SecureConnect Manager User's Guide

Ascend Communications, Inc.
Part Number: 7820-0369-001
For software version 3.0
September 10, 1998

Ascend Customer Service

Ascend Customer Service provides a variety of options for obtaining technical assistance, information about Ascend products and services, and software upgrades.

Finding information and software on the Internet

Visit Ascend's Web site at `http://www.ascend.com` for technical information, product information, and descriptions of available services.

Visit Ascend's FTP site at `ftp.ascend.com` for software upgrades, release notes, and addenda to this manual.

Obtaining Technical Assistance

You can obtain technical assistance by telephone, email, fax, or modem, as well as over the Internet.

Enabling Ascend to assist you

If you need to contact Ascend for help with a problem, make sure that you have the following information when you call or that you include it in your correspondence:

- Product name and model.
- Software and hardware options.
- Software version.
- If supplied by your carrier, Service Profile Identifiers (SPIDs) associated with your line.
- Your local telephone company's switch type and operating mode, such as AT&T 5ESS Custom or Northern Telecom National ISDN-1.
- Whether you are routing or bridging with your Ascend product.
- Type of computer you are using.
- Description of the problem.

Calling Ascend from within the United States

In the U.S., you can take advantage of Priority Technical Assistance or an Ascend Advantage Pak service contract, or you can call to request assistance.

Priority Technical Assistance

If you need to talk to an engineer right away, call (900) 555-ASND (2763) to reach Ascend's Priority Call queue. The charge of $2.95 per minute does not begin to accrue until you are connected to an engineer. Average wait times are less than three minutes.

Ascend Advantage Pak

Ascend Advantage Pak is a one-year service contract that includes overnight advance replacement of failed products, technical support, software maintenance releases, and software update releases. For more information, call (800) ASCEND-4 (272-3634), or access Ascend's Web site at `www.ascend.com` and select Services and Support, then Advantage Service Family.

Other telephone numbers

For a menu of Ascend's services, call (800) ASCEND-4 (272-3634). Or call (510) 769-6001 for an operator.

Contacting Ascend from outside the United States

You can contact Ascend by telephone from outside the United States at one of the following numbers:

Telephone outside the United States	(510) 769-8027
Austria/Germany/Switzerland	(+33) 492 96 5672
Benelux	(+33) 492 96 5674
France	(+33) 492 96 5673
Italy	(+33) 492 96 5676
Japan	(+81) 3 5325 7397

Middle East/Africa	(+33) 492 96 5679
Scandinavia	(+33) 492 96 5677
Spain/Portugal	(+33) 492 96 5675
UK	(+33) 492 96 5671

Note: For a list of support options in the Asia Pacific Region, refer to http://apac.ascend.com

Obtaining assistance through correspondence

Ascend maintains two email addresses for technical support questions. One is for customers in the United States, and the other is for customers in Europe, the Middle East, and Asia. If you prefer to correspond by fax, BBS, or regular mail, please direct your inquiry to Ascend's U.S. offices. Following are the ways in which you can reach Ascend Customer Service:

- Email from within the U.S.—support@ascend.com
- Email from Europe, the Middle East, or Asia—EMEAsupport@ascend.com
- Fax—(510) 814-2312
- Customer Support BBS (by modem)—(510) 814-2302

Write to Ascend at the following address:

Attn: Customer Service
Ascend Communications, Inc.
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502-3002

About This Guide

This guide explains Ascend SecureConnect Manager software. You can use SecureConnect Manager to create SecureConnect firewalls for Ascend Pipeline routers and personal computers running Ascend's IntragyAccess software. A SecureConnect firewall is a dynamic security feature that monitors and controls incoming and outgoing Internet Protocol (IP) traffic. When you create a SecureConnect firewall you can also configure Virtual Private Network (VPN) tunnels over which you can securely transmit and receive authenticated and encrypted data.

This guide also contains information about IntragyAccess software's SecureConnect Client (SCC) feature, Ascend Firewall Control Manager software, and the Ascend Firewall Control Protocol.

The IntragyAccess SecureConnect Client (SCC) feature is a software module that enables a SecureConnect firewall installed on your PC's remote-access interfaces to control what enters and leaves your PC. The software includes the SecureConnect Transport protocol and SecureConnect Adapters for each of your remote-access interfaces. The SCC feature can also encrypt and decrypt packets that you transmit and receive over the interfaces, creating a Virtual Private Network tunnel between your machine and the party with whom you are connected.

Firewall Control Manager (FCM) is a Web server CGI script that is a RADIUS client and SNMP management station. FCM receives user information from a RADIUS server, creates Firewall Control Protocol (FCP) packets that contain the user information, and sends the FCP packets to routers running SecureConnect firewalls. A router that receives FCP packets temporarily changes the behavior of its Ascend SecureConnect firewall on the basis of information in the FCP packets.

Firewall Control Protocol (FCP) is the means by which Firewall Control Manager creates packets containing user authorizations that FCM can send to Ascend routers with SecureConnect firewalls. Third party security products, such as virus scanners, can also incorporate the Firewall Control Protocol and send SecureConnect routers information that changes the behavior of their firewalls.

How to use this guide

Your understanding of firewalls and your experience creating firewalls determine the order in which you should you should read the chapters in this guide. Start with Chapter 4, “Creating a SecureConnect firewall,” if you never used Ascend’s Secure Access Manager software to create firewalls. The chapter includes a short overview of packet filtering and firewalls. Then read Chapter 1, “Introducing SCM, SCF and SCC.” That chapter contains instructions for installing SCM, enabling SecureConnect firewall on an Ascend unit, and installing SecureConnect Client of a PC. Finally, read Chapter 3, “Exploring the SCM Interface.”

If you created Secure Access firewalls with Ascend’s Secure Access Manager program, the SecureConnect Manager interface will seem familiar. However, you should read Chapter 1, “Introducing SCM, SCF and SCC,” before you attempt to create a SecureConnect firewall. SecureConnect Manager enables you to create firewalls that do much more than control access to an Ascend router and this chapter explains new firewall components, such as Main firewall rulesets, section rulesets, and tunnel rulesets. Then read Chapter 3, “Exploring the SCM Interface.”

If you want to create firewalls that enable users to communicate via secure, encrypted tunnels the information you need is in Chapter 5, “Tunneling with IPSec.”

Ascend Pipelines can change the behavior of their firewalls on the basis of user authentication. If you want particular users, or classes of users, to be permitted access to services that are blocked by your router’s main firewall, read Chapter 6, “Section Rulesets, FCP, and FCM.”

Following is a chapter-by-chapter description of the topics in this guide.

Chapter 1, “Introducing SCM, SCF and SCC,” introduces SecureConnect Manager (SCM) and briefly describes the components of SecureConnect firewalls: rulesets, Main firewall, firewall sections and firewall tunnels. This section of the guide also discusses firewall enablers called SecureConnect firewall (SAF) and SecureConnect Client (SCC).

Chapter 2, “Overview of packets and packet filtering,” includes a brief description of Internet Protocol (IP) packets and their components, such as source and destination addresses. The chapter also provides background information about types of filters and compares static and dynamic packet filtering.

Chapter 3, “Exploring the SCM Interface,” explains the SecureConnect Manager shell, screens and dialog boxes you use to configure firewall components’ rulesets and tunnel settings. The explanations describe the functions of the shell’s menu and SCM’s dialog text boxes, check boxes, and buttons. The descriptions include sample entries and selections for creating firewall component rules and tunnel settings.

Chapter 4, “Creating a SecureConnect firewall,” includes a brief description of IP packets and IP packet filtering. It explains how a SecureConnect firewall monitors information in the packets so it can compare them specifications in rules that determine whether or not the firewall should pass or block the packets. The chapter also explains how to use SecureConnect Manager to create the rules that define packets. The chapter concludes with explanations of two sample firewalls.

Chapter 5, “Tunneling with IPSec,” describes the Internet Protocol Security Protocol (IPSec), the basic construction of IP packets, the effect of IPSec encapsulation on IP packets, and the encryption algorithms you can use to perform packet encapsulation.

Chapter 6, “Section Rulesets, FCP, and FCM,” covers firewall section rulesets, which enable specially-authenticated individuals to access locations and services from which the firewall blocks most users. The chapter also describes the Firewall Control Protocol, the Firewall Control Manager program (FCM), and the SecureConnect Server, which includes FCM, Ascend Access Control RADIUS server (AAC), Access Control Manager (ACM), and Client Firewall Loader (CFL).

Appendix A, “Appendix: Ruleset categories,” is an alphabetized list of the services in the SecureConnect Manager Category box. You select these services to create firewall and tunnel rules. Each entry in the list includes a brief description of the service.

Appendix B, “Appendix: IPSec debug commands,” explains router debug commands and system messages related to IPSec.

Appendix C, “Appendix: RADIUS,” is a brief introduction to Remote Dial In User Service (RADIUS) authentication servers. It includes examples of user profile and `clients` file entries.

Note: The SecureConnect Manager User’s Guide includes information about RADIUS because the book explains how Ascend’s Firewall Control Protocol can change firewall behavior based on information that the Firewall Control Manager obtains from RADIUS user profiles. You cannot use RADIUS user profiles to authenticate users who dial in to a Pipeline unit, or to store authorization information about the types of connections you permit the users to establish. You can use RADIUS user profiles to authenticate and authorize users who dial in to MAX routers to request a connection. MAX routers support the SecureConnect firewall security feature, but do not support encrypted Virtual Private Network tunnels.

What you should know

Following are some topics that you should understand. They are germaine to the main topics of the SecureConnect Manager User Guide, but are not discussed at length in the guide. The information under the headings “Related publications” and “WWW search topics” list resources you can consult for more information about these topics.

- Internet Engineering Task Force Requests for Comments (IETF RFCs)
- Internet Protocols, such as TCP/IP, UDP, and SNMP
- Packets
- Routing packets
- LANs and WANs
- The Internet

- Leased lines
- Router and PC interfaces
- Static filter firewalls
- Encryption, algorithms, and keys

Documentation conventions

Ascend uses standard documentation conventions. The introductory section of each manual includes a section that describes the conventions, which are as follows:

Convention	Meaning
`Monospace text`	Represents text that appears on your computer's screen, or that could appear on your computer's screen.
`Boldface mono-space text`	Represents characters that you enter exactly as shown (unless the characters are also in ***`italics`***—see *Italics*, below). If you could enter the characters but are not specifically instructed to, they do not appear in boldface.
Italics	Represent variable information. Do not enter the words themselves in the command. Enter the information they represent. In ordinary text, italics are used for titles of publications, for some terms that would otherwise be in quotation marks, and to show emphasis.
[ ]	Square brackets indicate an optional argument you might add to a command. To include such an argument, type only the information inside the brackets. Do not type the brackets unless they appear in bold type.
|	Separates command choices that are mutually exclusive.
>	Points to the next level in the path to a parameter or menu item. The item that follows the angle bracket is one of the options that appears when you select the item that precedes the angle bracket.
Key1-Key2	Represents a combination keystroke. To enter a combination keystroke, press the first key and hold it down while you press one or more other keys. Release all the keys at the same time. (For example, Ctrl-H means hold down the Control key and press the H key.)
Press Enter	Means press the Enter, or Return, key or its equivalent on your computer.

Convention	Meaning
Note:	Introduces important additional information.
 **Caution:**	Warns that a failure to follow the recommended procedure could result in loss of data or damage to equipment.
 **Warning:**	Warns that a failure to take appropriate safety precautions could result in physical injury.

Related publications

The following RFCs and Ascend manuals contain information you might find helpful. The RFCs referred to are Internet Engineering Task Force (IETF) Requests for Comments.

RFC 791, "*Internet Protocol*," September 1981.

RFC 1157, "*Simple Network Management Protocol (SNMP)*," May 1990.

RFC 1321, "*The MD5 Message-Digest Algorithm*," April 1992.

RFC 1810, "*Report on MD5 Performance*," June 1995.

RFC 1825, "*Security Architecture for the Internet Protocol*," August 1995.

RFC 1826, "*IP Authentication Header*," August 1995.

RFC 1827, "*IP Encapsulating Security Payload (ESP)*," August 1995.

RFC 1851, "*The ESP Triple DES-CBC Transform*," October 1995.

RFC 1852, "*IP Authentication using Keyed SHA*," October 1995.

RFC 1883, "*Internet Protocol, Version 6 (IPv6) Specification*," December 1995.

RFC 2058, "*Remote Authentication Dial-In User Service (RADIUS)*," January 1997.

RFC 2085, "*HMAC-MD5 IP Authentication with Replay Prevention*," February 1997.

RFC2104, "*HMAC: Keyed-Hashing for Message Authentication*," February 1997.

Ascend Pipeline user guides

WWW search topics

Following are World Wide Web search topics that might enable you to find helpful information on the Web about subjects mentioned in this guide. The guide does not contain many Web site URLs because they frequently change, disappear, or are abandoned.

- Algorithm
- Authentication
- Authentication Header
- DES
- Encapsulating Security Payload
- Encryption
- Encryption key
- Firewall
- Hash code
- IPSec
- MD5
- RADIUS
- RFC
- Security Association
- SHA-1
- SNMP
- Tunnel
- Virtual Private Network

Figures

Tables

Introducing SCM, SCF and SCC

1

This chapter introduces SecureConnect Manager (SCM) and briefly describes the components of SecureConnect firewalls: rulesets, Main firewall, firewall sections and firewall tunnels. This section of the guide also discusses SecureConnect Firewall (SCF), the Ascend Pipeline router feature that enables you to install firewalls on the routers, and SecureConnect Client (SCC) the Ascend IntragyAccess software feature that enables you to install firewalls on PCs. The chapter concludes with instructions for installing SCM and enabling the Pipeline firewall feature. The chapter consists of the following sections:

Introduction

SecureConnect Manager (SCM) is a program with which you can create firewalls for routers and personal computers (PCs).

SCM-created firewalls contain rules that describe the kinds of traffic that can enter or leave a machine's network interfaces. Some of the firewall rules you can create with SCM can also describe the kinds of IP packets a machine can transmit or receive through an encrypted Virtual Private Network (VPN) tunnel. Traffic that is transmitted through an encrypted VPN tunnel is secure. It cannot be read if it is intercepted and the sender can be authenticated by the receiver.

When you use SCM to create firewall rules that define VPN tunnel traffic, you must also create a VPN tunnel configuration. The tunnel configuration specifies the means by which a machine encrypts plain traffic for transmission and how the machine decrypts encrypted traffic it receives. You can use SCM to save VPN tunnel configurations and firewall rules in firewall files that SCM can load on SecureConnect-enabled routers and PCs running Ascend's IntragyAccess software.

Note: The term Virtual Private Network refers to the use of the Internet Protocol Security (IPSec) protocol to create encapsulated, encrypted packets. Note that in other publications the phrase Virtual Private Network might describe another method of encapsulating one packet format inside another format. Encapsulating one format inside another hides information as it is being distributed. For example, you can hide information you want to send from one location to another if you put a letter inside an envelope, then place the envelope in a box. There are many ways to encapsulate a packet created by one protocol, such as TCP, inside the format of another protocol, such as IPSec. For example, an Ascend unit's user guide might describes how to use Ascend Tunnel Management Protocol (ATMP) to create a VPN.

This chapter includes overviews of SCM, the SecureConnect Firewall (SCF) router feature and the IntragyAccess SecureConnect Client feature. You must enable SCF on a router or install IntragyAccess on a PC if you intend to load SCM firewalls on either machine. The chapter also includes installation instructions for SCM and SecureConnect Client and instructions for enabling the SCF feature on a router.

What is SecureConnect Manager?

SecureConnect Manager (SCM) is a program for creating SecureConnect firewalls. SecureConnect firewalls control network access at the network on which you install them. A firewall monitors Internet Protocol (IP) packets arriving at the interface where the firewall is installed and compares the packets to well-defined descriptions of acceptable and non acceptable packets. SecureConnect firewalls are dynamic because their rules contain language that is activated, or triggered by information in the IP packets the firewall monitors. The dynamic, temporary changes the packets trigger can provide more security than the static rules in traditional packet filtering.

You can install SCM on a PC running the Windows 95 or Windows NT operating system. SCM's shell enables you to call up screens with which you can create the three components that you can include in a SecureConnect firewall: the Main firewall, a firewall section, and a tunnel.

SecureConnect firewall rulesets

Each firewall component contains a ruleset, or group of rules, that is derived from the SecureConnect template of firewall rules. Each of the template's rules defines a particular kind of traffic by its type of service, or protocol, its destination, and its source. By default, the template's rules do not permit the defined traffic to pass the firewall. Since firewalls are most effective when they stringently control access, most rules in a given ruleset are copies of the template's rules. They block the traffic they describe from entering or leaving a machine's network interface. The firewall rules you create for the Main firewall, a firewall's sections, and tunnel rulesets are edited template rules. Usually you change the template rules to permit specific traffic to pass the firewall.

Figure 1-1 shows the SCM shell. Inside the shell is the screen with which you configure the rules for the Main firewall.

Figure 1-1. SCM shell including Main firewall Ruleset Configuration screen

Main firewall

The Main firewall is composed of rules that determine what the firewall does with packets that are not defined by rules in the firewall's sections and tunnels. You might think of the Main firewall as the general purpose firewall that controls the traffic ordinary users send to a machine's interface.

A network gateway router's Main firewall ruleset might permit the network's internal users to send most kinds of traffic out of the network, but block external users from sending traffic to any network sites except public File Transfer Protocol (FTP) and World Wide Web (WWW) servers. To construct such a Main firewall ruleset, you would change many of the template rules' default outgoing

settings and retain the default incoming settings for all but the FTP and WWW rules.

Firewall sections

Sections are groups of special rules that contain null data where Main firewall and tunnel rules might contain such things as a remote user's IP address. A router supplies the missing data and activates the sections when it receives Firewall Control Protocol (FCP) packets from an FCP agent such as the Firewall Control Manager (FCM). For discussion of FCP packets and FCM see Chapter 6, "Section Rulesets, FCP, and FCM."

SecureConnect Manager's firewall sections feature enables you to create rules that permit specific, authenticated users to access services that are blocked by rules in the Main firewall ruleset. For example, a router's Main firewall ruleset might block access to two servers that contain private marketing and engineering databases. You can create section rulesets called MKT and ENG that contain rules which permit the members of the marketing and engineering departments to access the departmental servers.

The router can activate the section rulesets' rules if the Firewall Control Manager sends the router some Firewall Control Packets that contain information which completes the rules. The FCM can create the FCP packets if the Remote Authentication of Dial-up User Service (RADIUS) server which authenticates marketing and engineering group users finds the section ruleset information in their user authentication profiles and sends it to the FCM.

After the router uses the authentication profile information to complete the section's rules, the authenticated members of the marketing and engineering will be able to access their database servers. Members of each group will also be able to access everything permitted by the Main firewall, but neither group will be able to access the other's database.

You cannot create section rulesets for firewalls that will be loaded on PCs running IntragyAccess. The software that understands the Firewall Control Protocol is part of the Ascend router code, but it is not integrated into IntragyAccess.

Firewall tunnels

Note: Ascend Pipeline routers support Internet Protocol Security (IPSec), the encryption protocol used to create Virtual Private Network tunnels. Ascend MAX units do not support IPSec. Although you can install firewalls on an Ascend MAX units, these routers will not encrypt or decrypt packets. Do not include tunnel configurations in firewalls you create for MAX units.

A firewall tunnel requires a ruleset and sets of Transmit and Receive encryption settings called Security Associations. The tunnel ruleset defines the kinds of traffic a SecureConnect firewall encrypts and decrypts when transmitting and receiving information. The Transmit and Receive encryption settings determine how the traffic is encrypted and decrypted.

The encryption algorithms you can select when you configure a tunnel are specified in the IPSec standard. The standard's approved encryption transforms include MD5, SHA-1, HMAC-MD5, HMAC-SHA, Data Encryption Standard (DES) and Triple DES (3DES). IPSec, algorithms, and other components of Security Associations are explained in Chapter 5, "Tunneling with IPSec.".

The length of the key that you use with an encryption algorithm determines the strength of the encryption a Pipeline router performs. Pipeline routers support 40-bit keys for the DES algorithm. You can obtain a software upgrade that permits you to use 56-bit keys and the Triple DES algorithm, however the availability of the upgrade is subject to United States Commerce Department restrictions. Chapter 3, "Exploring the SCM Interface," and Chapter 5, "Tunneling with IPSec," contain more information about IPSec encryption algorithms and export restrictions.

Tunnel endpoint configuration

You cannot create a tunnel by configuring a ruleset and encryption settings on one router's firewall or one PC's firewall. Firewalls at each end of the tunnel must contain a firewall tunnel ruleset and encryption setting configuration. Very often each end's tunnel ruleset will contain a rule that identifies the other end as a Trusted Site. In such cases everything that the two ends send to each other is encrypted.

The firewall tunnel rulesets of a tunnel's two endpoints do not have to match, but the tunnel endpoints must coordinate their encryption settings. For example, a tunnel between endpoints A and B might be configured as follows:

- The tunnel ruleset in the firewall on the PC at tunnel endpoint A permits the transmission of Trivial File Transfer (TFTP) traffic to endpoint B.
- The tunnel ruleset in the firewall on the router at endpoint B does not permit transmission of TFTP traffic to endpoint A, but it does allow a form of email traffic to be transmitted to endpoint A.
- Endpoint A's tunnel Transmit encryption settings match endpoint B's tunnel Receive encryption settings and vice versa.

Endpoint A's outgoing TFTP traffic and endpoint B's outgoing email traffic arrive at their destinations in encrypted form. The router's SecureConnect Firewall feature and the PC's SecureConnect Client feature encrypt traffic if their tunnel rulesets permit the traffic to be transmitted through the tunnel. Endpoints A and B cannot transmit the same kinds of traffic over the tunnel, but each can successfully decrypt the other's transmission.

Note: Each endpoint's Main firewall ruleset controls transmissions not defined in the tunnel ruleset. In the example, endpoint B *can* transmit TFTP traffic to endpoint A if B's Main firewall ruleset permits outgoing TFTP traffic to A. Endpoint B simply will not encrypt the outgoing TFTP traffic.

Restrictions on the number of tunnels in firewalls

You can create as many tunnel configurations in a firewall as can be stored in a router's NVRAM memory. Practically, you might be able to configure one hundred tunnel configurations in a Pipeline unit's firewall. The number of tunnels you can configure for a firewall on a PC running IntragyAcess should be unlimited. PC users, however, are not likely to require more than a handful of tunnel configurations.

What is SecureConnect Firewall?

SecureConnect Firewall is a security feature of the TAOS operating system on most Ascend Pipeline and MAX routers. The SCF feature is integrated within the

operating system and you can install firewalls on your router if the feature is enabled. SCF is not available on MAX TNT routers.

Ascend Pipeline routers that support the SecureConnect Firewall feature include the Pipeline 50, 75, 85, 130 and 220 models. The SCF feature is enabled on these Pipeline routers when they are shipped. You do not have to enter a feature code to enable the feature before you install firewalls on Pipeline routers.

The SecureConnect Firewall feature is not enabled on MAX units when they are shipped so you must enter a feature code to enable SCF on MAX routers. You can obtain the SCF feature code from the Ascend Technical Assistance Center. Your TAC representative will give you a feature code that is based on your router's serial number. For instructions, see "Enabling SecureConnect Firewall" on page 1-11.

Note: The Pipeline models that support the SecureConnect Firewall feature also automatically support encrypted VPN tunnels because the ability to perform IPSec encryption is integrated within the Pipeline TAOS operating system code.

IPSec encryption is not supported in MAX TAOS code. When you enable the SecureConnect Firewall feature on a MAX unit you can install a firewall on the router, but the unit will not be able to encrypt and decrypt packets.

What is the IntragyAccess SecureConnect Client feature?

SecureConnect Client (SCC) is a feature of IntragyAccess that enables you to install SecureConnect firewalls on a PC. Firewalls installed with SCC control the traffic that enters and leaves all of the PC's remote access interfaces.

IntragyAccess is cross-platform desktop client software that provides integrated support for flexible desktop communications. When you enable the SCC feature, IntragyAccess installs the SecureConnect Transport protocol and a SecureConnect Adapter for each of the PC's remote access interfaces. The adapters intercept a PC's incoming and outgoing packets so they can be compared with descriptions of packets in a firewall's rules. When an intercepted packet matches the description of a packet in a firewall rule, the rule's instructions determine how the PC handles the packet.

If the firewall you install on the PC includes a tunnel configuration and associated tunnel ruleset, SCC can also encrypt and decrypt packets transmitted and received over the interfaces, creating a Virtual Private Network tunnel between the PC and the machine with which it is connected. The PC user can employ a dial up or ethernet connection to communicate with another site over an encrypted VPN if the firewall at the other end of the connection contains the complement of the tunnel configuration in the PC's user's firewall.

When you enable the IntragyAccess SecureConnect Client feature you also install a simple console interface that enables you to install firewalls, disconnect SCC Adapters, and view logs about the packets that pass through the PC's interfaces.

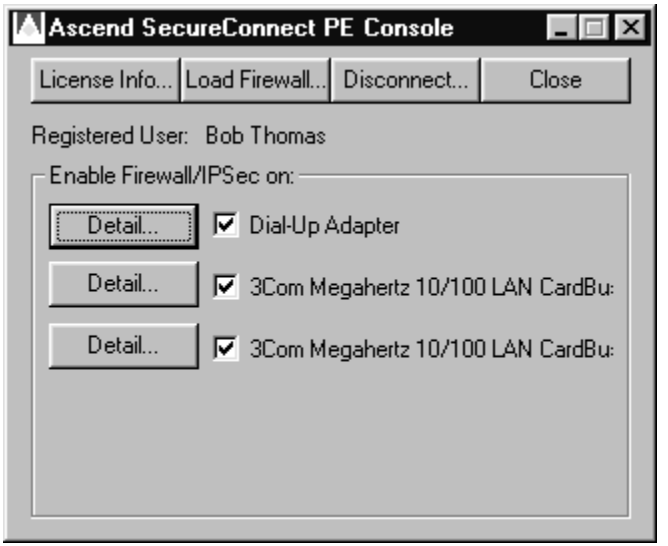


Figure 1-2. IntragyAccess SCC console

The SecureConnect Client console is not an interface for creating firewalls. You can only use SecureConnect Manager (SCM) to create SecureConnect firewalls. PC users can install SCM and create their own firewalls or they can obtain firewalls from a firewall administrator. Chapter 6, "Section Rulesets, FCP, and FCM,"contains information about methods that firewall administrators can use to

distribute firewall files to remote PC users who have installed IntragyAccess and enabled the SCC feature.

Installing SecureConnect Manager

In addition to being distributed on its own SecureConnect Manager diskettes, the SCM software is included on many of the CD-ROMs delivered with other Ascend products, including Pipeline and MAX routers. The SCM program is always packaged in a file named `scm.exe` that is a self-installing executable. This is true if you receive SCM on diskettes or on a CD-ROM.

SCM system requirements

Following are the system requirements for installing SecureConnect Manager:

- Windows 95 or Windows NT operating system
- 2 MB of hard-drive space
- 8 MB of RAM

Note: SCM is a 32-bit Windows application. Do not attempt to install SCM on Windows 3.x machines.

Installation Procedure

By default the setup program installs SecureConnect Manager in C:\ASCEND\SCM and creates an Ascend program group. To install and run SCM:

1. Click the Windows Start button and select Run.
2. Enter ***`D:\SCM\setup.exe`*** where ***`D`*** is the CD-ROM drive, or browse to find the file **`setup.exe`**.
3. Select Start > Programs > Ascend.
4. Double-click SecureConnect Manager.

Enabling SecureConnect Firewall

The Secure Access Firewall feature was added to Ascend router code in release 4.6. The SecureConnect Firewall feature, which is the first firewall feature that supports IPSec and encrypted Virtual Private Network tunnels, entered the Ascend router code in release 6.1.11. If your version of the router code follows 4.6, but precedes 6.1.11, you need to enter a code to turn on the router's firewall feature. If your version of the router code does not support SecureConnect Firewall and you want to create encrypted VPNs you must purchase the software upgrade discussed in "Firewall tunnels" on page 1-6.

Caution: Do not execute your unit's NVRAM Clear command unless you execute the FSAVE command immediately prior to clearing the unit's NVRAM memory. Your SecureConnect router's SecureConnect Firewall and IPSec encryption features are turned on when you receive the unit. NVRAM Clear erases the code that activates the SCF and IPSec features. Using FSAVE makes sure that the code is retained in the unit's flash memory. If you want to copy the code that activates the features, it is in your router's System > Feature Codes > IPSec menu.

Contact Ascend Customer Service to obtain a firewall feature code or to purchase the software upgrade for IPSec encryption. Customer Service contact information is in "What you should know."

To access your router's debug mode so that you can enter a code that enables the SecureConnect Firewall feature:

1. Rapidly enter the following two key combinations in sequence:
   `Esc[`
   `Esc=`
2. Press **`Ctrl-D`** then press **`D`** again.

If you purchase the encryption software upgrade, follow the instructions in your router documentation that explain how to load new router code, or download the latest router release notes from the Ascend web site:

http://www.ascend.com

Installing SecureConnect Client

To install IntragyAccess and enable the SecureConnect Client feature put the IntragyAccess CD-ROM in the PC's CD-ROM drive, then follow these instructions.

1 Select Start > Run.

2 Enter the letter assigned to your CD ROM drive.

3 Browse to find `securepe.exe`.

4 Click OK.

or

1 Open the Windows Explorer.

2 Find `securepe.exe` on the CD ROM drive.

3 Double click `securepe.exe`.

Complete the following steps after the splash screen of the SecureConnect Client installation program appears.

1 Click Finish to begin InstallShield.

2 Click Next.

3 Read the Ascend End User Agreement.

4 Click Yes.

5 Click Start > Control Panel > Network when installation of SecureConnect Client is complete.

The dialog's list of installed network components should contain SecurePE Adapter and SecurePE Transport.

6 Click Yes to restart your computer.

Overview of packets and packet filtering

2

This chapter includes a brief description of IP packets and IP packet filtering. It explains how a Secureconnect firewall monitors information in the packets and compares the information to specifications in rules. The results of the comparison determine whether the firewall permits the packets to flow through the router, or whether the firewall blocks the packets.

Packets

IP network hosts bundle their data into packets which are passed either between two hosts, or between a host and a router. The router forwards the packets towards another router or to their final destination host. Each packet transmitted during a session must be identifiable so that it can be delivered to the correct destination and compiled with the rest of the session's packets.

Many different types of IP packets can arrive at a gateway router's interface for distribution to other routers or hosts. Some may be from an outgoing Telnet session, for example, while others may be incoming packets from a remote World Wide Web server. Telnet and WWW are examples of standard IP protocols that have been defined by an international group called the Internet Engineering Task Force (IETF). The IETF develops and publishes standards for protocols so that each end of a data connection understands how to use them to transmit and receive data. There are many IP protocols and you can find information about them at the following WWW site:

`http://www.ds.internic.net/rfc/`

A packet's source, destination and protocol are included in packet components called headers that are attached to the packets as they pass through different layers of the TCP/IP (Transmission Control Protocol /Internet Protocol) stack. Each layer adds a header containing information about how its counterpart at the other end of the connection should handle the packet. Information that is important to the packet filtering process is included in these headers.

Table 2-1. Packet headers

Header Information	Description
IP source and destination addresses	The IP addresses assigned to individual machine's interfaces. Typically rendered in dotted quad format, such as 137.105.22.2
IP Protocol type	TCP, UDP or ICMP, for example.

Table 2-1. Packet headers (continued)

Header Information	Description
TCP source and destination ports	A two byte number associated with client and server processes, such as 21 for ftp and 23 for telnet
TCP flags	• SYN identifies the first packet in a TCP session. • ACK identifies all session packets other than the initial packet. • RST, the TCP RESET header bit • FIN, the close connection header bit

Chapter 5, “Tunneling with IPSec,” contains more information about packets and their construction.

Packet filtering

You can apply filters for packets in many ways. Some packet filters are software applications you install on network servers. Others, such as SecureConnect firewall, are integrated into operating systems on the router units that pass packets within a network or between networks. Most packet filters pass or deny packets based on packet header information. SecureConnect firewalls are one of the few implementations that also look into the packet’s data to determine what should be done with the packets.

Packet filters are groups of rules. The rules contain specific information that describes packets. The information in the rules might specify packet destination and source locations, protocols and port numbers that the filter or firewall searches for to determine whether packets should be passed or blocked. If a packet that arrives at a filter does not match the specifications in one of the filter’s rules, the filter discards the packet. If the packet does match a filter rule, the filter handles the packet according to the rule’s instructions.

For example, suppose one of a filter's rules says that no outgoing packets should be passed if they are destined for a remote World Wide Web server at IP address 175.119.32.5. The filter scrutinizes each outgoing pack it receives and discards all outgoing WWW protocol packets destined for the prohibited WWW server.

Static filters

Static packet filters are carefully arranged stacks of rules that determine what data is blocked or passed. The rules remain fixed, or static, after they are installed. The rules do not adapt to the traffic the filter receives, but they do monitor the traffic and control it like a sentry at a guard post. Static packet filtering is a standard security feature of Ascend routers. Consult the chapter of your Ascend unit's user guide on security filters for more information about the Data Filters and Call Filters you can create for Connection Profiles and Answer Profiles.

SecureConnect dynamic filtering

SecureConnect Firewall is a dynamic filter feature in Ascend units that you can use in place of, or in conjunction with, the units' standard static filtering. SecureConnect Firewall's packet filtering is different than static packet filtering because it is flexible, self-adjusting and temporal, meaning SecureConnect Firewalls control not only what passes in and out of your network, but when it can pass, and for how long it can pass.

SecureConnect Firewall uses templates of rules that contain the same types of specifications that static rules refer to when monitoring packets. But SecureConnect technology can also edit rules on the fly in response to IP packet traffic, incorporating values that TCP/IP protocols add to packets' headers into the rules. Static filters can only create holes and leave them open for any packets that match their rules. The rules in SecureConnect's template do not open permanent holes in the filter that was designed to provide security.

When a firewall finds that a packet matches a rule's specifications it opens a session for the rest of the packets that are being transmitted. Then the firewall incorporates information from the first packet into the rule so it becomes a trigger the firewall uses to recognize other packets in the session. The session's final

packet carries an identifying value that matches the trigger added to the rule. When SecureConnect sees the information that matches the rule's trigger it shuts the opening the firewall created for the session and drops the trigger information from the rule. In effect, the trigger information the firewall temporarily adds to a template rule enables the firewall to monitor the status of session and control how long it will keep open the hole it has created to provide access.

SecureConnect Firewall templates are configured by choices you select in SCM, the SecureConnect Manager. Using SecureConnect Manager you can create dynamic firewall rules based on IP options, packet direction, protocol, service, routing, destination, source, and TCP SYN, ACK, RST and FIN bits. One edited template can include specifications for over thirty standard protocols, service and applications. You can also build rules based on custom protocols you define.

Where to find more information about SecureConnect firewall rules

Chapter 3, "Exploring the SCM Interface," explains the SecureConnect Manager interface. Other parts of that chapter describe how you use the SCM interface to create firewall template rules. Chapter 6, "Section Rulesets, FCP, and FCM," contains information about creating special dormant firewall template rulesets called sections that users can activate when they have been authenticated by a RADIUS authentication server.

Exploring the SCM Interface

3

This chapter explains the SecureConnect Manager shell, screens, and dialog boxes you use to configure firewall components' rulesets and tunnel settings. The explanations describe the functions of the shell's menu and of SCM's dialog text boxes, check boxes, and buttons. The descriptions include sample entries and selections for creating firewall component rules and tunnel settings. The chapter consists of the following sections:

Starting SCM and displaying the shell

To start SCM, click the Windows Start button, select Programs > Ascend, and double-click SecureConnect Manager. The New Firewall dialog box (Figure 3-1) appears the first time you start SecureConnect Manager, or whenever you select File > New from the SEcureConnect Manager menu. Otherwise SecureConnect Manager automatically opens the last firewall file that you created and the New Firewall dialog box does not appear.

The box contains two radio buttons. One is labeled SecureConnect Personal Edition or SecureConnect Client, and the other is labeled Ascend Router w/SecureConnect. Select the button that describes the machine on which you will install the firewall you create in the current SCM session. Your selection determines the options that appear in the Target and Send dialog boxes described in “File > Exit command” on page 3-6.

Figure 3-1. New Firewall dialog

Initial shell display

The screen in Figure 3-2 is the SCM program’s shell as it appears after you select a destination for your first new firewall. In the figure, SCM has automatically opened a new firewall file. A blank ruleset configuration screen for configuring the new firewall’s Main firewall ruleset appears below the menu/icon bar. The shell’s menus and icons provide access to all the screens and dialog boxes you can use to configure a firewall’s Main firewall, section, and tunnel components. The shell can display multiple configuration screens simultaneously.

When you close SCM, the program retains information about the last firewall you configured. The next time you start SCM, the program opens that firewall's file and the shell displays the ruleset configuration screen you used to configure that firewall. You can select the File > New menu or click the New button on SCM's taskbar to close the file's ruleset configuration screen and open a new one.

Shell menu and taskbar

The SCM shell displays six menus when a firewall file is open and five menus when all firewall files are closed. Figure 3-2 shows all six menus. The FCP menu, which you select to create firewall sections, does not appear if you close all firewall files. Below the menu, six buttons provide shortcuts to commands in the File, Target, and Help menus.

