentrator supports SSH1 (protocol version 1.5), which uses two RSA keys for security. All communication over the connection is encrypted.

At the start of an SSH session, the VPN Concentrator sends both a *host key* and a *server key* to the client, which responds with a *session key* that it generates and encrypts using the host and server keys. The RSA key of the SSL certificate is used as the host key, which uniquely identifies the VPN Concentrator. See Configuration | System | Management Protocols | SSL.

Figure 9-10 Configuration | System | Management Protocols | SSH Screen

Configuration | System | Management Protocols | SSH

Configure SSH. Only SSH1 (protocol version 1.5) is supported.

Enable SSH <input checked="" type="checkbox"/>	Disabling will provide additional security.
SSH Port <input type="text" value="22"/>	The default port is 22. Changing the port will provide additional security.
Maximum Sessions <input type="text" value="4"/>	Enter the maximum number of concurrent SSH users. Maximum is 10, default is 4. <i>SSH sessions are also limited by the configured number of maximum Telnet sessions.</i>
Key Regeneration Period <input type="text" value="60"/>	Enter the server key regeneration period in minutes. Setting to 0 disables server key regeneration. Maximum is 1 week (10080), default is 1 hour (60).
<input checked="" type="checkbox"/> 3DES-168	
Encryption Protocols <input checked="" type="checkbox"/> RC4-128	Check the encryption algorithms to enable. Unchecking them all effectively disables SSH.
<input checked="" type="checkbox"/> DES-56	
<input type="checkbox"/> No Encryption	
Enable SCP <input checked="" type="checkbox"/>	Check to enable file transfers via SCP (secure copy) over SSH.

Apply Cancel

79489

Enable SSH

Check the **Enable SSH** check box to enable the SSH server. The box is checked by default. Disabling the SSH server provides additional security by preventing SSH access.

SSH Port

Enter the port number that the SSH server uses. The default value is 22.

Maximum Sessions

Enter the maximum number of concurrent SSH sessions allowed. The minimum number is 1. The default number is 4. The maximum number is 10. The maximum number of concurrent SSH sessions is also limited by the maximum number of Telnet connections configured on the Configuration | System | Management Protocols | Telnet screen.

Key Regeneration Period

Enter the server key regeneration period in minutes. If the server key has been used for an SSH session, the VPN Concentrator regenerates the key at the end of this period. The minimum is 0 minutes (which disables key regeneration), the default is 60 minutes, and the maximum is 10080 minutes (1 week). Use 0 (disable key regeneration) only for testing, since it lessens security.

Encryption Protocols

Check the **Encryption Protocols** check boxes for the encryption algorithms that the VPN Concentrator SSH server can negotiate with a client and use for session encryption. You must check at least one encryption algorithm to enable a secure session. *Unchecking all algorithms disables SSH.*

- 3DES-168 = Triple-DES encryption with a 168-bit key. This option is the most secure but requires the greatest processing overhead.
- RC4-128 = RC4 encryption with a 128-bit key. This option provides adequate security and performance.
- DES-56 = DES encryption with a 56-bit key. This option is least secure but provides the greatest export flexibility.
- No Encryption = Connect without encryption. This option provides no security and is for testing purposes only. It is unchecked by default.



Note

The VPN Concentrator does not support the IDEA or Blowfish algorithms.

Enable SCP

Check the **Enable SCP** check box to enable file transfers using secure copy (SCP) over SSH.

Apply / Cancel

To apply your SSH settings, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | Management Protocols screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Management Protocols screen.

Configuration | System | Management Protocols | XML

This screen lets you configure the VPN Concentrator to support an XML-based management interface. Enabling XML management allows VPN 3000 Concentrators to be more easily managed by a centralized management system. XML is enabled by default. To disable the XML option, clear the check box. To re-enable the XML option, click the check box.

On this screen, you can also configure the VPN Concentrator to enable HTTPS or SSH (or both) on the Concentrator's Public interface and to lock the XML interface to a specific HTTPS or SSH IP address.

Figure 9-11 Configuration | System | Management Protocols | XML Screen

Configuration | System | Management Protocols | XML

Configure XML management.

Enable Check to enable XML management. Note that HTTPS or SSH must be enabled.

Enable HTTPS on Public Check to enable HTTPS on the Public interface. This will allow XML over HTTPS through the Public interface.

HTTPS IP Address Enter the IP address and wildcard from which to allow HTTPS access on on the Public interface. **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. Entering 0.0.0.0 will match the specified address; entering 255.255.255.255 will match *all* addresses.

HTTPS Wildcard-mask

Enable SSH on Public Check to enable SSH on the Public interface. This will allow XML over SSH through the Public interface.

SSH IP Address Enter the IP address and wildcard from which to allow SSH access on on the Public interface. **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. Entering 0.0.0.0 will match the specified address; entering 255.255.255.255 will match *all* addresses.

SSH Wildcard-mask

58224

Enable

Check the **Enable** check box, the default, to enable the XML management capability. You must also enable HTTPS or SSH on the VPN 3000 Concentrator's Public interface. Because enabling the XML management capability facilitates managing the VPN 3000 Concentrator by an external management application, do not disable the XML management capability unless you have a specific reason for doing so.

Enable HTTPS on Public

Check the **Enable HTTPS on Public** check box to allow HTML or XML management over HTTPS on the VPN Concentrator's Public interface.

HTTPS IP Address

Enter the IP address from which to allow HTTPS access on the VPN Concentrator's Public interface.

HTTPS Wildcard-mask

Enter the wildcard mask for the HTTPS IP address.

**Note**

Enter a *wildcard* mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, and 0s in bit positions to match. For example, entering 0.0.0.0 matches the *specified* address; entering 255.255.255.255 matches *all* addresses.

Enable SSH on Public

Check the **Enable SSH on Public** check box to allow command-line or XML management over Secure Shell (SSH) on the VPN Concentrator's Public interface.

SSH IP Address

Enter the IP address from which to allow SSH access on the VPN Concentrator's Public interface.

SSH Wildcard-mask

Enter the wildcard mask for the SSH IP address.

**Note**

Enter a *wildcard* mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, and 0s in bit positions to match. For example, entering 0.0.0.0 matches the *specified* address; entering 255.255.255.255 matches *all* addresses.



Events

An *event* is any significant occurrence within or affecting the VPN 3000 Concentrator, such as an alarm, trap (an event message sent to an SNMP system is called a “trap”), error condition, network problem, task completion, threshold breach, or status change. The VPN Concentrator records events in an event log, which is stored in nonvolatile memory. You can also specify that certain events trigger a console message, a UNIX syslog record, an e-mail message, or an SNMP management system trap.

Event attributes include *class* and *severity level*.

Event Class

Event class denotes the source of the event and refers to a specific hardware or software subsystem within the VPN Concentrator. [Table 10-1](#) lists the event classes.

Table 10-1 VPN Concentrator Event Classes

Class Name	Class Description (Event Source)	Cisco-Specific Event Class?
AUTH	Authentication	N
AUTHDBG	Authentication debugging	Y
AUTHDECODE	Authentication protocol decoding	Y
AUTOUPDATE	Autoupdate subsystem	N
BMGT	Bandwidth management subsystem	Y
BMGTDBG	Bandwidth management debugging	Y
CAPI	Cryptography subsystem	N
CERT	Digital certificates subsystem including SCEP	N
CONFIG	Configuration subsystem	N
DHCP	DHCP subsystem	N
DHCPDBG	DHCP debugging	Y
DHCPDECODE	DHCP decoding	Y
DM	Data Movement subsystem	N
DNS	DNS subsystem	N
DNSDBG	DNS debugging	Y

Table 10-1 VPN Concentrator Event Classes (continued)

Class Name	Class Description (Event Source)	Cisco-Specific Event Class?
DNSDECODE	DNS decoding	Y
EVENT	Event subsystem	N
EVENTDBG	Event subsystem debugging	Y
EVENTMIB	Event MIB changes	Y
EXPANSIONCARD	Expansion card (module) subsystem	N
FILTER	Filter subsystem	N
FILTERDBG	Filter debugging	Y
FSM	Finite State Machine subsystem (for debugging)	Y
FTPD	FTP daemon subsystem	N
GENERAL	NTP subsystem and other general events	N
GRE	GRE subsystem	N
GREDBG	GRE debugging	Y
GREDECODE	GRE decoding	Y
HARDWAREMON	Hardware monitoring (fans, temperature, voltages, etc.)	N
HTTP	HTTP subsystem	N
IKE	ISAKMP/Oakley (IKE) subsystem	N
IKEDBG	ISAKMP/Oakley (IKE) debugging	Y
IKEDECODE	ISAKMP/Oakley (IKE) decoding	Y
IP	IP router subsystem	N
IPDBG	IP router debugging	Y
IPDECODE	IP packet decoding	Y
IPSEC	IP Security subsystem	N
IPSECDBG	IP Security debugging	Y
IPSECDECODE	IP Security decoding	Y
L2TP	L2TP subsystem	N
L2TPDBG	L2TP debugging	Y
L2TPDECODE	L2TP decoding	Y
LBSSF	Load Balancing subsystem	N
MIB2TRAP	MIB-II trap subsystem: SNMP MIB-II traps	N
OSPF	OSPF subsystem	N
PPP	PPP subsystem	N
PPDBG	PPP debugging	Y
PPDECODE	PPP decoding	Y
PPTP	PPTP subsystem	N
PPTPDBG	PPTP debugging	Y

Table 10-1 VPN Concentrator Event Classes (continued)

Class Name	Class Description (Event Source)	Cisco-Specific Event Class?
PPTPDECODE	PPTP decoding	Y
PSH	Operating system command shell	N
PSOS	Embedded real-time operating system	N
QUEUE	System queue	N
REBOOT	System rebooting	N
RM	Resource Manager subsystem	N
SMTTP	SMTP event handling	N
SNMP	SNMP trap subsystem	N
SSH	SSH subsystem	N
SSL	SSL subsystem	N
SYSTEM	Buffer, heap, and other system utilities	N
TCP	TCP subsystem	N
TELNET	Telnet subsystem	N
TELNETDBG	Telnet debugging	Y
TELNETDECODE	Telnet decoding	Y
TIME	System time (clock)	N
VRRP	VRRP subsystem	N
XML	XML	N

**Note**

The Cisco-specific event classes provide information that is meaningful only to Cisco engineering or support personnel. Also, the DBG and DECODE events require significant system resources and might seriously degrade performance. We recommend that you avoid logging these events unless Cisco requests it.

Event Severity Level

Severity level indicates how serious or significant the event is,. It indicates how likely it is to cause unstable operation of the VPN concentrator, whether it represents a high-level or low-level operation, or whether it returns little or great detail. Level 1 is most significant. [Table 10-2](#) describes the severity levels.

Table 10-2 VPN Concentrator Event Severity Levels

Level	Category	Description
1	Fault	A crash or non-recoverable error.
2	Warning	A pending crash or severe problem that requires user intervention.
3	Warning	A potentially serious problem that might require user action.
4	Information	An information-only event with few details.
5	Information	An information-only event with moderate detail.
6	Information	An information-only event with greatest detail.
7	Debug	Least amount of debugging detail.
8	Debug	Moderate amount of debugging detail.
9	Debug	Greatest amount of debugging detail.
10	Packet Decode	High-level packet header decoding
11	Packet Decode	Low-level packet header decoding
12	Packet Decode	Hex dump of header
13	Packet Decode	Hex dump of packet

Within a severity level category, higher-numbered events provide more details than lower-numbered events, without necessarily duplicating the lower-level details. For example, within the Information category, Level 6 provides greater detail than Level 4, but does not necessarily include the same information as Level 4.

Logging higher-numbered severity levels causes performance to deteriorate, since more system resources are used to log and handle these events.



Note

The Debug (7–9) and Packet Decode (10–13) severity levels are intended for use by Cisco engineering and support personnel. We recommend that you avoid logging these events unless Cisco requests it.

The VPN Concentrator, by default, displays all events of severity level 1 through 3 on the console. It writes all events of severity level 1 through 5 to the event log. You can change these defaults on the Configuration | System | Events | General screen, and you can configure specific events for special handling on the Configuration | System | Events | Classes screens.

Event Log

The VPN Concentrator records events in an event log, which is stored in nonvolatile memory. Thus the event log persists even if the system is powered off. For troubleshooting any system difficulty, or just to examine details of system activity, consult the event log first.

The Model 3015–3080 event log holds 2048 events, the Model 3005 holds 256 events. The log wraps when it is full; that is, newer events overwrite older events when the log is full.

For the event log, you can configure:

- Which event classes and severity levels to log.
- Whether to save the event log to a file in Flash memory when it is full (when it wraps). And if so:
 - The format of the information in the saved log file.
 - Whether to automatically send a copy of the saved log file via FTP to a remote system.

Event Log Data

Each entry (record) in the event log consists of several fields including:

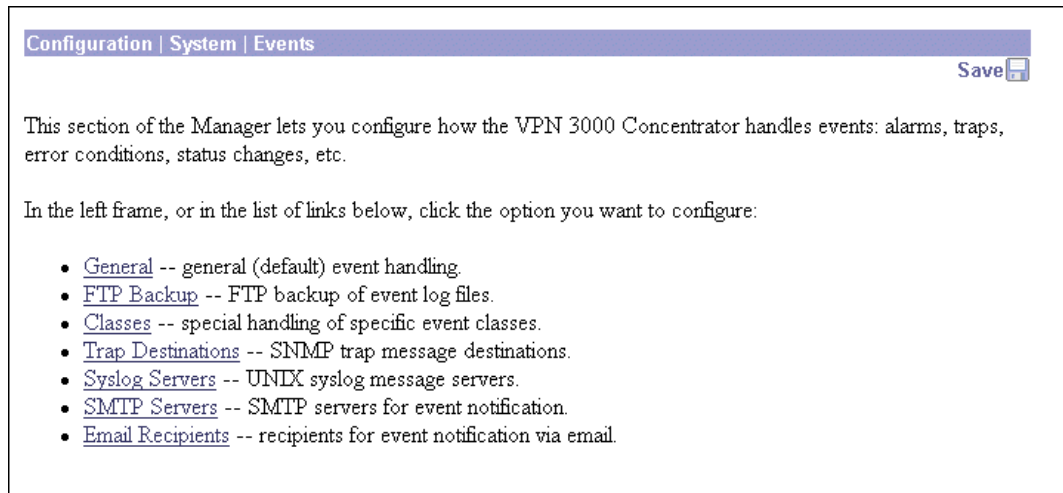
- A sequence number.
- Date and time.
- Event severity level.
- Event class and number.
- Event repetition count.
- Event IP address (only for certain events).
- Description string.

For more information, see the Monitoring | Filterable Event Log screen.

Configuration | System | Event

This section of the Manager lets you configure how the VPN Concentrator handles events. Events provide information for system monitoring, auditing, management, accounting, and troubleshooting.

Figure 10-1 Configuration | System | Events Screen



Configuration | System | Events | General

This Manager screen lets you configure the general, or default, handling of all events. These defaults apply to all event classes.

You can override these default settings by configuring specific events for special handling on the Configuration | System | Events | Classes screens.

Figure 10-2 Configuration | System | Events | General Screen

The screenshot shows a configuration window titled "Configuration | System | Events | General". Below the title bar, it says "This section lets you configure default event handling." The settings are as follows:

- Save Log on Wrap:** Check to save the event log to a file on wrap.
- Save Log Format:** Multiline (dropdown) Select the format of the saved log files.
- FTP Saved Log on Wrap:** Check to automatically FTP the saved log to a remote destination.
- Email Source Address:** [Text Field] Enter the email address that appears in the **From:** field.
- Syslog Format:** Original (dropdown) Select the format of Syslog messages.
- Severity to Log:** 1-5 (dropdown) Select the range of severity values to enter in the log.
- Severity to Console:** 1-3 (dropdown) Select the range of severity values to display on the console.
- Severity to Syslog:** None (dropdown) Select the range of severity values to send to a Syslog server.
- Severity to Email:** None (dropdown) Select the range of severity values to send via email to the recipient list.
- Severity to Trap:** None (dropdown) Select the range of severity values to send to an SNMP system.

At the bottom of the window are "Apply" and "Cancel" buttons. A vertical number "67174" is visible on the right side of the window frame.

Save Log on Wrap

Check the **Save Log on Wrap** check box to automatically save the event log when it is full. (The box is unchecked by default.) The Model 3015–3080 event log holds 2048 events, the Model 3005 holds 256 events. When the log is full, newer events overwrite older events; that is, entry 2049 overwrites entry 1, etc.

If you select automatic save, the system saves the log file to a file in Flash memory with the filename LOGNNNNN.TXT, where NNNNN is an increasing sequence number that starts with 00001 and restarts after 99999. The sequence numbers continue through reboots. For example, if four log files have already been saved, the next one saved after a reboot is LOG00005.TXT.

If Flash memory has less than 2.56 MB of free space, the system deletes the oldest log file(s) to make room for the newest saved log file. It also generates an event that notes the deletion. If there are no old log files to delete, the save function fails, and the system generates an event that notes the failure.

Each saved log file requires about 334 KB. To conserve space in Flash memory, we recommend that you periodically remove the saved log files. Keeping more than 10 to 12 files wastes space. The Administration | File Management | Files screen shows total, used, and free space in Flash memory.

**Note**

The VPN Concentrator automatically saves the log file if it crashes, and when it is rebooted, regardless of this Save Log on Wrap setting. This log file is named SAVELOG.TXT, and it overwrites any existing file with that name. The SAVELOG.TXT file is useful for debugging.

You can manage saved log files with options on this screen and on the Administration | File Management screens.

Save Log Format

Click the **Save Log Format** drop-down menu button to specify the format of the saved log files.

- **Multiline** = Entries are ASCII text and appear on multiple 80-character lines (default). Choose this format for easiest reading and printing.
- **Comma Delimited** = Each entry is a single record with fields separated by commas. Choose this format for subsequent processing by an application program such as a spreadsheet or accounting system.
- **Tab Delimited** = Each entry is a single record with fields separated by tab characters. Choose this format for subsequent processing by an application program such as a spreadsheet or accounting system.

Refer to the section on Monitoring | Filterable Event Log in *VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring* for details on event log fields.

FTP Saved Log on Wrap

Check the **FTP Saved Log on Wrap** check box to automatically send the saved event log file, when it wraps, via FTP to a remote computer. (The box is unchecked by default.) This option *copies* the log file but does not delete it from the VPN Concentrator. If you check this box, you must also configure FTP destination system parameters on the Configuration | System | Events | FTP Backup screen.

Email Source Address

Enter the address to put in the From: field of an e-mailed event message. Enter up to 48 alphanumeric characters with no spaces, for example: cisco@cisco.com. You should configure this field if you configure any Severity to Email events; if you leave it blank, the From: field has the same address as the To: field (the recipient's e-mail address).

Syslog Format

Click the **Syslog Format** drop-down menu button and choose the format for all events sent to UNIX syslog servers. Choices are:

- **Original** = Original VPN Concentrator event format with information on one line. Each entry in the event log consists of the following fields:

Sequence Date Time SEV=Severity Class/Number RPT=RepeatCount String

- *Sequence*: The sequence number of the event.
- *Date*: The date the event occurred. The date is in the following format: MM/DD/YYYY.
- *Time*: The time the event occurred. The time is in the following format: hh:mm:ss.ttt.
- *Severity*: The severity of the event (1-13). To see how this original severity level maps to Cisco IOS severity levels, see [Table 10-3](#).
- *Class/Number*: The event class and event number. For a list of event classes, see the “Events” chapter.
- *RepeatCount*: The number of times this particular event has occurred since the VPN Concentrator was last booted.
- *String*: The description of the event. The string sometimes includes the IP address of the user whose session generated the event.

For example:

```
3 12/06/1999 14:37:06.680 SEV=4 HTTP/47 RPT=17 10.10.1.35 New administrator login:
admin.
```

- **Cisco IOS Compatible** = Event format that is compatible with Cisco syslog management applications. Each entry in the event log is one line consisting of the following fields:

Sequence: Date Time TimeZone TimeZoneOffset %Class-Severity-Number: RPT=RepeatCount: String

- *Sequence*: The sequence number of the event.
- *Date*: The date the event occurred. The date is in the following format: YYYY MMM DD.
- *Time*: The time the event occurred. The time is in the following format: hh:mm:ss.ttt.
- *TimeZone*: The time zone in which the event occurred.
- *TimeZoneOffset*: The offset of the time zone from GMT.
- *Class*: The event class. For a list of event classes, see [Table 10-1](#).
- *Severity*: The Cisco IOS severity of the event (0-7). [Table 10-3](#) shows the mapping between Cisco IOS format severity levels and Original format severity levels.
- *Number*: The event number.
- *RepeatCount*: The number of times this particular event has occurred since the VPN Concentrator was last booted.
- *String*: The description of the event. The string sometimes includes the IP address of the user whose session generated the event.

For example:

```
3 1999 Dec 06 14:37:06.680 EDT -4:00 %HTTP-5-47:RPT=17 10.10.1.35: New administrator
login: admin.
```

The Original severities and the Cisco IOS severities differ. Original severities number from 1-13. (For the meaning of each Original severity, see [Table 10-2 on page 10-4](#).) Cisco IOS severities number from 0-7. [Table 10-3](#) shows the meaning of Cisco IOS severities and how they map to Original severities.

Table 10-3 Cisco IOS Severities

Cisco IOS Severity	Meaning	Original Severity
0	Emergencies	1
1	Alerts	Not used
2	Critical	2
3	Errors	Not used
4	Warning	3
5	Notification	4
6	Informational	5, 6
7	Debugging	7-13

Severity to Log

Click the **Severity to Log** drop-down menu button and choose the range of event severity levels to enter in the event log by default. The choices are: None, 1, 1-2, 1-3, ..., 1-13. The default is 1-5. Using the default means that all events of severity level 1 through severity level 5 are entered in the event log.



Note

Avoid configuring Severity to Log with ranges greater than 1-5 for all events. Configuring the severity ranges above 5 for all events greatly impacts system performance. Instead, configure only individual event classes with higher severities.

Severity to Console

Click the **Severity to Console** drop-down menu button and choose the range of event severity levels to display on the console by default. The choices are: None, 1, 1-2, 1-3, ..., 1-13. The default is 1-3. Using the default means that all events of severity level 1 through severity level 3 are displayed on the console.



Note

Avoid configuring Severity to Console with ranges greater than 1-5 for all events. Configuring the severity ranges above 5 for all events greatly impacts system performance. Instead, configure only individual event classes with higher severities.

Severity to Syslog

Click the **Severity to Syslog** drop-down menu button and choose the range of event severity levels to send to a UNIX syslog server by default. The choices are: None, 1, 1-2, 1-3, ..., 1-6. The default is None. Using the default means that no events are sent to a syslog server.

If you select any severity levels to send, you must also configure the syslog server(s) on the Configuration | System | Events | Syslog Servers screens.

**Note**

Avoid configuring Severity to Syslog with ranges greater than 1-5 for all events. Configuring the severity ranges above 5 for all events greatly impacts system performance. Instead, configure only individual event classes with higher severities. Setting a high range can disable your ability to manage the VPN Concentrator using the browser management interface. The more calls coming into a VPN Concentrator, the greater the likelihood that high severities for Severity to Syslog could cause a problem. If Severity to Syslog has such a high range that you cannot interact with the VPN Concentrator using the browser interface, use the console interface to access the Severity to Syslog parameter and set the level to a lower range, for example: 1-5. This action enables you to regain control through the browser management interface.

Severity to Email

Click the **Severity to Email** drop-down menu button and choose the range of event severity levels to e-mail to recipients by default. The choices are: None, 1, 1-2, 1-3. The default is None. Using the default means that no events are sent via e-mail.

If you select any severity levels to e-mail, you must also configure an SMTP server on the Configuration | System | Events | SMTP Servers screens, and you must configure e-mail recipients on the Configuration | System | Events | Email Recipients screens. You should also configure the preceding Email Source Address.

Severity to Trap

Click the **Severity to Trap** drop-down menu button and choose the range of event severity levels to send to an SNMP network management system by default. Event messages sent to SNMP systems are called “traps.” The choices are: None, 1, 1-2, 1-3. The default is None: no events are sent as SNMP traps.

If you select any severity levels to send, you must also configure SNMP destination system parameters on the Configuration | System | Events | Trap Destinations screens.

The VPN Concentrator can send the standard, or “well-known,” SNMP traps listed in [Table 10-4](#). To have an SNMP NMS receive them, you must configure the events as in the table, and configure a trap destination.

Table 10-4 Configuring “Well-Known” SNMP Traps

To Send this “Well-Known” SNMP Trap	Configure Either General Event Handling or this Event Class	With this Severity to Trap
coldStart	EVENT	1 or higher
linkDown	IP	1-3 or higher
linkUp	IP	1-3 or higher
authFailure (This trap is SNMP authentication failure, not tunnel authentication failure.)	SNMP	1-3 or higher

Apply / Cancel

To include your settings for default event handling in the active configuration, click **Apply**. The Manager returns to the Configuration | System | Events screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Events screen.

Configuration | System | Events | FTP Backup

This screen lets you configure parameters for using FTP to automatically back up saved event log files on a remote computer. If you enable FTP Saved Log on Wrap on the Configuration | System | Events | General screen, you must configure the FTP parameters on this screen.

The VPN Concentrator acts as an FTP client when executing this function.



Note

Another way to back up saved event log files on a remote computer is to enable an external Syslog server.

Figure 10-3 Configuration | System | Events | FTP Backup Screen

Configuration | System | Events | FTP Backup

This screen lets you configure FTP backup options for the log.

FTP Server Enter the IP address or hostname of the destination FTP server.

FTP Directory Enter the directory pathname for files on the FTP server.

FTP Username Enter the username to log on to the FTP server.

FTP Password Enter the password to log on to the FTP server.

Verify Re-enter the password to verify it.

Apply Cancel

67173

FTP Server

Enter the IP address or host name of the destination computer to receive copies of saved event log files via FTP. (If you have configured a DNS server, you can enter a host name; otherwise enter an IP address.)

FTP Directory

Enter the complete directory path name on the destination computer to receive copies of saved event log files. For example, c:\vpn\logfiles.

FTP Username

Enter the username for FTP login on the destination computer.

FTP Password

Enter the password to use with the FTP username. The field displays only asterisks.

Verify

Re-enter the FTP password to verify it. The field displays only asterisks.

Apply / Cancel

To include your FTP backup system settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | Events screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

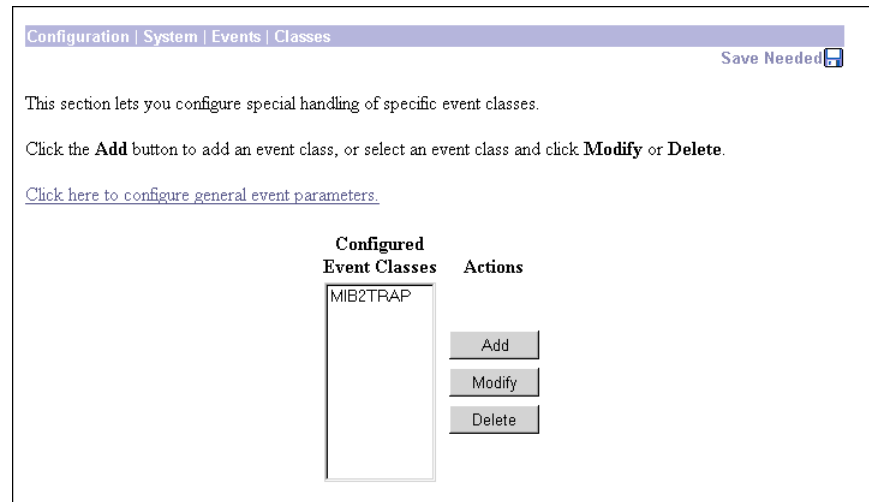
To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Events screen.

Configuration | System | Events | Classes

This section of the Manager lets you add, configure, modify, and delete specific event classes for special handling. You can thus override the general, or default, handling of event classes. For example, you might want to send e-mail for HARDWAREMON events of severity 1 and 2, whereas default event handling does not send any e-mail.

Event classes denote the source of an event and refer to a specific hardware or software subsystem within the VPN Concentrator. [Table 10-1](#) describes the event classes.

Figure 10-4 Configuration | System | Events | Classes Screen



To configure default event handling, click the highlighted link that says “*Click here to configure general event parameters.*”

Configured Event Classes

The Configured Event Classes list shows the event classes that have been configured for special handling. The initial default entry is MIB2TRAP, which are SNMP MIB-II events, or “traps,” that you might want to monitor with an SNMP network management system. Other configured event classes are listed in order by class number and name. If no classes have been configured for special handling, the list shows --Empty--.

Add / Modify / Delete

To configure and add a new event class for special handling, click **Add**. See Configuration | System | Events | Classes | Add.

To modify an event class that has been configured for special handling, select the event class from the list and click **Modify**. See Configuration | System | Events | Classes | Modify.

To remove an event class that has been configured for special handling, select the event class from the list and click **Delete**.

**Note**

There is no confirmation or undo.

The Manager refreshes the screen and shows the remaining entries in the list.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | Events | Classes | Add or Modify

These screens let you:

- Add and configure the special handling of a specific event class.
- Modify the special handling of a specific event class.

Figure 10-5 Configuration | System | Events | Classes | Add or Modify Screen

Configuration | System | Events | Classes | Add

This screen lets you add and configure an event class for special handling.

Class Name Select the event class to configure.

Enable Check to enable special handling of this class.

Severity to Log Select the range of severity values to enter in the log.

Severity to Console Select the range of severity values to display on the console.

Severity to Syslog Select the range of severity values to send to a Syslog server.

Severity to Email Select the range of severity values to send via email to the recipient list.

Severity to Trap Select the range of severity values to send to an SNMP system.

67161

Class Name

Add screen:

- Click the drop-down menu button and choose the event class you want to add and configure for special handling. (Please note that Select Class is an instruction reminder, not a class. [Table 10-1](#) describes the event classes.

Modify screen:

- The field shows the configured event class you are modifying. You cannot change this field.

All subsequent parameters on this screen apply to this event class only.

Enable

Check the **Enable** check box to enable the special handling of this event class. (The box is checked by default.)

Unchecking this box lets you set up the parameters for the event class but activate it later, or temporarily disable special handling without deleting the entry. The Configured Event Classes list on the Configuration | System | Events | Classes screen indicates disabled event classes. Disabled event classes are handled in accordance with the default parameters for all event classes.

Severity to Log

Click the **Severity to Log** drop-down menu button and choose the range of event severity levels to enter in the event log. Choices are: None, 1, 1-2, 1-3, ..., 1-13. The default is 1-5. Using the default means that events of severity level 1 through severity level 5 are entered in the event log.

Severity to Console

Click the **Severity to Console** drop-down menu button and choose the range of event severity levels to display on the console. The choices are: None, 1, 1-2, 1-3, ..., 1-13. The default is 1-3. Using the default means that events of severity level 1 through severity level 3 are displayed on the console.

Severity to Syslog

Click the **Severity to Syslog** drop-down menu button and choose the range of event severity levels to send to a UNIX syslog server. The choices are: None, 1, 1-2, 1-3, ..., 1-13. The default is None. Using the default means that no events are sent to a syslog server.

**Note**

Sending events to a syslog server generates IP packets, which can generate new events if this setting is above level 9. We strongly recommend that you keep this setting at or below level 6. Avoid setting this parameter above level 9.

If you select any severity levels to send, you must also configure the syslog server(s) on the Configuration | System | Events | Syslog Servers screens, and you should configure the Syslog Format on the Configuration | System | Events | General screen.

Severity to Email

Click the **Severity to Email** drop-down menu button and choose the range of event severity levels to send to recipients via e-mail. The choices are: None, 1, 1-2, 1-3. The default is None: no events are sent via e-mail.

If you select any severity levels to e-mail, you must also configure an SMTP server on the Configuration | System | Events | SMTP Servers screen, and you must configure e-mail recipients on the Configuration | System | Events | Email Recipients screens. You should also configure the Email Source Address on the Configuration | System | Events | General screen.

Severity to Trap

Click the **Severity to Trap** drop-down menu button and choose the range of event severity levels to send to an SNMP network management system. Event messages sent to SNMP systems are called “traps.” The choices are: None, 1, 1-2, 1-3, 1-4, 1-5. The default is None. Using the default means that no events are sent as SNMP traps.

If you select any severity levels to send, you must also configure SNMP destination system parameters on the Configuration | System | Events | Trap Destinations screens.

To configure “well-known” SNMP traps, see [Table 10-4](#) under Severity to Trap for Configuration | System | Events | General.

Add or Apply / Cancel

To add this event class to the list of those with special handling, click **Add**. Or to apply your changes to this configured event class, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | System | Events | Classes screen. Any new event class appears in the Configured Event Classes list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Events | Classes screen.

Configuration | System | Events | Trap Destinations

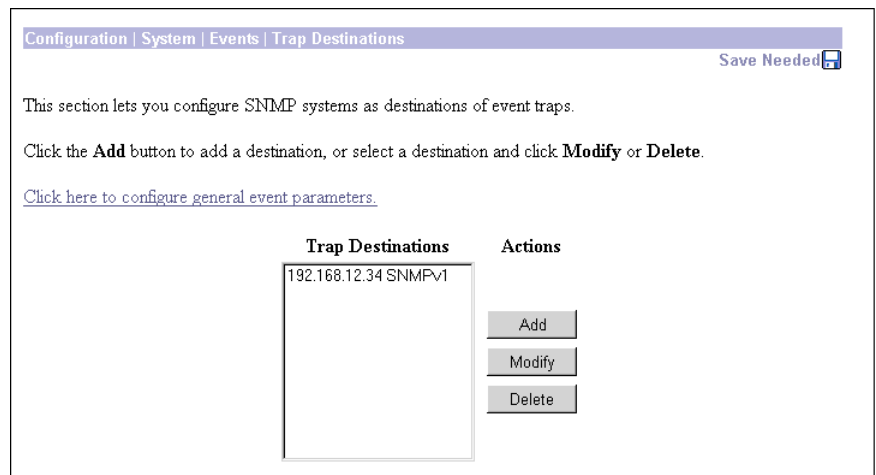
This section of the Manager lets you configure SNMP network management systems as destinations of event traps. Event messages sent to SNMP systems are called “traps.” If you configure any event handling—default or special—with values in Severity to Trap fields, you must configure trap destinations in this section.

To configure default event handling, click the highlighted link that says “*Click here to configure general event parameters.*” To configure special event handling, see the Configuration | System | Events | Classes screens.

To configure well-known SNMP traps, see [Table 10-4](#).

To have an SNMP-based network management system (NMS) receive any events, you must also configure the NMS to see the VPN Concentrator as a managed device or agent in the NMS domain.

Figure 10-6 Configuration | System | Events | Trap Destinations Screen



Trap Destinations

The Trap Destinations list shows the SNMP network management systems that have been configured as destinations for event trap messages, and the SNMP protocol version associated with each destination. If no trap destinations have been configured, the list shows --Empty--.

Add / Modify / Delete

To configure a new SNMP trap destination, click **Add**. See Configuration | System | Events | Trap Destinations | Add.

To modify an SNMP trap destination that has been configured, select the destination from the list and click **Modify**. See Configuration | System | Events | Trap Destinations | Modify.

To remove an SNMP trap destination that has been configured, select the destination from the list and click **Delete**.



Note

There is no confirmation or undo.

The Manager refreshes the screen and shows the remaining entries in the list.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | Events | Trap Destinations | Add or Modify

These screens let you:

- Add an SNMP destination system for event trap messages.
- Modify a configured SNMP destination system for event trap messages.

Figure 10-7 Configuration | System | Events | Trap Destinations | Add or Modify Screen

Configuration | System | Events | Trap Destinations | Add

Add a trap destination.

Destination Enter the IP address or hostname of the trap destination.

SNMP Version Select the SNMP version of the trap to send to this destination.

Community Enter the community string to use in the trap. Default is "public".

Port Enter the destination port for the trap.

67165

Destination

Enter the IP address or host name of the SNMP network management system that is a destination for event trap messages. (If you have configured a DNS server, you can enter a host name; otherwise enter an IP address.)

SNMP Version

Click the **SNMP Version** drop-down menu button and choose the SNMP protocol version to use when formatting traps to this destination. Choices are SNMPv1 (version 1; the default) and SNMPv2 (version 2).

Community

Enter the community string to use in identifying traps from the VPN Concentrator to this destination. The community string is like a password: it validates messages between the VPN Concentrator and this NMS destination. If you leave this field blank, the default community string is public.

Port

Enter the UDP port number by which you access the destination SNMP server. Use a decimal number from 0 to 65535. The default value is 162, which is the well-known port number for SNMP traps.

Add or Apply / Cancel

To add this system to the list of SNMP trap destinations, click **Add**. Or to apply your changes to this trap destination, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | System | Events | Trap Destinations screen. Any new destination system appears in the Trap Destinations list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

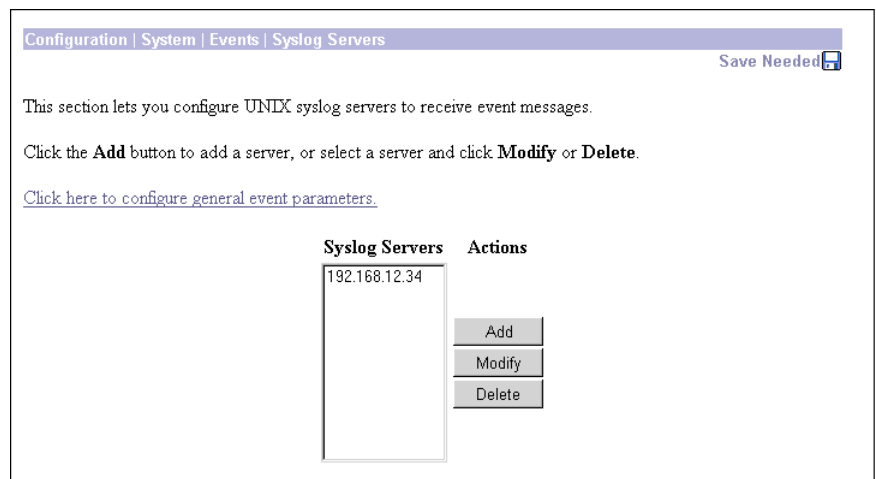
To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Events | Trap Destinations screen, and the Trap Destinations list is unchanged.

Configuration | System | Events | Syslog Servers

This section of the Manager lets you configure UNIX syslog servers as recipients of event messages. Syslog is a UNIX daemon, or background process, that records events. The VPN Concentrator can send event messages in two syslog formats to configured syslog systems. If you configure any event handling—default or special—with values in Severity to Syslog fields, you must configure syslog servers in this section.

To configure default event handling and syslog formats, click the highlighted link that says “Click here to configure general event parameters.” To configure special event handling, see the Configuration | System | Events | Classes screens.

Figure 10-8 Configuration | System | Events | Syslog Servers Screen



Syslog Servers

The Syslog Servers list shows the UNIX syslog servers that have been configured as recipients of event messages. You can configure a maximum of five syslog servers. If no syslog servers have been configured, the list shows --Empty--.

Add / Modify / Delete

To configure a new syslog server, click **Add**. See Configuration | System | Events | Syslog Servers | Add.

To modify a syslog server that has been configured, select the server from the list and click **Modify**. See Configuration | System | Events | Syslog Servers | Modify.

To remove a syslog server that has been configured, select the server from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the list.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | Events | Syslog Servers | Add or Modify

These screens let you:

- Add a UNIX syslog server as a recipient of event messages. You can configure a maximum of five syslog servers.
- Modify a configured UNIX syslog server that is a recipient of event messages.

Figure 10-9 Configuration | System | Events | Syslog Servers | Add or Modify Screen

Configuration | System | Events | Syslog Servers | Add

Add a syslog server.

Syslog Server Enter the IP address or hostname of the syslog server.

Port Enter the port used by the syslog server.

Facility Select the syslog facility tag for events sent to this server.

67164

Syslog Server

Enter the IP address or host name of the UNIX syslog server to receive event messages. (If you have configured a DNS server, you can enter a host name; otherwise, enter an IP address.)

Port

Enter the UDP port number by which you access the syslog server. Use a decimal number from 0 to 65535. The default value is 514, which is the well-known port number.

Facility

Click the **Facility** drop-down menu button and choose the syslog facility tag for events sent to this server. The facility tag lets the syslog server sort messages into different files or destinations. The choices are:

- User = Random user-process messages.
- Mail = Mail system.
- Daemon = System daemons.
- Auth = Security or authorization messages.
- Syslog = Internal syslogd-generated messages.
- LPR = Line printer subsystem.
- News = Network news subsystem.
- UUCP = UUCP (UNIX-to-UNIX Copy Program) subsystem.
- Reserved (9) through Reserved (14) = Outside the Local range, with no name or assignment yet, but usable.
- CRON = Clock daemon.
- Local 0 through Local 7 (default) = User defined.

Add or Apply / Cancel

To add this server to the list of syslog servers, click **Add**. Or to apply your changes to this syslog server, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | System | Events | Syslog Servers screen. Any new server appears in the Syslog Servers list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | Events | Syslog Servers screen, and the Syslog Servers list is unchanged.

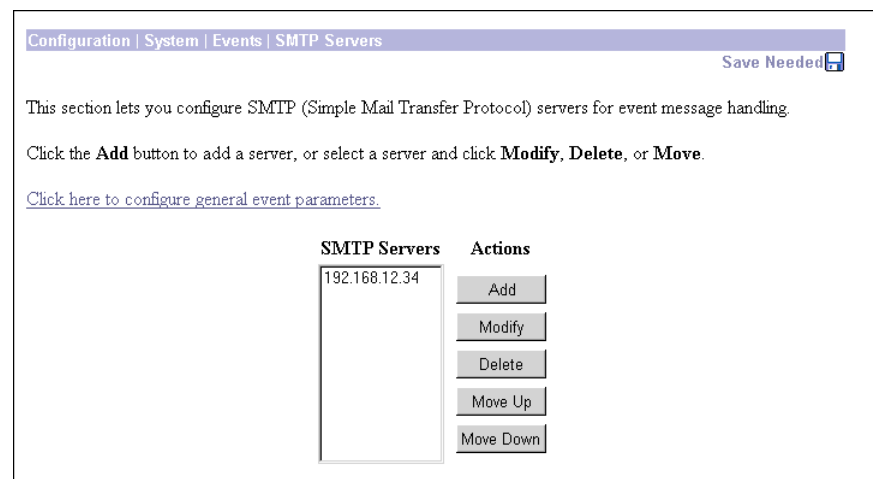
Configuration | System | Events | SMTP Servers

This section of the Manager lets you configure SMTP servers that you use to e-mail event messages to e-mail recipients. If you configure any event handling—default or special—with values in Severity to E-mail fields, you must identify at least one SMTP server to handle the outgoing e-mail, and you must name at least one e-mail recipient to receive the event messages. You can configure two SMTP servers: one primary and one backup in case the primary is unavailable.

To configure e-mail recipients, see the Configuration | System | Events | Email Recipients screen.

To configure default event handling, click the highlighted link that says “*Click here to configure general event parameters.*” To configure special event handling, see the Configuration | System | Events | Classes screens.

Figure 10-10 Configuration | System | Events | SMTP Servers Screen



SMTP Servers

The SMTP Servers list shows the configured SMTP servers in the order in which the system accesses them. You can configure two prioritized SMTP servers so that you have a backup server in case the primary server is offline, congested, etc. If no SMTP servers have been configured, the list shows --Empty--.

Add / Modify / Delete / Move

To configure a new SMTP server, click **Add**. See Configuration | System | Events | SMTP Servers | Add.

To modify a configured SMTP server, select the server from the list and click **Modify**. See Configuration | System | Events | SMTP Servers | Modify.

To remove a configured SMTP server, select the server from the list and click **Delete**.

**Note**

There is no confirmation or undo.

The Manager refreshes the screen and shows the remaining entries in the SMTP Servers list.

To change the order in which the system accesses configured SMTP servers, select the server from the list and click **Move [Up Arrow]** or **Move [Down Arrow]**. The Manager refreshes the screen and shows the reordered SMTP Servers list.

Reminder:

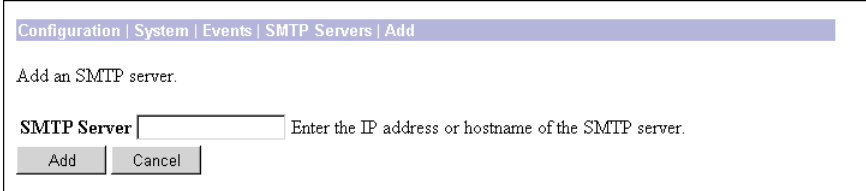
The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | Events | SMTP Servers | Add or Modify

These screens let you:

- Add an SMTP server to the list of configured SMTP servers. You can configure two SMTP servers: a primary and a backup.
- Modify the IP address or host name of a configured SMTP server.

Figure 10-11 Configuration | System | Events | SMTP Servers | Add or Modify Screen



Configuration | System | Events | SMTP Servers | Add

Add an SMTP server.

SMTP Server Enter the IP address or hostname of the SMTP server.

Add Cancel

67163

SMTP Server

Enter the IP address or host name of the SMTP server. (If you have configured a DNS server, you can enter a host name; otherwise, enter an IP address.)

Add or Apply / Cancel

To add this server to the list of SMTP servers, click **Add**. Or to apply your changes to this SMTP server, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | System | Events | SMTP Servers screen. Any new server appears in the SMTP Servers list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entry, click **Cancel**. The Manager returns to the Configuration | System | Events | SMTP Servers screen, and the SMTP Servers list is unchanged.

Configuration | System | Events | Email Recipients

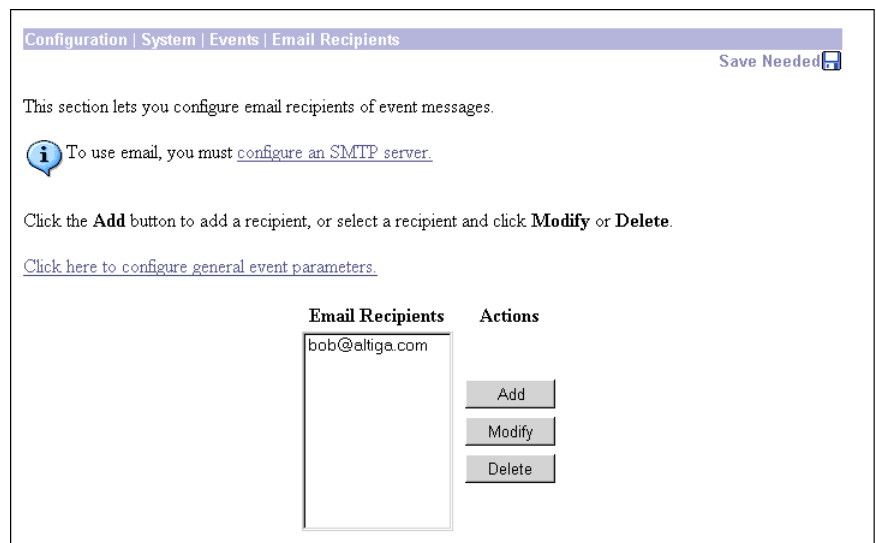
This section of the Manager lets you configure e-mail recipients of event messages. You can configure a maximum of five e-mail recipients, and you can customize the event message severity levels for each recipient.

If you configure any event handling (either default or special) with values in Severity to Email fields, you must name at least one e-mail recipient to receive the event messages, and you must identify at least one SMTP server to handle the outgoing e-mail. You should also configure the Email Source Address on the Configuration | System | Events | General screen.

To configure SMTP servers, see the Configuration | System | Events | SMTP Servers screen, or click the highlighted link that says “*configure an SMTP server.*”

To configure default event handling, click the highlighted link that says “*Click here to configure general event parameters.*” To configure special event handling, see the Configuration | System | Events | Classes screens.

Figure 10-12 Configuration | System | Events | Email Recipients Screen



Email Recipients

The Email Recipients list shows configured event message e-mail recipients in the order they were configured. You can configure a maximum of five e-mail recipients. If no e-mail recipients have been configured, the list shows --Empty--.

Add / Modify / Delete

To configure a new e-mail recipient, click **Add**. See Configuration | System | Events | Email Recipients | Add.

To modify an e-mail recipient who has been configured, select the recipient from the list and click **Modify**. See Configuration | System | Events | Email Recipients | Modify.

To remove an e-mail recipient who has been configured, select the recipient from the list and click **Delete**.



Note

There is no confirmation or undo.

The Manager refreshes the screen and shows the remaining recipients in the Email Recipients list.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | Events | Email Recipients | Add or Modify

These screens let you:

- Add and configure an event message e-mail recipient. You can configure a maximum of five e-mail recipients.
- Modify the parameters for a configured e-mail recipient.

Figure 10-13 Configuration | System | Events | Email Recipients | Add or Modify Screen

Email Address

Enter the recipient's complete e-mail address, for example: cisco@cisco.com.

Max Severity

Click the **Max Severity** drop-down menu button and choose the range of event severity levels to send to this recipient via e-mail. The choices are: None, 1, 1-2, 1-3. The default value is 1-3: configured events of severity level 1 through severity level 3 are sent to this recipient.

The event levels e-mailed to this recipient are the *lesser of* the Severity to Email setting for a customized event class, or this Max Severity setting. If an event class has not been customized, the events e-mailed are the *lesser of* this setting or the default Severity to Email setting. For example, if you configure IPSEC events with severity levels 1-3 to e-mail, all other events with no severity to e-mail, and cisco@cisco.com to receive e-mail events of severity levels 1-2, cisco will receive only IPSEC events of severity levels 1-2.

Add or Apply / Cancel

To add this recipient to the list of e-mail recipients, click **Add**. Or to apply your changes to this e-mail recipient, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | System | Events | Email Recipients screen. Any new recipient appears at the bottom of the Email Recipients list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window. To discard your entry, click **Cancel**. The Manager returns to the Configuration | System | Events | Email Recipients screen, and the Email Recipients list is unchanged.



General

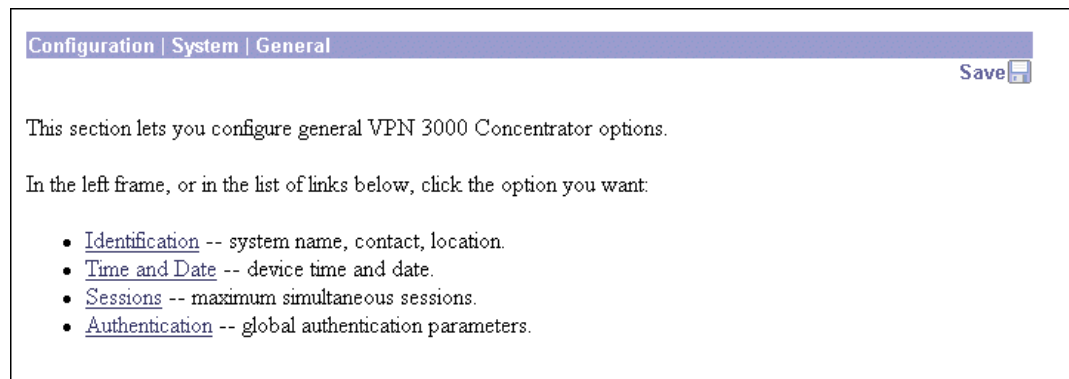
General configuration parameters include VPN 3000 Concentrator environment items: system identification, time, and date.

Configuration | System | General

This section of the Manager lets you configure general VPN Concentrator parameters.

- Identification: System name, contact person, system location.
- Time and Date: System time and date.
- Sessions: The maximum number of sessions.
- Authentication: General authentication parameters.

Figure 11-1 Configuration | System | General Screen



Configuration | System | General | Identification

This screen lets you configure system identification parameters that are stored in the standard MIB-II system object. Network management systems using SNMP can retrieve this object and identify the system. Configuring this information is optional.

Figure 11-2 Configuration | System | General | Identification Screen

System Name

Enter a system name that uniquely identifies this VPN Concentrator on your network, for example: VPN01. The maximum name length is 255 characters.

Contact

Enter the name of the contact person who is responsible for this VPN Concentrator. The maximum name length is 255 characters.

Location

Enter the location of this VPN Concentrator. The maximum length is 255 characters.

Apply / Cancel

To apply your system identification settings and include them in the active configuration, click **Apply**. The Manager returns to the Configuration | System | General screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | General screen.

Configuration | System | General | Time and Date

This screen lets you set the time and date on the VPN Concentrator. Setting the correct time is very important so that logging and accounting information is accurate.

Figure 11-3 Configuration | System | General | Time and Date Screen

Configuration | System | General | Time and Date

Configure the time and date.

i Setting the time on your VPN 3000 Concentrator is very important, so that logging and accounting information is correct.

The current time on the device is Monday, 01 October 2001 16:23:44.

New Time 16 : 42 : 42 | October | 1 | / 2001 | ((GMT+05:00) Karachi)

Enable DST Support

Apply Cancel

68234

Current Time

The screen shows the current date and time on the VPN Concentrator at the time the screen displays. You can refresh this by redisplaying the screen.

New Time

The values in the New Time fields are the time and date on the *browser PC* at the time the screen displays. Any entries you make apply to the *VPN Concentrator*, however.

In the appropriate fields, make any changes. The fields are, in order: Hour : Minute : Second Month / Day / Year Time Zone. Click the drop-down menu buttons to select Month and Time Zone.