The remaining sections of this chapter describe all the menu selections and their functions

Figure 3-2. The SCM shell when you first open SCM

File

Use the File menu to create, open, and save files, and to exit the SecureConnect Manager program. SCM can only open Fwall Source files, although it can save firewall configurations as compiled firewall profiles that it can load on Ascend routers and IntragyAccess SecureConnect Client PCs. You can read the extensions of the files in the \SCM directory to determine which files the program can open. Names of Fwall Source files have an extension of `.fw`, such as `Austin.fw`. Fwall Profiles and TNT Profiles that SCM cannot open have an extension of `.prf`, such as `Delia.prf`.

File > New command

Select File > New or click the first icon on the SCM shell taskbar to open a blank Main (Ruleset) screen in the SCM shell and close all open configuration screens. A prompt reminds you to save the current firewall if you have changed it.

Before displaying a new Main (Ruleset) screen, SCM displays the New Firewall dialog box so that you can specify the whether the new firewall is to be for a PC with SecureConnect Client or an Ascend Router with SecureConnect Firewall.

File > Open command

Select File > Open or click the second icon on the SCM shell taskbar to open an existing Fwall Source file. The command displays a dialog box from which you can select the drive, directory, and filename of the Fwall Source file you want to open. When you have selected the file to open, the shell displays the Main (Ruleset) screen, which shows the Main firewall and section configurations. If the selected firewall includes a tunnel configuration, the shell also displays a Tunnel/Ruleset Association screen containing tunnel settings.

When you select File > Open, SCM displays a prompt to remind you to save the current firewall if you have changed it.

File > Save command

Select File > Save or click the third icon on the SCM shell taskbar to save the ruleset, section and tunnel configuration of the open firewall as a Fwall Source file, Fwall Profile, or TNT Profile. The default is to save the file in the Fwall Source format (*`filename`*`.fw`). The first time you save a new firewall configuration, File > Save opens a dialog box from which you can enter a filename and select the file type, drive, and directory for the firewall you are saving. If you subsequently want to change the file's name, format, or location, you must use the File > Save As command.

File > Save As command

Select File > Save As to save the ruleset, section, and tunnel configuration of a previously saved firewall when you want to change the firewall's name or format of the saved firewall, or the location in which you save the firewall.

File > Exit command

Select File > Exit to shut down the SecureConnect Manager program.

Caution: File > Exit immediately closes SCM without prompting you to save unsaved firewall configurations.

Target menu

Select the Target menu to specify the router or PC for which you have designed the firewall, or to load the firewall on a machine you have specified. Use the menu's Option command to specify a machine and use the Send command to load a firewall.

The Target menu also includes four router-specific commands. The Get Config and Restore Config commands ensure that you can recreate all of a router's administration and connection settings after you load a firewall. The Load New Software and Reset Router commands makes it easy to load code which contains new SecureConnect Firewall feature updates.

Target > Options command

Select Target > Options to specify the router on which SCM will load the firewall you are currently configuring, or to name the firewall if SCM will load it on a SecureConnect Client personal computer. The information you enter in the dialog box that SCM opens when you select Target > Options is part of the firewall's configuration and is retained in a Fwall Source file if you save the completed firewall in that format.

The dialog box that SCM displays when you select Target > Options depends on the type of machine you selected in the New Firewall dialog box (Figure 3-1). If

you selected an Ascend Router, SCM opens the Target Machine Information dialog box (Figure 3-3). If the machine you selected was a PC with SecureConnect Client, SCM opens the SecurePE Target Information dialog box (Figure 3-4). Both dialog boxes contain option check boxes called “Auto Save to Disk”, “Debug Log in sam.log”, and “Save Full FW Source in .fw”. The options are described in Table 3-1 which explains the Target Machine Information dialog box selections and entries.

Note: To automatically save a firewall in a FWall Source file when you install the firewall you must select the Save Full FW Source in .fw option on the Target > Option or Target > Send dialog. SCM does not automatically create a Fwall Source file unless this option is turned on before you click the Target > Send dialog’s Install button.

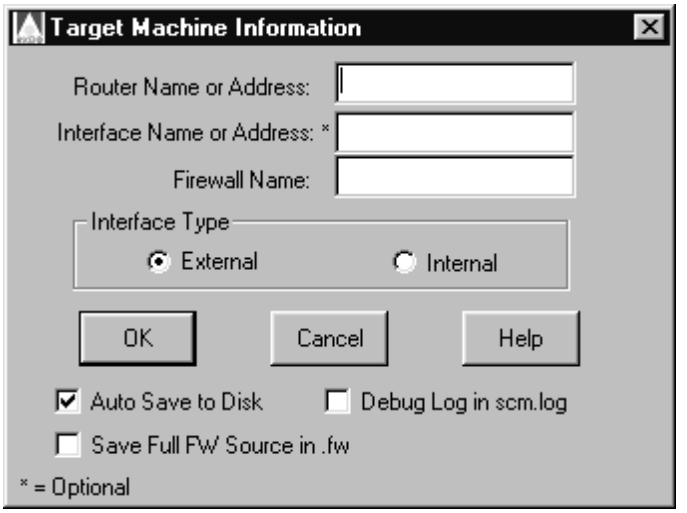


Figure 3-3. Target Machine Information dialog box

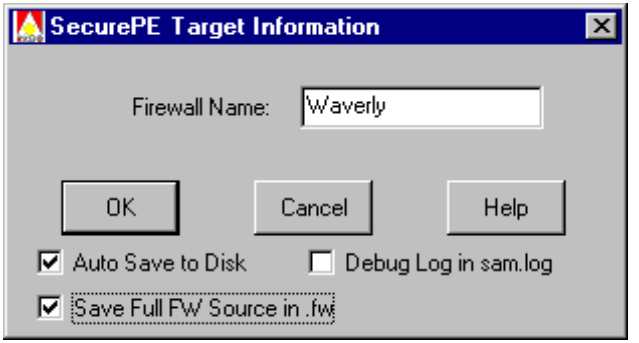


Figure 3-4. Target > Option display for SCC firewall

External and Internal interface option

The version of the Target > Option dialog box that appears when you create a firewall for an Ascend router contains External and Internal interface radio buttons. The External and Internal interface options do not cause SecureConnect Manager to install a firewall on a particular router interface. You select the router interface on which SCM installs a firewall when you enter the router's name or an interface address in the text boxes above the radio buttons.

The External and Internal options determine the direction (Incoming or Outgoing) and location of machines (Local and Remote) in the rules that you create in the firewall's Main ruleset. The default option is External. The External option is the correct selection for most of the firewalls you create because, usually, you will configure the Main firewall rules for a firewall on the interface that connects the router to the outside world (Figure 3-5). In this configuration the router and its firewall are between your private network and the rest of the world.

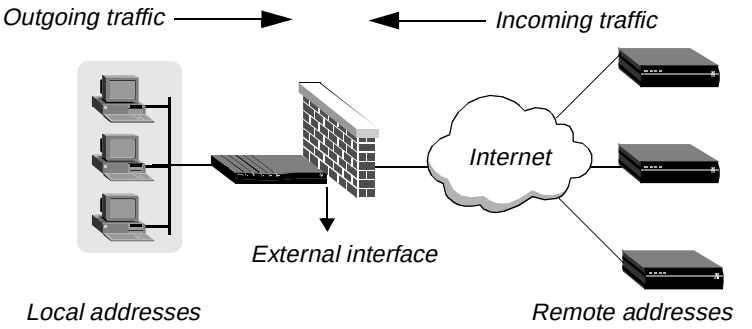


Figure 3-5. Typical firewall placement on a router's external interface

However, you might create a firewall for the router interface that connects the router to the private network (Figure 3-6). If you configure the rules so that the addresses of the private network are local and the packets that the private network sends to the router are outgoing, then the actions of the firewall might be the reverse of what you intend. Notice that the firewall is between the private network and the router and that the packets the router receives from the private network come into the router through the firewall. The packets do not go through the router before they are intercepted by the firewall. Therefore, in relation to the firewall, the private network is remote. The router and everything but the private network are local. Also, in relation to the firewall, the private network's packets are incoming and packets that pass through the router interface that does not have a firewall are outgoing.

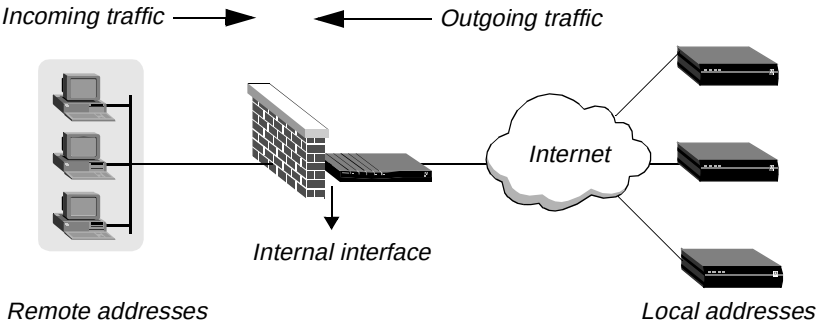


Figure 3-6. Firewall placement on a router's internal interface

In this situation, if you mistakenly specify that the private network is local and direction of its packets is outgoing, you can select the Internal interface option before you send the firewall to the router. The SecureConnect Firewall feature on the router will correct your error so you do not have to reconfigure all the rules in the firewall's Main ruleset.

Note: The Fwall source file is not affected if you select Internal to correct the configuration of a firewall's rules. The entries in the rules' location text boxes and the rules' direction selections remain the same in the file. To determine if firewall's creator selected the Internal option before sending a firewall to a router, use a text editor to open the firewall's Fwall Source file and look for the following line in the file:

IfType=1

Table 3-1 explains the Target Machine Information dialog box selections and entries.

Table 3-1. Target Machine Information dialog entries

Selection	Usage
Router Name/Address	Specifies the router's name or IP address. ("Export file values" on page 3-27 contains important information about how SCM handles this entry when you export tunnel configurations.)
Interface Name or Address	Optional entry for specifying name or address of router interface if it is different from the router's name or address.
Firewall Name	Specifies the firewall's name.
Interface Type	Specifies whether the firewall will be installed on a router's Internal or External interface. Generally, a router's Ethernet interface is Internal and its WAN interface is External. Opposite is true if another network router is the network's access to the Internet.

Table 3-1. Target Machine Information dialog entries (continued)

Selection	Usage
Enable IPSec	Specifies whether the router accepts and decrypts encrypted IP packets to determine whether the packets should pass the firewall. Automatically selected if the firewall includes a tunnel configuration.
Auto Save to Disk	Specifies that the firewall's configuration is automatically saved in a local Firewall Source file when you send (load) the firewall.
Debug Log in sam.log	Specifies that link establishment information for an attempt to load the firewall is recorded in a file called `sam.log`. Only necessary if SCM experiences difficulties during link establishment.
Save Full FW Source in .fw	Specifies that SCM saves a firewall language source file when you save or send a firewall.

Target > Send command

Select Target > Send to send a firewall configuration to an Ascend Router or a SecureConnect Client machine. The firewall's destination determines which of two dialog boxes appears when you select Target > Send. The dialog boxes are labeled Send Firewall to Router and Install Firewall on Local Machine. Aside from their names, these dialog boxes are the same as the Target > Options dialog boxes labeled Target Machine Information and SecurePE Target Information. The Target > Send dialog boxes contain the information you entered in the Target > Options dialog boxes.

If you create a firewall for a router and select Target > Send, SecureConnect Manager creates a firewall profile and automatically sends it to the router specified in the dialog box. If you change the information in the Target > Send dialog box so that its entries are different from the entries in the Target > Option dialog box, SecureConnect Manager uses the Target > Send information to

determine where it should load the firewall. This can be useful if you want to send a firewall to a different machine than the one for which you created the firewall.

If you create a firewall for a PC and select Target > Send, then SCM creates a firewall profile and saves it on the machine running SCM, giving the firewall the name that appears in the Install Firewall on Local Machine dialog box.

Note: You cannot use SecureConnect Manager to send a firewall directly to a SecureConnect Client PC. You can only load the firewall onto the machine that is running SecureConnect Manager. You must use another method to distribute to the PC the compiled firewall file that SCM creates when you click OK in the Install Firewall on Local Machine dialog box.

Editing Ethernet interface firewalls

When you want to edit a firewall installed on a router's Ethernet interface you must remove the firewall from the interface, edit the firewall, and reset the firewall on the interface. If you do not remove the firewall from the interface the router will not pick up the edits. Following is the procedure for removing, editing and resetting an Ethernet interface firewall on the router. (You do not need to follow this procedure if the firewall is on the router's WAN interface.)

1 Telnet to the router.

2 Select the Ethernet > Connections menu.

3 Select the connection, then select Session Options.

4 Select Data Filter and set the value to 0 (zero).

5 Save the configuration.

6 Edit the firewall and send it from SCM to the router, assigning the firewall a number on the router.

7 Open the Connection > Ethernet menu.

8 Set the Data Filter to the number assigned to the firewall you edited.

9 Save the Connection > Ethernet menu configuration.

Setting Filter Persistence when you assign a firewall to a router's WAN

interface

Set the Filter Persistence parameter in a Pipeline unit's Connection profile to Yes when you assign a SecureConnect firewall to the unit's WAN interface. The security of SecureConnect firewalls is based on their ability to monitor the states of connections so that the firewalls can dynamically open and close. Yet a firewall must remain up for period of time when a connection closes unexpectedly, in case a user did not intentionally end the session and desires to re-establish it. For example, if an FTP session drops the connection in midsession, a firewall that remains up can prevent the user from losing valuable data.

The Filter Persistence parameter enables the firewall to remain in place for the length of time specified by the firewall's Keepalive timeout setting.

The Filter Persistence parameter is located in the router's Ethernet > Connections > *profile*> Session Options menu. Your router's documentation includes instructions for setting the Filter Persistence parameter.

Target > Get Config command

Select Target > Get Config to automatically copy the configuration of the router specified in the Target Machine Information dialog box. The command causes the PC running SecureConnect Manager to contact the router and obtain the router's configuration settings. The Get Config from dialog box also appears when you select the command. Use the dialog box to specify where you want to save the configuration that SCM obtains from the router. The location of the file can be the SCM PC or another machine with which the PC can communicate.

Target > Restore Config command

Select Target > Restore Config to automatically load a router configuration on the router specified in the Target Machine Information dialog box. The file containing the router configuration can be located on the SecureConnect Manager PC or another machine. Use the Restore Config to dialog box to inform SCM of the file's location.

Target > Load New Software command

Select Target > Load New Software to automatically install router code on the router specified in the Target Machine Information dialog box. The file containing the router software can be located on the SecureConnect Manager PC or another machine. Use the Load New Software on dialog box to inform SCM of the location of the file that contains the software.

To obtain a new version of router code for a Pipeline or MAX unit, contact the Ascend Web site or the Ascend FTP server and download the code you need. If you contact the Web site, follow the Service and Support and software library links to find the heading labeled Current Releases and Incremental Binaries. Then select the release for your router. The Ascend Web site is at

`http://www.ascend.com`

To obtain a software release from the Ascend FTP server, FTP to

`ftp.ascend.com/pub/Software-Releases`

Target > Reset Router command

Select Target > Rest Router after you load new software on the router specified in the Target Machine Information dialog box. The reset command that SecureConnect Manager automatically sends the router causes the router to start running the new version of the TAOS operating system that you loaded.

VPN menu

Select the VPN menu to perform actions that affect the firewall's Virtual Private Network tunnels. You can:

- Configure firewall tunnels' encryption algorithms and keys.
- Create tunnel rulesets.
- Associate tunnel rulesets with tunnel configurations.
- Automatically create randomly generated encryption keys for your firewall's tunnels.

- Create export files, based on your tunnel configurations and rulesets, that the remote ends of the tunnels can easily incorporate into their firewalls.
- Create a default tunnel configuration on which SecureConnect Manager automatically bases all new tunnels.
- Enhance security by regularly changing tunnel settings using the VPN menu Randomize All Keys and Export All Tunnels commands. You can use also use these commands to re-establish security if you suspect that someone has obtained a firewall's tunnel's encryption keys.

VPN > VPN Configuration command

To create and configure tunnels for your firewall, select the VPN > VPN Configuration command, which displays the VPN Configuration dialog box (Figure 3-7). After you create the tunnels and their rulesets, you associate tunnel configurations with rulesets. Associating a tunnel and a ruleset links the tunnel with the rules that specify how the firewall handles incoming tunneled traffic and the outgoing traffic that should be encrypted for transmission over the tunnel.

You can also use the VPN Configuration dialog box to create Main rulesets of firewalls you want to export to the remote ends of your firewall's tunnels. This function enables you to configure a complete firewall for each end of a tunnel. ("Main R.S." on page 3-18 and "VPN > Export All Tunnels command" on page 3-25 explain Remote Main rulesets and the export of remote firewalls.)

The VPN Configuration dialog box is also accessible through SecureConnect Manager's Windows menu.

The VPN Configuration dialog box contains three lists named, respectively, Tunnel Names/Associated Rulesets, Local Tunnel Rulesets, and Remote Main Rulesets. Below each of the lists are buttons you can use to add or delete entries, edit the configurations of the lists' tunnels and ruleset rules, and associate entries from the Local and Remote ruleset lists with entries in the Tunnel list

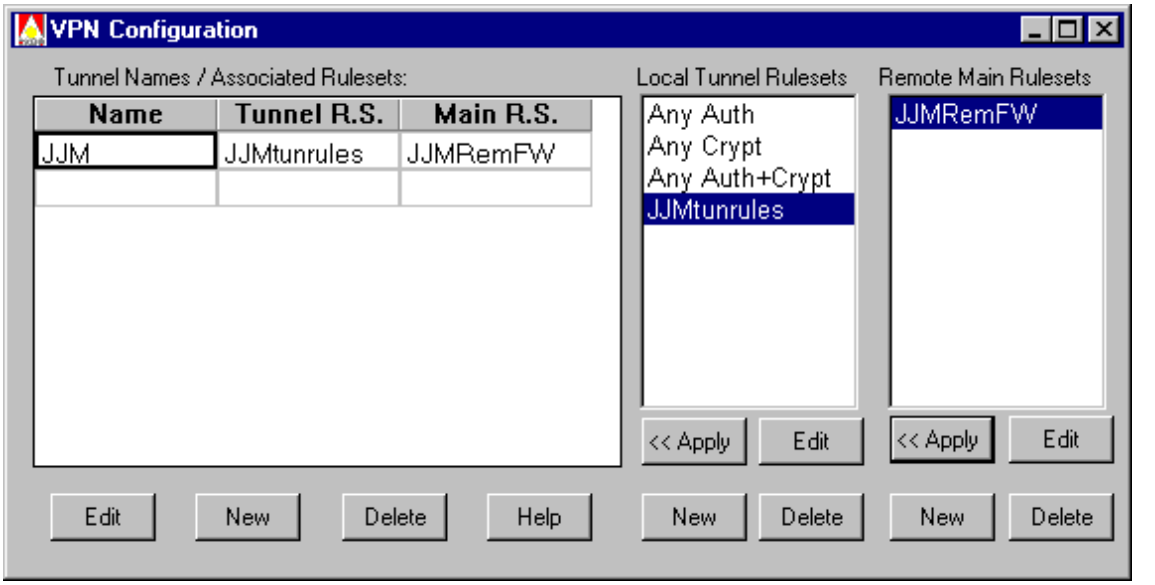


Figure 3-7. VPN Configuration dialog box

Tunnel Names/Associated Rulesets

The Tunnel Names/Associated Rulesets section of the VPN Configuration dialog box is a table in which Name, Tunnel R.S., and Main R.S are the columns. The rows in the table are the means by which you associate tunnels and rulesets. The last row in the table is always blank. You can create an additional blank row if you click the New button below the table, choose not to enter a tunnel name in the dialog box that appears (Tunnel Configuration — Figure 3-8), then close the dialog box.

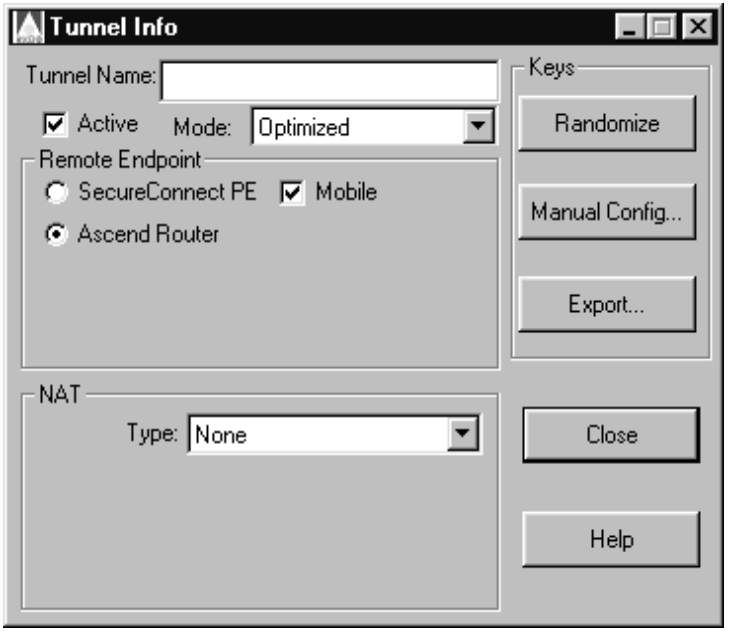


Figure 3-8. The Tunnel Info dialog box

Name

Each entry in the Name column is the name of one of the firewall's tunnels. You cannot enter or edit a tunnel name by selecting a cell in the Name column and typing an entry. To create a tunnel's name, and its configuration, select the New button beneath the table. When the Tunnel Info dialog box appears, enter a name in the Tunnel Name text box. When you close the dialog box the name appears in a new cell in the Name column, and the settings that appeared in the Tunnel Info dialog box become the settings for the new tunnel.

The Tunnel Info dialog box settings are based on defaults you configure in the Default Settings of New Tunnels dialog box shown in Figure 3-15. You can override the default settings by selecting the Tunnel Info dialog box Manual Config button. (For information about the choices you can select for tunnel defaults, see "VPN > Tunnel Defaults command" on page 3-30.

Tunnel R.S.

Entries in the Tunnel R.S. column of the Tunnel Names/Associated Rulesets table are the names of tunnel rulesets. Each tunnel ruleset in the column is associated with the tunnel that appears in the same row of the table. The tunnel ruleset associated with a tunnel contains the rules that specify the traffic that can pass through the tunnel. The Local Tunnel Ruleset table on the VPN Configuration dialog box contains the names of all the rulesets that you can associate with the firewall's tunnel configurations. (Table 3-2 explains the means by which you can associate a tunnel and a ruleset.)

Each tunnel in the firewall must be associated with a tunnel ruleset. Usually, you will create a tunnel ruleset, specify what its rules are, and manually associate the ruleset with one or more tunnels. However, if you create rules in any of three default tunnel rulesets, SecureConnect Manager automatically associates all the tunnels in the firewall with those rulesets.The default rulesets in the Local Tunnel Rulesets list are named Any Auth, Any Crypt and Any Auth+Crypt and the rules you create in these rulesets only apply to incoming encrypted packets. These rulesets are described in "Default Tunnel rulesets for incoming encrypted traffic" on page 3-24.

Main R.S.

Entries in the Main R.S. column of the table are the names of Main firewall rulesets that you, as a firewall administrator, might create for the remote ends of the firewall's tunnels. The rules in remote Main firewall rulesets control the untunneled traffic at the remote ends of your firewall's local tunnels. You might create remote Main firewall rulesets to ensure that the firewall rules at those locations provide adequate security for users who are not familiar with the SecureConnect Manager program.

If you create remote Main rulesets you must associate them with the local firewall's tunnels so that SecureConnect Manager can include the rulesets in the file that it creates when you use the program's export function. The SCM export function automatically creates files that contain the tunnel configuration, tunnel ruleset and, if available, the remote Main ruleset for the users at the other ends of the firewall's tunnels. You can distribute the files to the users so they can install them on their routers or PCs. "VPN > Export All Tunnels command" on page 3-25 contains more information about exporting tunnels and rulesets for remote sites.

If you create remote Main rulesets, you must use care when entering locations in the rulesets' rules. Remember that you are configuring the rules that control the untunneled traffic on someone else's router or PC, so the local and remote locations might be the reverse of the way you are inclined to perceive them. For example, if the remote end of a tunnel for which you are creating a Main firewall ruleset is a PC running SecureConnect Client, and the network behind your router contains all the machines that you want the PC to access, you must enter the PC's address in the rules' Local Servers location text boxes and your network's addresses in their Remote Clients location text boxes.

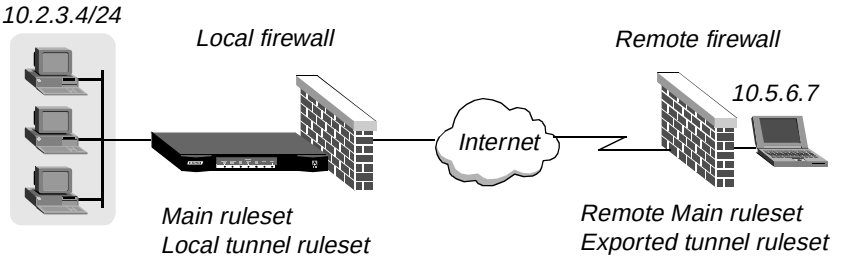


Figure 3-9. SCM export function creating remote firewall components

Using the IP addresses in Figure 3-9, you would enter the addresses as shown in Figure 3-10 to create a rule in a remote Main ruleset that enables POP Mail traffic from the 10.2.3.4/24 network to the laptop at 10.5.6.7.

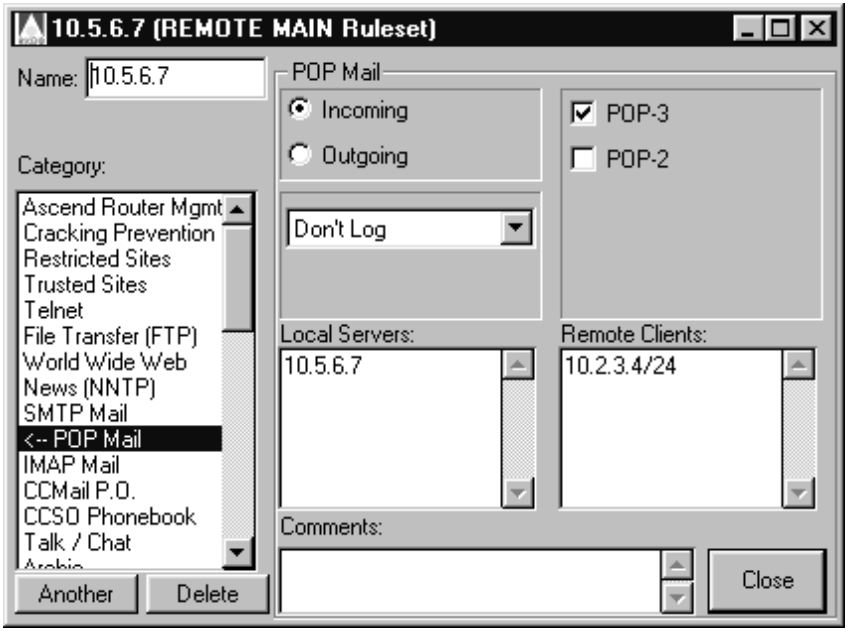


Figure 3-10. Configuring a rule in a remote Main ruleset

Tunnel and ruleset editing features

The buttons below the VPN Configuration dialog box lists (Figure 3-7) enable you to edit the lists' entries and to edit tunnel and ruleset configurations. Table 3-2 lists the ways you can use the VPN Configuration dialog to create, edit and associate tunnels and rulesets.

Table 3-2. Using VPN Configuration dialog box to create, edit, and associate tunnels and rulesets

To get this result:	perform these actions
Insert a new tunnel based on default tunnel settings	**1** Select a cell in the Name column above which you want to insert a tunnel name. **2** Click New under the list of tunnels, or press Enter to open the Tunnel Info dialog box. **3** Enter a name in the Tunnel Name text box. **4** Click Close or select the close icon  . SCM inserts a new row in the Tunnel Names/Associated Rulesets list. The tunnel name appears in the Name column.
Insert a new tunnel and override tunnel default settings	**1** Select a cell in the Name column above which you want to insert a tunnel name. **2** Click New under the list of tunnels, or press Enter to open the Tunnel Info dialog box. **3** Enter a name in the Tunnel Name text box. **4** Click Manual Config... **5** Change the default values in the Tunnel Manual Key Configuration dialog box. Click Randomize Keys if you want to automatically change the tunnel encryption keys. **6** Click OK. **7** Click the Tunnel Info dialog box Close button or select the close icon.

Table 3-2. Using VPN Configuration dialog box to create, edit, and associate tunnels and rulesets (continued)

To get this result:	perform these actions
Insert a copy of an existing tunnel	**1** Click on a tunnel name in the Name column. **2** Hit Enter to open the Tunnel Info dialog box. **3** Enter a name for the new tunnel. **4** Click Close or select the close icon  . The name of the copied tunnel appears below the original tunnel in the Name column. The rulesets associated with the copy and the original tunnel are the same, but the tunnels' keys for encrypting traffic are different.
Delete a tunnel	**1** Click on a tunnel name in the Name column. **2** Click Delete below the Tunnel Names/Associated Ruleset list. You cannot use the keyboard Delete key to remove a tunnel from the list.
Delete multiple tunnels	**1** Click on a tunnel name in the Name column, hold the mouse key down, and drag the cursor to select additional tunnels. **2** Release the mouse button. **3** Click Delete below the Tunnel Names/Associated Ruleset list. You cannot use the keyboard Delete key to remove a tunnel from the list.
Begin to edit a tunnel's configuration	**1** Click a tunnel name in the Name column. **2** Click Edit below the Tunnel Names/Associated Ruleset list to open the Tunnel Configuration dialog. or Double click on the tunnel you want to edit.

Table 3-2. Using VPN Configuration dialog box to create, edit, and associate tunnels and rulesets (continued)

To get this result:	perform these actions
Create a new ruleset.	**1** Click New under the Local Tunnel Rulesets or Remote Main Rulesets list to open the (Local Tunnel Ruleset) or (REMOTE Main Ruleset) screen in the SCM shell. **2** Click the category for which to create a rule. **3** Click the direction in which the rule permits packets to travel. **4** Click Enable, or click an option, such as POP-3 in the POP Mail category. **5** Select a logging option. **6** Enter the Local and Remote addresses between which you want to enable the traffic specified by the rule. **7** Repeat steps 2-6 to create additional rules. **8** Click  to close the dialog and add the ruleset to the list.
Begin to edit a ruleset's rules	**1** Click a ruleset in the Local Tunnel Rulesets or Remote Main Rulesets list. **2** Click Edit below the list that contains the selected ruleset to open the ruleset's configuration screen in the SCM shell. or Double Click the ruleset.
Associate a ruleset with a tunnel	**1** Click a tunnel name in the Name column. **2** Click a ruleset name in either of the ruleset lists. **3** Click Apply below the list that contains the selected ruleset.

Table 3-2. Using VPN Configuration dialog box to create, edit, and associate tunnels and rulesets (continued)

To get this result:	perform these actions
Associate a ruleset with multiple tunnels	**1** Click a tunnel name in the Name column, hold the mouse key down, and drag the cursor to select additional tunnels. **2** Click a ruleset name in either of the ruleset lists. **3** Click Apply below the list that contains the selected ruleset.

Default Tunnel rulesets for incoming encrypted traffic

As Figure 3-7 illustrates, the Local Tunnel Rulesets list in the VPN Configuration dialog box contains three default selections, named Any Auth, Any Crypt, and Any Auth+Crypt. SCM provides no default rulesets for specifying how all the firewall's tunnels handle outgoing encrypted traffic, and the program's Remote Main Rulesets list contains no default rulesets.

The rules you create for Any Auth, Any Crypt, and Any Auth+Crypt are automatically associated with all the firewall's tunnels. The default rulesets' rules only define how the firewall handles incoming encrypted traffic.

All incoming tunnel traffic that the firewall can identify contains encrypted information in authentication headers or encapsulated security payloads. Either or both of these creations of the IPSec protocol can be added to an IP packet so that it can securely tunnel across the Internet. For more information about IPSec, authentication headers (AH), and encapsulated security payloads (ESP), see Chapter 5, "Tunneling with IPSec." Following are descriptions of the default Local Tunnel Rulesets:

- The Any Auth ruleset's rules specify how the firewall handles incoming traffic that contains only an authentication header.
- The Any Crypt ruleset's rules specify how the firewall handles incoming traffic that contains only an encapsulated security payload.
- The Any Auth+Crypt ruleset's rules specify how the firewall handles incoming traffic that contains both an authentication header and an encapsulated security payload.

VPN > Randomize All Keys command

Select VPN > Randomize All Keys to make SecureConnect Manager change all of the encryption keys and Security Parameter Indexes (SPIs) in a firewall's M uses a random number generator to automatically create the tunnels' new key and SPI entries. For explanations of encryption keys, SPIs and other elements of IPSec, see Chapter 5, "Tunneling with IPSec."

VPN > Export All Tunnels command

Select VPN > Export All Tunnels to automatically create files which contain a tunnel configuration and associated tunnel ruleset that is based on one of the local firewall's tunnels. A remote user at one of the firewall's remote tunnel endpoints can use an export file to create a tunnel for his own firewall. The export function reverses the local tunnel settings and the addresses in the tunnel ruleset rules before creating the export file, as illustrated in Figure 3-11 and Figure 3-12.

You can also export a single tunnel configuration by clicking on the Tunnel Info dialog box Export button. The Tunnel Info dialog box appears when you click the VPN Configuration dialog box New or Edit buttons.

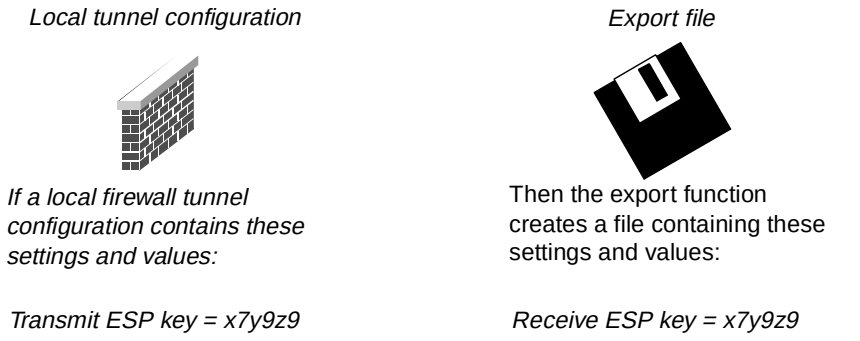
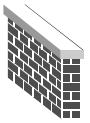
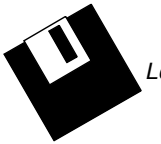


Figure 3-11. How export function creates remote tunnel configuration



Local tunnel ruleset rule in firewall

Category	*Options*	*Direction*	*Local*	*Remote*	*Logging*
FTP	*Enable*	*Incoming*	*200.20.2.2*	*100.10.1.1*	*Don't Log*



Local tunnel ruleset rule in export file

Category	*Options*	*Direction*	*Local*	*Remote*	*Logging*
FTP	*Enable*	*Outgoing*	*100.10.1.1*	*200.20.2.2*	*Don't Log*

Figure 3-12. How export function creates export file's local tunnel rules

By using the export version of the local firewall tunnel, the remote user can ensure that he can communicate securely with the local endpoint over an encrypted VPN. You can copy the files created by the export function to diskettes and distribute the diskettes to the remote tunnel endpoints, or you can place the files on a secure FTP server the remote users can access.

Caution: Make sure that the method you use to distribute export firewall files is secure, and that you do not send the firewall files over the Internet in the clear. Chapter 6, "Section Rulesets, FCP, and FCM,"explains how to set up a SecureConnect Server so that you can safely use the Internet to distribute export firewall files to PCs running the IntragyAccess SecureConnect Client feature.

When you select VPN > Export All Tunnels the function creates an export file for each of the firewall's tunnels and saves the files on the hard drive of the machine running SecureConnect Manager. Use the dialog box labeled Export All Tunnels to Directory to select the directory where SCM saves the export files.

Exporting Remote Main Rulesets

If you associate a Remote Main Ruleset with a firewall tunnel configuration, the ruleset is saved in the export file without changes, so a user who receives the file can use the ruleset as the remote tunnel endpoint's Main firewall. Remember to configure rules in a Remote Main Ruleset as though you are creating the Main firewall for the machine where the firewall is to be installed.

Export file values

Although most of the information that SecureConnect Manager saves in exported files is based on a firewall's tunnel configurations, SCM also places entries from a Target dialog box and the Tunnel Info dialog box in the files.

Target dialog box entries used in export files

Figure 3-13 shows entries in a Target Machine Information dialog box that SCM uses to produce the following lines in an export file.

TunName="Bluetunnel"

TunRemote="Blue"

The first line in this example specifies the name of the tunnel in the export file, `Bluetunnel`. SCM inserts the value of the Firewall Name field in this line. The second line specifies the location of the remote tunnel endpoint, `Blue`. SCM obtains the value it enters in this line from the Router Name or Address field or the Interface Name or Address field.