The time is military time; that is, it is based on a twenty-four hour clock. (For example, 1:00 PM is 13:00:00.)

The time zone selections are offset in hours relative to GMT (Greenwich Mean Time), which is the basis for Internet time synchronization.

Enter the Year as a four-digit number.

Enable DST Support

To enable DST support, check the **Enable DST Support** check box. During DST (Daylight-Saving Time), clocks are set one hour ahead of standard time. Enabling DST support means that the VPN Concentrator automatically adjusts the time zone for DST or standard time. *If your system is in a time zone that uses DST, you must enable DST support.*

Apply / Cancel

To apply your time and date settings, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | General screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | General screen.

Configuration | System | General | Sessions

This screen lets you limit the number of simultaneous active sessions to fewer sessions than the VPN Concentrator could potentially support. The maximum number of sessions supported is determined by the hardware and is model-dependent.

Table 11-1 Maximum Sessions for Each VPN Concentrator Model

VPN Concentrator Model	Maximum Number of Sessions
3005	100
3015	100
3030	1500
3060	5000
3080	10,000

Figure 11-4 Configuration | System | General | Sessions Screen (Model 3030)

Maximum Active Connections

The maximum number of concurrently active sessions permitted on this VPN Concentrator. Enter a value within the range indicated.

A value of zero (0) in this field means that there is no artificial limit below the maximum number of sessions supported by the hardware. In other words, for a VPN Concentrator 3030, a 0 in this field means that the maximum number of sessions is 1500.

Apply/Cancel

To apply your session settings, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | General screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | General screen.

Configuration | System | General | Global Authentication Parameters

By default, the VPN Concentrator authenticates both software clients and VPN 3002 hardware clients on the basis of their username. For clients to connect, you enter a string of characters (in a username field) as their identification. The VPN Concentrator considers the entire string to be a username and validates users on the basis of the entire string.

The group lookup feature allows clients to be authenticated on the basis of a group in addition to their username. If this feature is enabled, the VPN Concentrator checks the identification string to see if it contains the configured group delimiter. If the string contains the configured group delimiter, the VPN Concentrator interprets it as: *UsernameDelimiterGroupname*. It interprets the characters to the left of the delimiter as the user name and the characters to the right of the delimiter as the group name. It then authenticates the user on the basis of the group and applies the parameters of the specified group to the user. For example, if the user enters the string “JaneDoe#Cisco”, the VPN Concentrator interprets JaneDoe as the user, # as the delimiter, and Cisco as the group. It authenticates the user “JaneDoe” on the basis of the “Cisco” group and applies the Cisco group parameters.

If the string does not contain a group delimiter, the VPN Concentrator considers the entire string to be the user name. It validates users on the basis of the user name alone, and applies the parameters of the tunnel group to the user.

Figure 11-5 Configuration | System | General | Global Authentication Parameters Screen

Enable Group Lookup

Check the **Enable Group Lookup** check box to enable user authentication on the basis of both user name and group name. Uncheck the check box to disable group lookup.

Group Delimiter

If you configured Enable Group Lookup, click the **Group Delimiter** drop-down menu and choose one of the following characters to separate the user name from the group name in the authentication string: @, #, or !. The default delimiter is: @.



Client Update

Updating VPN Client software in an environment with a large number of devices in different locations can be a formidable task. For this reason, the VPN 3000 Concentrator includes a client update feature that simplifies the software update process. This feature works differently for VPN software clients and VPN 3002 Hardware Clients.

VPN Software Clients

The client update feature lets administrators at a central location automatically notify VPN Client users when it is time to update the VPN Client software.

When you enable client update, upon connection the central-site VPN Concentrator sends an IKE packet that contains an encrypted message that notifies VPN Client users about acceptable versions of executable system software. The message includes a location that contains the new version of software for the VPN Client to download. The administrator for that VPN Client can then retrieve the new software version, and update the VPN Client software.

You configure parameters that specify the acceptable versions of software and their locations. Updates are supported per group. This means that all members of a group can obtain the same updates from the same server at approximately the same time.

VPN 3002 Hardware Clients

The client update feature lets administrators at a central location automatically update software/firmware for VPN 3002 Hardware Clients deployed in diverse locations.

When you enable client update, upon connection the central-site VPN Concentrator sends an IKE packet that contains an encrypted message that notifies VPN 3002 hardware clients about acceptable versions of executable system software and their locations. If the VPN 3002 is not running an acceptable version, its software is automatically updated via TFTP.

To use client update, you need to have a TFTP server that can handle the volume and frequency of updates that your network requires. We recommend that you locate this server inside your network. The client update facility sends notify messages to VPN 3002s in batches of 10 at 5-minute intervals.

You configure parameters that specify the acceptable versions of software and their locations. Updates are supported per group. This means that all members of a group can obtain the same updates from the same server at approximately the same time.

The VPN 3002 logs event messages at the start of the update. When the update completes, the Hardware Client reboots automatically.

**Note**

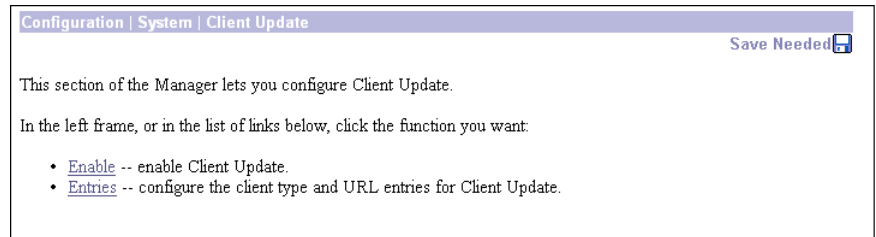
The VPN 3002 stores image files in two locations: the active location, which stores the image currently running on the system; and the backup location. Updating the image overwrites the stored image file in the backup location and makes it the active location for the next reboot. The client update process includes a test to validate the updated image. In the unlikely event that a client update is unsuccessful, the client does not reboot, and the invalid image does not become active. The update facility retries up to twenty times at 3-minute intervals. If an update is unsuccessful, the log files contain information indicating TFTP failures.

Configuration | System | Client Update

This section of the VPN 3000 Concentrator Manager lets you configure the client update feature.

- **Enable:** Enables or disables client update.
- **Entries:** Configures updates by client type, acceptable firmware and software versions, and their locations.

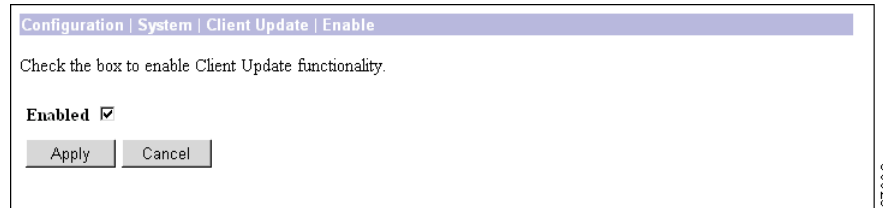
Figure 12-1 Configuration | System | Client Update Screen



Configuration | System | Client Update | Enable

This screen lets you disable or enable client update.

Figure 12-2 Configuration | System | Client Update | Enable Screen



Enable

Uncheck or check the **Enable** check box to disable or enable client update (by default, client update is enabled).

Apply or Cancel

To apply your change to client update, click **Apply**. This action includes your entry in the active configuration. The Manager returns to the Configuration | System | Client Update screen.

Reminder:

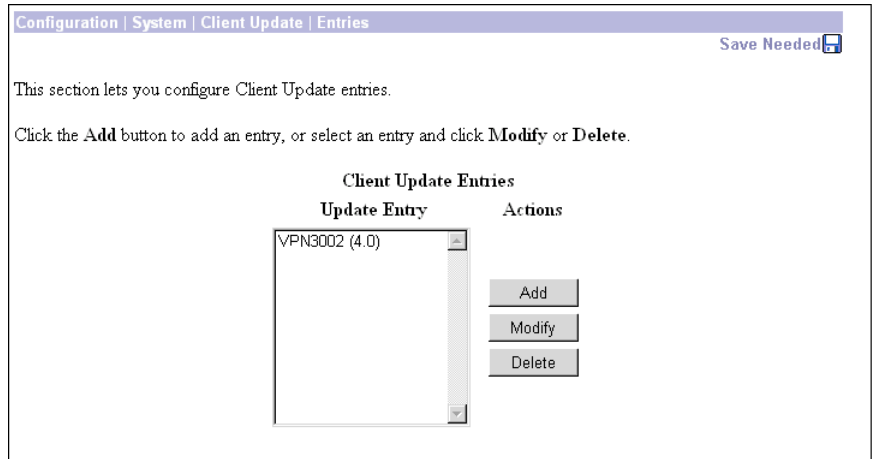
To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | Client Update screen, and the settings are unchanged.

Configuration | System | Client Update | Entries

This screen lets you add, modify, or delete client update entries.

Figure 12-3 Configuration | System | Client Update | Entries Screen



Update Entry

The update entry list shows the configured client update entries. Each entry shows the platform and acceptable software/firmware versions. If no updates have been configured, the list shows --Empty--.

Actions

To configure and add a new client update entry, click **Add**. The Manager opens the Configuration | System | Client Update | Entries | Add screen.

To modify parameters for a client update entry that has been configured, select the entry from the list and click **Modify**. The Manager opens the Configuration | System | Client Update | Modify screen.

To remove a client update entry that has been configured, select the entry from the list and click **Delete**.



Note

There is no confirmation or undo.

The Manager refreshes the screen and shows the remaining entries in the list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | Client Update | Entries | Add or Modify

These screens let you configure and change client update parameters.

Figure 12-4 Configuration | System | Client Update | Entries | Add or Modify Screens

Configuration | System | Client Update | Entries | Add

Add client update information.

Client Type Enter the client type (e.g. *windows* or *vpn3002*) that is to be updated.

URL Enter the URL of the file from which to update. The URL must point to an appropriate file type for the client.

Revisions Enter a comma separated list of valid revisions. The URL above *must* be one of these revisions.

Add Cancel

67016

Client Type

Enter the client type you want to update.

- For the VPN Client: Enter the windows operating systems to notify. The entry must be exact, including case and spacing:
 - **windows** includes *all* Windows-based platforms.
 - **win9x** includes Windows 95, Windows 98, and Windows ME platforms.
 - **winNT** includes Windows NT 4.0, Windows 2000, and Windows XP platforms.



Note

The VPN Concentrator sends a separate notification message for each entry in a Client Update list. Therefore your client update entries must not overlap. For example, the value Windows includes all Windows platforms, and the value WinNT includes Windows NT 4.0, Windows 2000 and Windows XP platforms. So you would not include both the values Windows and WinNT.

- For the VPN 3002 Hardware Client: Your entry must be **vpn3002**, including case and spacing.

URL

Enter the URL for the software/firmware image. This URL must point to a file appropriate for this client.

- For the VPN Client: To activate the Launch button on the VPN Client Notification, the URL must include the protocol HTTP or HTTPS and the server address of the site that contains the update. The format of the URL is: `http(s)://server_address:port/directory/filename`. The server address can be either an IP address or a hostname if you have configured a DNS server. For example:

`http://10.10.99.70/vpnclient-win-3.5.Rel-k9.exe`

The directory is optional. You need the port number only if you use ports other than 80 for http or 443 for https.

- For the VPN 3002 Hardware Client: The format of the URL is `tftp://server_address/directory/filename`. The server address can be either an IP address or a hostname if you have configured a DNS server. For example:

`tftp://10.10.99.70/vpn3002-3.5.Rel-k9.bin`

The directory is optional.

Revisions

Enter a comma-separated list of software or firmware images appropriate for this client. The following caveats apply:

- The revision list must include the software version for this update.
- Your entries must match exactly those on the URL for the VPN Client, or the TFTP server for the VPN 3002.
- The URL above must point to one of the images you enter.

If the client is already running a software version on the list, it does not need a software update. If the client is not running a software version on the list, an update is in order.

- A VPN Client user must download an appropriate software version from the listed URL.
- The VPN 3002 Hardware Client software is automatically updated via TFTP.

Add or Apply / Cancel

To add this client update entry to the list of configured update entries, click **Add**. Or, to apply your changes, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | System | Client Update screen. Any new entry appears at the bottom of the Update Entries list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | Client Update screen, and the Update Entries list is unchanged.



Tip

For more information about VPN Client updates, specifically the VPN Client Launch button, refer to the *VPN Client Administrator Guide*.



Load Balancing Cisco VPN Clients

If you have a remote-client configuration in which you are using two or more VPN Concentrators connected on the same network to handle remote sessions, you can configure these devices to share their session load. This feature is called *load balancing*. Load balancing directs session traffic to the least loaded device, thus distributing the load among all devices. It makes efficient use of system resources and provides increased performance and high availability.



Note

Load balancing is effective only on remote sessions initiated with the Cisco VPN Client (Release 3.0 and later) or the Cisco VPN 3002 Hardware Client (Release 3.5). All other clients, including LAN-to-LAN connections, can connect to a VPN Concentrator on which load balancing is enabled, but they cannot participate in load balancing.



Note

You cannot use load balancing with Virtual Router Redundancy Protocol (VRRP). In a VRRP configuration, the backup device remains idle unless the active VPN Concentrator fails. In a load balancing configuration, there are no idle devices.

To implement load balancing, you group together logically two or more devices on the same private LAN-to-LAN network, private subnet, and public subnet into a *virtual cluster*.

All devices in the virtual cluster carry session loads. One device in the virtual cluster, the *virtual cluster master*, directs incoming calls to the other devices, called *secondary devices*. The virtual cluster master monitors all devices in the cluster, keeps track of how busy each is, and distributes the session load accordingly. The role of virtual cluster master is not tied to a physical device; it can shift among devices. For example, if the current virtual cluster master fails, one of the secondary devices in the cluster takes over that role and immediately becomes the new virtual cluster master.

The virtual cluster appears to outside clients as a single *virtual cluster IP address*. This IP address is not tied to a specific physical device. It belongs to the current virtual cluster master; hence, it is virtual. A VPN Client attempting to establish a connection connects first to this virtual cluster IP address. The virtual cluster master then sends back to the client the public IP address of the least-loaded available host in the cluster. In a second transaction (transparent to the user), the client connects directly to that host. In this way, the virtual cluster master directs traffic evenly and efficiently across resources.



Note

All clients other than the Cisco VPN Client or the Cisco 3002 Hardware Client connect directly to the VPN Concentrator as usual; they do not use the virtual cluster IP address.

If a machine in the cluster fails, the terminated sessions can immediately reconnect to the virtual cluster IP address. The virtual cluster master then directs these connections to another active device in the cluster. Should the virtual cluster master itself fail, a secondary device in the cluster immediately and automatically takes over as the new virtual session master. Even if several devices in the cluster fail, users can continue to connect to the cluster as long as any one device in the cluster is up and available.

Preliminary Steps

Before you can configure load balancing on a VPN Concentrator, you must do the following:

- Configure the private and public interfaces.
- Configure the filters for the private and public interfaces to allow the Virtual Cluster Agent (VCA) load balancing protocol.

Configure Interfaces

In the Configuration | Interfaces window, check to see that the public and private interfaces have been defined and have status UP. If either interface is undefined, you must define it now. For more information on defining interfaces, see the section on Configuration | Interfaces.

Configure Filters

Complete the following steps to configure the filters for the private and public interfaces to allow the VCA load balancing protocol:

-
- Step 1** In the Configuration | Interfaces window, select **Ethernet1 (Private)**. The Configuration | Interfaces | Ethernet1 window appears.
 - Step 2** Select the **General** tab.
 - Step 3** Click the drop-down **Filter** menu button and choose **Private (Default)**.
 - Step 4** Click **Apply**.
 - Step 5** In the Configuration | Interface window, select **Ethernet2 (Public)**. The Configuration | Interfaces | Ethernet2 window appears.
 - Step 6** Select the **General** tab.
 - Step 7** Click the drop-down **Filter** menu button and choose **Public (Default)**.
 - Step 8** Click **Apply**.
 - Step 9** Open the Configuration | Policy Management | Traffic Management | Filters window.
 - Step 10** Select **Private (Default)** from the Filter list.
 - Step 11** Click **Assign Rules to Filter**. The Configuration | Policy Management | Traffic Management | Assign Rules to Filter window appears.
 - Step 12** Make sure that VCA In (forward/in) and VCA Out (forward/out) are in the Current Rules in Filter list. If they are not in this list, add them.
 - Step 13** Click **Done**.
 - Step 14** In the Configuration | Policy Management | Traffic Management | Filters window, select **Public (Default)** from the Filter list.
 - Step 15** Click **Assign Rules to Filter**. The Configuration | Policy Management | Traffic Management | Assign Rules to Filter window appears.
 - Step 16** Make sure that VCA In (forward/in) and VCA Out (forward/out) are in the Current Rules in Filter list. If they are not in this list, add them.
 - Step 17** Click **Done**.
 - Step 18** Click the **Save Needed** icon to save your edits.
-

Configuration | System | Load Balancing

This screen allows you to enable load balancing on the VPN Concentrator.

Enabling load balancing involves two steps:

- Step 1** Configure the cluster: establish a common virtual cluster IP address, UDP port (if necessary), and IPsec shared secret for the cluster. These values are identical for every device in the cluster.
- Step 2** Configure the device: enable load balancing on the device and define device-specific properties. These values vary from device to device.

Reminder:

Before you can enable load balancing on your VPN Concentrator, you must complete the steps outlined in the [Preliminary Steps](#) section.

Figure 13-1 Configuration | System | Load Balancing Screen

Configuration | System | Load Balancing

Configure Load Balancing. All devices in the cluster must share an identical **Cluster Configuration**. **Note: the public and private filters need to have the VCA In and VCA Out filter rules added. These filter rules may need to be modified if the VPN Virtual Cluster UDP Port is modified.**

Cluster Configuration

VPN Virtual Cluster IP Address Enter the cluster's virtual IP address.

VPN Virtual Cluster UDP Port Enter the cluster's UDP port.

Encryption Check to enable IPsec encryption between cluster devices.

IPsec Shared Secret Enter the IPsec Shared secret in the cluster.

Verify Shared Secret Re-enter the IPsec Shared secret in the cluster.

Device Configuration

Load Balancing Enable Check to enable load balancing for this device.

Priority Enter the priority of this device. The range is from 1 to 10.

NAT Assigned IP Address Enter the IP address that this device's IP address is translated to by NAT. Enter 0.0.0.0 if NAT is not being used, or the device is not behind a firewall using NAT.

67036

Cluster Configuration

Establish a virtual cluster by defining a common VPN virtual cluster IP address, UDP port, and shared secret. These values must be identical on every device in the virtual cluster.



Note

All devices in the virtual cluster must be on the same public and private IP subnet.

VPN Virtual Cluster IP Address

Enter the single IP address that represents the entire virtual cluster. Choose an IP address that is within the public subnet address range shared by all the VPN Concentrators in the virtual cluster.

VPN Virtual Cluster UDP Port

If another application is using this port, enter the UDP destination port number you want to use for load balancing.

Encryption

The VPN Concentrators in the virtual cluster communicate via LAN-to-LAN tunnels using IPSec. To ensure that all load-balancing information communicated between the VPN Concentrators is encrypted, check the **Encryption** check box.

IPSec Shared Secret

This option is available only if you have checked the preceding **Encryption** option. Enter the IPSec shared secret for the virtual cluster. The shared secret is a common password that authenticates members of the virtual cluster. IPSec uses the shared secret as a pre-shared key to establish secure tunnels between virtual cluster peers.

Verify Shared Secret

Re-enter the IPSec shared secret.

Device Configuration

Configure the following fields to establish this VPN Concentrator as a member of the virtual cluster.

Load Balancing Enable

Check the **Load Balancing Enable** check box to include this VPN Concentrator in the virtual cluster.

Priority

Enter a priority for this VPN Concentrator within the virtual cluster. The priority is a number from 1 to 10 that indicates the likelihood of this device becoming the virtual cluster master either at start-up or when an existing master fails. The higher you set the priority (for example 10), the more likely this device becomes the virtual cluster master.

If your virtual cluster includes different models of VPN Concentrators, we recommend that you choose the device with the greatest load capacity to be the virtual cluster master. For this reason, priority defaults are hardware dependent. (See [Table 13-1](#).)

Table 13-1 Priority Defaults for VPN Concentrators

VPN Concentrator Model	Priority Default
3005	1
3015	3
3030	5
3060	7
3080	9

If your virtual cluster is made up of identical devices (for example, if all the devices in the virtual cluster are VPN Concentrator 3060s), set the priority of every device to 10. Setting all identical devices to the highest priority shortens the length of time needed to select the virtual cluster master.

Which Device Becomes the Virtual Cluster Master?

If the devices in the virtual cluster are powered up at different times, the first device to be powered up assumes the role of virtual cluster master. Because every virtual cluster requires a master, each device in the virtual cluster checks at power-up to ensure that the cluster has a virtual master. If none exists, that device takes on the role. Devices powered up and added to the cluster later become secondary devices.

If all the devices in the virtual cluster are powered up simultaneously, the device with the highest priority setting becomes the virtual cluster master.

If two or more devices in the virtual cluster are powered up simultaneously and both have the highest priority setting, the one with the lowest IP address becomes the virtual cluster master.

Once the virtual cluster is established and operating, if the VPN Concentrator that holds the role of the virtual cluster master should fail, the secondary device with the highest priority setting takes over. Again in this case, if two or more devices in the virtual cluster both have the highest priority setting, the one with the lowest IP address becomes the virtual cluster master.

NAT Assigned IP Address

If this VPN Concentrator is behind a firewall using NAT, NAT has assigned it a public IP address. Enter the NAT IP address.

If this device is not using NAT, enter 0.0.0.0. The default setting is 0.0.0.0.

Apply/Cancel

To add this VPN concentrator to the specified virtual cluster and thus establish load balancing on this device, click **Apply**. The Manager returns to the Configuration | System screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System screen.



User Management

Groups and users are core concepts in managing the security of VPNs and in configuring the VPN Concentrator. Groups and users have attributes, configured via parameters, that determine their access to and use of the VPN. *Users* are members of *groups*, and groups are members of the *base group*. If you do not assign a user to a particular group, that user is by default a member of the base group. This section of the Manager lets you configure those parameters.

Groups simplify system management. To streamline the configuration task, the VPN Concentrator provides a base group that you configure first. The base-group parameters are those that are most likely to be common across all groups and users. As you configure a group, you can simply specify that it “inherit” parameters from the base group; and a user can also “inherit” parameters from a group. Thus you can quickly configure authentication for large numbers of users.

Of course, if you decide to grant identical rights to all VPN users, then you do not need to configure specific groups. But VPNs are seldom managed that way. For example, you might allow a Finance group to access one part of a private network, a Customer Support group to access another part, and an MIS group to access other parts. Further, you might allow specific users within MIS to access systems that other MIS users cannot access.

You can configure detailed parameters for groups and users on the VPN Concentrator internal authentication server. External RADIUS authentication servers also can return group and user parameters that match those on the VPN Concentrator; other authentication servers do not; they can, however, authenticate users. The Cisco software CD-ROM includes a copy of the Cisco Secure ACS RADIUS server.

The VPN Concentrator internal authentication server is adequate for a small user base. The maximum number of groups and users (combined) that you can configure in the internal server depends on your VPN Concentrator model. (See [Table 14-1](#).) For larger numbers of users, we recommend using the internal server to configure groups (and perhaps a few users) and using a RADIUS server to authenticate the users.

Table 14-1 Maximum Number of Groups and Users for the Internal Authentication Server

VPN Concentrator Model	Maximum Number of Groups and Users (Combined)
3005	100
3015	100
3030	500
3060	1000
3080	1000

The VPN Concentrator checks authentication parameters in this order:

- First: User parameters. If any parameters are missing, the system looks at:
- Second: Group parameters. If any parameters are missing, the system looks at:
- Third, for IPSec users only: IPSec tunnel-group parameters. These are the parameters of the IPSec group used to create the tunnel. The IPSec group is configured on the internal server. If any parameters are missing, the system looks at base group parameters. For VPN 3002 Hardware Client parameters, which enable or disable interactive hardware client authentication and individual user authentication, the IPSec tunnel group parameters take precedence over parameters set for users and groups.
- Last: Base-group parameters.

If you use a non-RADIUS server, only the IPSec tunnel-group or base-group parameters apply to users.

Some additional points to note:

- Base-group parameters are the default, or system-wide, parameters.
- A user can be a member of only one group.
- A user that is not a member of a group can nevertheless assume attributes from that group if you join the groupname to the username using a delimiter. See Configuration | System | General | Global Authentication Parameters for details on how to select and use a delimiter.
- Users who are not members of a specific group are, by default, members of the base group. Therefore, to ensure maximum security and control, you should assign all users to appropriate groups, and you should configure base-group parameters carefully.
- You can change group parameters, thereby changing parameters for all its members at the same time.
- You can delete a group, but when you do, all its members revert to the base group. Deleting a group, however, does not delete its members' user profiles.
- You can override the base-group parameters when you configure groups and users, and give groups and users more or fewer rights with this exception:

For PPTP and L2TP authentication protocols, you can allow specific groups and users to use *fewer* protocols than the base group, but not more.

For all other parameters, groups' and users' rights can be greater than the base group. For example, you can give a specific user 24-hour access to the VPN, but give the base group access during business hours only.

- You apply filters to groups and users, and thus govern *tunneled* data traffic through the VPN Concentrator. You also apply filters to network interfaces, and thus govern *all* data traffic through the VPN Concentrator. See the Configuration | Policy Management | Traffic Management screens.
- We can supply a “dictionary” of Cisco-specific user and group parameters for external RADIUS servers.

We recommend that you *define* groups when planning your VPN, and that you *configure* groups and users on the VPN Concentrator in this order:

1. Base-group parameters.
2. Group parameters.
3. User parameters.

Before configuring groups and users, you should configure:

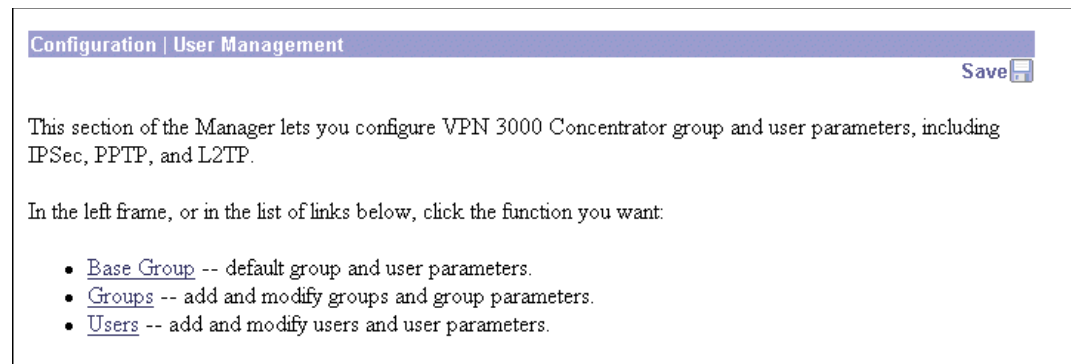
- System policies: network lists, access hours, filters, rules, and IPSec security associations (see Configuration | Policy Management).

- Authentication servers, and specifically the internal authentication server (see Configuration | System | Servers).

Configuration | User Management

This section of the Manager lets you configure base-group, group, and individual user parameters. These parameters determine access and use of the VPN Concentrator.

Figure 14-1 Configuration | User Management Screen



Configuration | User Management | Base Group

This Manager screen lets you configure the default, or base-group, parameters. Base-group parameters are those that are most likely to be common across all groups and users, and they streamline the configuration task. Groups can “inherit” parameters from this base group, and users can “inherit” parameters from their group or the base group. You can override these parameters as you configure groups and users. Users who are not members of a group are, by default, members of the base group.

On this screen, you configure the following kinds of parameters:

- General Parameters: Security, access, performance, and protocols.
- IPSec Parameters: IP Security tunneling protocol.
- Mode Config Parameters: Banner, password storage, split-tunneling policy, default domain name, IPSec over UDP, backup servers.
- Client FW Parameters: VPN Client personal firewall requirements.
- HW Client Parameters: Interactive hardware client and individual user authentication; network extension mode.
- PPTP/L2TP Parameters: PPTP and L2TP tunneling protocols.

Before configuring these parameters, you should configure:

- Access Hours (Configuration | Policy Management | Access Hours).
- Rules and filters (Configuration | Policy Management | Traffic Management | Rules and Filters).
- IPSec Security Associations (Configuration | Policy Management | Traffic Management | Security Associations).
- Network Lists for filtering and split tunneling (Configuration | Policy Management | Traffic Management | Network Lists).
- User Authentication servers, and specifically the internal authentication server (Configuration | System | Servers | Authentication).

Using the Tabs

This screen includes three tabbed sections. Click each tab to display its parameters. As you move from tab to tab, the Manager retains your settings. When you have finished setting parameters on all tabbed sections, click **Apply** or **Cancel**.

General Parameters Tab

This tab lets you configure general security, access, performance, and protocol parameters that apply to the base group.

Figure 14-2 Configuration | User Management | Base Group Screen, General Tab

Configuration User Management Base Group		
General Parameters		
Attribute	Value	Description
Access Hours	-No Restrictions-	Select the access hours for this group.
Simultaneous Logins	3	Enter the number of simultaneous logins for users in this group.
Minimum Password Length	8	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout	30	(minutes) Enter the idle timeout for this group.
Maximum Connect time	0	(minutes) Enter the maximum connect time for this group.
Filter	-None-	Select the filter assigned to this group.
Primary DNS		Enter the IP address of the primary DNS server for this group.
Secondary DNS		Enter the IP address of the secondary DNS server.
Primary WINS		Enter the IP address of the primary WINS server for this group.
Secondary WINS		Enter the IP address of the secondary WINS server.
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	Select the SEP cards this group can be on.
Tunneling Protocols	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec	Select the tunneling protocols this group can connect with.
Strip Realm	<input type="checkbox"/>	Check to remove the realm qualifier of the user name during authentication.

Apply Cancel

68262

Access Hours

Click the **Access Hours** drop-down menu button and select the named hours when remote-access users can access the VPN Concentrator. Configure access hours on the Configuration | Policy Management | Access Hours screen. Default entries are:

- -No Restrictions- = No named access hours applied (the default), which means that there are no restrictions on access hours.
- Never = No access at any time.
- Business Hours = Access 9 a.m. to 5 p.m., Monday through Friday.

Additional named access hours that you have configured also appear on the list.

Simultaneous Logins

Enter the number of simultaneous logins permitted for a single internal user. The minimum is 0, which disables login and prevents user access; default is 3. While there is no maximum limit, allowing several could compromise security and affect performance.

Minimum Password Length

Enter the minimum number of characters for user passwords. The minimum is 1, the default is 8, and the maximum is 32. For security purposes, we strongly recommend 8 or higher.

Allow Alphabetic-Only Passwords

Check the **Allow Alphabetic-Only Passwords** check box to allow user passwords with alphabetic characters only (the default). This option applies only to users who are configured in and authenticated by the VPN Concentrator internal authentication server. To protect security, we strongly recommend that you *not* allow such passwords. Require passwords to be a mix of alphabetic characters, numbers, and symbols, such as 648e&9G#.

Idle Timeout

Enter the idle timeout period in minutes. If there is no communication activity on a user connection in this period, the system terminates the connection. The minimum is 1 minute, the default is 30 minutes, and the maximum is 2147483647 minutes (over 4000 years). To disable timeout and allow an unlimited idle period, enter **0**.

**Note**

This parameter does not apply to individual users as they authenticate to the remote network. The idle timeout value set in the Hardware Client tab of the Configuration | User Management | Base Group or/Groups | Add/Modify screen is the timeout value that applies.

Maximum Connect Time

Enter the maximum user connection time in minutes. At the end of this time, the system terminates the connection. The minimum is 1 minute, and the maximum is 2147483647 minutes (over 4000 years). To allow unlimited connection time, enter **0** (the default).

Filter

Filters consist of rules that determine whether to allow or reject tunneled data packets coming through the VPN Concentrator, based on criteria such as source address, destination address, and protocol. Cisco supplies three default filters, which you can modify. To configure filters and rules, see the [Configuration | Policy Management | Traffic Management](#) screens.

Click the **Filter** drop-down menu button and select the base-group filter:

- --None-- = No filter applied, which means there are no restrictions on tunneled data traffic. This is the default selection.
- Private (Default) = Allow all packets except source-routed IP packets. (This is the default filter for the private Ethernet interface.)
- Public (Default) = Allow inbound and outbound tunneling protocols plus ICMP and VRRP. Allow fragmented IP packets. Drop everything else, including source-routed packets. (This is the default filter for the public Ethernet interface.)
- External (Default) = No rules applied to this filter. Drop all packets. (This is the default filter for the external Ethernet interface.)

Additional filters that you have configured also appear on the list.

Primary DNS

Enter the IP address, in dotted decimal notation, of the primary DNS server for base-group users. The system sends this address to the client as the first DNS server to use for resolving host names. If the base group doesn't use DNS, leave this field blank. See the [Note on DNS and WINS entries](#) section under [Configuration | User Management | Groups | Add or Modify \(Internal\)](#).

Secondary DNS

Enter the IP address, in dotted decimal notation, of the secondary DNS server for base-group users. The system sends this address to the client as the second DNS server to use for resolving host names.

Primary WINS

Enter the IP address, in dotted decimal notation, of the primary WINS server for base-group users. The system sends this address to the client as the first WINS server to use for resolving host names under Windows NT. If the base group does not use WINS, leave this field blank. (See the [Note on DNS and WINS entries](#) on [page 14-49](#)).

Secondary WINS

Enter the IP address, in dotted decimal notation, of the secondary WINS server for base-group users. The system sends this address to the client as the second WINS server to use for resolving host names under Windows NT.

SEP Card Assignment

The VPN Concentrator can contain up to four SEP (Scalable Encryption Processing) modules that handle encryption functions, which are compute-intensive. Two SEP modules handle a number of sessions (users) up to the system maximum. The system maximum is 1000 sessions for the VPN Concentrator 3080 and 5000 sessions for the VPN Concentrator 3060. Two additional modules can provide automatic failover for the first two. This parameter lets you configure the load on each SEP module.

Check the **SEP Card Assignment** check box to assign the load to a given SEP module. By default, all boxes are checked, and we recommend that you keep the default. If your system does not have a given SEP module, the parameter is ignored.

Tunneling Protocols

Check the desired **Tunneling Protocols** check boxes to select the VPN tunneling protocols that user clients can use. Configure parameters on the IPsec or PPTP/L2TP tabs as appropriate. Clients can use only the selected protocols.

You cannot check both IPsec and L2TP over IPsec. The IPsec parameters differ for these two protocols, and you cannot configure the base group for both.

- PPTP = Point-to-Point Tunneling Protocol (checked by default). PPTP is a client-server protocol, and it is popular with Microsoft clients. Microsoft Dial-Up Networking (DUN) 1.2 and 1.3 under Windows 95/98 support it, as do versions of Windows NT 4.0 and Windows 2000.
- L2TP = Layer 2 Tunneling Protocol (checked by default). L2TP is a client-server protocol. It combines many features from PPTP and L2F (Layer 2 Forwarding).
- IPsec = IP Security Protocol (checked by default). IPsec provides the most complete architecture for VPN tunnels, and it is perceived as the most secure protocol. Both LAN-to-LAN (peer-to-peer) connections and client-to-LAN connections can use IPsec. The Cisco VPN Client is an IPsec client specifically designed to work with the VPN Concentrator. However, the VPN Concentrator can establish IPsec connections with many protocol-compliant clients.
- L2TP over IPsec = L2TP using IPsec for security (unchecked by default). L2TP packets are encapsulated within IPsec, thus providing an additional authentication and encryption layer for security. L2TP over IPsec is a client-server protocol that provides interoperability with the Windows 2000 VPN client. It is also compliant, but not officially supported, with other remote-access clients.



Note

If no protocol is selected, no user clients can access or use the VPN.

Strip Realm

Check the **Strip Realm** check box to remove the realm qualifier of the user name during authentication. If you check this Strip Realm box, authentication is based on the *username* alone. Otherwise, authentication is based on the full *username@realm* string. You must check this box if your server is unable to parse delimiters.

IPSec Parameters Tab

This tab lets you configure IP Security Protocol parameters that apply to the base group. If you checked IPSec or L2TP over IPSec under Tunneling Protocols on the General Parameters tab, configure this section.

Figure 14-3 Configuration | User Management | Base Group Screen, IPSec Tab

Configuration User Management Base Group		
General IPSec Client Config Client FW HW Client PPTP/L2TP		
IPSec Parameters		
Attribute	Value	Description
IPSec SA	ESP-3DES-MD5	Select the IPSec Security Association assigned to this group.
IKE Peer Identity Validation	If supported by certificate	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	<input checked="" type="checkbox"/>	Check to enable the use of IKE keepalives for members of this group.
Tunnel Type	Remote Access	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.
Remote Access Parameters		
Group Lock	<input type="checkbox"/>	Lock the users into this group.
Authentication	Internal	Select the authentication method for members of this group. This parameter does not apply to Individual User Authentication .
IP Comp	None	Select the method of IP Compression for members of this group.
Default Preshared Key		Enter the preshared key to be used with clients that do not support groups.
Reauthentication on Rekey	<input type="checkbox"/>	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Mode Configuration	<input checked="" type="checkbox"/>	Check to initiate the exchange of Mode Configuration parameters with the client. This must be checked if version 2.5 (or earlier) of the the Altiga/Cisco client are being used by members of this group.
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

78207

IPSec SA

Click the **IPSec SA** drop-down menu button and select the IPSec Security Association (SA) assigned to IPSec clients. During tunnel establishment, the client and server negotiate a Security Association that governs authentication, encryption, encapsulation, key management, etc. You configure IPSec Security Associations on the Configuration | Policy Management | Traffic Management | Security Associations screens.

To use IPSec with remote-access clients, you must assign an SA. With IPSec LAN-to-LAN connections, the system ignores this selection and uses parameters from the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN screens.

The VPN Concentrator supplies these default selections:

- --None-- = No SA assigned. Select this option if you need to configure groups with several different SAs.
- ESP-DES-MD5 = This SA uses DES 56-bit data encryption for both the IKE tunnel and IPSec traffic, ESP/MD5/HMAC-128 authentication for IPSec traffic, and MD5/HMAC-128 authentication for the IKE tunnel.
- ESP-3DES-MD5 = This SA uses Triple-DES 168-bit data encryption and ESP/MD5/HMAC-128 authentication for IPSec traffic, and DES-56 encryption and MD5/HMAC-128 authentication for the IKE tunnel. This is the default selection.
- ESP/IKE-3DES-MD5 = This SA uses Triple-DES 168-bit data encryption for both the IKE tunnel and IPSec traffic, ESP/MD5/HMAC-128 authentication for IPSec traffic, and MD5/HMAC-128 authentication for the IKE tunnel.
- ESP-3DES-NONE = This SA uses Triple-DES 168-bit data encryption and no authentication for IPSec traffic, and DES-56 encryption and MD5/HMAC-128 authentication for the IKE tunnel.
- ESP-L2TP-TRANSPORT = This SA uses DES 56-bit data encryption and ESP/MD5/HMAC-128 authentication for IPSec traffic (with ESP applied only to the transport layer segment), and it uses Triple-DES 168-bit data encryption and MD5/HMAC-128 for the IKE tunnel. Use this SA with the L2TP over IPSec tunneling protocol.
- ESP-3DES-MD5-DH7 = This SA uses Triple-DES 168-bit data encryption and ESP/MD5/HMAC-128 authentication for both IPSec traffic and the IKE tunnel. It uses Diffie-Hellman Group 7 (ECC) to negotiate Perfect Forward Secrecy. This option is intended for use with the movianVPN client, but you can use it with other clients that support D-H Group 7 (ECC).

Additional SAs that you have configured also appear on the list.

IKE Peer Identity Validation

Click the **IKE Peer Identity Validation** drop-down menu button, and select the type of peer identity validation.

**Note**

This option applies only to tunnel negotiations based on certificates.

During IKE tunnel establishment, the peer provides its identity: either an IP address, a fully qualified domain name (FQDN), or a distinguished name (DN). It also presents a certificate, which contains none, some, or all of these fields. If IKE peer identity validation is enabled, the VPN Concentrator compares the peer's identity to the like field in the certificate to see if the information matches. If the information matches, then the peer's identity is validated and the VPN Concentrator establishes the tunnel. If the information does not match, the VPN Concentrator drops the tunnel. This feature provides an additional level of security.

IKE Peer Identity Validation can be useful for binding a peer to a particular IP address or domain name. For example, if the IP address that the peer provided as an identification during tunnel establishment does not match the IP address in its certificate, the VPN Concentrator fails to validate the peer and drops the tunnel.

Ideally all the VPN Concentrator peers are configured to provide matching types of identity and certificate fields. In this case, enabling Peer Identity Validation ensures that the VPN Concentrator checks the validity of every peer, and only validated peers connect. But in actuality, some peers might not be configured to provide this data. The peer provides a certificate, but that certificate might not contain any of the matching fields required for an identity check. (For example, the peer might provide an IP address for its identity and its certificate might contain only a distinguished name.) If a peer does not provide sufficient information for the VPN Concentrator to check its identity, there are two possibilities: the VPN Concentrator either establishes the session or drops it. If you want the VPN Concentrator to drop sessions of peers that do not provide sufficient information to perform an identity check, choose **Required**. If you want the VPN Concentrator to establish sessions for peers that do not provide sufficient identity information to perform a check, select **If supported by Certificate**.

- **Required** = Enable the IKE peer identity validation feature. If a peer's certificate does not provide sufficient information to perform an identity check, drop the tunnel.
- **If supported by certificate** = Enable the IKE peer identity validation feature. If a peer's certificate does not provide sufficient information to perform an identity check, allow the tunnel.
- **Do not check** = Do not check the peer's identity at all. Selecting this option disables the feature.

IKE Keepalives

Check the **IKE Keepalives** check box to enable IKE keepalives. (IKE keepalives is enabled by default.) This feature lets the VPN Concentrator monitor the continued presence of a remote peer and to report its own presence to that peer. If the peer becomes unresponsive, the VPN Concentrator removes the connection. Enabling IKE keepalives prevents hung connections when the IKE peer loses connectivity.

There are various forms of IKE keepalives. For this feature to work, both the VPN Concentrator and its remote peer must support a common form. This feature works with the following peers:

- Cisco VPN Client (Release 3.0 and above)
- Cisco VPN 3000 Client (Release 2.x)
- Cisco VPN 3002 Hardware Client
- Cisco VPN 3000 Series Concentrators
- Cisco IOS software
- Cisco Secure PIX Firewall

Non-Cisco VPN clients do not support IKE keepalives.

If you are configuring a group of mixed peers, and some of those peers support IKE keepalives and others do not, enable IKE keepalives for the entire group. The feature does not affect the peers that do not support it.

If you disable IKE keepalives, connections with unresponsive peers remain active until they time out, so we recommend you keep your idle timeout short. To change your idle timeout, see the Configuration | User Management | Groups | Add screen, General tab.



Note

To reduce connectivity costs, disable IKE keepalives if this group includes any clients connecting via ISDN lines. ISDN connections normally disconnect if idle, but the IKE keepalives mechanism prevents connections from idling and therefore from disconnecting.



Note

If you have a LAN-to-LAN configuration using IKE main mode, make sure the two peers have the same IKE keepalives configuration: both must have IKE keepalives enabled or both must have it disabled.

Tunnel Type

Click the **Tunnel Type** drop-down menu button and select the type of IPSec tunnel that clients use:

- LAN-to-LAN = IPSec LAN-to-LAN connections between two VPN Concentrators (or between a VPN Concentrator and another protocol-compliant security gateway). See the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN section. If you select this type, ignore the rest of the parameters on this tab.
- Remote Access = Remote IPSec client connections to the VPN Concentrator (the default). If you select this type, configure Remote Access Parameters.

Remote Access Parameters

These base-group parameters apply to remote-access IPSec client connections only. If you select Remote Access for Tunnel Type, configure these parameters.

Group Lock

Check the **Group Lock** check box to restrict users to remote access through this group only. The IPSec client connects to the VPN Concentrator via a group name and password, and then the system authenticates a user via a username and password. If this box is unchecked (the default), the system authenticates a user without regard to the user's assigned group.

Authentication

Whenever a VPN software or VPN 3002 hardware client attempts a tunneled connection to a network behind a VPN Concentrator, that client is authenticated by means of a username and password. This authentication occurs when the tunnel initiates.

Click the **Authentication** drop-down menu button and select the authentication method (authentication server type) to use with this group's remote-access IPSec clients. Both VPN Clients and VPN 3002 hardware clients authenticate on the first server of the type you configure.

This selection identifies the authentication *method*, not the specific server. Configure authentication servers on the Configuration | System | Servers | Authentication screens or Configuration | User Management | Groups | Authentication Servers screens.

For the VPN 3002, this selection applies to authentication using a saved username and password and to interactive hardware client authentication. Individual users behind the VPN 3002 authenticate according to the priority order of all authentication servers configured, regardless of type. For more information on the different ways in which a VPN 3002 can authenticate, see the section, "[HW Client Parameters Tab](#)."



Note

To configure user-based authentication for Cisco VPN Clients, choose an Authentication method, then follow the additional steps outlined under Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add, Modify, or Copy.

Selecting any authentication method (other than None) enables ISAKMP Extended Authentication, also known as XAUTH.

- None = No IPSec user authentication method. If you checked L2TP over IPSec under Tunneling Protocols, use this selection.
- RADIUS = Authenticate clients via external RADIUS server.
- RADIUS with Expiry = Authenticate clients via external RADIUS server. If the password has expired, notify the client and offer the opportunity to create a new password.
- NT Domain = Authenticate clients via external Windows NT Domain system.
- SDI = Authenticate clients via external RSA Security Inc. SecureID system.
- Internal = Authenticate clients via the internal VPN Concentrator authentication server. This is the default selection.

Enabling RADIUS with Expiry allows the VPN Concentrator to use MS-CHAP-v2 when authenticating an IPSec client to an external RADIUS server. That RADIUS server must support both MS-CHAP-v2 and the Microsoft Vendor Specific Attributes. Refer to the documentation for your RADIUS server to verify that it supports these capabilities.

Because of the use of MS-CHAP-v2, when you enable RADIUS with Expiry on the VPN Concentrator, the VPN Concentrator can provide enhanced login failure messages to the VPN Client describing specific error conditions. These conditions are:

- Restricted login hours.
- Account disabled.
- No dial-in permission.
- Error changing password.
- Authentication failure.

**Note**

For RADIUS with Expiry to work with a VPN 3002, the VPN 3002 must have the Require Interactive Hardware Client Authentication feature enabled.

IPComp

If all members of this group are remote dial-in users connecting with modems, enabling data compression might speed up their data transmission rates. Data compression shrinks data by replacing repeating information with symbols that use less space. Click the **IPComp** drop-down menu button to enable data compression using IPComp.

- None = No data compression.
- LZS = Enable data compression using the LZS compression algorithm.

**Caution**

Data compression increases the memory requirement and CPU utilization for each user session and consequently decreases the overall throughput of the VPN Concentrator. For this reason, *we recommend that you enable data compression only if every member of the group is a remote user connecting with a modem.* If any members of the group connect via broadband, do not enable data compression for the group. Instead, divide the group into two groups, one for modem users and the other for broadband users. Enable data compression only for the group of modem users.

Default Preshared Key

Enter the preshared secret. Use a minimum of four and a maximum of 32 alphanumeric characters.

This option allows the following VPN clients to connect to the VPN Concentrator:

- VPN clients that use pre-shared secrets but do not support the concept of a “group,” such as the Microsoft Windows XP L2TP/IPSec client.
- VPN router devices that are creating inbound connections from non-fixed IP addresses using pre-shared secrets.

Reauthentication on Rekey

Check the **Reauthentication on Rekey** check box to enable reauthentication, or uncheck the box to disable it.

The VPN Concentrator prompts the user to enter an ID and password during Phase 1 IKE negotiations. If you enable reauthentication, the VPN Concentrator also prompts for user authentication whenever a rekey occurs. Reauthentication provides additional security.

- If the configured rekey interval is very short, users might find the repeated authorization requests inconvenient. With interactive hardware client authentication enabled, a short rekey interval causes the tunnel to drop. In either case, either make the rekey interval a long one, or disable reauthentication. (To check your VPN Concentrator's configured rekey interval, see the Lifetime Measurement, Data Lifetime, and Time Lifetime fields on the Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add or Modify screen.)

Mode Configuration

Check the **Mode Configuration** check box to use Mode Configuration with IPSec clients (also known as the ISAKMP Configuration Method or Configuration Transaction). This option exchanges configuration parameters with the client while negotiating Security Associations. If you check this box, configure the desired Mode Configuration Parameters; otherwise, ignore them. The box is checked by default.

To use split tunneling, you must check this box.

If you checked L2TP over IPSec under Tunneling Protocols, *do not* check this box.



Note

IPSec uses Mode Configuration to pass all configuration parameters to a client: IP address, DNS and WINS addresses, etc. You *must* check this box to use Mode Configuration. Otherwise, those parameters—even if configured with entries—are not passed to the client.



Note

The Cisco VPN Client (IPSec client) supports Mode Configuration, but other IPSec clients might not. For example, the Microsoft Windows 2000 IPSec client does *not* support Mode Configuration. (The Windows 2000 client uses the PPP layer above L2TP to receive its IP address from the VPN Concentrator.) Determine compatibility before using this option with other vendors' clients. While this functionality might work with other clients, Cisco does not certify or formally support this environment for other clients.

Client Configuration Parameters Tab

These base-group parameters apply to IPSec clients.

Figure 14-4 Configuration | User Management | Base Group, Client Configuration Parameters Tab

Configuration User Management Base Group		
Client Configuration Parameters		
Cisco Client Parameters		
Attribute	Value	Description
Banner		Enter the banner for this group. Only software clients see the banner.
Allow Password Storage on Client	<input type="checkbox"/>	Check to allow the IPSec client to store the password locally.
IPSec over UDP	<input type="checkbox"/>	Check to allow a client to operate through a NAT device using UDP encapsulation of ESP.
IPSec over UDP Port	<input type="text" value="10000"/>	Enter the UDP port to be used for IPSec through NAT (4001 - 49151, except port 4500, which is reserved for NAT-T).
IPSec Backup Ser	<input type="text" value="Use client configured list"/> 	<ul style="list-style-type: none"> Select a method to use or disable backup servers. Enter up to 10 IPSec backup server addresses/names starting from high priority to low. Enter each IPSec backup server address/name on a single line.
Microsoft Client Parameters		
Intercept DHCP Configure Message	<input type="checkbox"/>	Check to use group policy for clients requesting Microsoft DHCP options.
Subnet Mask	<input type="text" value="255.255.255.255"/>	Enter the subnet mask for clients requesting Microsoft DHCP options.
Common Client Parameters		
Split Tunneling Policy	<input checked="" type="radio"/> Tunnel everything <input type="checkbox"/> Allow the networks in list to bypass the tunnel <input type="radio"/> Only tunnel networks in list	Select the method and network list to be used for Split Tunneling. Tunnel Everything: Send all traffic through the tunnel. Allow the Networks in the list to bypass the tunnel: The VPN Client may choose to send traffic to addresses in this list to the client's LAN. Send all other traffic through the tunnel. NOTE: This setting only applies to the Cisco Client. Tunnel Networks in List: Send traffic to addresses in this list through the VPN tunnel. Send all other traffic unencrypted.
Split Tunneling Network List	<input type="text" value="--None--"/>	
Default Domain Name	<input type="text"/>	Enter the default domain name given to users of this group.
Split DNS Names	<input type="text"/>	Enter the set of domains, separated by commas without spaces, to be resolved through the Split Tunnel.
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

78455

Banner

Enter the banner, or welcome text, that this group's IPsec clients see when they log in. The maximum length is 510 characters. You can use any characters, including newline (the Enter key, which counts as two characters).

Allow Password Storage on Client

Check the **Allow Password Storage on Client** check box to allow IPsec clients to store their login passwords on their local client systems. If you do not allow password storage (the default), IPsec users must enter their password each time they seek access to the VPN. For maximum security, we recommend that you *not allow* password storage.

This parameter has no bearing on interactive hardware client authentication or individual user authentication for a VPN 3002.

IPsec over UDP

Check the **IPsec over UDP** check box to allow the Cisco VPN Client (IPsec client) or VPN 3002 hardware client to connect to the VPN Concentrator via UDP through a firewall or router using NAT. The box is unchecked by default. See the following discussion.

IPsec over UDP Port

Enter the UDP port number to use on the VPN Concentrator if you allow IPsec through NAT. Enter a number in the range 4001 through 49151; default is 10000.

About IPsec over UDP

IPsec over UDP, sometimes called IPsec through NAT, lets you use the Cisco VPN Client or VPN 3002 hardware client to connect to the VPN Concentrator via UDP through a firewall or router that is running NAT. This feature is proprietary, it applies only to remote-access connections, and it requires Mode Configuration. Using this feature might slightly degrade system performance.

Enabling this feature creates runtime filter rules that forward UDP traffic for the configured port even if other filter rules on the interface drop UDP traffic. These runtime rules exist only while there is an active IPsec through NAT session. The system passes inbound traffic to IPsec for decryption and unencapsulation, and then passes it to the destination. The system passes outbound traffic to IPsec for encryption and encapsulation, applies a UDP header, and forwards it.

You can configure more than one group with this feature enabled, and each group can use a different port number. Port numbers must be in the 4001 through 49151 range, which is a subset of the IANA Registered Ports range.

The Cisco VPN Client must also be configured to use this feature (it is configured to use it by default). The VPN Client Connection Status dialog box indicates if the feature is being used. Refer to the VPN Client User Guide.

The VPN 3002 hardware client does not require configuration to use IPsec through NAT.

The Administration | Sessions and Monitoring | Sessions screens indicate if a session is using IPsec through NAT, and the Detail screens show the UDP port.



Note

The following restrictions apply to multiple simultaneous connections using IPsec over UDP:

Multiple simultaneous connections from VPN Client or VPN 3002 hardware client users behind a PAT (Port Address Translation) device can work, but only if the PAT device assigns a unique source port for each simultaneous user.

Some PAT devices use UDP source port = 500 for all IKE sessions, even if there are multiple sessions. This allows only one session at a time; the second connection brought up from behind this type of PAT device causes the first session to be torn down. (This is unrelated to whether or not a PAT device supports “ESP” PAT, or if you are using the IPSec UDP functionality.)

Therefore, for multiple simultaneous IPSec over UDP connections, use a PAT device that maps each additional session to use unique UDP source ports. Alternatively, connect additional users to different destination VPN Concentrators.

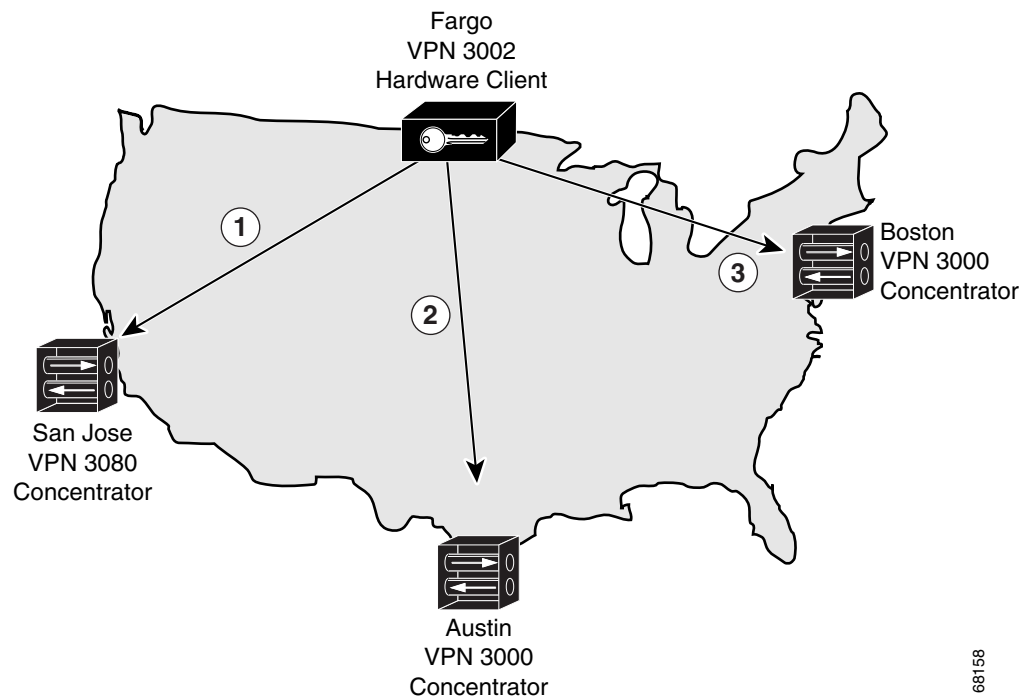
IPSec Backup Servers

IPSec backup servers let a VPN 3002 Hardware Client connect to the central site when its primary central-site VPN Concentrator is unavailable. You configure backup servers for a VPN 3002 either on the VPN 3002, or on a group basis at the primary central-site VPN Concentrator. If you configure backup servers on the central-site VPN Concentrator, that VPN Concentrator pushes the backup server policy to the VPN 3002 hardware clients in the group.

By default the policy is to use the backup server list configured on the VPN 3002. Alternatively, the VPN Concentrator can push a policy that supplies a list of backup servers in order of priority (replacing the backup server list on the VPN 3002 if one is configured), or it can disable the feature and clear the backup server list on the VPN 3002 if one is configured.

Figure 14-5 illustrates how the backup server feature works.

Figure 14-5 Backup Server Implementation



68158

XYZ corporation has large sites in three cities: San Jose, California; Austin, Texas; and Boston, Massachusetts. They just opened a regional sales office in Fargo, North Dakota. To provide access to the corporate network from Fargo, they use a VPN 3002 that connects to a VPN 3080 in San Jose (1). If the VPN 3002 is unable to contact the corporate network, Fargo cannot place orders. However, the IPSec backup server feature lets the VPN 3002 connect to one of several other sites, in this case using Austin (2) and Boston (3) as backup servers, in that order.

The VPN 3002 in Fargo first attempts to reach San Jose. If the initial IKE packet for that connection (1) times out (8 seconds), the VPN 3002 tries to connect to Austin (2). Should this negotiation also time out, the VPN 3002 tries to connect to Boston (3). These attempts continue until the VPN 3002 has tried all servers on its backup server list, to a maximum of 10.

Be aware of the following characteristics of the backup server feature:

- If the VPN 3002 cannot connect after trying all backup servers on the list, it does not automatically retry.
 - In Network Extension mode, the VPN 3002 attempts a new connection after 4 seconds.
 - In Client mode, the VPN 3002 attempts a new connection when the user presses the Connect Now button on the Monitoring | System Status screen, or when data passes from the VPN 3002 to the VPN Concentrator.
- A VPN 3002 must connect to the primary VPN Concentrator to download a backup server list configured on the primary VPN Concentrator. If that Concentrator is unavailable, and if the VPN 3002 has a previously configured backup server list, it can connect to the servers on that list.
- A VPN 3002 can download a backup server list only from the primary VPN Concentrator. It cannot download a backup server list from a backup server.
- The VPN Concentrators that you configure as backup servers do not have to be aware of each other.
- If you change the configuration of backup servers, or delete a backup server during an active session between a VPN 3002 and a backup server, the session continues without adopting that change. New settings take effect the next time the VPN 3002 connects to its primary VPN Concentrator.

You can configure the backup server feature from the primary VPN Concentrator or the VPN 3002. From the VPN Concentrator, configure backup servers on either of the Configuration | User Management | Base Group or Groups | Mode Configuration screens. On the VPN 3002, configure backup servers on the Configuration | System | Tunneling Protocols | IPSec screen.

The list you configure on the VPN 3002 applies only if the option, Use Client Configured List, is set in the IPSec Backup Servers parameter. To set this parameter, go to the Mode Configuration tab of the Configuration | User Management | Groups | Add/Modify screen for the primary VPN Concentrator to which the VPN 3002 connects.

**Note**

The group name, user name, and passwords that you configure for the VPN 3002 must be identical for the primary VPN Concentrator and all backup servers. Also, if you require interactive hardware client authentication and/or individual user authentication for the VPN 3002 on the primary VPN Concentrator, be sure to configure it on backup servers as well. See the [HW Client Parameters Tab](#) for more information.

Configuring Backup Servers on the Central-Site VPN Concentrator

To configure backup servers on the primary central-site VPN Concentrator, accept the default, Use list below in the IPsec Backup Servers drop down menu.

Enter either the IP addresses or the hostnames of the VPN Concentrators that are to be backup servers. The IP address is the IP address of the VPN Concentrator public interface.



Note

If you are using hostnames, it is wise to have backup DNS and WINS servers on a separate network from that of the primary DNS and WINS servers. Otherwise, if clients behind the VPN 3002 obtain DNS and WINS information from the VPN 3002 through DHCP, and the connection to the primary server is lost, and the backup servers have different DNS and WINS information, clients cannot be updated until the DHCP lease expires. Further, if you use hostnames and the DNS server is unavailable, significant delays can occur.

You can enter up to 10 backup servers, in order of highest to lowest priority. Enter each backup server on a single line, using the Enter or Return key for each new line.

Should there be a backup server list already configured on the VPN 3002, this list on the central-site VPN Concentrator replaces it, and becomes the list of backup servers on the VPN 3002 hardware client.

If you change the configuration of backup servers, or delete a backup server during an active session between a VPN 3002 and a backup server, the session continues without adopting that change. New settings take effect in the next new session.

Configuring Backup Servers from the VPN 3002

To configure backup servers on the VPN 3002, accept the default, Use client configured list in the IPsec Backup Servers drop-down menu. You then configure backup servers in the VPN 3002 Configuration | System | Tunneling Protocols | IPsec screen. Refer to the Tunneling chapter in the *VPN 3002 Hardware Client User Reference* for instructions.

Disabling Backup Servers

To disable the backup server feature, select **Disable and clear client configured list** in the IPsec Backup Servers drop-down menu. If you disable the feature from the primary VPN Concentrator, the feature is disabled and the list of backup servers configured on the VPN 3002, if there is one, is cleared.

Intercept DHCP Configure Message

DHCP Intercept lets Microsoft XP clients implement split-tunneling with a VPN Concentrator. The VPN Concentrator replies directly to the Microsoft Windows XP client DHCP Inform message, providing that client with the subnet mask, domain name, and classless static routes for the tunnel IP address. For Windows clients prior to XP, DHCP Intercept provides the domain name and subnet mask. This is useful in environments in which using a DHCP server is not advantageous.



Note

A Microsoft XP anomaly results in the corruption of domain names if split tunnel options exceed 255 bytes. The VPN Concentrator limits the number of routes it sends to 27-40 routes, with the number of routes dependent on the classes of the routes, to avoid this problem.

Check the box to enable DHCP Intercept.

Subnet Mask

Enter the subnet mask for clients requesting Microsoft DHCP options.

Split Tunneling Policy

Split tunneling lets an IPsec client conditionally direct packets over an IPsec tunnel in encrypted form, or to a network interface in cleartext form. Packets not bound for destinations on the other side of the IPsec tunnel do not have to be encrypted, sent across the tunnel, decrypted, and then routed to a final destination. Split tunneling thus eases the processing load, simplifies traffic management, and speeds up untunneled traffic.

**Note**

To implement split tunneling for Microsoft XP clients, you must meet several conditions:

- Set the Split Tunneling Policy to “Only tunnel networks in list.”
- Configure network lists and default domain names in the Common Client Parameters section of this screen.
- Change the default setting on the client PC’s Internet Protocol (TCP/IP) Properties window. The path is Control Panel > Network Connections > VPN > VPN Properties > Networking > Internet Protocol (TCP/IP) > Select Properties > Internet Protocol (TCP/IP) Properties window. Select Advanced and uncheck the box.

**Note**

If you enable both split tunneling and individual user authentication for a VPN 3002, users must authenticate only when sending traffic bound for destinations on the other side of the IPsec tunnel.

Split tunneling is primarily a traffic management feature, not a security feature. In fact, for optimum security, we recommend that you *not* enable split tunneling. However, since only the VPN Concentrator—and not the IPsec client—can enable split tunneling, you can control implementation here and thus protect security. Split tunneling is disabled by default on both the VPN Concentrator and the client. You enable and configure the feature on the VPN Concentrator, and then the VPN Concentrator uses Mode Configuration to push it to, and enable it on, the IPsec client.

Split tunneling applies only to single-user remote-access IPsec tunnels, not to LAN-to-LAN connections.

The default split tunneling policy is Tunnel Everything. Tunnel Everything disables split tunneling. When Tunnel Everything is configured, all traffic from remote clients in this group travels over the secure IPsec tunnel in encrypted form. No traffic goes in the clear or to any other destination than the VPN Concentrator. Remote users in this group reach internet networks through the corporate network and do not have access to local networks.

If users in this group need access to local networks, choose Allow Networks in List to Bypass Tunnel. This option allows you to define a list of networks to which traffic goes in the clear. This feature is useful for remote users who want to access devices on their local network, such as printers, while they are connected to the corporate network through a tunnel.

To configure the Allow Networks in List to Bypass Tunnel option, choose **VPN Client Local LAN** from the Split Tunnel Network List menu. The VPN Client Local LAN option allows all users in the group to access all devices on their local networks. If you want to restrict users’ access to particular devices on their local network, you need to know the addresses of the local devices the remote users in this group want to access. Create a network list of these addresses, then choose that network list from the Split Tunneling Network List menu. You can apply only one network list to a group, but one network list can

contain up to 10 network entries. (See the Configuration | Policy Management | Traffic Management | Network Lists screens for more information on creating network lists.) You also must enable Local LAN Access on the VPN Client. See the *VPN Client Administrator Guide* for more details.

**Note**

The Allow Networks in List to Bypass Tunnel option allows remote users to access *only* devices that are located on the *same* network interface as the tunnel. If a remote user's local LAN is located on a different network interface than the tunnel, the user cannot access it.

To allow remote users to access internet networks without tunneling through the corporate network, enable split tunneling. To enable split tunneling, choose **Only Tunnel Networks in List**. To configure this option, create a network list of addresses to tunnel. Then select this network list from the Split Tunneling Network List menu. Data to all other addresses is sent in the clear and routed by the remote user's internet service provider.

We recommend that you keep the base-group default, and that you enable and configure the split tunneling policy selectively for each group.

- Tunnel everything = Send all data via the secure IPSec tunnel.
- Allow networks in list to bypass the tunnel = Send all data via the secure IPSec tunnel except for data to addresses on the network list. The purpose of this option is to allow users who are tunneling all traffic to access devices such as printers on their local networks. This setting applies only to the Cisco VPN Client.
- Only tunnel networks in list = Send data to addresses on the network list via secure IPSec tunnel. Data bound for any other address goes in the clear. The purpose of this option is to allow remote users to access internet networks without requiring them to be tunneled through the corporate network.

Split Tunneling Network List

Click the drop-down menu button and select the split tunneling address list to use with this group's remote-access IPSec clients.

Both the **Allow Networks in List to Bypass Tunnel** option and the **Only Tunnel Networks in List** option make split tunneling decisions on the basis of a network list, which is a list of addresses on the private network. But the network list functions differently in each configuration.

In an **Allow Networks in List to Bypass Tunnel** configuration, The IPSec client uses the network list as an *exclusion* list: a list of addresses to which traffic should be sent in the clear. All other traffic is routed over the IPSec tunnel.

In an **Only Tunnel Networks in List** configuration, the IPSec client uses the network list as an *inclusion* list: a list of networks for which traffic should be sent over the IPSec tunnel. The IPSec client establishes an IPSec Security Association (SA) for each network specified in the list. Outbound packets with destination addresses that match one of the SAs are sent over the tunnel; everything else is sent as clear text to the locally connected network.

- None = No network address lists are configured.
- VPN Client Local LAN (default) = All addresses on the client's local network. The VPN Client Local LAN network list is a wildcard value that represents the client's local network. It corresponds to the address 0.0.0.0/0.0.0.0, which represents the IP address of the client's network card on which the tunnel is established. This option is the default associated with Allow Networks in List to Bypass Tunnel. It does not apply to the Only Tunnel Networks in List option.

Default Domain Name

Enter the default domain name that the VPN Concentrator passes to the IPSec client, for the client's TCP/IP stack to append to DNS queries that omit the domain field. This domain name applies only to tunneled packets. For example, if this entry is xyzcorp.com, a DNS query for mail becomes mail.xyzcorp.com. The maximum name length is 255 characters. The Manager checks the domain name for valid syntax.

Split DNS Names

Split DNS lets an internal DNS server resolve a list of centrally-defined Local Domain Names, while ISP-assigned DNS servers resolve all other DNS requests. It is used in split-tunneling connections; the internal DNS server resolves the domain names for traffic through the tunnel, and the ISP-assigned DNS servers resolve DNS requests that travel in the clear to the Internet.

Split DNS is not supported on Microsoft clients.

Enter each domain name to be resolved by the internal server. Use commas but no spaces to separate the names.

Client FW Parameters Tab

This tab lets you configure firewall parameters for VPN Clients.

**Note**

Only VPN Clients running Microsoft Windows can use these firewall features. They are presently not available to hardware clients or other (non-Windows) software clients.

A *firewall* isolates and protects a computer from the Internet by inspecting each inbound and outbound individual packet of data to determine whether to allow or drop it. Firewalls provide extra security if remote users in a group have split tunneling configured. In this case, the firewall protects the user's PC, and thereby the corporate network, from intrusions by way of the Internet or the user's local LAN.

Remote users connecting to the VPN Concentrator with the VPN Client can choose from three possible firewall options.

In the first scenario, a remote user has a personal firewall installed on the PC. The VPN Client enforces firewall policy defined on the local firewall, and it monitors that firewall to make sure it is running. If the firewall stops running, the VPN Client drops the connection to the VPN Concentrator. (This firewall enforcement mechanism is called *Are You There (AYT)*, because the VPN Client monitors the firewall by sending it periodic "are you there?" messages; if no reply comes, the VPN Client knows the firewall is down and terminates its connection to the VPN Concentrator.) The network administrator might configure these PC firewalls originally, but with this approach, each user can customize his or her own configuration.

In the second scenario, you might prefer to enforce a centralized firewall policy for personal firewalls on VPN Client PCs. A common example would be to block Internet traffic to remote PCs in a group using split tunneling. This approach protects the PCs, and therefore the central site, from intrusions from the Internet while tunnels are established. This firewall scenario is called *push policy* or *Central Protection Policy (CPP)*. On the VPN Concentrator, you create a set of traffic management rules to enforce on the VPN Client, associate those rules with a filter, and designate that filter as the firewall policy. The VPN Concentrator pushes this policy down to the VPN Client. The VPN Client then in turn passes the policy to the local firewall, which enforces it.

A third scenario is to use a separate firewall server—the Zone Labs Integrity Server (IS)—to secure remote PCs on Windows platforms. The IS maintains policies for remote VPN Client PCs and monitors the PCs to ensure policy enforcement. The IS also communicates with the VPN Concentrator to allow and terminate connections, exchange session and user information, and report status information. For more details on how the VPN Concentrator interacts with the VPN Client, personal firewalls, and the Zone Labs Integrity Server, see the *VPN Client Administrator Guide*. For information on configuring the Zone Labs Integrity Server, refer to Zone Labs' documentation.

Figure 14-6 Configuration | User Management | Base Group | Client FW Parameters Tab

VPN Client Firewall Policy		
Attribute	Value	Description
Firewall Setting	<input checked="" type="radio"/> No Firewall <input type="radio"/> Firewall Required <input type="radio"/> Firewall Optional	Select whether or not to require that the client firewall specified below be installed and active. Refer to the client documentation for details about using this feature.
Firewall	Custom Firewall	Select the firewall vendor and product required for clients in this group. For client firewalls not listed, select Custom Firewall and enter the vendor and product IDs.
Custom Firewall	Vendor ID	Separate multiple product IDs with commas. To indicate all products by a particular vendor, enter product ID 255. The product description is optional.
	Product ID	
	Description	
Firewall Policy	<input checked="" type="radio"/> Policy defined by remote firewall (AYT) <input type="radio"/> Policy Pushed (CPP): --None-- <input type="radio"/> Policy from Server	Select the policy for the protection provided by the client firewall.

Apply Cancel

79322

Firewall Setting

By default, no firewall is required for remote users in this group. If you want users in this group to be firewall-protected, choose either the Firewall Required or Firewall Optional setting.

If you choose Firewall Required, all users in this group must use the designated firewall. The VPN Concentrator drops any session that attempts to connect without the designated, supported firewall installed and running. In this case, the VPN Concentrator notifies the VPN Client that its firewall configuration does not match.

If you have remote users in this group who do not yet have firewall capacity, choose Firewall Optional. The Firewall Optional setting allows all the users in the group to connect. Those who have a firewall can use it; users that connect without a firewall receive a warning message. This setting is useful if you are creating a group in which some users have firewall support and others do not—for example, you may have a group that is in gradual transition, in which some members have set up firewall capacity and others have not yet done so.

Click the radio button to select a firewall setting:

- No Firewall = No firewall is required for remote users in this group.
- Firewall Required = All remote users in this group must use a specific firewall. Only those users with the designated firewall can connect.



Note If you require a firewall for a group, make sure the group does not include any clients other than Windows VPN Clients. Any other clients in the group (including VPN 3002 Hardware Clients) will be unable to connect.

- Firewall Optional = All remote users in this group can connect. Those that have the designated firewall can use it. Those who do not have a firewall receive a warning message.

Firewall

Choose a firewall for the users in this group. Keep in mind when choosing that the firewall you designate correlates with the firewall policies available. The specific firewall you configure determines which firewall policy options are supported. (See [Table 14-3](#) for details.)

Click the drop-down menu button, and select the type of firewall required for users in this group.

- Cisco Integrated Client Firewall = The stateful firewall built into the VPN Client.
- Network ICE BlackICE Defender = The Network ICE BlackICE Agent or Defender personal firewall.
- Zone Labs ZoneAlarm = The Zone Labs ZoneAlarm personal firewall.
- Zone Labs ZoneAlarm Pro = The Zone Labs ZoneAlarm Pro personal firewall.
- Zone Labs ZoneAlarm or ZoneAlarm Pro = Either the Zone Labs ZoneAlarm personal firewall or the Zone Labs ZoneAlarm Pro personal firewall.
- Zone Labs Integrity = The Zone Labs Integrity Client.
- Custom Firewall = A combination of the firewalls listed above, or other firewalls not listed above. If you choose this option, you must create your own list of firewalls in the Custom Firewall field.



Note You do not need to use the Custom option for Release 3.5. Currently, all supported firewalls are covered by the other Firewall menu options.

Custom Firewall

On the VPN Concentrator, you can configure a custom firewall. Currently there are no supported firewall configurations that you can not choose from the menu on the VPN Concentrator. This feature is mainly for future use. Nevertheless, the following table lists the vendor codes and products that are currently supported.

Table 14-2 Custom Vendor and Product codes

Vendor	Vendor Code	Products	Product Code
Cisco Systems	1	Cisco Integrated Client (CIC)	1
Zone Labs	2	Zone Alarm	1
		Zone AlarmPro	2
		Zone Labs Integrity	3
NetworkICE	3	BlackIce Defender/Agent	1

Enter a single vendor code; enter one or more product codes.

The VPN Concentrator can support any firewall that the VPN Client supports. Refer to the *VPN Client Administrator Guide* for the latest list of supported clients.

Vendor ID

Enter the vendor code for the firewall(s) that remote users in this group are using. Enter only one vendor.

Product ID

Enter the product code or codes for the firewall(s) that remote users in this group are using. To indicate any supported product, enter 255. Separate multiple codes with commas. Indicate code ranges with hyphens, for example: 4-20.

Description

Enter a description (optional) for the custom firewall.

Firewall Policy

Depending on which firewall you configured, certain Firewall Policy options are available. (See [Table 14-3](#).)

Table 14-3 Firewall Policy Options Available for Each Firewall

Firewall	Policy Defined by Remote Firewall	Policy Pushed	Policy from Server
Cisco Integrated Client Firewall	No	Yes	No
Network ICE BlackICE Defender	Yes	No	No
Zone Labs ZoneAlarm	Yes	Yes	No
Zone Labs ZoneAlarm Pro	Yes	Yes	No
Zone Labs ZoneAlarm or Zone Labs ZoneAlarm Pro	Yes	Yes	No
Zone Labs Integrity	No	No	Yes
Custom Firewall	N/A (This field is for future use.)		

Choose the source for the VPN Client firewall policy.

- Policy defined by remote firewall (AYT) = Remote users in this group have firewalls located on their PCs. The local firewall enforces the firewall policy on the VPN Client. The VPN Concentrator allows VPN Clients in this group to connect only if they have the designated firewall installed and running. If the designated firewall is not running, the connection fails. Once the connection is established, the VPN Client polls the firewall every 30 seconds to make sure that it is still running. If the firewall stops running, the VPN Client ends the session.
- Policy Pushed (CPP) = The VPN Concentrator enforces on the VPN clients in this group the traffic management rules defined by the filter you choose from the Policy Pushed (CPP) drop-down menu. The choices available on the menu are filters defined on this VPN Concentrator, including the default filters. Keep in mind that the VPN Concentrator pushes these rules down to the VPN client, so you should create and define these rules relative to the VPN client, not the VPN Concentrator. For example, “in” and “out” refer to traffic coming into the VPN Client or going outbound from the VPN Client.

If the VPN Client also has a local firewall, the policy pushed from the VPN Concentrator works with the policy of the local firewall. Any packet that is blocked by the rules of *either* firewall is dropped.

- Policy from Server = Users in this group use a Zone Labs Integrity Server to configure and manage firewall security on their remote PCs. If you choose this option, you must also configure the server address on the Configuration | System | Servers | Firewall Server screen

HW Client Parameters Tab

The Hardware Client Parameters tab lets you configure interactive hardware client authentication and individual user authentication for the base group. You can enable either feature, both features together, or neither. By default, interactive hardware client authentication and individual user authentication are disabled.

Figure 14-7 Configuration | User Management | Base Group, HW Client Parameters Tab

Hardware Client Parameters		
Attribute	Value	Description
Require Interactive Hardware Client Authentication	<input type="checkbox"/>	Check to require the hardware client to be interactively authenticated at each connection attempt.
Require Individual User Authentication	<input type="checkbox"/>	Check to require users behind a hardware client to be authenticated.
User Idle Timeout	30	Enter the session idle timeout in minutes. Use 0 for no timeout.
Cisco IP Phone Bypass	<input type="checkbox"/>	Check to allow Cisco IP Phones to bypass Individual User Authentication behind a hardware client.
Allow Network Extension Mode	<input type="checkbox"/>	Check to allow hardware clients using Network Extension Mode to connect.

Apply Cancel

79338

Require Interactive Hardware Client Authentication

Check the **Require Interactive Hardware Client Authentication** check box to enable interactive authentication for the VPN 3002.

Require Individual User Authentication

Check the **Require Individual User Authentication** box to enable individual user authentication.

User Idle Timeout

Enter the idle timeout period in minutes. If there is no communication activity on a user connection in this period, the system terminates the connection. The minimum is 1 minute, the default is 30 minutes, and the maximum is 2147483647 minutes (over 4000 years). To disable timeout and allow an unlimited idle period, enter **0**.

Cisco IP Phone Bypass

Check the **Cisco IP Phone Bypass** box to allow IP phones to bypass the interactive individual user authentication processes. Interactive hardware client authentication remains in effect if you have enabled it.

Allow Network Extension Mode

This feature lets you restrict the use of network extension mode on the VPN 3002. Check the box to allow VPN 3002s to use network extension mode.

**Note**

If you disallow network extension mode, the default setting, the VPN 3002 can connect to this VPN Concentrator in PAT mode only. If you disallow network extension mode here, be careful that all VPN 3002s in the group are configured for PAT mode. If a VPN 3002 is configured to use network extension mode and the VPN Concentrator to which it connects disallows network extension mode, the VPN 3002 will attempt to connect every 4 seconds, and every attempt will be rejected; this is the equivalent of denial of service attack.

About Interactive Hardware Client Authentication

Interactive hardware client authentication provides the central site with additional security by requiring the VPN 3002 to authenticate with a username and password that you enter manually each time the VPN 3002 initiates a tunnel. With this feature enabled the VPN 3002 does not have a saved username and password. When you enter the username and password, the VPN 3002 sends these credentials to the VPN Concentrator to which it connects. The VPN Concentrator facilitates authentication, on either the internal or an external authentication server. If the username and password are valid, the tunnel is established.

You configure interactive hardware client authentication in Hardware Client tab of the Configuration | User Management | Groups screen on the VPN Concentrator at the central site, which then pushes the policy to the VPN 3002.

You specify the *type* of authentication server in the IPSec tab of the Configuration | User Management | Groups screen on the VPN Concentrator. The VPN 3002 authenticates on the first server of that type that you configure in the Configuration | System | Servers | Authentication screen or Configuration | User Management | Groups | Authentication Servers screen. If the VPN 3002 cannot reach that server, it authenticates on the next server of that type in the list of authentication servers.

Enabling and Later Disabling Interactive Hardware Client Authentication

When you enable interactive hardware client authentication for a group, the VPN Concentrator pushes that policy to the VPN 3002s in the group. If you have previously set a username and password on the VPN 3002, the software deletes them from the configuration file. When you try to connect, the software prompts you for a username and password.

If, on the VPN Concentrator, you subsequently disable interactive hardware authentication for the group, it is enabled locally on the VPN 3002s, and the software continues to prompt for a username and password. This lets the VPN 3002 connect, even though it lacks a saved username and password, and the VPN Concentrator has disabled interactive hardware client authentication.

If you subsequently configure a username and password (in the VPN 3002 Configuration | System | Tunneling Protocols | IPSec screen), the feature is disable, and the prompt no longer displays. The VPN 3002 connects to the VPN Concentrator using the saved username and password.

About Individual User Authentication

Individual user authentication protects the central site from access by unauthorized persons on the same LAN as the VPN 3002.

When you enable individual user authentication, each user that connects through a VPN 3002 must open a web browser and manually enter a valid username and password to access the network behind the VPN Concentrator, even though the tunnel already exists.

**Note**

You cannot use the command-line interface to log in if user authentication is enabled. You must use a browser.

- If you have a default home page on the remote network behind the VPN Concentrator, or direct the browser to a website on the remote network behind the VPN Concentrator, the VPN 3002 directs the browser to the proper pages for user login. When you successfully log in, the browser displays the page you originally entered.
- If you try to access resources on the network behind the VPN Concentrator that are not web-based, for example, email, the connection will fail until you authenticate.
- To authenticate, you must enter the IP address for the private interface of the VPN 3002 in the browser Location or Address field. The browser then displays the login screen for the VPN 3002. To authenticate, click the Connect/Login Status button.
- One user can log in for a maximum of four sessions simultaneously.

Individual users authenticate according to the order of authentication servers that you configure for a group. To configure authentication servers for individual user authentication, see the sections, Configuration | User Management | Base Group/Groups | Authentication Servers | Add/Modify.

Summary of VPN 3002 Authentication Features

Table 14-4 summarizes how authentication of the VPN 3002 works by default, and how it works with interactive hardware client authentication and individual user authentication enabled. Be aware that you can use both interactive hardware client authentication or individual user authentication simultaneously, or either one and not the other.

Table 14-4 Authenticating the VPN 3002 Hardware Client and Users

Authentication with Saved Username and Password	Interactive Hardware Client Authentication	Individual User Authentication
Authenticates the VPN 3002.	Authenticates the VPN 3002.	Authenticates a user or device on the private LAN behind the VPN 3002.
On the VPN 3002, you configure the username and password in either of these screens: <ul style="list-style-type: none"> • Configuration Quick IPSec. • Configuration System Tunneling Protocols IPSec. 	You do not configure the username and password on the VPN 3002.	You do not configure the username and password on the VPN 3002.
The VPN 3002 saves the username and password.	The VPN 3002 does not save the username and password.	The VPN 3002 does not save the username and password.
Requires no user interaction subsequent to initial configuration.	You are prompted to enter a username and password each time the VPN 3002 initiates the tunnel.	You open a web browser and enter a username and password when prompted, even though the tunnel already exists. You cannot use the command-line interface.
The default option.	You enable on the VPN Concentrator. The VPN Concentrator pushes the policy to the VPN 3002.	You enable on the VPN Concentrator. The VPN Concentrator pushes the policy to the VPN 3002.
The VPN 3002 authenticates on the first server of the type that you configure. If the VPN 3002 cannot reach that server, it authenticates on the next server of that type in the list of authentication servers.		Individual users authenticate according to the order of authentication servers configured, regardless of type.
		Individual users can authenticate according to the values of an embedded group rather than the tunnel group. See the next section.

Associating Users with Different Groups for Authentication

When you configure a VPN 3002, you assign it to a group on the VPN Concentrator to which it connects. This is the *tunnel group* to which the VPN 3002 belongs. The attributes of the tunnel group determine how the VPN 3002 authenticates.

For purposes of authentication, you can associate users behind the VPN 3002 with a group other than the tunnel group. You accomplish this by embedding a different group name within the username. To embed this second group name, you configure and use a delimiter, (@, #, or !) that associates the second group with the user. The format to use is *username<delimiter>groupname*, for example, *UserA@bluegroup*.

When you embed a groupname within a username:

- An individual user authenticates according to the priority order of the authentication servers you configure for the group embedded within its username.
- If you use external authentication servers, you have the flexibility of storing usernames and passwords for the VPN 3002 on one server, and those for individual users behind the VPN 3002 on another server or servers.
- Users behind the same VPN 3002 can authenticate to different external servers. You configure this by embedding different groups for various users. For example, *UserA@bluegroup* might authenticate to a RADIUS server, while *UserD@greengroup* authenticates to an SDI server, or to a different RADIUS server.



Note

The VPN 3002 always gets settings for interactive hardware client authentication from the tunnel group, not the embedded group.

Table 14-5 summarizes how UserA, UserB, and UserC connect to the central site through a VPN 3002.

Table 14-5 Example: How Authentication Servers Work Using Embedded Groups

Username	Tunnel Group	Embedded Group	Authentication Server for the VPN 3002	Authentication Server for the Individual User
UserA	bluegroup	None	An authentication server configured for bluegroup.	User A uses an authentication server configured for bluegroup.
UserB@redgroup	bluegroup	redgroup	An authentication server configured for bluegroup.	User B uses an authentication server configured for redgroup.
UserC@greengroup	bluegroup	greengroup	An authentication server configured for bluegroup.	The VPN 3002 authenticates using an authentication server configured for greengroup.

Configuring a Group Delimiter

To configure and use a group delimiter, follow these steps.

-
- Step 1** In the Configuration | System | General | Global Authentication parameters screen on the VPN Concentrator:
- Enable Group Lookup
 - Select a delimiter (@, #, or !).
- Step 2** In the General tab of the Configuration | User Management | Groups | Add/Modify screen, check the Strip Realm box to remove the group name embedded in the username during authentication.
-

To use a second group for individual user authentication, enter the username with the embedded group in the form *username<delimiter>groupname* in the username field in one of these screens:

- In the Monitoring | System Status screen, click the **Connect Now** button. You are prompted for a username and password.
- In the Manager Login screen, click **Connection/Login Status**. If individual user authentication is required, the **Log In Now** prompt displays. When you click that button, you are prompted for a username and password.

Backup Servers with Interactive Hardware Client and Individual User Authentication

Be sure to configure any backup servers for the VPN 3002 with the same values as the primary VPN Concentrator for interactive hardware client authentication and individual user authentication. For information about configuring backup servers, see the section, [Client Configuration Parameters Tab](#), earlier in this chapter.

Accounting with Interactive Hardware Client and Individual User Authentication

If a VPN 3002 authenticates to a VPN Concentrator, and you have enabled accounting, the VPN Concentrator notifies the RADIUS accounting server when the VPN 3002 logs on and off. It also keeps track of individual users. See the section, [Configuration | System | Servers | Accounting](#) of this book.

PPTP/L2TP Parameters Tab

This tab lets you configure PPTP and L2TP parameters that apply to the base group. During tunnel establishment, the client and server negotiate access and usage based on these parameters. Only clients that meet these criteria are allowed access. If you checked PPTP, L2TP, or L2TP over IPsec under Tunneling Protocols on the General Parameters tab, configure these parameters.

Figure 14-8 Configuration | User Management | Base Group Screen, PPTP/L2TP Tab

Configuration User Management Base Group		
PPTP/L2TP Parameters		
Attribute	Value	Description
Use Client Address	<input type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2 <input type="checkbox"/> EAP Proxy	Check the authentication protocols allowed. Refer to the online help for authentication protocol dependencies. Unchecking all options means that no authentication is required.
PPTP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	Select the allowed encryption methods for PPTP connections for this group.
PPTP Compression	<input type="checkbox"/>	Check to enable MPPC compression for PPTP connections for this group.
L2TP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2 <input type="checkbox"/> EAP Proxy	Check the authentication protocols allowed. Refer to the online help for authentication protocol dependencies. Unchecking all options means that no authentication is required.
L2TP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	Select the allowed encryption methods for L2TP connections for this group.
L2TP Compression	<input type="checkbox"/>	Check to enable MPPC compression for L2TP connections for this group.

Apply Cancel

79358

Use Client Address

Check the **Use Client Address** check box to accept and use an IP address that the client supplies. A client must have an IP address to function as a tunnel endpoint; but for maximum security, we recommend that you control IP address assignment and that you do not allow client-supplied IP addresses (the default).

Make sure the setting here is consistent with the setting for Use Client Address on the Configuration | System | Address Management | Assignment screen.

PPTP Authentication Protocols

Check the **PPTP Authentication Protocols** check boxes for the authentication protocols that PPTP clients can use. To establish and use a VPN tunnel, users should be authenticated in accordance with a protocol.



Caution

Unchecking *all* authentication options means that *no* authentication is required. That is, PPTP users can connect with *no* authentication. This configuration is allowed so you can test connections, but it is not secure.

These choices specify the allowable authentication protocols in order from least secure to most secure.

- **PAP = Password Authentication Protocol.** This protocol passes cleartext username and password during authentication and is not secure. We strongly recommend that you not allow this protocol (the default).
- **CHAP = Challenge-Handshake Authentication Protocol.** In response to the server challenge, the client returns the encrypted [challenge plus password], with a cleartext username. It is more secure than PAP, but it does not encrypt data. It is allowed by default.
- **MSCHAPv1 = Microsoft Challenge-Handshake Authentication Protocol version 1.** This protocol is similar to, but more secure than, CHAP. In response to the server challenge, the client returns the encrypted [challenge plus encrypted password], with a cleartext username. Thus the server stores, and compares, only encrypted passwords, rather than cleartext passwords as in CHAP. This protocol also generates a key for data encryption by MPPE (Microsoft Point-to-Point Encryption). This protocol is allowed by default. If you check Required under PPTP Encryption, you must allow one or both MSCHAP protocols and no other.
- **MSCHAPv2 = Microsoft Challenge-Handshake Authentication Protocol version 2.** This protocol is even more secure than MSCHAPv1. It requires mutual client-server authentication, uses session-unique keys for data encryption by MPPE, and derives different encryption keys for the send and receive paths. This protocol is not allowed by default. The VPN Concentrator internal user authentication server supports this protocol, but external authentication servers do not. If you check Required under PPTP Encryption, you must allow one or both MSCHAP protocols and no other.
- **EAP Proxy = Extensible Authentication Protocol, defined in RFC 2284.** EAP enables the VPN Concentrator to proxy the entire PPTP/L2TP authentication process to an external RADIUS authentication server. It provides additional authentication options for the Microsoft VPN Client (L2TP/IPSec), including EAP/MD5, Smartcards and certificates (EAP/TLS), and RSA SecurID (EAP/SDI). It requires that you configure an EAP enabled RADIUS server. You cannot configure EAP if you are using encryption. It is configurable at the base group or group levels.

PPTP Encryption

Check the **PPTP Encryption** check boxes for the data encryption options that apply to PPTP clients.

- **Required** = During connection setup, PPTP clients must agree to use Microsoft encryption (MPPE) to encrypt data or they will not be connected. This option is unchecked by default. If you check this option, you must also allow only MSCHAPv1 and/or MSCHAPv2 under PPTP Authentication Protocols, and you must also check 40-bit and/or 128-bit here. Do not check this option if you use NT Domain user authentication; NT Domain authentication cannot negotiate encryption.
- **Require Stateless** = During connection setup, PPTP clients must agree to use stateless encryption to encrypt data or they will not be connected. With stateless encryption, the encryption keys are changed on every packet; otherwise, the keys are changed after some number of packets or whenever a packet is lost. Stateless encryption is more secure, but it requires more processing. However, it might perform better in a lossy environment (where packets are lost), such as the Internet. This option is not checked by default. Do not check this option if you use NT Domain user authentication; NT Domain authentication cannot negotiate encryption.
- **40-bit** = PPTP clients are allowed to use the RSA RC4 encryption algorithm with a 40-bit key. This is significantly less secure than the 128-bit option. Microsoft encryption (MPPE) uses this algorithm. This option is checked by default. If you check **Required**, you must check this option and/or the 128-bit option.
- **128-bit** = PPTP clients are allowed to use the RSA RC4 encryption algorithm with a 128-bit key. Microsoft encryption (MPPE) uses this algorithm. This option is checked by default. If you check **Required**, you must check this option and/or the 40-bit option. The U.S. government restricts the distribution of 128-bit encryption software.

PPTP Compression

If all members of this group are remote dial-in users connecting with modems, enabling data compression might speed up their data transmission rates. Data compression shrinks data by replacing repeating information with symbols that use less space. Check the box to enable data compression for PPTP. PPTP data compression uses the Microsoft Point to Point Compression (MPPC) protocol.

**Note**

MPPC data compression increases the memory requirement and CPU utilization for each user session. Consequently, using data compression reduces the overall throughput of the VPN Concentrator and lowers the maximum number of sessions your VPN Concentrator can support. *We recommend you enable data compression only if every member of the group is a remote user connecting with a modem.* If any members of the group connect via broadband, do not enable data compression for the group. Instead, divide the group into two groups, one for modem users and the other for broadband users. Enable data compression only for the group of modem users.

**Note**

PPTP data compression is only supported for clients that use stateless encryption.

L2TP Authentication Protocols

Check the **L2TP Authentication Protocols** check boxes for the authentication protocols that L2TP clients can use. To establish and use a VPN tunnel, users should be authenticated in accordance with a protocol.



Caution

Unchecking *all* authentication options means that *no* authentication is required. That is, L2TP users can connect with *no* authentication. This configuration is allowed so you can test connections, but it is not secure.

These choices specify the allowable authentication protocols in order from least secure to most secure.

- **PAP = Password Authentication Protocol.** This protocol passes cleartext username and password during authentication and is not secure. We strongly recommend that you not allow this protocol (the default).
- **CHAP = Challenge-Handshake Authentication Protocol.** In response to the server challenge, the client returns the encrypted [challenge plus password], with a cleartext username. It is more secure than PAP, but does not encrypt data. It is allowed by default.
- **MSCHAPv1 = Microsoft Challenge-Handshake Authentication Protocol version 1.** This protocol is similar to, but more secure than, CHAP. In response to the server challenge, the client returns the encrypted [challenge plus encrypted password], with a cleartext username. Thus the server stores—and compares—only encrypted passwords, rather than cleartext passwords as in CHAP. This protocol also generates a key for data encryption by MPPE (Microsoft Point-to-Point Encryption). This protocol is allowed by default. If you check Required under L2TP Encryption, you must allow one or both MSCHAP protocols and no other.
- **MSCHAPv2 = Microsoft Challenge-Handshake Authentication Protocol version 2.** This protocol is even more secure than MSCHAPv1. It requires mutual client-server authentication, uses session-unique keys for data encryption by MPPE, and derives different encryption keys for the send and receive paths. This protocol is not allowed by default. The VPN Concentrator internal user authentication server supports this protocol, but external authentication servers do not. If you check Required under L2TP Encryption, you must allow one or both MSCHAP protocols and no other.
- **EAP Proxy = Extensible Authentication Protocol, defined in RFC 2284.** EAP enables the VPN Concentrator to proxy the entire PPTP/L2TP authentication process to an external RADIUS authentication server. It provides additional authentication options for the Microsoft VPN Client (L2TP/IPSec), including EAP/MD5, Smartcards and certificates (EAP/TLS), and RSA SecurID (EAP/SDI). It requires that you configure an EAP enabled RADIUS server. You cannot configure EAP if you are using encryption. It is configurable at the base group or group levels.

L2TP Encryption

Check the **L2TP Encryption** check boxes for the data encryption options that apply to L2TP clients.

- **Required** = During connection setup, L2TP clients must agree to use Microsoft encryption (MPPE) to encrypt data or they will not be connected. This option is unchecked by default. If you check this option, you must also allow only MSCHAPv1 and/or MSCHAPv2 under L2TP Authentication Protocols, and you must also check 40-bit and/or 128-bit here. Do not check this option if you use NT Domain user authentication; NT Domain authentication cannot negotiate encryption.
- **Require Stateless** = During connection setup, L2TP clients must agree to use stateless encryption to encrypt data or they will not be connected. With stateless encryption, the encryption keys are changed on every packet; otherwise, the keys are changed after some number of packets or whenever a packet is lost. Stateless encryption is more secure, but it requires more processing. However, it might perform better in a lossy environment (where packets are lost), such as the Internet. This option is unchecked by default. Do not check this option if you use NT Domain user authentication; NT Domain authentication cannot negotiate encryption.
- **40-bit** = L2TP clients are allowed to use the RSA RC4 encryption algorithm with a 40-bit key. This is significantly less secure than the 128-bit option. Microsoft encryption (MPPE) uses this algorithm. This option is unchecked by default. If you check Required, you must check this option and/or the 128-bit option.
- **128-bit** = L2TP clients are allowed to use the RSA RC4 encryption algorithm with a 128-bit key. Microsoft encryption (MPPE) uses this algorithm. This option is unchecked by default. If you check Required, you must check this option and/or the 40-bit option.

L2TP Compression

If all members of this group are remote dial-in users connecting with modems, enabling data compression might speed up their data transmission rates. Data compression shrinks data by replacing repeating information with symbols that use less space. Check the L2TP Compression check box to enable data compression for L2TP. L2TP data compression uses the Microsoft Point to Point Compression (MPPC) protocol.

**Note**

MPPC data compression increases the memory requirement and CPU utilization for each user session. Consequently, using data compression reduces the overall throughput of the VPN Concentrator and lowers the maximum number of sessions your VPN Concentrator can support. *We recommend you enable data compression only if every member of the group is a remote user connecting with a modem.* If any members of the group connect via broadband, do not enable data compression for the group. Instead, divide the group into two groups, one for modem users and the other for broadband users. Enable data compression only for the group of modem users.

**Note**

L2TP data compression is only supported for clients that use stateless encryption.

Apply / Cancel

When you finish setting base-group parameters on all tabs, click **Apply** at the bottom of the screen to include your settings in the active configuration. The Manager returns to the Configuration | User Management screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | User Management screen.

Configuration | User Management | Groups

This section of the Manager lets you configure access and usage parameters for specific groups. A group is a collection of users treated as a single entity. Groups inherit parameters from the base group.

For information on groups and users, see the section: [User Management](#)

Configuring internal groups in this section means configuring them on the VPN Concentrator internal authentication server. The system automatically configures the internal server when you add the first internal group.

Configuring external groups means configuring them on an external authentication server such as RADIUS.



Note

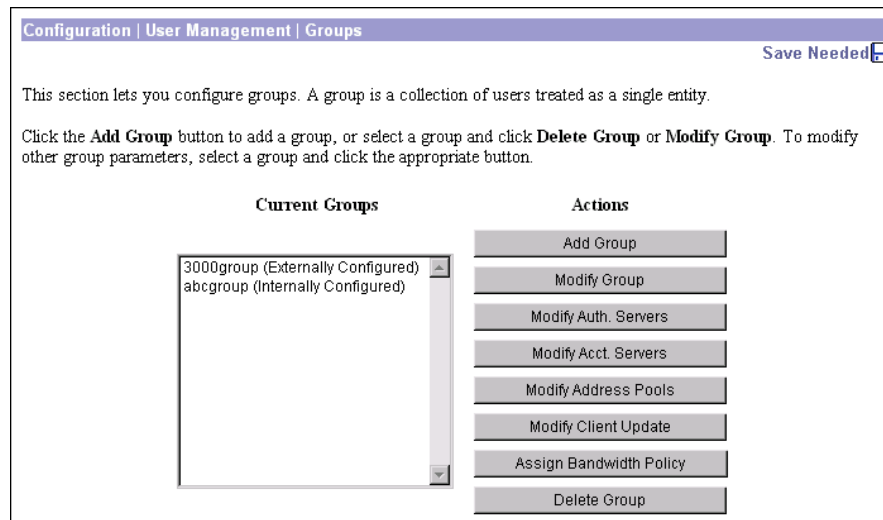
If a RADIUS server is configured to return the Class attribute (#25), the VPN Concentrator uses that attribute to authenticate the Group Name. On the RADIUS server, the attribute must be formatted as: *OU=groupname*; where *groupname* is identical to the Group Name configured on the VPN Concentrator. For example:
OU=Finance;



Note

If you are using an external authentication server, keep in mind that user names and group names must be unique. When naming a group, do not pick a name that matches the name of any external user; and conversely, when assigning a name to an external user, do not choose the name of any existing group.

Figure 14-9 Configuration | User Management | Groups Screen



Current Groups

The Current Groups list shows configured groups in alphabetical order, and if they are internal or external. If no groups have been configured, the list shows --Empty--.

Actions

To configure and add a new group, click **Add Group**. The Manager opens the Configuration | User Management | Groups | Add screen.

To modify parameters for a group that has been configured, select the group from the list and click **Modify Group**. The Manager opens the appropriate internal or external Configuration | User Management | Groups | Modify screen.

To modify authentication server parameters, select the group from the list and click **Modify Auth. Servers**. The Manager opens the Configuration | User Management | Groups | Authentication Servers screen.

To modify accounting server parameters, select the group from the list and click **Modify Acct. Servers**. The Manager opens the Configuration | User Management | Groups | Accounting Servers screen.

To modify address pools, select the group from the list and click **Modify Address Pools**. The Manager opens the Configuration | User Management | Groups | Address Pools screen.

To modify client update entries, select the group from the list and click **Modify Client Update**. The Manager opens the Configuration | User Management | Groups | Client Update screen.

To assign a bandwidth management policy, select the group from the list and click **Assign Bandwidth Policy**. The Manager opens the Configuration | User Management | Groups | Bandwidth Policy screen.

To remove a group that has been configured, select the group from the list and click **Delete Group**.



Note

There is no confirmation or undo. However, deleting a group that has certificate group matching rules defined for it also deletes these rules. In this case, the VPN Concentrator displays a warning message asking you to confirm that you really want to delete the group.

The Manager refreshes the screen and shows the remaining groups in the list. *When you delete a group, all its members revert to the base group.* Deleting a group, however, does not delete the user profiles of the members.

You cannot delete a group that is configured as part of a LAN-to-LAN connection. See the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done screen.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | User Management | Groups | Add or Modify (Internal)

These screens let you:

- Add: Configure and add a new group.
- Modify: Change parameters for a group that you have previously configured on the internal server. The screen title identifies the group you are modifying.

For many of these parameters, you can simply specify that the group “inherit” parameters from the base group, which you should configure first. You can also override the base-group parameters as you configure groups. See the Configuration | User Management | Base Group screen.

On this screen, you configure the following kinds of parameters:

- Identity Parameters: Name, password, and type.
- General Parameters: Security, access, performance, and protocols.
- IPSec Parameters: IP Security tunneling protocol.
- Mode Config Parameters: Banner, password storage, split-tunneling policy, default domain name, IPSec over UDP, backup servers.
- Client FW Parameters: VPN Client personal firewall requirements.
- HW Client Parameters: Interactive hardware client authentication and individual user authentication.
- PPTP/L2TP Parameters: PPTP and L2TP tunneling protocols.

Using the Tabs

This screen includes four tabbed sections. Click each tab to display its parameters. As you move from tab to tab, the Manager retains your settings. When you have finished setting parameters on all tabbed sections, click **Add/Apply** or **Cancel**.

Identity Parameters Tab

This tab lets you configure the name, password, and authentication server type for this group.

Figure 14-10 Configuration | User Management | Groups | Add or Modify (Internal) Screen, Identity Tab

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity General IPSec Client Config Client FW HW Client PPTP/L2TP

Identity Parameters		
Attribute	Value	Description
Group Name	<input type="text"/>	Enter a unique name for the group.
Password	<input type="password"/>	Enter the password for the group.
Verify	<input type="password"/>	Verify the group's password.
Type	Internal ▾	External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.

Add Cancel

79340

Group Name

Enter a unique name for this specific group. The name cannot match any existing user or group name. (If you are using an external authentication server, see the note about naming [on page 14-41](#).)

The maximum name length is 64 characters. Entries are case-sensitive. Changing a group name automatically updates the group name for all users in the group.

If you are setting up a group for remote access users connecting with digital certificates, first find out the value of the Organizational Unit (OU) field of the user's identity certificate. (Ask your certificate administrator for this information.) The group name you assign must match this value exactly. If some users in the group have different OU values, set up a different group for each of these users.

If the Group Name field configured here and the OU field of the user's identity certificate do not match, when the user attempts to connect, the VPN Concentrator considers the user to be a member of the base group. The base group parameter definitions might be configured differently than the user wants or expects. If the base group does not support digital certificates, the connection fails.

See the note about configuring the RADIUS Class attribute under "[Configuration | User Management | Groups](#)".

Password

Enter a unique password for this group. The minimum password length is 4 characters. The maximum is 32 characters. Entries are case-sensitive. The field displays only asterisks.

Verify

Re-enter the group password to verify it. The field displays only asterisks.

Type

Click the **Type** drop-down menu button and select the authentication server type (authentication method) for this group:

- Internal = Use the internal VPN Concentrator authentication server. This is the default selection. If you select this type, configure the parameters on the other tabs on this screen. The VPN Concentrator automatically configures its internal server when you add the first internal group.
- External = Use an external authentication server, such as RADIUS, for this group. If you select this type, *ignore the rest of the tabs and parameters on this screen*. The external server supplies the group parameters if it can; otherwise the base-group parameters apply.

General Parameters Tab

This tab lets you configure general security, access, performance, and tunneling protocol parameters that apply to this internally configured group.