If the entries in the Target Machine Information dialog box and the Send Firewall to Router dialog boxes are different, SCM uses the values in Send Firewall to Router when it creates the export files. Therefore, if you change the name of the router to `Green` in the Send Firewall to Router dialog box, the export files will contain this line:

TunRemote="Green"

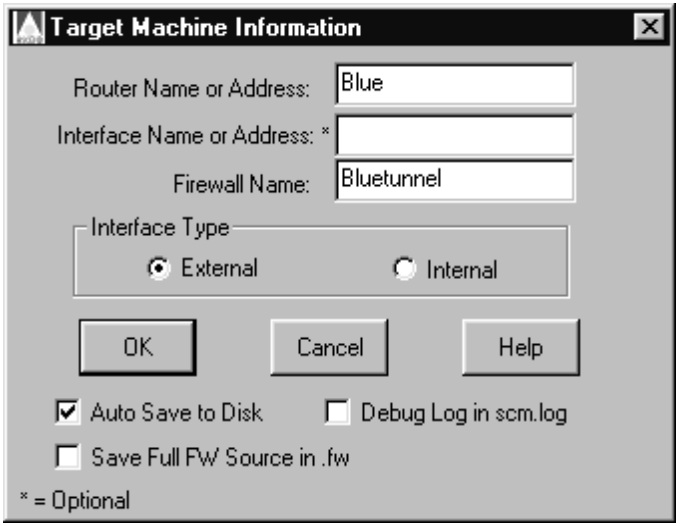


Figure 3-13. Target information used to create export files

Tunnel Info entry used in export files

SCM does not use an entry from the Target dialog boxes or the VPN Configuration dialog box to specify the tunnel ruleset name in the export file. The entry that it uses is the value of the Tunnel Name field in the Tunnel Info dialog box. SCM would use the entry in Figure 3-14 to produce a line like this in export files:

```
### Ruleset=RemoteTun1
```

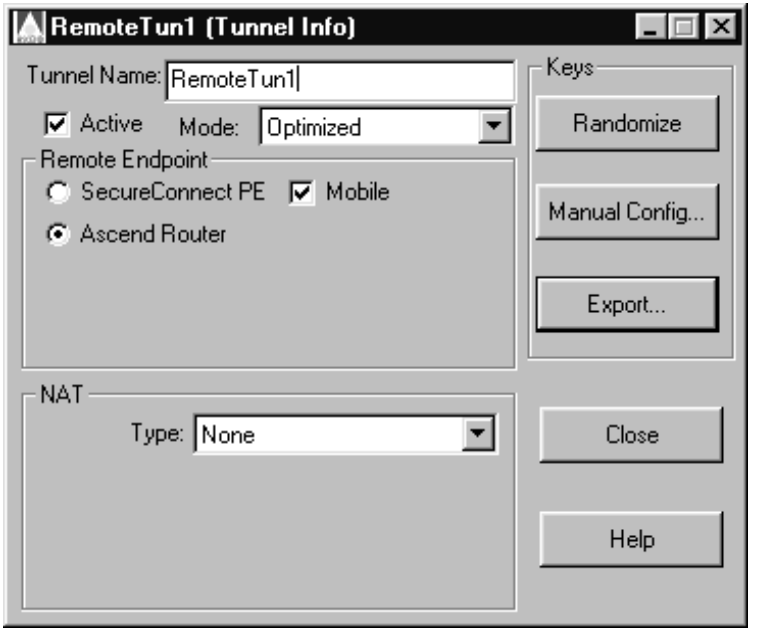


Figure 3-14. Entry SCM uses to create tunnel ruleset name in export files

Caution: SecureConnect Manager might save invalid information in tunnel export files if you do not enter the appropriate information in the Target dialog boxes before you use the export function.

For example, if you enter a router name instead of an IP address in the Target dialog box, SecureConnect Manager might enter the wrong remote tunnel endpoint in export files. Before SCM creates the export files, it will attempt to resolve the router name to make sure that the name is associated with an IP address. If SCM resolves the name, it will use it as the remote tunnel endpoint in the export files, but if the name resolves to an IP address that is not where you install the firewall, the remote tunnel endpoint in the export files will be wrong.

You will also find that your export files are incomplete if you do not enter information in a Target dialog box before you create the export files. This can happen if you create a tunnel configuration and click the Export button on the Tunnel Info dialog box before you enter target information. SCM saves export

files based on the information that is available, and the program does not prompt you to enter information in Target Machine Information if the dialog box's fields are empty.

VPN > Tunnel Defaults command

Select VPN > Tunnel Defaults to open the Default Settings of New Tunnels dialog box (Figure 3-15). Use the many drop-down lists, radio buttons and check boxes in this dialog box to create the settings for your default tunnel configuration.

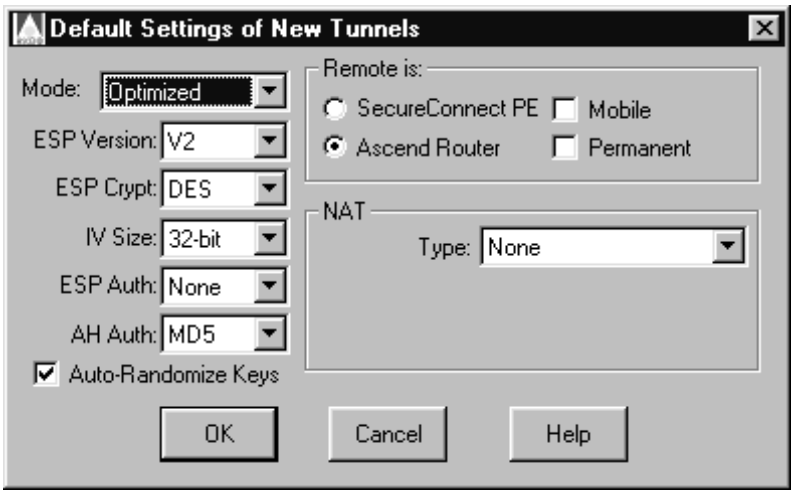


Figure 3-15. VPN > Tunnel Default dialog box

Mode

The IPSec protocol supports two methods for encapsulating IP packets, Transport mode and Tunnel mode. The drop-down list that appears when you select Mode contains three selections, Optimized, Transport, and Tunnel.

In Transport mode, IPSec does not encrypt the entire contents of a packet. The IP header and the Authentication Header are not encrypted so the Central Processing Unit (CPU) that decapsulates the packet has less work to do and the

source of the packet is not hidden. Use Transport mode if you are using IPSec to encrypt packets within a LAN.

In Tunnel mode, IPSec does encrypt the entire contents of the packet and it adds an IP header in front of the Encapsulating Security Payload. The additional IP header contains the IP addresses of the machines that encapsulate and decapsulate the packet, but the packet's original source and destination IP addresses are hidden in the ESP. The Tunnel mode requires more computing cycles than the Transport mode, but it is probably more secure.

If you select the third option, Optimized, SecureConnect Manager chooses the best alternative between the Transport and Tunnel modes.

Encryption options

Default Settings of New Tunnels contains five drop-down lists related to encryption and authentication. The selections in the lists are stipulated by the IETF IPSec standard RFCs.

ESP Version

Four of lists in the dialog box are related to the Encapsulating Security Payload (ESP). SecureConnect Manager and the SecureConnect Firewall feature support two versions of the ESP protocol. Version 1 is defined by the standard published in RFC 1828. Version 2 is described in an IETF draft document. Ascend supports both versions so that its IPSec products are compatible with the current best implementations of the protocol. ESP version 1 does not support authentication of the ESP, but version 2 does. If you select version 2, you must also select a message digest transform from the ESP Auth list.

The level of security provided by ESP version 2 is comparable the security provided by adding an Authentication Header and an ESP to tunneled packets. Each IPSec implementation provides encryption and authentication, and the tunnel endpoint must use a similar amount of processing power when it handles either type of IPSec packet.

The two ESP versions are not compatible, so you cannot configure one end of the tunnel to receive ESP version 1 packets if the other end of the tunnel is configured to transmit ESP version 2 packets.

Note: You can configure tunnels so that the endpoints do not add ESPs to the packets. However, there is no selection in the ESP version list for this type of tunnel. Select None in the ESP Crypt list if you only want the tunnel endpoints to add Authentication Headers to the IPSec packets.

Chapter 5, "Tunneling with IPSec," and SCM Help contain explanations of the encryption algorithm options.

ESP Crypt

In the ESP drop-down list, select the type of encryption the tunnel endpoints use to encrypt packet data. All Pipeline routers and PCs running IntragyAccess SCC can be tunnel endpoints that use DES(40) encryption to create an ESP. To use the DES and 3DES selections you must obtain the SecureConnect Firewall software upgrade. The upgrade is subject to the export restrictions described in Chapter 1, "Introducing SCM, SCF and SCC."

Table 3-3. ESP Crypt selections

ESP Crypt selection	Description
None	No algorithm selected to create ESP for tunneled packets. Tunnel endpoint only adds Authentication Headers to packets.
DES(40)	If ESP version 1 is selected, then endpoint uses DES algorithm and a 40-bit key to encrypt packet data. An ESP is added to tunnel packets. If ESP version 2 is selected, then endpoint uses DES algorithm and a 40-bit key to encrypt packet data. Endpoint also uses a Hashed Message Algorithm Code (HMAC) transform on the packet to produce a digest that is added to the ESP. Digest provides authentication of the ESP that is added to tunnel packets.

Table 3-3. ESP Crypt selections (continued)

ESP Crypt selection	Description
DES	If ESP version 1 is selected, then endpoint uses DES algorithm with 56-bit key. If ESP version 2 is selected, then endpoint uses DES algorithm with 56-bit key. Endpoint also uses a HMAC transform on the packet to produce an authentication digest that is added to the ESP.
3DES	If ESP version 1 is selected, then endpoint uses DES algorithm with 56-bit key in three rounds of encryption. If ESP version 2 is selected, then endpoint uses DES algorithm with 56-bit key in three rounds of encryption. Endpoint also uses a HMAC transform on the packet to produce an authentication digest that is added to the ESP.

IV Size

In the IV Size list, specify whether the ESP should include a 32-bit or 64-bit initialization vector. If you select ESP version 1 you can specify either size. If you select ESP version 2 the initialization vector must be 64 bits.

ESP Auth

If you select ESP version 2, you can also select an HMAC message digest transform from the ESP Auth list. The tunnel endpoint uses the transform to create a digest of the packet and it puts the digest in the ESP to provide authentication. The selections in the ESP Auth list are None, Message Digest 5 (MD5) and Secure Hash Algorithm-1 (SHA1). ESP version 1 does not support ESP authentication. Message digest transforms are not subject to export restrictions.

The MD5 transform is a one-way hash algorithm that produces a 128-bit digest of the data that is hashed. The MD5 selection in the ESP Auth list is the HMAC

version of the digest. Version 2 of ESP requires that the output of the HMAC MD5 hash be truncated to 96 bits before the digest is added to the ESP.

The SHA-1 transform is also a one-way hash algorithm and it produces a 160-bit digest. The SHA1 selection in the ESP Auth list is the HMAC version of SHA-1 and ESP version 2 specifies that the output of the hash must be truncated to 96 bits before the digest is added to the ESP.

Note: MD5 and SHA1selections appear to be active in the ESP Auth list when you select ESP version 1. If you configure a tunnel with ESP version 1 and select MD5 or SHA1 in the ESP Auth list, SCM automatically inserts the value None for the file's ESP Auth setting in the firewall file.

AH Auth

Authentication Headers contain digests of data that the receiving end of the tunnel can use to authenticate the sender of an IPSec packet. The selections in the AH Auth list are similar to those that SCM provides in the ESP Auth list. They include MD5, SHA1, MD5-HMAC and SHA1-HMAC. As noted in the previous discussion of ESP Auth transforms, MD5 produces a 128-bit digest, SHA1 produces a 160-bit digest, and the HMAC versions of the transforms produce truncated 96-bit digests of the original output.

If you select ESP version 2 when you configure a tunnel, and you use ESP authentication, you should consider whether or not to select AH authentication for the tunnel configuration. Your security will not improve by adding additional authentication and you will increase the time it takes the tunnel endpoints to encrypt and decrypt IPSec packets.

Remote tunnel endpoint options

In the Default Settings of New Tunnels dialog box, the area labeled `Remote is:`. contains radio buttons you can click to specify whether the default machine at the other end of your firewall's tunnels is a router or a PC running IntragyAccess SCC. You can also click a check box to specify whether the default tunnel's remote endpoint is a permanent or mobile location. If you click the Mobile check box, the Permanent check box disappears.

The SecureConnect Firewall + VPN feature can work as long as one of the tunnel endpoints is permanent. Click the Mobile box if the remote tunnel endpoint is a

machine which might have a different IP address each time the tunnel connection is made, such as a laptop running IntragyAccess with SCC.

Auto-Randomize Keys

Select Auto-Randomize Keys if you want SecureConnect Manager to create randomly-generated keys and SPIs for any tunnel that is based on the default tunnel configuration.

NAT (Network Address Translation)

In the Default Settings of New Tunnels dialog box, the area labeled NAT contains a drop-down list of Network Address Translation (NAT) options. Select the option that indicates one of the following:

- Whether or not the router on which you install the firewall performs NAT
- Whether the machine at the remote end of a tunnel receives a NAT address from the router at the local end of the tunnel

Network Address Translation enables a router to route packets to, or from, a network machine that does not have a unique IP address. Each machine that sends or receives IP packets through a public network must have a unique IP address so that the network can find the machine. The Internet has grown so fast that the supply of unique IP addresses is diminishing. NAT reduces the drain on available unique IP addresses because it enables system administrators to assign non-unique IP addresses to machines within their own network.

When a router that performs NAT receives an outgoing packet from a machine on the internal network, it changes the packet's non-unique source address to a unique IP address before it routes the packet to the public network. The NAT router can handle the incoming and outgoing traffic for the internal machine because the router keeps a table that correlates the machine's non-unique address with the unique IP address the router gives the packets.

NAT is an IETF standard described in RFC 1631. The RFC specifies that the machines on the internal network be assigned addresses from the class A network 10.0.0.0.

Your Ascend unit's user guide explains how to configure the unit to perform NAT. For example, if you use the Pipeline Companion interface, select Protocols

and check Enable NAT Routing. Most Pipeline units include a Dynamic Host Configuration Protocol (DHCP) server that provides unique IP addresses the units use to perform NAT. The IP Address Management section in your Pipeline User's Guide includes instructions for configuring your Pipeline unit's DHCP server.

None

Select None if you do not want the router on which you install the firewall to perform Network Address Translation on the local tunnel endpoint's outgoing, tunneled packets. If the router's NAT function is on when you select None, the router will still not perform NAT on the outgoing packets the firewall sends into the tunnel.

The NAT option is on if the router's Ethernet > NAT > Routing option is set to Yes.

Same As Physical

Select Same As Physical if the router on which you install the firewall is to perform NAT on outgoing packets the router receives from the local tunnel endpoint.

If you select Same As Physical, the router's Ethernet > NAT > Routing option must be set to Yes.

Reverse

Select Reverse if you want packets which the router receives from the remote end of the tunnel to appear to be sent by a host on the local network. When you select Reverse, the router on which you install the firewall changes the source address of incoming packets it receives from the remote end of the tunnel. The router also changes the destination address of outgoing packets that the local tunnel endpoint sends in response. This process is called Reverse Tunnel NAT (RTNAT). The router can only perform RTNAT on incoming packets from the remote tunnel endpoint, or on packets sent by the local endpoint once the tunnel has been established.

For example, as Figure 3-16 shows, the router might change the source address from 137.195.3.2 to a local network address, such as 10.10.10.5. The router changes the source address before it routes the packets, so the remote machine can access services that are available to machines on the local network. The router also changes the destination address on outgoing packets sent by local network to the remote tunnel endpoint, so the packets can be forwarded to the remote endpoint's unique IP address.

If you select Reverse, the router's Ethernet > NAT > Routing option must be set to Yes.

Note: If you create a new tunnel which is based on a default configuration in which the NAT value is Reverse, you must specify how the router obtains the local network address it adds to the remote tunnel endpoint's packets. For more information about where the router gets local network addresses it uses in the Reverse Tunnel NAT process, see "Creating a default configuration that enables translation of tunnel endpoint addresses," in Chapter 4, "Creating a SecureConnect firewall."

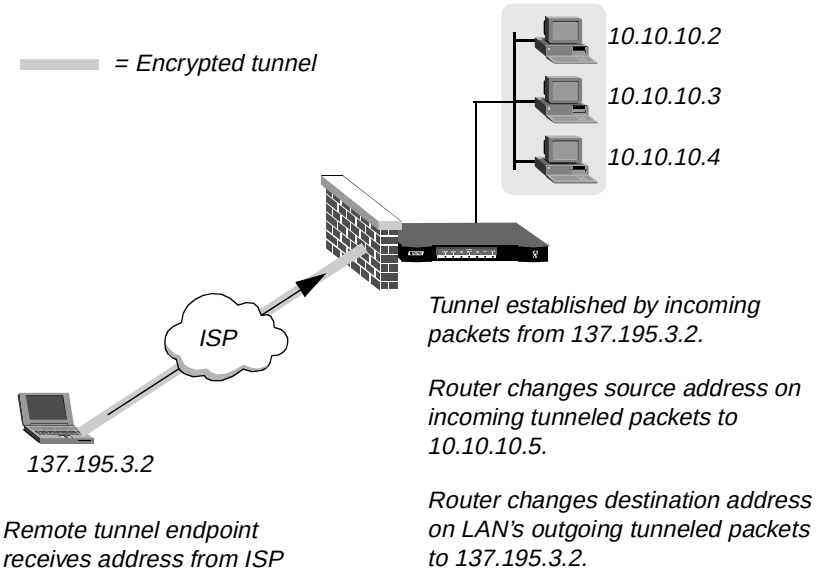


Figure 3-16. Reverse Tunnel Network Address Translation (RTNAT)

FCP menu

FCP stands for Firewall Control Protocol. Select the FCP menu to create special subsections of the firewall's Main ruleset. The subsections, referred to as section rulesets, enable you to temporarily permit classes of users more access, or different access, than the Main firewall permits.

The FCP menu is visible when you are working in the Main (Ruleset) screen. The FCP menu is not visible when the SCM shell is empty, or when the VPN Configuration dialog is active in the shell.

FCP > Add Section command

Select FCP > Add Section to create a new section ruleset. Enter the new section ruleset's name in the Add FCP Labelled Section dialog box, then use the Main (Ruleset) screen to create the section ruleset's rules. As shown in Figure 3-17, SCM adds a Section button and a drop-down list to the Main (Ruleset) screen when the firewall contains a section ruleset. To configure or edit a section ruleset, select its name from the drop-down list. To edit the Main firewall ruleset, select Main from the section drop-down list. You cannot create or edit tunnel rulesets from the Main (Ruleset) screen

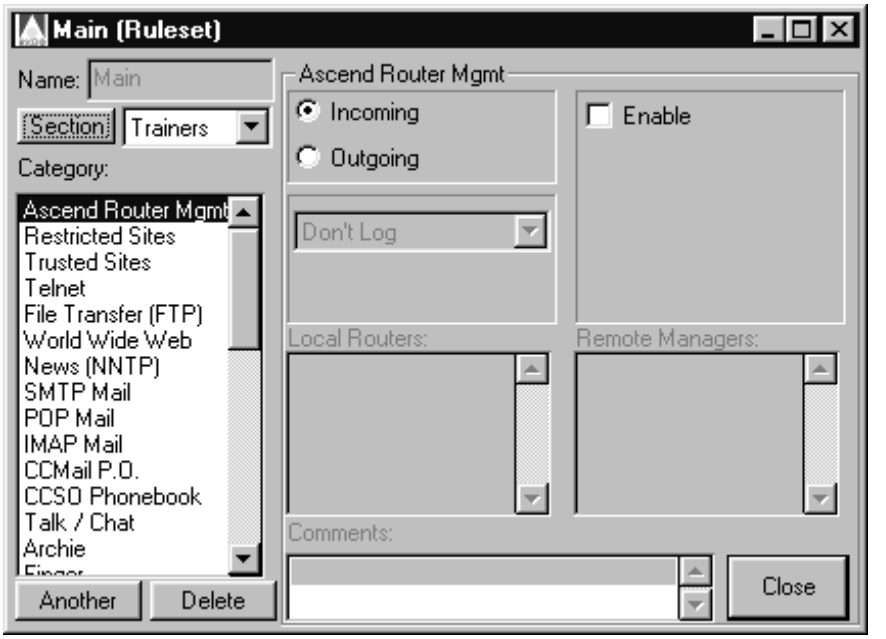


Figure 3-17. Main (Ruleset) screen during section ruleset configuration.

FCP Section Configuration

In addition to creating a section's ruleset rules, you must specify how the firewall determines when a connection opened by a section ruleset rule should close. When you select a section name and click the Section button, the FCP Section Configuration dialog box (Figure 3-18) appears.

Type

In the Type area, select Timeout or Keepalive as the type of timer to apply to each connection. For Timeout, the timer specifies the absolute number of seconds the connection will remain open. A Keepalive timer resets each time the traffic enabled by the section ruleset appears at the firewall. Connections controlled by a Keepalive timer remain open as long as the timer resets, or until a specified period of time passes in which there is no traffic.

Section Timeout Source

After you select the type of timer, you must select a Section Timeout Source. If you select FCP, the firewall uses a timeout value the router receives in an FCP message sent by the Firewall Control Manager. If you select SCM, the firewall uses value you enter in the Seconds field.

Chapter 6, “Section Rulesets, FCP, and FCM,” contains information about Firewall Control Protocol (FCP), Firewall Control Manager (FCM) and section rulesets.

Seconds

If SCM is the Section Timeout Source, a field labeled Seconds appears in the FCP Section Configuration dialog box. Relate the value you enter in the Seconds field to the type of timer you select. For example, if you select Timeout, enter a value for the absolute number of seconds the connection can remain open. If you select Keepalive, enter the number of seconds that the Keepalive timer can wait for traffic before the timer closes the connection.

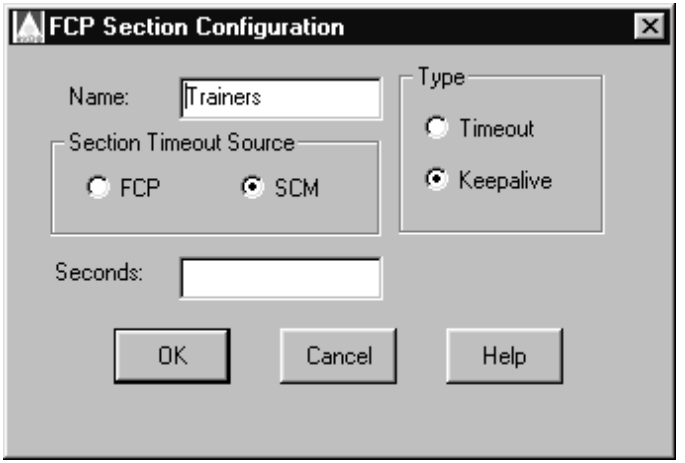


Figure 3-18. FCP Section Configuration dialog box

FCP > Delete Section command

Select FCP > Delete Section to remove a section ruleset from the firewall. When the Delete FCP Section dialog box appears, select a section from the list and click Delete.

Window menu

Select the Window menu to change the active Window in the SCM shell or to arrange the views of open windows.

In the Window menu, VPN Configuration opens the VPN Configuration dialog box and Main Ruleset opens the Main (Ruleset) window.

Select the Cascade or Tile commands to arrange the way open, resized windows appear together in the shell.

Select Arrange Icons to organize reduced windows along the bottom edge of the shell.

Help menu

In the Help menu the This Screen command changes the mouse cursor to a help pointer. You can then move the pointer to an object on the SCM screen and click your left mouse button to display information about that object.

If you select Contents a list of general topics covered by SCM Help appears. Index displays the complete list of topics included in SCM Help, and About displays the SCM version.

Ruleset configuration screen components

The Main (Ruleset), (LOCAL TUNNEL Ruleset), and (REMOTE MAIN Ruleset) screens are substantially the same, with minor variations in the list of categories you can select to create ruleset rules. The main components of each

screen are a category list, location text boxes, and a list of logging options. You can enter comments about the ruleset's rules in the Comment text box.

Category list

The Category list, on the left side of the ruleset screen is a scrollable list of protocols, services, and applications you select to build rules in a ruleset. Some of the options, such as Cracking Prevention, are highly recommended components for all firewalls. Others are site dependent. For example, you can select the Multimedia option to create a rule that permits real time audio and video protocols. When you select a category the screen displays options for that category, such as Enable, Incoming, Outgoing, and versions of the service or protocol.

Note: Appendix A, "Appendix: Ruleset categories," contains short profiles of services and protocols in Categories. You can also obtain this information by selecting Help from the menu bar or taskbar.

Special categories

The list of categories contains four special selections that enable you to define custom categories, to create rules based on the Firewall Control Protocol (FCP), and to create a rule for that describes packets that can never be encrypted for transmission over a VPN tunnel. Firewall Control Protocol is explained in Chapter 6, "Section Rulesets, FCP, and FCM."

Custom categories

Use custom categories to create firewall components for protocols that are not included in the Category list. Select Custom IP Protocol if you need to enable incoming or outgoing TCP or UDP traffic by port number and type of packet. If your router provides packet bridging, you can enable incoming or outgoing Ethernet packets by selecting the Custom Non-IP Protocol category.

Naming custom rules that you create

To remember what your custom rules enable, you can name each Custom IP Protocol and Custom Non-IP Protocol rule you create. If you enter a name in the rule's Name field, it appears in the Category list.

Custom IP Protocol category

In addition to the standard category options discussed in the next section, a drop-down list and Port Number text box appear in the SCM window when you select the Custom IP Protocol category.

The port number you enter identifies the port where the Custom IP Protocol connection takes place. The port number is on the local IP address if the connection is incoming and on the remote IP address if the connection is outgoing.

The drop-down list options include:

Table 3-4. Custom IP Protocol options

Option	Description
Inactive	Retains incoming /outgoing designation, port number, and location text box information for selected Custom IP Protocol category, but deactivates rule defined by category's entries.
TCP Session	Enabled Custom IP Protocol packets are TCP packets. Protocol is identified by entry in Port Number text box
UDP Session	Enabled Custom IP Protocol packets are UDP packets. Protocol is identified by entry in the Port Number text box.

Table 3-4. Custom IP Protocol options (continued)

Option	Description
UDP Query/Resp	Custom IP Protocol is a query and response protocol such as RADIUS or SNMP. Incoming and outgoing packets for session are enabled because firewall notes destination and source locations in query packet and passes response packet(s) that contain the same location and port information.
UDP Packet Dst Spec	Only enables UDP packets to the destination IP address at port number entered in the Port Number text box. Firewall does not pass response packets from destination to source.
UDP Packet Src Spec	Only enables UDP packets from Port Number of the source IP address. Firewall does not pass response packets from destination to source.

Custom Non-IP Protocol category

The Custom Non-IP Protocol category provides the Ethertype (Hex) a text box in which you can enter a hexadecimal number that corresponds to a packet's Ethernet Type field. Use the Custom Non-IP Protocol to build a firewall for bridged Ethernet packets. Appendix A, "Appendix: Ruleset categories," includes a table of hexadecimal equivalents for common Ethernet types.

Fwall Control Protocol category

Select the Fwall Control Protocol category to permit a firewall to temporarily incorporate information the router receives in Firewall Control Protocol (FCP) packets into rules that only apply for the duration of an authenticated user's session. FCP packets are described in Chapter 6, "Section Rulesets, FCP, and FCM."

The Fwall Control Protocol rule places blanks in the firewall that are filled in by information received in FCP packets sent to the router by an agent such as the Ascend Firewall Control Manager. However, enabling the Fwall Control Protocol

rule creates firewall rules that are more general than the specific rules you create in a firewall section.

Use caution when click the Fwall Control Protocol rule's check boxes. The options automatically enable incoming and outgoing packets on the basis of the packets' underlying general protocol, such as TCP or UDP, not a specific protocol, such as Telnet or POP Mail. Table 3-5 describes The Fwall Control Protocol rule's options.

Table 3-5. Fwall Control Protocol rule options and effects

Option	Rule name	Rule's effect
TCP	tcpin tcpout	Allow incoming/outgoing TCP sessions with addresses/ports supplied by FCM.
TCP	ftpin ftpout	Allow incoming/outgoing FTP sessions with addresses/ports supplied by FCM.
UDP	udpsin udpsout	Allow incoming/outgoing UDP highport to highport sessions, such as TFTP.
UDP	udpqin udpqout	Allow incoming/outgoing UDP query/response sessions, such as SNMP.
UDP	udppkin udppkout	Allow incoming/outgoing single UDP packets for which no response is expected or allowed, such as Syslog packets.
Trusted	trust	Allow all packets matching the addresses sent in FCP packets.
Restricted	restrict	Restrict all packets matching addresses sent in FCP packets.

Table 3-5. Fwall Control Protocol rule options and effects (continued)

Option	Rule name	Rule's effect
Logging	log trace	Log/trace all packets matching addresses sent in FCP packets.

Never Tunnel TCP category

The Never Tunnel TCP category enables you to define a rule of the highest priority. A Never Tunnel TCP rule is placed on top of the firewall's stack of rules when SecureConnect Manager compiles the firewall. Normally the first rules in a firewall's stack describe the packets that must be tunneled, but a Never Tunnel rule takes precedence over even the firewall's tunnel rules.

You might create a Never Tunnel TCP rule to increase throughput when a user should be able to send unencrypted packets to a specific location even though the firewall's tunnel ruleset causes all other outgoing packets of that type to be encrypted. For example, if a user's firewall lists a network gateway router as a Trusted Site in a Tunnel Ruleset, the firewall encrypts all of the packets the user sends to the network behind the router. If the network includes a site to which the user should be sending unencrypted packets, (a public FTP server, for example), you can create a Never Tunnel TCP rule in which that site is listed as the remote address. When a user's SecureConnect Client PC parses its firewall's rules, the packets the user sends to the public FTP server match the Never Tunnel TCP rule at the top of the stack, so the firewall will pass the PC's outgoing, unencrypted FTP packets.

For additional information about using the rule Chapter 6, "Section Rulesets, FCP, and FCM."

Options for defining rules

Begin defining a rule for a category you selected by clicking the category's options. Some options are displayed for most of the categories you select, such as Enable, Incoming, and Outgoing. However, you can define different options for many of the categories you select to create ruleset rules.

Enable

Click the Enable radio button to create a rule that permits the category's packets to pass the firewall. If SecureConnect Manager does not display an Enable radio button, select the category's protocol or service options. For example, if you select the category IP Address Resolution, SCM displays the ARP and RARP protocol options. These options are acronyms for Address Resolution Protocol and Reverse Address Resolution Protocol. If you select ARP and RARP, you create one rule that permits both types of IP Address Resolution packets. Generally, options are not mutually exclusive, so you can select more than one of them. Figure 3-19 illustrates how you can select the IMAP Mail protocols v2/v4 and v3 options simultaneously to create one rule that enables the packets of three IMAP protocol versions to pass through a firewall.

Appendix A, "Appendix: Ruleset categories," also contains detailed information on options, such as ARP and RARP.

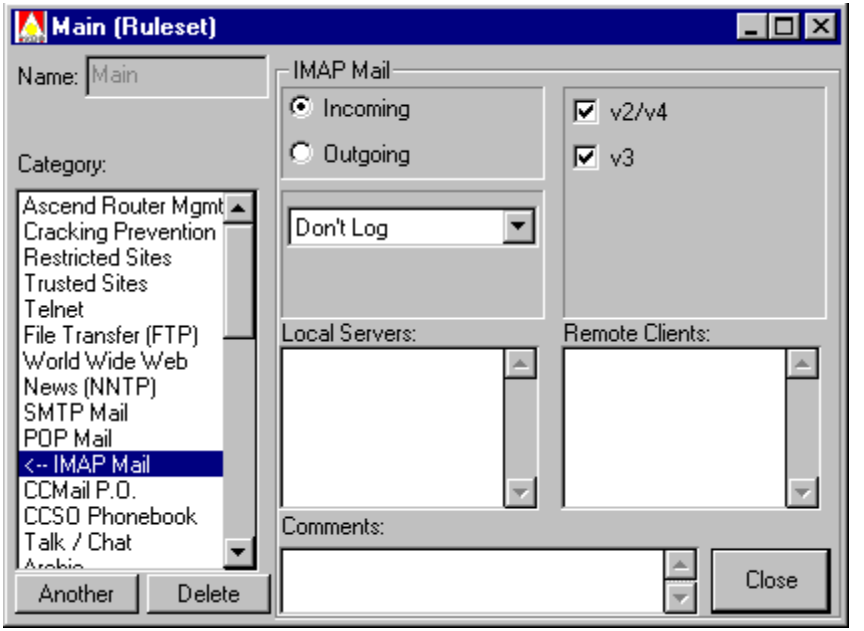


Figure 3-19. The IMAP Mail service with version options v2/v4 and v3

Grouped services

Some service selections such as Routing Information, Ping/Traceroute and Unix Utilities, group similar or related protocols and services under a single category. For example, as Figure 3-20 shows, when you select the category Routing Information you can choose from among four routing protocols whose packets you want the firewall to permit. The protocols include RIP, OSPF, EGP and BGP.

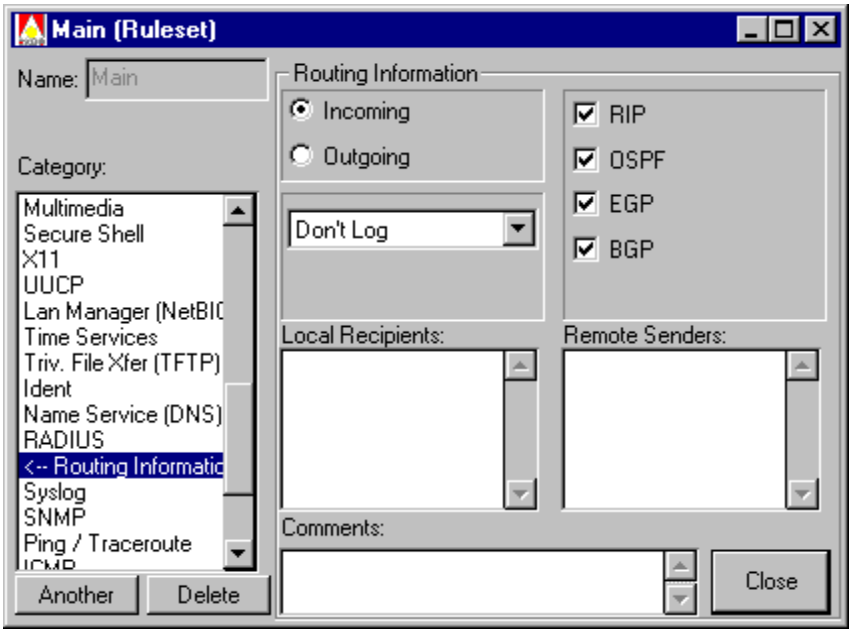


Figure 3-20. Routing Information RIP, OSPF, EGP, and BGP options

Incoming and Outgoing

Click the Incoming or Outgoing radio button to specify the direction in which the firewall permits the packets to flow. Remember that Incoming and Outgoing directions are relative to the position of the firewall on the router. If the firewall is on the router interface between the router and the user sending the packets, then the user's packets are incoming. For example, if the firewall is on the router's Ethernet interface, the packets the router receives from the LAN are incoming, not outgoing.

The arrow next to the name of the rule indicates the direction in which the rule enables traffic. If a double-headed arrow is next to the category name, the rule enables incoming and outgoing traffic. Figure 3-21 displays arrows next to the FTP, World Wide Web and SMTP categories.

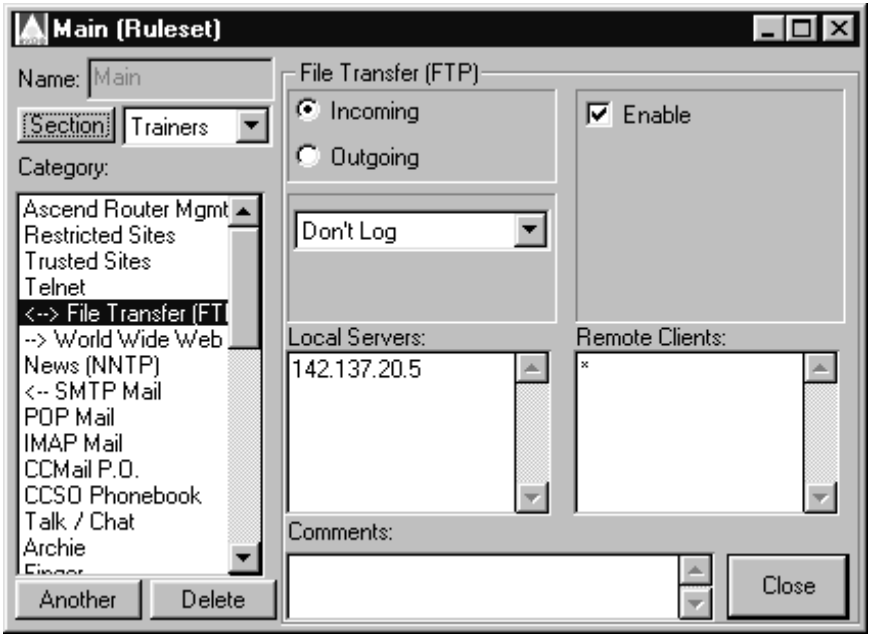


Figure 3-21. Arrows indicate the direction in which the rule enables traffic

Note: SecureConnect Manager automatically enables response packets for bi-directional categories like FTP and Telnet. You do not need to enable incoming from specific sites if you enable outgoing from a local client.

The Another button

You can create another listing of the same category by selecting the category you wish to duplicate and clicking the button labeled Another which is located below the list. You can use the new entry to create a new rule based on that category. Figure 3-22 illustrates the creation of a new FTP category.