Figure 14-11 Configuration | User Management | Groups | Add or Modify (Internal) Screen, General Tab

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | **General** | IPsec | Client Config | Client FW | HW Client | PPTP/L2TP

General Parameters			
Attribute	Value	Inherit?	Description
Access Hours	No Restrictions	<input checked="" type="checkbox"/>	Select the access hours assigned to this group.
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	<input checked="" type="checkbox"/>	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this group.
Filter	-None-	<input checked="" type="checkbox"/>	Enter the filter assigned to this group.
Primary DNS		<input checked="" type="checkbox"/>	Enter the IP address of the primary DNS server.
Secondary DNS		<input checked="" type="checkbox"/>	Enter the IP address of the secondary DNS server.
Primary WINS		<input checked="" type="checkbox"/>	Enter the IP address of the primary WINS server.
Secondary WINS		<input checked="" type="checkbox"/>	Enter the IP address of the secondary WINS server.
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	<input checked="" type="checkbox"/>	Select the SEP cards this group can be assigned to.
Tunneling Protocols	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec	<input checked="" type="checkbox"/>	Select the tunneling protocols this group can connect with.
Strip Realm	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to remove the realm qualifier of the user name during authentication.

Add Cancel

783335

Value / Inherit?

On this tabbed section:

- The **Inherit?** check box refers to base-group parameters: Does this specific group inherit the given setting from the base group? To inherit the setting, check the box (default). To override the base-group setting, uncheck the check box. If you uncheck the check box, you must also enter or change any corresponding **Value** field; do not leave the field blank.
- The **Value** column thus shows either base-group parameter settings that also apply to this group (**Inherit?** checked), or unique parameter settings configured for this group (**Inherit?** cleared).

**Note**

The setting of the **Inherit?** check box takes priority over an entry in a **Value** field. Examine this box before continuing and be sure its setting reflects your intent.

Access Hours

Click the **Access Hours** drop-down menu button and select the named hours when this group's remote-access users can access the VPN Concentrator. Configure access hours on the Configuration | Policy Management | Access Hours screen. Default entries are:

- **-No Restrictions-** = No named access hours applied, which means that there are no restrictions on access hours.
- **Never** = No access at any time.
- **Business Hours** = Access 9 a.m. to 5 p.m., Monday through Friday.

Additional named access hours that you have configured also appear on the list.

Simultaneous Logins

Enter the number of simultaneous logins permitted for a single internal user in this group. The minimum is 0, which disables login and prevents user access. While there is no maximum limit, allowing several could compromise security and affect performance.

Minimum Password Length

Enter the minimum number of characters for this group's user passwords. The minimum is 1, and the maximum is 32. To protect security, we strongly recommend 8 or higher.

Allow Alphabetic-Only Passwords

Check the **Allow Alphabetic-Only Passwords** check box to allow this group's user passwords with alphabetic characters only. This option applies only to users who are configured in and authenticated by the VPN Concentrator internal authentication server. To protect security, we strongly recommend that you not allow such passwords. Require passwords to be a mix of alphabetic characters, numbers, and symbols, such as 648e&9G#.

Idle Timeout

Enter the group's idle timeout period in minutes. If there is no communication activity on a user connection in this period, the system terminates the connection. The minimum is 1, and the maximum is 2147483647 minutes (over 4000 years). To disable timeout and allow an unlimited idle period, enter 0.

Maximum Connect Time

Enter the group's maximum user connection time in minutes. At the end of this time, the system terminates the connection. The minimum is 1, and the maximum is 2147483647 minutes (over 4000 years). To allow unlimited connection time, enter 0.

Filter

Filters consist of rules that determine whether to allow or reject tunneled data packets coming through the VPN Concentrator, based on criteria such as source address, destination address, and protocol. Cisco supplies three default filters, which you can modify. To configure filters and rules, see the Configuration | Policy Management | Traffic Management screens.

Click the **Filter** drop-down menu button and select the filter to apply to this group's users:

- --None-- = No filter applied, which means there are no restrictions on tunneled data traffic.
- Private (Default) = Allow all packets except source-routed IP packets. (This is the default filter for the private Ethernet interface.)
- Public (Default) = Allow inbound and outbound tunneling protocols plus ICMP and VRRP. Allow fragmented IP packets. Drop everything else, including source-routed packets. (This is the default filter for the public Ethernet interface.)
- External (Default) = No rules applied to this filter. Drop all packets. (This is the default filter for the external Ethernet interface.)

Additional filters that you have configured also appear on the list.

Note on DNS and WINS Entries:

If the base group uses DNS or WINS, and:

- this group uses the base-group setting: check the appropriate **Inherit?** box (the default).
- this group uses different DNS or WINS servers: uncheck the appropriate **Inherit?** check box and enter this group's server IP address(es).
- this group does not use DNS or WINS: uncheck the appropriate **Inherit?** check box and enter 0.0.0.0 in the IP address field.

If the base group does not use DNS or WINS, and:

- this group also does not use DNS or WINS: check the appropriate **Inherit?** check box (the default).
- this group uses DNS or WINS: uncheck the appropriate **Inherit?** check box and enter this group's server IP address(es).

Primary DNS

Enter the IP address, in dotted decimal notation, of the primary DNS server for this group's users. The system sends this address to the client as the first DNS server to use for resolving host names. See the preceding note.

Secondary DNS

Enter the IP address, in dotted decimal notation, of the secondary DNS server for this group's users. The system sends this address to the client as the second DNS server to use for resolving host names. See the preceding note.

Primary WINS

Enter the IP address, in dotted decimal notation, of the primary WINS server for this group's users. The system sends this address to the client as the first WINS server to use for resolving host names under Windows NT. See the preceding note.

Secondary WINS

Enter the IP address, in dotted decimal notation, of the secondary WINS server for this group's users. The system sends this address to the client as the second WINS server to use for resolving host names under Windows NT. See the preceding note.

SEP Card Assignment

The VPN Concentrator can contain up to four SEP (Scalable Encryption Processing) modules that handle encryption functions, which are compute-intensive. Two SEP modules handle up to 5000 sessions (users)—the system maximum. Two additional modules can provide automatic failover for the first two. This parameter lets you configure the load on each SEP module.

Check the **SEP Card Assignment** check box to assign this group's load to a given SEP module. If your system does not have a given SEP module, the parameter is ignored.

Tunneling Protocols

Check the desired **Tunneling Protocols** check boxes to select the VPN tunneling protocols that this group's user clients can use. Configure parameters on the IPsec or PPTP/L2TP tabs as appropriate. Clients can use only the selected protocols.

You cannot check both IPsec and L2TP over IPsec. The IPsec parameters differ for these two protocols, and you cannot configure a single group for both.

- PPTP = Point-to-Point Tunneling Protocol. PPTP is a client-server protocol, and it is popular with Microsoft clients. Microsoft Dial-Up Networking (DUN) 1.2 and 1.3 under Windows 95/98 support it, as do versions of Windows NT 4.0 and Windows 2000.
- L2TP = Layer 2 Tunneling Protocol. L2TP is a client-server protocol. It combines many features from PPTP and L2F (Layer 2 Forwarding).
- IPsec = IP Security Protocol. IPsec provides the most complete architecture for VPN tunnels, and it is perceived as the most secure protocol. Both LAN-to-LAN (peer-to-peer) connections and client-to-LAN connections can use IPsec. The Cisco VPN Client is an IPsec client specifically designed to work with the VPN Concentrator. However, the VPN Concentrator can establish IPsec connections with many protocol-compliant clients.
- L2TP over IPsec = L2TP using IPsec for security. L2TP packets are encapsulated within IPsec, thus providing an additional authentication and encryption layer for security. L2TP over IPsec is a client-server protocol that provides interoperability with the Windows 2000 VPN client. It is also compliant, but not officially supported, with other remote-access clients.



Note

If no protocol is selected, none of the client users in this group can access or use the VPN.

Strip Realm

Check the **Strip Realm** check box to remove the realm qualifier of the user name during authentication. If you check this Strip Realm box, authentication is based on the *username* alone. Otherwise, authentication is based on the full *username@realm* string. You must check this box if your server is unable to parse delimiters.

IPSec Parameters Tab

This tab lets you configure IP Security Protocol parameters that apply to this internally configured group. If you checked IPsec or L2TP over IPsec under Tunneling Protocols on the General Parameters tab, configure this section.

Figure 14-12 Configuration | User Management | Groups | Add or Modify (Internal) Screen, IPSec Tab

IPSec Parameters			
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	<input checked="" type="checkbox"/>	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	<input checked="" type="checkbox"/>	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable the use of IKE keepalives for members of this group.
Tunnel Type	Remote Access	<input checked="" type="checkbox"/>	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.
Remote Access Parameters			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into this group.
Authentication	Internal	<input checked="" type="checkbox"/>	Select the authentication method for members of this group. This parameter does not apply to Individual User Authentication .
IPComp	None	<input checked="" type="checkbox"/>	Select the method of IP Compression for members of this group.
Reauthentication on Rekey	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Mode Configuration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to initiate the exchange of Mode Configuration parameters with the client. This must be checked if version 2.5 (or earlier) of the Altiga/Cisco client is being used by members of this group.

Add Cancel

79337

Value / Inherit?

On this tabbed section:

- The Inherit? check box refers to base-group parameters: Does this specific group inherit the given setting from the base group? To inherit the setting, check the box (default). To override the base-group setting, uncheck the check box. If you uncheck the check box, you must also enter or change any corresponding Value field; do not leave the field blank.
- The Value column thus shows either base-group parameter settings that also apply to this group (Inherit? checked), or unique parameter settings configured for this group (Inherit? cleared).



Note

The setting of the Inherit? check box takes priority over an entry in a Value field. Examine this box before continuing and be sure its setting reflects your intent.

IPSec SA

Click the **IPSec SA** drop-down menu button and select the IPSec Security Association (SA) assigned to this group's IPSec clients. During tunnel establishment, the client and server negotiate a Security Association that governs authentication, encryption, encapsulation, key management, etc. You configure IPSec Security Associations on the Configuration | Policy Management | Traffic Management | Security Associations screens.

To use IPSec with remote-access clients, you must assign an SA. With IPSec LAN-to-LAN connections, the system ignores this selection and uses parameters from the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN screens.

The VPN Concentrator supplies these default selections:

- --None-- = No SA assigned.
- ESP-DES-MD5 = This SA uses DES 56-bit data encryption for both the IKE tunnel and IPSec traffic, ESP/MD5/HMAC-128 authentication for IPSec traffic, and MD5/HMAC-128 authentication for the IKE tunnel.
- ESP-3DES-MD5 = This SA uses Triple-DES 168-bit data encryption and ESP/MD5/HMAC-128 authentication for IPSec traffic, and DES-56 encryption and MD5/HMAC-128 authentication for the IKE tunnel.
- ESP/IKE-3DES-MD5 = This SA uses Triple-DES 168-bit data encryption for both the IKE tunnel and IPSec traffic, ESP/MD5/HMAC-128 authentication for IPSec traffic, and MD5/HMAC-128 authentication for the IKE tunnel.
- ESP-3DES-NONE = This SA uses Triple-DES 168-bit data encryption and no authentication for IPSec traffic, and DES-56 encryption and MD5/HMAC-128 authentication for the IKE tunnel.
- ESP-L2TP-TRANSPORT = This SA uses DES 56-bit data encryption and ESP/MD5/HMAC-128 authentication for IPSec traffic (with ESP applied only to the transport layer segment), and it uses Triple-DES 168-bit data encryption and MD5/HMAC-128 for the IKE tunnel. Use this SA with the L2TP over IPSec tunneling protocol.
- ESP-3DES-MD5-DH7 = This SA uses Triple-DES 168-bit data encryption and ESP/MD5/HMAC-128 authentication for both IPSec traffic and the IKE tunnel. It uses Diffie-Hellman Group 7 (ECC) to negotiate Perfect Forward Secrecy. This option is intended for use with the movianVPN client, but you can use it with other clients that support D-H Group 7 (ECC).

Additional SAs that you have configured also appear on the list.

IKE Peer Identity Validation

Click the **IKE Peer Identity Validation** drop-down menu button, and choose the type of peer identity validation.

**Note**

This option applies only to tunnel negotiations based on certificates.

During IKE tunnel establishment, the peer provides its identity: either an IP address, a fully qualified domain name (FQDN), or a distinguished name (DN). It also presents a certificate, which contains none, some, or all of these fields. If IKE peer identity validation is enabled, the VPN Concentrator compares the peer's identity to the like field in the certificate to see if the information matches. If the information matches, then the peer's identity is validated and the VPN Concentrator establishes the tunnel. If the information does not match, the VPN Concentrator drops the tunnel. This feature provides additional security.

IKE peer identity validation can be useful for binding a peer to a particular IP address or domain name. For example, if the IP address that the peer provided as an identification during tunnel establishment does not match the IP address in its certificate, the VPN Concentrator fails to validate the peer and drops the tunnel.

Ideally all VPN Concentrator peers are configured to provide matching types of identity and certificate fields. In this case, enabling peer identity validation ensures that the VPN Concentrator checks the validity of every peer, and only validated peers connect. But in actuality, some peers might not be configured to provide this data. Some peers might provide certificates that do not contain any of the matching fields required for an identity check. If a peer does not provide sufficient information for the VPN Concentrator to check its identity, there are two possibilities: the VPN Concentrator either establishes the session or drops it. If you want the VPN Concentrator to drop sessions of peers that do not provide sufficient information to perform an identity check, choose **Required**. If you want the VPN Concentrator to establish sessions for peers that do not provide sufficient identity information to perform a check, select **If supported by Certificate**.

- **Required** = Enable the IKE peer identity validation feature. If a peer's certificate does not provide sufficient information to perform an identity check, drop the tunnel.
- **If supported by certificate** = Enable the IKE peer identity validation feature. If a peer's certificate does not provide sufficient information to perform an identity check, allow the tunnel.
- **Do not check** = Do not check the peer's identity at all. Selecting this option disables the feature.

IKE Keepalives

Check the **IKE Keepalives** check box to enable IKE keepalives. (IKE keepalives is enabled by default.) This feature lets the VPN Concentrator monitor the continued presence of a remote peer and to report its own presence to that peer. If the peer becomes unresponsive, the VPN Concentrator removes the connection. Enabling IKE keepalives prevents hung connections when the IKE peer loses connectivity.

There are various forms of IKE keepalives. For this feature to work, both the VPN Concentrator and its remote peer must support a common form. This feature works with the following peers:

- Cisco VPN Client (Release 3.0 or later)
- Cisco VPN 3000 Client (Release 2.x)
- Cisco VPN 3002 Hardware Client
- Cisco VPN 3000 Series Concentrators
- Cisco IOS software
- Cisco Secure PIX Firewall

Non-Cisco VPN clients do not support IKE keepalives.

If you are configuring a group of mixed peers, and some of those peers support IKE keepalives and others do not, enable IKE keepalives for the entire group. The feature does not affect the peers that do not support it.

If you disable IKE keepalives, connections with unresponsive peers remain active until they time out, so we recommend you keep your idle timeout short. To change your idle timeout, see the Configuration | User Management | Groups | Add screen, General tab.



Note

To reduce connectivity costs, disable IKE keepalives if this group includes any clients connecting via ISDN lines. ISDN connections normally disconnect if idle, but the IKE keepalives mechanism prevents connections from idling and therefore from disconnecting.



Note

If you have a LAN-to-LAN configuration using IKE main mode, make sure the two peers have the same IKE keepalives configuration: both must have IKE keepalives enabled or both must have it disabled.

Tunnel Type

Click the **Tunnel Type** drop-down menu button and select the type of IPSec tunnel that this group's clients use:

- LAN-to-LAN = IPSec LAN-to-LAN connections between two VPN Concentrators (or between a VPN Concentrator and another protocol-compliant security gateway). See Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN. If you select this type, ignore the rest of the parameters on this tab.
- Remote Access = Remote IPSec client connections to the VPN Concentrator. If you select this type, configure Remote Access Parameters.

Remote Access Parameters

These group parameters apply to remote-access IPSec client connections only. If you select Remote Access for Tunnel Type, configure these parameters.

Group Lock

Check the **Group Lock** check box to restrict users to remote access through this group only. The IPSec client connects to the VPN Concentrator via a group name and password, and then the system authenticates a user via a username and password. If this box is unchecked, the system authenticates a user without regard to the user's assigned group.

Authentication

Whenever a VPN software or VPN 3002 hardware client attempts a tunneled connection to a network behind a VPN Concentrator, that client is authenticated by means of a username and password. This authentication occurs when the tunnel initiates, and is the authentication type for interactive hardware client authentication for the VPN 3002. This parameter does not apply to individual user authentication for the VPN 3002.

Click the **Authentication** drop-down menu button and select the user authentication method (authentication server type) to use with this group's remote-access IPSec clients. Both VPN Clients and VPN 3002 hardware clients authenticate on the first server of the type you configure.

This selection identifies the authentication *method*, not the specific server. Configure authentication servers on the Configuration | System | Servers | Authentication screens or Configuration | User Management | Groups | Authentication Servers screens.

For the VPN 3002, this selection applies to authentication using a saved username and password and to interactive hardware client authentication. Individual users behind the VPN 3002 authenticate according to the priority order of all authentication servers configured, regardless of type. For more information on the different ways in which a VPN 3002 can authenticate, see the section, "[HW Client Parameters Tab](#)."



Note

To configure user-based authentication for Cisco VPN Clients, choose an Authentication option, then follow the additional steps outlined under Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add, Modify, or Copy. You do this in all cases, regardless of whether you enable interactive hardware client authentication or individual user authentication.

Selecting any authentication method (other than None) enables ISAKMP Extended Authentication, also known as XAUTH.

- None = No IPSec user authentication method. If you checked L2TP over IPSec under Tunneling Protocols, use this selection.
- RADIUS = Authenticate users via external RADIUS server.
- RADIUS with Expiry = Authenticate users via external RADIUS server. If the password has expired, notify the user and offer the opportunity to create a new password.
- NT Domain = Authenticate users via external Windows NT Domain system.
- SDI = Authenticate users via external RSA Security Inc. SecureID system.
- Internal = Authenticate users via internal VPN Concentrator authentication server.

IPComp

If all members of this group are remote dial-in users connecting with modems, enabling data compression might speed up their data transmission rates. Data compression shrinks data by replacing repeating information with symbols that use less space. Click the **IPComp** drop-down menu button to enable data compression using IPComp.

- None = No data compression.
- LZS = Enable data compression using the LZS compression algorithm.



Note

Data compression increases the memory requirement and CPU utilization for each user session and consequently decreases the overall throughput of the VPN Concentrator. For this reason, we recommend you enable data compression only if every member of the group is a remote user connecting with a modem. If any members of the group connect via broadband, do not enable data compression for the group. Instead, divide the group into two groups, one for modem users and the other for broadband users. Enable data compression only for the group of modem users.

Reauthentication on Rekey

Check the **Reauthentication on Rekey** check box to enable reauthentication, or uncheck it to disable it.

The VPN Concentrator prompts the user to enter an ID and password during Phase 1 IKE negotiations. If you enable reauthentication, the VPN Concentrator also prompts for user authentication whenever a rekey occurs. Reauthentication provides additional security.

If the configured rekey interval is very short, users might find the repeated authorization requests inconvenient. In this case, disable reauthentication. (To check your VPN Concentrator's configured rekey interval, see the Lifetime Measurement, Data Lifetime, and Time Lifetime fields on the Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add or Modify screen.)

Mode Configuration

Check the **Mode Configuration** check box to use Mode Configuration with this group's IPSec clients (also known as the ISAKMP Configuration Method or Configuration Transaction). This option exchanges configuration parameters with the client while negotiating Security Associations. If you check this box, configure the desired Mode Configuration Parameters; otherwise, ignore them.

To use split tunneling, you must check this box.

If you checked L2TP over IPSec under Tunneling Protocols, *do not* check this box.



Note

IPSec uses Mode Configuration to pass *all* configuration parameters to a client: IP address, DNS and WINS addresses, etc. You must check this box to use Mode Configuration. Otherwise, those parameters—even if configured with entries—are not passed to the client.



Note

The Cisco VPN Client (IPSec client) supports Mode Configuration, but other IPSec clients might not. For example, the Microsoft Windows 2000 IPSec client does *not* support Mode Configuration. (The Windows 2000 client uses the PPP layer above L2TP to receive its IP address from the VPN Concentrator.) Determine compatibility before using this option with other vendors' clients.

Client Configuration Parameters Tab

These parameters apply to this group’s IPsec clients. It has three sections: one for parameters specific to Cisco clients, one for Microsoft clients, and a third for common client parameters.

Figure 14-13 Configuration | User Management | Groups | Add or Modify, Client Configuration Parameters Tab

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPsec | Client Config | Client FW | HW Client | PPTP/L2TP

Client Configuration Parameters

Cisco Client Parameters

Attribute	Value	Inherit?	Description
Banner	<input type="text"/>	<input checked="" type="checkbox"/>	Enter the banner for this group. Only software clients see the banner.
Allow Password Storage on Client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow the IPsec client to store the password locally.
IPsec over UDP	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow a client to operate through a NAT device using UDP encapsulation of ESP.
IPsec over UDP Port	<input type="text" value="10000"/>	<input checked="" type="checkbox"/>	Enter the UDP port to be used for IPsec through NAT (4001 - 49151, except port 4500, which is reserved for NAT-T).
IPsec Backup Servers	Use Client Configured List <input type="text"/>	<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> Select a method to use or disable backup servers. Enter up to 10 IPsec backup server addresses/names starting from high priority to low. Enter each IPsec backup server address/name on a single line.

Microsoft Client Parameters

Intercept DHCP Configure Message	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to use group policy for clients requesting Microsoft DHCP options.
Subnet Mask	<input type="text" value="255.255.255.255"/>	<input checked="" type="checkbox"/>	Enter the subnet mask for clients requesting Microsoft DHCP options.

Common Client Parameters

Split Tunneling Policy	<input checked="" type="radio"/> Tunnel everything <input type="checkbox"/> Allow the networks in list to bypass the tunnel <input type="radio"/> Only tunnel networks in the list	<input checked="" type="checkbox"/>	Select the method and network list to be used for Split Tunneling. Tunnel Everything: Send all traffic through the tunnel. Allow the networks in the list to bypass the tunnel: The VPN Client may choose to send traffic to addresses in this list to the client's LAN. Send all other traffic through the tunnel. NOTE: This setting only applies to the Cisco VPN Client. Tunnel networks in the list: Send traffic to addresses in this list through the tunnel. Send all other traffic to the client's LAN.
Split Tunneling Network List	<input type="text" value="--None--"/>	<input checked="" type="checkbox"/>	
Default Domain Name	<input type="text"/>	<input checked="" type="checkbox"/>	Enter the default domain name given to users of this group.
Split DNS Names	<input type="text"/>	<input checked="" type="checkbox"/>	Enter the set of domains, separated by commas without spaces, to be resolved through the Split Tunnel.

Add Cancel

78456

Banner

Enter the banner, or welcome text, that this group's IPsec clients see when they log in. The maximum length is 510 characters. You can use any characters, including newline (the Enter key, which counts as two characters).

Allow Password Storage on Client

Check the **Allow Password Storage on Client** check box to allow this group's IPsec clients to store their login passwords on their local client systems. If you do not allow password storage, IPsec users must enter their password each time they seek access to the VPN. For maximum security, we recommend that you *not allow* password storage.

This parameter has no bearing on interactive hardware client authentication or individual user authentication for a VPN 3002.

IPsec over UDP

Check the **IPsec over UDP** check box to allow the Cisco VPN Client (IPsec client) or VPN 3002 to connect to the VPN Concentrator via UDP through a firewall or router using NAT.

IPsec over UDP Port

Enter the UDP port number to use if you allow IPsec over UDP. Enter a number in the range 4001 through 49151. The default value is 10000.

See the discussion *About IPsec over UDP* under Configuration | User Management | Base Group.

IPsec Backup Servers

IPsec backup servers enable a VPN 3002 Hardware Client to connect to the central site when its primary central-site VPN Concentrator is unavailable. You configure backup servers for a VPN 3002, either on the VPN 3002 or on a group basis at the central-site Concentrator. If you configure backup servers on the central-site VPN Concentrator, that VPN Concentrator pushes the backup server policy to the VPN 3002 hardware clients in the group. The default policy is to use the backup server list configured on the VPN 3002.

Alternatively, the VPN Concentrator can push a policy that supplies a list of backup servers in order of priority (replacing the backup server list on the VPN 3002 if one is configured), or it can disable the feature and clear the backup server list on the VPN 3002.

See the [“IPsec Backup Servers”](#) of this chapter for an illustrated explanation of how the backup server feature works.



Note

The group name, user name, and passwords that you configure for the VPN 3002 must be identical for the primary VPN Concentrator and all backup servers. Also, if you require interactive hardware client authentication and/or individual user authentication for the VPN 3002, be sure to configure it on backup servers as well. See the [HW Client Parameters Tab](#) for more information.

Configuring Backup Servers from the Central-Site Concentrator

To configure backup servers on the primary central-site VPN Concentrator, accept the default, Use list below, in the IPsec Backup Servers drop down menu.

Enter either the IP addresses or the hostnames of the VPN Concentrators that are to be backup servers. The IP address is the IP address of the VPN Concentrator public interface.



Note

If you are using hostnames, it is wise to have backup DNS and WINS servers on a separate network from that of the primary DNS and WINS servers. Otherwise, if clients behind the VPN 3002 obtain DNS and WINS information from the VPN 3002 through DHCP, and the connection to the primary server is lost, and the backup servers have different DNS and WINS information, clients cannot be updated until the DHCP lease expires. Further, if you use hostnames and the DNS server is unavailable, significant delays can occur.

You can enter up to 10 backup servers, in order of highest to lowest priority. Enter each backup server on a single line, using the Enter or Return key for each new line.

Should there be a backup server list already configured on the VPN 3002, this list on the central-site VPN Concentrator replaces it, and becomes the list of backup servers on the VPN 3002 hardware client.

If you change the configuration of backup servers, or delete a backup server during an active session between a VPN 3002 and a backup server, the session continues without adopting that change. New settings take effect in the next new session.

Configuring Backup Servers from the VPN 3002

To configure backup servers on the VPN 3002, accept the default, Use client configured list in the IPsec Backup Servers drop-down menu. You then configure backup servers in the VPN 3002 Configuration | System | Tunneling Protocols | IPsec screen. Refer to the Tunneling chapter in the *VPN 3002 Hardware Client User Reference* for instructions.

Disabling Backup Servers

To disable the backup server feature, select **Disable and clear client configured list** in the IPsec Backup Servers drop-down menu. If you disable the feature from the primary VPN Concentrator, the feature is disabled and the list of backup servers configured on the VPN 3002, if there is one, is cleared.

Intercept DHCP Configure Message

DHCP Intercept lets Microsoft XP clients implement split-tunneling with a VPN Concentrator. The VPN Concentrator replies directly to the Microsoft Windows XP client DHCP Inform message, providing that client with the subnet mask, domain name, and classless static routes for the tunnel IP address. This is useful in environments in which using a DHCP server is not advantageous.



Note

A Microsoft XP anomaly results in the corruption of domain names if split tunnel options exceed 255 bytes. The VPN Concentrator limits the number of routes it sends to 27-40 routes, with the number of routes dependent on the classes of the routes, to avoid this problem.

Check the box to enable DHCP Intercept.

Subnet Mask

Enter the subnet mask for clients requesting Microsoft DHCP options.



Note

To implement split tunneling for Microsoft XP clients, you must also configure network lists and default domain names in the Common Client Parameters section of this screen.

Split Tunneling Policy

Split tunneling lets an IPsec client conditionally direct packets over an IPsec tunnel in encrypted form, or to a network interface in cleartext form. Packets not bound for destinations on the other side of the IPsec tunnel do not have to be encrypted, sent across the tunnel, decrypted, and then routed to a final destination. Split tunneling thus eases the processing load, simplifies traffic management, and speeds up untunneled traffic.



Note

If you enable both split tunneling and individual user authentication for a VPN 3002, users must authenticate only when sending traffic bound for destinations on the other side of the IPsec tunnel.

Split tunneling is primarily a traffic management feature, not a security feature. In fact, for optimum security, we recommend that you *not* enable split tunneling. However, since only the VPN Concentrator—and not the IPsec client—can enable split tunneling, you can control implementation here and thus protect security. Split tunneling is disabled by default on both the VPN Concentrator and the client. You enable and configure the feature on the VPN Concentrator, and then the VPN Concentrator uses Mode Configuration to push it to, and enable it on, the IPsec client.

Split tunneling applies only to single-user remote-access IPsec tunnels, not to LAN-to-LAN connections.

The default split tunneling policy is Tunnel Everything. Tunnel Everything disables split tunneling. When Tunnel Everything is configured, all traffic from remote clients in this group travels over the secure IPsec tunnel in encrypted form. No traffic goes in the clear or to any other destination than the VPN Concentrator. Remote users in this group reach internet networks through the corporate network and do not have access to local networks.

If users in this group need access to local networks, choose Allow Networks in List to Bypass Tunnel. This option allows you to define a list of networks to which traffic goes in the clear. This feature is useful for remote users who want to access devices on their local network, such as printers, while they are connected to the corporate network through a tunnel.

To configure the Allow Networks in List to Bypass Tunnel option, choose **VPN Client Local LAN** from the Split Tunnel Network List menu. The VPN Client Local LAN option allows all users in the group to access all devices on their local networks. If you want to restrict users' access to particular devices on their local network, you need to know the addresses of the local devices the remote users in this group want to access. Create a network list of these addresses, then choose that network list from the Split Tunneling Network List menu. You can apply only one network list to a group, but one network list can contain up to 10 network entries. (See the Configuration | Policy Management | Traffic Management | Network Lists screens for more information on creating network lists.) You also must enable Local LAN Access on the VPN Client. See the *VPN Client Administrator Guide* for more details.

**Note**

The Allow Networks in List to Bypass Tunnel option allows remote users to access *only* devices that are located on the *same* network interface as the tunnel. If a remote user's local LAN is located on a different network interface than the tunnel, the user cannot access it.

To allow remote users to access internet networks without tunneling through the corporate network, enable split tunneling. To enable split tunneling, choose **Only Tunnel Networks in List**. To configure this option, create a network list of addresses to tunnel. Then select this network list from the Split Tunneling Network List menu. Data to all other addresses is sent in the clear and routed by the remote user's internet service provider.

We recommend that you keep the base-group default, and that you enable and configure the split tunneling policy selectively for each group.

- Tunnel everything = Send all data via the secure IPSec tunnel.
- Allow networks in list to bypass the tunnel = Send all data via the secure IPSec tunnel except for data to addresses on the network list. The purpose of this option is to allow users who are tunneling all traffic to access devices such as printers on their local networks.
- Only tunnel networks in list = Send data to addresses on the network list via secure IPSec tunnel. Data bound for any other address goes in the clear. The purpose of this option is to allow remote users to access internet networks without requiring them to be tunneled through the corporate network.

Split Tunneling Network List

Click the drop-down menu button and select the split tunneling address list to use with this group's remote-access IPSec clients.

Both the Allow Networks in List to Bypass Tunnel option and the Only Tunnel Networks in List option make split tunneling decisions on the basis of a network list, which is a list of addresses on the private network. But the network list functions differently in each configuration.

In an Allow Networks in List to Bypass Tunnel configuration, The IPSec client uses the network list as an exclusion list: a list of addresses to which traffic should be sent in the clear. All other traffic is routed over the IPSec tunnel.

In an Only Tunnel Networks in List configuration, the IPSec client uses the network list as an *inclusion* list: a list of networks for which traffic should be sent over the IPSec tunnel. The IPSec client establishes an IPSec Security Association (SA) for each network specified in the list. Outbound packets with destination addresses that match one of the SAs are sent over the tunnel; everything else is sent as clear text to the locally connected network.

- None = No network address lists are configured.
- VPN Client Local LAN (default) = All addresses on the client's local network. The VPN Client Local LAN network list is a wildcard value that represents the client's local network. It corresponds to the address 0.0.0.0/0.0.0.0, which represents the IP address of the client's network card on which the tunnel is established. This option is the default associated with Allow Networks in List to Bypass Tunnel. It does not apply to the Only Tunnel Networks in List option.

Default Domain Name

Enter the default domain name that the VPN Concentrator passes to the IPsec client, for the client's TCP/IP stack to append to DNS queries that omit the domain field. This domain name applies only to tunneled packets. For example, if this entry is xyzcorp.com, a DNS query for mail becomes mail.xyzcorp.com. The maximum name length is 255 characters. The Manager checks the domain name for valid syntax.

Split DNS Names

Split DNS lets an internal DNS server resolve a list of centrally-defined Local Domain Names, while ISP-assigned DNS servers resolve all other DNS requests. It is used in split-tunneling connections; the internal DNS server resolves the domain names for traffic through the tunnel, and the ISP-assigned DNS servers resolve DNS requests that travel in the clear to the Internet.

Enter each domain name to be resolved by the internal server. Use commas but no spaces to separate the names.

Client FW Parameters Tab

This tab lets you configure firewall parameters for VPN Clients.

**Note**

Only VPN Clients running Microsoft Windows can use these firewall features. They are not presently available to hardware clients or other (non-Windows) software clients.

A *firewall* isolates and protects a computer from the Internet by inspecting each inbound and outbound individual packet of data to determine whether to allow or drop it. Firewalls provide extra security if remote users in a group have split tunneling configured. In this case, the firewall protects the user's PC, and thereby the corporate network, from intrusions by way of the Internet or the user's local LAN.

Remote users connecting to the VPN Concentrator with the VPN Client can choose from two possible firewall options.

In the first scenario, a remote user has a personal firewall installed on the PC. The VPN Client enforces firewall policy defined on the local firewall, and it monitors that firewall to make sure it is running. If the firewall stops running, the VPN Client drops the connection to the VPN Concentrator. (This firewall enforcement mechanism is called *Are You There (AYT)*, because the VPN Client monitors the firewall by sending it periodic "are you there?" messages; if no reply comes, the VPN Client knows the firewall is down and terminates its connection to the VPN Concentrator.) The network administrator might configure these PC firewalls originally, but with this approach, each user can customize his or her own configuration.

In the second scenario, you might prefer to enforce a centralized firewall policy for personal firewalls on VPN Client PCs. A common example would be to block Internet traffic to remote PCs in a group using split tunneling. This approach protects the PCs, and therefore the central site, from intrusions from the Internet while tunnels are established. This firewall scenario is called *push policy* or *Central Protection Policy (CPP)*. On the VPN Concentrator, you create a set of traffic management rules to enforce on the VPN Client, associate those rules with a filter, and designate that filter as the firewall policy. The VPN Concentrator pushes this policy down to the VPN Client. The VPN Client then in turn passes the policy to the local firewall, which enforces it.

A third scenario is to use a separate firewall server—the Zone Labs Integrity Server (IS)—to secure remote PCs on Windows platforms. The IS maintains policies for remote VPN Client PCs and monitors the PCs to ensure policy enforcement. The IS also communicates with the VPN Concentrator to allow and terminate connections, exchange session and user information, and report status information. For more details on how the VPN Concentrator interacts with the VPN Client, personal firewalls, and the Zone Labs Integrity Server, see the *VPN Client Administrator Guide*. For information on configuring the Zone Labs Integrity Server, refer to Zone Labs' documentation.

Figure 14-14 Configuration | User Management | Groups | Add or Modify (Internal) Screen, Client FW Parameters Tab

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity General IPsec Client Config Client FW HW Client PPTP/L2TP

VPN Client Firewall Policy			
Attribute	Value		Description
Firewall Setting	<input checked="" type="radio"/> No Firewall <input type="radio"/> Firewall Required <input type="radio"/> Firewall Optional		Select whether or not to require that the client firewall specified below be installed and active. Refer to the client documentation for details about using this feature.
Firewall	Custom Firewall		Select the firewall vendor and product required for clients in this group. For client firewalls not listed, select Custom Firewall and enter the vendor and product IDs.
Custom Firewall	Vendor ID	<input type="text"/>	<input checked="" type="checkbox"/> Separate multiple product IDs with commas. To indicate all products by a particular vendor, enter product ID 255. The product description is optional.
	Product ID	<input type="text"/>	
	Description	<input type="text"/>	
Firewall Policy	<input checked="" type="radio"/> Policy defined by remote firewall (AYT) <input type="radio"/> Policy Pushed (CPP): <input type="text" value="--None--"/> <input type="radio"/> Policy from Server		Select the policy for the protection provided by the client firewall.

Add Cancel

79332

Value/Inherit?

On this tabbed section:

- The **Inherit?** check box refers to base-group parameters: Does this specific group inherit the given setting from the base group? To inherit the setting, check the box (default). To override the base-group setting, clear the check box. If you clear the check box, you must also enter or change the corresponding **Value** field; do not leave the field blank.
- The **Value** column thus shows either base-group parameter settings that also apply to this group (**Inherit?** checked), or unique parameter settings configured for this group (**Inherit?** cleared).



Note

The setting of the **Inherit?** check box takes priority over an entry in a **Value** field. Examine this box before continuing and be sure its setting reflects your intent.

Firewall Setting

By default, no firewall is required for remote users in this group. If you want users in this group to be firewall-protected, choose either the Firewall Required or Firewall Optional setting.

If you choose Firewall Required, all users in this group must use the designated firewall. The VPN Concentrator drops any session that attempts to connect without the designated, supported firewall installed and running. In this case, the VPN Concentrator notifies the VPN Client that its firewall configuration does not match.

If you have remote users in this group who do not yet have firewall capacity, choose Firewall Optional. The Firewall Optional setting allows all the users in the group to connect. Those who have a firewall can use it; users that connect without a firewall receive a warning message. This setting is useful if you are creating a group in which some users have firewall support and others do not—for example, you may have a group that is in gradual transition, in which some members have set up firewall capacity and others have not yet done so.

Click the radio button to select a firewall setting:

- No Firewall = No firewall is required for remote users in this group.
- Firewall Required = All remote users in this group must use a specific firewall. Only those users with the designated firewall can connect.



Note

If you require a firewall for a group, make sure the group does not include any clients other than Windows VPN Clients. Any other clients in the group (including VPN 3002 Hardware Clients) will be unable to connect.

- Firewall Optional = All remote users in this group can connect. Those that have the designated firewall can use it. Those who do not have a firewall receive a warning message.

Firewall

Choose a firewall for the users in this group. Keep in mind when choosing that the firewall you designate correlates with the firewall policies available. The specific firewall you configure determines which firewall policy options are supported. (See [Table 14-7](#) for details.)

Click the drop-down menu button, and select the type of firewall required for users in this group.

- Cisco Integrated Client Firewall = The stateful firewall built into the VPN Client.
- Network ICE BlackICE Defender = The Network ICE BlackICE Agent or Defender personal firewall.
- Zone Labs ZoneAlarm = The Zone Labs ZoneAlarm personal firewall.
- Zone Labs ZoneAlarm Pro = The Zone Labs ZoneAlarm Pro personal firewall.
- Zone Labs ZoneAlarm or ZoneAlarm Pro = Either the Zone Labs ZoneAlarm personal firewall or the Zone Labs ZoneAlarm Pro personal firewall.
- Zone Labs Integrity = The Zone Labs Integrity Client.
- Custom Firewall = A combination of the firewalls listed above, or other firewalls not listed above. If you choose this option, you must create your own list of firewalls in the Custom Firewall field.



Note

You do not need to use the Custom option for Release 3.5. Currently, all supported firewalls are covered by the other Firewall menu options.

Custom Firewall

On the VPN Concentrator, you can configure a custom firewall. Currently there are no supported firewall configurations that you can not choose from the menu on the VPN Concentrator. This feature is mainly for future use. Nevertheless, the following table lists the vendor codes and products that are currently supported.

Table 14-6 Custom Vendor and Product codes

Vendor	Vendor Code	Products	Product Code
Cisco Systems	1	Cisco Integrated Client (CIC)	1
Zone Labs	2	Zone Alarm	1
		Zone AlarmPro	2
		Zone Labs Integrity	3
NetworkICE	3	BlackIce Defender/Agent	1

Enter a single vendor code; enter one or more product codes.

The VPN Concentrator can support any firewall that the VPN Client supports. Refer to the *VPN Client Administrator Guide* for the latest list of supported clients.

Vendor ID

Enter the vendor code for the firewall(s) that remote users in this group are using. Enter only one vendor.

Product ID

Enter the product code or codes for the firewall(s) that remote users in this group are using. To indicate any supported product, enter 255. Separate multiple codes with commas. Indicate code ranges with hyphens, for example: 4-20.

Description

Enter a description (optional) for the custom firewall.

Firewall Policy

Depending on which firewall you configured, certain Firewall Policy options are available. (See [Table 14-7](#).)

Table 14-7 Firewall Policy Options Available for Each Firewall

Firewall	Policy Defined by Remote Firewall	Policy Pushed	Policy from Server
Cisco Integrated Client Firewall	No	Yes	No
Network ICE BlackICE Defender	Yes	No	No
Zone Labs ZoneAlarm	Yes	Yes	No
Zone Labs ZoneAlarm Pro	Yes	Yes	No
Zone Labs ZoneAlarm or Zone Labs ZoneAlarm Pro	Yes	Yes	No
Zone Labs Integrity	No	No	Yes
Custom Firewall	N/A (This field is for future use.)		

Choose the source for the VPN Client firewall policy.

- Policy defined by remote firewall (AYT) = Remote users in this group have firewalls located on their PCs. The local firewall enforces the firewall policy on the VPN Client. The VPN Concentrator allows VPN Clients in this group to connect only if they have the designated firewall installed and running. If the designated firewall is not running, the connection fails. Once the connection is established, the VPN Client polls the firewall every 30 seconds to make sure that it is still running. If the firewall stops running, the VPN Client ends the session.
- Policy Pushed (CPP) = The VPN Concentrator enforces on the VPN clients in this group the traffic management rules defined by the filter you choose from the Policy Pushed (CPP) drop-down menu. The choices available on the menu are filters defined on this VPN Concentrator, including the default filters. Keep in mind that the VPN Concentrator pushes these rules down to the VPN client, so you should create and define these rules relative to the VPN client, not the VPN Concentrator. For example, “in” and “out” refer to traffic coming into the VPN Client or going outbound from the VPN Client.

If the VPN Client also has a local firewall, the policy pushed from the VPN Concentrator works with the policy of the local firewall. Any packet that is blocked by the rules of *either* firewall is dropped.

- Policy from Server = Users in this group use a Zone Labs Integrity Server to configure and manage firewall security on their remote PCs. If you choose this option, you must also configure the server address on the Configuration | System | Servers | Firewall Server screen.

HW Client Parameters Tab

This tab lets you configure interactive hardware client authentication and individual user authentication for the group. You can enable either feature, both features together, or neither. By default, interactive hardware client authentication and individual user authentication are disabled.

Figure 14-15 Configuration | User Management | Groups | Add or Modify, HW Client Parameters Tab

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity General IPsec Client Config Client FW **HW Client** PPTP/L2TP

Hardware Client Parameters			
Attribute	Value	Inherit?	Description
Require Interactive Hardware Client Authentication	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to require the hardware client to be interactively authenticated at each connection attempt.
Require Individual User Authentication	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to require users behind a hardware client to be authenticated.
User Idle Timeout	30	<input checked="" type="checkbox"/>	Enter the session idle timeout in minutes. Use 0 for no timeout.
Cisco IP Phone Bypass	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow Cisco IP Phones to bypass Individual User Authentication behind a hardware client.
Allow Network Extension Mode	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow hardware clients using Network Extension Mode to connect.

Add Cancel

79336

Require Interactive Hardware Client Authentication

Check the **Require Interactive Hardware Client Authentication** check box to enable interactive authentication for the VPN 3002.

Require Individual User Authentication

Check the **Require Individual User Authentication** check box to enable individual user authentication.

User Idle Timeout

Enter the idle timeout period in minutes. If there is no communication activity on a user connection in this period, the system terminates the connection. The minimum is 1 minute, the default is 30 minutes, and the maximum is 2147483647 minutes (over 4000 years). To disable timeout and allow an unlimited idle period, enter 0.

Cisco IP Phone Bypass

Check the **Cisco IP Phone Bypass** check box to allow IP phones to bypass the interactive individual user authentication processes. Interactive hardware client authentication remains in effect if you have enabled it.

Allow Network Extension Mode

This feature lets you restrict the use of network extension mode on the VPN 3002. Check the box to allow hardware clients in the group to use network extension mode.

**Note**

If you disallow network extension mode, the default setting, the VPN 3002 can connect to this VPN Concentrator in PAT mode only. If you disallow network extension mode here, be careful that all VPN 3002s in the group are configured for PAT mode. If a VPN 3002 is configured to use network extension mode and the VPN Concentrator to which it connects disallows network extension mode, the VPN 3002 will attempt to connect every 4 seconds, and every attempt will be rejected; this is the equivalent of denial of service attack.

About Interactive Hardware Client Authentication

Interactive hardware client authentication provides the central site with additional security by requiring the VPN 3002 to authenticate with a username and password that you enter manually each time the VPN 3002 initiates a tunnel. With this feature enabled the VPN 3002 does not have a saved username and password. When you enter the username and password, the VPN 3002 sends these credentials to the VPN Concentrator to which it connects. The VPN Concentrator facilitates authentication, on either the internal or an external authentication server. If the username and password are valid, the tunnel is established.

You configure interactive hardware client authentication in Hardware Client tab of the Configuration | User Management | Groups screen on the VPN Concentrator at the central site, which then pushes the policy to the VPN 3002.

You specify the *type* of authentication server in the IPSec tab of the Configuration | User Management | Groups screen on the VPN Concentrator. The VPN 3002 authenticates on the first server of that type that you configure in the Configuration | System | Servers | Authentication screen or Configuration | User Management | Groups | Authentication Servers screen. If the VPN 3002 cannot reach that server, it authenticates on the next server of that type in the list of authentication servers.

Enabling and Later Disabling Interactive Hardware Client Authentication

When you enable interactive hardware client authentication for a group, the VPN Concentrator pushes that policy to the VPN 3002s in the group. If you have previously set a username and password on the VPN 3002, the software deletes them from the configuration file. When you try to connect, the software prompts you for a username and password.

If, on the VPN Concentrator, you subsequently disable interactive hardware authentication for the group, it is enabled locally on the VPN 3002s, and the software continues to prompt for a username and password. This lets the VPN 3002 connect, even though it lacks a saved username and password, and the VPN Concentrator has disabled interactive hardware client authentication.

If you subsequently configure a username and password (in the VPN 3002 Configuration | System | Tunneling Protocols | IPSec screen), the feature is disable, and the prompt no longer displays. The VPN 3002 connects to the VPN Concentrator using the saved username and password.

About Individual User Authentication

Individual user authentication protects the central site from access by unauthorized persons on the same LAN as the VPN 3002.

When you enable individual user authentication, each user that connects through a VPN 3002 must open a web browser and manually enter a valid username and password to access the network behind the VPN Concentrator, even though the tunnel already exists.

**Note**

You cannot use the command-line interface to log in if user authentication is enabled. You must use a browser.

- If you have a default home page on the remote network behind the VPN Concentrator, or direct the browser to a website on the remote network behind the VPN Concentrator, the VPN 3002 directs the browser to the proper pages for user login. When you successfully log in, the browser displays the page you originally entered.
- If you try to access resources on the network behind the VPN Concentrator that are not web-based, for example, email, the connection will fail until you authenticate.
- To authenticate, you must enter the IP address for the private interface of the VPN 3002 in the browser Location or Address field. The browser then displays the login screen for the VPN 3002. To authenticate, click the Connect/Login Status button.
- One user can log in for a maximum of four sessions simultaneously.

Individual users authenticate according to the order of authentication servers that you configure for a group. To configure authentication servers for individual user authentication, see the sections, Configuration | User Management | Base Group/Groups | Authentication Servers | Add/Modify.

Summary of VPN 3002 Authentication Features

Table 14-8 summarizes how authentication of the VPN 3002 works by default, and how it works with interactive hardware client authentication and individual user authentication enabled. Be aware that you can use both interactive hardware client authentication or individual user authentication simultaneously, or either one and not the other.

Table 14-8 Authenticating the VPN 3002 Hardware Client and Users

Authentication with Saved Username and Password	Interactive Hardware Client Authentication	Individual User Authentication
Authenticates the VPN 3002.	Authenticates the VPN 3002.	Authenticates a user or device on the private LAN behind the VPN 3002.
On the VPN 3002, you configure the username and password in either of these screens: <ul style="list-style-type: none"> • Configuration Quick IPSec. • Configuration System Tunneling Protocols IPSec. 	You do not configure the username and password on the VPN 3002.	You do not configure the username and password on the VPN 3002.
The VPN 3002 saves the username and password.	The VPN 3002 does not save the username and password.	The VPN 3002 does not save the username and password.
Requires no user interaction subsequent to initial configuration.	You are prompted to enter a username and password each time the VPN 3002 initiates the tunnel.	You open a web browser and enter a username and password when prompted, even though the tunnel already exists. You cannot use the command-line interface.
The default option.	You enable on the VPN Concentrator. The VPN Concentrator pushes the policy to the VPN 3002.	You enable on the VPN Concentrator. The VPN Concentrator pushes the policy to the VPN 3002.
The VPN 3002 authenticates on the first server of the type that you configure. If the VPN 3002 cannot reach that server, it authenticates on the next server of that type in the list of authentication servers.		Individual users authenticate according to the order of authentication servers configured, regardless of type.
		Individual users can authenticate according to the values of an embedded group rather than the tunnel group. See the next section.

Associating Users with Different Groups for Authentication

When you configure a VPN 3002, you assign it to a group on the VPN Concentrator to which it connects. This is the *tunnel group* to which the VPN 3002 belongs. The attributes of the tunnel group determine how the VPN 3002 authenticates.

For purposes of authentication, you can associate users behind the VPN 3002 with a group other than the tunnel group. You accomplish this by embedding a second, different group name within the username. To embed this second group name, you configure and use a delimiter, (@, #, or !) that associates the second group with the user. The format to use is *username<delimiter>groupname*, for example, *UserA@bluegroup*.

When you embed a groupname within a username:

- An individual user authenticates according to the priority order of the authentication servers you configure for the group embedded within its username.
- If you use external authentication servers, you have the flexibility of storing usernames and passwords for the VPN 3002 on one server, and those for individual users behind the VPN 3002 on another server or servers.
- Users behind the same VPN 3002 can authenticate to different external servers. You configure this by embedding different groups for various users. For example, *UserA@bluegroup* might authenticate to a RADIUS server, while *UserD@greengroup* authenticates to an SDI server, or to a different RADIUS server.



Note

The VPN 3002 always gets settings for interactive hardware client authentication from the tunnel group, not the embedded group.

Table 14-9 summarizes how UserA, UserB, and UserC connect to the central site through a VPN 3002.

Table 14-9 Example: How Authentication Servers Work Using Embedded Groups

Username	Tunnel Group	Embedded Group	Authentication Server for the VPN 3002	Authentication Server for the Individual User
UserA	bluegroup	None	An authentication server configured for bluegroup.	User A uses an authentication server configured for bluegroup.
UserB@redgroup	bluegroup	redgroup	An authentication server configured for bluegroup.	User B uses an authentication server configured for redgroup.
UserC@greengroup	bluegroup	greengroup	An authentication server configured for bluegroup.	The VPN 3002 authenticates using an authentication server configured for greengroup.

Configuring a Group Delimiter

To configure and use a group delimiter, follow these steps.

-
- Step 1** In the Configuration | System | General | Global Authentication parameters screen on the VPN Concentrator:
- Enable Group Lookup
 - Select a delimiter (@, #, or !).
- Step 2** In the General tab of the Configuration | User Management | Groups | Add/Modify screen, check the Strip Realm box to remove the group name embedded in the username during authentication.
-

To use a second group for individual user authentication, enter the username with the embedded group in the form *username<delimiter>groupname* in the username field in one of these screens:

- In the Monitoring | System Status screen, click the **Connect Now** button. You are prompted for a username and password.
- In the Manager Login screen, click **Connection/Login Status**. If individual user authentication is required, the Log In Now prompt displays. When you click that button, you are prompted for a username and password.

Backup Servers with Interactive Hardware Client and Individual User Authentication

Be sure to configure any backup servers for the VPN 3002 with the same values as the primary VPN Concentrator for interactive hardware client authentication and individual user authentication. For information about configuring backup servers, see the section, [Client Configuration Parameters Tab](#), earlier in this chapter.

Accounting with Interactive Hardware Client and Individual User Authentication

If a VPN 3002 authenticates to a VPN Concentrator, and you have enabled accounting, the VPN Concentrator notifies the RADIUS accounting server when the VPN 3002 logs on and off. It also keeps track of individual users. See the section, [Configuration | System | Servers | Accounting](#) of this book

PPTP/L2TP Parameters Tab

This section of the screen lets you configure PPTP and L2TP parameters that apply to this internally configured group. During tunnel establishment, the client and server negotiate access and usage based on these parameters. Only clients that meet these criteria are allowed access. If you checked PPTP, L2TP, or L2TP over IPsec under Tunneling Protocols on the General Parameters tab, configure these parameters.

Figure 14-16 Configuration | User Management | Groups | Add or Modify (Internal) Screen, PPTP/L2TP Tab

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPsec | Client Config | Client FW | HW Client | **PPTP/L2TP**

PPTP/L2TP Parameters			
Attribute	Value	Inherit?	Description
Use Client Address	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2 <input type="checkbox"/> EAP Proxy	<input checked="" type="checkbox"/>	Check the authentication protocols allowed by this group. The choices available are determined by base group settings. Refer to the online help for authentication protocol dependencies. Unchecking all options means that no authentication is required.
PPTP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	<input checked="" type="checkbox"/>	Select the allowed encryption methods for PPTP connections for this group.
PPTP Compression	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable compression for PPTP connections for this group.
L2TP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2 <input type="checkbox"/> EAP Proxy	<input checked="" type="checkbox"/>	Check the authentication protocols allowed by this group. The choices available are determined by base group settings. Refer to the online help for authentication protocol dependencies. Unchecking all options means that no authentication is required.
L2TP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	<input checked="" type="checkbox"/>	Select the allowed encryption methods for L2TP connections for this group.
L2TP Compression	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable compression for L2TP connections for this group.