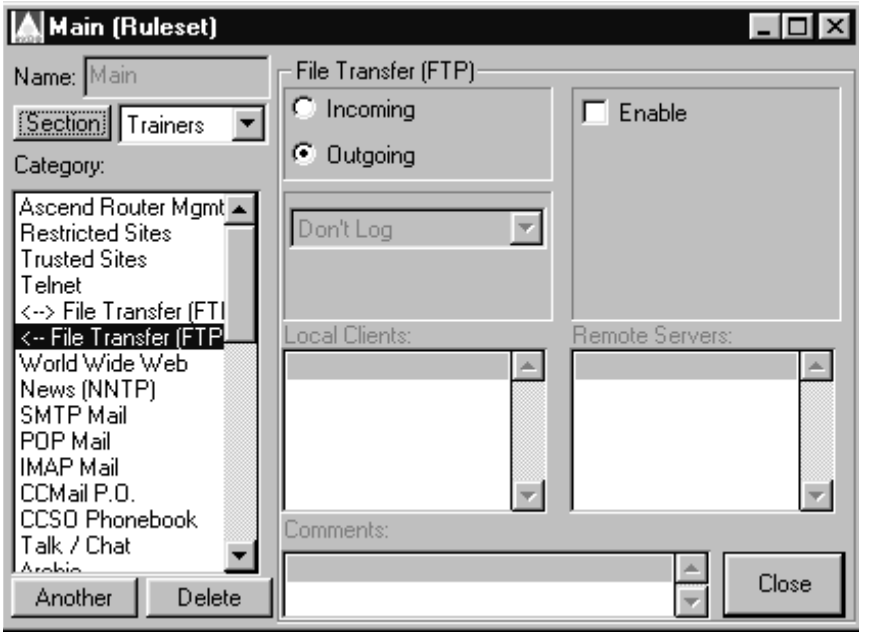


Figure 3-22. Creating a second FTP entry in a firewall

The Delete button

If you have used the Another button to create a second appearance of a selection in the Category list, you can remove it by clicking the Delete button below the list. You cannot use the Delete button to delete a category that has no duplicates. If you want to disable the rule defined by such a category, select the category and clear the Enable check box.

Location text boxes

There are two text boxes in which you can identify the sources and destinations of the packets defined in a firewall rule. The text boxes are not active until you click Enable or select one of the category's version or protocol options. You can enter the names or IP addresses of individual machines or network submasks in the local and remote text boxes.

If a firewall rule allows incoming packets, the local text box is labeled Local Clients and the remote text box is labeled Remote Servers (as shown in Figure 3-21). If a firewall rule enables outgoing packets the labels are Local Servers and Remote Clients (as shown in Figure 3-22). Some SCM categories do not follow this standard, but the location text box headings that are different are related to the actions of particular firewall security features. For example, if you choose IPSec, the text box headings are Local Gateways and Remote Gateways. The Custom Non-IP Protocol category has no location text boxes in which to enter IP address information, since you select the rule to specify packets which do not conform to the IP protocol.

Note: Generally, when you create rules in a Main firewall ruleset you must enter information in each location text box because the rule is incomplete when a local or remote location text box is empty. However, you can leave location text boxes blank when you create rules in section rulesets.

Address formats

You can use a number of formats to specify source and destination locations in a category's location text boxes. Fully qualified domain names are recommended, but you can also enter IP addresses with or without subnet masks, and wildcards.

Domain names

Enter a domain name in a location text box, if possible. A Domain name is the preferred format for the following reasons:

- Domain names are not affected by changes in domain IP addresses.
- SCM attempts to resolve all domain names in the firewall. You will receive an error message if SCM cannot resolve a domain name and SCM will not allow you to send the firewall to the router. It will, however, allow you to save the firewall as an `.fw` file if it can't resolve a domain name.
- A successfully resolved domain name is retained near its IP addresses in a saved firewall's `.fw` file. The domain name's appearances in the `.fw` file make it easier to locate all occurrences of the domain's IP addresses when you search for them in the ASCII text.

  Note: If you use domain names, you must make sure that the workstation running SCM can access a Domain Name System (DNS) server.

IP addresses

If you enter locations as IP addresses, you may include subnet masks. To specify a mask, enter a slash at the end of the 32-bit address and then append the mask, either in a dotted-decimal format, or as a decimal number representing the number of ones. For example, the following two masks are equivalent.

- 192.0.11.0/255.255.255.0
- 192.0.11.0/24

Wildcard entries

An asterisk (*) in a location text box functions as a wildcard. For example, if you enter an asterisk in the remote text box of an incoming FTP firewall, the client(s) in the local text box can receive FTP packets from any remote server. Although the asterisk can be very useful for indicating that all addresses are enabled in the local or remote location text boxes, you must use it carefully to avoid vulnerabilities in your firewall.

Multiple location entries in one location text box

Each location text box is large enough to accept a combination of domain names, IP addresses, and wildcards. Pressing the Enter key to separate the sites in a location text box does not create a one-to-one relationship between the local and remote entries that appear on the same line. For example, the rule created by the entries shown in Figure 3-23 permits each of the four remote clients to telnet to each of the four local servers.

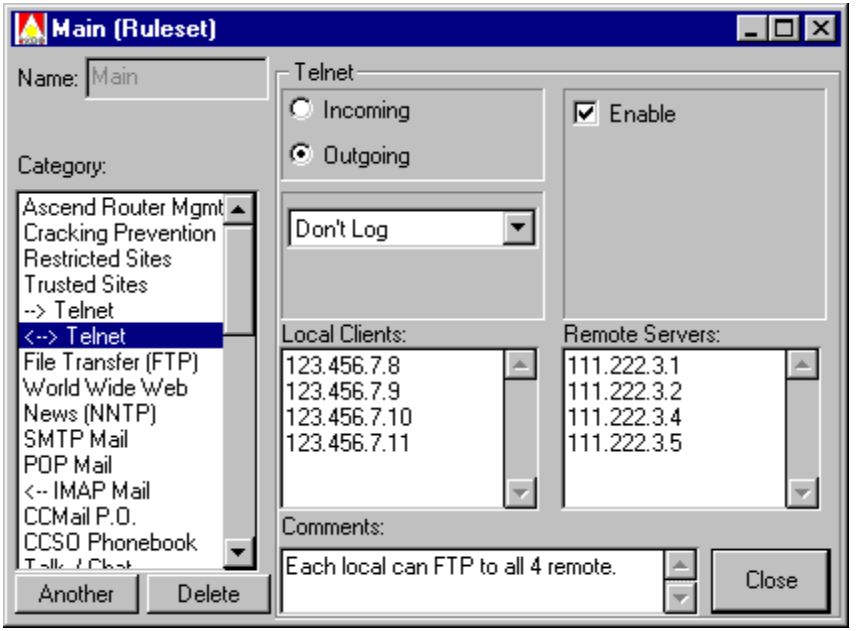


Figure 3-23. Rule enabling four remote clients to telnet to four local servers

Logging options

When the firewall rejects a packet, Syslog automatically receives information about the incident. To obtain information about sessions the firewall permits, you can select one of several SecureConnect Manager logging options (shown in Table 3-6). To activate the list, you must select Enable, or one of a category's service or protocol options.

Table 3-6. Logging options

Option	If selected, specifies
Don't Log	Prevent logging
Log Sessions	Log the packets that start a session
Log All Packets	Log all packets in a session

Table 3-6. Logging options (continued)

Option	If selected, specifies
Trace All Packets	Trace the routes of packets that are not rejected

When you choose to log or trace packets, you can display the captured information when the Ascend unit is in debug mode. You enter debug mode by executing the following four keystrokes within one second: **ESC [ESC =**. You can also display the logged information on a network host by using the Syslog facility.

Syslog messages appear in the following format:

```
date time router name ASCEND: interface message
```

The *message* portion can include one or more fields, which are described in detail in the appendix.

Table 3-7 describes the fields in Syslog messages, which records a blocked attempt to send FTP packets from remote IP address 156.150.203.90 to local IP address 194.70.42.65:

```
Mar 22 17:02:06 redfish ASCEND wan0 tcp 194.70.2.65;21
156.150.203.90 84! pass
```

Table 3-7. Sample syslog entries

Field	Entry	Description
date	Mar 22	Date message logged by Syslog
time	17:02:06	Time message logged by Syslog
router name	redfish	Router that sent message
	ASCEND:	
interface	wan0	Name of interface on which firewall is installed

Table 3-7. Sample syslog entries (continued)

Field	Entry	Description
message *protocol*	tcp	Protocol of packet traversing firewall
message *local*	194.70.42.65;21	Destination address of received packet and port number for FTP command session
message *direction*		Packet direction
message *remote*	156.150.203.90	Source address of received packet
message *length*	84	Length of packet in 8-bit bytes (octets)
message *log*	!pass	Log label indicating firewall blocked packet

Comment text box

You can enter comments about the rules you create in the Comment text box at the bottom of the ruleset configuration screen. The comments are saved in the firewall source file when you save the firewall.

Creating a SecureConnect firewall

4

This chapter explains how firewall administrators use SecureConnect Manager to create firewall rules in Main, section, and tunnel rulesets. It begins with a review that includes basic instructions for using the screens and dialog boxes described in Chapter 3, “Exploring the SCM Interface.” It concludes with examples based on common network configurations.

Before you begin

The SecureConnect Firewall template of rules prevents any packets from passing through the firewall. You must change the template rules before the firewall permits connections.

If your company has a security policy, consult it before you begin creating SecureConnect Firewalls. Next, gather information about your local network and the remote clients and servers that should be provided access through the firewalls. For example, decide which services the firewall should permit and which it should deny. Then find out the locations of servers that house the services the firewall should permit and the locations of servers to which the firewall should deny access.

When you decide where your firewall will allow access and where it will deny it, record the domain names, hostnames, or IP addresses of the locations. Then create a diagram that displays your network, your firewall, and the locations beyond the firewall with which your network should be able to communicate. Use the domain names and IP addresses you have collected to label the routers, hosts, and servers in the diagram.

Appendix A, "Appendix: Ruleset categories," is an alphabetical list of the services, protocols and applications you can select to create SecureConnect Firewall rules. The short descriptions of the services, protocols and applications in the appendix may be helpful when you are weighing what to permit and what to deny.

Also consider whether services or protocols are required for maintaining your networks' connections. For example, some Internet Service Providers (ISPs) must receive routing protocol packets from hosts that use their connections, or they mark the hosts' links inactive. If your ISP requires routing packets, your firewall must permit outgoing routing protocol packets.

Identifying SecureConnect firewall support on your unit

Before you begin building firewalls with SecureConnect Manager, consider how the SecureConnect Firewall feature works on your Ascend unit.

- You can load 3 firewalls on a Pipeline unit and 12 firewalls on a MAX unit.

- Pipeline units support encrypted Virtual Private Networking, but MAX units do not. Do not configure tunnels in firewalls you create for MAX units.
- Available NVRAM determines the number of encrypted Virtual Private Network Tunnels a Pipeline firewall can contain. Refer to your user guide to determine how much NVRAM is installed on your unit. If your unit is a Pipeline 220, you can install additional NVRAM.

Entering local and remote information

Before you begin to create firewall rules, review the following points about entering location information:

- Local and remote location text boxes are inactive until you click Enable, or select a service or protocol version.
- Labels above location text boxes change according to packet direction. For outgoing packets, text boxes labels are usually labeled Local Clients and Remote Servers. For incoming packets, most text boxes are labeled Local Servers and Remote Clients. The location labels are completely different for some categories. For example, a Restricted Sites rule prevents packets from passing through the firewall and the labels on the category's enable and location boxes form the phrase, "Don't Allow Anything Between Local And Remote".
- You must enter local and remote information for each firewall rule you create, unless you are creating section ruleset rules. You may enter one, or many, sites in each location text box. Chapter 6, "Section Rulesets, FCP, and FCM," covers section rulesets.
- You can enter fully qualified domain names, hostnames, and IP addresses in location text boxes. Qualified domain names are recommended, but only if you make sure the unit running SCM and the unit on which the firewall is installed can access a Domain Name Service Server.
- The asterisk (*) wildcard is acceptable in either or both location text boxes. If you enter an asterisk in a location text box, any address or domain name matches that location.
- Some protocols in the category list are bidirectional, such as FTP and Telnet. For such categories, you need not enable Incoming from a rule's remote sites if you enable Outgoing from a local client. The SecureConnect firewall feature automatically enables the protocol's response packets to pass through the firewall.

Selecting categories

You should know the following information concerning the selection of categories for the creation of firewall rules.

- You can select more than one category to create rules in a ruleset.
- You can select two custom categories to create rules for protocols that are not listed in the SecureConnect Manager's Category list. You can name the custom rules you create and add them to the Category list.
- Many categories contain protocol version options. Others categories, such as Multimedia, enable you to select multiple examples of a service or protocol. Selecting a protocol version or service is the same as clicking Enable.
- You might have to select particular categories for your firewall. For example, you must select Address Resolution Protocol (ARP) if you're installing the firewall on an Ethernet interface, and you must select Name Service (DNS) if you enter domain names in rules.

Saving and exporting firewall files

- You can save incomplete firewalls on a local hard drive or diskette. You can later open the saved file and add the missing information.
- To edit your firewall, open the firewall source file in SecureConnect Manager, then use the program to change the firewall rules.
- When you export a firewall, SCM saves a file that contains the firewall tunnel's VPN configuration and its associated tunnel ruleset. If you associated a remote Main ruleset with the tunnel configuration, SCM also places that ruleset in the export file. The file is saved in the Mixed Binary format, which means, the format of the file SCM writes depends on the type of machine that exists at the other end of the tunnel. If the remote tunnel endpoint is a PC running IntragyAccess SCC, SCM saves an `.fwb` file. If the machine is a router, SCM saves an `.fw` file.

Caution: Do not open a firewall source file in a word processor and attempt to manually edit the file. You might inadvertently change the meaning of a firewall rule, or damage the file so that SCM cannot read it.

Creating local firewall rulesets

Following are examples that explain how to create rules in a local firewall's Main ruleset and section ruleset. The examples show how to select categories, protocol versions, and the directions of packets, and to enter location information. In addition, the section ruleset example configures a section timeout source.

Main ruleset rules

The following example creates an outgoing FTP rule in the Main ruleset of a router's firewall. The FTP rule permits a local client to initiate file transfer connections with two remote servers and it turns on the SCM logging feature. The location entries the example uses in the FTP rule location text boxes are the domain names shown in Figure 4-1. You do not need to create an FTP rule that permits the return packets from the remote servers because the router's SecureConnect Firewall feature automatically enables return FTP packets from the remote servers.

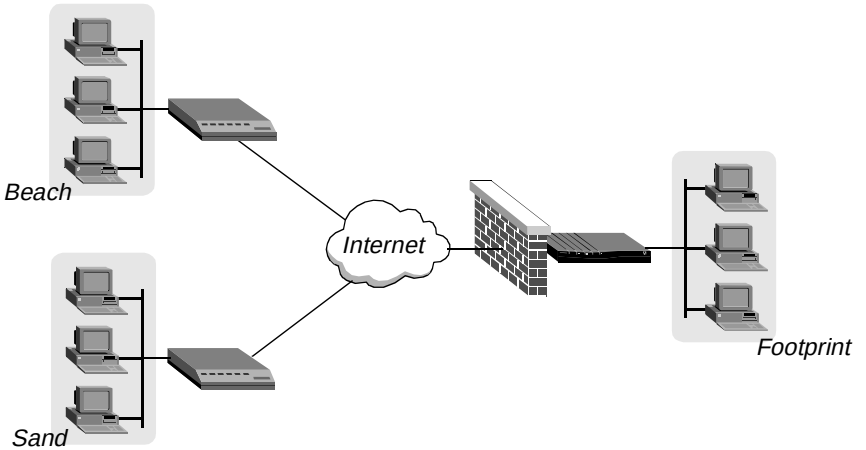


Figure 4-1. Diagram of local and remote locations in FTP rule

Creating an outgoing FTP rule

1. Select File > New.
2. Click Ascend Router w/ SecureConnect in New Firewall dialog.
3. Select FTP in the Category list in Main (Ruleset).
4. Click Outgoing, then click Enable.
5. Enter `Footprint` in Local Clients.
6. Enter `Sand` in Remote Servers, then press Enter, then enter `Beach` in Remote Servers.
7. Select Log Sessions in the list of logging options.

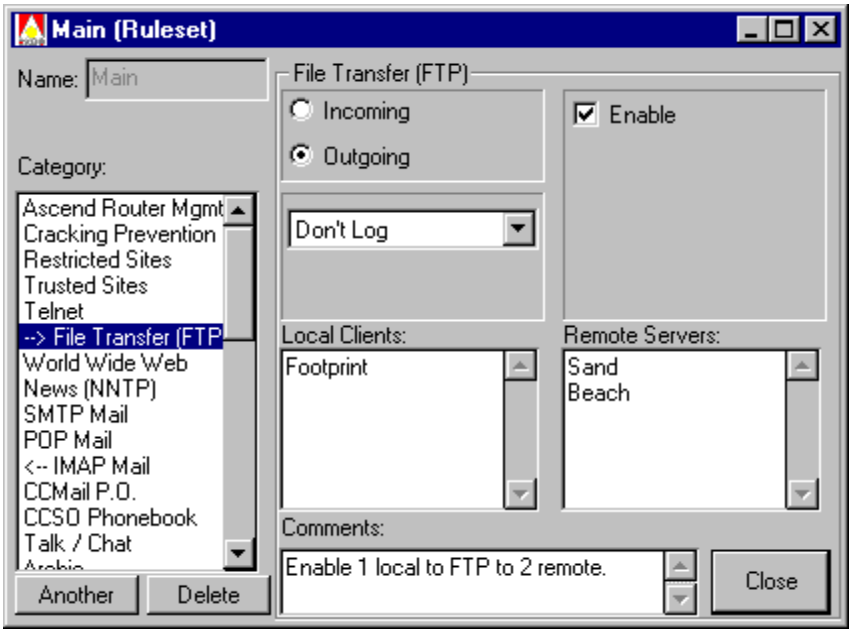


Figure 4-2. Creating an outgoing FTP rule in a firewall's Main ruleset

Section ruleset rules

The following example creates a section ruleset and adds a World Wide Web rule in the section ruleset. The rule enables incoming packets from a user at a remote site that are destined for a local Web server at IP address 123.123.4.5. The

example does not include a step for entering the Remote Client location in the rule because the router supplies an address or domain name it receives in a Firewall Control Protocol (FCP) message sent by the Firewall Control Manager (FCM). The example also shows how to configure a section timeout, which controls how long the session enabled by the section rule can last.

Chapter 6, "Section Rulesets, FCP, and FCM," explains how the Ascend Firewall Control Manager receives user authorizations from a RADIUS authentication server and prepares FCP messages it sends to the router. The chapter also describes the entries in RADIUS `client` and `users` files that enable you to use section rulesets in SecureConnect Firewalls.

Creating a section ruleset

1. Select File > New.
2. Click Ascend Router w/ SecureConnect in the New Firewall dialog.
3. Select FCP > Add Section.
4. Enter `Website` in the New Section field of the Add FCP Labelled Section dialog box.
5. Click Add.

Configuring a section timeout

You must configure a section's timeout values so that the firewall can end a connection permitted by a section ruleset rule. Timeout values include a type of timeout, a length of time, and a timeout source. For more information about timeout values, see Chapter 3, "Exploring the SCM Interface."

After you create the first section ruleset in a firewall, SCM adds a Section list above the Category list on the Main (Ruleset) screen. Next to the list SCM adds a Section button. Before you begin to configure the section timeout values, make sure that the name of the section appears in the Section box. In this example, the SCM saves the timeout values in the firewall. The router does not receive the values in FCP messages sent by the Firewall Control Manager.

1. Click the Section button on Main (Ruleset).
2. Click SCM and Keepalive in the FCP Section Configuration dialog box.
3. Enter 3000 in the Seconds field.

4 Click OK.

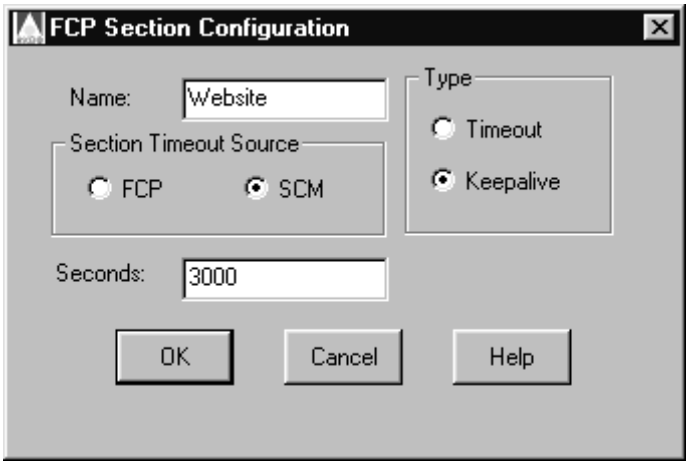


Figure 4-3. Section timeout configuration selections

Creating a section ruleset rule

Before you begin to create a section ruleset, make sure Section box contains the name of the section in which you want to create a rule. If you see another name there, click the Section button, then select the correct name.

1 Select World Wide Web in the Category list.

2 Click Incoming.

3 Click WWW, WAIS, Gopher, and Secure WWW (SSL).

4 Enter `123.123.4.5` in Local Servers.

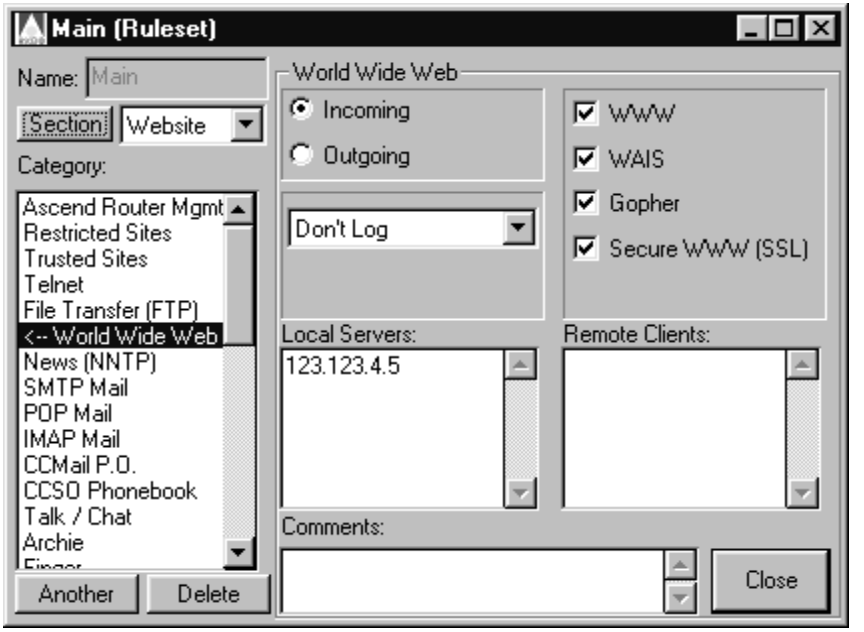


Figure 4-4. Section ruleset rules usually do not contain a remote location

Creating local firewall tunnel configurations and rulesets

This example illustrates how you create all the firewall components for encrypted tunnels, including an IPSec rule, a tunnel configuration and a tunnel ruleset. SecureConnect tunnel configurations are based on a firewall's default tunnel configuration, so the example begins with the creation of a default tunnel configuration. Next, the example shows how to create an IPSec rule in a Main ruleset. The third and fourth steps create a tunnel configuration and a tunnel ruleset. Encrypted tunnels only work if both ends of the connection have firewalls with matching tunnel configurations, so the example ends by explaining how to use the SCM export function to create a tunnel configuration and tunnel ruleset for the remote end of the tunnel.

The example is based on the diagram shown in Figure 4-5.

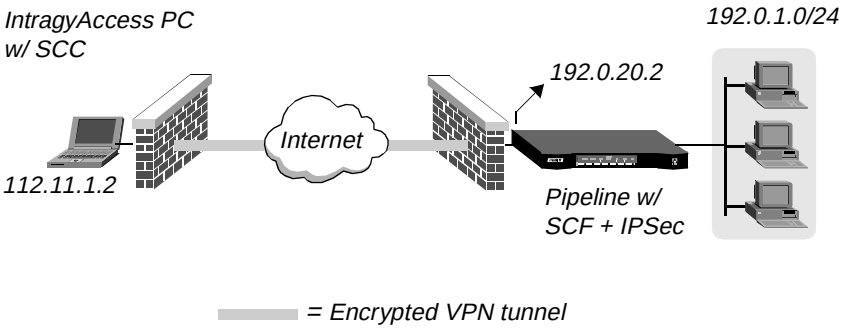


Figure 4-5. Diagram of encrypted VPN tunnel created by sample

Creating a default tunnel configuration

A default tunnel configuration provides the values that SCM uses for all new tunnel configurations. When you create a new tunnel you can manually change the default settings by clicking the Manual Config button on the Tunnel Info dialog box. The following example shows how to create a default tunnel configuration.

1 Select File > New.

2 Click Ascend Router w/ SecureConnect in New Firewall dialog.

3 Select VPN > Tunnel Defaults.

4 Select values for mode, encryption, and authentication settings.

5 Click Auto-Randomize Keys.

6 Select the options that describe the remote tunnel endpoint.

7 Select the option that specifies whether Network Address Translation (NAT) is turned on in the local router, or whether the local router performs Reverse Tunnel NAT on packets it receives from the remote tunnel endpoint.

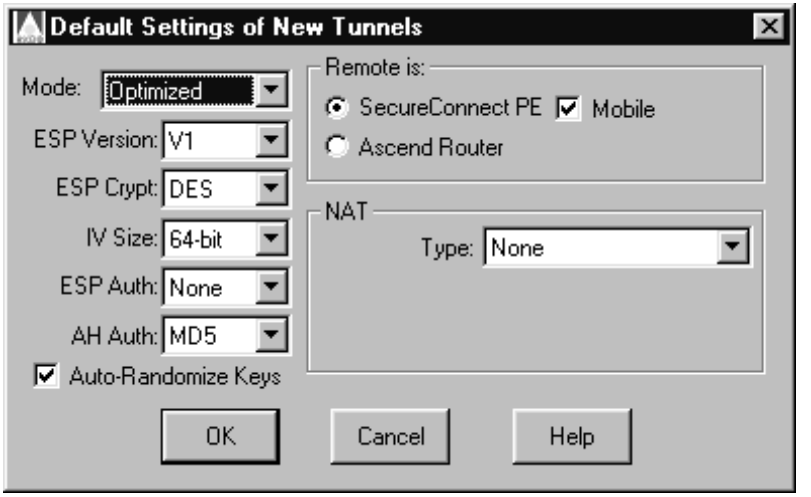


Figure 4-6. Selecting default settings for firewall tunnels

If you select the values shown in Figure 4-6, your firewall's default tunnel configuration creates tunnels that cause the actions listed in Table 4-1. In addition, the default tunnel configuration specifies that the local tunnel endpoint is a router in which the Network Address Translation feature is off, and that remote tunnel endpoint is a PC running IntragyAccess with the SecureConnect Client feature.

For more information about these values, IPSec, and encrypted tunnels, see Chapter 5, "Tunneling with IPSec."

Table 4-1. Actions caused by sample default values in Figure 4-6

Selected value	SCM or SCF action
Optimized	When SCM creates the firewall, it determines whether the local tunnel endpoint's SCF feature creates outgoing packets in Transport mode or Tunnel mode. For information on IPSec modes, see Chapter 3, "Exploring the SCM Interface."
V1	SCF uses version 1 of the ESP protocol.
DES	SCF uses the Data Encryption Standard (DES) algorithm to create the ESP.
64-bit	SecureConnect Firewall inserts a 64-bit initialization vector in the ESP.
None	SCF does not insert a hash digest of the ESP contents in the ESP.
AH Auth	SCF uses the Messages Digest 5 (MD5) transform to create the Authentication Header.
Auto-Randomize Keys	SCM creates randomly-generated keys that SCF uses with the encryption and authentication algorithms. SCM also randomly generates the value of the tunnel configuration Security Parameter Index (SPI).

Specifying characteristics of the default remote tunnel endpoint

When you configure a default tunnel configuration, you must specify the kind of machine that exists at the remote end of the tunnel. To specify the kind of machine, you must indicate what the machine is and whether it has a permanent IP address. You must also indicate whether a form of Network Address Translation is involved in the tunnel configuration.

The remote tunnel endpoint specifications that you set in the Default Settings of New Tunnels dialog box appear in the Tunnel Info dialog box when you create a new tunnel configuration. For example,Figure 4-7 displays the Tunnel Info dialog box that appears if you specify that the default machine is an Ascend router which has a permanent IP address. The Tunnel Info dialog box contains a field in which you can enter the unit's IP address. It also contains a field in which you can specify an interface IP address if you are installing the firewall that contains the tunnel configuration on that interface.

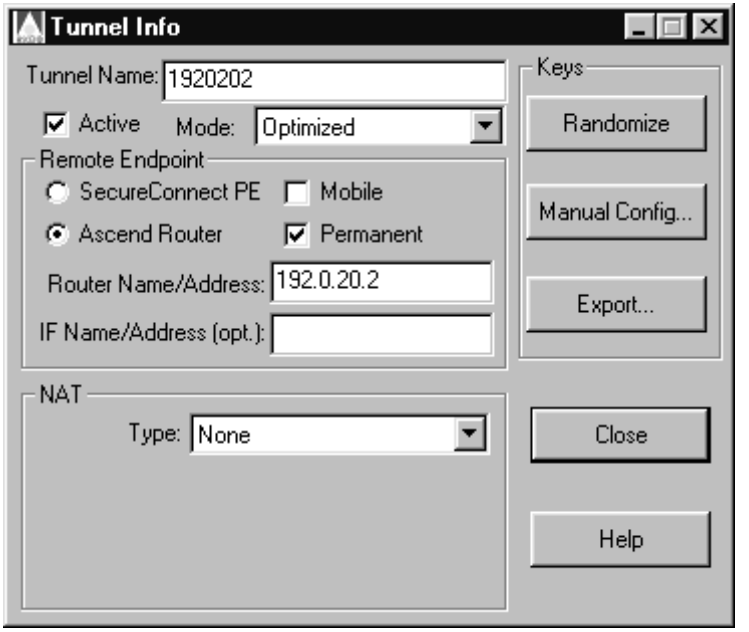


Figure 4-7. Tunnel Info fields specify a router with a permanent IP address

If you specify that the default remote tunnel endpoint is a mobile PC, the Tunnel Info dialog box appears as displayed in Figure 4-8.

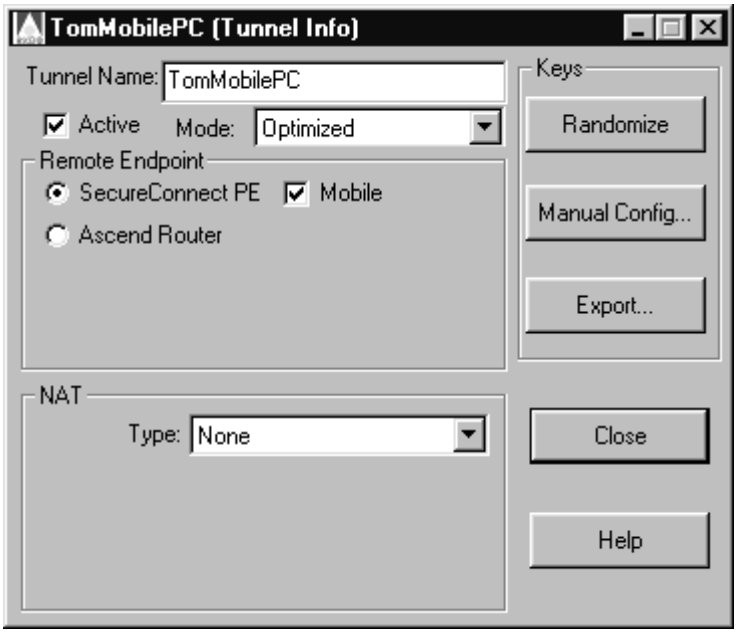


Figure 4-8. Tunnel Info fields specify a mobile PC

Specifying the type of remote tunnel endpoint machine

The remote tunnel endpoint can be either a PC running IntragyAccess SecureConnect Client software or an Ascend router. If the machine is an Ascend router, the unit must be a Pipeline model. MAX units do not support IPSec, so they cannot be the remote end of a tunnel configuration. You specify whether the machine is a PC or a router by clicking SecureConnect Client or Ascend Router in the Remote is: section of the Default Settings of New Tunnels dialog box.

Specifying whether the remote endpoint IP address is known

You can create a tunnel configuration in which the remote endpoint which has no permanent IP address. This situation might occur frequently if the remote tunnel endpoint uses an Internet Service Provider to connect to the network and the ISP provides the endpoint with a different IP address every time the user connects. If you cannot specify the remote tunnel endpoint's permanent IP address, click

Mobile in the Remote is: section of the Default Settings of New Tunnels dialog box. If you know the remote endpoint's assigned IP address, click Permanent.

Creating a default configuration that enables translation of tunnel endpoint addresses

Your default tunnel configuration might involve a private network in which the machines have been assigned addresses that cannot be used to connect over a public network. To overcome the limitation caused by private addresses, a router can use Network Address Translation (NAT) to temporarily give the machines' outbound packets a different source address. SecureConnect Manager also enables you to configure a tunnel so that a router can use a SecureConnect feature called Reverse Tunnel NAT (RTNAT). When you select this feature, a router can change the source address of incoming encrypted packets from sites that want their machines to appear to be part of a private network.

The instructions that follow explain how to create a default tunnel configuration that includes NAT or RTNAT. This section also describes how to specify the means by which a router obtains local addresses it uses to perform RTNAT translations.

More information about NAT is in "NAT (Network Address Translation)" in Chapter 3, "Exploring the SCM Interface." In addition, the Pipeline User's Guide includes an explanation of NAT. The unit's guide also includes a chapter on IP address management that describes how to set the NAT function on the unit.

RTNAT

Reverse Tunnel Network Address Translation (RTNAT) is a SecureConnect Firewall option that enables the router on which you install a firewall to translate a remote tunnel endpoint's unique IP address to a private network address. Changing the address enables the remote endpoint to access sites within the private network that are blocked to machines that are not part of the network.

For example, one of the options of a Pipeline unit's NAT feature enables you to route all inbound traffic from the remote side of the Pipeline to a default server on the local network. When you set the RTNAT feature in a tunnel configuration in the Pipeline's firewall, the Pipeline changes the source address on packets that pass through the tunnel, so the packets appear to be from the local network. The

Pipeline can route the altered packets anywhere in the local network, instead of forwarding them to the default server. Changing the packets' source address might also permit the packets to pass through internal firewalls that block traffic from outside the local network.

When you select Reverse to turn on the SecureConnect RTNAT option, the router on which you install the firewall performs the RTNAT function. If you export the firewall that includes the tunnel configuration to the remote endpoint , the machine there automatically performs NAT.

Note: Tunnels configured with the RTNAT feature can only be initiated by the remote tunnel endpoint. The local tunnel endpoint cannot initiate the tunnel connection. However, after the remote end establishes the tunnel connection, sites at the local tunnel endpoint can send encrypted packets to the remote tunnel endpoint, if the remote tunnel ruleset permits the traffic.

Specifying the NAT value for the default tunnel

To specify whether the router must perform NAT or RTNAT, select one of the values in the NAT section of the Default Settings for New Tunnels dialog box.

- Select None if the router's NAT function is on, but you do not want the router to perform NAT on tunneled packets.
- Select Same As Physical if the router must translate non-unique addresses of local tunnel endpoint machines to unique IP addresses.
- Select Reverse if you want the router to translate the unique IP address of the tunnel's remote endpoint to a local, private network address. See "Creating a new tunnel configuration" in this chapter for more information about creating a new tunnel that includes the NAT value, Reverse.

Note: Selecting None, Same As Physical or Reverse does not turn on the local router's NAT function. You must use the unit's menu or configuration interface to set the NAT function to Yes. For instructions on how to enable your unit's NAT function, see the unit's documentation. If you export a local firewall tunnel configuration in which the value of NAT is Reverse, the exported file does turn on NAT in the remote router or PC.

Specifying how the router obtains addresses for RTNAT

The values described below are not available when you create a default tunnel configuration, even if Reverse is the value you specify for NAT in the Default Settings for New Tunnels dialog box.

If you create a new tunnel based on a default configuration that includes the NAT value Reverse, you must use the Tunnel Info dialog box to specify the method by which the router can obtain a non-unique address to replace the IP address of the remote tunnel endpoint in packets that are sent through the tunnel. To access the Tunnel Info dialog box, select VPN > VPN Configuration and click New under the Tunnel Names/Associated Rulesets table.

Note: You can only select the values that relate to address pools if the router on which you are installing the firewall is a Pipeline 220. The Pipeline 50, 75, 85 and 130 models do not support address pools that the router can use for RTNAT. To configure pools on a Pipeline 220, use the Ethernet > Mod Config > WAN Options menu.

- Select Pool if you want the router to obtain a local address from the first available address pool on a Pipeline 220 unit. Do not select Pools if the router on which you install the firewall is a Pipeline 50, 75, 85, or 130.
- Select Specific Pool if you want the router to obtain a local address from a specific address pool on a Pipeline 220. After you select Specific Pool, enter the number of the pool from which the Pipeline 220 should take the first available address.
- Select Specific Name/Address if you want the router to use a specific address or domain name. After you select Specific Name/Address enter the address or name in the field that appears in the Tunnel Info dialog box. SecureConnect Manager will save the entry and include the information in the compiled firewall it sends to the router.
- Select Resolve Tunnel Name if the tunnel name is the tunnel endpoint's domain name. SecureConnect Manager resolves the domain name and saves the address in the firewall before it compiles the firewall and sends it to the router. If you select Resolve Tunnel Name, you must enter the domain name and address in the Domain Name Server that SecureConnect Manager will contact.