Add Cancel

Value / Inherit?

On this tabbed section:

- The Inherit? check box refers to base-group parameters: Does this specific group inherit the given setting from the base group? To inherit the setting, check the box (default). To override the base-group setting, uncheck the check box. If you uncheck the check box, you must also enter or change any corresponding Value field; do not leave the field blank.
- The Value column thus shows either base-group parameter settings that also apply to this group (Inherit? checked), or unique parameter settings configured for this group (Inherit? cleared).



Note

The setting of the Inherit? check box takes priority over an entry in a Value field. Examine this box before continuing and be sure its setting reflects your intent.

Use Client Address

Check the **Use Client Address** check box to accept and use an IP address that this group's client supplies. A client must have an IP address to function as a tunnel endpoint; but for maximum security, we recommend that you control IP address assignment and *not allow* client-specified IP addresses.

Make sure the setting here is consistent with the setting for Use Client Address on the Configuration | System | Address Management | Assignment screen.

PPTP Authentication Protocols

Check the **PPTP Authentication Protocols** check boxes for the authentication protocols that this group's PPTP clients can use. To establish and use a VPN tunnel, users should be authenticated in accordance with some protocol.



Caution

Unchecking *all* authentication options means that *no* authentication is required. That is, PPTP users can connect with *no* authentication. This configuration is allowed so you can test connections, but it is not secure.

These choices specify the allowable authentication protocols in order, from least secure to most secure.

You can allow a group to use *fewer* protocols than the base group, but not more. You cannot allow a grayed-out protocol.

- PAP = Password Authentication Protocol. This protocol passes cleartext username and password during authentication and is not secure. We strongly recommend that you not allow this protocol.
- CHAP = Challenge-Handshake Authentication Protocol. In response to the server challenge, the client returns the encrypted [challenge plus password], with a cleartext username. It is more secure than PAP, but does not encrypt data.
- MSCHAPv1 = Microsoft Challenge-Handshake Authentication Protocol version 1. This protocol is similar to, but more secure than, CHAP. In response to the server challenge, the client returns the encrypted [challenge plus encrypted password], with a cleartext username. Thus the server stores—and compares—only encrypted passwords, rather than cleartext passwords as in CHAP. This protocol also generates a key for data encryption by MPPE (Microsoft Point-to-Point Encryption). If you check Required under PPTP Encryption, you must allow one or both MSCHAP protocols and no other.
- MSCHAPv2 = Microsoft Challenge-Handshake Authentication Protocol version 2. This protocol is even more secure than MSCHAPv1. It requires mutual client-server authentication, uses session-unique keys for data encryption by MPPE, and derives different encryption keys for the send and receive paths. The VPN Concentrator internal user authentication server supports this protocol, but external authentication servers do not. If you check Required under PPTP Encryption, you must allow one or both MSCHAP protocols and no other.
- EAP Proxy = Extensible Authentication Protocol, defined in RFC 2284. EAP lets the VPN Concentrator proxy the entire PPTP/L2TP authentication process to an external RADIUS authentication server. It provides additional authentication options for the Microsoft VPN Client, including EAP/MD5, Smartcards and certificates (EAP/TLS), and RSA SecurID (EAP/SDI). It requires that you configure an EAP enabled RADIUS server. You cannot enable EAP Proxy if you are using PPP encryption. It is configurable at the base group or group levels.

PPTP Encryption

Check the **PPTP Encryption** check boxes for the data encryption options that apply to the PPTP clients of this group.

- **Required** = During connection setup, the PPTP clients of this group must agree to use Microsoft encryption (MPPE) to encrypt data or they will not be connected. If you check this option, you must also allow only MSCHAPv1 and/or MSCHAPv2 under PPTP Authentication Protocols, and you must also check 40-bit and/or 128-bit here.
- **Require Stateless** = During connection setup, the PPTP clients of this group must agree to use stateless encryption to encrypt data or they will not be connected. With stateless encryption, the encryption keys are changed on every packet; otherwise, the keys are changed after some number of packets or whenever a packet is lost. Stateless encryption is more secure, but it requires more processing. However, it might perform better in a lossy environment (where packets are lost), such as the Internet.
- **40-bit** = The PPTP clients of this group are allowed to use the RSA RC4 encryption algorithm with a 40-bit key. This is significantly less secure than the 128-bit option. Microsoft encryption (MPPE) uses this algorithm. If you check **Required**, you must check this option and/or the 128-bit option.
- **128-bit** = The PPTP clients of this group are allowed to use the RSA RC4 encryption algorithm with a 128-bit key. Microsoft encryption (MPPE) uses this algorithm. If you check **Required**, you must check this option and/or the 40-bit option.



Note

The U.S. government restricts the distribution of 128-bit encryption software.

PPTP Compression

If all members of this group are remote dial-in users connecting with modems, enabling data compression might speed up their data transmission rates. Data compression shrinks data by replacing repeating information with symbols that use less space. Check the **PPTP Compression** check box to enable data compression for PPTP. PPTP data compression uses the Microsoft Point to Point Compression (MPPC) protocol.



Note

MPPC data compression increases the memory requirement and CPU utilization for each user session. Consequently, using data compression reduces the overall throughput of the VPN Concentrator and lowers the maximum number of sessions your VPN Concentrator can support. *We recommend you enable data compression only if every member of the group is a remote user connecting with a modem.* If any members of the group connect via broadband, do not enable data compression for the group. Instead, divide the group into two groups, one for modem users and the other for broadband users. Enable data compression only for the group of modem users.



Note

PPTP data compression is only supported for clients that use stateless encryption.

L2TP Authentication Protocols

Check the **L2TP Authentication Protocols** check boxes for the authentication protocols that this group's L2TP clients can use. To establish and use a VPN tunnel, users should be authenticated in accordance with a protocol.

**Caution**

Unchecking *all* authentication options means that *no* authentication is required. That is, L2TP users can connect with *no* authentication. This configuration is allowed so you can test connections, but it is not secure.

These choices specify the allowable authentication protocols in order from least secure to most secure.

You can allow a group to use *fewer* protocols than the base group, but not more. You cannot allow a grayed-out protocol.

- PAP = Password Authentication Protocol. This protocol passes cleartext username and password during authentication and is not secure. We strongly recommend that you *not allow* this protocol.
- CHAP = Challenge-Handshake Authentication Protocol. In response to the server challenge, the client returns the encrypted [challenge plus password], with a cleartext username. It is more secure than PAP, but does not encrypt data.
- MSCHAPv1 = Microsoft Challenge-Handshake Authentication Protocol version 1. This protocol is similar to, but more secure than, CHAP. In response to the server challenge, the client returns the encrypted [challenge plus encrypted password], with a cleartext username. Thus the server stores—and compares—only encrypted passwords, rather than cleartext passwords as in CHAP. This protocol also generates a key for data encryption by MPPE (Microsoft Point-to-Point Encryption). If you check Required under L2TP Encryption, you must allow one or both MSCHAP protocols and no other.
- MSCHAPv2 = Microsoft Challenge-Handshake Authentication Protocol version 2. This protocol is even more secure than MSCHAPv1. It requires mutual client-server authentication, uses session-unique keys for data encryption by MPPE, and derives different encryption keys for the send and receive paths. The VPN Concentrator internal user authentication server supports this protocol, but external authentication servers do not. If you check Required under L2TP Encryption, you must allow one or both MSCHAP protocols and no other.
- EAP Proxy = Extensible Authentication Protocol, defined in RFC 2284. EAP enables the VPN Concentrator to proxy the entire PPTP/L2TP authentication process to an external RADIUS authentication server. It provides additional authentication options for the Microsoft VPN Client (L2TP/IPSec), including EAP/MD5, Smartcards and certificates (EAP/TLS), and RSA SecurID (EAP/SDI). It requires that you configure an EAP enabled RADIUS server. You cannot configure EAP if you are using encryption. It is configurable at the base group or group levels.

L2TP Encryption

Check the **L2TP Encryption** check boxes for the data encryption options that apply to this group's L2TP clients.

- **Required** = During connection setup, this group's L2TP clients must agree to use Microsoft encryption (MPPE) to encrypt data or they will not be connected. If you check this option, you must also allow only MSCHAPv1 and/or MSCHAPv2 under L2TP Authentication Protocols, and you must also check 40-bit and/or 128-bit here.
- **Require Stateless** = During connection setup, this group's L2TP clients must agree to use stateless encryption to encrypt data or they will not be connected. With stateless encryption, the encryption keys are changed on every packet; otherwise, the keys are changed after some number of packets or whenever a packet is lost. Stateless encryption is more secure, but it requires more processing. However, it might perform better in a lossy environment (where packets are lost), such as the Internet.
- **40-bit** = This group's L2TP clients are allowed to use the RSA RC4 encryption algorithm with a 40-bit key. This is significantly less secure than the 128-bit option. Microsoft encryption (MPPE) uses this algorithm. If you check Required, you must check this option and/or the 128-bit option.
- **128-bit** = This group's L2TP clients are allowed to use the RSA RC4 encryption algorithm with a 128-bit key. Microsoft encryption (MPPE) uses this algorithm. If you check Required, you must check this option and/or the 40-bit option.

L2TP Compression

If all members of this group are remote dial-in users connecting with modems, enabling data compression might speed up their data transmission rates. Data compression shrinks data by replacing repeating information with symbols that use less space. Check the **L2TP Compression** check box to enable data compression for L2TP. L2TP data compression uses the Microsoft Point to Point Compression (MPPC) protocol.



Note

MPPC data compression increases the memory requirement and CPU utilization for each user session. Consequently, using data compression reduces the overall throughput of the VPN Concentrator and lowers the maximum number of sessions your VPN Concentrator can support. *We recommend you enable data compression only if every member of the group is a remote user connecting with a modem.* If any members of the group connect via broadband, do not enable data compression for the group. Instead, divide the group into two groups, one for modem users and the other for broadband users. Enable data compression only for the group of modem users.



Note

L2TP data compression is only supported for clients that use stateless encryption.

Add or Apply / Cancel

When you finish setting or changing parameters on all tabs, click **Add** or **Apply** at the bottom of the screen to Add this specific group to the list of configured groups, or to Apply your changes. Both actions include your settings in the active configuration. The Manager returns to the Configuration | User Management | Groups screen. Any new groups appear in alphabetical order in the Current Groups list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click the **Cancel** button. The Manager returns to the Configuration | User Management | Groups screen, and the Current Groups list is unchanged.

Configuration | User Management | Groups | Modify (External)

This screen lets you change identity parameters for an external group that you have previously configured. The screen title identifies the group you are modifying.

Figure 14-17 Configuration | User Management | Groups | Modify (External) Screen

Identity Parameters		
Attribute	Value	Description
Group Name	3000group	Enter a unique name for the group.
Password	*****	Enter the password for the group.
Verify	*****	Verify the group's password.
Type	External	External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.

Group Name

Enter a unique name for this specific group. You can edit this field as desired. The maximum name length is 64 characters. Entries are case-sensitive. Changing a group name automatically updates the group name for all users in the group.

See the note about configuring the RADIUS Class attribute under [“Configuration | User Management | Groups”](#).

Password

Enter a unique password for this group. The minimum password length is 4 characters. The maximum length is 32 characters. Entries are case-sensitive. The field displays only asterisks.

Verify

Re-enter the group password to verify it. The field displays only asterisks.

Type

Click the **Type** drop-down menu button and select the authentication server type for the group:

- **Internal** = To change this group to use the internal VPN Concentrator authentication server, select this type. If you change this group from External to Internal, the Manager displays the Configuration | User Management | Groups | Modify (Internal) screen when you click **Apply**, so you can configure all the parameters.
- **External** = To use only an external authentication server, such as RADIUS, keep this selection. The external server supplies the group parameters if it can; otherwise the base-group parameters apply.

Apply / Cancel

When you finish changing these parameters, click **Apply** to include your settings in the active configuration. The Manager returns to the Configuration | User Management | Groups screen and refreshes the Current Groups list. However, if you change group type to Internal, the Manager displays the Configuration | User Management | Groups | Modify (Internal) screen so you can configure all the parameters.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your changes, click **Cancel**. The Manager returns to the Configuration | User Management | Groups screen, and the Current Groups list is unchanged.

Configuration | User Management | Groups | Authentication Servers

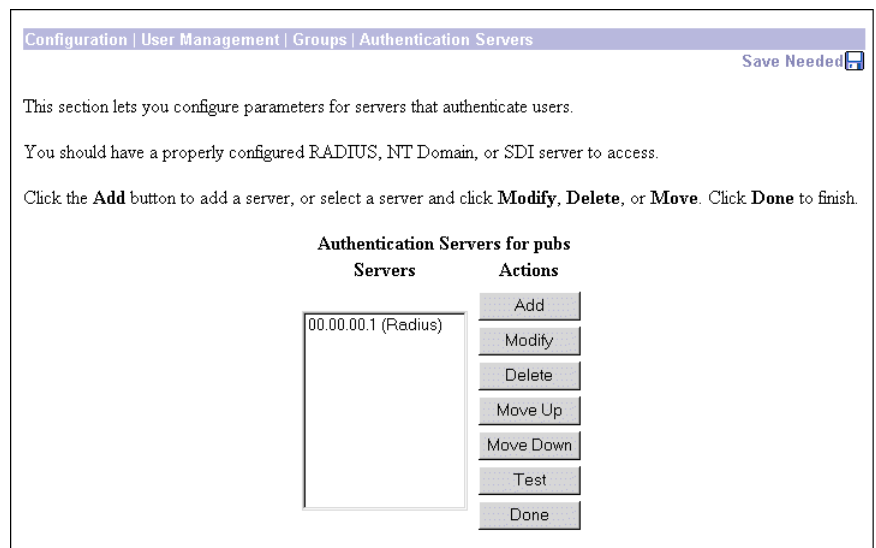
This screen lets you add, modify, delete, or change the priority order of authentication servers for a group. You can add external RADIUS, NT Domain and SDI servers for authenticating users. To add an internal server, go to the Configuration | System | Servers | Authentication screen. For further information about internal servers, see “[Configuration | System | Servers | Authentication](#)”.

If individual user authentication is enabled, the authentication servers you configure for the group here are used in the order of priority you set here. If you do not configure an external authentication server here, individual user authentication uses the internal authentication server on the VPN Concentrator.

Before you configure an external server, be sure that the external server you reference is itself properly configured and that you know how to access it (IP address or host name, TCP/UDP port, secret/password, etc.). The VPN Concentrator functions as the client of these servers.

You can configure and prioritize up to 10 authentication servers. The first server of a given type is the primary server for that type, and the rest are backup servers in case the primary is inoperative. If no authentication servers are configured for the group, the Global authentication server list applies.

Figure 14-18 Configuration | User Management | Groups | Authentication Servers Screen



Servers

The servers list shows the configured authentication servers, in priority order. Each entry shows the server identifier and type, by IP address or by host name, for example: 192.168.12.34 (RADIUS). If no servers have been configured the list shows --Empty--. The first server of each type is the primary, the rest are backup.

Actions

To configure and add a new authentication server, click **Add**. The Manager opens the Configuration | User Management | Groups | Authentication Servers | Add screen.

To modify parameters for an authentication server that has been configured, select the server from the list and click **Modify**. The Manager opens the Configuration | User Management | Groups | Authentication Servers | Modify screen.

To remove a server that has been configured, select the server from the list and click **Delete**.

**Note**

There is no confirmation or undo.

The Manager refreshes the screen and shows the remaining servers in the list. *When you delete a server, any clients with no other authentication server configured use the server configured for the base group.*

To change the priority order for an authentication server click **Move Up** or **Move Down** to move it up or down on the list of servers configured for this group.

To test a configured external user authentication server, select the server from the list and click **Test**. The Manager opens the Configuration | System | Servers | Authentication | Test screen. There is no need to test the internal server, and trying to do so returns an error message.

When you are finished configuring authentication servers, click **Done**. This action includes your settings in the active configuration. The Manager returns to the Configuration | User Management | Groups screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | User Management | Groups | Authentication Servers | Add or Modify

These screens let you:

- Add: Configure and add a new user authentication server.
- Modify: Modify parameters for a configured user authentication server.

Click the drop-down menu button and select the Server Type. The screen and its available fields change depending on the Server Type. Choices are:

- RADIUS = An external RADIUS server (default).
- NT Domain = An external Windows NT Domain server.
- SDI = An external RSA Security Inc. SecurID server.

Find your selected Server Type.

Server Type = RADIUS

Configure these parameters for a RADIUS authentication server.

Figure 14-19 Configuration | User Management | Groups | Authentication Servers | Add or Modify RADIUS Screen

Authentication Server

Enter the IP address or host name of the RADIUS authentication server, for example: 192.168.12.34. The maximum length is 32 characters. (If you have configured a DNS server, you can enter a host name in this field; otherwise, enter an IP address. For maximum security, use an IP address.)

Server Port

Enter the UDP port number by which you access the server. Enter 0 (the default) to have the system supply the default port number, 1645.

**Note**

The latest RFC states that RADIUS should be on UDP port number 1812, so you might need to change this default value to 1812.

Timeout

Enter the time in seconds to wait after sending a query to the server and receiving no response, before trying again. The minimum time is 1 second. The default is 4 seconds. The maximum is 30 seconds.

Retries

Enter the number of times to retry sending a query to the server after the timeout period. If there is still no response after this number of retries, the VPN Concentrator declares this server inoperative and uses the next RADIUS authentication server in the list. The minimum number of retries is 0. The default is 2. The maximum is 10.

Server Secret

Enter the RADIUS server secret (also called the shared secret), for example: C8z077f. The maximum length is 64 characters. The field shows only asterisks.

Verify

Re-enter the RADIUS server secret to verify it. The field shows only asterisks.

Add or Apply / Cancel

To add the new server to the list of configured user authentication servers, click **Add**. Or to apply your changes to the configured server, click **Apply**. Both actions include your entries in the active configuration. The Manager returns to the Configuration | User Management | Groups | Authentication Servers screen. Any new server appears at the bottom of the Authentication Servers list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | Servers | Authentication screen, and the Authentication Servers list is unchanged.

Server Type = NT Domain

Configure these parameters for a Windows NT Domain authentication server.

Figure 14-20 Configuration | User Management | Groups | Authentication Servers | Add or Modify NT Domain Screen

Configuration | User Management | Groups | Authentication Servers | Add

Configure and add a user authentication server.

Server Type **NT Domain** Select the type of authentication server.

Authentication Server Address Enter the IP address.

Server Port Enter 0 for default port (139).

Timeout Enter the timeout for this server (seconds).

Retries Enter the number of retries for this server.

Domain Controller Name Enter the NT Primary Domain Controller name for this authentication server.

87011

Authentication Server Address

Enter the IP address of the NT Domain authentication server, for example: 192.168.12.34. Use dotted decimal notation.

Server Port

Enter the TCP port number by which you access the server. Enter 0 (the default) to have the system supply the default port number, 139.

Timeout

Enter the time in seconds to wait after sending a query to the server and receiving no response, before trying again. The minimum time is 1 second. The default time is 4 seconds. The maximum time is 30 seconds.

Retries

Enter the number of times to retry sending a query to the server after the timeout period. If there is still no response after this number of retries, the VPN Concentrator declares this server inoperative and uses the next NT Domain authentication server in the list. The minimum number of retries is 0. The default number is 2. The maximum number is 10.

Domain Controller Name

Enter the NT Primary Domain Controller host name for this server, for example: PDC01. The maximum host name length is 16 characters. You *must* enter this name, and it *must* be the correct host name for the server for which you entered the IP Address in Authentication Server Address; if it is incorrect, authentication fails.

Add or Apply / Cancel

To add the new server to the list of configured user authentication servers, click **Add**. Or to apply your changes to the configured server, click **Apply**. Both actions include your entries in the active configuration. The Manager returns to the Configuration | User Management | Groups | Authentication Servers screen. Any new server appears at the bottom of the Authentication Servers list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | Servers | Authentication screen, and the Authentication Servers list is unchanged.

Server Type = SDI

Configure these parameters for an RSA Security Inc. SecurID authentication server.

VPN Concentrator software version 3.6 supports both versions prior to SDI 5.0 and version 5.0.

Server Type = SDI

Configure these parameters for an RSA Security Inc. SecurID authentication server.

VPN Concentrator software version 3.6 supports both version 5.0 and versions prior to SDI 5.0.

SDI Version pre-5.0

SDI versions prior to 5.0 use the concept of an SDI master and an SDI slave server which share a single node secret file (SECURID). On the VPN Concentrator you can configure one pre-5.0 SDI master server and one SDI slave server globally, and one SDI master and one SDI slave server per each group.

SDI Version 5.0

SDI version 5.0 uses the concepts of an SDI primary and SDI replica servers. A primary and its replicas share a single node secret file. On the VPN Concentrator you can configure one SDI 5.0 server globally, and one per each group.

A version 5.0 SDI server that you configure on the VPN Concentrator can be either the primary or any one of the replicas. See the section below, “[SDI Primary and Replica Servers](#)” for information about how the SDI agent selects servers to authenticate users.

You can have one SDI primary server, and up to 10 replicas; use the SDI documentation for configuration instructions. The primary and all the replicas can authenticate users. Each primary and its replicas share a single node secret file. The node secret file has its name based on the hexadecimal value of the ACE/Server IP address with .sdi appended. SDI servers that you configure here apply to this group.

Two-step Authentication Process

SDI version 5.0 uses a two-step process to prevent an intruder from capturing information from an RSA SecurID authentication request and using it to authenticate to another server. The Agent first sends a lock request to the SecurID server before sending the user authentication request. The server locks the username, preventing another (replica) server from accepting it. This means that the same user cannot authenticate to two VPN Concentrators using the same authentication servers simultaneously. After a successful username lock, the VPN Concentrator sends the passcode.

SDI Primary and Replica Servers

The VPN Concentrator obtains the server list when the first user authenticates to the configured server, which can be either a primary or a replica. The VPN Concentrator then assigns priorities to each of the servers on the list, and subsequent server selection derives at random from those assigned priorities. The highest priority servers have a higher likelihood of being selected.

Two-step Authentication Process

SDI version 5.0 uses a two-step process to prevent an intruder from capturing information from an RSA SecurID authentication request and using it to authenticate to another server. The Agent first sends a lock request to the SecurID server before sending the user passcode. The server locks the username, preventing another (replica) server from accepting it. This means that the same user cannot authenticate to two VPN Concentrators using the same authentication servers simultaneously.

Figure 14-21 Configuration | User Management | Groups | Authentication Servers | Add or Modify SDI Screen

Authentication Server

Enter the IP address or host name of the SDI authentication server, for example: 192.168.12.34. The maximum number of characters is 32. (If you have configured a DNS server, you can enter a host name in this field; otherwise, enter an IP address.)

Server Port

Enter the UDP port number by which you access the server. Enter 0 (the default) to have the system supply the default port number, 5500.

Timeout

Enter the time in seconds to wait after sending a query to the server and receiving no response, before trying again. The minimum time is 1 second. The default is 4 seconds. The maximum is 30 seconds.

Retries

Enter the number of times to retry sending a query to the server after the timeout period. If there is still no response after this number of retries, the VPN Concentrator declares this server inoperative and uses the next SDI authentication server in the list. The minimum number of retries is 0. The default is 2. The maximum is 10.

Add or Apply / Cancel

To add the new server to the list of configured user authentication servers, click **Add**. Or to apply your changes to the configured server, click **Apply**. Both actions include your entries in the active configuration. The Manager returns to the Configuration | User Management | Groups | Authentication Servers screen. Any new server appears at the bottom of the Authentication Servers list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | Servers | Authentication screen, and the Authentication Servers list is unchanged.

Configuration | User Management | Groups | Authentication Servers | Test

This screen let you test a configured external user authentication server to determine that:

- The VPN Concentrator is communicating properly with the authentication server.
- The server correctly authenticates a valid user.
- The server correctly rejects an invalid user.

Figure 14-22 Configuration | User Management | Groups | Authentication Servers | Test Screen

Configuration | System | Servers | Authentication | Test

Enter a username and password with which to test. Please wait for the operation to complete or timeout.

User Name

Password

OK Cancel

67314

User Name

To test connectivity and valid authentication, enter the username for a valid user who has been configured on the authentication server. The maximum username length is 64 characters. Entries are case-sensitive.

To test connectivity and authentication rejection, enter a username that is invalid on the authentication server.

Password

Enter the password for the username. The maximum password length is 32 characters. Entries are case-sensitive. The field displays only asterisks.

OK / Cancel

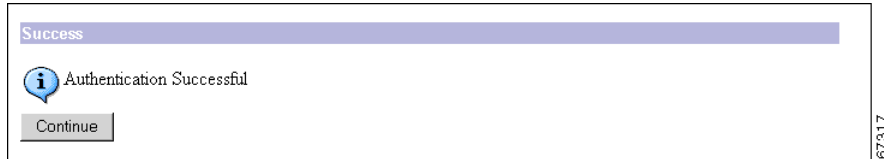
To send the username and password to the selected authentication server, click **OK**. The authentication and response process takes a few seconds. The Manager displays a Success or Error screen.

To cancel the test and discard your entries, click **Cancel**. The Manager returns to the Configuration | User Management | Groups | Authentication Servers screen.

Authentication Server Test: Success

If the VPN Concentrator communicates correctly with the authentication server, and the server correctly authenticates a valid user, the Manager displays a Success screen.

Figure 14-23 Authentication Server Test: Success Screen



Continue

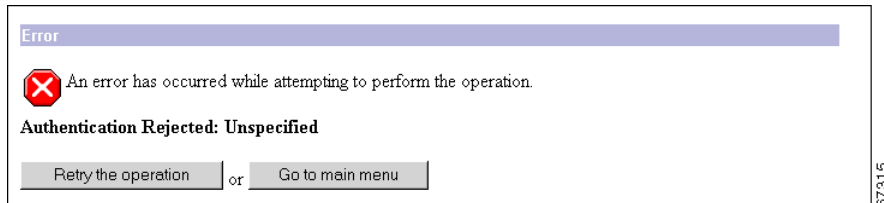
To return to the Configuration | User Management | Groups | Authentication Servers | Test screen, click **Continue**. You can then test authentication for another username.

To return to the Configuration | User Management | Groups | Authentication Servers screen, or any other screen, click the desired title in the left frame (the Manager table of contents).

Authentication Server Test: Authentication Rejected Error

If the VPN Concentrator communicates correctly with the authentication server, *and the server correctly rejects an invalid user*, the Manager displays an Authentication Rejected Error screen.

Figure 14-24 Authentication Server Test: Authentication Rejected Error Screen



To return to the Configuration | User Management | Groups | Authentication Servers | Test screen, click **Retry the operation**.

To go to the main VPN Concentrator Manager screen, click **Go to main menu**.

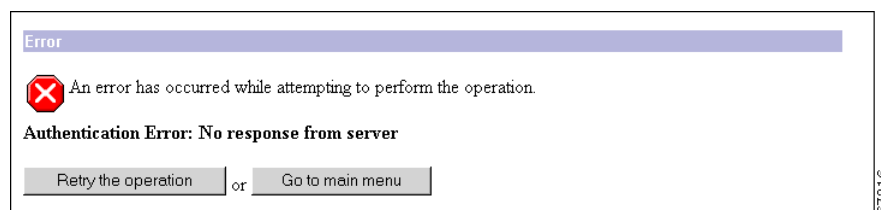
Authentication Server Test: Authentication Error

If the VPN Concentrator cannot communicate with the authentication server, the Manager displays an Authentication Error screen. Error messages include:

- No response from server = There is no response from the selected server within the configured timeout and retry periods.
- No active server found = The VPN Concentrator cannot find an active, configured server to test.

The server might be improperly configured or out of service, the network might be down or clogged, etc. Check the server configuration parameters, be sure the server is operating, check the network connections, etc.

Figure 14-25 Authentication Server Test: Authentication Error Screen



To return to the Configuration | User Management | Groups | Authentication Servers | Test screen, click **Retry the operation**.

To go to the main VPN Concentrator Manager screen, click **Go to main menu**.

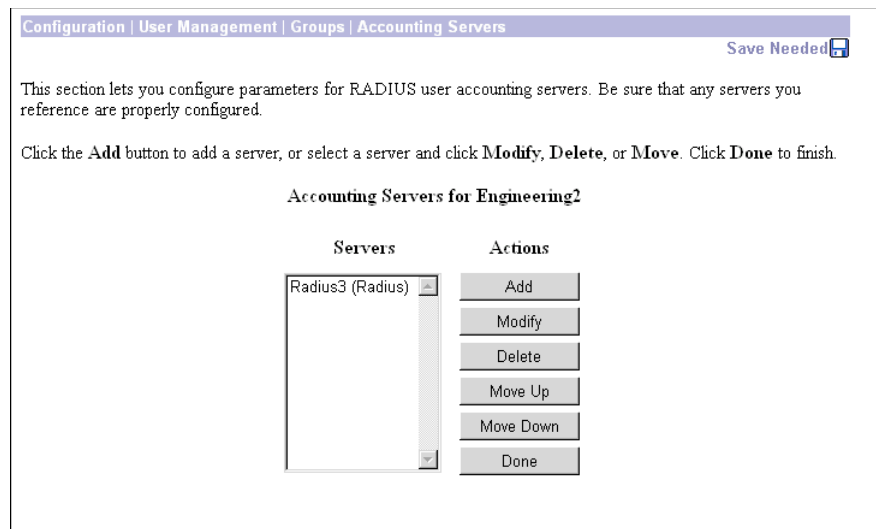
Configuration | User Management | Groups | Accounting Servers

This screen lets you add, modify, delete, or move external RADIUS accounting servers for a group. Accounting servers collect data on user connect time, packets transmitted, etc., under the VPN tunneling protocols: PPTP, L2TP, and IPSec. For more information on RADIUS accounting servers, see “Configuration | System | Servers | Accounting”.

You can configure and prioritize up to 10 accounting servers. The first server is the primary, and the rest are backup servers in case the primary is inoperative. If no accounting servers are configured for a group, the Global accounting server list applies.

Before you configure an accounting server here, be sure that the server you reference is itself properly configured and that you know how to access it (IP address or host name, UDP port, server secret, etc.). The VPN Concentrator functions as the client of these servers.

Figure 14-26 Configuration | User Management | Groups | Accounting Servers Screen



Servers

The Servers list shows the configured servers, in priority order. Each entry shows the server identifier and type, for example: 192.168.12.34 (Radius). If no servers have been configured, the list shows --Empty--. The first server is the primary, the rest are backup.

Actions

To configure and add a new accounting server, click **Add**. The Manager opens the Configuration | User Management | Groups | Accounting Servers | Add screen.

To modify parameters for an accounting server that has been configured, select the server from the list and click **Modify**. The Manager opens the Configuration | User Management | Groups | Accounting Servers | Modify screen.

To remove a server that has been configured, select the server from the list and click **Delete**.



Note

There is no confirmation or undo.

The Manager refreshes the screen and shows the remaining servers in the list. *When you delete a server, any clients with no other accounting server configured use the server configured for the base group.*

To change the priority order for an accounting server click **Move Up** or **Move Down** to move it up or down on the list of servers configured for this group.

When you are finished configuring accounting servers, click **Done**. This action includes your settings in the active configuration. The Manager returns to the Configuration | User Management | Groups screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | User Management | Groups | Accounting Servers | Add or Modify

This section lets you add or modify RADIUS accounting servers for a group.

Figure 14-27 Configuration | User Management | Groups | Accounting Servers | Add or Modify Screen

Configuration | User Management | Groups | Accounting Servers | Add

Configure and add a RADIUS user accounting server.

Accounting Server Enter IP address or hostname.

Server Port Enter the server UDP port number.

Timeout Enter the timeout for this server (seconds).

Retries Enter the number of retries for this server.

Server Secret Enter the RADIUS server secret.

Verify Re-enter the server secret.

87008

Accounting Server

Enter the IP address or host name of the RADIUS accounting server, for example: 192.168.12.34. (If you have configured a DNS server, you can enter a host name in this field; otherwise, enter an IP address.)

Server Port

Enter the UDP port number by which you access the accounting server. The default port number is 1646.



Note

The latest RFC states that RADIUS accounting servers should be on UDP port number 1813, so you might need to change this default value to 1813.

Timeout

Enter the time in seconds to wait after sending a query to the accounting server and receiving no response, before trying again. The minimum time is 1 second. The default time is 1 second. The maximum time is 30 seconds.

Retries

Enter the number of times to retry sending a query to the accounting server after the timeout period. If there is still no response after this number of retries, the system declares this server inoperative and uses the next accounting server in the list. The minimum number of retries is 0. The default is 3. The maximum is 10.

Server Secret

Enter the server secret (also called the shared secret), for example: C8z077f. The field shows only asterisks.

Verify

Re-enter the server secret to verify it. The field shows only asterisks.

Add or Apply / Cancel

To add this server to the list of configured user accounting servers, click **Add**. Or, to apply your changes to this user accounting server, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | User Management | Groups | Accounting Servers screen. Any new server appears at the bottom of the Accounting Servers list.

Reminder:

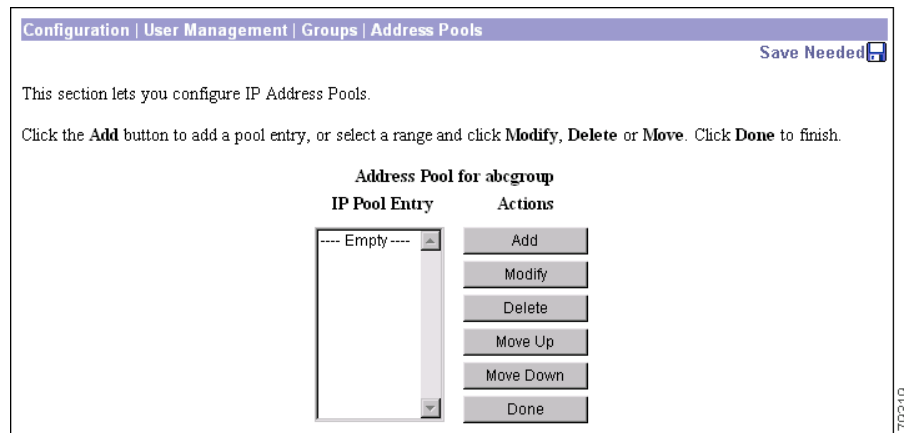
To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | User Management | Groups | Accounting Servers screen, and the Accounting Servers list is unchanged.

Configuration | User Management | Groups | Address Pools

This screen lets you configure IP address pools from which the VPN Concentrator assigns addresses to clients on a per-group basis. If no address pools are defined for a group, the globally defined address pools apply.

Figure 14-28 Configuration | User Management | Groups | Address Pools Screen



IP Pool Entry

The IP Pool Entry list shows the configured address pools for the group, in priority order. Each entry shows the range of IP addresses. If no address pools have been configured, the list shows --Empty--.

Actions

To configure and add a new address pool, click **Add**. The Manager opens the Configuration | User Management | Groups | Address Pools | Add screen.

To modify an address pool that has been configured, select the pool entry from the list and click **Modify**. The Manager opens the Configuration | User Management | Groups | Address Pools | Modify screen.

To remove an address pool that has been configured, select the pool from the list and click **Delete**. When you are finished configuring address pools, click **Done**. This action includes your settings in the active configuration. The Manager returns to the Configuration | User Management | Groups screen.

To change the priority order for an address pool, click **Move Up** or **Move Down** to move it up or down on the list of address pools configured for this group.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | User Management | Groups | Address Pools | Add or Modify

These screens let you:

- Add a new pool of IP addresses from which the VPN Concentrator assigns addresses to clients.
- Modify an IP address pool that you have previously configured.

The IP addresses in the pool range must not be assigned to other network resources.

Figure 14-29 Configuration | User Management | Groups | Address Pools | Add or Modify Screen

Configuration | User Management | Groups | Address Pools | Add

Add an address pool.

Range Start Enter the start of the IP pool address range.

Range End Enter the end of the IP pool address range.

Add Cancel

67014

Range Start

Enter the first IP address available in this pool. Use dotted decimal notation, for example: 10.10.147.100.

Range End

Enter the last IP address available in this pool. Use dotted decimal notation, for example: 10.10.147.177.

Add or Apply / Cancel

To add this IP address pool to the list of configured pools, click **Add**. Or to apply your changes to this IP address pool, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | User Management | Groups | Address Pools screen. Any new pool appears at the end of the IP Pool Entry list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | User Management | Groups | Address Pools screen, and the IP Pool Entry list is unchanged.

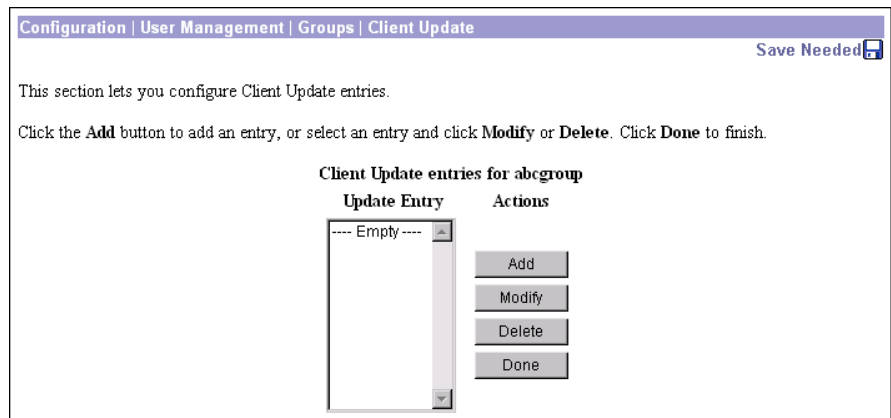
Configuration | User Management | Groups | Client Update

This screen lets you configure client update entries.

The VPN Concentrator can automate the process of updating client software. The feature applies to the VPN Client and to the VPN 3002 hardware client as follows. When configured

- VPN Clients automatically receive notification that they should update their software from the named URL
- VPN 3002 hardware client software is automatically updated via TFTP.

Figure 14-30 Configuration | User Management | Groups | Client Update screen



Update entry

The Update Entry list displays configured client update entries.

Actions

To configure and add a new client update entry, click **Add**. The Manager opens the Configuration | User Management | Groups | Client Update | Add screen.

To modify an address pool that has been configured, select the entry from the list and click **Modify**. The Manager opens the Configuration | User Management | Groups | Client Update | Modify screen.

To remove an client update entry that has been configured, select the entry from the list and click **Delete**. When you are finished configuring client update entries, click **Done**. This action includes your settings in the active configuration. The Manager returns to the Configuration | User Management | Groups screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | User Management | Groups | Client Update | Add or Modify

These screens let you configure client update parameters.

Figure 14-31 Configuration | User Management | Groups | Client Update | Add or Modify Screens

Configuration | User Management | Groups | Client Update | Add

Add client update information.

Client Type Enter the client type (e.g. *windows* or *vpn3002*) that is to be updated.

URL Enter the URL of the file from which to update. The URL must point to an appropriate file type for the client.

Revisions Enter a comma separated list of valid revisions. The URL above *must* be one of these revisions.

Add Cancel

67017

Client Type

Enter the client type you want to update.

- For the VPN Client: Enter the Windows operating systems to notify:
 - **windows** includes all Windows based platforms.
 - **win9x** includes Windows 95, Windows 98, and Windows ME platforms.
 - **winnt** includes Windows NT 4.0, Windows 2000, and Windows XP platforms.

The entry must be exact, including case and spacing.



Note

The VPN Concentrator sends a separate notification message for each entry in a Client Update list. Therefore your client update entries must not overlap. For example, the value *windows* includes all Windows platforms, and the value *WinNT* includes Windows NT 4.0, Windows 2000 and Windows XP platforms. So you would not include both *windows* and *WinNT*.

- For the VPN 3002 Hardware Client: Your entry must be **vpn3002**, including case and spacing.

URL

Enter the URL for the software/firmware image. This URL must point to a file appropriate for this client.

- For the VPN Client: To activate the Launch button on the VPN Client Notification, the URL must include the protocol HTTP or HTTPS and the server address of the site that contains the update. The format of the URL is: `http(s)://server_address:port/directory/filename`. The server address can be either an IP address or a hostname if you have configured a DNS server. For example:

```
http://10.10.99.70/vpnclient-win-3.5.Rel-k9.exe
```

The directory is optional. You need the port number only if you use ports other than 80 for http or 443 for https.

- For the VPN 3002 Hardware Client: The format of the URL is `tftp://server_address/directory/filename`. The server address can be either an IP address or a hostname if you have configured a DNS server. For example:

```
tftp://10.10.99.70/vpn3002-3.5.Rel-k9.bin
```

The directory is optional.

Revisions

Enter a comma separated list of software or firmware images appropriate for this client. The following caveats apply:

- The revision list must include the software version for this update.
- Your entries must match exactly those on the URL for the VPN Client, or the TFTP server for the VPN 3002.
- The URL above must point to one of the images you enter.

If the client is already running a software version on the list, it does not need a software update. If the client is not running a software version on the list, an update is in order.

- A VPN Client user must download an appropriate software version from the listed URL.
- The VPN 3002 Hardware Client software is automatically updated via TFTP.

Add or Apply / Cancel

To add this client update entry to the list of configured update entries, click **Add**. Or, to apply your changes, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | User Management | Groups | Client Update screen. Any new entry appears at the bottom of the Update Entries list.

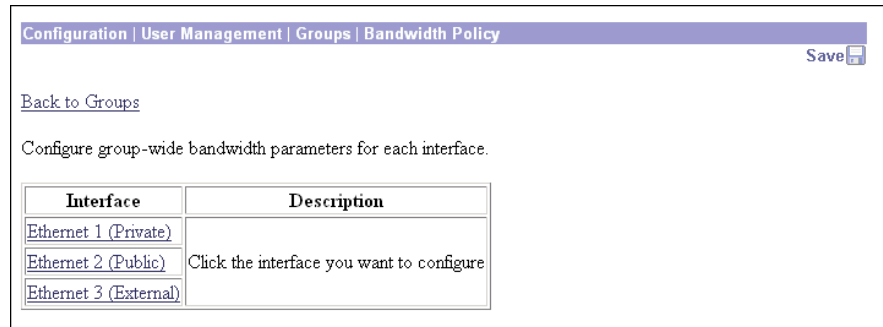
Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | User Management | Groups | Client Update screen, and the Update Entries list is unchanged.

Configuration | User Management | Groups | Bandwidth Policy

Figure 14-32 Configuration | User Management | Groups | Bandwidth Policy Screen



Click the interface on which you want to configure Bandwidth Management for this group.

To apply a bandwidth policy to a group on an interface, bandwidth management must be enabled on that interface. If you choose an interface on which bandwidth management is disabled, this warning appears. (See [Figure 14-33](#).) You must enable bandwidth management on the interface before you can continue.

Figure 14-33 Configuration | User Management | Groups | Bandwidth Policy | Interfaces Screen 1



If you choose an interface on which bandwidth management is enabled, the Configuration | User Management | Groups | Bandwidth Policy | Interfaces screen appears. (See [Figure 14-4](#).)

Configuration | User Management | Groups | Bandwidth Policy | Interfaces

This screen lets you apply a group-wide bandwidth policy.

To configure bandwidth policy for interfaces, use the Bandwidth tab on the [Configuration | Interfaces | Ethernet 1 2 3](#) screen.

Before you can apply a bandwidth policy to a group, you must first:

- Define the policy. You do not define the policy itself on this screen. To define bandwidth policies, use the Configuration | Policy Management | Traffic Management | Bandwidth Policies screen.
- Enable bandwidth management on the interface the group is using. To enable bandwidth management on an interface, use the Configuration | Interfaces | Ethernet 1 2 3 screen, Bandwidth Parameters tab.
- If you want the group to use a bandwidth *reservation* policy, you must first apply a bandwidth reservation policy to the interface the group is using. To apply a policy to an interface, use the Configuration | Interfaces | Ethernet 1 2 3 screen, Bandwidth Parameters tab.

Figure 14-34 Configuration | User Management | Groups | Bandwidth Policy Screen

Configuration | User Management | Groups | Bandwidth Policy | Interfaces Save Needed

Configure group-wide bandwidth parameters. To share global available bandwidth, instead of a specific reservation, enter 0 in the **Bandwidth Aggregation** textbox.

Ethernet 1 (Private)

Policy Select the bandwidth policy to apply to this interface.

Bandwidth Aggregation Enter the aggregate reserved group bandwidth for this interface.

78685

Policy

Select a bandwidth policy for the group for this interface. If you do not want to apply a Bandwidth Management policy here, then select **None**.

Bandwidth Aggregation

Enter a value for the minimum bandwidth to reserve for this group and select a unit of measurement:

- bps—bits per second
- kbps—one thousand bits per second
- Mbps—one million bits per second

The default value of Bandwidth Aggregation is 0. The default unit of measurement is bps. If you want the group to share in the available bandwidth on the interface, enter 0.

Configuration | User Management | Users

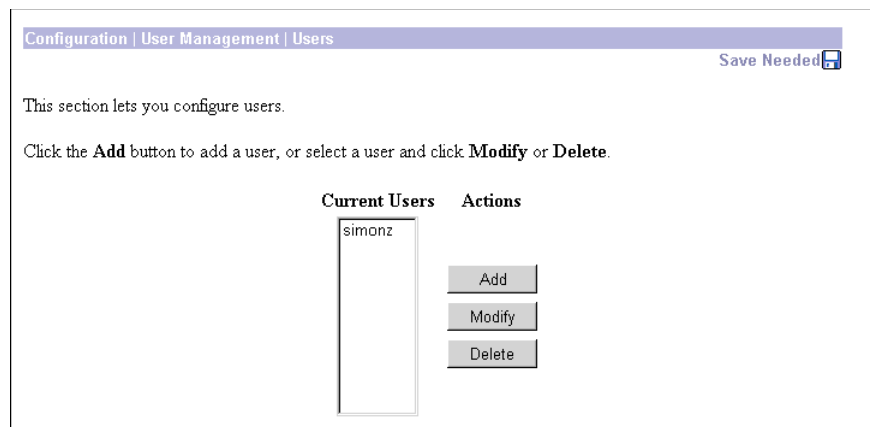
This section of the Manager lets you configure access, usage, and authentication parameters for users. Users inherit parameters from the specific group to which they belong.

Configuring users in this section means configuring them in the VPN Concentrator internal authentication server. If you have not configured the internal authentication server, this screen displays a notice that includes a link to the Configuration | System | Servers | Authentication screen. The system also automatically configures the internal server when you add the first user.

See the discussion of groups and users in the *User Management* section at the beginning of this chapter. Remember:

- The maximum number of groups and users (combined) that you can configure depends on your VPN Concentrator model. (See [Table 14-1](#).)
- A user can be a member of only one group.
- Users who are not members of a specific group are, by default, members of the base group. Therefore, to ensure maximum security and control, you should assign all users to appropriate specific groups, and you should configure base-group parameters carefully.

Figure 14-35 Configuration | User Management | Users Screen



Current Users

The Current Users list shows configured users in alphabetical order. If no users have been configured, the list shows --Empty--.

Add / Modify / Delete

To configure a new user, click **Add**. The Manager opens the Configuration | User Management | Users | Add screen.

To modify a user that has been configured, select the user from the list and click **Modify**. The Manager opens the Configuration | User Management | Users | Modify screen.

To remove a user that has been configured, select the user from the list and click **Delete**.

**Note**

There is no confirmation or undo.

The Manager refreshes the screen and shows the remaining users in the list.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | User Management | Users | Add or Modify

These Manager screens let you:

- **Add:** Configure a new user and that user's parameters on the internal authentication server.
- **Modify:** Change parameters for a user that you have previously configured on the internal authentication server. The screen title identifies the user you are modifying.

For many of these parameters, you can simply specify that the user “inherit” parameters from a group; and a user can be assigned either to a configured group or to the base group. Users who are not members of a configured group are, by default, members of the base group.

On this screen, you configure four kinds of parameters:

- **Identity Parameters:** name, password, group, and IP address.
- **General Parameters:** access, performance, and allowed tunneling protocols.
- **IPSec Parameters:** IP Security tunneling protocol.
- **PPTP/L2TP Parameters:** PPTP and L2TP tunneling protocols.



Tip

To streamline the configuration process, just fill in the Identity Parameters tab (assigning the user to a configured group), and click **Add**. Then select the user and click **Modify**. The user inherits the group parameters, and the Modify screen shows group parameters instead of base-group parameters.

Before configuring these parameters, you should configure the base-group parameters on the Configuration | User Management | Base Group screen, and configure group parameters on the Configuration | User Management | Groups screen.

Using the Tabs

This screen includes four tabbed sections. Click each tab to display its parameters. As you move from tab to tab, the Manager retains your settings. When you have finished setting parameters on all tabbed sections, click **Add/Apply** or **Cancel**.

Identity Parameters Tab

This tab lets you configure the name, password, group, and IP address for this user.

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity Parameters		
Attribute	Value	Description
User Name	<input type="text"/>	Enter a unique user name.
Password	<input type="password"/>	Enter the user's password. The password must satisfy the group password requirements.
Verify	<input type="password"/>	Verify the user's password.
Group	--Base Group--	Enter the group to which this user belongs.
IP Address	<input type="text"/>	Enter the IP address assigned to this user.
Subnet Mask	<input type="text"/>	Enter the subnet mask assigned to this user.

Add Cancel

User Name

Enter a unique name for this user. The maximum name length is 64 characters. Entries are case-sensitive. If you change this name, this user profile *replaces* the existing profile.

Password

Enter a unique password for this user. The minimum length must satisfy the minimum for the group to which you assign this user (base group or specific group). The maximum length is 32 characters. Entries are case-sensitive. The field displays only asterisks.

Verify

Re-enter the user password to verify it. The field displays only asterisks.

Group

Click the **Group** drop-down menu button and select the group to which you assign this user. The list shows specific groups you have configured, plus:

- Base Group-- = The default group with its base-group parameters.

IP Address

Enter the IP address, in dotted decimal notation, assigned to this user. Enter this address only if you assign this user to the base group or an internally configured group, and if you configure Use Address from Authentication Server on the Configuration | System | Address Management | Assignment screen. Otherwise, leave this field blank.

Subnet Mask

Enter the subnet mask, in dotted decimal notation, assigned to this user. Enter this mask only if you configure an IP address in the preceding field; otherwise leave this field blank.

General Parameters Tab

This tab lets you configure general access, performance, and allowed tunneling protocols that apply to this user.

Figure 14-36 Configuration | User Management | Users | Add or Modify Screen, General Tab

Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

General Parameters			
Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select the access hours assigned to this user.
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter the number of simultaneous logins for this user.
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) Enter the idle timeout for this user.
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this user.
Filter	-None-	<input checked="" type="checkbox"/>	Enter the filter assigned to this user.
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	<input checked="" type="checkbox"/>	Select the SEP cards this user can be assigned to.
Tunneling Protocols	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec	<input checked="" type="checkbox"/>	Select the tunneling protocols this user can connect with.

Add Cancel

67345

Value / Inherit?

On the General tabbed section:

- The Inherit? checkbox refers to group parameters: Does this specific user inherit the given setting from the group?
 - Add screen = inherit base-group parameter setting.
 - Modify screen = inherit assigned-group parameter setting, which can be the base group or a configured group.

To inherit the group setting, check the box (default). To override the group setting, uncheck the box. If you uncheck the check box, you must enter or change any corresponding Value field; do not leave the field blank.

- The Value column thus shows either group parameter settings that also apply to this user (Inherit? checked), or unique parameter settings configured for this user (Inherit? cleared). You cannot configure a grayed-out parameter.



Note

The setting of the Inherit? check box takes priority over an entry in a Value field. Examine this box before continuing and be sure its setting reflects your intent.

Access Hours

Click the **Access Hours** drop-down menu button and select the named hours when this user can access the VPN Concentrator. Configure access hours on the Configuration | Policy Management | Access Hours screen. Default entries are:

- -No Restrictions- = No named access hours applied, which means that there are no restrictions on access hours.
- Never = No access at any time.
- Business Hours = Access 9 a.m. to 5 p.m., Monday through Friday.

Additional named access hours that you have configured also appear on the list.

Simultaneous Logins

Enter the number of simultaneous logins permitted for this user. The minimum value is 0, which disables login and prevents user access.

**Note**

While there is no maximum limit, allowing several could compromise security and affect performance.

Idle Timeout

Enter this user's idle timeout period in minutes. If there is no communication activity on the user's connection in this period, the system terminates the connection. The minimum time is 1 minute, and the maximum time is 2147483647 minutes (over 4000 years). To disable timeout and allow an unlimited idle period, enter 0.

Maximum Connect Time

Enter this user's maximum connection time in minutes. At the end of this time, the system terminates the connection. The minimum time is 1 minute, and the maximum time is 2147483647 minutes (over 4000 years). To allow unlimited connection time, enter 0.

Filter

Filters consist of rules that determine whether to allow or reject tunneled data packets coming through the VPN Concentrator, based on criteria such as source address, destination address, and protocol. Cisco supplies three default filters, which you can modify. To configure filters and rules, see the Configuration | Policy Management | Traffic Management screens.