Creating a new tunnel configuration

This example shows how to use the example's default configuration to create a new tunnel configuration.

1. Select VPN > VPN Configuration.
2. Click New below the Tunnel Names/Associated Rulesets table.
3. Enter a name in the Tunnel Info dialog box Name field.
4. Click Close.

Creating a Main ruleset IPSec rule to enable encrypted traffic

This step in the example explains how to create an IPSec rule in a firewall's Main ruleset. The IPSec rule enables the firewall to accept encrypted VPN tunnel traffic. If the Main ruleset does not contain an IPSec rule, the firewall will block encapsulated packets created by the IPSec protocol.

You can configure a IPSec rule so that the router accepts incoming encrypted packets that contain an Encapsulating Security Payload, an Authentication Header, or both IPSec components. The category's location text boxes are labeled Local Gateways and Remote Gateways. Gateways are the machines that perform IPSec encapsulation and decapsulation. In the example, the PC running IntragyAccess SecureConnect Client software performs IPSec functions, and it is also the destination of IPSec-encapsulated packets sent by hosts on the LAN behind the Pipeline in Figure 4-5. Any of the LAN hosts might be the destination of the PC's IPSec-encapsulated packets, but the Pipeline is the gateway to that end of the tunnel.

1. Select the IPSec category.
2. Click ESP and AH.
3. Enter 192.0.20.2 in Local Gateways.
4. Enter 112.11.2.1 in Remote Gateways.

Creating tunnel rulesets

Following are examples that describe how to create tunnel rulesets. The first example shows how to create a tunnel ruleset rule if the router on which you install the firewall does not perform NAT on the tunnel packets. The second and third examples describe how to create tunnel ruleset rules when NAT is set to Same As Physical and Reverse, respectively.

Creating a tunnel ruleset if NAT is set to None

Tunnel ruleset rules determine the types of packets that SecureConnect Firewall encrypts. The actions described here create a Trusted Sites for the firewall installed on the SCF Pipeline displayed in Figure 4-5. The Pipeline does not perform NAT on outgoing packets it permits through the tunnel.

When you create a Trusted Sites rule in a tunnel ruleset, you enable the firewall to accept all encrypted packets the remote location(s) sends the local site(s). The rule also causes the SecureConnect Firewall feature to encrypt all packets the local site(s) send the remote location(s).

1. Click New beneath the Local Tunnel Rulesets list in the VPN Configuration dialog box.
2. Enter `New Ruleset` in the Name field in (LOCAL TUNNEL Ruleset).
3. Select the Trusted Sites category.
4. Click Allow All Traffic.
5. Enter `192.0.1.0/24` in Between Local.
6. Enter `112.11.2.1` in And Remote.
7. Click Close.

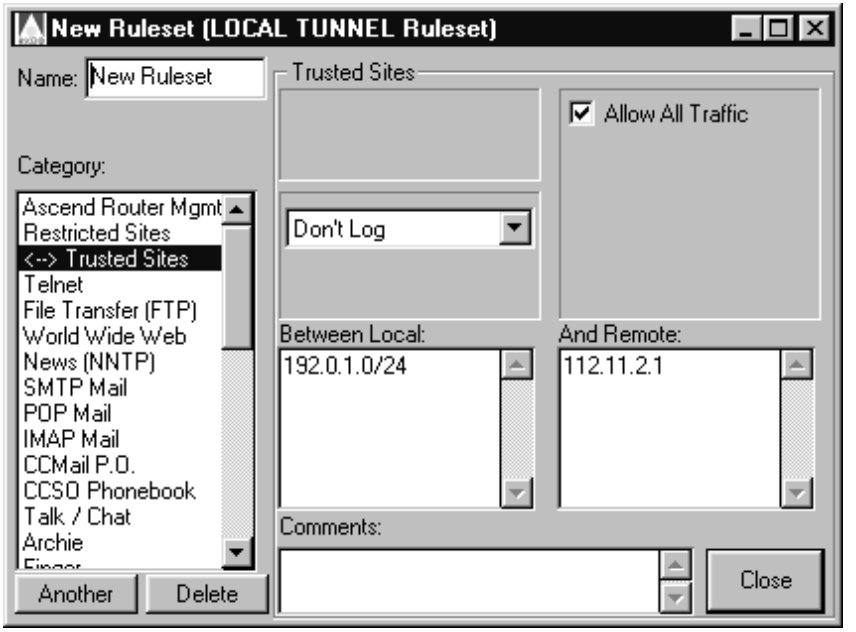


Figure 4-9. Creating the sample rule in (LOCAL TUNNEL Ruleset

Creating a tunnel ruleset if NAT is set to Same As Physical

If you specify that the value of the NAT option in the tunnel configuration is Same As Physical, follow these steps, which show how to enter the local and remote addresses in the tunnel ruleset rules. When the NAT value is Same As Physical, the router translates the source address in the local tunnel endpoint's outgoing packets, changing it from a non-unique address to a unique IP address. You should know the specific IP address that the router will use when it performs NAT, or you might know the subnet from which the router will select an IP address. Enter a specific IP address or the subnet in the local location text box.

Creating a tunnel ruleset if NAT is set to Reverse

If you specify Reverse (RTNAT), the router translates the remote tunnel endpoint's source address from a unique IP address to a local network address. When you create the tunnel ruleset rules, you might not know the address that the router will use when it performs RTNAT. For example, the remote endpoint

might receive its address from an ISP, and the ISP might assign the remote endpoint a different IP address each time it connects. For this reason, enter an asterisk (*) in the tunnel ruleset rules' remote location text boxes.

Associating a tunnel ruleset with a tunnel configuration

Associating a tunnel ruleset with the tunnel configuration enables the SecureConnect Firewall feature to determine which types of packets to permit in an encrypted VPN tunnel. This step explains how to use the VPN configuration Apply button to associate the ruleset and tunnel configuration created in the previous examples.

1. Select New Tunnel in the Name column of the VPN Configuration dialog box (Figure 4-10).
2. Select New Ruleset in the Local Tunnel Ruleset list.
3. Click Apply below the Local Tunnel Ruleset list.
4. Click the close icon.

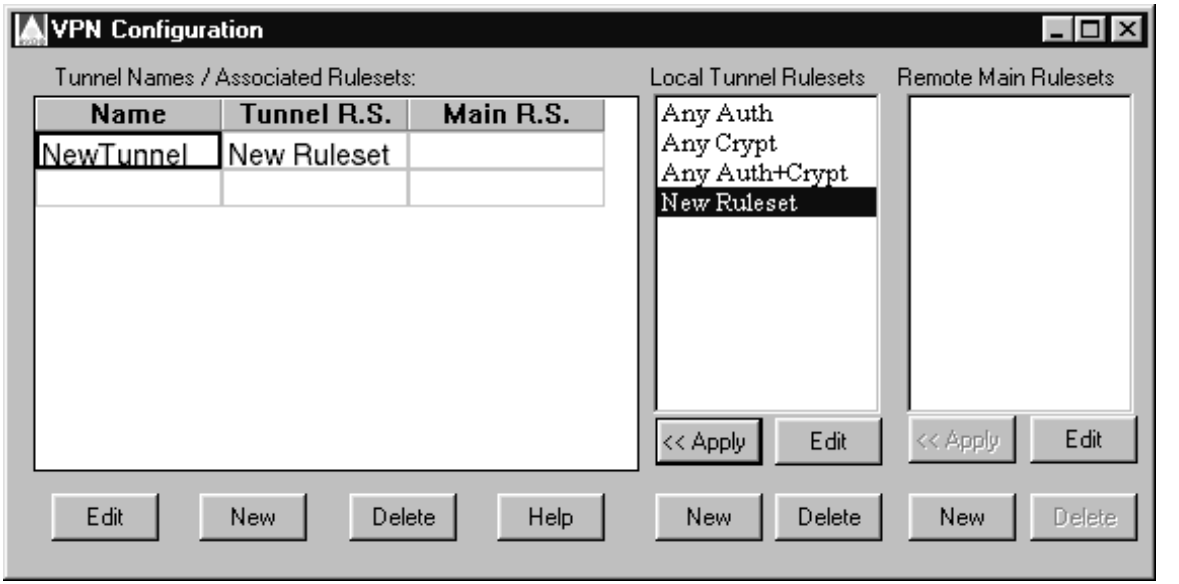


Figure 4-10. VPN Configuration dialog box with sample entries

Creating and exporting a firewall for the remote tunnel endpoint

Using the SecureConnect Manager export feature, a firewall administrator who creates the local firewall for a tunnel connection also can create the remote endpoint's tunnel configuration, tunnel ruleset, and Main ruleset. The SCM export feature makes sure there are matching tunnel configurations and rulesets at each end of the tunnel.

This example explains how to export a tunnel configuration, a tunnel ruleset and a remote Main ruleset to a file that the remote tunnel endpoint user can copy to a machine running IntragyAccess SecureConnect Client (SCC). The SCC feature enables the user to install the export file's dynamic firewall and tunnel components. The example begins with the creation of a remote Main ruleset, then shows how to use the export feature. It ends by explaining how to use SCC to install a SecureConnect firewall.

Note: The example does not describe how to create a local firewall tunnel configuration and tunnel ruleset. Creating those firewall components is covered in the previous section, "Creating local firewall tunnel configurations and rulesets" .

The example is based on the connections shown in Figure 4-11. The PC firewall permits communications with hosts on a LAN connected to a Pipeline, and with a World Wide Web server on another network. The Web server's IP address is 200.10.2.1. Traffic between the PC and the Pipeline LAN travels an encrypted VPN tunnel.

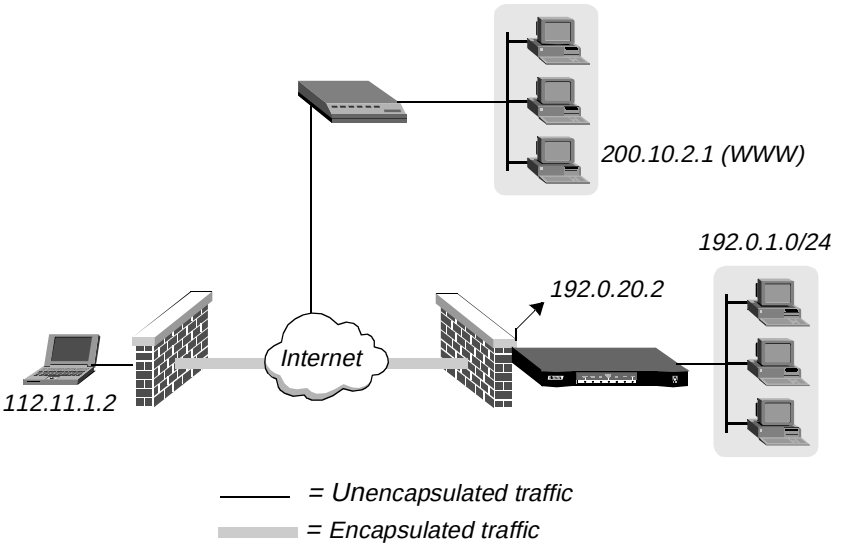


Figure 4-11. Connections permitted by Main and tunnel rulesets

Creating a remote Main ruleset for a remote tunnel endpoint

To create a remote Main firewall you can export for a remote tunnel endpoint, proceed as though you were creating the site's local firewall. Note that you do not have to enable the ruleset's IPSec rule. SCM automatically enables the IPSec rule because you only create remote Main rulesets for remote tunnel endpoints, and tunnels only work if an IPSec rule is enabled at both ends of the tunnel. This example describes how to create a Trusted Sites rule and a World Wide Web rule in a remote Main ruleset, and to associate the ruleset with a tunnel configuration.

Note: When you use the export function, it does not change any of the selections and entries in a remote Main ruleset. The export function does reverse local and remote addresses in the tunnel ruleset rules created for the local firewall. It also switches the values of the Transmit and Receive settings in the local firewall's tunnel configuration. The section "VPN > Export All Tunnels command" in Chapter 3, "Exploring the SCM Interface," describes the affect of the export function on tunnel ruleset rules and tunnel configuration settings.

To create a remote Main ruleset you can associate with the sample tunnel configuration created in the previous example, “Creating local firewall tunnel configurations and rulesets” :

1 Select VPN > VPN Configuration.

2 Select New under the Remote Main Ruleset list.

3 Enter `Remote PC` in the (REMOTE MAIN Ruleset) screen Name field (Figure 4-13).

To create a Trusted Sites rule in the remote Main ruleset:

1 Select the Trusted Sites category.

2 Click Allow All Traffic.

3 Enter `112.11.2.1` in Between Local.

4 Enter `192.0.1.0/24` in And Remote.

To create the World Wide Web rule in the remote Main ruleset:

1 Select the World Wide Web category.

2 Click Outgoing.

3 Click the category’s WWW, WAIS, Gopher and Secure WWW (SSL) options.

4 Enter `112.11.2.1` in Local Clients.

5 Enter `200.10.2.1` in Remote Servers.

6 Click Close.

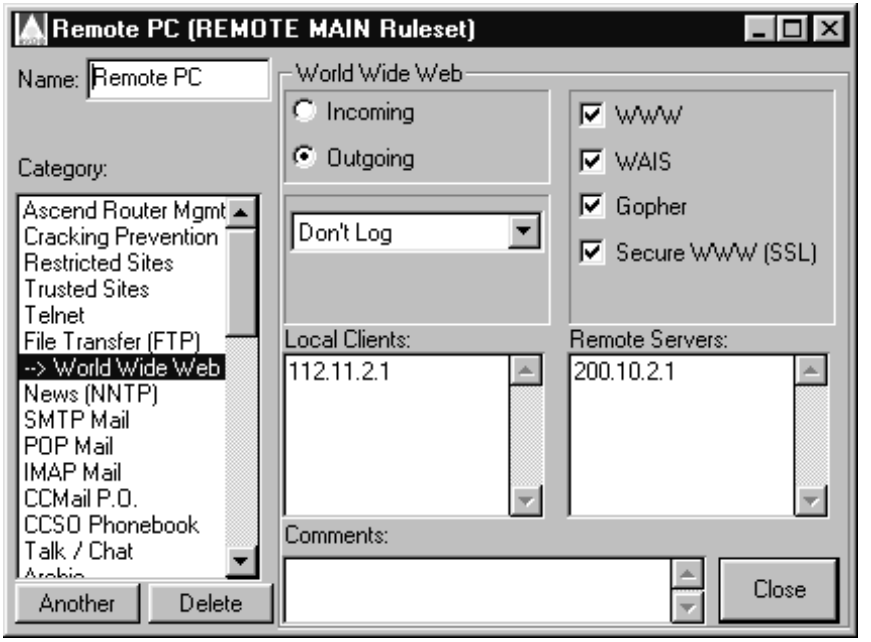


Figure 4-12. Creating a rule in the remote Main ruleset

To associate the remote Main ruleset with the tunnel:

1 Select New Tunnel in the Name column of the Tunnel Names/Associated Rulesets table.

2 Select Remote PC in the Remote Main Rulesets list.

3 Click Apply under the Remote Main Rulesets list.

4 Click the close icon button.

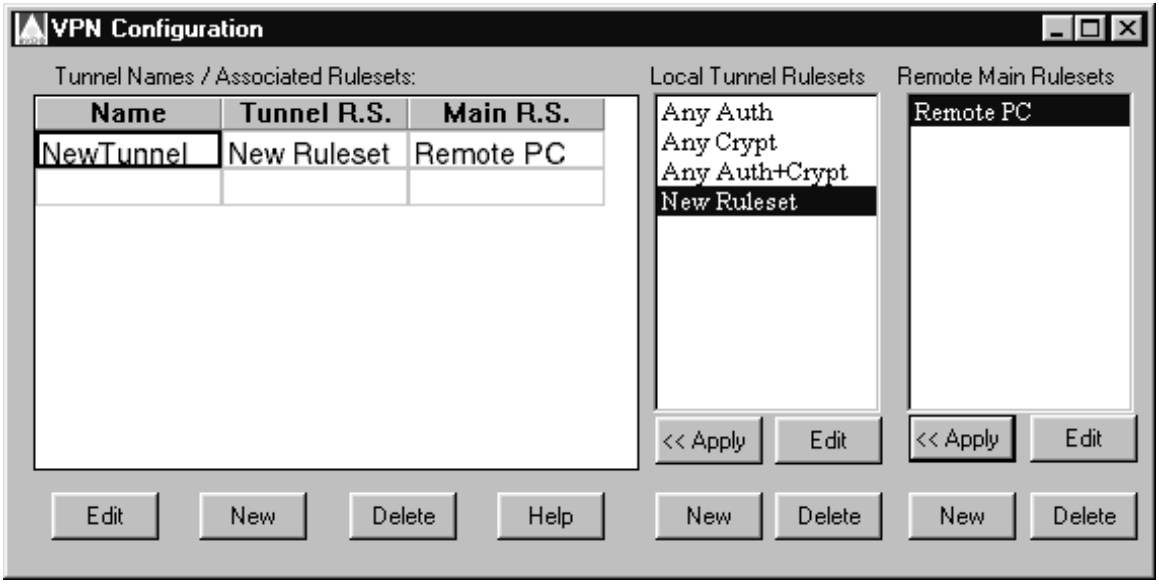


Figure 4-13. Associating remote Main ruleset with tunnel configuration

Creating export firewalls for remote tunnel endpoints

You can use the SecureConnect Manager export function to create an export file for a specific tunnel, or you can use it to create one export file for each tunnel in the firewall. SCM derives the names of the export files it creates from the names of the firewall tunnels. This example describes both methods for making export files.

When you export tunnels, you must choose the format of the file that SecureConnect Manager creates. The format must be appropriate for the type of machine on which you will copy the export file. If you want SCM to select the format for you, select the Mixed Source Binary format. SCM will format the file according the remote tunnel endpoint specified in the Tunnel Info dialog box. If you want to specify the file format yourself, select the Fwall Source format if the remote endpoint is a router, or select Fwall Binary if the machine is a PC running IntragyAccess SecureConnect Client software.

Creating an export file for a specific tunnel configuration

To create an export file based on a specific tunnel configuration, use the Export function in the Tunnel Info dialog box. For example, to create an export file based on the tunnel displayed in Figure 4-13:

1. Select VPN > VPN Configuration.
2. Select New Tunnel from the Name column in the Tunnel Rulesets/Associated Rulesets table.
3. Select Edit under the Tunnel Rulesets/Associated Rulesets table.
4. Click Export in the Tunnel Info dialog box.
5. In the Export All Tunnels to Directory dialog box, select a directory in which SCM will save the export files it creates.
6. Select the format of the export file from the list that includes, Mixed Binary, Fwall Source, and Fwall Binary.
7. Click Save.

Creating export files for all tunnel configurations

To create an export file for each of the tunnel configurations in the firewall that is open in SCM, use the Export All Tunnels function in the VPN menu.

1. Select VPN > Export All Tunnels.
2. In the Export All Tunnels to Directory dialog box, select a directory in which SCM will save the export files it creates.
3. Select the format of the export file from the list that includes, Mixed Binary, Fwall Source, and Fwall Binary.
4. Click Save.

Creating a sample firewall

SecureConnect Manager contains two sample firewalls. The firewall files are named `example1.fw` and `example2.fw`. This section explains how to create the firewall named `example1.fw`. The firewall permits wide-ranging local-to-remote access and blocks almost all remote-to-local access. The firewall

in `example2.fw` is similar, but it permits remote access to three specific local servers.

You can use `example1.fw` as a guide when you create your own firewall, or simply change the sample firewall rules' IP addresses to those of your network and save the file to your router.

Network configuration for the example firewalls

Figure 4-14 shows the router on which the sample firewall is installed and the local clients that are affected by the firewall. The router carries an IP address of 192.0.0.1 and the clients' IP addresses are 192.0.0.2 through 192.0.0.4. The remote servers in the figure represent all remote servers and are not identified by specific IP addresses.

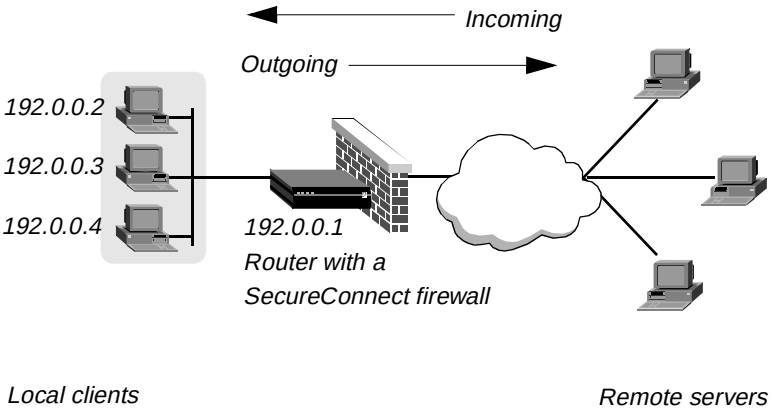


Figure 4-14. Network configuration for sample outgoing-only firewall

Outgoing-only firewall

The firewall file named `example1.fw` creates a firewall which permits many kinds of outgoing packets from any local IP addresses. The firewall blocks almost all incoming packets directed at the 192.0.0/24 network. Table 4-2 lists the SCM selections which created `example1.fw`. Note that actual IP addresses

rarely appear next to Local under the Location Options column. Most entries under Location Options contain asterisks. Asterisks indicate that this option applies to all local IP addresses.

The sample firewall does not permit outgoing packets for the following services because some are security risks and others are little used protocols. Selecting them needlessly inflates the size of the firewall.

- POP Mail POP-2
- IMAP Mail v3
- CCSO Phonebook
- Talk/Chat
- LAN Manager Name and File Printer Services
- Routing Information
- SNMP

Table 4-2. Selections that create Example 1 firewall

Categories	Category options	Direction options	Location options
Cracking Prevention	Scan Detection Reject Src Routing Anti-Spoofing	N/A	192.0.0.0/24
Restricted Sites	Don't Allow Anything	N/A	Local 192.0.0.1 Remote *
Telnet	Enable	Outgoing	Local * Remote *
File Transfer (FTP)	Enable	Outgoing	Local * Remote *

Table 4-2. Selections that create Example 1 firewall (continued) (continued)

Categories	Category options	Direction options	Location options
World Wide Web	WWW WAIS Gopher SecureWWW (SSL)	Outgoing	Local * Remote *
News (NNTP)	Enable	Outgoing	Local * Remote *
SMTP Mail	Enable	Outgoing	Local * Remote *
POP Mail	POP-3	Outgoing	Local * Remote *
IMAP Mail	v2/v4	Outgoing	Local * Remote *
Archie	Enable	Outgoing	Local * Remote *
Finger	Enable	Outgoing	Local * Remote *
Whois	Enable	Outgoing	Local * Remote *
Multimedia	RealAudio™ VDOLive™ StreamWorks™	Outgoing	Local * Remote *

Table 4-2. Selections that create Example 1 firewall (continued) (continued)

Categories	Category options	Direction options	Location options
Secure Shell	Enable	Outgoing	Local * Remote *
UUCP	Enable	Outgoing	Local * Remote *
Lan Manager (NetBIOS)	File/Printer Name Service	Outgoing	Local * Remote *
Time Services	NTP rdate daytime TSP (timed)	Outgoing	Local * Remote *
IPSec	ESP Packets AH Packets	Outgoing	Local * Remote *
Ident	Enable	Outgoing	Local * Remote *
Name Service (DNS)	Queries	Outgoing	Local * Remote *
Ping/Traceroute	Ping Traceroute	Outgoing	Local * Remote *
ICMP	Errors (in/out) Info Requests Redirect	Incoming (Only Errors) Outgoing (All options)	Local * Remote *

Tunneling with IPSec

5

This chapter describes the Internet Protocol Security protocol (IPSec), the basic construction of IP packets, the effect of IPSec encapsulation on IP packets, and the encryption algorithms you can use to perform packet encapsulation The chapter consists of the following sections:.

Introduction

Tunneling, or encapsulation, describes the ability of a SecureConnect firewall to reconfigure outgoing traffic so that it is secure, or to receive, decapsulate, and decipher incoming encapsulated traffic from a remote source. Chapter 3, “Exploring the SCM Interface,” discusses how to use the selections in the VPN menu to make a firewall’s tunnel rulesets and to configure a firewall tunnel’s encryption methods and keys.

To illustrate what tunneling is like, imagine a strange, virtually unmarked truck on a public highway. The highway on which the truck is traveling is filled with other vehicles that have windows, permitting you to see what the vehicles are transporting. The other vehicles’ markings also inform you where they are coming from and where they are going. The strange truck has no windows. On its door is a sign that says Warehouse A. Above its windshield is another sign that says Western Distribution Center, which you assume is its destination.

Suppose you know where the Western Distribution Center is located, so you drive there and arrive there as the truck backs up to a loading dock. Unfortunately, the dock is enclosed, so you cannot see the workers unload the truck’s contents. Or suppose you are following the truck when its door inadvertently opens, giving you a glimpse of the boxes inside. You can see the boxes, which are sealed with a stamp you assume is the sender’s identification, but you can’t read the stamp or the boxes’ labels. Although you have seen the contents of the truck, it is impossible to determine what the truck is distributing, who sent the contents, or to whom the contents are being delivered.

Your experience in this story is somewhat like that of a person who is snooping the Internet and encounters encapsulated IPSec data being transmitted from one gateway to another.

Benefits of tunneling

As the example illustrates, some of the essential benefits of tunneling are:

- Using a public thoroughfare rather than a private, expensive conduit to transmit traffic.

- Permitting onlookers to see where the traffic enters and exits the public thoroughfare, but hiding the ultimate source and destination of the traffic's contents.
- Enclosing the traffic's contents so they cannot be identified in transit.
- Labeling the traffic's contents so the receiver can identify the sender.

SecureConnect Firewall provides these tunneling benefits, and more, because it uses the Internet Protocol Security (IPSec) protocol to encapsulate ordinary IP packets. In very simple terms, IPSec encapsulation performs three functions that change IP packets before they are transmitted.

First, it encrypts parts of the packet, using algorithms and keys that both ends of the tunnel connection know.

Second, this encrypted payload and a header that can identify the sender are added to the packet. A header is one of the components of an IP packet. The encrypted payload secures the packet's data. The header proves, or authenticates, the sender's identity.

Third, a new header is placed in the packet. The header contains the IP addresses of the machines which send the packet to the Internet and receive it from the Internet. This header is inserted before the packet's original IP address header so that the packet's true source and destination are hidden.

IPSec tunneling

Ascend's implementation of tunneling in SecureConnect Firewalls is based on IPSec, a protocol developed by the Internet Engineering Task Force (IETF). The IETF is an open community of individuals and organizations concerned with developing and refining the Internet's architecture and protocols. IPSec is the creation of an IETF work group, whose goal is to develop a network-layer protocol that uses cryptography to provide four basic security elements for IP packets transmitted and received over the Internet. In addition, IPSec can also provide replay protection and non repudiation. The IETF IPSec Working Group

has published some elements of the IPSec security architecture as proposed standards, and others are under development and review.

Note: Ascend's implementation of IPSec for SecureConnect firewalls complies with the best practices of the IETF IPSec Working Group's IPSec protocol. Because some of the underlying elements of the protocol's architecture, such as the Encapsulating Security Payload, are in review, Ascend's implementation of IPSec might change.

What IPSec provides

The goal of the IPSec protocol is to provide the following types of security for traffic transmitted over a public network such as the Internet. For an explanation of how encapsulation of IP packets by the IPSec protocol provides these forms of security, see "How IPSec works" on page 5-7.

- Authentication, which proves that the received data is the same as the transmitted data and that the avowed sender is the actual sender.
- Confidentiality, which prevents someone other than the intended receiver from deciphering the transmitted data.
- Integrity, which proves that the received data has not been altered during transmission.
- Non repudiation, which proves that the sender did transmit the data even if he or she denies doing so.

More about the IETF

The IETF publishes the proposed standards developed by its working groups in a document called a Request For Comment (RFC). Each RFC is identified by a number. The RFC documents the IPSec Working Group has published for proposed standards are numbers 1825–1829, 2104, and 2085. Other RFC documents that have been or are related to the development of IPSec include RFCs 1321, 1810, 1851, 1852, and 1883. You can find these documents, and many other draft documents related to the IPSec Working Group's projects, at the group's web site:

`http://www.ietf.org/html.charters/ipsec-charter.html`

To obtain more information about IPSec, you can also subscribe to the working group's mailing list by sending email to:

```
ipsec-request@tis.com.
```

IP packets

Two versions of IP currently coexist. you can use IPSec to encapsulate either version's packets. IPv4 is the current standard, described in RFC 791. IPv6, a proposed standard described in RFC 1883, is the later version. It simplifies the format of the IP packet header described in the IPv4 standard. IPv6 also supports larger source and destination addresses in the IP header and additional extension headers. Each version requires that an IP packet include an IP header that contains a packet's source and destination addresses.

Packet headers

Compare the IP headers shown in Figure 5-1 and Figure 5-2 to see the difference between the formats of the IPv4 and IPv6 headers.

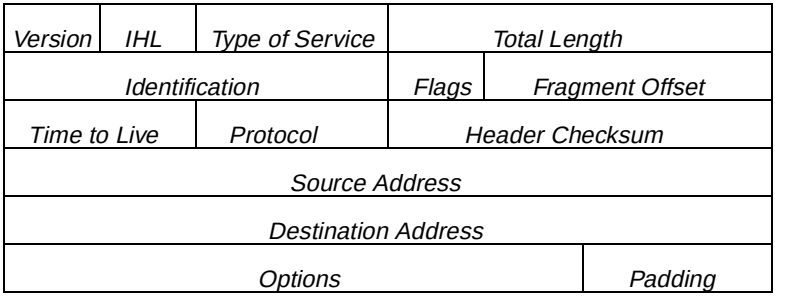


Figure 5-1. IP header defined as defined in IPv4

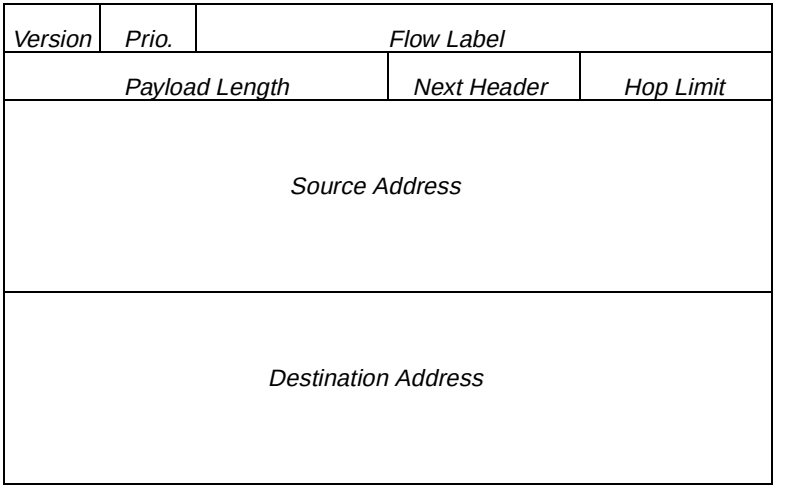


Figure 5-2. IP header as defined in IPv6

As you can see the IPv6 header is simpler than the IPv4 header, and the spaces it allocates for a packet's source and destination addresses are four times as large as those in the earlier version of the protocol. However, the changes do not affect IPSec.

Packet format

The format of the entire packet is not very different from one version of the protocol to the other. Aside from the inclusion of a place for the extended headers it supports, the IPv6 packet is essentially the same as the v4 packet, as shown in Figure 5-3.

Each format is rather like a letter. Consider the IP header as similar to an envelope on which you write the delivery and return addresses. The TCP header is like the designation *Air Mail* or *Special Delivery* that you might write on a letter to explain the means by which you want the letter delivered. This header might explain that the packet is a Transmission Control Protocol (TCP) packet of the File Transfer Protocol (FTP) type, or a UDP or ICMP packet. Following the TCP header is the data the packet contains, which corresponds with the actual letter you place in the envelope.

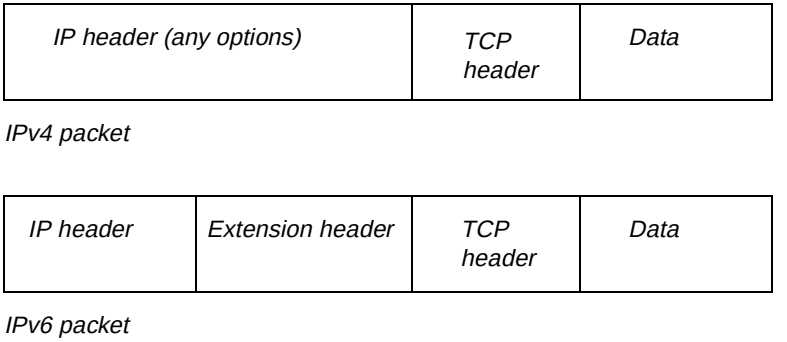


Figure 5-3. Structure of IPv4 and IPv6 packet.

How IPSec works

If you recognize the similarity between a packet and a letter, you will also see that performing IPSec encapsulation on a packet resembles placing a letter inside a larger envelope on which the addresses are more general than on the inner envelope. For example, if the addresses on the inner envelope are those of two individuals, the addresses on the outer envelope might be the companies for which the individuals work. To extend the analogy to encompass all that IPSec can do with a packet, IPSec might encrypt the contents of the letter and might add some marking to the inner envelope to prove that the person listed on the inner envelope's return address is the actual sender of the letter.

In separate functions, IPSec encapsulation can authenticate a packet's sender or encrypt a packet's data. You can configure a firewall's IPSec tunnel so that the machine with the firewall performs both security functions on the same packet. Ascend's implementation of IPSec also permits you to use a single encryption encapsulation process to authenticate your encryption of a packet's data.

IPSec transport and tunnel modes

The IPSec protocol describes two different modes of encapsulating packets. The examples in this chapter illustrate the IPSec tunnel mode, in which new IP

headers containing the addresses of a packet's source and destination gateways are inserted at the beginning of the packet to hide the true source and destinations which appear in the packet's original IP header.

Ascend also supports transport mode, which was developed for packets traversing a LAN. In transport mode, IPSec does not insert a new IP header in the packet.

SecureConnect Manager options for selecting the IPSec mode include Tunnel, Transport and Optimized. If you select Optimized, SecureConnect Manager selects the appropriate mode, based on location information in the firewall tunnel ruleset rules.

IPSec Authentication Headers

Figure 5-4 illustrates the effect of IPSec's authentication encapsulation function on an IPv4 packet. The top packet in the figure is the original IP packet, and the bottom packet is the IPsec-encapsulated packet. The encapsulation depicted in Figure 5-4 adds a new IP header and an Authentication Header (AH) in front of the original IP header. The packet's data is not encrypted.

The AH contains a message digest of the entire packet. The message digest ensures the sender is someone with whom the recipient shares a key. The digest also ensures that the data that is received has not been altered en route. A message digest is a fixed-length output derived from running data and a key through a Message Authentication Code (MAC) algorithm. The key provides the assurance that the sender is legitimate and the fact that the entire packet is used to produce the message digest ensures that the packet has not been changed. The receiver of an encapsulated packet containing an AH knows each sender's key and algorithm and applies them in a reverse process to create the received packet's message digest. The receiver drops the packet if the results do not match the expected outcome.

For information about entering keys and choosing the algorithm that will be used to create a tunnel's Authentication Headers, see Chapter 3, "Exploring the SCM Interface."

Figure 5-5 is an illustration of an Authentication Header. Compare it with Figure 5-7, which illustrates an Encapsulating Security Payload (ESP). Both IPSec components contain a Security Parameter Index (SPI), and each can

contain a Sequence Number Field. (These are explained in the section "SPI and Sequence Number Field" on page 5-13.) Notice that the ESP can also contain an Authentication Data field, as described in "Authenticating encrypted data" on page 5-12.

IPSec authentication algorithms

Ascend's implementation of IPSec supports two MAC authentication algorithms called MD5 and SHA-1. Ascend's IPSec also supports hashed versions of the two codes. The hashed versions, called HMAC-MD5 and HMAC-SHA might be more secure than the unhashed versions, because they perform a second pass of the original algorithm, and the second pass applies a key based on the data's message digest.