Click the **Filter** drop-down menu button and select the filter to apply to this user:

- --None-- = No filter applied, which means there are no restrictions on tunneled data traffic.
- Private (Default) = Allow all packets except source-routed IP packets. (This is the default filter for the private Ethernet interface.)
- Public (Default) = Allow inbound and outbound tunneling protocols plus Internet Control Message Protocol (ICMP) and Virtual Router Redundancy Protocol (VRRP). Allow fragmented IP packets. Drop everything else, including source-routed packets. (This is the default filter for the public Ethernet interface.)
- External (Default) = No rules applied to this filter. Drop all packets. (This is the default filter for the external Ethernet interface.)

Additional filters that you have configured also appear on the list.

SEP Card Assignment

The VPN Concentrator can contain up to four Scalable Encryption Processing (SEP) modules that handle encryption functions, which are compute-intensive. Two SEP modules handle up to 5000 sessions (users)—the system maximum. Two additional modules can provide automatic failover for the first two. This parameter lets you configure the load on each SEP module.

Check the **SEP Card Assignment** check box to assign this user to a given SEP module. If your system does not have a given SEP module, the parameter is ignored.

Tunneling Protocols

Check the desired **Tunneling Protocols** check boxes to select the VPN tunneling protocols that this user can use. Configure parameters on the IPsec or PPTP/L2TP tabs as appropriate. Users can use only the selected protocols.

You cannot check both IPsec and L2TP over IPsec. The IPsec parameters differ for these two protocols, and you cannot configure a single user for both.

- PPTP = Point-to-Point Tunneling Protocol. PPTP is a client-server protocol, and it is popular with Microsoft clients. Microsoft Dial-Up Networking (DUN) 1.2 and 1.3 under Windows 95/98 support it, as do versions of Windows NT 4.0, Windows 2000, and Windows XP.
- L2TP = Layer 2 Tunneling Protocol. L2TP is a client-server protocol. It combines many features from PPTP and L2F (Layer 2 Forwarding).
- IPsec = IP Security Protocol. IPsec provides the most complete architecture for VPN tunnels, and it is perceived as the most secure protocol. Both LAN-to-LAN (peer-to-peer) connections and client-to-LAN connections can use IPsec. The Cisco VPN Client is an IPsec client specifically designed to work with the VPN Concentrator. However, the VPN Concentrator can establish IPsec connections with many protocol-compliant clients.
- L2TP over IPsec = L2TP using IPsec for security. L2TP packets are encapsulated within IPsec, thus providing an additional authentication and encryption layer for security. L2TP over IPsec is a client-server protocol that provides interoperability with the Windows 2000 VPN client. It is also compliant, but not officially supported, with other remote-access clients.

**Note**

If no protocol is selected, this user cannot access or use the VPN.

IPSec Parameters Tab

This tab lets you configure IP Security Protocol parameters that apply to this user. If you checked IPSec or L2TP over IPSec under Tunneling Protocols on the General Parameters tab, configure this section.

Figure 14-37 Configuration | User Management | Users | Add or Modify Screen, IPSec Tab

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

IPSec Parameters			
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	<input checked="" type="checkbox"/>	Select the IPSec Security Association assigned to this user.
Store Password on Client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow the IPSec client to store the password locally.

Add Cancel

Value / Inherit?

On this tabbed section:

- The Inherit? check box refers to group parameters: Does this specific user inherit the given setting from the group?
 - Add screen = inherit base-group parameter setting.
 - Modify screen = inherit assigned-group parameter setting, which can be the base group or a configured group.

To inherit the group setting, check the box (default). To override the group setting, uncheck the box. If you uncheck the check box, you must enter or change any corresponding Value field; do not leave the field blank.

- The Value column thus shows either group parameter settings that also apply to this user (Inherit? checked), or unique parameter settings configured for this user (Inherit? cleared). You cannot configure a grayed-out parameter.



Note

The setting of the Inherit? check box takes priority over an entry in a Value field. Examine this box before continuing and be sure its setting reflects your intent.

IPSec SA

Click the **IPSec SA** drop-down menu button and select the IPSec Security Association (SA) assigned to this IPSec user. During tunnel establishment, the user client and server negotiate a Security Association that governs authentication, encryption, encapsulation, key management, etc. You configure IPSec Security Associations on the Configuration | Policy Management | Traffic Management | Security Associations screens.

To use IPSec with remote-access clients, you must assign an SA. With IPSec LAN-to-LAN connections, the system ignores this selection and uses parameters from the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN screens.

The VPN Concentrator supplies these default selections:

- --None-- = No SA assigned.
- ESP-DES-MD5 = This SA uses DES 56-bit data encryption for both the IKE tunnel and IPSec traffic, ESP/MD5/HMAC-128 authentication for IPSec traffic, and MD5/HMAC-128 authentication for the IKE tunnel.
- ESP-3DES-MD5 = This SA uses Triple-DES 168-bit data encryption and ESP/MD5/HMAC-128 authentication for IPSec traffic, and DES-56 encryption and MD5/HMAC-128 authentication for the IKE tunnel.
- ESP/IKE-3DES-MD5 = This SA uses Triple-DES 168-bit data encryption for both the IKE tunnel and IPSec traffic, ESP/MD5/HMAC-128 authentication for IPSec traffic, and MD5/HMAC-128 authentication for the IKE tunnel.
- ESP-3DES-NONE = This SA uses Triple-DES 168-bit data encryption and no authentication for IPSec traffic, and DES-56 encryption and MD5/HMAC-128 authentication for the IKE tunnel.
- ESP-L2TP-TRANSPORT = This SA uses DES 56-bit data encryption and ESP/MD5/HMAC-128 authentication for IPSec traffic (with ESP applied only to the transport layer segment), and it uses Triple-DES 168-bit data encryption and MD5/HMAC-128 for the IKE tunnel. Use this SA with the L2TP over IPSec tunneling protocol.
- ESP-3DES-MD5-DH7 = This SA uses Triple-DES 168-bit data encryption and ESP/MD5/HMAC-128 authentication for both IPSec traffic and the IKE tunnel. It uses Diffie-Hellman Group 7 (ECC) as part of the IKE tunnel establishment. You can use this option only with the movianVPN client.

Additional SAs that you have configured also appear on the list.

Store Password on Client

Check the **Store Password on Client** check box to allow this IPSec user (client) to store the login password on the client system. If you do not allow password storage, IPSec users must enter their password each time they seek access to the VPN. For maximum security, we recommend that you *not allow* password storage.

This parameter has no bearing on interactive hardware client authentication or individual user authentication for a VPN 3002.

PPTP/L2TP Parameters Tab

This tab lets you configure PPTP and L2TP parameters that apply to this user. During tunnel establishment, the user client and server negotiate access and usage based on these parameters. Only clients that meet these criteria are allowed access. If you checked PPTP, L2TP, or L2TP over IPsec under Tunneling Protocols on the General Parameters tab, configure these parameters.

Figure 14-38 Configuration | User Management | Users | Add or Modify Screen, PPTP/L2TP Tab

Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity	General	IPSec	PPTP/L2TP
PPTP/L2TP Parameters			
Attribute	Value	Inherit?	Description
Use Client Address	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	<input checked="" type="checkbox"/>	Enter the authentication protocols this user is allowed to use. This is used to <i>remove</i> protocols from the list of acceptable authentication protocols. Unchecking <i>all</i> options means that <i>no</i> authentication is required.
L2TP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	<input checked="" type="checkbox"/>	Enter the authentication protocols this user is allowed to use. This is used to <i>remove</i> protocols from the list of acceptable authentication protocols. Unchecking <i>all</i> options means that <i>no</i> authentication is required.

Add Cancel

Value / Inherit?

On this tabbed section:

- The Inherit? check box refers to group parameters: Does this specific user inherit the given setting from the group?
 - Add screen = inherit base-group parameter setting.
 - Modify screen = inherit assigned-group parameter setting, which can be the base group or a configured group.

To inherit the group setting, check the check box (default). To override the group setting, uncheck the box. If you uncheck the check box, you must enter or change any corresponding Value field; do not leave the field blank.

- The Value column thus shows either group parameter settings that also apply to this user (Inherit? checked), or unique parameter settings configured for this user (Inherit? cleared). You cannot configure a grayed-out parameter.



Note

The setting of the Inherit? check box takes priority over an entry in a Value field. Verify that the status of the checkbox reflects your intended settings before you proceed.

Use Client Address

Check the **Use Client Address** checkbox to accept and use an IP address that the client supplies. A client must have an IP address in order to function as a tunnel endpoint; for maximum security, we recommend that you control the assigning of IP addresses and *do not allow* client-specified IP addresses.

Make sure the setting here is consistent with the setting for Use Client Address on the Configuration | System | Address Management | Assignment screen.

PPTP Authentication Protocols

Check the **PPTP Authentication Protocols** check boxes for the authentication protocols that this PPTP user (client) can use. To establish and use a VPN tunnel, users should be authenticated in accordance with some protocol.



Caution

Unchecking *all* authentication options means that *no* authentication is required. That is, PPTP users can connect with *no* authentication. This configuration is allowed so you can test connections, but it is not secure.

These choices specify the allowable authentication protocols in order from least secure to most secure. You can allow a user to use *fewer* protocols than the assigned group, but not more. You cannot allow a grayed-out protocol.

- PAP = Password Authentication Protocol. This protocol passes cleartext username and password during authentication and is not secure. We recommend that you *not allow* this protocol.
- CHAP = Challenge-Handshake Authentication Protocol. In response to the server challenge, the client returns the encrypted [challenge plus password], with a cleartext username. It is more secure than PAP, but it does not encrypt data.
- MSCHAPv1 = Microsoft Challenge-Handshake Authentication Protocol version 1. This protocol is similar to, but more secure than, CHAP. In response to the server challenge, the client returns the encrypted [challenge plus encrypted password], with a cleartext username. Thus the server stores—and compares—only encrypted passwords, rather than cleartext passwords as in CHAP. This protocol also generates a key for data encryption by MPPE (Microsoft Point-to-Point Encryption).
- MSCHAPv2 = Microsoft Challenge-Handshake Authentication Protocol version 2. This protocol is more secure than MSCHAPv1. It requires mutual client-server authentication, uses session-unique keys for data encryption by MPPE, and derives different encryption keys for the send and receive paths.

L2TP Authentication Protocols

Check the **L2TP Authentication Protocols** check boxes for the authentication protocols that this L2TP user (client) can use. To establish and use a VPN tunnel, users should be authenticated in accordance with some protocol.



Caution

Unchecking *all* authentication options means that *no* authentication is required. That is, L2TP users can connect with *no* authentication. This configuration is allowed so you can test connections, but it is not secure.

These choices specify the allowable authentication protocols in order from least secure to most secure. You can allow a user to use *fewer* protocols than the assigned group, but not more. You cannot allow a grayed-out protocol.

- PAP = Password Authentication Protocol. This protocol passes cleartext username and password during authentication and is not secure. We strongly recommend that you not allow this protocol.
- CHAP = Challenge-Handshake Authentication Protocol. In response to the server challenge, the client returns the encrypted [challenge plus password], with a cleartext username. It is more secure than PAP, but it does not encrypt data.
- MSCHAPv1 = Microsoft Challenge-Handshake Authentication Protocol version 1. This protocol is similar to, but more secure than, CHAP. In response to the server challenge, the client returns the encrypted [challenge plus encrypted password], with a cleartext username. Thus the server stores—and compares—only encrypted passwords, rather than cleartext passwords as in CHAP. This protocol also generates a key for data encryption by MPPE (Microsoft Point-to-Point Encryption).
- MSCHAPv2 = Microsoft Challenge-Handshake Authentication Protocol version 2. This protocol is even more secure than MSCHAPv1. It requires mutual client-server authentication, uses session-unique keys for data encryption by MPPE, and derives different encryption keys for the send and receive paths.

Add or Apply/Cancel

When you finish setting or changing parameters on all tabs, click **Add** or **Apply** at the bottom of the screen to Add this user to the list of configured internal users, or to Apply your changes. Both actions include your settings in the active configuration. The Manager returns to the Configuration | User Management | Users screen. Any new users appear in alphabetical order in the Current Users list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | User Management | Users screen, and the Current Users list is unchanged.



Policy Management

Managing a VPN, and protecting the integrity and security of network resources, includes carefully designing and implementing policies that govern who can use the VPN, when, and what data traffic can flow through it. User management deals with “who can use it”; see [“User Management”](#) for that discussion. Policy management deals with “when” and “what data traffic can flow through it”; this section covers those topics.

You configure when remote users access the VPN under Access Hours.

You configure “what data traffic can flow through it” under Traffic Management. The Cisco VPN 3000 Concentrator hierarchy is straightforward: you use *filters* that consist of *rules*; and for IPSec rules, you apply *Security Associations (SAs)*. Therefore, you first configure rules and SAs, then use them to construct filters.

Basically, a *filter* determines whether to forward or drop a data packet traversing the system. It examines the data packet in accordance with one or more *rules*—direction, source address, destination address, ports, and protocol—which determine whether to forward, apply IPSec and forward, or drop. And it examines the rules in the order they are arranged on the filter.

You apply filters to Ethernet interfaces, and thus govern *all* traffic through an interface. You also apply filters to groups and users, and thus govern *tunneled* traffic through an interface.

With IPSec, the VPN Concentrator negotiates *Security Associations* during tunnel establishment that govern authentication, key management, encryption, encapsulation, etc. Thus IPSec also determines how to transform a data packet before forwarding it. You apply Security Associations to IPSec rules when you include those rules in a filter, and you apply SAs to groups and users.

The VPN Concentrator also lets you create network lists, which are lists of network addresses that are treated as a single object. These lists simplify the configuration of rules for complex networks. You can also use them to configure split tunneling for groups and users, and to configure IPSec LAN-to-LAN connections.

To fully configure the VPN Concentrator, you should first develop policies (network lists, rules, SAs, and filters), since they affect Ethernet interfaces, groups, and users. And once you have developed policies, we recommend that you configure and apply filters to interfaces before you configure groups and users.

Traffic management on the VPN Concentrator also includes NAT (Network Address Translation) functions that translate private network addresses into legitimate public network addresses. Again, you develop rules to configure and use NAT.

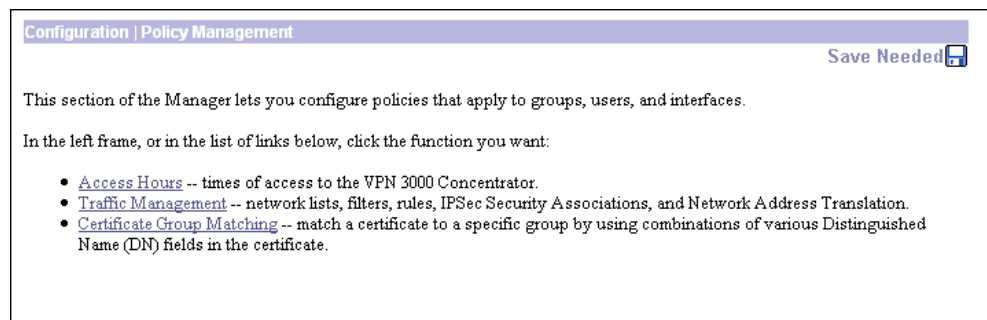
Configuration | Policy Management

This section of the Manager lets you configure policies that apply to groups, users, and VPN Concentrator Ethernet interfaces.

Policies govern:

- Access Hours: when remote users can access the VPN Concentrator.
- Traffic Management: what data traffic can flow through the VPN Concentrator, as governed by:
 - Network Lists: lists of networks grouped as single objects.
 - Rules: detailed parameters that govern the handling of data packets.
 - SAs: IPSec Security Associations.
 - Filters: structures for applying aggregated rules.
 - NAT: Network Address Translation.
 - Bandwidth Policies: policies prioritizing network traffic.
- Certificate Group Matching: which fields in a distinguished name to use for matching a user's certificate to a permission group.

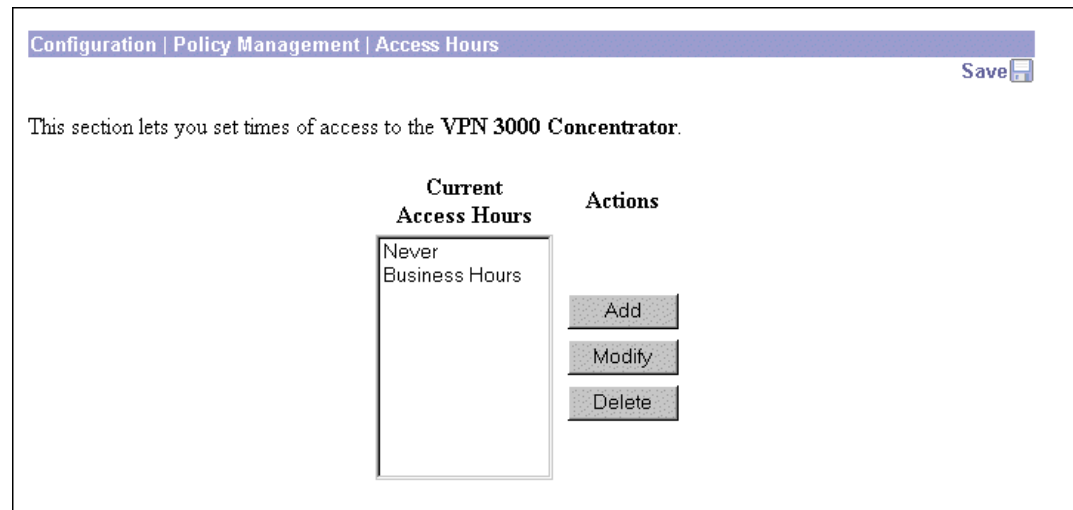
Figure 15-1 Configuration | Policy Management Screen



Configuration | Policy Management | Access Hours

This section of the Manager lets you configure access times, to control when remote-access groups and users can access the VPN Concentrator. You assign access hours to groups and users under Configuration | User Management. Access hours do not apply to LAN-to-LAN connections.

Figure 15-2 Configuration | Policy Management | Access Hours Screen



Current Access Hours

The Current Access Hours list shows the names of configured access times. The Cisco-supplied default access times are:

- Never = Never. No access at any time.
- Business Hours = Monday through Friday, 9 a.m. to 5 p.m.

Additional access times that you configure appear in the list.

Add / Modify / Delete

To configure and add a new access time to the list, click **Add**. The Manager opens the Configuration | Policy management | Access Hours | Add screen.

To modify a configured access time, select the entry from the list and click **Modify**. The Manager opens the Configuration | Policy management | Access Hours | Modify screen.

To remove a configured access time, select the entry from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the Current Access Hours list.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | Policy Management | Access Hours | Add or Modify

These Manager screens let you:

- Add: Configure and add a new access time to the list of configured access times.
- Modify: Modify a configured access time. Changing an access time has no effect on connected users, since the parameter is checked only when the tunnel is established. The change affects subsequent connections, however.

Figure 15-3 Configuration | Policy Management | Access Hours | Add or Modify Screens

Configuration | Policy Management | Access Hours | Add

Configure and add a new set of access hours.

Name: Specify a unique name for this set of access hours.

Sunday	during ▼	<input type="text" value="00:00:00"/>	-	<input type="text" value="23:59:59"/>
Monday	during ▼	<input type="text" value="00:00:00"/>	-	<input type="text" value="23:59:59"/>
Tuesday	during ▼	<input type="text" value="00:00:00"/>	-	<input type="text" value="23:59:59"/>
Wednesday	during ▼	<input type="text" value="00:00:00"/>	-	<input type="text" value="23:59:59"/>
Thursday	during ▼	<input type="text" value="00:00:00"/>	-	<input type="text" value="23:59:59"/>
Friday	during ▼	<input type="text" value="00:00:00"/>	-	<input type="text" value="23:59:59"/>
Saturday	during ▼	<input type="text" value="00:00:00"/>	-	<input type="text" value="23:59:59"/>

67256

Name

Enter a unique name for this set of access hours. Maximum is 48 characters.

Sunday - Saturday

For each day of the week, click the **Sunday - Saturday** drop-down menu button and choose:

- during = Allow access *during* the hours in the range (default).
- except = Allow access at times *except* the hours in the range.

Enter or edit hours in the range fields. Times are inclusive: starting time through ending time. Enter times as HH:MM:SS and use 24-hour notation, for example: enter 5:30 p.m. as 17:30. By default, all ranges are 00:00:00 to 23:59:59.

Add or Apply / Cancel

To add this access time to the list, click **Add**. Or to apply your changes for this access time, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | Policy Management | Access Hours screen. Any new entry appears in the Current Access Times list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | Policy Management | Access Hours screen, and the Current Access Times list is unchanged.

Configuration | Policy Management | Traffic Management

This section of the Manager lets you configure network lists, rules, filters, and security associations, as well as network address translation and bandwidth policies. These features let you control the data traffic through the VPN Concentrator.

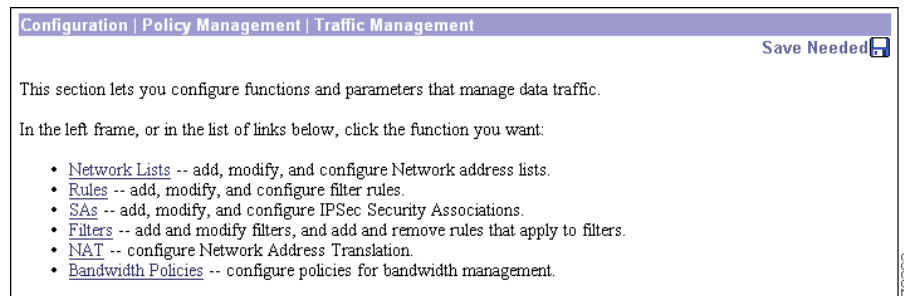
- Network lists let you treat lists of network addresses as a single object, thus simplifying the configuration of rules for complex networks.
- Filters consist of rules; and IPSec rules (rules in which you configure an Apply IPSec action) also have security associations. Therefore you first configure any network lists, then rules and SAs, and finally filters.

A filter applies its rules to data packets coming through the system, in the order the rules are arranged on the filter. If a packet matches all the parameters specified in the rule, the system takes the action specified in the rule. If at least one rule parameter does not match, it applies the next rule; and so on. If no rule matches, the system takes the default action specified in the filter.

You apply filters to interfaces under Configuration | Interfaces, and these are the most important filters for security since they apply to all traffic. You also apply filters to groups and users under Configuration | User Management; these filters apply to *tunneled* traffic only.

- Network address translation (NAT) translates private network addresses into an IANA-assigned public network address, and vice versa, and thus allows traffic routing between networks that have overlapping private network addresses.
- Bandwidth policies let you set minimum and maximum amounts of bandwidth per group.

Figure 15-4 Configuration | Policy Management | Traffic Management Screen



Configuration | Policy Management | Traffic Management | Network Lists

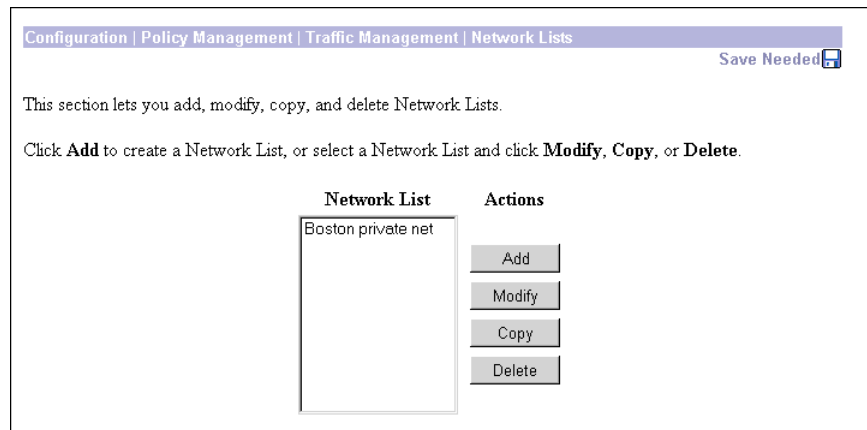
This section of the Manager lets you configure network lists, which are lists of networks that are grouped as single objects. Network lists make configuration easier: for example, you can use a network list to configure one filter rule for a set of networks rather than configuring separate rules for each network.

You can use network lists in configuring filter rules (see Configuration | Policy Management | Traffic Management | Rules). You can also use them to configure split tunneling for groups and users (see Configuration | User Management), and to configure IPSec LAN-to-LAN connections (see Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN).

The Manager can automatically generate a network list containing the private networks reachable from the Ethernet 1 (Private) interface. It generates this list by reading the routing table, and Inbound RIP must be enabled on that interface.

A single network list can contain a maximum of 10 network entries. The Manager does not limit the number of network lists you can configure.

Figure 15-5 Configuration | Policy Management | Traffic Management | Network Lists Screen



67281

Network List

The Network List field shows the names of the network lists you have configured. If no lists have been configured, the field shows --Empty--.

Add / Modify / Copy / Delete

To configure and add a new network list, click **Add**. The Manager opens the Configuration | Policy Management | Traffic Management | Network Lists | Add screen.

To modify a configured network list, select the list and click **Modify**. The Manager opens the Configuration | Policy Management | Traffic Management | Network Lists | Modify screen.

To copy a configured network list, modify it, and save it with a new name, select the list and click **Copy**. See the Configuration | Policy Management | Traffic Management | Network Lists | Copy screen.

To delete a configured network list, select the list and click **Delete**. If the network list is configured on a filter rule or an IPSec LAN-to-LAN connection, the Manager displays an error message indicating the action to take before you can delete the list. *Otherwise, there is no confirmation or undo.* The Manager deletes the list, refreshes the screen, and shows the remaining network lists.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | Policy Management | Traffic Management | Network Lists | Add, Modify, or Copy

These screens let you:

- Add: Configure and add a new network list.
- Modify: Modify a previously configured network list.
- Copy: Copy a configured network list, modify its parameters, save it with a new name, and add it to the configured network lists.

On the Add and Modify screens, the Manager can automatically generate a network list containing the private networks reachable from the Ethernet 1 (Private) interface. It generates this list by reading the routing table, and Inbound RIP must be enabled on that interface.

Figure 15-6 Configuration | Policy Management | Traffic Management | Network Lists | Add, Modify, or Copy Screens

Configuration | Policy Management | Traffic Management | Network Lists | Add

Configure and add a new Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name

Name of the Network List you are adding. The name must be unique.

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

Network List

67258

List Name

Enter a unique name for this network list. Maximum 48 characters, case-sensitive. Spaces are allowed.

If you use the Generate Local List feature on the Add screen, enter this name *after* the system generates the network list.

Network List

Enter the networks in this network list. Enter each network on a single line using the format n.n.n.n/w.w.w.w, where n.n.n.n is a network IP address and w.w.w.w is a wildcard mask.



Note

Enter a *wildcard mask*, which is the reverse of a subnet mask. A wildcard mask has ones in bit positions to ignore, zeros in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.

If you omit the wildcard mask, the Manager supplies the default wildcard mask for the class of the network address. For example, 192.168.12.0 is a Class C address, and default wildcard mask is 0.0.0.255.

You can include a maximum of 200 network/wildcard entries in a single network list.

Generate Local List

On the Add or Modify screen, click the **Generate Local List** button to have the Manager automatically generate a network list containing the first 200 private networks reachable from the Ethernet 1 (Private) interface. It generates this list by reading the routing table (see Monitoring | Routing Table), and Inbound RIP must be enabled on that interface (see Configuration | Interfaces). The Manager refreshes the screen after it generates the list, and you can then edit the Network List and enter a List Name.



Note

If you click **Apply**, the generated list replaces any existing entries in the Network List.

Add or Apply / Cancel

To add this network list to the configured network lists, click **Add**. Or to apply your changes to this network list, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | Policy Management | Traffic Management | Network Lists screen. Any new entry appears at the bottom of the Network List field.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | Policy Management | Traffic Management | Network Lists screen, and the Network Lists field is unchanged.

Configuration | Policy Management | Traffic Management | Rules

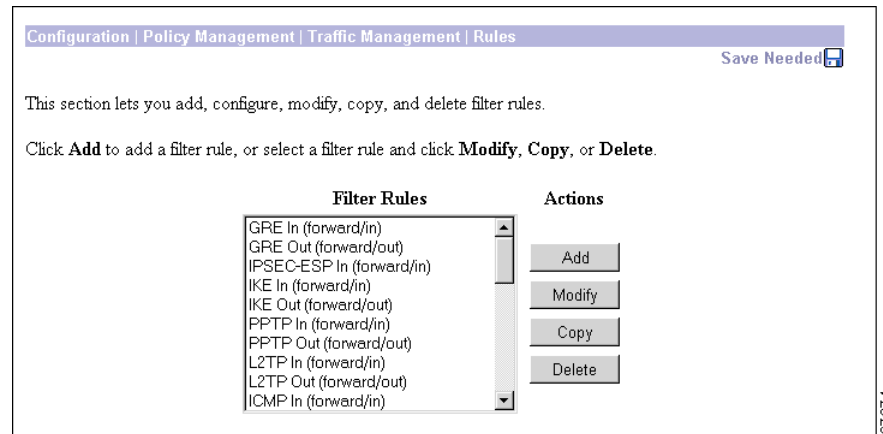
This section of the Manager lets you add, configure, modify, copy, and delete filter rules. You use rules to construct filters.



Caution

The Cisco-supplied default rules are intended as templates that you should examine and modify to fit your network and security needs. Unmodified, or incorrectly applied, they could present security risks. You should also be especially careful about adding rules to the Public (Default) filter. For example, the default Incoming HTTP rules are intended to allow an administrator outside the private network to manage the VPN Concentrator with a browser. Unmodified, they could allow browser connections to any system on the private network. If you apply these rules to a filter, you should at least change the Source and Destination Address to limit the connections.

Figure 15-7 Configuration | Policy Management | Traffic Management | Rules Screen



Filter Rules

The Filter Rules list shows the configured rules that are available to apply to filters. The list shows the rule name and the action/direction in parentheses. The rules are listed in the order they are configured.

Cisco supplies several default rules that you can modify and use. See [Table 15-1](#) for their parameters, and see Configuration | Policy Management | Traffic Management | Rules | Add for explanations of the parameters.

For all the default rules except VRRP In and Out, these parameters are identical:

- Action = Forward
- Source Address = Use IP Address/Wildcard-Mask = 0.0.0.0/255.255.255.255 = any address
- Destination Address = Use IP Address/Wildcard-Mask = 0.0.0.0/255.255.255.255 = any address

For maximum security and control, we recommend that you change the Source Address and Destination Address to fit your network addressing and security scheme.

Table 15-1 Cisco-Supplied Default Filter Rules

Filter Rule Name	Direction	Protocol	TCP Connection	TCP/UDP Source Port	TCP/UDP Destination Port	ICMP Packet Type
Any In	Inbound	Any	Don't Care	Range 0-65535	Range 0-65535	0-255
Any Out	Outbound	Any	Don't Care	Range 0-65535	Range 0-65535	0-255
CRL over LDAP In	Inbound	TCP	Don't Care	LDAP (389)	Range 0-65535	—
CRL over LDAP Out	Outbound	TCP	Don't Care	Range 0-65535	LDAP (389)	—
GRE In	Inbound	GRE	—	—	—	—
GRE Out	Outbound	GRE	—	—	—	—
ICMP In	Inbound	ICMP	—	—	—	0-18
ICMP Out	Outbound	ICMP	—	—	—	0-18
IKE In	Inbound	UDP	—	Range 0-65535	IKE (500)	—
IKE Out	Outbound	UDP	—	IKE (500)	Range 0-65535	—
Incoming HTTP In	Inbound	TCP	Don't Care	Range 0-65535	HTTP (80)	—
Incoming HTTP Out	Outbound	TCP	Don't Care	HTTP (80)	Range 0-65535	—
Incoming HTTPS In	Inbound	TCP	Don't Care	Range 0-65535	HTTPS (443)	—
Incoming HTTPS Out	Outbound	TCP	Don't Care	HTTPS (443)	Range 0-65535	—
IPSec-ESP In	Inbound	ESP	—	—	—	—
L2TP In	Inbound	UDP	—	Range 0-65535	L2TP (1701)	—
L2TP Out	Outbound	UDP	—	L2TP (1701)	Range 0-65535	—
LDAP In	Inbound	TCP	Don't Care	Range 0-65535	LDAP (389)	—

Table 15-1 Cisco-Supplied Default Filter Rules (continued)

Filter Rule Name	Direction	Protocol	TCP Connection	TCP/UDP Source Port	TCP/UDP Destination Port	ICMP Packet Type
LDAP Out	Outbound	TCP	Don't Care	LDAP (389)	Range 0-65535	—
OSPF In	Inbound	OSPF	—	—	—	—
OSPF Out	Outbound	OSPF	—	—	—	—
Outgoing HTTP In	Inbound	TCP	Don't Care	HTTP (80)	Range 0-65535	—
Outgoing HTTP Out	Outbound	TCP	Don't Care	Range 0-65535	HTTP (80)	—
Outgoing HTTPS In	Inbound	TCP	Don't Care	HTTPS (443)	Range 0-65535	—
Outgoing HTTPS Out	Outbound	TCP	Don't Care	Range 0-65535	HTTPS (443)	—
PPTP In	Inbound	TCP	Don't Care	Range 0-65535	PPTP (1723)	—
PPTP Out	Outbound	TCP	Don't Care	PPTP (1723)	Range 0-65535	—
RIP In	Inbound	UDP	—	RIP (520)	RIP (520)	—
RIP Out	Outbound	UDP	—	RIP (520)	RIP (520)	—
SSH In	Inbound	TCP	Don't Care	Range 0-65535	SSH (22)	—
SSH Out	Outbound	TCP	Don't Care	SSH (22)	Range 0-65535	—
Telnet/SSL In	Inbound	TCP	Don't Care	Range 0-65535	Telnet/SSL (992)	—
Telnet/SSL Out	Outbound	TCP	Don't Care	Telnet/SSL (992)	Range 0-65535	—
VCA In	Inbound	UDP	—	Range 0-65535	9023	—
VCA Out	Outbound	UDP	—	9023	Range 0-65535	—
VRRP In ¹	Inbound	Other 112	—	—	—	—
VRRP Out ¹	Outbound	Other 112	—	—	—	—

1. For VRRP In and VRRP Out, the Destination Address is 224.0.0.18/0.0.0.0, which is the IANA-assigned IP multicast address for VRRP.

Add / Modify / Copy / Delete

To configure a new rule, click **Add**. The Manager opens the Configuration | Policy Management | Traffic Management | Rules | Add screen.

To modify a rule that has been configured, select the rule from the list and click **Modify**. The Manager opens the Configuration | Policy Management | Traffic Management | Rules | Modify screen.

To copy a configured rule, modify it, and save it with a new name, select the rule from the list and click **Copy**. See the Configuration | Policy Management | Traffic Management | Rules | Copy screen.

To delete a configured rule, select the rule from the list and click **Delete**.

- If the rule *is not* being used in a filter, the Manager deletes the rule, refreshes the screen, and shows the remaining rules in the list. *There is no confirmation or undo.*
- If the rule *is* being used in a filter, the Manager asks you to confirm the deletion. See the Configuration | Policy Management | Traffic Management | Rules | Delete screen.
- You cannot delete a rule that is configured as part of a LAN-to-LAN connection. See the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done screen.

**Note**

Deleting a rule deletes it from every filter that uses it and deletes it from the VPN Concentrator active configuration. To *remove* a rule from a filter but retain it in the active configuration, see the Configuration | Policy Management | Traffic Management | Assign Rules to Filter screen.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | Policy Management | Traffic Management | Rules | Add, Modify, or Copy

These Manager screens let you:

- Add: Configure and add a new filter rule to the list of filter rules.
- Modify: Modify a previously configured filter rule.
- Copy: Copy a configured rule, modify its parameters, save it with a new name, and add it to the list of filter rules.

The VPN Concentrator applies rule parameters to data traffic (packets) in the order presented on this screen (from Protocol down) to see if they match. If all parameters match, the system takes the specified Action. If at least one parameter does not match, the system ignores the rest of this rule and examines the packet in accordance with the next rule, and so forth.

**Note**

On the Modify screen, any changes take effect as soon as you click Apply. Changes affect *all* filters that use this rule. If this rule is being used by an active filter, changes might affect tunnel traffic.

Creating Rules for a Firewall Filter

If you are creating rules for a VPN Client firewall filter:

- Keep in mind that the VPN Concentrator pushes these rules down to the VPN Client, so you should create and define these rules relative to the VPN Client, not the VPN Concentrator. In this type of configuration, “in” and “out” refer to traffic inbound to and outbound from the VPN Client.
- When configuring firewall rules, be aware that the VPN Client integrated firewall is stateful only for TCP, UDP, and ICMP protocols. For all other protocols, it uses packet filtering.
- Two of the parameters on this screen are not relevant: TCP Connection and ICMP Packet Type. The VPN Client ignores these parameters.
- Choose either Drop or Forward from the Action drop-down menu. The other choices are not relevant to firewall configuration and the VPN Client ignores them.

For more information on configuring rules for VPN Client firewall filters, refer to the *VPN Client Administrator Guide*.

Figure 15-8 Configuration | Policy Management | Traffic Management | Rules | Add, Modify, or Copy Screen

Configuration | Policy Management | Traffic Management | Rules | Add

Configure and add a new filter rule.

Rule Name	<input type="text"/>	Name of this filter rule. The name must be unique.
Direction	<input type="text" value="Inbound"/>	Select the data direction to which this rule applies.
Action	<input type="text" value="Drop"/>	Specify the action to take when this filter rule applies.

Protocol	<input type="text" value="Any"/>	Select the protocol to which this rule applies. For
or Other	<input type="text"/>	Other protocols, enter the protocol number.
TCP Connection	<input type="text" value="Don't Care"/>	Select whether this rule should apply to an established TCP connection.

Source Address

Network List	<input type="text" value="Use IP Address/Wildcard-mask below"/>	Specify the source network address list or the IP address and wildcard mask that this rule checks.
IP Address	<input type="text" value="0.0.0.0"/>	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard-mask	<input type="text" value="255.255.255.255"/>	

Destination Address

Network List	<input type="text" value="Use IP Address/Wildcard-mask below"/>	Specify the destination network address list or the IP address and wildcard mask that this rule checks.
IP Address	<input type="text" value="0.0.0.0"/>	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard-mask	<input type="text" value="255.255.255.255"/>	

TCP/UDP Source Port

Port	<input type="text" value="Range"/>	For TCP/UDP, specify the source port ranges that this rule checks. For a single port number, use the same number for the start and end.
or Range	<input type="text" value="0"/> to <input type="text" value="65535"/>	

TCP/UDP Destination Port

Port	<input type="text" value="Range"/>	For TCP/UDP, specify the destination port ranges that this rule checks. For a single port number, use the same number for the start and end.
or Range	<input type="text" value="0"/> to <input type="text" value="65535"/>	

ICMP Packet Type

	<input type="text" value="0"/> to <input type="text" value="255"/>	For ICMP, specify the range of ICMP packet types that this rule checks.
--	--	---

67289

Rule Name

Enter a unique name for this rule. Maximum is 48 characters.

Direction

Click the **Direction** drop-down menu button and choose the data direction to which this rule applies:

- Inbound = Into the VPN Concentrator interface; or into the VPN tunnel from the remote client or host. (This is the default selection.)
- Outbound = Out of the VPN Concentrator interface; or out of the VPN tunnel to the remote client or host.

**Note**

If you are configuring this rule to use for a VPN Client firewall filter, the direction is relative to the VPN Client, not the VPN Concentrator. For example, “Inbound” in a VPN Client firewall filter means into the VPN Client interface.

Action

Click the **Action** drop-down menu button and choose the action to take if the data traffic (packet) matches all parameters that follow.

**Note**

If you are configuring this rule to use for a VPN Client firewall filter, you must choose either Drop or Forward.

The choices are:

- Drop = Discard the packet (the default choice).
- Forward = Allow the packet to pass.
- Drop and Log = Discard the packet and log a filter debugging event (FILTERDBG event class). See Configuration | System | Events and see the following note.
- Forward and Log = Allow the packet to pass and log a filter debugging event (FILTERDBG event class). See the following note.
- Apply IPSec = Apply IPSec to the packet. Apply packet authentication, encryption, etc. in accordance with parameters that are specified in a Security Association. You must configure a Security Association if you choose this action. Also, you can assign an SA to this rule only if you choose this (or the following) action; see Configuration | Policy Management | Traffic Management | Security Associations. See following note.
- Apply IPSec and Log = Apply IPSec to the packet and log a filter debugging event (FILTERDBG event class). See the following notes.

**Note**

The Log actions are intended for use only while debugging filter activity. Since they generate and log an event for every matched packet, they consume significant system resources and might seriously degrade performance.

**Note**

The Apply IPsec actions are for LAN-to-LAN traffic only, not for remote-access traffic. Remote-access IPsec traffic is authenticated and encrypted in accordance with the SAs negotiated with the remote client (tunnel group) and user. In LAN-to-LAN connections, individual hosts on the LANs do not negotiate SAs. The VPN Concentrator automatically creates and applies appropriate rules when you create a LAN-to-LAN connection; see Configuration | System | Tunneling Protocols | IPsec LAN-to-LAN.

Protocol or Other

This parameter refers to the IANA (Internet Assigned Numbers Authority) assigned protocol number in an IP packet. The descriptions include the IANA number, in brackets, for reference.

Click the **Protocol or Other** drop-down menu button and choose the protocol to which this rule applies.

- Any = Any protocol [255] (the default choice).
- ICMP = Internet Control Message Protocol [1] (used by ping, for example). If you choose this protocol, you should also configure ICMP Packet Type.
- TCP = Transmission Control Protocol [6] (connection-oriented, for example: FTP, HTTP, SMTP, and Telnet). If you choose this protocol, you should configure TCP Connection and TCP/UDP Source Port or Destination Port.
- EGP = Exterior Gateway Protocol [8] (used for routing to exterior networks).
- IGP = Interior Gateway Protocol [9] (used for routing within a domain).
- UDP = User Datagram Protocol [17] (connectionless, for example: SNMP). If you choose this protocol, you should also configure TCP/UDP Source Port or Destination Port.
- ESP = Encapsulation Security Payload [50] (applies to IPsec).
- AH = Authentication Header [51] (applies to IPsec).
- GRE = Generic Routing Encapsulation [47] (used by PPTP).
- RSVP = Resource Reservation Protocol [46] (reserves bandwidth on routers).
- IGMP = Internet Group Management Protocol [2] (used in multicasting).
- OSPF = Open Shortest Path First [89] (interior routing protocol).
- Other = Other protocol not listed here. If you choose Other here, you must enter the IANA-assigned protocol number in the Other field.

TCP Connection

**Note**

Do not configure this field if you are using this rule for a client firewall filter.

Click the **TCP Connection** drop-down menu button and choose whether this rule applies to packets from established TCP connections. For example, you might want a rule to forward only those TCP packets that originate from established connections on the public network interface, to provide maximum protection against “spoofing.”

The choices are:

- Established = Apply rule to packets from established TCP connections only.
- Don't Care = Apply rule to any TCP packets, whether from established connections or new connections (the default choice).

Source Address

Specify the packet source address that this rule checks (the address of the sender).

Network List

Click the **Network List** drop-down menu button and choose the configured network list that specifies the source addresses. A network list is a list of network addresses that are treated as a single object. See the Configuration | Policy Management | Traffic Management | Network Lists screens. Otherwise, you can choose:

- Use IP Address/Wildcard-mask, which lets you enter a network address.

If you choose a configured network list, the Manager ignores entries in the IP Address and Wildcard-mask fields.

**Note**

An IP address is used with a *wildcard mask* to provide the desired granularity. A *wildcard mask* is the reverse of a subnet mask. The wildcard mask has ones in bit positions to ignore, zeros in bit positions to match. For example:

0.0.0.0/255.255.255.255 = any address

10.10.1.35/0.0.0.0 = only 10.10.1.35

10.10.1.35/0.0.0.255 = all 10.10.1.nnn addresses

IP Address

Enter the source IP address in dotted decimal notation. Default is 0.0.0.0.

Wildcard-mask

Enter the source address wildcard mask in dotted decimal notation. Default is 255.255.255.255.

Destination Address

Specify the packet destination address that this rule checks (the address of the recipient).

Network List

Click the **Network List** drop-down menu button and choose the configured network list that specifies the destination addresses. A network list is a list of network addresses that are treated as a single object. See the Configuration | Policy Management | Traffic Management | Network Lists screens. Otherwise, you can choose Use IP Address/Wildcard-mask, which lets you enter a network address.

If you choose a configured network list, the Manager ignores entries in the IP Address and Wildcard-mask fields. See the preceding *wildcard mask* note.

IP Address

Enter the destination IP address in dotted decimal notation. The default value is 0.0.0.0.

Wildcard-mask

Enter the destination address wildcard mask in dotted decimal notation. The default value is 255.255.255.255.

TCP/UDP Source Port

If you chose TCP or UDP under Protocol, choose the source port number that this rule checks.

Many different protocols or processes run in TCP or UDP environments, and each TCP or UDP process running on a network host is assigned a port number. Thus an IP address plus a port number uniquely identifies a process on a network host. Only TCP and UDP protocols use port numbers. The Internet Assigned Numbers Authority (IANA) manages port numbers and classifies them as Well Known, Registered, and Dynamic (or Private). The Well Known ports are those from 0 through 1023; the Registered Ports are those from 1024 through 49151; and the Dynamic ports are those from 49152 through 65535.

Port or Range

Click the **Port or Range** drop-down menu button and choose the process (port number):

- ECHO (7) = Used by ping for network testing.
- DISCARD (9) = Used for network debugging and measurement.
- FTP-DATA (20) = File Transfer Protocol, data port.
- FTP (21) = File Transfer Protocol, control port.
- SSH (22) = Secure Shell Protocol.
- TELNET (23) = Terminal emulation.
- SMTP (25) = Simple Mail Transfer Protocol.
- DNS (53) = Domain Name System.
- TFTP (69) = Trivial File Transfer Protocol.

- FINGER (79) = Network user inquiry.
- HTTP (80) = Hypertext Transfer Protocol.
- POP3 (110) = Post Office Protocol, version 3.
- NNTP (119) = Network News Transfer Protocol.
- NTP (123) = Network Time Protocol.
- NetBIOS Name Service (137) = Network Basic Input Output System, host name assignment.
- NetBIOS (138) = NetBIOS datagram service.
- NetBIOS Session (139) = NetBIOS session management.
- IMAP (143) = Internet Mail Access Protocol.
- SNMP (161) = Simple Network Management Protocol.
- SNMP-TRAP (162) = SNMP event or trap handling.
- BGP (179) = Border Gateway Protocol.
- LDAP (389) = Lightweight Directory Access Protocol.
- HTTPS (443) = HTTP over a secure session (TLS/SSL).
- SMTPS (465) = SMTP over a secure session (TLS/SSL).
- IKE (500) = Internet Key Exchange Protocol (was ISAKMP/Oakley).
- SYSLOG (514) = UNIX syslog server (UDP only).
- RIP (520) = Routing Information Protocol (UDP only).
- NNTPS (563) = NNTP over a secure session (TLS/SSL).
- LDAP/SSL (636) = LDAP over a secure session (TLS/SSL).
- Telnet/SSL (992) = Telnet over a secure session (TLS/SSL).
- LapLink (1547) = Remote file management and mail.
- L2TP (1701) = Layer 2 Tunneling Protocol.
- PPTP (1723) = Point-to-Point Tunneling Protocol.
- Range = To specify a range of port numbers, or to specify a port not on the Cisco-supplied list, select **Range** here (the default selection) and enter—in the **Range [start] to [end]** fields—the inclusive range of port numbers to which this rule applies. To specify a single port number, enter the same number in both fields. Defaults are 0 to 65535 (all ports). The Range fields are ignored if you choose a specific port from the drop-down list.

TCP/UDP Destination Port

If you chose TCP or UDP under Protocol, choose the destination port number that this rule checks. See the preceding explanation of port numbers under TCP/UDP Source Port.

Port or Range

Click the **Port or Range** drop-down menu button and choose the process (port number). The choices are the same as listed under TCP/UDP Source Port, Port or Range.

ICMP Packet Type

**Note**

Do not configure this field if you are using this rule for a client firewall filter.

The ICMP protocol has many messages that are identified by a type number. For example:

0 = Echo Reply

8 = Echo

13 = Timestamp

14 = Timestamp Reply

17 = Address Mask Request

18 = Address Mask Reply

The Internet Assigned Numbers Authority (IANA) manages these ICMP type numbers.

If you selected ICMP under Protocol, enter the range of ICMP packet type numbers to which this rule applies. To specify a single packet type, enter the same number in both fields. Defaults are 0 to 255 (all packet types). For example, to specify the Timestamp and Timestamp Reply types only, enter **13** to **14**.

Add or Apply / Cancel

To add this rule to the list of configured filter rules, click **Add**. Or to apply your changes to this rule, click **Apply**. On the **Modify** screen, any changes take effect as soon as you click **Apply**. If the rule is being used by an active filter, changes might affect tunnel traffic. The Manager returns to the Configuration | Policy Management | Traffic Management | Rules screen. Any new rule appears in the Filter Rules list.

Reminder:

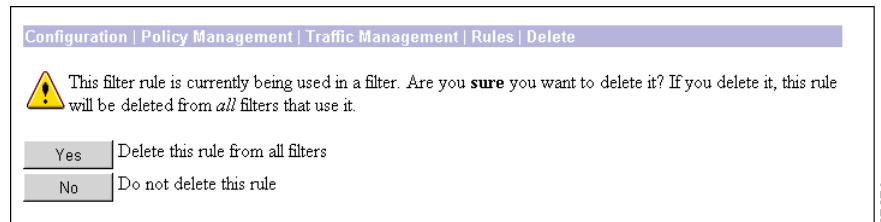
The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | Policy Management | Traffic Management | Rules screen, and the Filter Rules list is unchanged.

Configuration | Policy Management | Traffic Management | Rules | Delete

This screen asks you to confirm deletion of a rule that is being used in a filter. Doing so deletes the rule from *all* filters that use it, and deletes it from the VPN Concentrator active configuration. To *remove* a rule from a filter but retain it in the active configuration, see the Configuration | Policy Management | Traffic Management | Assign Rules to Filter screen.

Figure 15-9 Configuration | Policy Management | Traffic Management | Rules | Delete Screen

**Note**

The Manager deletes the rule from the filter as soon as you click **Yes**. If this rule is being used by an active filter, deletion might affect data traffic.

Yes / No

To delete this rule from all filters that use it, and delete it from the active configuration, click **Yes**. *There is no undo*. The Manager returns to the Configuration | Policy Management | Traffic Management | Rules screen and shows the remaining rules in the Filter Rules list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To not delete this rule, click **No**. The Manager returns to the Configuration | Policy Management | Traffic Management | Rules screen, and the Filter Rules list is unchanged.

Configuration | Policy Management | Traffic Management | Security Associations

This section of the Manager lets you add, configure, modify, and delete Security Associations (SAs). SAs apply only to IPSec tunnels. During tunnel establishment the two parties negotiate Security Associations that govern authentication, encryption, encapsulation, key management, etc. In other words, while rules and filters specify *what* traffic to manage, SAs tell *how* to do it.

IPSec configurations actually involve two SA negotiation phases: first, to establish the tunnel (the IKE SA); and second, to govern traffic within—the use of—the tunnel (the IPSec SA). You must configure IKE proposals before configuring Security Associations. See Configuration | System | Tunneling Protocols | IPSec | IKE Proposals, or click the IKE Proposals link on this screen.

You apply SAs to filter rules that are configured with an Apply IPSec action, for LAN-to-LAN traffic. See Configuration | Policy Management | Traffic Management | Rules. The VPN Concentrator automatically creates and applies appropriate rules when you create a LAN-to-LAN connection; see Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN. You also apply SAs to groups and users, for remote-access traffic, under the IPSec Parameters section on the appropriate Configuration | User Management screens.

You can use IPSec in both client-to-LAN (remote-access) configurations and LAN-to-LAN configurations. The Cisco VPN Client complies with the IPSec protocol and is specifically designed to work with the VPN Concentrator. However, the VPN Concentrator can establish IPSec connections with many protocol-compliant clients. Likewise, the VPN Concentrator can establish LAN-to-LAN connections with other protocol-compliant VPN devices (often called “secure gateways”). The instructions in this section, however, assume peer VPN Concentrators.

The Cisco VPN Client supports these IPsec attributes:

- Main mode for negotiating phase one ISAKMP Security Associations (SAs) when using digital certificates for authentication
- Aggressive mode for negotiating phase one of establishing ISAKMP Security Associations (SAs) when using preshared keys for authentication
- Authentication Algorithms:
 - ESP-MD5-HMAC-128
 - ESP-SHA1-HMAC-160
- Authentication Modes:
 - Preshared Keys
 - X.509 Digital Certificates
- Diffie-Hellman Groups 1, 2, and 5
- Encryption Algorithms:
 - DES-56
 - 3DES-168
 - ESP-NULL
 - AES-128
 - AES-192
 - AES-256

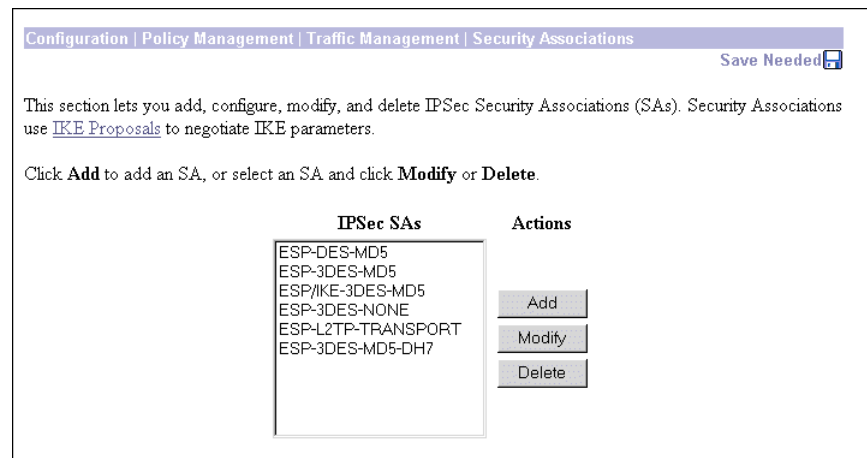


Note

AES encryption algorithms work only with VPN Concentrator software versions 3.6 and later.

- Extended Authentication (XAuth)
- Mode Configuration (also known as ISAKMP Configuration Method)
- Tunnel Encapsulation Mode
- IP compression (IPComp) using LZS

Figure 15-10 Configuration | Policy Management | Traffic Management | Security Associations Screen



67049

IPSec SAs

The IPSec SAs list shows the configured SAs that are available. The SAs are listed in the order they are configured.

Cisco supplies default SAs that you can use or modify; see [Table 15-2](#) and [Table 15-3](#). See the Configuration | Policy Management | Traffic Management | Security Associations | Add section for explanations of the parameters.

Table 15-2 Cisco-Supplied Default Security Associations , Part 1

SA Name				
Parameter	ESP-DES-MD5	ESP-3DES-MD5	ESP/IKE-3DES-MD5	ESP-3DES-NONE
Inheritance	From Rule	From Rule	From Rule	From Rule
IPSec Parameters				
Authentication Algorithm	ESP/MD5/HM AC-128	ESP/MD5/HM AC-128	ESP/MD5/HM AC-128	None
Encryption Algorithm	DES-56	3DES-168	3DES-168	3DES-168
Encapsulation Mode	Tunnel	Tunnel	Tunnel	Tunnel
Perfect Forward Secrecy	Disabled	Disabled	Disabled	Disabled
Lifetime Measurement	Time	Time	Time	Time
Data Lifetime	10000 KB	10000 KB	10000 KB	10000 KB
Time Lifetime	28800 sec	28800 sec	28800 sec	28800 sec
IKE Parameters				
IKE Peer	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Negotiation Mode	Main	Main	Main	Main
Digital Certificate	None (Use Preshared Keys)	None (Use Preshared Keys)	None (Use Preshared Keys)	None (Use Preshared Keys)
IKE Proposal	IKE-DES-MD5	IKE-DES-MD5	IKE-3DES-MD5	IKE-3DES-MD5

Table 15-3 Cisco-Supplied Default Security Associations, Part 2

SA Name	ESP-L2TP-TRANSPORT	ESP-3DES-MD5-DH7	ESP-3DES-MD5-DH5	ESP-AES-128-SHA
Parameter				
Inheritance	From Rule	From Rule	Rule	Rule
IPSec Parameters				
Authentication Algorithm	ESP/MD5/HMAC-128	ESP/MD5/HMAC-128	ESP/MD5/HMAC-128	ESP/SHA1/HMAC-160
Encryption Algorithm	DES-56	3DES-168	3DES-168	AES-128
Encapsulation Mode	Transport	Tunnel	Tunnel	Tunnel
Perfect Forward Secrecy	Disabled	Disabled	Disabled	Disabled
Lifetime Measurement	Time	Time	Time	Time
Data Lifetime	10000 KB	10000 KB	10000 KB	10000 KB
Time Lifetime	3600 sec	28800 sec	28800 sec	28800 sec
IKE Parameters				
IKE Peer	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Negotiation Mode	Main	Aggressive	Aggressive	Aggressive
Digital Certificate	None (Use Preshared Keys)	None (Use Preshared Keys)	None (Use Preshared Keys)	None (Use Preshared Keys)
IKE Proposal	IKE-3DES-MD5	IKE-3DES-MD5-DH7	CiscoVPNClient-3DES-MD5-DH5	CiscoVPNClient-AES128-SHA

Add / Modify / Delete

To configure a new SA, click **Add**. The Manager opens the Configuration | Policy Management | Traffic Management | Security Associations | Add screen.

To modify an SA that has been configured, select the SA from the list and click **Modify**. The Manager opens the Configuration | Policy Management | Traffic Management | Security Associations | Modify screen.

To delete a configured SA, select the SA from the list and click **Delete**.

- If the SA *has not* been assigned to a filter rule—even if it has been assigned to a group or user—the Manager deletes the SA, refreshes the screen, and shows the remaining SAs in the list. *There is no confirmation or undo.*
- If the SA *has* been assigned to a filter rule, the Manager asks you to confirm the deletion. See the Configuration | Policy Management | Traffic Management | Security Associations | Delete screen.
- You cannot delete an SA that is configured as part of a LAN-to-LAN connection. See the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done screen.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | Policy Management | Traffic Management | Security Associations | Add or Modify

These screens let you:

- Add: Configure and add a new Security Association to the list of configured SAs.
- Modify: Modify a configured Security Association.



Note

On the Modify screen, any changes take effect as soon as you click **Apply**. If the SA is being used by an active filter rule or group, changes might affect tunnel traffic.

Figure 15-11 Configuration | Policy Management | Traffic Management | Security Associations | Add or Modify Screen

Configuration | Policy Management | Traffic Management | Security Associations | Modify

Modify a configured Security Association.

SA Name	<input type="text" value="ESP-DES-MD5"/>	Specify the name of this Security Association (SA).
Inheritance	<input type="text" value="From Rule"/>	Select the granularity of this SA.

IPSec Parameters

Authentication Algorithm	<input type="text" value="ESP/MD5/HMAC-128"/>	Select the packet authentication algorithm to use.
Encryption Algorithm	<input type="text" value="DES-56"/>	Select the ESP encryption algorithm to use.
Encapsulation Mode	<input type="text" value="Tunnel"/>	Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy	<input type="text" value="Disabled"/>	Select the use of Perfect Forward Secrecy.
Lifetime Measurement	<input type="text" value="Time"/>	Select the lifetime measurement of the IPSec keys.
Data Lifetime	<input type="text" value="10000"/>	Specify the data lifetime in kilobytes (KB).
Time Lifetime	<input type="text" value="28800"/>	Specify the time lifetime in seconds.

IKE Parameters

IKE Peer	<input type="text" value="0.0.0.0"/>	Specify the IKE Peer for a LAN-to-LAN IPSec connection.
Negotiation Mode	<input type="text" value="Main"/>	Select the IKE Negotiation mode to use.
Digital Certificate	<input type="text" value="UK332"/>	Select the Digital Certificate to use.
Certificate Transmission	<input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only	Choose how to send the digital certificate to the IKE peer.
IKE Proposal	<input type="text" value="IKE-DES-MD5"/>	Select the IKE Proposal to use as IKE initiator.

88529

SA Name

Enter a unique name for this Security Association. Maximum is 48 characters.

Inheritance

This parameter specifies the granularity, or how many tunnels to build for this connection. Each tunnel uses a unique key.

Click the **Inheritance** drop-down menu button and choose:

- From Rule = One tunnel for each rule in the connection. A rule can specify multiple networks, thus many hosts can use the same tunnel. This is the default—and recommended—selection.
- From Data = One tunnel for every address pair within the address ranges specified in the rule. Each host uses a separate tunnel, and hence, separate keys. This selection is more secure but requires more processing overhead.

IPSec Parameters

These parameters apply to IPSec SAs, which are Phase 2 SAs negotiated under IPSec, where the two parties establish conditions for use of the tunnel.

Authentication Algorithm

This parameter specifies the data, or packet, authentication algorithm. Packet authentication proves that data comes from whom you think it comes from; it is often referred to as “data integrity” in VPN literature. The IPSec ESP (Encapsulating Security Payload) protocol provides both encryption and authentication.

Click the **Authentication Algorithm** drop-down menu button and choose the algorithm:

- None = No data authentication.
- ESP/MD5/HMAC-128 = ESP protocol using HMAC (Hashed Message Authentication Coding) with the MD5 hash function using a 128-bit key. This is the default selection.
- ESP/SHA/HMAC-160 = ESP protocol using HMAC with the SHA-1 hash function using a 160-bit key. This selection is more secure but requires more processing overhead.

Encryption Algorithm

This parameter specifies the data, or packet, encryption algorithm. Data encryption makes the data unreadable if intercepted.

Click the **Encryption Algorithm** drop-down menu button and choose the algorithm:

- Null = No packet encryption.
- DES-56 = Use DES encryption with a 56-bit key.
- 3DES-168 = Use Triple-DES encryption with a 168-bit key. This is the default selection, and it is the most secure.

Encapsulation Mode

This parameter specifies the mode for applying ESP encryption and authentication; in other words, what part of the original IP packet has ESP applied.

Click the **Encapsulation Mode** drop-down menu button and choose the mode:

- Tunnel = Apply ESP encryption and authentication to the entire original IP packet (IP header and data), thus hiding the ultimate source and destination addresses. This is the default selection, and it is the most secure.
- Transport = Apply ESP encryption and authentication only to the transport layer segment (data only) of the original IP packet. This mode protects packet contents but not the ultimate source and destination addresses. Use this mode for Windows 2000 client compatibility.

Perfect Forward Secrecy

This parameter specifies whether to use Perfect Forward Secrecy, and the size of the numbers to use, in generating Phase 2 IPsec keys. Perfect Forward Secrecy is a cryptographic concept where each new key is unrelated to any previous key. In IPsec negotiations, Phase 2 keys are based on Phase 1 keys unless Perfect Forward Secrecy is specified. Perfect Forward Secrecy uses Diffie-Hellman techniques to generate the keys.

Click the **Perfect Forward Secrecy** drop-down menu button and choose the Perfect Forward Secrecy option:

- Disabled = Do not use Perfect Forward Secrecy. IPsec session keys are based on Phase 1 keys. This is the default choice.
- Group 1 (768-bits) = Use Perfect Forward Secrecy, and use Diffie-Hellman Group 1 to generate IPsec session keys, where the prime and generator numbers are 768 bits. This option is more secure but requires more processing overhead.
- Group 2 (1024-bits) = Use Perfect Forward Secrecy, and use Diffie-Hellman Group 2 to generate IPsec session keys, where the prime and generator numbers are 1024 bits. This option is more secure than Group 1 but requires more processing overhead.
- Group 7 (ECC) = Use Perfect Forward Secrecy, and use Diffie-Hellman Group 7 (ECC) to generate IPsec session keys, where the elliptic curve field size is 163 bits. This option is the fastest and requires the least overhead. It is intended for use with the movianVPN client, but you can use it with any peers that support Group 7 (ECC).

Lifetime Measurement

This parameter specifies how to measure the lifetime of the IPsec SA keys, which is how long the IPsec SA lasts until it expires and must be renegotiated with new keys. It is used with the Data Lifetime or Time Lifetime parameters.

**Note**

If the peer proposes a shorter lifetime measurement, the VPN Concentrator uses that lifetime measurement instead.

Click the **Lifetime Measurement** drop-down menu button and choose the measurement method:

- Time = Use time (seconds) to measure the lifetime of the SA (the default). Configure the Time Lifetime parameter.
- Data = Use data (number of kilobytes) to measure the lifetime of the SA. Configure the Data Lifetime parameter.
- Both = Use both time and data, whichever occurs first, to measure the lifetime. Configure both Time Lifetime and Data Lifetime parameters.
- None = No lifetime measurement. The SA lasts until terminated for other reasons. It lasts a maximum of 86400 seconds (24 hours).

Data Lifetime

If you chose Data or Both under Lifetime Measurement, enter the number of kilobytes of payload data after which the IPsec SA expires. Minimum is 100 KB, default is 10000 KB, maximum is 2147483647 KB.

Time Lifetime

If you chose Time or Both under Lifetime Measurement, enter the number of seconds after which the IPsec SA expires. Minimum is 60 seconds, default is 28800 seconds (8 hours), maximum is 2147483647 seconds (about 68 years).

IKE Parameters

These parameters govern IKE SAs, which are Phase 1 SAs negotiated under IPsec, where the two parties establish a secure tunnel within which they then negotiate the IPsec SAs. In this IKE SA they exchange automated key management information under the IKE (Internet Key Exchange) protocol (formerly called ISAKMP/Oakley).

All these parameters (except IKE Peer) must be configured the same on both parties; the IKE Peer entries must mirror each other. If you create multiple IPsec SAs for use between two IKE peers, the IKE SA parameters must be the same on all SAs.

For best performance and interoperability, we strongly recommend that you use the default parameters where appropriate.

IKE Peer

This parameter applies only to IPSec LAN-to-LAN configurations. It is ignored for IPSec client-to-LAN configurations.

Enter the IP address of the remote peer VPN Concentrator. Use dotted decimal notation. This must be the IP address of the public interface on the peer VPN Concentrator.

This IP address must also match the Peer IP Address on the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add or Modify screen. It must also match the Group Name for the LAN-to-LAN connection. When you configure the connection on the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add screen, the Manager automatically creates a group with the Peer IP address as the Group Name. See Configuration | User Management for information on groups.

When you configure this parameter on the *remote* peer, enter the IP address of *this* VPN Concentrator. The entries must mirror each other.

Negotiation Mode

This parameter sets the mode for exchanging key information and setting up the SAs. It sets the mode that the initiator of the negotiation uses; the responder auto-negotiates.

Click the **Negotiation Mode** drop-down menu button and choose the mode:

- Aggressive = A faster mode using fewer packets and fewer exchanges, but which does not protect the identity of the communicating parties.
- Main = A slower mode using more packets and more exchanges, but which protects the identities of the communicating parties. This mode is more secure and it is the default selection.

Digital Certificate

This parameter specifies whether to use preshared keys or a PKI (Public Key Infrastructure) digital identity certificate to authenticate the peer during Phase 1 IKE negotiations. See the discussion under Administration | Certificate Management.

Click the **Digital Certificate** drop-down menu button and choose the option. The list shows any digital certificates that have been installed, plus the following option:

- None (Use Preshared Keys) = Use preshared keys to authenticate the peer during Phase 1 IKE negotiations. This is the default selection.

Certificate Transmission

If you configured authentication using digital certificates, choose the type of certificate transmission.

- Entire certificate chain = Send the peer the identity certificate and all issuing certificates. Issuing certificates include the root certificate and any subordinate CA certificates.
- Identity certificate only = Send the peer only the identity certificate.

IKE Proposal

This parameter specifies the set of attributes that govern Phase 1 IPSec negotiations, which are known as IKE proposals. See the Configuration | System | Tunneling Protocols | IPSec | IKE Proposals screen. When the VPN Concentrator is acting as an IPSec initiator, this is the *only* IKE proposal it negotiates. As an IPSec responder, the VPN Concentrator checks all active IKE proposals in priority order, to see if it can find one that agrees with parameters in the initiator's proposed SA. You must configure, activate, and prioritize IKE proposals before configuring Security Associations.

Click the **IKE Proposal** drop-down menu button and choose the IKE proposal. The list shows only active IKE proposals in priority order. Cisco-supplied default active proposals are:

- CiscoVPNClient-3DES-MD5 = Use preshared keys (XAUTH) and MD5/HMAC-128 for authentication. Use 3DES-168 encryption. Use D-H Group 2 to generate SA keys. This selection allows XAUTH user-based authentication and is the default.
- IKE-3DES-MD5 = Use preshared keys and MD5/HMAC-128 for authentication. Use 3DES-168 encryption. Use D-H Group 2 to generate SA keys.
- IKE-3DES-MD5-DH1 = Use preshared keys and MD5/HMAC-128 for authentication. Use 3DES-168 encryption. Use D-H Group 1 to generate SA keys. This selection is compatible with the Cisco VPN 3000 Client.
- IKE-DES-MD5 = Use preshared keys and MD5/HMAC-128 for authentication. Use DES-56 encryption. Use D-H Group 1 to generate SA keys. This selection is compatible with the Cisco VPN 3000 Client.
- IKE-3DES-MD5-DH7 = Use preshared keys and MD5/HMAC-128 for authentication. Use 3DES-168 encryption. Use D-H Group 7 (ECC) to generate SA keys. This IKE proposal is intended for use with the movianVPN client; it can also be used with any peer that supports ECC groups for D-H.

Add or Apply / Cancel

To add this Security Association to the list of configured SAs, click **Add**. Or to apply your changes to this Security Association, click **Apply**. On the **Modify** screen, any changes take effect as soon as you click **Apply**. *If this SA is being used by an active filter rule or group, changes might affect tunnel traffic.* Both actions include your entry in the active configuration. The Manager returns to the Configuration | Policy Management | Traffic Management | Security Associations screen. Any new SA appears at the bottom of the IPSec SAs list.

Reminder:

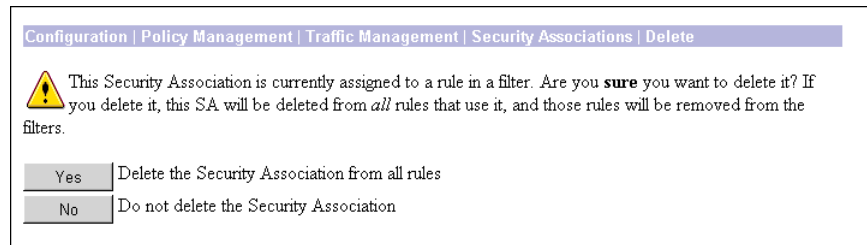
To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | Policy Management | Traffic Management | Security Associations screen, and the IPSec SAs list is unchanged.

Configuration | Policy Management | Traffic Management | Security Associations | Delete

This screen asks you to confirm deletion of a Security Association that is assigned to a rule in a filter. *Doing so deletes the SA from the VPN Concentrator active configuration, deletes the SA from all rules that use it, and removes those rules from filters.*

Figure 15-12 Configuration | Policy Management | Traffic Management | Security Associations | Delete Screen



Note

The Manager deletes the SA as soon as you click **Yes**. If this SA is being used by an active filter, deletion might affect tunnel traffic.

Yes / No

To delete this SA from all rules that use it, and delete it from the active configuration, click **Yes**. *There is no undo.* The Manager returns to the Configuration | Policy Management | Traffic Management | Security Associations screen and shows the remaining SAs in the IPSec SAs list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To not delete this SA, click **No**. The Manager returns to the Configuration | Policy Management | Traffic Management | Security Associations screen, and the IPSec SAs list is unchanged.

Configuration | Policy Management | Traffic Management | Filters

This section of the Manager lets you add, configure, modify, copy, and delete filters, and assign rules to filters.

Filters consist of rules. A filter applies its rules to data packets coming through the system, in the order the rules are arranged on the filter. If a packet matches all the parameters specified in the rule, the system takes the Action specified in the rule. If at least one rule parameter does not match, it applies the next rule; and so on. If no rule matches, the system takes the Default Action specified in the filter.

Configuring a filter involves two steps:

-
- Step 1** Configure the basic filter parameters (name, default action, etc.) by clicking **Add Filter**, **Modify Filter**, or **Copy Filter**.
- Step 2** Assign rules to a filter by clicking **Assign Rules to Filter**.
-

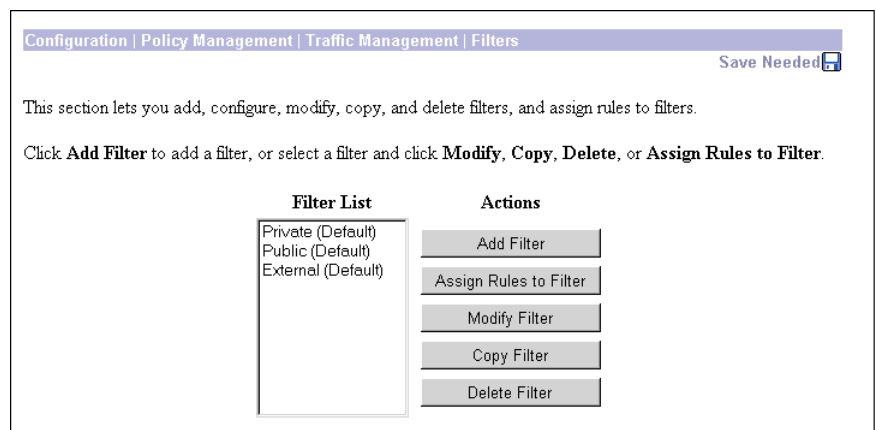
You apply filters to interfaces under Configuration | Interfaces, and these are the most important filters for security since they govern all traffic through an interface. You also apply filters to groups and users under Configuration | User Management, and thus govern *tunneled* traffic through an interface.



Caution

The Cisco-supplied default filters and rules are intended as templates that you should examine and configure to fit your network and security needs. If left in their default configuration or if incorrectly configured, they could present security risks. You should also be especially careful about adding rules to the Public (Default) filter, which allows only tunneled and ICMP traffic.

Figure 15-13 Configuration | Policy Management | Traffic Management | Filters Screen



Filter List

The Filter List shows configured filters, listed in the order they are configured.

Cisco supplies default filters that you can use and modify; see [Table 15-4](#).

Table 15-4 Cisco-Supplied Default Filters

Parameter	Private (Default)	Public (Default)	External (Default)
Description	Default filter for the Private Interface	Default filter for the Public Interface	Default filter for the External Interface
Default Action	Drop	Drop	Drop
Source Routing	No	No	No
Fragments	Yes	Yes	Yes
Current Rules in Filter	Any In (forward/in) Any Out (forward/out)	GRE In (forward/in) IPSEC-ESP In (forward/in) IKE In (forward/in) PPTP In (forward/in) L2TP In (forward/in) ICMP In (forward/in) VRRP In (forward/in) GRE Out (forward/out) IKE Out (forward/out) PPTP Out (forward/out) L2TP Out (forward/out) ICMP Out (forward/out) VRRP Out (forward/out)	-Empty-

Add Filter

To configure and add a new filter, click **Add Filter**. The Manager opens the Configuration | Policy Management | Traffic Management | Filters | Add screen. The Manager then automatically lets you assign rules to the filter.

Assign Rules to Filter

To assign or change rules in a configured filter, select the filter from the list and click **Assign Rules to Filter**. The Manager opens the Configuration | Policy Management | Traffic Management | Assign Rules to Filter screen, which lets you assign and order the rules that apply to this filter.

Modify Filter

To modify the basic parameters—but not the rules—for a filter that has been configured, click **Modify Filter**. The Manager opens the Configuration | Policy Management | Traffic Management | Filters | Modify screen.

Copy Filter

To create a new filter by copying the basic parameters and rules from a filter that has been configured, click **Copy Filter**. The Manager opens the Configuration | Policy Management | Traffic Management | Filters | Copy screen.

Delete Filter

To delete a configured filter, select the filter from the list and click **Delete Filter**. See the following notes. The Manager refreshes the screen and shows the remaining entries in the Filter List.



Note

You *cannot* delete a filter that has been applied to an interface. If you try to do so, the Manager displays an error message.



Note

You *can* delete a filter that has been applied to a group or user, *and there is no confirmation or undo*. Doing so might affect their use of the VPN.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | Policy Management | Traffic Management | Filters | Add, Modify, or Copy

These screens let you:

- Add: Configure the basic parameters for a new filter and add it to the list.
- Modify: Modify the basic parameters for a configured filter.
- Copy: Create a new filter that is a copy of a configured filter, and configure its basic parameters. The copy also includes all the rules and SAs of the original filter *except* rules with an Apply IPsec action.

You configure the rules in a filter on the Configuration | Policy Management | Traffic Management | Assign Rules to Filter screen.



Note

On the Modify screen, any changes take effect as soon as you click **Apply**. If this filter is being used by an interface or group, changes might affect data traffic.

Figure 15-14 Configuration | Policy Management | Traffic Management | Filters | Add, Modify, or Copy Screen

Configuration | Policy Management | Traffic Management | Filters | Add

Configure and add a new filter.

Filter Name	<input type="text"/>	Name of the filter you are adding. The name must be unique.
Default Action	<input type="text" value="Drop"/>	Select the default action to take when no rules on this filter apply.
Source Routing	<input type="checkbox"/>	Check to have this filter allow IP source routed packets to pass.
Fragments	<input checked="" type="checkbox"/>	Check to have this filter allow fragmented IP packets to pass.
Description	<input type="text"/>	
<input type="button" value="Add"/> <input type="button" value="Cancel"/>		

67255

Filter Name

Enter a unique name for this filter. Maximum is 48 characters.

Default Action

Click the **Default Action** drop-down menu button and choose the action that this filter takes if a data packet *does not match* any of the rules on this filter. The choices are:

- Drop = Discard the packet (the default choice).
- Forward = Allow the packet to pass.
- Drop and Log = Discard the packet and log a filter debugging event (FILTERDBG event class). See Configuration | System | Events and see the following note.
- Forward and Log = Allow the packet to pass and log a filter debugging event (FILTERDBG event class). See the following note.

**Note**

The Log actions are intended for use only while debugging filter activity. Since they generate and log an event for every matched packet, they consume significant system resources and might seriously degrade performance.

Source Routing

Check the **Source Routing** check box to allow IP source routed packets to pass. A source routed packet specifies its own route through the network and does not rely on the system to control forwarding. This box is unchecked by default, because source-routed packets can present a security risk.

Fragments

Check the **Fragments** check box to allow fragmented IP packets to pass. Large data packets might be fragmented on their journey through networks, and the destination system reassembles them. While you would normally allow fragmented packets to pass, you might disallow them if you suspect a security problem. This box is checked by default.

Description

Enter a description of this filter. This optional field is a convenience for you or other administrators; use it to describe the purpose or use of the filter. Maximum is 255 characters.

Add or Apply / Cancel

Add screen:

- To add this filter to the list of filters, click **Add**. The Manager opens the Configuration | Policy Management | Traffic Management | Assign Rules to Filter screen, which lets you assign and order the rules that apply to this filter.

Modify screen:

- To apply your changes to this filter, click **Apply**. The Manager returns to the Configuration | Policy Management | Traffic Management | Filters screen, and the modified filter appears in same location in the Filter List. *Any changes take effect as soon as you click Apply. If this filter is being used by an active interface or group, changes might affect data traffic.*

Copy screen:

- To apply your settings and add this filter to the list of filters, click **Apply**. The Manager returns to the Configuration | Policy Management | Traffic Management | Filters screen, and the new filter appears in the Filter List. To assign or change rules on the filter, select the filter from the list and click **Assign Rules to Filter**.

To discard your changes, click **Cancel**. The Manager returns to the Configuration | Policy Management | Traffic Management | Filters screen, and the Filter List is unchanged.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | Policy Management | Traffic Management | Assign Rules to Filter

This section of the Manager lets you add, remove, and prioritize the rules in a filter, and assign Security Associations to rules that are configured with an Apply IPsec action.

A filter applies its rules to data packets coming through the system, in the order the rules are arranged on the filter. If a rule matches, the system takes the Action specified in the rule. If not, it applies the next rule; and so on. If no rule matches, the system takes the Default Action specified in the filter.

The Manager groups applied rules by direction (inbound or outbound), with inbound rules first. You can prioritize rules only within a direction.

You configure rules on the Configuration | Policy Management | Traffic Management | Rules screens.



Note

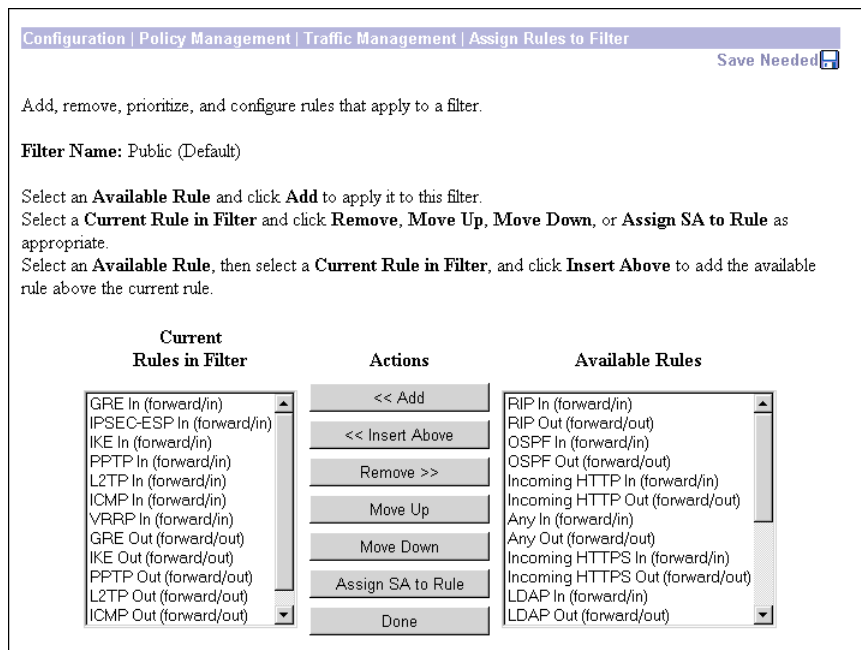
Rules affect the operation of the filter as soon as you add, remove, or prioritize them. If the filter is being used by an active interface or group, changes might affect data traffic.



Note

Be careful about adding or changing rules on the Public (Default) filter. You could compromise security.

Figure 15-15 Configuration | Policy Management | Traffic Management | Assign Rules to Filter Screen



Filter Name

The name of the filter for which you are configuring the rules. You cannot change this name here. (See Configuration | Policy Management | Traffic Management | Filters | Modify.)

Current Rules in Filter

This list shows the rules currently assigned to the filter. Use the scroll controls (if present) to see all the rules in the list. If no rules have been assigned, the list shows --Empty--. Each entry shows the rule name and the action/direction in parentheses; Apply IPsec rules include their Security Association.

Available Rules

This list shows all the rules currently configured on the system (all the rules in the active configuration) that have not been assigned to this filter. Use the scroll controls (if present) to see all the rules in the list. Each entry shows the rule name and the action/direction in parentheses. (Since Security Associations are added to Apply IPsec rules only when those rules are assigned to a filter, this list does not show SAs.)

<< Add

To add a rule to the filter, select the rule from the Available Rules list and click << **Add**. The Manager moves the rule to the Current Rules in Filter list, modifies the active configuration, refreshes the screen, and by default orders the current rules with all inbound rules preceding all outbound rules.

If you add a rule that has an Apply IPsec action configured, the Manager displays the Configuration | Policy Management | Traffic Management | Assign Rules to Filter | Add SA to Rule screen, which lets you add a Security Association to the rule. The Manager also, by default, adds Apply IPsec rules to the top of the group of rules with the same direction (inbound or outbound).

<< Insert Above

To add an available rule above a current rule, select the rule from the Available Rules list, then select a target rule in the Current Rules in Filter list, and click **Insert Above**. The Manager moves the rule to the Current Rules in Filter list, modifies the active configuration, refreshes the screen, and orders the new rule above the current rule. Both selected rules must have the same direction (inbound or outbound).

If you add a rule that has an Apply IPsec action configured, the Manager displays the Configuration | Policy Management | Traffic Management | Assign Rules to Filter | Add SA to Rule screen, which lets you add a Security Association to the rule.

>> Remove

To remove a rule from the filter, select the rule from the Current Rules in Filter list and click >> **Remove**. The Manager moves the rule to the Available Rules list, modifies the active configuration, refreshes the screen, and shows the remaining current rules in the filter.

You cannot remove a rule that is configured as part of a LAN-to-LAN connection. See the Configuration | System | Tunneling Protocols | IPsec LAN-to-LAN | Add | Done screen.

Move Up / Move Down

To change the order in which a rule is applied within the filter, select the rule from the Current Rules in Filter list and click **Move Up** or **Move Down**. The Manager reorders the current rules, modifies the active configuration, refreshes the screen, and shows the reordered list. If you try to move a rule out of its direction group (inbound or outbound), the Manager displays an error message.

Assign SA to Rule

To modify the Security Association applied to a current rule that has an Apply IPSec action configured, select the rule from the Current Rules in Filter list and click **Assign SA to Rule**. The Manager displays the Configuration | Policy Management | Traffic Management | Assign Rules to Filter | Change SA on Rule screen.

Done

When you are finished configuring the rules in this filter, click **Done**. The Manager returns to the Configuration | Policy Management | Traffic Management | Filters screen and refreshes the Filter List.

Reminder:

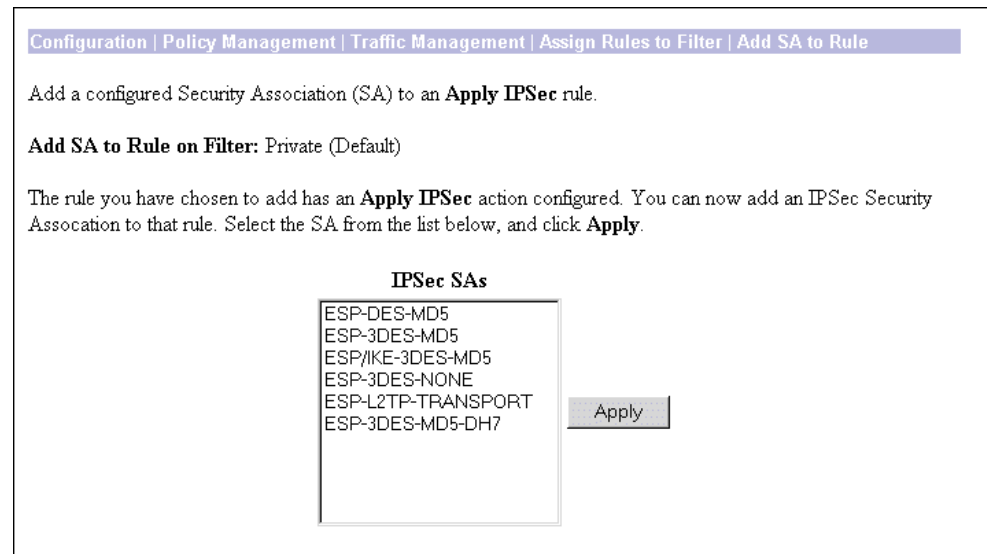
The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | Policy Management | Traffic Management | Assign Rules to Filter | Add SA to Rule

This screen lets you add a configured Security Association to a rule that has an Apply IPSec action configured. You can assign only one SA to a rule.

You configure Security Associations on the Configuration | Policy Management | Traffic Management | Security Associations screens.

Figure 15-16 Configuration | Policy Management | Traffic Management | Assign Rules to Filter | Add SA to Rule Screen



Add SA to Rule on Filter:

The Manager shows the name of filter to which you are adding a rule that has an Apply IPSec action configured. You cannot change this name here. See Configuration | Policy Management | Traffic Management | Filters | Modify.

IPSec SAs

The IPSec SAs list shows the configured SAs that are available, that is, all the SAs in the active configuration.

Apply

To add an SA to the rule, select the SA from the list and click **Apply**. The Manager returns to the Configuration | Policy Management | Traffic Management | Assign Rules to Filter screen for the filter you are configuring, modifies the active configuration, and updates the Current Rules in Filter list to show the rule with its SA.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | Policy Management | Traffic Management | Assign Rules to Filter | Change SA on Rule

This screen lets you change the configured Security Association that is applied to a rule that has an Apply IPSec action configured. You can assign only one SA to a rule.

On this screen, you change which SA is applied. You configure SAs themselves on the Configuration | Policy Management | Traffic Management | Security Associations screens.



Note

The change takes effect as soon as you click **Apply**. If this filter is being used by an interface or group, the change might affect tunnel traffic.

Figure 15-17 Configuration | Policy Management | Traffic Management | Assign Rules to Filter | Change SA on Rule Screen

Change SA on Rule in Filter

The Manager shows the name of the filter to which the IPSec rule is assigned. You cannot change this name here. See Configuration | Policy Management | Traffic Management | Filters | Modify.

IPSec SAs

The IPSec SAs list shows the configured SAs that are available (all the SAs in the active configuration). By default, the SA that is currently applied to the rule is selected.

Apply / Cancel

To apply a different SA to this rule, select the SA from the list and click **Apply**. The Manager returns to the Configuration | Policy Management | Traffic Management | Assign Rules to Filter screen for the filter you are configuring, modifies the active configuration, and updates the Current Rules in Filter list to show the rule with its new SA. *The change takes effect as soon as you click Apply. If this filter is being used by an active interface or group, the change might affect tunnel traffic.*

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard the change and keep the current SA on the rule, click **Cancel**. The Manager returns to the Configuration | Policy Management | Traffic Management | Assign Rules to Filter screen for the filter you are configuring, and the Current Rules in Filter list is unchanged.

Configuration | Policy Management | Traffic Management | NAT

This section of the Manager lets you configure and enable NAT (Network Address Translation). NAT translates private network addresses into an IANA-assigned public network address, and vice versa, and thus allows traffic routing between the networks.

A NAT session is a translation instance. When a packet passing through the VPN Concentrator matches a NAT rule and is translated, a NAT session begins. The NAT session records details of the translation, including the source IP address and port, the destination IP address and port, and the translated, or mapped, address and port.

A NAT rule defines the criteria that a packet must meet to be translated. For interface NAT rules, criteria include the protocol: portless, UDP, or TCP. For LAN-to-LAN connections, the criteria are the source, translated and destination IP addresses.

To use NAT, we recommend that you first configure NAT rules, then enable the function.

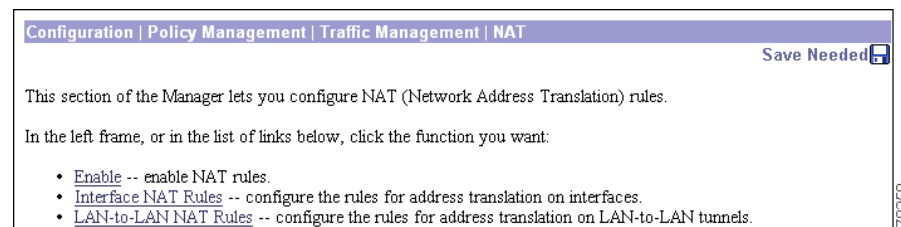
You can change NAT rules while NAT is enabled. Doing so affects subsequent sessions, but not current sessions, as long as the changed rule still allows the current session; if it doesn't traffic will stop.

For inbound packets, the destination address and port are mapped. For outbound traffic, the source address and port are mapped.

As packets pass through the VPN Concentrator, NAT sessions are searched for a match prior to applying NAT rules. If a match exists, the packet is translated in the same way as the packet that caused the session to initiate, and the session continues, allowing the VPN Concentrator to maintain address and port continuity within a session. NAT sessions expire and are deleted if they are unused for a certain time period, which varies depending on the protocol. Therefore, unless the NAT rule is a static rule, NAT sessions between the same clients may have different translated addresses for different NAT sessions.

For a detailed explanation of NAT and PAT, see <http://www.cisco.com/warp/public/556/nat-cisco.shtml>.

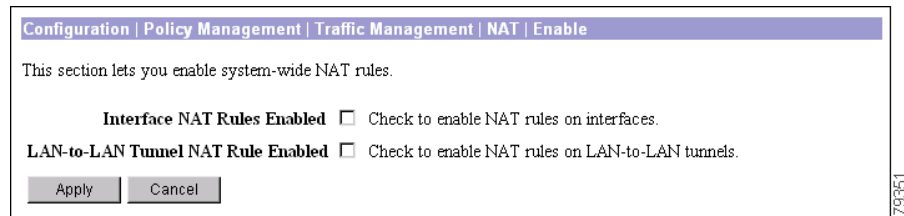
Figure 15-18 Configuration | Policy Management | Traffic Management | NAT Screen



Configuration | Policy Management | Traffic Management | NAT | Enable

This screen lets you enable NAT operation for Interfaces, which applies NAT to all non-tunneled traffic flowing through the public interface, and for LAN-to-LAN tunnels. We recommend that you configure NAT rules before you enable the function.

Figure 15-19 Configuration | Policy Management | Traffic Management | NAT | Enable Screen



Interface NAT Rules Enabled

Check the **Interface NAT Rules Enabled** check box to enable NAT rules for interfaces, or uncheck it to disable these NAT rules. By default, the box is unchecked.

LAN-to-LAN Tunnel NAT Rule Enabled

Check the LAN-to-LAN Tunnel NAT Rule Enabled check box to enable NAT rules for LAN-to-LAN connections, or uncheck it to disable these NAT rules. By default, the box is unchecked.

Apply / Cancel

To enable or disable NAT rules, and include your setting in the active configuration, click **Apply**. The Manager returns to the Configuration | Policy Management | Traffic Management | NAT screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

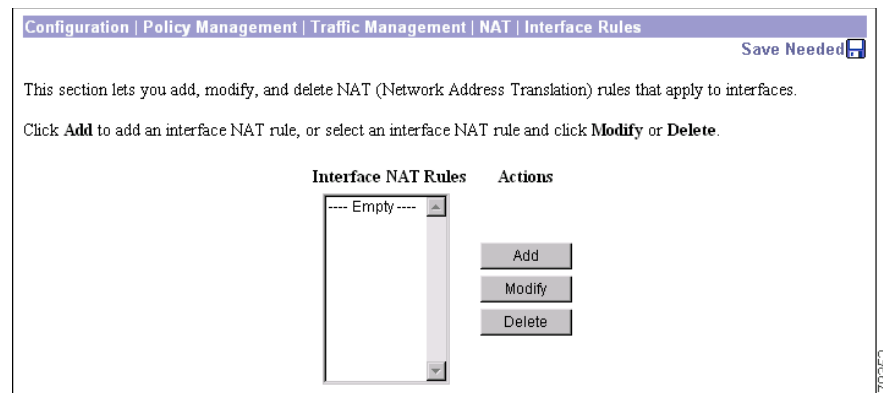
To discard your entry and leave the active configuration unchanged, click **Cancel**. The Manager returns to the Configuration | Policy Management | Traffic Management | NAT screen.

Configuration | Policy Management | Traffic Management | NAT | Interface Rules

This section of the Manager lets you add, configure, modify, and delete Interface NAT rules. We recommend that you first configure and add rules, then enable the function. To configure Interface NAT rules, you must first configure a VPN Concentrator public interface; see Configuration | Interfaces.

You need at least one rule for each private network that the VPN Concentrator connects to, and that uses NAT.

Figure 15-20 Configuration | Policy Management | Traffic Management | NAT | Interface Rules Screen



Interface NAT Rules

The Interface NAT Rules list shows NAT rules that have been configured. If no rules have been configured, the list shows --Empty--. The format of each rule is: *Private Address/Subnet-Mask-on Interface (Action)*; for example, 10.0.0.0/8 on Ethernet 2 (Public) (TCP).

Add / Modify / Delete

To configure and add a new Interface NAT rule to the list of configured rules, click **Add**. The Manager opens the Configuration | Policy Management | Traffic Management | NAT | Interface Rules | Add screen. If you have not configured a public interface, the Manager displays the Configuration | Policy Management | Traffic Management | NAT | Rules | No Public Interfaces screen.

To modify a configured NAT rule, select the rule from the NAT Rules list and click **Modify**. The Manager opens the Configuration | Policy Management | Traffic Management | NAT | Interface Rules | Modify screen.

To delete a configured NAT rule, select the rule from the NAT Rules list and click **Delete**.

**Note**

There is no confirmation or undo.

The Manager refreshes the screen and shows the remaining rules in the list.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | Policy Management | Traffic Management | NAT | Rules | No Public Interfaces

The Manager displays this screen if you have not configured a public interface on the VPN Concentrator and you try to add a NAT rule. The public interface need not be enabled, but it must be configured with an IP address and the Public Interface parameter enabled.

You should designate only one VPN Concentrator interface as a public interface.

Figure 15-21 Configuration | Policy Management | Traffic Management | NAT | Rules | No Public Interfaces Screen

Configuration | Policy Management | Traffic Management | NAT | Rules | No Public Interfaces

You need to have a public interface configured before adding a NAT rule. Select and click on an interface you want to configure:

Interface	Status	IP Address	Subnet Mask
Ethernet 2 (Public)	Not Configured		
WAN Interface in slot 2, port A	Not Configured		
WAN Interface in slot 2, port B	Not Configured		

67279

Click the highlighted link to configure the desired public interface. The Manager opens the appropriate Configuration | Interfaces screen.

Configuration | Policy Management | Traffic Management | NAT | Interface Rules | Add or Modify

These screens let you:

- Add: Configure and add new Interface NAT rules.
- Modify: Modify a previously configured Interface NAT rule.

You must configure a public interface on the VPN Concentrator before you can add an Interface NAT rule. See the Configuration | Interfaces screens.

Figure 15-22 Configuration | Policy Management | Traffic Management | NAT | Interface Rules | Add or Modify Screen

Configuration | Policy Management | Traffic Management | NAT | Interface Rules | Add

Add a new interface NAT rule.

Interface Select the interface to put this NAT rule on.

Private Address

IP Address

Subnet Mask Specify the private IP address and subnet mask that this rule checks.

Action

Map Portless Protocols

Map UDP

Map TCP

FTP Proxy

Select the translation action for this rule.

79353

Interface

Add screen:

- Click the drop-down menu button and select the configured public interface for this Interface NAT rule. The list shows all interfaces that have the Public Interface parameter enabled. See Configuration | Interfaces.

Modify screen:

- The screen shows the configured public interface for this Interface NAT rule. You cannot change the interface. To move the rule to another interface, you must delete this rule and add a new one for the other interface.

Private Address

Specify the private network (subnet) addresses that NAT translates to and from the public address.

IP Address

Enter the private IP address in dotted decimal notation, for example: 10.0.0.1.

Subnet Mask

Enter the subnet mask appropriate for the private IP address range. Use dotted decimal notation; the default is 255.255.255.255. For example, to translate all private addresses in class A network 10, enter **255.0.0.0**.

In the NAT Rules list, the subnet mask is shown as the number of ones; for example, 255.255.0.0 is shown as /16.

Action

Check the box(es) to choose the translation action(s) for this NAT rule:

- Map Portless Protocols = Translate addresses for packets with protocols that do not use ports and thus do not involve port mapping (default). For example, this action supports ping, which uses ICMP.
- Map UDP = Map ports within outbound UDP packets to dynamic ports (49152 to 65535) on the public IP address, and vice versa.
- Map TCP = Map ports within outbound TCP packets to dynamic ports (49152 to 65535) on the public IP address, and vice versa.
- FTP Proxy = Provide FTP proxy server functions and map outbound ports to dynamic ports (49152 to 65535) on the public IP address. FTP requires specialized NAT behavior; this action allows outgoing FTP transactions to function properly.

Add or Apply / Cancel

To add this rule to the list of configured Interface NAT rules, click **Add**. Or to apply your changes to this Interface NAT rule, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | Policy Management | Traffic Management | NAT | Interface Rules screen. Any new rule appears at the bottom of the Interface NAT Rules list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | Policy Management | Traffic Management | NAT | Rules screen, and the Interface NAT Rules list is unchanged.

Configuration | Policy Management | Traffic Management | NAT | LAN-to-LAN Rules

This section of the Manager lets you add, configure, modify, and delete LAN-to-LAN NAT rules that apply only to traffic that passes over LAN-to-LAN tunnels. We recommend that you first configure and add rules, then enable the function.

About LAN-to-LAN NAT

Private networks often use the same private address spaces. For connecting VPN networks, this duplication of IP addresses can prevent communication, because traffic from one private network to another using the same address space is perceived as local, and therefore does not travel to the second network. You can use NAT to solve this problem, translating private network addresses to legitimate public network addresses as packets enter the tunnel, rather than assigning new IP addresses to the networks.

Mapping rules that you configure determine how LAN-to-LAN NAT translates network addresses. There are three types of mapping rules:

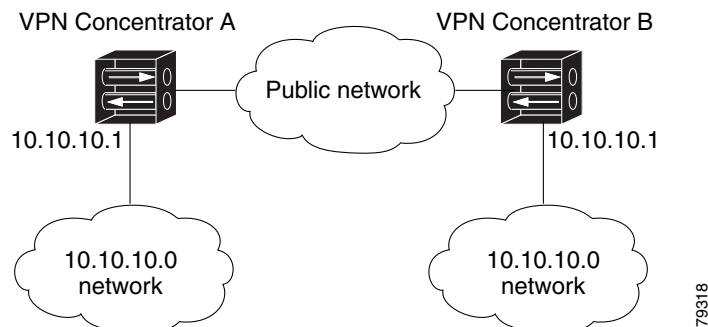
- *Static* LAN-to-LAN NAT rules map source IP addresses to Translated IP addresses on a one-to-one basis. Static rules apply both to
 - *inbound* traffic, which is traffic received over a LAN-to-LAN tunnel.
 - *outbound* traffic, which is traffic bound for a LAN-to-LAN tunnel.

Static rules are restricted to networks in which the local network and mapped network are of the same size. Port mappings are unnecessary, and are not performed.

- *Dynamic* LAN-to-LAN NAT rules map source IP addresses to one of a pool of available translated IP addresses, or to a single address. Dynamic mappings apply only to outbound traffic.
- *PAT* LAN-to-LAN NAT rules are dynamic rules with Port Address Translation. PAT rules apply to outbound traffic only

Figure 15-23 is an example of a network topology that has complete overlap in the address spaces for the networks behind VPN Concentrators A and B.

Figure 15-23 LAN-to-LAN NAT Example



79318

The LAN-to-LAN NAT mapping rules for these VPN Concentrators are as follows:

VPN Concentrator	Rule and Type	Mappings
VPN Concentrator A	A - Dynamic/PAT	10.10.10.0/24 -> 20.20.20.9
VPN Concentrator B	B - Static NAT	10.10.10.0/24 -> 30.30.30.0/24

The VPN Concentrators are configured as follows:

- A LAN-to-LAN tunnel connects networks 20.20.20.0/24 and 30.30.30.0/24.
- Concentrator A is configured to route traffic destined for 30.30.30.0 through the LAN-to-LAN tunnel.
- Concentrator B is configured to route traffic destined for 20.20.20.0 through the LAN-to-LAN tunnel.

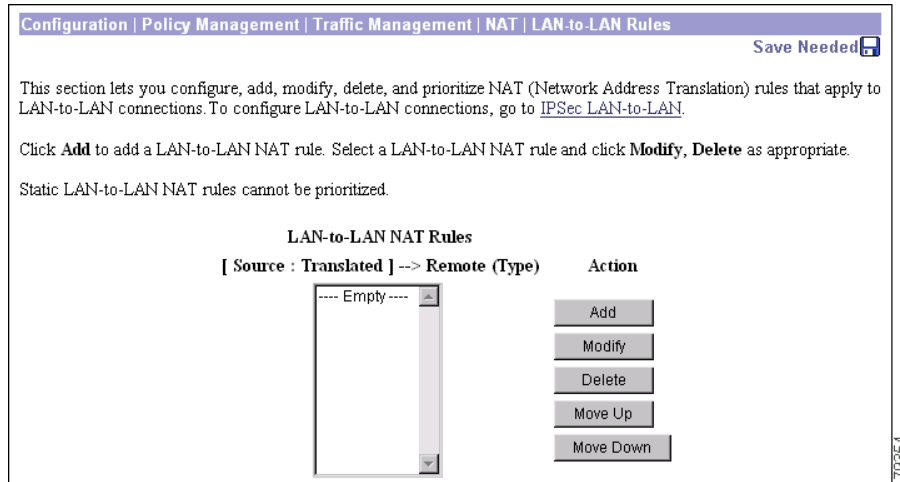
A client with the IP address of 10.10.10.2 on network A sends a message to a server on network B with an IP address of 10.10.10.4. The clients on Network A already know the static address translation of the servers on Network B. Table [Table 15-5](#) describes the message flow and the NAT translations that occur.

Table 15-5 LAN-to-LAN NAT Message Flow for LAN-to-LAN Tunnel Networks 20.20.20.0/24 and 30.30.30.0/24.

Concentrator A				Concentrator B		
Private network 10.10.10.0	After outbound NAT translation	After inbound NAT translation	tunnel direction	After inbound NAT translation	After outbound NAT translation	Private network 10.10.10.0
Host with source IP address of 10.10.10.2 sends a message to server on network B with destination IP address of 30.30.30.4	Source IP address translates to 20.20.20.9, using Rule A to create Session A1. Destination IP address is 30.30.30.4.		-> ->	Source IP address is 20.20.20.9. Destination IP address 30.30.30.4 translates to 10.10.10.4, using Rule B to create Session B1.		Server with destination IP address 10.10.10.4 receives packet from host with source IP address of 20.20.20.9.
						 VV
		Source IP address is 30.30.30.4. Destination IP address translates to 10.10.10.2, with Concentrator A using mapping information from Session A1.	<- <-		Source IP address translates to 30.30.30.4, with Concentrator B using mapping information from Session B1. Destination IP address is 20.20.20.9.	Server with source IP address of 10.10.10.4 replies to host with destination IP address of 20.20.20.9.

You configure LAN-to-LAN NAT rules in the Configuration | Policy Management | NAT | LAN-to-LAN Rules screen.

Figure 15-24 Configuration | Policy Management | Traffic Management | NAT | LAN-to-LAN Rules Screen



LAN-to-LAN NAT Rules

The LAN-to-LAN NAT Rules list show rules that have been configured. The format is [Source : Translated] -> Remote (Type). If no LAN-to-LAN NAT rules have been configured, the list shows --Empty--.

Source

This is the host IP address and wildcard mask on the private network.