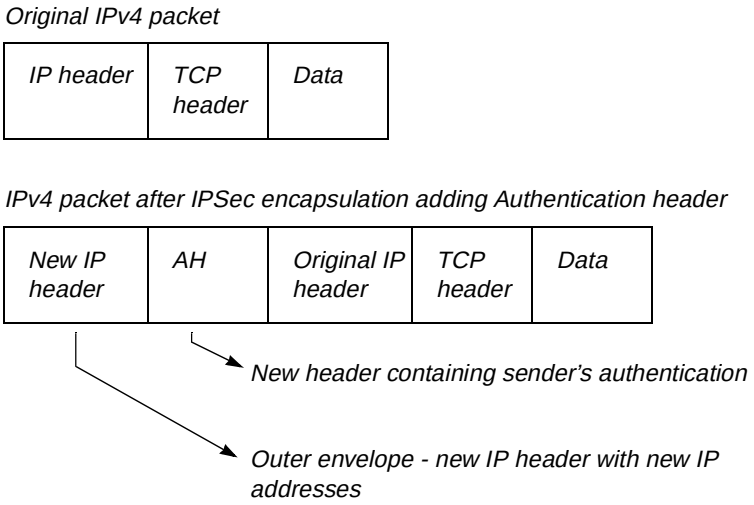


Figure 5-4. Effect of IPSec authentication encapsulation function

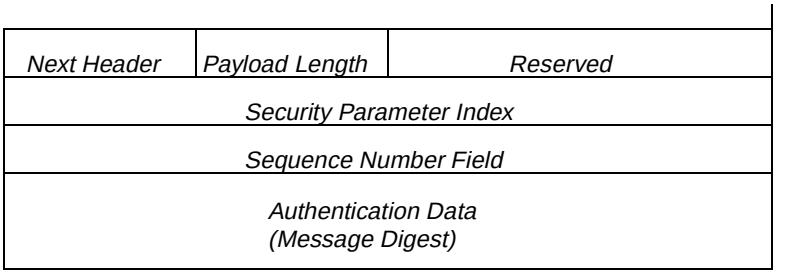


Figure 5-5. Structure of Authentication Header

IPSec Encapsulating Security Payloads

Figure 5-6 illustrates the effect of IPSec's encryption encapsulation function on an IPv6 packet. The top packet in the figure is the original IP packet and the bottom packet is the IPsec-encapsulated packet. The encapsulation depicted in Figure 5-6 adds a new IP header, a new extension header, an Encapsulating Security Payload (ESP) and an ESP trailer. The ESP, which contains the encrypted form of the packet's data, is inserted in front of the original IP header. The ESP trailer contains padding and the Next Header field. It is appended at the end of the packet.

IPSec encryption algorithms

The algorithms by which IPSec encrypts a packet's data before placing the encrypted data in the ESP are derivations of the Data Encryption Standard (DES) algorithm. Ascend Pipeline units can encrypt data with the DES algorithm and keys that are 40-bits long.

If you want to increase the strength of the encryption your Pipeline router can perform, you can obtain a software upgrade that enables your Pipeline to encrypt with 56-bit keys and the Triple DES algorithm. The Pipeline software upgrade is currently subject to United States Commerce Department restrictions on the export of encryption software. The restrictions do not apply to United States and Canadian customers, banks, and subsidiaries of United States companies located in countries outside the United States and Canada. No encryption software can be exported to Cuba, Iran, Iraq, Libya, or North Korea. Pipeline routers shipped to these countries cannot perform IPSec encryption and users in those countries cannot obtain the encryption software upgrade. For more information about DES

export restrictions, see Appendix D, “Appendix: Warranty,” and Chapter 3, “Exploring the SCM Interface.”.

DES(40) and DES use the same algorithm, but with DES(40) you can only use a 40-bit key in the encryption process. With DES you can use a 56-bit key. When you select the 3DES algorithm, packet data is encrypted three times with the DES algorithm and each pass uses a different key. 3DES provides stronger encryption than either DES(40) or DES.

You receive an error message from SecureConnect Manager if your Pipeline does not support 56-bit DES or 3DES and you attempt to install a firewall with a tunnel configuration that includes these levels of encryption.

IV Size

IV stands for Initialization Vector. An IV is placed at the beginning of the Payload Data Field, before the raw encrypted data in all ESPs. The Payload Field in a packet’s ESP is of variable length. The IPSec ESP encryption algorithms require an IV because it provides cryptographic synchronization on a packet-by-packet basis.

Note: The size of the IV can be either 32 bits or 64 bits if the encryption algorithm you select is version 1 of DES(40), DES, or 3DES. The size of the IV must be 64 bits if you select version 2 of any of the DES-based algorithms.

For more information about selecting the size of the IV, see Chapter 3, “Exploring the SCM Interface.”

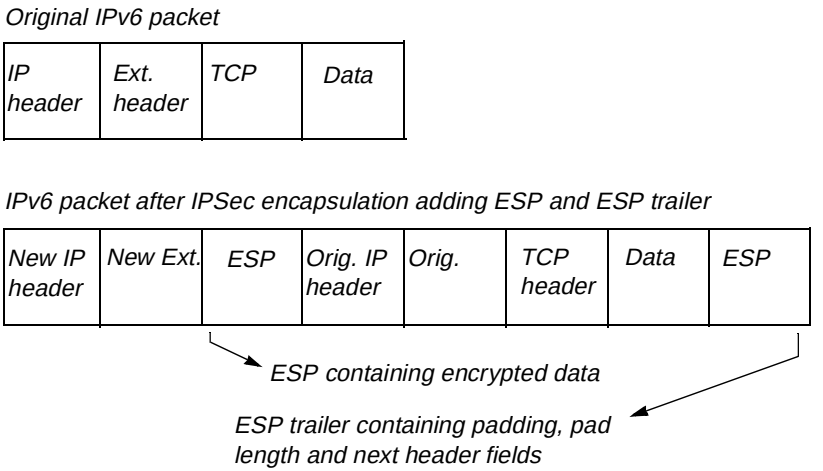


Figure 5-6. Effect of IPSec encryption encapsulation function

Authenticating encrypted data

SecureConnect Manager's list of encryption algorithm options also includes selections that enable you to authenticate the encryption-process output in the ESP. When you configure tunnel options, you can select version 2 of one of the DES encryption options, such as DES V2, then select one of the HMAC authentication algorithms, HMAC-MD5 or HMAC-SHA1. This procedure causes the IPSec protocol to apply to the ESP's encrypted data the same process that it uses for packet authentication. The ESP authentication process places the authentication data inside the ESP, but not in the portion of the ESP that contains the encrypted version of the packet's data. Figure 5-7 illustrates the ESP structure. The figure shows which parts of the ESP are covered by the authentication process described in this section, and which parts of the ESP contain encrypted data.

Note: If you authenticate the ESP, the benefit is similar to that of authenticating the entire packet. Therefore, you might forego authenticating the packet if you are going to authenticate the output of the ESP encryption process.

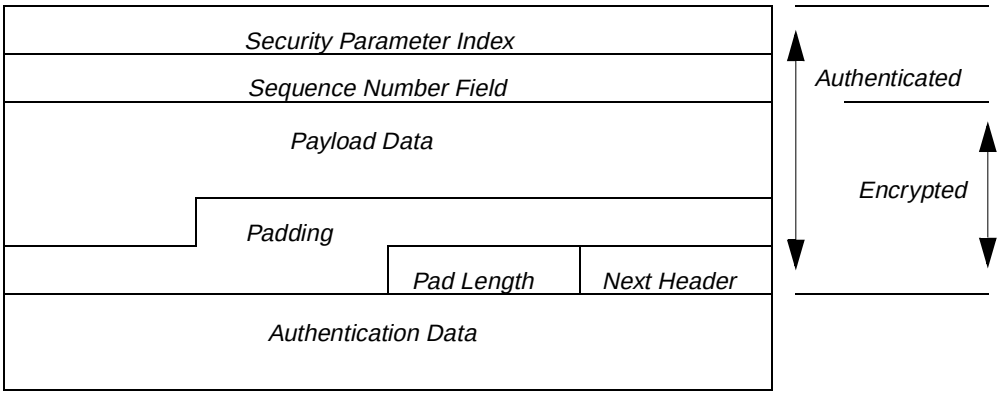


Figure 5-7. Structure of an authenticated Encapsulating Security Payload

SPI and Sequence Number Field

The illustrations of the Authentication Header and the Encapsulating Security Payload in Figure 5-5 and Figure 5-7, respectively, show that each contains a Security Parameter Index (SPI) and a Sequence Number Field.

Security Parameter Index

An SPI is a 32-bit value that is included in an AH and in an ESP. If an encapsulated packet contains both an AH and an ESP, the two SPIs are different values. The AH SPI is linked with the key and algorithm that produced the packet's authenticating message digest. The ESP SPI is linked with the algorithm and key that encrypted the packet's data. The source of a tunneled packet adds the packet's AH and ESP SPIs during encapsulation. The entity that decapsulates the packet uses the SPIs inside the packet's AH and ESP to determine the keys and the algorithms that the source used to encapsulate the packet. Therefore, each end of the tunnel must be able to access a record in which a key, an algorithm, and an SPI are associated with each other. This association is called a Security Association (SA), and the encapsulating source's SA and decapsulating receiver's SA must be identical.

Chapter 3, “Exploring the SCM Interface,” explains how to enter an SPI in a tunnel configuration.

Sequence Number Field

The Sequence Number Field in an AH or an ESP is a number that increments by one for every packet that the source sends across an IPSec tunnel. The number in the field is not used to organize packets as they arrive at the destination. It is an optional entry that provides replay protection in the event that someone intercepts a packet and tries to use it to impersonate the sender at another time.

Although the IPSec protocol says that using the sequence number for replay protection is optional, it is not a selection you can choose on a SecureConnect Manager VPN configuration screen. Ascend’s IPSec implementation always adds a sequence number in outgoing packets. It ignores the sequence number in incoming packets, because the option is a recent addition to the protocol and other implementations might not support replay protection.

Section Rulesets, FCP, and FCM

6

This chapter covers firewall section rulesets, which enable RADIUS-authenticated individuals to access locations and services from which the firewall blocks most users. The chapter also describes the Firewall Control Protocol, the Firewall Control Manager program (FCM), and the SecureConnect Server, which includes FCM, Ascend Access Control RADIUS server (AAC), Access Control Manager (ACM), and Client Firewall Loader (CFL).

Introduction

This chapter is about SecureConnect firewall section rulesets and related topics that include the Firewall Control Protocol, the Firewall Control Manager CGI script and remote user authentication. It describes why you might use section rulesets and how FCP, FCM and user authentication enable you to use section rulesets.

In addition, this chapter explains how to install the Firewall Control Manager script and how to configure entries in Ascend Access Control RADIUS files so the authentication server can authenticate a user and send the user's authorization information to the FCM. The examples that explain the Access Control file entries are also applicable if you use a different RADIUS server for user authentication. Any RADIUS server will support FCP and FCM if you install the Ascend Access Control dictionary of user attributes in the RADIUS server's directory.

Firewall Control Manager, Ascend Access Control and Access Control Manager, an interface for configuring entries in Access Control data files, are components of the SecureConnect Server. The SecureConnect Server is included on the SecureConnect Manager CD ROM and you can use a simple InstallShield program to install all of the server components on one host. Installation instructions for the SecureConnect Server are in "Installing the SecureConnect Server programs" on page 6-19.

Providing network access for special users

With a manageable set of firewall rules, a firewall administrator can control network access, but some individuals, or groups, need exceptional access to sites that are blocked by rules that apply to the rest of the users.

Consider what administrators must do to answer individuals' or groups' requests for exceptions to the rules that control network access. They add rule after rule to static firewall rulesets, until it is an interlocked construction that ultimately resembles a skyscraper built of children's blocks. The building might begin with a solid base, but it usually winds up permanently full of holes and odd abutments that cannot be filled in or smoothed over.

One approach: Dynamic firewalls

Dynamic firewall rules are superior to static rules because they control access by temporarily opening the firewall to permit approved traffic and closing it when the approved session is ended. This eliminates the permanent effect that exceptions have on the integrity of the firewall. Still, administrators of dynamic firewall solutions such as the original version of SecureConnect, must deal with exceptions by adding IP addresses to existing rules or by creating additional rules for a single category or protocol.

For example, suppose an administrator of a SecureConnect firewall that does not support section rulesets creates an FTP rule that permits any IP address to access the company's public FTP server. The company also has another FTP server that only the company's salespeople should be able to access. The administrator could provide the access salespeople require by creating another SecureConnect FTP rule. To create the rule, the administrator could enter in its remote locations list all the IP addresses that salespeople may use to initiate an incoming FTP session. However, the IP addresses of mobile salespeople change frequently, the administrator constantly has to update the ruleset.

A better approach: SecureConnect firewall section rulesets

SecureConnect Manager's section rulesets provide a better solution. The administrator can create a Main ruleset that does not need to be changed to accommodate user exceptions to normal access. Instead, the administrator handles the exceptions by creating a section ruleset that contains a dormant *salesperson-only* FTP rule. The section rule permits connections to the sales FTP server from locations that the router receives from an agent such as Firewall Control Manager, after the salespeople authenticate themselves. A Firewall Control Protocol (FCP) agent generally receives the values it sends in FCP messages from an authentication server. The dormant section's rule contains a blank where a location or port number usually appears, and the SecureConnect router temporarily completes the rule by using information received from the agent.

The information the agent sends the router arrives in an FCP message. For the duration of a user's connection, the information from the FCP message stays in the rule. When the connection ends, the rule becomes dormant again.

Using section rulesets to design a solution

You should create section rulesets to handle the exceptional access needs of particular users or groups. You should not create a personalized firewall section for each user who seeks access through the firewall. Be judicious and let your security policy guide you in creating a Main firewall ruleset that accommodates the access needs of a typical user. Then create sections for users and groups that require something more than the access permitted by the Main firewall ruleset. Remember that users who can activate section rulesets are also permitted all the access provided by the Main ruleset, so you do not have to duplicate the Main ruleset's rules within a section's ruleset.

Table 4-2 in Chapter 4, "Creating a SecureConnect firewall," might help you create a firewall if you have not previously used SecureConnect MaManager. The table lists SecureConnect selections for creating a generic firewall that allows most outgoing packets and blocks most incoming packets.

Firewall Control Protocol

Firewall Control Protocol (FCP) enables you to use a section ruleset like the one permits the sales group to access its FTP server. FCP defines a new set of router SNMP (Simple Network Management Protocol) variables that an agent, such as the Ascend Firewall Control Manager (FCM), can to send to SecureConnect firewall routers. FCM uses SNMP request packets to deliver the variables to a router. When a router receives the requests, it uses the variable's values to dynamically, and temporarily, activate a section ruleset and populate its rules with IP addresses or port numbers.

The SNMP variables and their values are stored in RADIUS user profiles as special attribute/value pairs called Ascend-FCP-Parameters. When you create a user profile, you can enter values for Ascend-FCP-Parameter attributes that specify which router the Firewall Control Manager should contact, the section ruleset that the router activates, and the IP addresses and ports that the router inserts in the section rules. FCM receives the attribute/value pairs from the RADIUS server when a user authenticates. Table 6-1 lists the variables that can be sent in FCP packets, and describes what the variables provide to a router with SecureConnect Firewall section rulesets.

Table 6-1. Ascend-FCP-Parameter variables FCM sends in FCP packets

Name	Description
agnt	Name of the router to which FCM sends FCP packets.
rule	Name of a SecureConnect firewall section ruleset rule that can be altered by the contents of the FCP packet.
lcad	IP address of a local client or server that the section rule should incorporate.
lcam	IP address mask of a local network that the section rule should incorporate.
lcpo	Port number of a local host or server that the section rule should incorporate, or the first number in a range of ports.
lcpm	Last port in a range that begins with the local host or server port number specified by the `lcpo` variable.
rmad	IP address of a remote client or server that the section rule should incorporate.
rmam	IP address mask of a remote network that the section rule should incorporate.
rmpo	Port number of a remote host or server that the section rule should incorporate, or the first number in a range of ports.
rmpm	Last port in a range that begins with the remote host or server port number specified by the `lcpo` variable.
rtad	IP address of a host sharing the network with your router. The `rtad` IP address enables you to select the firewall you want to affect. Firewalls are installed on interfaces, and `rtad` forces packets to be routed via the interface through which packets are sent to the `rtad` IP address.

Table 6-1. Ascend-FCP-Parameter variables FCM sends in FCP packets

Name	Description
time	Length of time in seconds that the altered SecureConnect rule remains in effect.

FCP support for authentication of SNMP packets

SNMP is a powerful tool for changing the operational state and behavior of systems such as Ascend routers. But the SNMP protocol is insecure and does not include a provision for authenticating packets that appear to have been sent by an agent such as Firewall Control Manager. FCP establishes a way for SecureConnect Firewall routers to authenticate SNMP packets. However, FCP does not require that a router authenticate SNMP requests, even though it is a very important aid to maintaining security.

Ascend routers are configured so that SNMP management stations that can send the routers SNMP packets are assigned one of two community names in the router's Ethernet > Mod config > SNMP Options profile. The two community parameters are Read_comm and R/W_comm. Stations that can send SNMP packets that change a router's operation are assigned the R/W_comm community name. Each community name parameter has a value.

FCP establishes a new format for the R/W_comm community-name value in SNMP requests. The new format enables a router to authenticate the agent that sent the request. The old format of the R/W_comm community-name value is still valid, but routers have no means of authenticating the sender of the packet if the value is written in the old format. For security, all FCP packets must contain the new format of the R/W_comm community-name value, so a router can authenticate the FCP agent that sent them.

The new format for the R/W_comm community-name value has three components: a name, a vertical bar and a secret. Following lines compare the old and new formats for the R/W_comm community name value.

```
R/W_comm=name
```

```
R/W_comm=name|secret
```

Note: The vertical bar is a component of the format, and you must use it when you create an it when you create an R/W_comm community name value in the format established by FCP. Usually when you see a vertical bar in Ascend documentation, it indicates that what follows is an exclusive option. See "Documentation conventions" in the chapter called, "About this guide."

"How FCM determines remote addresses to send in FCP packets" on page 6-19 describes two methods for ensuring that a router will authenticate FCP packets sent by Firewall Control manager.

Firewall Control Manager

FCM is a CGI script you can install on a Windows NT Web server. The FCM script is a RADIUS authentication-server client that displays HTML forms, as shown in (Figure 6-1), in which users can submit their names and passwords to a RADIUS server and receive authentication or challenges from the server. You can easily edit FCM's simple HTML pages to add graphics, backgrounds, and HTML text.

The FCM script is also an FCP agent for SecureConnect routers. FCM sends the routers FCP packets containing user authorizations FCM receives from RADIUS. The user authorizations are the values of Ascend-FCP-Parameter attributes in authenticated users' RADIUS profiles. The Ascend-FCP-Parameter attribute values are the FCP variables listed in Table . The router incorporates the RADIUS authorization information into dormant firewall section rules.

FCM can send authorization attributes to a router if the router is named in a RADIUS user profile's Ascend-FCP-Parameter attribute or if the router's IP address or domain name is the value of DefaultAgentName in `fcm.cfg`, the FCM configuration file. (See "Installing the SecureConnect Server programs" on page 6-19.)

You can use FCM as a user entry interface for any RADIUS application, but it was designed to work with Ascend's Access Control RADIUS server and

SecureConnect products. Each is enhanced by the ability of the Firewall Control Manager to provide a bridge between the de facto standard user authentication and authorization protocol, RADIUS, and the integrated dynamic router firewall feature.

Figure 6-1. Example of FCM HTML document for user authentication.

Configuring RADIUS for FCM and FCP

To use section rulesets, you must create a RADIUS `clients` file entry for FCM and a user profile for each user who is to be authenticated through FCM. You can use a text editor or the Access Control Manager interface to create the entries in the `clients` and `users` files. “Installing the SecureConnect Server programs” on page 6-19 contains instructions for installing Ascend Access Control

RADIUS server and Access Control Manager. If you install Secure Connect Server you will also install examples of Access Control `clients` and `users` files you can use as the basis for creating your own RADIUS server data files.

Creating a clients file entry for FCM

Since FCM is a RADIUS client you must create an entry for FCM in the RADIUS server's `clients` file. All RADIUS configuration files are constructed of plain text that is saved in a format like that of a `.txt` file created by a word processor. You can open the `clients` file in a text editor to create client entries or you can use the Access Control Manager interface to create the entries.

RADIUS servers other than Ascend Access Control require that a `clients` file entry contain values for a Client Name field and a Key field. (Access Control calls the Client Name field the System Name field.)

The value you enter for the field called Client Name, or System Name, is the client's IP address or domain name. The value you enter for the Key field is a secret with which RADIUS can authenticate the client.

If you place vendor-specific attributes, such as Ascend-FCP-Parameter, in user profiles, RADIUS also requires that you enter a value in the entry's Type field. The value of the field identifies the vendor that manufactured the client and created the user profile attribute. For example, the `clients` file entry for FCM must include a Type field value of `Ascend-nas` so Ascend Access Control will send FCM Ascend-FCP-Parameter values.

Following is the format of a `clients` file entry, and an example of an entry that you can use for the Firewall Control Manager. In the line that shows the format of a file entry, `System Name` is one field.

```
System Name Key Type Version Prefix
FCM iclda type=ascend:nas 1
```

Creating a user profile that can activate a section ruleset

Ascend created the Ascend-FCP-Parameter attribute and added it to the Access Control RADIUS dictionary so the Access Control RADIUS server could send

FCM authorization attributes that could affect a firewall rule. To create a user profile that can change the behavior of a router's firewall, you must include Ascend-FCP-Parameters in the profile's reply-item lines (that is, the indented lines that follow the first line, as described in Appendix C, "Appendix: RADIUS.").

Table 6-2 contains a list of the Ascend-FCP-Parameter attribute values you can enter in a user profile. They are the same as the SNMP variables in Table 6-1.

Adding the Ascend-FCP-Parameter attribute to a RADIUS dictionary

The Ascend-FCP-Parameter attribute was added to the Ascend Access Control dictionary in version 1.0Ai3. If your copy of Ascend Access Control predates version 1.0Ai3 you can obtain the latest version of the dictionary from the Ascend Access Control Web site and copy the file into your Access Control data directory.

If you are using another version of RADIUS you can add the Ascend-FCP-Parameter attribute to your `dictionary` file. Vendor-developed attributes such as Ascend-FCP-Parameter can be added to the dictionary by using the Vendor-Specific attribute number (26) as described in the RADIUS protocol. Consult your RADIUS documentation to find out how to add the Ascend-FCP-Parameter to your RADIUS `dictionary` file.

Following is the format of the Ascend Access Control dictionary file entry for the attribute. Your RADIUS dictionary file probably uses a different format and might require that you drop the leading tag (`Ascend.attr`.

```
# Ascend Firewall Control Protocol (FCP) Parameter
Ascend.attr Ascend-FCP-Parameter 119 string (*, 0)
```

Sample profile containing the Ascend-FCP-Parameter

Following is an example of a complete user profile that contains Ascend-FCP-Parameter attribute values for changing the behavior of a firewall.

```
grape  Authentication-Type=ACE,
    Ascend-FCP-Parameter="agnt=stein;comm=write|sowtgdbc",
    Ascend-FCP-Parameter="rule=teltowww",
```

```
Ascend-FCP-Parameter="lcad=137.57.8.8",
Ascend-FCP-Parameter="lcpo=21",
Ascend-FCP-Parameter="lcpm=80"
```

Note that you can enter more than one value for the Ascend-FCP-Parameter attribute in a user profile, and you can enter multiple values on one line. Also note that an Ascend-FCP-Parameter attribute's values are surrounded by quotation marks unless you enter two values on one line, in which case the pair of values is enclosed in quotation marks.

For example, the following line contains two values for the Ascend-FCP-Parameter attribute. The attribute/value pairs, `agnt=stein` and `comm=write|sowtgdc`, are separated by a semicolon:

```
Ascend-FCP-Parameter="agnt=stein;comm=write|sowtgdbc",
```

The Ascend-FCP-Parameter attribute values in this user's profile will cause changes in the behavior of the firewall on the router to which FCM sends an FCP message containing the profile's reply-items. The `agnt` value (`stein`) specifies the router to which FCM will send the message. The `comm` value (`write|sowtgdbc`) specifies the secret FCM will include in the FCP packets so that the router stein can authenticate the packets. Following are the ways that the behavior of Stein's firewall will change when the router receives the FCP packets:

- `Ascend-FCP-Parameter="rule=teltowww"`, activates a firewall section ruleset named teltowww.
- `Ascend-FCP-Parameter="lcad=137.57.8.8",` enters the IP address 137.57.8.8 in the local text boxes of the ruleset's enabled rules. This causes the firewall to pass incoming packets described by the enabled rules if the packets are destined for 137. 57.8.8.
- Together, `Ascend-FCP-Parameter="lcpo=21"` and `Ascend-FCP-Parameter="lcpm=80"` defines the ruleset's enabled rules. They specify that the firewall passes packets destined for 137.57.8.8 if the destination port numbers in the packets fall between, or include, ports 21 and 80.

`lcad` and `rmad` location information in user profiles

The router interface on which a firewall is installed determines whether the location of the remote user who authenticates by means of FCM should be the local or remote site in a section's rules. Pay close attention to IP addresses you enter as the Ascend-FCP-Parameter attribute's local address (`lcad`) and remote address (`rmad`) values. For example, the IP address of a user who contacts an ISP to gain Internet access should be the Ascend-FCP-Parameter attribute's `lcad` value, but the IP address of a user contacting a network via the Internet should be the attribute's `rmad` value.

FCM assumes that the user's location is the remote address that should be inserted in a section's rules, so you might have to override FCM's assumption by including a line such as the following in a user's profile

```
Ascend-FCP-Parameter = "lcad=user's location",
```

To help you determine whether or not the include such a line in a user profile you should consider the following questions before you create the user's profile.

- Where is the firewall in relation to the router, or on what router interface is the firewall installed?
- On the basis of the firewall's location on the router, is the dial-in user local or remote?
- What IP address should be the value of the firewall rule's local address?
- What IP address should be the value of the firewall rule's remote address?

"How FCM interprets user profile reply-item information" on page 6-18contains additional information you should know about using the `lcad` and `rmad` variables in user profiles.

rmad and rtad

You can install more than one firewall on a router because routers can have more than one interface and firewalls are installed on router interfaces. Usually the router uses the value of the `rmad` variable to determine which firewall the FCP packets it receives from FCM is meant to affect. The router looks at the location provided by the `rmad` variable and finds the interface through which it would route packets to that location. It assumes that the firewall on that interface contains the section ruleset for which the FCP packets are meant.

If the firewall is not installed on the interface through which the router would send packets to the `rmad` location, you can make the router search for a different interface by including the `rtad` variable in a user's profile. The router then uses the `rtad` address instead of the `rmad` address to find the interface that contains the firewall section ruleset you want to activate. If you do not use `rtad` to force the router to search for a different interface, the router will be unable to find the rule, or rules, referred to in the user's profile. When the router cannot find the correct firewall, it sends SNMP error messages to that effect. Figure 6-2 illustrates the use of `rtad`. Enter the IP address of the `rtad` location in the user's profile to direct the router to select the correct firewall.

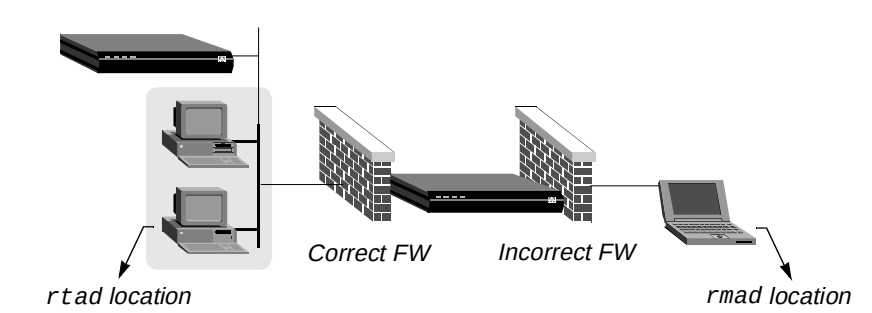


Figure 6-2. Use of `rtad` variable to cause router to select correct firewall.

Using the group specifier to activate multiple firewall sections

You can assign each Ascend-FCP-Parameter attribute value in a user profile an optional group specifier so that a single user profile can generate FCP messages that affect the behavior of multiple section rulesets in a router's firewall.

FCM prepares separate FCP messages on the basis of the value of the group specifier. All attribute values that you do not assign a group specifier are sent to the router in another FCP transaction.

Group names must be alphanumeric, can contain no more than 31 characters, and are not case-sensitive. The order of the Ascend-FCP-Parameter attribute values within the user profile is not significant, unless you create conflicting entries, in which case the last entry governs.

Following is an example that shows the addition of a group specifier. It shows that two FCP variable/value pairs, `sect=internalweb` and `time=3600` belong to group A.

```
Ascend-FCP-Parameter = “group=A;sect=internalweb;time=3600”
```

The group name `common` is reserved. You can assign the group specifier `common` to any attributes whose values you want all the groups in the user profile to share. For example, if the user profile contains attribute values with the specifiers `A`, `B`, and `C` and you want the value of each group's `time` variable to be 3000, you can enter the following line in the user profile:

```
Ascend-FCP-Parameter = “group=common;time=3000”,
```

This replaces the following three lines in the user profile:

```
Ascend-FCP-Parameter = “group=A;time=3000”,
Ascend-FCP-Parameter = “group=B;time=3000”,
Ascend-FCP-Parameter = “group=C;time=3000”,
```

Each group, except the group named `common,` generates an FCP transaction. This includes the unnamed group for attributes that have not been assigned a group specifier. Following is a list of the values that FCM assembles for an FCP transaction based on a shared group specifier:

- The default `agnt` value found in the `fcm.cfg` file
- The default `comm` value found in the `fcm.cfg` file
- The default `rmad` value found in the `fcm.cfg` file
- The default `lcad` value found in the `fcm.cfg` file
- All values from the group named `common`
- All values from the specified group

The value for any variable assigned the group name `common` overrides any default values obtained from the `fcm.cfg` file. The value for a given variable in a specific group overrides any value for the same variable that is assigned the group name `common` group or any of the `fcm.cfg` defaults.

As an example, assume the user's IP address is 12.23.34.45, and that FCM's configuration file `fcm.cgf` contains entries that specify the following default values:

```
    DefaultAgentName=123.234.45.56
    DefaultCommunityString=write|somekey
```

Also, assume that the user's RADIUS profile is:

```
charlie   Password = "chan"
    Ascend-FCP-Parameter = "group=1;lcad=11.22.33.44",
    Ascend-FCP-Parameter = "group=1;lcam=255.255.255.0",
    Ascend-FCP-Parameter = "group=1;time=7200",
    Ascend-FCP-Parameter = "group=common;agnt=54.43.32.21",
    Ascend-FCP-Parameter = "group=common;comm=write|key",
    Ascend-FCP-Parameter = "group=common;sect=internalweb",
    Ascend-FCP-Parameter = "group=common;time=3600",
    Ascend-FCP-Parameter = "group=XXX;lcad=44.33.22.11",
    Ascend-FCP-Parameter = "group=XXX;sect=stdftp",
    Ascend-FCP-Parameter = "group=XXX;opts=someoptions"
```

Table 6-2 lists the information that FCM receives from the user profile and the `fcm.cfg` file.

Table 6-2. Sources of FCM information for FCP messages

Group specifier or Default	Variable	Value
Default (from `fcm.cfg`)	DefaultAgentName	123.234.45.56
Default (from `fcm.cfg`)	DefaultCommunityString	write|key
Default (from `fcm.cfg`)	rmad	12.23.24.45
Default (from `fcm.cfg`)	lcad	12.23.24.45
Common (from profile)	agnt	54.43.32.21
Common (from profile)	comm	write|key

Table 6-2. Sources of FCM information for FCP messages (continued)

Group specifier or Default	Variable	Value
Common (from profile)	rule	internalweb
Common (from profile)	time	3600
Group 1 (from profile)	lcad	11.22.33.44
Group 1 (from profile)	lcam	255.255.255.0
Group 1 (from profile)	time	7200
Group XXX (from profile)	lcad	44.33.22.11
Group XXX (from profile)	sect	stdftp

After FCM accumulates all the information in Table 6-2, it uses it to prepare two FCP messages and sends the messages to the SecureConnect router at IP address 54.43.32.21. When the router receives the messages it changes its firewall by activating two section rulesets, inserting various addresses in the sections' rules, and setting timeout values for the user's sessions.

Table 6-3. Contents of FCP messages based on Table 6-2

Contents of FCP message based on Group 1 specifier and Defaults	Contents of FCP message based on Group XXX specifier and Defaults
agnt=54.43.32.21	agnt=54.43.32.21
comm=write|key	comm=write|key
rmad=12.23.24.45	rmad=12.23.24.45
sect=internalweb	sect=stdftp
lcad=11.22.33.44	lcad=44.33.22.11
lcam=255.255.255.0	time=3600

Table 6-3. Contents of FCP messages based on Table 6-2 (continued)

Contents of FCP message based on Group 1 specifier and Defaults	Contents of FCP message based on Group XXX specifier and Defaults
time=7200	

Creating multiple profiles for the same user

You can create multiple profiles for a single user, but you have to distinguish each profile by creating a different value for the username or password attribute for each profile. Then the information the user submits for authentication determines which profile's Ascend-FCP-Parameter values the RADIUS server sends to FCM.

If your reason for creating multiple profiles is that you want the user profile attributes to affect different sections in a firewall, the group specifier feature described in "Use of rtad variable to cause router to select correct firewall.," provides a simpler method.

Multiple users affecting the same firewall

Multiple users can affect the same firewall section ruleset simultaneously. SecureConnect Firewall creates a new group of firewall rules for each user when more than one authenticated user causes FCM to send FCP packets to the same firewall on the router. Section rules are associated with each user's address, so the rules that affect the first user are not changed by the FCP packets that contain the atribute values for a subsequent user. Timeouts only affect the user whose profile made the change in the firewall's rules. Each user is bound by his or her own timeout value.

What is the Ascend-Remote-FW attribute?

Ascend-Remote-FW is another FCP-related attribute you can add to the RADIUS dictionary. You can insert the Ascend-Remote-FW attribute/value pair in a user's profile if the user's PC has SecureConnect Client installed. The attribute's value is a string that contains the name of a firewall file that you create with SecureConnect Manager and save on the server that is running FCM. The string

you enter as the name of the firewall is the one you enter when you use SecureConnect Manager to save the firewall source file.

Ascend-Remote-FW is a vendor-specific attribute created by Ascend. It only appears in the Ascend Access Control dictionary so you have to add it if you are using a different RADIUS server. To do so, see your RADIUS documentation. Following is the way the Ascend-Remote-FW attribute appears in the Access Control `dictionary` file.

```
Ascend.attr Ascend-Remote-FW 114 string (*, 0)
```

When FCM receives the Ascend-Remote-FW reply-item from the RADIUS server, it searches for the firewall on the FCM server. If FCM finds the firewall file, it calls the program called Client Firewall Loader (CFL). CFL automatically loads the named firewall onto the remote user's SecureConnect PC. (CFL is part of the SecureConnect Server suite of programs discussed in "Installing the SecureConnect Server programs" on page 6-19). If FCM cannot find the firewall file it sends an error message. ("FCM and SNMP error messages" on page 6-34 explains FCM error messages.)

CFL sends the user's SecureConnect Client machine a firewall that can include a Main firewall ruleset or a Main ruleset and a tunnel configuration. When requesting authentication, the user should use a secure protocol such as SSL to contact the FCM Web server to download a firewall. CFL is explained in "Before you install SecureConnect Server" on page 6-20.

How FCM interprets user profile reply-item information

If you know how FCM handles the information it receives, and understand the assumptions that FCM follows if it does not receive pieces of information, you can more readily decide what Ascend-FCP-Parameter attribute values you should place in user profiles.

How FCM determines which router to send FCP packets

When you install FCM ,you can specify default values for the router that FCM will contact and for the secret by which the router can authenticate FCM's FCP packets. The default FCM values are saved in the FCM configuration file called `fcm.cfg`. (Defining FCM defaults is described in "Installing the SecureConnect Server programs" on page 6-19.)

For example, if you set a default value for the router and the secret, you could eliminate the following line from the sample user profile:

```
Ascend-FCP-Parameter="agnt=stein;comm=write|sowtgdbc",
```

User profiles do not need such a line if FCM is supposed to send the profile's Ascend-FCP-Parameter reply-items to FCM's default router. If the reply-items are to be sent to a router that is not listed as the FCM default, the profile must contain the `agnt` and `comm` values.

How FCM determines remote addresses to send in FCP packets

FCM checks the information it receives from the authentication server to determine whether it includes a value for the Ascend-FCP-Parameter's `rmad` variable. If the server does not send a value for that variable because it doesn't appear in the user's profile, FCM assumes that the authenticating user's IP address is the value of `rmad` and sends `rmad = user's location` to the router in an FCP message. The IP address or domain name a router receives as the value for the `rmad` variable is what the router inserts into the Remote Client or Remote Server location of the rules in a firewall section ruleset. For example, if a user profile contains the line shown below, FCP sends the IP address 157.73.8.8 to the router, and the router inserts that IP address into the section ruleset's rules.

Ascend-FCP-Parameter="rmad=157.73.8.8"

If you do not include a line like this in a user profile, and if you do not want the user's location to be entered in a section ruleset's rules, you can enter a remote address in the section ruleset rules' Remote Clients or Remote Servers box when you create the firewall.

Installing the SecureConnect Server programs

This section contains instruction for installing SecureConnect Server programs.

The SecureConnect Manager CD-ROM contains SecureConnect Server, the suite of programs that includes Ascend Access Control RADIUS server, Access Control Manager, and Firewall Control Manager. The CD-ROM includes an InstallShield program you can use to install any or all of the SecureConnect

Server's programs on a PC running Windows NT 4.0. If you wish, you can install all of the SecureConnect Server programs and SecureConnect Manager on the same machine.

Before you install SecureConnect Server

Before you begin to install the programs of the SecureConnect Server, make sure that the target machine has a web server installed and that you are prepared to answer the questions that the installer program will ask. If you are installing the trial version of Access Control, make sure that you have requested a 30-dau license and installed it.

FCM Web server requirement

Firewall Control Manager is a Common Gateway Interface (CGI) script and is functional only if you install it on a machine that is running a web server. Many commercial and freeware web servers are available in stores and on the WWW. If you install Secure Connect Server on a machine running Windows NT Server 4.0 the operating system includes a Web server called Internet Information Server. The SecureConnect installation program offers the default IIS directories as locations where you might install Firewall Control Manager, but you can install FCM in any directory your Web server uses for CGI scripts and HTML documents.