Translated

This is the translated IP address and wildcard mask for the local address of this LAN-to-LAN connection. This is also the translated address space.

Remote

This is the destination IP address and wildcard mask for this LAN-to-LAN connection. The rule is applied only to packets bound for this address space. The address space must be part of the destination address space of a LAN-to-LAN connection.

Type

This identifies the type of LAN-to-LAN NAT Rule:

- *Static* LAN-to-LAN NAT rules map source IP addresses to Translated IP addresses on a one-to-one basis. Static rules apply both to
 - *inbound* traffic, which is traffic received over a public interface.
 - *outbound* traffic, which is traffic bound for a public interface.

Static rules are restricted to networks in which the local network and mapped network are of the same size. Port mappings are unnecessary, and are not performed.

- *Dynamic* LAN-to-LAN NAT rules map source IP addresses to one of a pool of available translated IP addresses, or to a single address. Dynamic mappings apply only to outbound traffic.
- *PAT* LAN-to-LAN NAT rules are dynamic rules with Port Address Translation. PAT rules apply to outbound traffic only.

Add / Modify / Delete

To configure and add a new LAN-to-LAN NAT rule, click **Add**. The Manager opens the Configuration | Policy Management | Traffic Management | NAT | LAN-to-LAN Rules | Add screen.

To modify a configured NAT rule, select the rule from the NAT Rules list and click **Modify**. The Manager opens the Configuration | Policy Management | Traffic Management | NAT | LAN-to-LAN Rules | Modify screen.

To delete a configured NAT rule, select the rule from the LAN-to-LAN NAT Rules list and click **Delete**.

**Note**

There is no confirmation or undo.

The Manager refreshes the screen and shows the remaining rules in the list.

Move Up / Move Down

You can use the Move Up and Move Down buttons to sort LAN-to-LAN NAT rules in priority order, except

- Static rules have priority over dynamic rules.
- You cannot prioritize static rules. The VPN Concentrator gives static rules for smaller networks a higher priority than those for larger networks. Therefore, the priority order of static rules is:
 - Host-to-host
 - Class C
 - Class B
 - Class A

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | Policy Management | Traffic Management | NAT | LAN-to-LAN Rules | Add or Modify

This screen lets you add or modify NAT LAN-to-LAN rules.

Figure 15-25 Configuration | Policy Management | Traffic Management | NAT | LAN-to-LAN Rules | Add or Modify Screens

Configuration | Policy Management | Traffic Management | NAT | LAN-to-LAN Rules | Add Save Needed

Add a new LAN-to-LAN NAT rule.

NAT Type

Static **Static:** maps source IP addresses to translated IP addresses on a one-to-one basis. Static mappings apply to both inbound and outbound traffic.

Dynamic **Dynamic:** maps source IP addresses to one of a pool of available translated IP addresses. Dynamic mappings apply to outbound traffic only.

PAT **PAT:** Dynamic mapping with Port Address Translation. PAT applies to outbound traffic only.

Source Network: specifies the source IP address and wildcard mask to be translated.
Translated Network: specifies the translated IP address and wildcard mask for the **Local Network**. It is the local address of the LAN-to-LAN connection.
Remote Network: specifies the destination IP address and wildcard mask for which this rule applies. To allow any remote network, set IP address/wildcard mask to 0.0.0.0/255.255.255.255. It is the remote address of the LAN-to-LAN connection.

	Source Network	Translated Network	Remote Network
IP Address		:	
		->	0.0.0.0
Wildcard Mask		:	
		->	255.255.255.255

79365

NAT Type

This identifies the type of LAN-to-LAN NAT Rule:

- *Static* LAN-to-LAN NAT rules map source IP addresses to Translated IP addresses on a one-to-one basis. Static rules apply both to
 - *inbound* traffic, which is traffic received over a public interface.
 - *outbound* traffic, which is traffic bound for a public interface.

Static rules are restricted to networks in which the local network and mapped network are of the same size. Port mappings are unnecessary, and are not performed.

- *Dynamic* LAN-to-LAN NAT rules map source IP addresses to one of a pool of available translated IP addresses, or to a single address. Dynamic mappings apply only to outbound traffic.
- *PAT* LAN-to-LAN NAT rules are Edenic rules with Port Address Translation. PAT rules apply to outbound traffic only.

Guideline for Defining NAT Rules and Types

Understand this caveat as you define NAT rules for LAN-to-LAN connections:

If you expect inbound traffic, you need to define a static LAN-to-LAN NAT rule. This is because with any other type of NAT rule, the translated address is impossible to predict, leaving the sender no way of identifying the IP address to which it should send packets.

Source Network

This is the network IP address and wildcard mask the rule translates.

Translated Network

This is the translated IP address and wildcard mask for the local network of this LAN-to-LAN connection.

Remote Network

This is the destination IP network and wildcard mask for this LAN-to-LAN connection.

**Note**

If you have a network with any remote access clients, you must specifically define the remote network, and not accept the default values of 0.0.0.0/255.255.255.255. If you were to accept these default values, and the source network and wildcard mask of the rule overlaps or is the same as the network addresses assigned to remote access clients, the VPN Concentrator attempts to NAT traffic intended for the remote access clients for the LAN-to-LAN connection instead, and that traffic never reaches the remote access clients. The only exception to this is for remote access clients that get their IP addresses from a third network, in which case you can use default values for this parameter.

IP Address

Enter the source IP address in dotted decimal notation. Default is 0.0.0.0.

Wildcard Mask

Enter the wildcard mask in dotted decimal notation. Default is 255.255.255.255.

**Note**

A wildcard mask is the reverse of a subnet mask. The wildcard mask has ones in bit positions to ignore, zeros in bit positions to match. For example:

0.0.0.0/255.255.255.255 = any address

10.10.1.35/0.0.0.0 = only 10.10.1.35

10.10.1.35/0.0.0.255 = all 10.10.1.nnn addresses

**Note**

There is no confirmation or undo.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

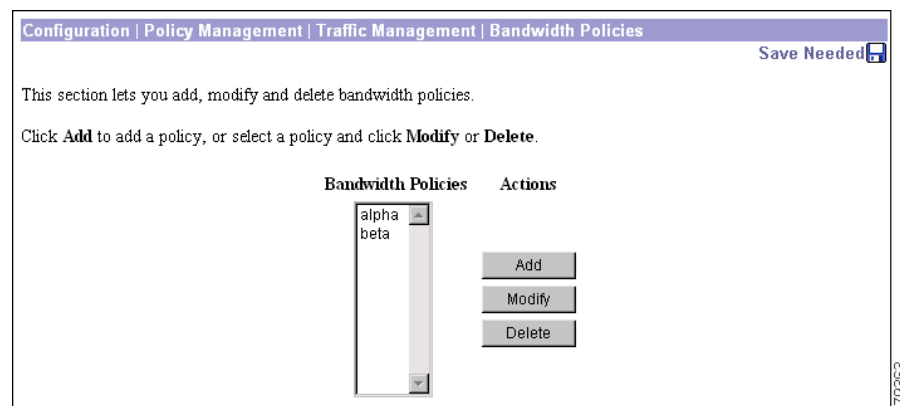
Configuration | Policy Management | Traffic Management | Bandwidth Policies

This section of the Manager lets you configure bandwidth management policies. You can configure a bandwidth policy to do one or all of the following:

- Reserve a minimum amount of bandwidth per session
- Limit users within groups to a maximum amount of bandwidth

Once you configure bandwidth policies, you can apply them either to an interface, or a group, or both. If you apply a policy to an interface only, it applies to each user on the interface. If you apply a policy to a group, it applies only to the users in that group. If you apply one policy to an interface and a different policy to a group, users who are members of that group use the group policy, and all other users use the interface policy.

Figure 15-26 Configuration | Policy Management | Traffic Management | Bandwidth Policies Screen



Add / Modify / Delete

To create a new bandwidth policy, click **Add**. The Manager opens the Configuration | Policy Management | Traffic Management | Bandwidth Policies | Add screen.

To modify a configured bandwidth policy, select the policy in the Bandwidth Policies list and click **Modify**. The Manager opens the Configuration | Policy Management | Traffic Management | Bandwidth Policies | **Modify** screen

To delete a configured bandwidth policy, select the policy in the Bandwidth Policies list and click **Delete**.

Configuration | Policy Management | Traffic Management | Bandwidth Policies | Add or Modify

This screen lets you:

Add: Configure and add a bandwidth policy

Modify: Modify a previously configured bandwidth policy

Overview of Bandwidth Management

There are two aspects of bandwidth management: bandwidth policing and bandwidth reservation. *Bandwidth policing* limits the maximum rate of tunneled traffic. The VPN Concentrator transmits traffic it receives below this rate; it drops traffic above this rate. *Bandwidth reservation* sets aside a minimum bandwidth rate for tunneled traffic. Using bandwidth management, you can allocate bandwidth to groups and users equitably, thus preventing certain groups or users from consuming a majority of the bandwidth.

Bandwidth management applies only to tunneled traffic (L2TP, PPTP, IPSec) and is most commonly applied to the *public* interface.



Tip

If you receive an error message when you're configuring any bandwidth management feature, check the event log. The event log gives very specific feedback for bandwidth management errors.

Bandwidth Reservation

Bandwidth reservation sets aside a minimum limit of bandwidth per tunnel for tunneled traffic. Each user receives at least a set amount of bandwidth. When there is little traffic on the box, users receive more than their allocated minimum of bandwidth. When the box becomes busy, they receive at least that much. When the combined total of the reserved bandwidth amounts of all active tunnels on an interface approaches the limit of the total bandwidth available on that interface, the VPN Concentrator refuses further connections to users who demand more reserved bandwidth than is available.

You can configure bandwidth reservation on just an interface (usually the public). In this case, every user who connects on the public interface receives the same reserved minimum bandwidth. If, in addition, you configure reserved bandwidth on a particular group, users in that group can claim an amount of reserved bandwidth that differs from that of the other users on the interface. You cannot configure reserved bandwidth on a specific group unless you have first configured reserved bandwidth on the interface.

Example One: A Bandwidth Reservation Policy Applied to an Interface

Suppose the link rate on your public interface is 1,544 kbps. And suppose you apply a reserved bandwidth policy to that interface that sets the reserved bandwidth to the default: 56 kbps per user. With this link rate and policy setting, only a total of 27 users can connect to the VPN Concentrator at one time. (1544 kbps per interface divided by 56 kbps per user equals 27 connections.)

- The first user who logs on to the VPN Concentrator gets his reserved 56 kbps plus the remainder of the bandwidth (1488 kbps).
- The second user who logs on to the VPN Concentrator gets his reserved 56 kbps plus he shares the remainder of the bandwidth (1432 kbps) with the first user.
- When the twenty-seventh user connects, all users are throttled to their minimum of 56 kbps per connection.
- When the twenty-eighth user attempts to connect, the VPN Concentrator refuses the connection. It does not allow any additional connections because it cannot supply the minimum 56 kbps reserve to more users.

Example Two: Bandwidth Reservation Policies Applied to an Interface and a Group

Add bandwidth reservation on a particular group to the above example. The group “Executives” reserves 112 kbps of the public interface bandwidth for any member of the group.

- The first user who logs on to the VPN Concentrator is not in the Executive group. He gets his reserved 56 kbps plus the remainder of the bandwidth (1488 kbps).
- Then, the president logs in. She gets her 112 kbps plus she shares the remainder of the bandwidth (1376 kbps) with the first user.
- As more executives and non-executives connect, they each receive the specified amount of bandwidth (112 kbps or 56 kbps) plus they share the bandwidth that remains. The VPN Concentrator allows users to connect until it can no longer provide the minimum reserve (56 kbps for a non-executive, 112 kbps for an executive).

Keep in mind that there may be many groups using the VPN Concentrator, each with different bandwidth policies.

Bandwidth Aggregation

From Example Two, you can see that configuring bandwidth reservation alone can lead to a scenario in which high priority, high bandwidth users are unable to connect to a congested VPN Concentrator because of their bandwidth requirements. For this case, the VPN Concentrator provides a feature called bandwidth aggregation. Bandwidth aggregation allows a particular group to reserve a fixed portion of the total bandwidth on the interface. (This fixed portion is known as an *aggregation*.) Then, as users from that group connect, each receives a part of the total bandwidth allocated for the group. Users who are not in that group cannot share this reserved portion, even if no one else is using it. When one group makes a reserved bandwidth aggregation, it does not affect the bandwidth allocated to users who are not in that group; however, those other users are now sharing a smaller amount of total bandwidth. Fewer of them can connect.

Suppose the company president in Example Three wants two top executives to be able to access the VPN Concentrator at any time. In this case, you can configure a bandwidth aggregation of $x/2$ (or half the bandwidth) for the group “Top Executives.” Half the bandwidth of the interface would then be set aside for the use of this group. This means however, that all the other users on the interface compete for the remaining half of the bandwidth.

LAN-to-LANs and Bandwidth Reservation

Configure bandwidth reservation for a LAN-to-LAN connection as you would for a group with one user. In this way, you reserve a set amount of bandwidth for the connection. (The users on the LAN-to-LAN connection are not managed, only the connection.) When you apply a bandwidth reservation policy to a LAN-to-LAN connection, the VPN Concentrator automatically adds bandwidth aggregation.

Bandwidth Policing

Bandwidth policing sets a maximum limit, a cap, on the rate of tunneled traffic. The VPN Concentrator transmits traffic it receives below this rate; it drops traffic above this rate.

Because traffic is bursty, some flexibility is built into policing. Policing involves two thresholds: the *policing rate* and the *burst size*. The policing rate is the maximum limit on the rate of sustained tunneled traffic. The burst size indicates the maximum size of an instantaneous burst of bytes allowed before traffic is capped back to the policing rate. The VPN Concentrator allows for instantaneous bursts of traffic greater than the policing rate up to the burst rate. But should traffic bursts consistently exceed the burst rate, the VPN Concentrator enforces the policing rate threshold.

Configuring Bandwidth Management

To configure bandwidth management, follow these steps:

-
- Step 1** Using this section of the Manager: define one or more bandwidth management policies.
 - Step 2** On the Configuration | Interfaces | Ethernet 2 screen, [Bandwidth Parameters Tab](#):
 - a. Enable bandwidth management on the public (or any other) interface.
 - b. Specify the link rate.
 - c. Assign a bandwidth policy to the interface to assign a default policy for all users on that interface.
If you are further planning to assign a bandwidth reservation policy to a specific group, this default policy must include bandwidth reservation.
 - Step 3** If you also want to manage bandwidth for a specific group, use the [Configuration | User Management | Groups | Bandwidth Policy](#) screen to apply a bandwidth policy to that group.
 - Step 4** If you want to manage bandwidth for a specific LAN-to-LAN connection, use the [Bandwidth Policy](#) parameters on the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN screen to apply a bandwidth policy to that connection.
-

Note the following dependencies when assigning bandwidth management policies to an interface and a group combined:

- If you apply only a policing policy (i.e. no reservation policy) to an interface, you cannot subsequently assign bandwidth reservation policies to groups using that interface. If you want to apply a bandwidth reservation policy to a group, you must first apply a bandwidth reservation policy to the interface.
- If you apply a reservation policy to an interface, all other policies applied to groups on that interface also include bandwidth reservation.

Use [Table 15-6](#) as a guide to these dependencies when you configure this feature.

Table 15-6 Conceptual Overview of Bandwidth Management Configuration

In order to...	Configure the following...				
	Enable Bandwidth Management on the Public Interface	Use this Type of Bandwidth Management Policy...			Apply the Bandwidth Management Policy to:
		Bandwidth Policing	Bandwidth Reservation	Bandwidth Aggregation	
Allow users and tunnels to consume bandwidth as needed on a first-come first-served basis.	-	-	-	-	-
Reserve every user on the interface a default minimum amount of the bandwidth of the interface.	Yes	-	Yes	-	Interface
Reserve every user in a particular group an equal minimum amount of the bandwidth of the interface. (Users not in the group use the bandwidth reservation assigned to the interface.)	Yes	-	Yes	-	Interface and group
Set aside a fixed amount of bandwidth for the exclusive use of members of a specific group. (Users not in this group cannot access this bandwidth, even if it is unused.)	Yes	-	Yes	Yes	Apply bandwidth reservation to the interface and apply bandwidth aggregation to the group.
Reserve a set amount of bandwidth for the exclusive use of a LAN-to-LAN tunnel. Ensure that bandwidth is always available for the LAN-to-LAN tunnel. (In other words, ensure that the LAN-to-LAN tunnel can always connect, even if the VPN Concentrator is congested.)	Yes	-	Yes	Yes (Done automatically)	Interface and LAN-to-LAN
Limit all users on the interface to a set bandwidth threshold.	Yes	Yes	-	-	Interface
Limit all users in a particular group to a set bandwidth threshold.	Yes	Yes	-	-	Apply either bandwidth reservation or policing to the Interface. Apply policing to the group

Once you know which bandwidth management features you want to apply to which level (interface, group, or LAN-to-LAN), follow the steps in [Table 15-7](#) to configure them.

Table 15-7 Bandwidth Management Configuration Guide

Task	Use this Screen...	Do this...
Create a Bandwidth Management Policy	Configuration Policy Management Traffic Management Bandwidth Policies Add	Name the policy, then apply reservation and/or policing and set the corresponding parameters.
Enable Bandwidth Management on the Public Interface	Configuration Interfaces Ethernet 2, Bandwidth tab	Check the Bandwidth Management check box. Set the link rate. Apply a bandwidth management policy.
Use Bandwidth Policing	Configuration Policy Management Traffic Management Bandwidth Policies Add or Modify	Create a policing policy: Check the Policing check box and enter the policing rate and burst size.
Use Bandwidth Reservation	Configuration Policy Management Traffic Management Bandwidth Policies Add or Modify	Create a reservation policy: Check the Bandwidth Reservation check box and enter the minimum bandwidth.
Use Bandwidth Aggregation	Configuration User Management Groups Bandwidth Policy Interfaces	Set Aggregate Bandwidth to a value greater than zero.
Assign Bandwidth Policy(ies) to:		
• Interface	Configuration Interfaces Ethernet 2, Bandwidth tab	Choose a policy from the Bandwidth Policy drop-down menu.
• Group	Configuration User Management Groups Bandwidth Policy Interfaces	Choose a policy from the Policy drop-down menu.
• LAN-to-LAN	Configuration System Tunneling Protocols IPSec LAN-to-LAN Add or Modify	Choose a policy from the Bandwidth Policy drop-down menu.

Figure 15-27 Configuration | Policy Management | Traffic Management | Bandwidth Policies | Add or Modify screen

When configuring a bandwidth policy, you must enable (check) either **Bandwidth Reservation** or **Policing**. You can enable both policies.

Policy Name

Enter a unique policy name that can help you remember the policy. The maximum length is 32 characters.

Bandwidth Reservation

To reserve a minimum amount of bandwidth for each session, check the **Bandwidth Reservation** check box.

Minimum Bandwidth

The minimum bandwidth is the amount of bandwidth reserved per user during periods of congestion. Enter a value for the minimum bandwidth and select one of the following units of measurement. The range is between 8000 bps and 100 Mbps. The default is 56000 (bps)

- bps—bits per second
- kbps—one thousand bits per second
- Mbps—one million bits per second

Policing

To enable policing, check the **Policing** check box.

Policing Rate

Enter a value for Policing Rate and select the unit of measurement. The VPN Concentrator transmits traffic that is moving below the policing rate and drops all traffic that is moving above the policing rate. The range is between 56000 bps and 100 Mbps. The default is 56000 (bps)

- bps—bits per second
- kbps—one thousand bits per second
- Mbps—one million bits per second

Normal Burst Size

The VPN Concentrator drops traffic that are above the normal burst size. The normal burst size is the amount of instantaneous burst that the VPN Concentrator can send at any give time.

To set the burst size, use the following formula: $(\text{Policing Rate}/8) * 1.5$. For example, if you want to limit users to 250 kbps of bandwidth, set the police rate to 250 kbps and set the burst size to 46875, that is: $(250000 \text{ bps}/8) * 1.5$.

Enter the Normal Burst Size and select the unit of measurement. The default is 10500 bytes. The minimum is 10500 bytes.

- bytes
- Kbytes—one thousand bytes
- Mbytes—one million bytes

Add/Cancel

To add this policy to the configuration, click **Add**. To cancel the action, click **Cancel**.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | Policy Management | Traffic Management | Bandwidth Policies screen, and the Bandwidth Policies list is unchanged.

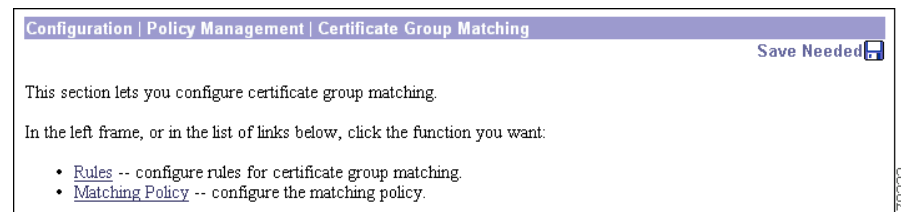
Configuration | Policy Management | Certificate Group Matching

This section of the Manager allows you to define rules to match a user's certificate to a permission group based on fields in the distinguished name (DN). In releases previous to 3.6, the VPN Concentrator used the OU field from a user's certificate to assign that user to a permission group. For example, if the OU field of a user's certificate was "Sales," the VPN Concentrator assigned that user to the "Sales" permission group. The certificate group matching feature allows you identify members of a permission group on the basis of other criteria: you can use other fields of the certificate or you can have all certificate users share a permission group.

To match users' permission groups based on other fields of the certificate, you must define rules that specify which fields to match for a group and then enable each rule for that selected group. A group must already exist in the configuration before you can create a rule for it. You can assign multiple rules to the same group. When multiple rules are assigned to the same group, a match results for the first rule that tests true.

Once you have defined rules, you must configure a certificate group matching policy to define the method you want to use to identify the permission groups of certificate users: match the group from the rules, match the group from the OU field, or use a default group for all certificate users. You can use any or all of these methods.

Figure 15-28 Configuration | Policy Management | Certificate Group Matching Screen



Rules

Click the **Rules** link to create certificate group matching rules.

Matching Policy

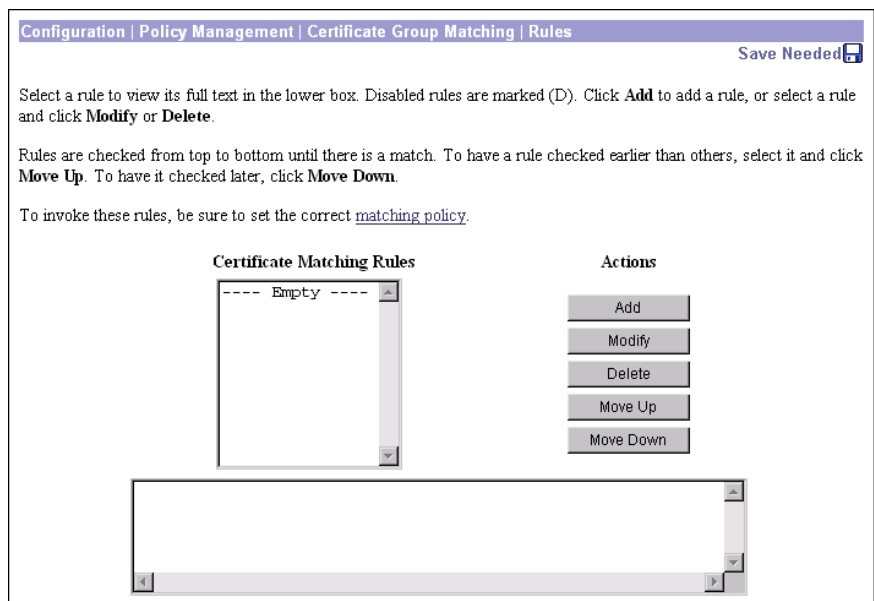
Click the **Matching Policy** link to choose a method to identify the permission groups of certificate users.

Configuration | Policy Management | Certificate Group Matching | Rules

This screen lets you:

- Add: Configure and add a new rule for certificate group matching.
- Modify: Modify a previously configured certificate group matching rule.
- Delete: Remove a rule from the configuration.
- Move Up: Change the order of the rule so that it is checked earlier.
- Move Down: Change the order of the rule so that it is checked later.

Figure 15-29 Configuration | Policy Management | Certificate Group Matching | Rules Screen



Add/Modify Rule

To configure and add a new rule, click **Add** on the Configuration | Policy Management | Certificate Group Matching | Rules screen.

To modify an existing rule, select a rule in the Certificate Matching Rules box and click **Modify**. When you select a rule, the complete text appears in the box below the Certificate Matching Rules box.

Delete

To delete a configured rule, select the rule from the list in the Certificate Matching Rules box and click **Delete**. The Manager refreshes the screen and shows the remaining rules in the list.

Move Up

To have the VPN Concentrator check the rule earlier in the order, select the rule and click **Move Up**.

Move Down

To have the VPN Concentrator check the rule later in the order, select the rule and click **Move Down**.

Configuration | Policy Management | Certificate Group Matching | Rules | Add or Modify

These screens let you:

- Add: Configure and add a new certificate group matching rule.
- Modify: Modify a previously configured certificate matching rule.

Figure 15-30 Configuration | Policy Management | Certificate Group Matching | Rules | Add or Modify Screen

Configuration | Policy Management | Certificate Group Matching | Rules | Add

Create a new rule for certificate group matching from the fields below. A rule contains a group name and matching criteria that define the group. The VPN Concentrator checks the information in the certificate against these criteria; all the criteria must match the certificate to establish the group.

Note that the Value string must be enclosed in double quotes. These quotes are added automatically.

You can also create a rule by entering its text directly in the **Matching Criterion** box. If you create a rule in this way, separate the components with commas. Also, be sure to add double quotes around the value. If the value itself contains double quotes, replace them with two double quotes. For example, enter the value "Tech" Eng as: ""Tech"" Eng". An example of a matching criterion is: OU="Engineering",ISSUER-O="Cisco"

Enable Check to enable the rule.

Group --Base Group-- Select the group to which this rule applies.

Distinguished Name	Operator	Value
Subject CommonName (CN)	Equals (=)	

Matching Criterion

Add Cancel

79349

Enable

To allow the VPN Concentrator to use the rule you are adding or modifying, click **Enable**. To disable the rule, clear the Enable field. If the rule is disabled, it is marked with (D) in the Certificate Matching Rules box.

Group

Select the group to assign this rule to from the pull-down menu. You can assign this rule only to groups that are currently defined in the configuration. If the group you want to use is not in the list, you must first go to Configuration | User Management | Groups and define the group.

Distinguished Name Component

Select the type of distinguished name (Subject or Issuer) and the fields you want to use in the rule.

A distinguished name can contain a selection from the following fields:

Field	Content
-------	---------

Subject and Issuer consist of a specific-to-general identification hierarchy: CN, OU, O, L, SP, and C. These labels and acronyms conform to X.520 terminology.

Subject	The person or system that uses the certificate. For a CA root certificate, the Subject and Issuer are the same.
---------	---

Issuer	The CA or other entity (jurisdiction) that issued the certificate.
--------	--

Field	Content
-------	---------

Common Name (CN)	The name of a person, system, or other entity. This is the lowest (most specific) level in the identification hierarchy.
------------------	--

Surname (SN)	The family name or last name of the certificate owner.
--------------	--

Country (C)	The two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
-------------	---

Locality (L)	The city or town where the organization is located.
--------------	---

State/Province (S/P)	The state or province where the organization is located.
----------------------	--

Organization (O)	The name of the company, institution, agency, association, or other entity.
------------------	---

Organizational Unit (OU)	The subgroup within the organization.
--------------------------	---------------------------------------

Title (T)	The title of the certificate owner, such as Dr.
-----------	---

Name (N)	The name of the certificate owner.
----------	------------------------------------

Given Name (GN)	The first name of the certificate owner.
-----------------	--

Initials (I)	The first letters of each part of the certificate owner's name.
--------------	---

Email Address (EA)	The email address of the person, system or entity that owns the certificate
--------------------	---

Generational Qualifier (GENQ)	A generational qualifier such as Jr, Sr, or III.
-------------------------------	--

DN Qualifier (DNQ)	A specific DN attribute.
--------------------	--------------------------

Operator

Field	Content
Equals (=)	The distinguished name field must exactly match the value.
Not Equals (!=)	The distinguished name field must not match the value.
Contains (*)	The distinguished name field must contain the value within it.
Does Not Contain (!*)	The distinguished name field must not contain the value within it.

Value

The value to be matched against. The VPN Concentrator automatically places text values within double quotes. To enter values manually, follow the rules on the screen. Values are not case-sensitive.

Append

To enter the next part of a rule, click **Append**. When you click Append, the VPN Concentrator adds on the part you have defined to the rule that appears under Matching Criteria. In this way, you can build a complex rule testing on multiple components. The VPN Concentrator checks the information in the certificate against all parts of the rule. All parts must test true for the rule to match for this group.

Matching Criterion

The matching criterion text box displays the rule. You can create or edit the rule directly in this box. If you create a rule in this way, separate the components with commas. Also, be sure to add double quotes around the value. If the value itself contains double quotes, replace them with two double quotes. For example, enter the value *"Tech" Eng* as: `"\"Tech\" Eng"`.

Add/Cancel

After entering all parts of the rule for this group, click **Add** to complete the action or **Cancel** to cancel it.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | Policy Management | Certificate Group Matching | Rules screen, and the Rules list is unchanged.

Configuration | Policy Management | Certificate Group Matching | Policy

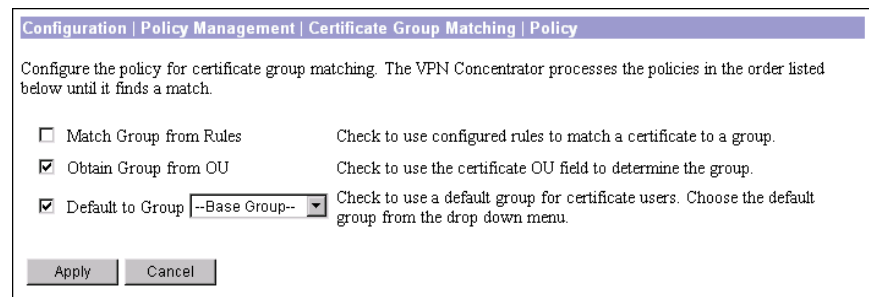
This screen lets you configure a policy for certificate group matching. The VPN Concentrator processes the enabled policies in the order listed until it finds a match.

There are three ways to match a certificate to a group:

- **Match Group from Rules:** Uses the rules you have defined to match a certificate to a group.
- **Obtain Group from OU:** Uses the organizational unit field to determine the group to which to match the certificate. (This was the standard policy in releases previous to 3.6.)
- **Default to Group:** Lets you select a default group for certificate users that is used when neither of the above methods resulted in a match.

By default, the first choice is not checked and the second and third choices are checked.

Figure 15-31 Configuration | Policy Management | Certificate Group Matching | Policy Screen



Match Group from Rules

To use the rules you have defined for certificate group matching, click to select **Match Group from Rules**.

Obtain Group from OU

To use the organizational unit in the certificate to specify the group to match, click to select **Obtain Group from OU**. This choice is enabled by default.

Default to Group

To use a default group or the Base Group for certificate users, click to select **Default to Group**. Then select the group from the drop down box. The group must already exist in the configuration. If the group does not appear in the list, you must define it by using the Configuration | User Management | Groups screen. This choice is enabled for the Base Group by default.

Apply/Cancel

After checking the policies you want to use for certificate group matching, click **Apply**. Or to cancel, click **Cancel**.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | Policy Management | Certificate Group Matching | Policy screen, and the Policy list is unchanged.



A

access hours, configuring [15-3](#)
 add [15-4](#)
 modify [15-4](#)

accounting record attributes, RADIUS [5-16](#)

accounting servers
 configuring [5-16](#)
 modify [5-18](#)

add
 access hours [15-4](#)
 address pool [6-6](#)
 email recipient of events [10-32](#)
 event class [10-17](#)
 filter (traffic management) [15-39](#)
 filter rule (traffic management) [15-15](#)
 IPSec LAN-to-LAN connection [7-14](#)
 NAT rule [15-54](#)
 network list [15-9](#)
 NTP host [5-29](#)
 OSPF area [8-12](#)
 security association (traffic management) [15-29](#)
 security association to rule on filter [15-45](#)
 SMTP server for events [10-29](#)
 SNMP community [9-13](#)
 SNMP event destination [10-22](#)
 static route for IP routing [8-5](#)
 syslog server to receive events [10-25](#)
 user on internal server (user management) [14-107](#)

address management, configuring [6-2](#)

address pools
 configuring [6-5](#)
 add [6-6](#)

 modify [6-6](#)

alarm thresholds, power, configuring [3-6](#)

Are You There (AYT) firewall policy [14-24, 14-28, 14-63, 14-67](#)

assignment of IP addresses, configuring [6-3](#)

assign rules to filter (traffic management) [15-42](#)

authentication parameters
 changing group delimiter [11-6](#)
 global [11-6](#)
 order of checking [14-2](#)

authentication servers
 configuring [5-2](#)
 internal [5-11](#)
 modify [5-5](#)
 NT Domain [5-7](#)
 RADIUS [5-5](#)
 SecurID [5-9, 14-88](#)
 internal [14-1](#)
 testing [5-13, 14-91](#)

autodiscovery, network [7-11, 7-20](#)

automatic software update, *See* client update [12-1](#)

automatic switchover (redundancy) [8-18](#)

B

bandwidth management
 bandwidth aggregation [15-65](#)
 bandwidth policing [15-64, 15-66](#)
 bandwidth reservation [15-64](#)
 burst size [15-66](#)
 configuring [15-66](#)
 enabling on interface [3-20, 15-63, 15-66](#)
 in LAN-to-LAN configuration [15-66, 15-67](#)

overview of [15-64](#)
 policing rate [15-66](#)
 policy
 assigning to group [14-103, 15-66](#)
 assigning to interface [3-21, 15-66](#)
 assigning to LAN-to-LAN [7-20, 15-66](#)
 specifying the link rate [3-20, 15-66](#)
 bandwidth policies
 configuring [15-63](#)
 banner for IPSec clients, configuring [14-17, 14-58](#)
 base group, configuring (user management) [14-4](#)
 base group global preshared secret [14-14](#)
 bibliography [xiii](#)
 browser
 installing SSL certificate [1-5](#)
 navigation toolbar, do not use with Manager [1-3](#)
 Netscape Navigator, problems with [1-3](#)
 requirements [1-2](#)
 built-in servers, configuring
 See management protocols [9-1](#)
 burst size [15-66](#)

C

Central Protection Policy (CPP) [14-24, 14-28, 14-63, 14-67, 15-15](#)
 certificate group matching [15-71](#)
 defining rules [15-71](#)
 fields [15-74](#)
 policy [15-77](#)
 configuring [15-71](#)
 rules
 adding [15-72, 15-74](#)
 assigning to groups [15-74](#)
 deleting [15-72](#)
 enabling [15-74](#)
 modifying [15-72, 15-74](#)
 reordering [15-72](#)
 change security association on rule [15-47](#)

Cisco Secure ACS RADIUS server [14-1](#)
 Cisco VPN Client
 IPSec attributes [7-9, 15-24](#)
 IPSec support [14-8, 14-50, 14-113](#)
 route advertisement [8-22](#)
 supports Mode Configuration [14-15, 14-56](#)
 client firewall [14-24, 14-63](#)
 and split tunneling [14-24, 14-63](#)
 Are You There (AYT) policy [14-24, 14-28, 14-63, 14-67](#)
 Central Protection Policy (CPP) [14-24, 14-28, 14-63, 14-67, 15-15](#)
 configuring rules for firewall filters [14-24, 14-63, 15-15, 15-17, 15-19, 15-22](#)
 custom [14-27, 14-66](#)
 local [14-24, 14-63](#)
 supported products [14-26, 14-65](#)
 vendor and product codes [14-27, 14-66](#)
 Zone Labs Integrity Server [14-24, 14-28, 14-63, 14-67](#)
 client update [12-1](#)
 enabling [12-3](#)
 image files [12-2](#)
 compression
 IPComp [14-14, 14-56](#)
 MPPC [14-37, 14-39, 14-76, 14-78](#)
 configuration section of Manager [2-1](#)
 connecting to VPN Concentrator
 using HTTP [1-4](#)
 using HTTPS [1-20](#)
 conventions
 documentation [xii](#)
 typographic [xii](#)
 copy
 filter (traffic management) [15-39](#)
 filter rule (traffic management) [15-15](#)
 IKE proposal [7-30](#)
 network list [15-9](#)
 crash, system, saves log file [10-8](#)

D

data
 formats [xv](#)

date and time, configuring [11-3](#)

Daylight-Saving Time, enabling [11-4](#)

default
 event handling, configuring [10-7](#)
 filter rules
 table [15-12](#)
 using [15-11](#)
 filters
 table [15-37](#)
 using [15-36](#)
 gateways, configuring for IP routing [8-7](#)
 IKE proposals, table [7-27](#)
 security associations, table [15-26, 15-27](#)
 tunnel gateway, configuring [8-7](#)

delete
 filter rule (traffic management) [15-23](#)
 group (user management) [14-42](#)
 internal authentication server [5-12](#)
 security association (traffic management) [15-35](#)
 user on internal server (user management) [14-106](#)

DHCP
 functions within the VPN Concentrator,
 configuring [8-14](#)
 servers, configuring [5-22](#)
 modify [5-24](#)

digital certificates
 in IPSec LAN-to-LAN [7-17](#)

display settings [1-3](#)

DNS
 configuring for group [14-49](#)
 servers, configuring [5-20](#)

documentation
 additional [xii](#)
 conventions [xii](#)

E

email recipients of events, configuring [10-30](#)
 add [10-32](#)

Ethernet interfaces
 See also interfaces

event classes
 configuring for special handling [10-15](#)
 add [10-17](#)
 modify [10-17](#)
 table [10-1](#)

event log [10-5](#)
 capacity [10-5](#)
 deleting from flash memory [10-7](#)
 file size [10-8](#)
 save [10-7](#)
 saved at system reboot [10-8](#)
 saved if system crashes [10-8](#)
 saving in flash memory [10-7](#)
 saving via FTP [10-8, 10-13](#)

events
 configuring default handling [10-7](#)
 configuring handling [10-6](#)
 configuring special handling [10-15](#)
 section of Manager [10-1](#)

event severity levels, table [10-4](#)

event trap destinations, configuring [10-20](#)

Extended Authentication, IPSec [14-13, 14-55](#)

F

filter [15-1](#)
 add (traffic management) [15-39](#)
 add security association to rule on [15-45](#)
 assign rules to (traffic management) [15-42](#)
 configuring (traffic management) [15-36](#)
 configuring on base group [14-7](#)
 configuring on group [14-48](#)
 configuring on interface

Ethernet [3-12](#)

configuring on user [14-112](#)

copy (traffic management) [15-39](#)

default

- table [15-37](#)
- using [15-36](#)

modify (traffic management) [15-39](#)

filter rules [15-1](#)

- add (traffic management) [15-15](#)
- configuring [15-11](#)
- copy (traffic management) [15-15](#)
- default

 - table [15-12](#)
 - using [15-11](#)

- delete (traffic management) [15-23](#)
- modify (traffic management) [15-15](#)

filters

- firewall [15-15](#)

firewall [14-24, 14-63](#)

firewall, client [14-63](#)

- See* client firewall [14-63](#)

firewall, client, *See* client firewall [14-24](#)

flash memory

- saving log files in [10-7](#)

formats

- data [xv](#)

fragmentation policy

- IPSec [3-13, 7-19](#)

FTP

- configuring internal server [9-2](#)
- using to save log files [10-8, 10-13](#)

G

gateways, default [8-7](#)

general parameters, configuring [11-1](#)

global authentication parameters [11-6](#)

groups, configuring, user management [14-41](#)

- delete [14-42](#)

- modify external [14-80](#)
- modify internal [14-43](#)

H

hold down routes

- adding to routing table [8-22](#)

HTTP

- configuring internal server [9-4](#)
- using with Manager [1-4](#)

HTTPS

- configuring internal server [9-4](#)
- connecting using [1-20](#)
- login screen [1-20](#)

I

IKE keepalives [14-12, 14-54](#)

IKE proposals

- active [7-28](#)
- add [7-30](#)
- configuring [7-26](#)

 - copy [7-30](#)
 - modify [7-30](#)

- copy [7-30](#)
- default, table [7-27](#)
- inactive [7-28](#)
- in IPSec LAN-to-LAN [7-18](#)
- in security association [15-24](#)
- modify [7-30](#)

IKE security association

- See* security associations

inheritance, of group and user parameters [1-3](#)

installing SSL certificate

- with Internet Explorer [1-6](#)
- with Netscape [1-13](#)

Install SSL Certificate (screen) [1-5](#)

interfaces

- configuring [3-2](#)
- Ethernet, configuring [3-9](#)
 - OSPF [3-17](#)
 - RIP [3-15](#)
 - speed [3-12](#)
 - transmission mode [3-12](#)
- filter
 - Ethernet [3-12](#)
- public [3-11, 7-13, 15-53](#)
- section of Manager [3-1](#)
- status [3-4](#)
- internal authentication server
 - configuring [5-11](#)
 - deleting [5-12](#)
 - maximum groups and users [14-1](#)
- Internet Explorer, requirements [1-2](#)
- IP addresses
 - configuring assignment of [6-3](#)
- IPComp data compression [14-14, 14-56](#)
- IP routing
 - configuring [8-2](#)
 - section of Manager [8-1](#)
- IPSec
 - banner for clients [14-17, 14-58](#)
 - Cisco VPN Client [7-9, 14-8, 14-50, 14-113, 15-24](#)
 - configuring [7-9](#)
 - base group [14-8, 14-9](#)
 - group (internal) [14-50, 14-51](#)
 - user (internal server) [14-113, 14-114](#)
 - data compression [14-14, 14-56](#)
 - discussion [7-9](#)
 - fragmentation policy [3-13, 7-19](#)
 - Mode Configuration [14-15, 14-56](#)
 - rules [15-6](#)
 - security associations
 - See* security associations
 - XAuth [14-13, 14-55](#)
- IPSec LAN-to-LAN
 - automatic parameters [7-15, 7-25, 15-18](#)

- configuring [7-11](#)
 - add connection [7-14](#)
 - no public interfaces screen [7-13](#)
 - parameters for redundant systems [8-18](#)
- Done (screen) [7-25](#)
- rules that apply IPSec [15-18](#)
- using network lists [7-16, 7-20, 7-23](#)
- IPSec NAT-T [7-19](#)
- IPSec over TCP [7-34](#)
- IPSec through NAT
 - configuring
 - base group [14-17](#)

J

- JavaScript, requirements [1-2](#)

K

- keepalives, *See* IKE keepalives [14-54](#)

L

L2TP

- configuring
 - base group [14-8, 14-35](#)
 - group (internal) [14-50, 14-74](#)
 - user (internal server) [14-113, 14-116](#)
- configuring system-wide parameters [7-6](#)
- data compression [14-39, 14-78](#)
- L2TP over IPSec
 - configuring
 - base group [14-8](#)
 - group (internal) [14-50](#)
 - user (internal server) [14-113](#)
 - default security association to use [14-10, 14-52, 14-115](#)
 - do not use Mode Configuration [14-15, 14-56](#)
 - IKE proposal required [7-28](#)

no IPSec user authentication [14-13, 14-55](#)
 Windows 2000 client support [7-1, 14-8, 14-50, 14-113](#)

LAN-to-LAN

See IPSec LAN-to-LAN

load balancing [13-1](#)

and VRRP [8-18, 13-1](#)

configuring [13-4](#)

cluster [13-5](#)

device [13-6](#)

preliminary steps [13-2](#)

device priority [13-6](#)

defaults [13-6](#)

virtual cluster [13-1](#)

virtual cluster master [13-1](#)

local LAN access for VPN client [14-21, 14-60](#)

log files

See event log

logging in the VPN Concentrator Manager [1-21](#)

login

name

factory default (Manager) [1-21](#)

password, factory default (Manager) [1-21](#)

screen [1-4](#)

HTTPS [1-20](#)

Internet Explorer [1-10](#)

Netscape [1-17](#)

address pool [6-6](#)

authentication server [5-5](#)

DHCP server [5-24](#)

event class [10-17](#)

filter (traffic management) [15-39](#)

filter rule (traffic management) [15-15](#)

group (external) (user management) [14-80](#)

group (internal) (user management) [14-43](#)

IKE proposal [7-30](#)

NAT rule [15-54](#)

network list [15-9](#)

NTP host [5-29](#)

OSPF area [8-12](#)

security association (traffic management) [15-29](#)

SMTP server for events [10-29](#)

SNMP community [9-13](#)

SNMP event trap destination [10-22](#)

static route, for IP routing [8-5](#)

syslog server to receive events [10-25](#)

user on internal server (user management) [14-107](#)

monitor / display settings [1-3](#)

movianVPN client support [7-18, 7-32, 14-10, 14-52, 14-115, 15-31, 15-34](#)

MPPC data compression [14-37, 14-39, 14-76, 14-78](#)

MTU [3-12](#)

M

management protocols, configuring [9-1](#)

Manager table of contents [1-23](#)

MIB-II

system object [11-2](#)

Mode Configuration, IPSec [14-15, 14-56](#)

and split tunneling [14-15, 14-56](#)

Cisco VPN Client supports [14-15, 14-56](#)

modify

access hours [15-4](#)

accounting server [5-18](#)

N

NAT

configuring [15-49](#)

enable [15-50](#)

no public interfaces screen [15-53](#)

NAT rules, configuring [15-51](#)

add [15-54](#)

modify [15-54](#)

NAT-T (NAT Traversal) [7-19, 7-35](#)

NAT transparency [7-34](#)

navigating

the VPN Concentrator Manager [1-23](#)

- Netscape Navigator
 - problems with [1-3](#)
 - requirements [1-2](#)
 - network autodiscovery [7-11, 7-20](#)
 - network lists [15-1](#)
 - configuring [15-7](#)
 - add [15-9](#)
 - automatic generation [15-10](#)
 - copy [15-9](#)
 - modify [15-9](#)
 - IPSec LAN-to-LAN [7-16, 7-20, 7-23](#)
 - network time, configuring
 - See* NTP [5-26](#)
 - No Public Interfaces screen
 - IPSec LAN-to-LAN [7-13](#)
 - NAT [15-53](#)
 - NT Domain, configuring authentication server [5-7](#)
 - NTP, configuring [5-26](#)
 - hosts (servers) [5-28](#)
 - add [5-29](#)
 - modify [5-29](#)
 - synchronization [5-27](#)
-
- O**
- organization of the VPN Concentrator Manager [1-22](#)
 - OSPF [3-1, 3-2](#)
 - configuring
 - on Ethernet interface [3-17](#)
 - system-wide parameters [8-9](#)
 - with reverse route injection [8-21](#)
 - OSPF areas, configuring [8-11](#)
 - add [8-12](#)
 - modify [8-12](#)
-
- P**
- password
 - factory default (Manager) [1-21](#)
 - policing rate [15-66](#)
 - policy management
 - configuring [15-2](#)
 - section of Manager [15-1](#)
 - power thresholds, configuring [3-6](#)
 - PPTP
 - configuring
 - base group [14-8, 14-35](#)
 - group (internal) [14-50, 14-74](#)
 - user (internal server) [14-113, 14-116](#)
 - configuring system-wide parameters [7-3](#)
 - data compression [14-37, 14-76](#)
 - pre-shared secret [14-14](#)
 - product codes for client firewalls [14-27, 14-66](#)
-
- R**
- RADIUS
 - accounting, configuring [5-16](#)
 - accounting record attributes [5-16](#)
 - Cisco Secure ACS RADIUS server [14-1](#)
 - Class attribute format to authenticate group name [14-41](#)
 - configuring, authentication server [5-5](#)
 - reboot system
 - saves log file [10-8](#)
 - redundancy
 - configuring, system [8-18](#)
 - references (bibliography) [xiii](#)
 - requirements
 - browser [1-2](#)
 - Internet Explorer [1-2](#)
 - JavaScript [1-2](#)
 - Netscape Navigator [1-2](#)
 - reverse route injection [7-20](#)
 - RIP [3-1, 3-2](#)
 - configuring on Ethernet interface [3-15](#)
 - with network autodiscovery [7-20](#)
 - with reverse route injection [8-21](#)

routes, adding to routing table
 network autodiscovery [7-20](#)
 reverse route injection [7-20](#)

RRI *See* reverse route injection

RSA Security [5-9, 14-88](#)

rules [15-1](#)

add security association to, on filter [15-45](#)

assign to filter (traffic management) [15-42](#)

change security association on [15-47](#)

filter, configuring [15-11](#)

rules, NAT, configuring [15-51](#)

add [15-54](#)

modify [15-54](#)

S

SAs *See* security associations

SAVELOG.TXT file [10-8](#)

screen

login [1-4](#)

login, using HTTPS [1-20](#)

SDI [5-9, 14-88](#)

SecurID [5-9, 14-88](#)

SecurID, configuring authentication server [5-9, 14-88](#)

security associations [15-1](#)

add to rule on filter [15-45](#)

change on rule [15-47](#)

configuring [15-24](#)

add [15-29](#)

delete [15-35](#)

modify [15-29](#)

default, table [15-26, 15-27](#)

IKE proposals in [15-24](#)

negotiation phases [15-24](#)

servers, configuring system access to [5-1](#)

sessions

maximum permitted [11-5](#)

changing [11-5](#)

SMTP servers, configuring for events [10-27](#)

add [10-29](#)

modify [10-29](#)

SNMP

configuring internal server [9-10](#)

event trap destinations, configuring [10-20](#)

add [10-22](#)

modify [10-22](#)

traps, configuring "well-known" [10-12](#)

SNMP communities, configuring [9-12](#)

add [9-13](#)

modify [9-13](#)

software update, automatic [12-1](#)

enabling [12-3](#)

image files [12-2](#)

speed, configuring Ethernet interface [3-12](#)

split tunneling [14-21, 14-60](#)

and firewalls [14-24, 14-63](#)

split tunneling, IPSec

requires Mode Configuration [14-15, 14-56](#)

split tunneling network list [14-22, 14-61](#)

SSH

configuring internal server [9-18](#)

host key [9-18](#)

server key [9-18](#)

server key regeneration [9-19](#)

session key [9-18](#)

SSL

client authentication [9-16](#)

configuring internal server [9-14](#)

SSL certificate [9-14](#)

installing in browser [1-5](#)

installing with Internet Explorer [1-6](#)

installing with Netscape [1-13](#)

viewing with Internet Explorer [1-11](#)

viewing with Netscape [1-18](#)

VPN Concentrator [1-5](#)

static routes, configuring for IP routing [8-3](#)

add [8-5](#)

modify [8-5](#)

strip realm [14-8](#)
 switchover, automatic (redundancy) [8-18](#)
 syslog servers, configuring for events [10-24](#)
 add [10-25](#)
 modify [10-25](#)
 system configuration section of Manager [4-1](#)
 system identification, configuring [11-2](#)

T

table of contents, Manager [1-23](#)
 Telnet
 configuring internal server [9-8](#)
 Telnet over SSL
 configuring internal server [9-8](#)
 shareware client [9-8](#)
 TFTP
 and automatic software update [12-1](#)
 configuring internal server [9-6](#)
 The [8-21](#)
 time and date, configuring [11-3](#)
 time zone, configuring [11-3](#)
 traffic management, configuring [15-6](#)
 transmission mode, configuring Ethernet interface [3-12](#)
 traps, configuring
 "well-known" [10-12](#)
 destination systems [10-20, 10-22](#)
 general events [10-12](#)
 specific events [10-19](#)
 troubleshooting
 consult event log [10-5](#)
 tunnel default gateway, configuring [8-7](#)
 tunneling protocols
 configuring [7-2](#)
 section of Manager [7-1](#)
 typographic conventions [xii](#)

U

user attributes, default
 See base group [14-4](#)
 user management
 configuring [14-3](#)
 section of Manager [14-1](#)
 users, configuring on internal server (user management) [14-105](#)
 add [14-107](#)
 delete [14-106](#)
 modify [14-107](#)

V

vendor codes for client firewalls [14-27, 14-66](#)
 viewing SSL certificates
 with Internet Explorer [1-11](#)
 with Netscape [1-18](#)
 virtual cluster [13-1](#)
 configuration [13-5](#)
 IP address [13-1](#)
 master [13-1](#)
 VPN 3002 Hardware Client
 route advertisement [8-22](#)
 software update [12-1](#)
 VPN Concentrator Manager
 logging in [1-21](#)
 navigating [1-23](#)
 organization of [1-22](#)
 sidebar (figure) [1-23](#)
 VRRP
 configuring [8-18](#)

W

welcome text for IPSec clients, configuring [14-17, 14-58](#)
 wildcard masks [7-21, 7-24, 15-10, 15-19](#)
 Windows 2000 client

and Mode Configuration [14-15](#), [14-56](#)
configure transport mode [15-31](#)
L2TP over IPSec support [7-1](#), [14-8](#), [14-50](#), [14-113](#)
PPTP support [14-8](#), [14-50](#), [14-113](#)
WINS, configuring for group [14-49](#)
wireless support *See* movianVPN client support [7-32](#)

X

XAuth [14-13](#), [14-55](#)
XML
 configuring as system management protocol [9-20](#)

Z

Zone Labs Integrity Server [14-24](#), [14-28](#), [14-63](#), [14-67](#)