Access Control license requirement

If you intend to install Ascend Access Control visit the Ascend WWW site at the location listed below before you start the SecureConnect Server InstallShield program. The site contains a form for requesting a 30 day license or a permanent license for Access Control. Both the AAC server and Access Control Manager require that a license be installed on the host running the software.

`http://www.ascend.com/products/accesscontrol`

Documentation for AAC and ACM is available at the same web site.

Questions asked by the installation program

The SecureConnect installation program uses information you provide to automatically install the SecureConnect programs you select. If you choose the typical installation, it will install all three programs. If you choose a custom installation, you can select the programs that will be installed. Before installing the programs, you must answer questions about the programs you have selected. Prepare for the installation by obtaining the information necessary to identify the items in the following list.

- Destination directories for Access Control and Access Control Manager.
- Directory of the Web server.
- Directory that holds the Web server's CGI scripts.
- Directory that holds the Web server's HTML documents.
- Web server's IP Address or domain name.
- Web server's port number if it is different than the default port (80).
- RADIUS server (or AAC) IP address or host name.
- RADIUS port, if it is different than the default (port 1645).
- RADIUS secret by which the server will authenticate a Network Access Server, such as an Ascend router.
- IP address or domain name of the router that FCM will contact if there is no FCP `agnt` variable in a user's profile.
- Default community string that FCM will send a route if there is no `comm` variable in a user's profile.
- Directory where SecureConnect Manager saves exported firewalls that the Client Firewall Loader can download to remote tunnel endpoints. Export firewall files contain an IPSec tunnel configuration that matches the router firewall's tunnel configuration.
- Action that the Client Firewall Loader should take after downloading a firewall to a remote tunnel endpoint. The choices are:
  - Erase export firewall file from the server.
  - Save backup of downloaded export firewall file.
  - Leave export firewall file as is.

The last two items in the list of information that you must obtain before installing SecureConnect Server deal with the Client Firewall Loader (CFL). CFL is part of the SecureConnect Server, and you need to answer the questions to complete the SecureConnect server installation, even if you do not intend to use the CFL.

CFL is for SecureConnect Client users, especially on those machines which are the remote tunnel endpoints of a SecureConnect router's firewall.

CFL automatically download a firewall file to a SCC user when FCM authenticates the user.

When the RADIUS profile of an authenticated user contains an Ascend-Remote-FW authorization reply-item, FCM looks on the SecureConnect Server for the firewall file that is named by that reply-item. (For details, see "What is the Ascend-Remote-FW attribute?" on page 6-17.) When FCM finds the firewall file it calls CFL, which downloads the file to the user's PC. SecureConnect Client installs the firewall on the PC's interfaces. If the firewall file was created with the SecureConnect Manager export function, the firewall file contains a Main firewall ruleset and a tunnel configuration that automatically enable encrypted Virtual Private Network sessions between the PC and a router. (Details of the SecureConnect Manager's Export function are explained in Chapter 3, "Exploring the SCM Interface.")

When you install SecureConnect Server you are asked what you wish the FCM to do with the firewall file that was saved on the server after it has been installed on the remote user's PC by the Client Firewall Loader. You have three options, the most secure of which is to erase the file from the server. If you would like to retain the file, but make it unavailable for download, you can choose to save the file as a backup, in which case the file is renamed in such a way that it no longer appears to be a downloadable firewall file. The last option is leave the firewall file as it was before it was downloaded to a SecureConnect Client machine.

Note: Ascend's development of the functinality for using FCM and CFL to download exported SecureConnect firewalls that contain tunnel configuration for the router's remote tunnel endpoints did not ignore the need for security in such a transaction. If the remote site uses secure methods, such as SSL and authentication certificates, to communicate between Web browsers and a Web server, Ascend stands behind the security of using FCM and CFL to safely download tunnel configurations .

The purpose of developing the firewall export function for SecureConnect Manager, FCM, and CFL was to simplify the difficult task of configuring matching Security Associations for both ends of an IPSec tunnel. The SecureConnect export function enables the exchange of keys and algorithms by another medium and ensures that the mistakes that can occur when keys, algorithms, and SPIs are manually entered can be avoided.

Ascend will implement protocols that are expected to enable the secure exchange of public and private keys when available. For now, FCM and CFL offer the ability to download SecureConnect firewalls created by SecureConnect Manager. System administrators are also encouraged to disseminate SecureConnect Firewall tunnel configurations by any secure method, such as by diskette.

SecureConnect Server installation

SecureConnect Server programs are in a subdirectory of the SecureConnect Manager CD ROM. Insert the CD ROM into the drive of the host on which you intend to install SecureConnect Server and follow the steps in this section.

1. Select Start>Run from the Windows NT taskbar.
2. Enter *drive*`\scs\setup.exe` where *drive* is the letter of the CD ROM drive. For example:

   ```
   d:\scs\setup.exe
   ```

3. Click OK.
4. Enter information as you are prompted by the InstallShield program. (“Questions asked by the installation program” on page 6-21 lists the kinds of information you need.)

Authenticating with FCM to affect rulesets

Once you have installed the SecureConnect programs, a Web server and, possibly, your own RADIUS server, users can contact FCM to authenticate themselves and set in motion the process of activating SecureConnect Firewall section rulesets. The rest of this chapter explains:

- How users contact FCM and provide authentication information that FCM can forward to a RADIUS server.

- How to create Main firewall rules that enable users to contact the Webserver on which FCM is installed. The Main ruleset might need to contain rules other than the one which permits sessions to the FCM Web server.
- How to create rules in section rulesets so that the router can incorporate information it receives in FCP messages from FCM into the blanks left in the ruleset's rules.
- FCM and SNMP error messages that the user or the administrator of the router might receive during the process of authentication and the passing of FCP packets between FCM and the router.

How users communicate with FCM to obtain RADIUS authentication

Users begin communications with FCM by pointing a Web browser at the FCM Web server's URL (Universal Resource Locator). FCM responds by sending the user's browser the initial HTML page from a set of four developed for FCM (Figure 6-1.) Each page that FCM can send is a template you can alter in any way, so long as you don't disturb the templates' forms and comments.

The four HTML pages enable a user to submit a name and password, to receive notification of authentication success or failure, and to respond to server-issued challenges. Figure 6-3 is an example of a page that FCM can send to the user's Web browser to acknowledge successful authentication by a RADIUS server.

After receiving the user's name and password, the RADIUS server responds to FCM so it can send the user the appropriate reply. If RADIUS does not authenticate the user, the user can resubmit information. If RADIUS issues the user a challenge the user can submit an answer to the challenge. If resubmission of the name and password fails or if the response to the challenge is not accepted, the user can keep submitting the information entered on the initial or challenge pages as long as the RADIUS server will accept the requests.

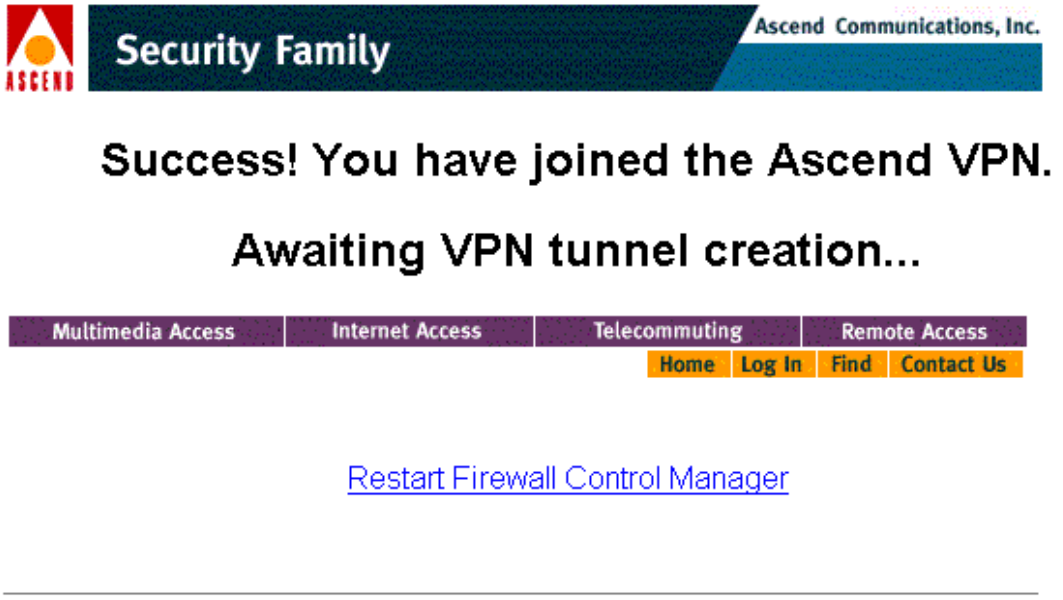


Figure 6-3. Example of a page FCM sends upon successful authentication

How users contact FCM

Following are steps users can take to send authentication requests to FCM.

1. Dial in to an Ascend unit.
2. Access a Web browser.
3. Enter the URL of the Web server that contains the FCM CGI script.
4. Enter username and password, or supply the information requested by the initial FCM HTML page.
5. Click Submit.

- The user ‘s initial dial in connection to an Ascend unit is authenticated by means described in his user profile or connection profile. Authentication methods might include PAP, CHAP, or Dial-back, among others.
- The Main firewall ruleset which control’s the user’s access permit incoming WWW packets to pass to the FCM Web server.
- `authinit.html`, the default HTML page FCM displays in the user’s Web browser, does not permit you to hit Enter to submit information to FCM.

Creating Main firewall rules that permit FCM authentication

When you implement FCM to authenticate users and affect SecureConnect firewalls, you might need to include rules in your firewalls that permit packets to be transmitted between the various entities involved in FCM authentication. Whether you need to include some of the following suggestions will depend on where the firewalls are located on the router. For example, if your firewall stands between the FCM server and the RADIUS server, it must permit the servers to transmit SNMP packets to each other. Similarly, if a user must pass through a firewall to contact the FCM server, then the firewall must permit WWW packets to pass between the user and the FCM server.

Following are some rules you might need to include in the firewall’s Main ruleset and the reasons the rules might be necessary.

Rules	Purpose
Enable incoming remote WWW packets to a local server.	This rule permits users seeking authentication to contact the FCM server through a firewall on the WAN interface when FCM is on the local network. Most firewalls already allow outgoing WWW packets from local users.
Enable incoming and outgoing SNMP packets between the FCM server and a router on the FCM Ethernet.	These rules permit FCM and a router to transmit and receive each other’s SNMP packets when a firewall is on the Ethernet interface and FCM is on the Ethernet.
Enable incoming and outgoing Routing Information packets between the FCM server and the router.	This rule permits the exchange of routing information between the local and remote addresses identified in the firewall rule.

Rules	Purpose
Enable ARP packets through an Ethernet interface firewall	This rule permits an FCM server and a RADIUS server to send ARP packets through a firewall on the Ethernet interface when both machines are on the same Ethernet. If you do not enable ARP on an Ethernet interface's firewall the hosts on the Ethernet will be unable to communicate with, or through, the router.

Creating Main firewall rules that are affected by FCP packets

Rules in section rulesets are not the only rules you can create that are affected by information the router receives in FCM-delivered FCP packets. Before you decide to create section rulesets, consider the kinds of rules you can create in the Main firewall ruleset that can be affected by FCP packets.

When you select the Fwall Control Protocol category for Main firewall rulesets, as shown in Figure 6-4, you can choose any of five options for creating rules in the Main firewall ruleset that can be affected by FCP packets sent by FCM. Table 6-4, below, lists the category's options and describes what you enable when you select them.

When you select *TCP* or *UDP* in the Fwall Control Protocol category you are really creating the four TCP rules or the six UDP rules that appear in Table 6-4. For example, when you select *TCP* you automatically enable the rules named tcpin, tcpout, ftpin and ftpout.

Caution: The rules you enable when you select Fwall Control Protocol category options in the Main firewall ruleset are very different than the rules you enable in section rulesets. Fwall Control Protocol rules can affect all of the packets the firewall's interface receives, not just one particular protocol such as POP Mail. For example, when you check the category's Trusted option you enable all incoming and outgoing traffic between the sites listed as the `lcad` and `rmad` values in the FCP packets that the router receives.

Chapter 3, “Exploring the SCM Interface,” also contains information related to this topic.

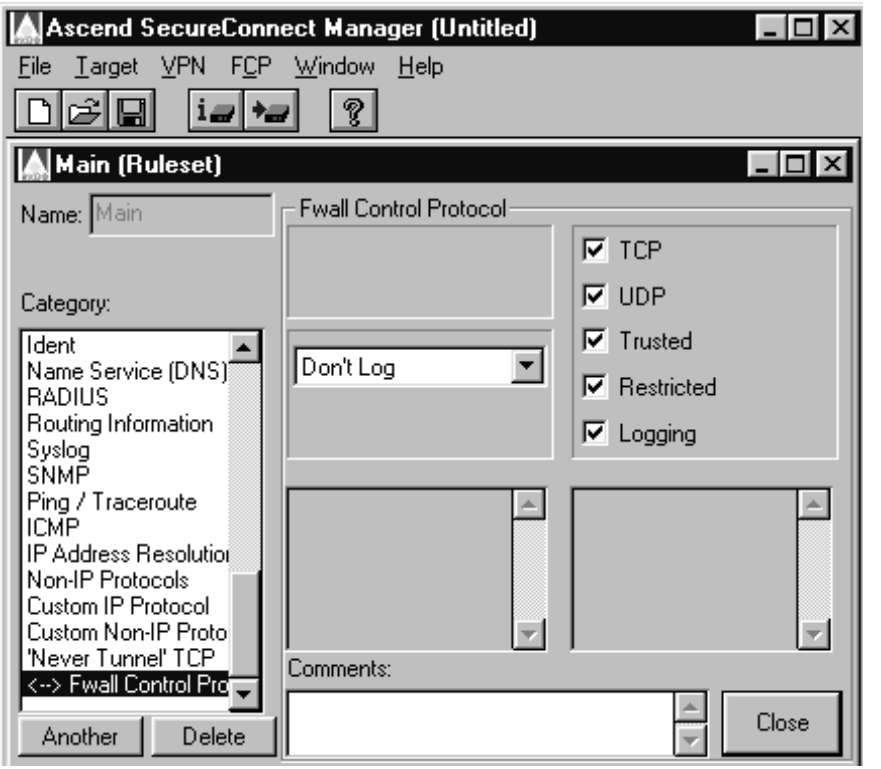


Figure 6-4. SCM interface, Fwall Control Protocol boxes checked.

Table 6-4. Fwall Control Protocol options and the rules they create

Option	Rules enabled	Effect
TCP	tcpin tcpout	Allows incoming/outgoing TCP sessions with addresses/ports supplied by FCP.
	ftpin ftpout	Allows incoming/outgoing FTP sessions with addresses/ports supplied by FCP.

Table 6-4. Fwall Control Protocol options and the rules they create (continued)

Option	Rules enabled	Effect
UDP	udpsin udpsout	Allows incoming/outgoing UDP highport to highport sessions, such as tftp that contain the addresses/ports supplied by FCP.
	udpqin udpqout	Allows incoming/outgoing UDP query/response sessions, such as SNMP that contain the addresses/ports supplied by FCP.
	udppkin udppkout	Allows incoming/outgoing UDP query/response sessions, such as SNMP that contain the addresses/ports supplied by FCP.
Trusted	trust	Allows all packets matching the addresses sent in FCP packets.
Restricted	restrict	Restricts all packets matching the addresses sent in FCP packets.
Logging	log trace	Logs/traces all packets matching the addresses sent in FCP packets.

Using FCM and a Never Tunnel TCP rule in Main firewall

Another rule you might need to add to the Main firewall ruleset when remote users contact FCM to authenticate is the Never Tunnel TCP rule, which is described in Chapter 3, “Exploring the SCM Interface,”. Never Tunnel TCP enables you to define a rule of the highest priority that is placed on top of the firewall’s stack of rules.

A Never Tunnel rule uniquely solves an issue that occurs in the following situation:

- The firewall at a remote site causes all the site’s packets that are destined for the network gateway to be IPSec-encapsulated because each site’s firewall contains a tunnel ruleset in which the other site is listed as a Trusted Site.

- The user at the remote site must send packets that have not been encapsulated by the IPSec protocol to a location in the network so the user can be authenticated at that location before he can connect to the gateway.

In this situation, how does the remote site send packets that have not been IPSec-encapsulated if the firewall automatically causes all outgoing packets destined for the network to be IPSec-encapsulated? The solution is that the Main Ruleset of the firewall at the remote site contains a Never Tunnel TCP rule that defines the outgoing packets the user must send to be authenticated and the Main Ruleset in the gateway's firewall contains a corresponding rule the enables incoming packets from the remote site. Each site's Never Tunnel TCP rule contains the addresses of the two sites and a port number, such as 443 for HTTPS Secure Socket Layer packets, or 24 for Telnet packets.

A particular use of the Never Tunnel TCP rule might be when authenticating remote users must contact an Ascend SecureConnect Server to securely download a firewall for a SecureConnect Client PC. The SecureConnect Server is the combination of an authentication server, such as Ascend's Access Control RADIUS server, the FCM (Firewall Control Manager), and the CFL (Client Firewall Distributor). SecureConnect Server is discussed in "Installing the SecureConnect Server programs"

Typically, Never Tunnel TCP rules should be created when remote users contact the FCM CGI script on a SecureConnect server so they can download a firewall containing a tunnel configuration. The rule is configured with port 443, the default port for at which Web servers receive HTTPS packets for Secure Socket Layer connections.

Creating a firewall section

Following parts of this chapter describe the steps for creating section rulesets and the ruleset's rules. The procedures for creating section ruleset rules are virtually the same as those you use to create rules in any part of a firewall, including the Main firewall and tunnel rulesets. However, you do not enter information in the location textboxes in which you want the router to insert information it receives in FCP messages. "How firewall's interpret empty location and port values in

rules," in this chapter explains how the firewall interprets empty location and port textboxes in the Main ruleset's rules and in a section ruleset's rules.

Note: You cannot create section rulesets within a tunnel or create a tunnel configuration that applies to a section ruleset. You can only create section rulesets within the framework of the Main firewall ruleset and tunnels are not associated with the Main ruleset. That is why a textbox labeled Tunnels never appears on the Main Ruleset configuration screen and why the FCP menu does not appear on SCM's toolbar when you are configuring a tunnel ruleset.

Creating a firewall section ruleset

SCM's toolbar contains a menu called FCP. Select the FCP > Add Section menu to add a dormant ruleset to the firewall that is not part of the Main firewall ruleset. A new textbox labeled Section appears above the categories on the Main Ruleset configuration screen when you create the firewall's first section ruleset. The Section textbox contains the name of the new section and the word Main. The textbox entries allows you to select the Main firewall ruleset or the new section when you want to edit one or the other. Additional section ruleset names appear in the list as you create them.

Creating a section ruleset's rules

Before you begin selecting categories for rules in a section ruleset, make sure that the name of the ruleset appears in the section textbox of the Main Ruleset configuration screen as shown in Figure 6-5.

The list of categories and protocols in the Category box changes when you select one of the section rulesets in the Section textbox. A few categories that you can select for the Main firewall ruleset are not available when you create a section ruleset's rules. The missing categories include those which don't fit the context of a section, such as Fwall Control Protocol, and those which can't be practically implemented in a section ruleset, such as Cracking Prevention.

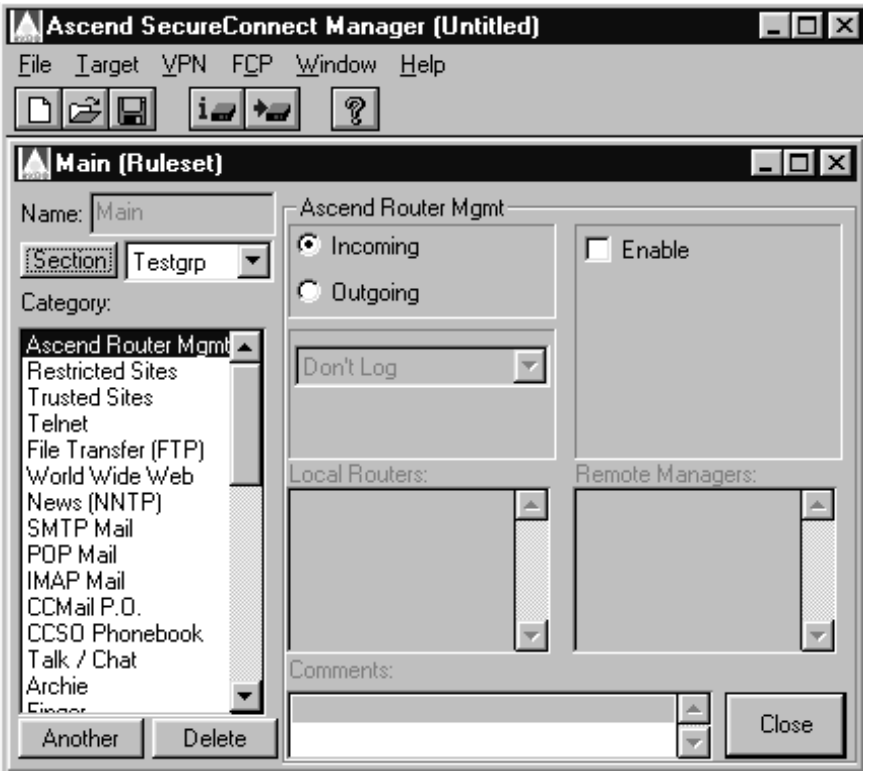


Figure 6-5. Creating rules in a section ruleset named Testgrp

Procedure

Following are general procedures for creating a section ruleset rule. The steps might be slightly different if you select a category such as Trusted Sites, which does not require you to enter location information, or World Wide Web, which requires that you select one or more options including WWW, Gopher WAIS, and SSL.

Note: Chapter 4, "Creating a SecureConnect firewall," contains explicit instructions for creating a section ruleset rule.

1 Select a section name in the Section textbox.

2 Select a category or protocol in the Category list.

3 Click Incoming or Outgoing.

4 Click Enable.

5 Enter an IP address of domain name in either of the location textboxes if you don't want the router to insert a value from an FCP message into that portion of the rule.

6 Leave location and/or port textboxes empty if you want the router to insert a value from an FCP message into that portion of the rule.

7 Repeat steps 1-6 to create all the section ruleset's rules.

8 Click Close.

How firewall's interpret empty location and port values in rules

A firewall does not interpret empty address and port values in section ruleset rules the same way as it does empty values in Main firewall or tunnel ruleset rules.

When a firewall encounters a blank where an address or port value should be in a Main or tunnel ruleset rule which you intended to permit packets, the firewall cannot perform as you intended. For example, suppose you select the FTP category in the Main ruleset, click incoming and enable, and enter a local server destination, but you leave the remote clients IP address box vacant. You haven't specified the source of the incoming FTP packets, so no incoming FTP packets can match the rule.

Conversely, you must leave some value or values empty in the rules you enable in section rulesets so that there is a place where the router can insert the values it receives in FCP messages. If you created the rule described above in a section ruleset named `Trainers,` the vacancy where the source of the incoming FTP packets should be indicates that the router should place the value of `rmad` in the rule that appears in messages where the value of `rule` is Trainers.

Figure 6-6 shows a Main ruleset configuration screen that would create a rule like the one described above that allows FTP rule to a local server named `trainftp`.

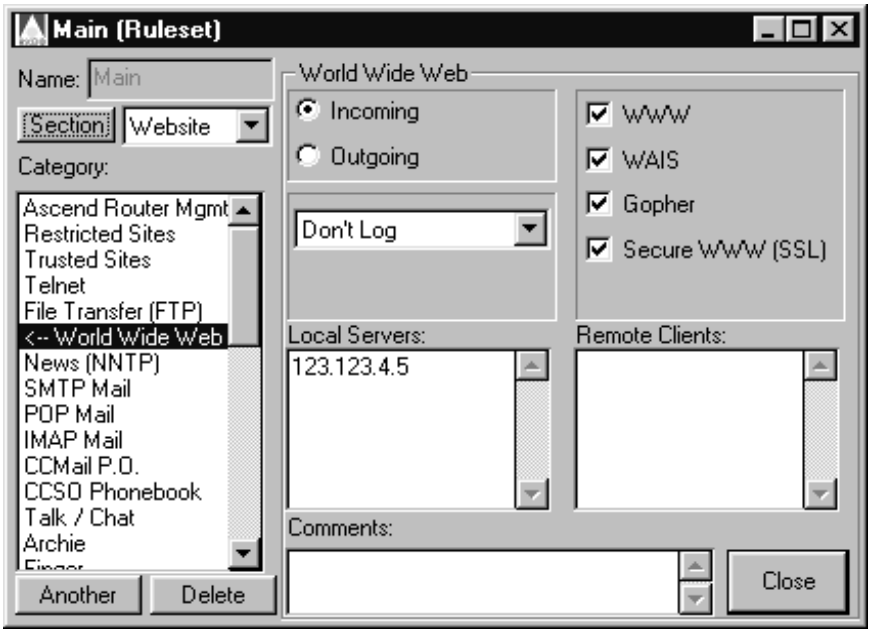


Figure 6-6. Creating a section rule in which FCP values can be inserted.

Configuring a section timeout

The Timeout and Keepalive options are two different methods for determining how a session enabled by a section ruleset ends. You select one or the other and specify a source from which to obtain the Timeout or Keepalive value. For details on configuring a timeout type and a timeout source, see “FCP > Add Section command,” in Chapter 3, “Exploring the SCM Interface.”

FCM and SNMP error messages

Following are two short sections that describe error messages users might encounter when using FCM, or that the router might generate when receiving FCP packets from FCM.

FCM error messages

You might receive an error message response from FCM if authentication or authorization fails. An authentication failure message indicates that your user name and/or password did not match a RADIUS user profile on the RADIUS server FCM contacted to authenticate you. An authorization error message may indicate that one of the following conditions exists:

- FCM could not create FCP packets based on the user profile the RADIUS server used to authenticate the user.
- The router could not find the firewall named in FCM's FCP packets. "SNMP error messages" on page 6-35 discusses how to use SNMP error messages captured in the FCM Web server's `error_log` file to determine why the router cannot find the firewall. Also see "rmad and rtad" on page 6-12 for information about this subject.

SNMP error messages

Following are some common error messages you might receive when FCM sends FCP packets to a router with SecureConnect firewalls. These messages appear in a file called error_log in your Web server's log directory. Table 6-5 contains a description of the messages and possible causes for receiving them.

- Alarm clock
- SNMP error status:2
- SNMP error status:3

Table 6-5. SNMP error messages and probable causes

Message	Probable cause
Alarm clock	The router address or the community name is incorrect and FCM is not receiving an expected response because SNMP requires agents to drop packets if they containing unrecognized community names. This message indicates that the agent or community string is misconfigured in a user profile's Ascend-FCP-Parameter attribute or FCM's default configuration. FCM might be sending FCP packets to the wrong router or providing a bad value for the comm=name|secret variable.
SNMP error status:2	Unrecognized SNMP object ID. Although this might be related to sending the FCP packets to the wrong router, the probable cause is that the router software does not recognize the FCP variables. This indicates that the router's software might be a release that predates SNMP authentication and FCP packets. Obtain new code for the router.
SNMP error status:3	Invalid value for object. The router is unable to comply with a request sent in an SNMP packet. This error message indicates one of two problems. **1** The rule name in the FCP packet is not on the firewall that the router used when it applied the FCP request. **2** The router could not find a firewall that corresponds to `rmad` or `rtad` in the FCP packet. Check the following: • Is the packet going to the correct router? • Is the firewall with the name sent in the FCP packet loaded and activated? • Is the firewall on the correct network interface/ • Is the router selecting the wrong network interface based on the value of `rmad` or `rtad` sent in the FCP packet?

Appendix: Ruleset categories

A

This chapter contains an alphabetized list of thumbnail descriptions of the services in the Category box.

Archie

This selection creates holes for Archie database searches. This will almost always be used by enabling outgoing Archie from anywhere (*) to anywhere (*). It is unlikely that you will have your own Archie server, so the Incoming section will probably be disabled.

Ascend Router Mgmt

Ascend Router Mgmt is only needed if a firewall is between the workstation running SecureConnect Manager (SCM) and the router. Ascend Router Mgmt simultaneously opens an outgoing telnet port and an incoming TFTP port during router configuration.

Ascend Router Mgmt also performs an Allow Estab. Type service that keeps the telnet/TFTP session up while a firewall is loaded.

CCSO Phonebook

CCSO Phonebook is a distributed database protocol for use on the Internet. It keeps track of personal and account information. CCSO was developed at the

University of Illinois Urbana-Champaign and is mainly used by universities to handle student accounts.

Cracking Prevention

Cracking Prevention protects the network from outside attack by the methods listed below. Always select Scan Detection, Anti-Spoofing and Reject Src Routing. (See the note under Scan Detection.)

Conversely, there are only a few reasons for turning on Allow Estab. and these are explained in “Allow Estab” on page A-3.

Scan Detection

Scan Detection prevents outside entities from performing automated scans of the address space. These scans are used by the SATAN tool to locate and probe systems on a network.

Dynamic firewall filters do not use Local Network addresses to enable Scan Detection. The filter rules are totally generic to location. Sometimes an outside host’s attempt to use a valid service that it is not allowed to use may cause the Scan Detection to take action against that host.

Note: Activating Scan Detection may create excessive lockouts of important sites. It is possible that a remote site trying to access a denied service may generate traffic resembling the pattern the SATAN filter is looking for.

Anti-Spoofing

Anti-Spoofing prevents a machine on one side of the firewall from impersonating a machine from the other side of the firewall. For example, when Anti-Spoofing is enabled the firewall will block incoming traffic that carries an IP address from a local network.

Enable Anti-Spoofing so you can specify IP addresses that should not appear in packets arriving at the router from beyond the firewall. Anti-Spoofing is unique among security category options because you do not have to enter information in both the local and remote location textboxes to enable an Anti-Spoofing firewall.

You must enter information in one or the other, but the Anti-Spoofing rule is still correctly configured if you leave one of the location textboxes blank.

Note: Spoofing cannot be prevented if any protected computer systems trust machines outside the firewall. Nor can spoofing be detected if all internal network IP addresses have not been entered in the Local Networks box.

Usually, you designate the IP addresses that should not be spoofed by entering information in the local textbox so the firewall will block incoming packets that impersonate packets from internal machines. However, the IP address or hostname does not always have to be entered in the local textbox. When the router is a dial in user's access to the Internet, you prevent spoofing of the dial in user's packets by entering the user's IP address or hostname in the remote location textbox.

Caution: Do not enter asterisks in the location textboxes Enter hostnames, network addresses or subnets.

Reject Src Routing

Reject Src Routing refers to a cracking technique in which routing information is supplied by an external host. This routing information might override normal routing paths taken by internal systems and routers, potentially redirecting packets to inappropriate destinations. When activated, the Reject Src Routing option prevents source routed packets from entering or leaving the local network.

Allow Estab

If this option is selected, any in-progress TCP sessions will continue when a filter is loaded. If Allow Estab. is off, active TCP sessions are abruptly terminated when a filter loads.

You should leave this option turned off because Allow Estab. opens a potential hole for hackers, but it is very useful in these situations:

- During experimentation with the router's filter configuration you may change filters in Connection Profiles and Answer Profiles quite often. Allow Estab. prevents disruption of the flow of traffic through the router.

- If you don't have a Universal Power Source (UPS) and your power often fails, sessions in progress will continue when the power comes up.

Custom IP Protocol, Custom Non-IP Protocol

The Custom IP Protocol and Custom Non-IP Protocol categories allow you to define protocols that do not appear in SCM's Category box. The Another feature button allows you to add as many Custom categories as you need to satisfy all your odd custom protocol needs.

Custom IP Protocol definitions are based on a port number and a type of protocol. The types of protocols you may use to define a custom protocol are:

- **TCP Session:** The enabled Custom IP Protocol packets are TCP packets. The protocol is identified by the entry in the Port Number textbox.
- **UDP Session**: The enabled Custom IP Protocol packets are UDP packets. The protocol is identified by the entry in the Port Number textbox.
- **UDP Query/Resp.**: The Custom IP Protocol is a query and response protocol such as RADIUS or SNMP. Incoming and outgoing packets for the session are enabled because the firewall notes the destination and source locations in the query packet and passes the response packet(s) containing the same location and port information.
- **UDP Packet Dst Spec**: This option only enables UDP packets to the destination IP address at the port number entered in the Port Number textbox. The firewall does not pass response packets from the destination to the source.
- **UDP Packet Src Spec**: This option only enables UDP packets from Port Number of the source IP address. The firewall does not pass response packets from the destination to the source.

Note that the Custom IP Protocol category doesn't fulfill the needs of a complex protocol that uses some dynamic mixture of different ports of TCP and/or UDP, but it can handle basic cases such as a database engine or IRC server that runs over TCP on port 325, or a RADIUS server that is answering on port 1001 instead of the semi-standard 1645. In the vast majority of cases, it will allow desired traffic to pass through a firewall.

Custom Non-IP Protocol

The Custom Non-IP Protocol category's options include a textbox for entering a hexadecimal number that corresponds to a packet's Ethernet type field. Use the Custom Non-IP Protocol to build a firewall for bridged Ethernet packets. The table that follows this reference section entry includes hexadecimal equivalents for common Ethernet types.

Name Service (DNS)

The Domain Name Service, or DNS, is a hierarchical service for translating host names to IP addresses. It permits users to enter a host name such as `moon` or `ftp.xyz.com` rather than an IP address such as 192.52.32.5 when attempting to contact another machine.

Within each domain there are one or more name servers. The name server for a domain maintains a set of maps for resolving host name lookups. The name server uses these maps to translate between the names of hosts within its domain and their IP addresses. If the name server is asked for a name or address outside the scope of its domain, it searches to find a name server with the appropriate information. In general, most name servers act as both clients and servers, since they must resolve both the names and addresses of outside entities for local clients, and the names and addresses of internal entities for remote clients. Generally, you should enable outgoing Domain Name Service queries.

Selecting the Incoming and Queries checkboxes permits locations listed in the Remote Clients text box to query the specified Local Servers. Enabling outgoing Zone Transfers is a security risk because it permits dumps of the Local Server's address maps to be transmitted through the firewall to remote hosts.

File Transfer Protocol (FTP)

File Transfer Protocol is used more frequently than anything else to transfer files over the Internet. Anonymous FTP is, in fact, the means by which many programs are shared for commercial purposes like beta testing. Anyone can access an internal Anonymous FTP server and make use of the resources that are available there.

From a security standpoint, one of the most important features of an FTP session is its need for two connections or channels. One channel between the user and the FTP server is used to exchange commands. The second channel is used to transfer the requested data to or from the server. In the process, the router must allow access to internal ports because it is not privy to information about the internal port used by the second, or data, channel. Consequently, a gap in network security may be created.

SecureConnect Firewall closes the security gap because the firewall is triggered by information it sees in the packets passing through it. This information includes the source and destination ports the FTP server and the user machine will use for the data channel. Recognizing the establishment of the FTP session and the ports which will be used, the firewall only opens the internal port requested for the connection and closes it when the final packet of the session passes through the firewall.

Finger

The Finger application provides information on users of a system. Unlike whois, finger does not rely on static databases of registered information. Instead, finger queries the specified host for information on the specified user. The returned information includes data on how long the user has been logged in and how much idle time the user has accrued.

ICMP

ICMP (Internet Control Message Protocol) is used for many infrastructure tasks like Ping and Traceroute.

Errors

ICMP sends error messages when a host or network is unreachable, or a packet's options are malformed (Errors).

Info Requests

ICMP sends requests for information like a network address, or an address netmask, from other machines

Redirect

ICMP sends redirects to inform one host that it should use a different route to contact another, specific host.

ICMP errors often provide useful and important information to other hosts. Enabling outgoing Errors may be beneficial since this is the type of packet the router uses to inform an outsider that it has been denied access to a particular host/service.

Enabling incoming errors may also help your network operate more efficiently, although an attacker could disrupt your connectivity with certain remote networks by bombarding you with spoofed “Unreachable” or “Prohibited” packets.

Unless you encounter a problem, you probably won't need to enable the Info Requests in either direction - the most common ones, “Echo Request” (type 8) and “Echo Reply” (type 0) are already covered by the Ping rule.

Usually you should turn Redirect OFF because it allows an unverified source to suggest changes to your routing tables. That could lead to problems. At any rate, ICMP Redirect messages don't have much use on a WAN interface (unless you have multiple WAN interfaces) and hardly ever occur in normal operation.

Ident

The Ident protocol is described in RFC 1413. It provides a method for a host that has received a TCP connection request to query the originating machine and learn the username of owner of the process that requested the connection. Newer versions of the Unix sendmail program (8.x) support use of ident to help eliminate spoofing of addresses in mail messages. (Of course, this can only work if the machine being queried supports ident, and if the originator of the connection request has not gained root access to the system).

Ident can be very useful in tracking security problems created by users who don't have root access on the machines they are originating from. It can also provide information about valid usernames on your machines to the unscrupulous. RFC 1413 recommends that you consider access to ident in a similar manner to “finger” access.

If you are running `sendmail` version 8, it is probably a good idea to enable outgoing Ident from your mail server to anywhere (*). This will help sendmail learn as much as possible about the true origin of incoming mail. If you aren't bothered by the possibility of another site learning valid usernames on you system, you can enable incoming ident as well, to give other mail servers the same courtesy.

IMAP Mail

SecureConnect supports two versions of the IMAP protocol:

- v2/v4
- v3

IMAP (Internet Message Access Protocol) is a mail protocol useful for low bandwidth connections. It provides users with more complex interactions and efficient access than POP, the most widely used mail protocol. All mail messages stay on the server in IMAP and the user can choose to see part of the message rather than transferring it totally to a local workstation.

IP Address Resolution

IP Address Resolution includes two options:

- (ARP) Address Resolution Protocol
- (RARP) Reverse Address Resolution Protocol

ARP enables you to obtain the Media Access Control (MAC) address of another host if you know that host’s IP address.

A firewall installed on an Ethernet interface must allow ARP or the hosts on the Ethernet will be unable to communicate with or through the router.

RARP enables you to find another host’s IP address if you know that host’s MAC address. Usually this is used with bootp and diskless networks.

IPSec

IPSec, or IP Security, has two options:

- AH
- ESP

IPSec is the Internet Protocol standard for security and will be part of IPv6. IPSec has two parts, Authentication Header (AH) and Encapsulating Security Payload (ESP).

The AH is added to the packet to provide data integrity and authentication.

The ESP provides confidentiality as well as data integrity and authentication. ESP supports public and private key encryption.

Lan Manager (NetBIOS)

File/Printer

This enables file and printer sharing via the popular Lan Manager protocol used by Windows 95 and Windows for Workgroups. The released versions of these operating systems have serious security holes, so you shouldn't open Lan Manager holes to sites you don't totally trust. Before you do open these holes you should read the security bulletins about LAN Manager.

Multimedia

SecureConnect Firewall supports two options under Multimedia:

- RealAudio™
- StreamNet™
- VDOLive™

RealAudio™, StreamNet™, and VDOLive™ are multimedia software that provide "real time" audio and visual streams over the Internet. These are fairly new as of the writing of this document and the number of sites that actually broadcast music and video is not large.

News (NNTP)

News, or Network News Transfer Protocol, applications such as rn are used to access a wide variety of information on diverse topics ranging from technical information to art. Many news groups are discussion groups. News users post articles for the group on politics or sensitive subjects like explicit sexuality. News is distributed in a relay fashion. Sites receive news, feed it to other sites, who feed it to other sites.

Use the SecureConnect News (NNTP) rule to control which sites can send news and which sites can receive news.

Non-IP Protocols

Non-IP Protocols refer to IPX (Internetwork Packet Exchange) and AppleTalk.

Ping/Traceroute

Ping

Ping is used to test connectivity between two machines anywhere on the network. Enabling outgoing ping allows a local machine to send a ping request to a remote site. During a window of time the remote site can send an echo response back.

Enabling Incoming allows Ping in the opposite direction.

Currently, the window for a response is 30 seconds

Usually there is no danger in allowing both incoming and outgoing pings between all hosts. The main security risk is that an attacker can learn the addresses of valid hosts on your internal network by pinging all possible addresses and seeing which ones reply.

Another possible problem is a denial of service attack, but this is limited by the bandwidth of your WAN connection. Ping denial of service will flood your network with pings.

The Scan Detection in Cracking Prevention turns on filter rules which detect attempts to probe multiple addresses on your internal network with pings. After

the 3rd different address, Scan Detection shuts off all access to the offending host for 5 minutes.

Traceroute

Traceroute shows the approximate path taken by packets traveling between two systems. Incoming traceroutes are a security risk because details of your internal network topology could be revealed.

Usually it is okay, and often useful, to allow outgoing traceroute.

POP Mail

SecureConnect Firewall supports filtering on two POP mail protocols:

- POP-2
- POP-3

POP Mail differs from SMTP which is used to exchange mail between servers. POP Mail is a protocol for handling electronic mailbox services between a client and a server. Usually you use POP Mail to access an internal server which is holding your e-mail. In this regard, POP Mail is similar to telnet or FTP in that you should limit remote accessibility to specific servers which won't provide access to other, vulnerable, and valuable, internal resources.

RADIUS

SecureConnect Firewall provides two options for the RADIUS category:

- RADIUS
- RADIUS Acct.

RADIUS (Remote Authentication Dial In User Service) is a database server developed by Livingston Enterprises Inc. It provides authentication for dialup sessions and accounting information used for billing and troubleshooting.

Restricted Sites

Restricted Sites totally locks out specific sites, internal or external. The sites cannot communicate with hosts on the other side of the WAN link.

When you choose Restricted Sites the location textboxes' labels change to Grounded Locals and Undesirable Outsiders.

Routing Information

Routing information protocols are used by stand alone routers and by systems acting as IP routers to identify possible routes between networks and hosts. When multiple routes are available, routers can dynamically adapt to changing network conditions.

You can also use routing information protocols to help to identify aspects of a network's topology or to mislead a host into mis-routing packets. SCM enables you to construct firewall rules that control transmission and reception of the packets of four popular routing information protocols, including:

- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)
- Exterior Gateway Protocol (EGP)
- Border Gateway Protocol (BGP)

You can select more than one of the routing protocols simultaneously.

Secure Shell

This enables ssh terminal sessions. ssh is a secure shell available freely from various places on the Internet. ssh uses TCP port 22.

SMTP Mail

SMTP Mail is one of the most common forms of UNIX mail. SMTP, or Simple Mail Transfer Protocol, is the primary protocol used by sendmail and many other popular mail transport agents. The SCM SMTP Mail option allows you to control the flow of SMTP packets into and out of the network. Separate controls are

provided for Incoming and Outgoing mail. SCM control of SMTP is very much like its control of News (NNTP). Usually, Remote Clients contains an asterisk (*) character, so any remote host may connect to the local mail server listed in the Local Servers box.

SNMP

This protocol permits network management stations to gather data and change configurations of SNMP-manageable network machines.

Syslog

syslog is often used to store system information to allow someone to check the system's status. Do not allow outside access to the syslog server.

Talk/Chat

Talk and chat protocols allow interactive user communication via the Internet. Using these protocols one user's typed messages are displayed in near real-time on the screen of another user. There are several applications and protocols available for this purpose. SCM Talk / Chat options allow filtering of packets for any or all of the talk, ntalk (New Talk), and irc (Internet Relay Chat) applications. Packets can be filtered in either the incoming or outgoing directions.

Note: Due to the semantics of the talk and ntalk protocols, it is impossible to totally block out incoming talk sessions when outgoing is enabled, or vice versa. At the packet level, the process of answering a talk request in one direction appears nearly identical to that of making an initial talk request in the other direction. A hole must be opened for a short period to allow an incoming answer to an outgoing request. During this time another talk request from the same remote host to the same local host may get through. The window of time is set to 120 seconds

Telnet

Telnet is one of the most common TCP-based services because it is used to remotely access a command shell on another computer. Because of its utility in

providing remote terminal access, most networks don't place many restrictions on outgoing telnet sessions. However, Telnet access from external sites should be strictly controlled.

Time Services

NTP

NTP is the Network Time Protocol for synchronizing clocks on multiple machines. Note that NTP is a peer-to-peer protocol, so it can't be selectively enabled just for incoming, or just for outgoing.

rdate

rdate is a simpler time protocol used by many systems with limited memory resources. Unlike NTP, it is possible to allow outgoing rdate so a local machine can learn the proper time from a remote machine without allowing incoming rdate. If your clock source is outside the firewall, you will need to enable outgoing rdate from your router to the remote time source.

daytime

daytime is another simple protocol which prints the current date in a (non-standardized) ASCII string. Although it isn’t in common use, you may find the odd machine that needs it for some reason.

TSP (Timed)

TSP is the Time Synchronization Protocol. It uses a daemon called `timed` on each network host in a master-slave relationship where one daemon is the master and the rest are the slaves. This protocol uses UDP broadcast messages.

Trivial File Transfer (TFTP)

Among other uses, TFTP, the Trivial File Transfer Protocol, is used by many diskless systems to load their kernel from a disk server. Ascend routers can

download files from a TFTP server, as well as send core files to a TFTP server to aid in debugging problems.

Part of the simplicity of TFTP is the lack of any security measures. Therefore, you must be extremely careful about who is allowed to use TFTP, especially incoming TFTP.

Trusted Sites

Trusted sites are external servers or clients you trust implicitly, possibly because of a business relationship in which you need to share resources. Be very wary of selecting Trusted Sites. Packets to and from Trusted Sites will pass through the firewall. In this regard Trusted Sites are the opposite of Restricted Sites.

Unix Utilities

The UNIX R-commands are a set of commands that allow Remote operations on other hosts. They are both extremely powerful and extremely dangerous because they represent one of the more significant potential security hazards on UNIX systems. The rlogin command allows users to remotely log into other machines. The rexec and rsh facilities are both used to execute commands on remote systems without establishing an interactive login session. While there are system level security measures that are designed to protect against unauthorized intrusions via UNIX R-commands, any system which has been improperly configured can be at risk of external attack.

As with the other options in this section, be careful about giving access to incoming printer sessions—you wouldn't want someone to use up all your paper! Of course, most lpr servers have another layer of security as well, but you can never be too careful.

UUCP

UUCP is the UNIX to UNIX copy program. The UUCP protocols allow file transfer, mail transfer, and remote program execution via either TCP/IP connections or through the use of point-to-point dialup modem connections.

The UUCP filtering options allow the user to control UUCP traffic entering or leaving the network. Controls operate much like those discussed for News and FTP. Selecting Incoming with the Enable checkbox allows incoming UUCP traffic between the specified Local Servers and Remote Clients. Selecting Outgoing with the Enable checkbox allows outgoing UUCP traffic between the specified Local Clients and Remote Servers.

Whois

The whois application allows users to query databases of user and host ID information. Many US government organizations, including the Department of Defense, maintain whois servers. Whois can also be used to query the Internet Registry at rs.internic.net for identifying information on users and hosts.

World Wide Web

Although the application is called World Wide Web in SCM, it really refers to Internet connections. The security risk associated with Internet services is similar to that posed by FTP servers. By definition, the Internet exists to allow connections between internal and external networks. Therefore you must carefully decide where you will allow access on your network, so that you can protect private resources while providing public information.

SCM options for control of Internet traffic include any of four information services. Selecting WWW also enables Secure HTTP, which provides encryption and authentication.

WWW

The well known standard for World Wide Web communications.

WAIS

Wide Area Information Service enables users to submit a query to large databases to obtain a list of documents containing information described by the query.

Gopher

Gopher is a menu-based tool for browsing server directories.

Secure WWW (SSL)

Secure WWW (SSL) is a protocol that enables users to send encrypted traffic between a host and a web server. Port 443 is reserved for SSL connections.

X11

This selection allows you to conduct X11 display sessions across the firewall. However, only allow X11 to specific hosts as needed. Be very careful about allowing it to (or from) all hosts internally or externally.

The direction of X11 packets is confusing so SCM makes the security considerations of “incoming X11” and “outgoing X11” more consistent with those of other SCM “incoming” and “outgoing” selections.

SCM considers an “outgoing” session to be one where the user (display) is local and the program is remote.

Conversely, a SCM “incoming” session is one where the user (display) is remote and the program is local.

In X11 terms, the “server” is the display where the user is sitting. The “client” is the application running (possibly) on another machine. Technically, an “outgoing” session is one where the display server is remote and the client application is local.

Keep in mind, however, that since an “outgoing” X11 session in SCM terms starts up from the outside (the syn packet comes from the remote machine), it is possible for a malicious outsider (at the proper address) to run programs that display garbage on your X11 displays.

The “:0.0”, “:0.1”, and “:0.2” options allow you to selectively enable access to the 1st, 2nd, and 3rd displays on each machine. Usually a machine only has one display.

XDM is the protocol used by X11 displays and display managers to find each other and start up desktop sessions. This option should only be enabled if you have an X terminal whose display manager is running on a machine on the other side of the firewall. Since this normally isn't the case, the XDM option should usually be turned off.

Ethertype hexadecimal values for non-IP protocol

Table A-1 provides a list of hexadecimal values for common non-IP protocols. Use these values to create custom non-IP firewalls.

Table A-1. Hexadecimal values for non-IP protocols

Non-IP Protocol	Hexadecimal value
3Com Corp.	6010-6014
Aeonic Systems	8036
Allen-Bradley	80E0
Allen-Bradley	80E3
Apollo	8019
Apollo Computer	80F7
Applitek Corp.	80C7
ARP (for IP and for CHAOS)	0806
AT&T	8008
AT&T	8046
AT&T	8047
AT&T	8069
Autophon (Switzerland)	806A

Table A-1. Hexadecimal values for non-IP protocols (continued)

Non-IP Protocol	Hexadecimal value
Banyan Systems	0BAD
BBN Simnet Private	5208
BBN VITAL LAN Bridge cache wakeup	FF00
Berkeley Trailer encapsulation	1001-100F
Berkeley Trailer negotiation	1000
Bridge Communications	9003
Bridge Communications XNS Systems Mgmt.	9001
Bridge Communications XNS Systems Mgmt.	9002
CHAOSnet	0804
Cisco System Inc. Combinet Packet Protocol (CPP)	8731-8738
ComDesign	806C
Compugraphic Corp.	806D
Counterpart Computer	8062
Counterpoint Computers	8081
Counterpoint Computers	8082
Counterpoint Computers	8083
Cronus Direct	8004

Table A-1. Hexadecimal values for non-IP protocols (continued)

Non-IP Protocol	Hexadecimal value
Cronus VLN	8003
Dansk Data Elektronic A/S (Denmark)	807B
Datability	809C
Datability	809Î
Datability	809E
Datability	80E4-80F0
DEC DECNet customer use	6006
DEC DECNet diagnostics	6005
DEC DECnet Phase IV	6003
DEC DECNet SCA	6007
DEC Ethernet CSMA/CD Encryption Protocol	803D
DEC LAN traffic monitor	803F
DEC LANBridge	8038
DEC LAT	6004
DEC MOP dump/load assistance	6001
DEC MOP remote console	6002
DEC Unassigned	6000
DEC unassigned	6009

Table A-1. Hexadecimal values for non-IP protocols (continued)

Non-IP Protocol	Hexadecimal value
DEC unassigned	8039
DEC unassigned	803A
DEC unassigned	803B
DEC unassigned	803C
DEC unassigned	803E
DEC unassigned	8040
DEC unassigned	8041
DEC unassigned	8042
Digital Communications Assoc.	80C0
Digital Communications Assoc.	80C1
Digital Communications Assoc.	80C2
Digital Communications Assoc.	80C3
DoD IP	0800
ECMA Internet	0803
Evans and Sutherland	805D
Excelan	8010
ExperData (France)	8049
Experimental (Conflicts with 802.3 length fields)	0101-01FF
General Dynamics	8068

Table A-1. Hexadecimal values for non-IP protocols (continued)

Non-IP Protocol	Hexadecimal value
Harris Corp.	80CD
Harris Corp.	80CE
HP Probe protocol	8005
IBM SNA Services over Ethernet	80D5
IEEE 802.3 length field	0000-05DC
Integraph Corp.	80C8-80CC
Integrated Solutions	80DF
Integrated Solutions TRFS (Transparent Remote File System)	80DE
Kinetics	80F4
Kinetics	80F5
Kinetics Appletalk ARP (AARP)	80F3
Kinetics Ethertalk-Appletalk over Ethernet	809B
KTI	8139-813D
Landmark Graphics Corp.	806E-8077
Little Machines	8060
Loopback (Configuration Test Protocol)	9000
LRT (England)	7020-7029
Matra (France)	807A

Table A-1. Hexadecimal values for non-IP protocols (continued)

Non-IP Protocol	Hexadecimal value
Merit Internodal	807C
NBS Internet	0802
Nestar	8006
Nixdorf Computer (West Germany)	80A3
Novell	8138
Novell (old) NetWare IPX (ECONFIG E Option)	8137
Pacer Software	80C6
PCS Basic Block Protocol	4242
Planning Research Corp.	8044
Proteon	7030
PUP address translation (Conflicts with 802.3 length fields)	0201
Retix	80F2
Reverse ARP	8035
Rosemount Corp.	80D3
Rosemount Corp.	80D4
SGI "bounce server" (obsolete)	8016
SGI diagnostic type (obsolete)	8013
SGI network games (obsolete)	8014

Table A-1. Hexadecimal values for non-IP protocols (continued)

Non-IP Protocol	Hexadecimal value
SGI reserved type (obsolete)	8015
Siemens Gammasonics Inc.	80A4-80B3
Spider Systems Ltd. (England)	809F
Stanford V Kernel production	805C
Symbolics Private	081C
Symbolics Private	8107
Symbolics Private	8108
Symbolics Private	8109
Taylor Inst.	80CF-80D2
Tigan, Inc.	802F
Tymshare	802E
UB Networks Debugger	0900
UB Networks download	7000
UB NIU	7001
UB NIU	7002
University of Massachusetts at Amherst	8065
University of Massachusetts at Amherst	8066
VALID	1600

Table A-1. Hexadecimal values for non-IP protocols (continued)

Non-IP Protocol	Hexadecimal value
Varian Assoc.	80DD
Veeco Integrated Automation	8067
Versatile Message Translation ProtocolRFC-1045 (Stanford)	805B
VG Laboratory Systems	8131
VitaLink Communications	807D
VitaLink Communications	807E
VitaLink Communications	807F
VitaLink Communications	8080
Waterloo Microsystems	8130
Wellfleet Communications	80FF-8103
X.25 Level 3	0805
X.75 Internet	0801
Xerox 802.3 PUP Address Translation	0A00
Xerox PUP (Conflicts with 802.3 length fields)	0200
Xerox XNS IDP	0600
XNS Compatibility	0807
Xyplex	0888-088A
Xyplex	8088

Table A-1. Hexadecimal values for non-IP protocols (continued)

Non-IP Protocol	Hexadecimal value
Xyplex	8089
Xyplex	808A

Appendix: IPSec debug commands

B

This appendix covers the new debug commands added to support the IP Security feature.:

IPsecSADump

This command displays all SAs currently residing in the database. You enter the command without optional arguments:

>IPsecSADump

This type of information displays:

```
SA at 0x2c3f90 (scheme 1):
  flags=21 <ACTIVE,ESP,MOBILE>
  SPI=2, dst=Mobile(Unset), ESP type=DES3_CBC IV Size=64,
IV=0x26575d3ea7478374
```

```
SA at 0x2c3ed0 (scheme 1):
  flags=21 <ACTIVE,ESP,MOBILE>
  SPI=2, dst=Localhost, ESP type=DES_CBC IV Size=32,
IV=0x57f00cb6a80ff349
SA at 0x2c3e10 (scheme 1):
  flags=22 <ACTIVE,AH,MOBILE>
  SPI=1, dst=Mobile(Unset), AH type=SHA1
SA at 0x2c3d50 (scheme 1):
  flags=22 <ACTIVE,AH,MOBILE>
  SPI=1, dst=Localhost, AH type=MD5
```

Table B-1 describes the information elements.

Table B-1. IPsecSADump command output

Element	Description
flags	Specifies the state and characteristics of the SA. This field can have one of the following values: `ACTIVE`—The SA is active. `INACTIVE`—The SA is inactive. `ESP`—The SA uses an ESP (IP Encapsulating Security Payload, RFC 1827) encryption transform. `AH`—The SA uses an AH (IP Authentication Header, RFC 1826) authentication transform. `MOBILE`—The SA is part of a mobile IP Security scheme. `LOCKED`—The SA is part of a static IP Security scheme.
SPI	Specifies the Security Parameters Index (SPI) that the Ascend unit uses, along with the destination address, to select the SA.

Element	Description
dst	Specifies the destination address associated with the SA. This field can specify one of these values: *local_hostname*—Specifies the name of the local router. *dest_ipaddr* —Specifies the name of the destination host. Mobile (Unset)—Specifies an unitialized mobile SA.
type	Specifies the type of transform in use: MD5—Indicates the AH-MD5 authentication transform (RFC 1828). SHA1—Indicates the AH-SHA-1 authentication transform (RFC 1852). DES_CBC—Indicates the ESP-DES-CBC (RFC 1829) encryption transform. DES3_CBC—Indicates the ESP-3DES-EDE-CBC (RFC 1851) encryption transform.
IV size	**Description:** Specifies the number of bits in the initialization vector for the ESP-3DES-EDE-CBC encryption transform.
IV	Specifies the 3DES key.

IPsecSchemeDump

This command displays one or all IP Security schemes currently residing in the database. You enter the command using this syntax:

>IPsecSchemeDump ***integer***

If you specify the ***integer*** argument when entering this command, the Ascend unit displays the scheme indicated by the number. If you do not specify an integer, the command displays all schemes in the database.

When you enter the command, this type of information displays:

SCHEME 1 at 0x2c3d10:

flags=1 <ACTIVE>

dst=Unset(Mobile)

Incoming AH SA at 0x2c3d50, Outgoing AH SA at 0x2c3e10

Incoming ESP SA at 0x2c3ed0, Outgoing ESP SA at 0x2c3f90

Table B-2 describes the information elements.

Table B-2. IPsecSchemeDump command output

Element	Description
flags	Specifies the state of the scheme. This field can have one of the following values: `ACTIVE`—The scheme is active. `INACTIVE`—The scheme is inactive.
dst	Specifies the destination address associated with the scheme. This field can specify one of these values: *`dest_ipaddr`* —Specifies the name of the destination host. `Mobile (Unset)`—Specifies an unitialized mobile SA.
`Incoming...` message	Specifies the Security Associations (SAs) that the router receives, as well as the internal router memory address in which the data is stored. ESP indicates that the SA uses an ESP (IP Encapsulating Security Payload, RFC 1827) encryption transform. AH indicates that the SA uses an AH (IP Authentication Header, RFC 1826) authentication transform.
`Outgoing...` message	Specifies the Security Associations (SAs) that the router transmits, as well as the internal router memory address in which the data is stored.

IPsecdblog

This command toggles the debug message status for IP security. You enter the command using this syntax:

> **IPsecdblog d|s y|n**

Table B-3 describes the information elements.

Table B-3. IPsecdblog command arguments

Argument	Description
d y	Specifies that the Ascend unit prints IP Security debugging messages to the debug monitor.
d n	Specifies that the Ascend unit does not print IP Security debugging messages to the debug monitor.
s y	Specifies that the Ascend unit prints IP Security debugging messages to Syslog.
s n	Specifies that the Ascend unit does not print IP Security debugging messages to Syslog.

IP Security syslog and debug messages

This release includes the following new messages. They can appear in syslog or in the debug monitor.

Table B-4. IP security syslog and debug messages

Message	Description
`IPSEC: Scheme` *num*`: Expected remote` *x.x.x.x*`, got` *y.y.y.y*`.`	The router received a packet with SPIs matching scheme *num*, but the packet came from *x.x.x.x* instead of scheme *num*'s configured tunnel address of *y.y.y.y.*

Table B-4. IP security syslog and debug messages

Message	Description
`IPSEC: Scheme num1: Expecting SPI num2, got SPI num3`	The router received a packet with both AH and ESP encapsulations, but the two SPIs do not match.
`IPSEC: Scheme num1: Expecting no encryption, got SPI num2.`	The router received a packet with SPI *num2*, AH on the outside, and ESP on the inside, but scheme *num1* does not have encryption configured.
`IPSEC: Failed encap on inactive scheme num`	The router received a packet for scheme *num* while updating that scheme in the VT100 interface. This message indicates a transient condition.
`IPSEC: Scheme num: Bogus ICMP Destination Unreachable: Source Route Failed`	The host at the remote end is in an error condition. The router does not send source-routed IPSEC packets, so it should not be receiving this ICMP error message.
`IPSEC: SHA1: Received invalid AH: SPI num x.x.x.x -> y.y.y.y`	The router received an AH-SHA packet, but the authentication did not match the one configured in the VT100 interface.
`IPSEC: Received unknown SPI num, x.x.x.x -> y.y.y.y`	Received an AH- or ESP-encapsulated packet, but SPI *num* is not configured on the Ascend unit.
`IPSEC: Scheme num1: Expecting no authentication, got SPI num2`	Received a packet with SPI *num2*, AH on the outside, and ESP on the inside, but scheme *num1* does not have authentication configured.
`IPSEC: Scheme num: Received packet encapsulation does not match scheme`	Scheme *num* is configured to use both AH and ESP encapsulation, but the packet used only one type of encapsulation.

Table B-4. IP security syslog and debug messages

Message	Description
`IPSEC: Scheme` *num*`: Bogus ICMP Destination Unreachable: Port Unreachable`	The host at the remote end is in an error condition. The ICMP message refers to bad TCP or UDP port numbers, but the router is sending AH and ESP packets, which do not contain port numbers.
`IPSEC: MD5: Received invalid AH: SPI` *num x.x.x.x -> y.y.y.y*	The router received an AH-MD5 packet, but the authentication did not match the one configured in the VT100 interface.
`IPSEC: Scheme` *num1*`: SPI` *num2* `is not AH,` *x.x.x.x -> y.y.y.y*	The router received an SPI *num2* AH packet, but SPI *num2* is configured for ESP.
`IPSEC: Scheme` *num1*`: SPI` *num2* `is not ESP,` *x.x.x.x -> y.y.y.y*	The router received an SPI *num2* ESP packet, but SPI *num2* is configured for AH.
`IPSEC: Scheme` *num*`: Tunnel endpoint` *x.x.x.x* `is > 64 hops away`	You have misconfigured your scheme to indicate a tunnel endpoint the router cannot find.
`IPSEC: Scheme` *num*`: Tunnel endpoint` *x.x.x.x* `doesn't speak AH`	You have misconfigured your scheme to indicate a tunnel endpoint that cannot handle AH encapsulation.
`IPSEC: Scheme` *num*`: Tunnel endpoint` *x.x.x.x* `doesn't speak ESP`	You have misconfigured your scheme to indicate a tunnel endpoint that cannot handle ESP encapsulation.
`IPSEC: Scheme` *num*`: Tunnel endpoint` *x.x.x.x* `is unreachable`	You have misconfigured your scheme to indicate a tunnel endpoint the router cannot reach.

FWALLversion debug command

The FWALLversion debug command now returns a space-delimited list of all firewall versions that the router accepts. If IP security is enabled, the version information is followed by the letter *i*. For example, a current router displays this information:

> **FWALLversion**

FWversion: 1 2 i

The router accepts version 1 or version 2 firewalls. IP security can be enabled for both.

Version changes

The firewall version number is now 2, although the Ascend unit accepts version 1 firewalls and they work properly.

Language changes

The firewall language saved by SAM (the SecureConnect Manager program for Windows) in.fw files has four new keywords. You can use these keywords to control how the Ascend unit applies IP Security transforms to incoming and outgoing packets. Table B-5 describes each keyword.

Table B-5. SCM keywords

Keyword	Description
scheme=[*scheme*]	Encapsulate transmitted packets using the information contained in ***scheme***. On reception, match the received packet against the parameters in ***scheme***, matching only if all parameters match. If no scheme argument appears, the Ascend unit uses the scheme remembered using a dynamic trigger rule. Use this keyword without the ***scheme*** argument only in dynamic rule templates.
auth	Match only received packets that have been successfully authenticated.
crypt	Match only received packets that were successfully decrypted.

Firewall syslog message changes

The one-line message summary lines that display when a firewall logs a packet can now display IP Security-specific information:

- Logged IP packets with a protocol field of 50 display as *esp* instead of *50*.
- Logged IP packets with a protocol field of 51 displays as *ah* instead of *51*.
- Received IP packets that have been successfully authenticated display with the addition of the string *auth* to the end of the logged message.

Received IP packets that have been successfully decrypted display with the addition of the string *crypt* to the end of the logged message.

Appendix: RADIUS

C

This appendix covers these topics:

RADIUS

Note: The SecureConnect Manager User's Guide includes information about RADIUS because the book explains how Ascend's Firewall Control Protocol can change firewall behavior based on information that the Firewall Control Manager obtains from RADIUS user profiles. You cannot use RADIUS user profiles to authenticate users who dial in to a Pipeline unit, or to store authorization information about the types of connections you permit the users to establish. You can use RADIUS user profiles to authenticate and authorize users who dial in to MAX routers to request a connection. MAX routers support the SecureConnect firewall security feature, but do not support encrypted Virtual Private Network tunnels.

Remote Dial In User Service (RADIUS) is a means for authenticating and authorizing a network's dial-in users and outbound users. As defined in IETF RFC 2138, RADIUS is a method of identifying each user who wants access to a network. Each user is required to supply some information which matches data stored in a file called `users` on the RADIUS server. The server's `users` file is a database of user profiles. Each profile in the `users` file contains entries called attribute/value pairs. Attribute/value pairs that are required in each profile provide the user's name and some form of password or authentication method.

Profiles might also contain other entries that define a user's connection and the network services he or she can use.

Note: Ascend Access Control is a RADIUS server, and the SecureConnect Server includes a 30 day trial version of Access Control.

RADIUS attributes are divided into two classes. One class is called *authentication*. RADIUS uses authentication attributes to find a user's profile and to verify the user's identity. The second class is called *authorization*. RADIUS uses authorization attributes to define user connections and services. RADIUS sends authorization attributes it finds in a user's profile to the machine the user contacted to make a network connection. Authentication and authorization attributes are also referred to as *check-items* and *reply-items*, respectively.

RADIUS user profiles

In a RADIUS `users` file, information about an individual user constitutes a *user profile*. Each user's profile begins with a line that flush left and identifies the user. For example:

```
User-Name = djones
```

`User-Name` is a RADIUS attribute, and in this example, the attribute's value is `djones`. `User-Name` is an authentication attribute. All authentication attributes must be on the first line of the user's profile, although the first line may wrap if necessary, as long as the software does not insert a newline indicator. End the authentication line with a comma. Authorization attributes (*reply-items*) follow on indented lines. Each reply-item line must begin with white space, and each reply-item line, except the last line in the user's profile, must end with a comma. The format of a user profile is as follows:

```
User-name check-item [, check-item]...,
    reply-item,
    reply-item
```

Vendor-specific RADIUS attributes for user profiles

The RADIUS protocol defines many attributes and their possible values, and the protocol is extensible. Vendors can create new attributes as long as the attributes comply with the standards of the RADIUS protocol. Each implementation of

RADIUS comes with a dictionary of attributes. The Access Control dictionary of attributes and values is significantly larger than the standard RADIUS dictionary because it includes attributes based on Ascend's router configuration parameters. An example of a vendor-created attribute is Ascend-FCP-Parameter ("RADIUS clients" on page C-3). Ascend developed this attribute so user profiles can contain information that FCM can receive and package in FCP packets it sends to SecureConnect routers to change the behavior of the routers' firewalls.

RADIUS clients

Users who want to be authenticated don't contact a RADIUS server. They contact a Network Access Server, or client, and the client contacts RADIUS. The server only communicates with clients it can identify. Each client from which RADIUS will accept an authentication request is listed file called `clients`, which, like the `users` file, is located in the RADIUS data directory FCM is a RADIUS client.

The format of a RADIUS server `clients` file entry is:

```
Client Name Key Type Version
```

Clients send an Access-Request packet to a RADIUS server. The packet usually contains a user's name and might include a password. When RADIUS can authenticate both the client that sends the request and the user referred to in the request, the server sends the client an Access-Accept packet. Access-Accept packets might contain authorization attributes from user profiles.

Firewall Control Manager is a RADIUS client.

Appendix: Warranty

D

This appendix contains the Ascend End User Agreement that covers the purchase and use of SecureConnect Manager software.:

ASCEND END USER AGREEMENT

License

The term “Software” includes all Ascend and third party (“Supplier”) software provided to you with this Ascend product, and includes any accompanying documentation (the “Documentation”). The term “Software” also includes any updates of the Software provided to you by Ascend at its option. Subject to the terms of this Agreement, Ascend grants to you, and you accept, a personal, non-exclusive, and nontransferable (except as set forth below) license to use the object code version of the Software on a single computer. The Software is “in use” on a computer when it is loaded into the temporary memory (i.e. RAM) or installed into the permanent memory (e.g. hard drive, CD-ROM or other storage device) of that computer, except that a copy installed on a network server for the sole purpose of distribution to other computers is not “in use.” If you permanently install the Software on the hard disk or other storage device of a computer (other than a network server) and you use that computer more than 80% of the time it is in use, then you may also use the Software on a portable or home computer. You may make a reasonable number of copies of the Software

and Documentation for backup or archival purposes only, so long as Ascend's and its licensors' copyright notices are reproduced on such copies.

Limitations on Use

You may not copy, rent, lease, sell, sublicense, assign, loan, time-share or otherwise transfer or distribute copies of the Software or Documentation to others, except as set forth in this agreement. You may physically transfer the Software from one computer to another provided that you do not retain any copies of the Software, including any copies stored on a computer. You may permanently transfer this license to another user, but only if you transfer or destroy all copies of the Software and Documentation, and the recipient agrees in writing to be bound by all of the terms of this agreement.

You agree that you will not decompile, disassemble, or otherwise reverse engineer the Software, and you will use your best efforts to prevent your employees and contractors from doing so, except to the extent that such restriction is expressly prohibited by applicable law. You may not modify, adapt, create a derivative work, merge, or translate the Software or the Documentation without the prior written consent of Ascend.

Specific Suppliers may be identified in the Documentation. You agree to any additional terms and conditions specific to particular Suppliers or Products, as described in the Documentation, which are incorporated herein by reference.

Intellectual Property Rights

You acknowledge that Ascend or its Suppliers retain exclusive ownership of all copyrights, trademarks, patents and/or other intellectual property rights in the Software and the Documentation. You are not granted any rights in the Software or Documentation other than the license rights expressly set forth above.

Term and Termination

The term of this license is for the duration of any copyright in the Software. This license automatically terminates if you fail to comply with any of the terms and conditions of this agreement. You agree that, upon such termination, you will either destroy (or permanently erase) all copies of the Software and

Documentation, or return the original Software and Documentation to Ascend. You may terminate this license at any time by destroying the Software and Documentation and any permitted copies.

Limited Warranty and Limited Remedy

Ascend warrants to the original end user purchaser only that the Software as delivered at the time of purchase will substantially conform to the Documentation, and that the original diskettes and Documentation are free from defects in material and workmanship under normal use, for a period of ninety (90) days from the original end user's purchase thereof (the “Limited Warranty Period”), provided the Software is used with compatible computer hardware and operating systems. This limited warranty is void if failure of the Software has resulted from accident, abuse, or misapplication. Ascend's entire liability, and your sole and exclusive remedy shall be, at Ascend's option, either to (a) correct or help you work around or avoid a reproducible Error, (c) replace defective diskettes or Documentation or (b) authorize a refund, so long as the Software and Documentation are returned with a copy of your receipt within ninety (90) days of your date of purchase together with a brief written statement describing the alleged Error. An “Error” is a defect in the Software that causes it not to perform substantially in accordance with the limited warranty set forth above. Any replacement Software or Documentation will be warranted for the remainder of the original warranty period only.

No Liability of Suppliers

You acknowledge that your rights under this Agreement, in the nature of warranty or otherwise, are solely against Ascend. NO SUPPLIER MAKES ANY WARRANTY, ASSUMES ANY LIABILITY, OR UNDERTAKES TO FURNISH TO YOU ANY SUPPORT OR INFORMATION CONCERNING PRODUCTS OR ANY PORTION OF PRODUCTS. You hereby release all Suppliers from any claims, damages or losses arising from the use of Products, regardless of the form of action.

Disclaimer of Warranties

EXCEPT AS SPECIFICALLY PROVIDED ABOVE, THE SOFTWARE AND THE DOCUMENTATION IS PROVIDED “AS IS,” WITHOUT WARRANTY

OF ANY KIND. ALL OTHER WARRANTIES ARE DISCLAIMED, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT OR THAT THE SOFTWARE'S FUNCTIONS WILL MEET YOUR REQUIREMENTS OR THAT ITS OPERATION WILL BE UNINTERRUPTED OR ERROR FREE. EXCEPT AS SET FORTH IN THIS AGREEMENT, THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE AND THE DOCUMENTATION IS WITH YOU. IF THEY PROVE DEFECTIVE AFTER THEIR PURCHASE, YOU, AND NOT ASCEND OR ITS SUPPLIERS, ASSUME THE ENTIRE COST OF SERVICE OR REPAIR. If a disclaimer of implied warranties is not permitted by law, the duration of any such implied warranty is limited to ninety (90) days from the date of purchase by the original end user purchaser. Some jurisdictions do not allow the exclusion of implied warranties or limitations on how long an implied warranty may last, so such limitations or exclusions may not apply to you. This limited warranty gives you specific legal rights, and you may also have other rights which vary from jurisdiction to jurisdiction.

Liability Exclusions and Limitations

IN NO EVENT SHALL ASCEND OR ANY SUPPLIER BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES OF ANY KIND (INCLUDING LOST PROFITS, LOSS OF USE OR INTERRUPTION OF BUSINESS), OR FOR LEGAL FEES, ARISING OUT OF THE USE OF THE SOFTWARE OR THE DOCUMENTATION, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT PRODUCT LIABILITY OR OTHERWISE, EVEN IF ASCEND HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL ASCEND'S AGGREGATE LIABILITY FOR ANY CLAIM EXCEED THE LICENSE FEE PAID BY YOU. This limitation shall apply notwithstanding any failure or inability to provide the limited remedies set forth above. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation(s) or exclusion(s) may not apply to you.

Proprietary Rights-Contracts with Certain U.S. Government

Agencies

If the Software is acquired under the terms of a Department of Defense or civilian agency contract, the Software is “commercial item” as that term is defined at 48 C.F.R. 2.101 (Oct. 1995), consisting of “commercial computer software” and “commercial computer software documentation” as such terms are used in 48 C.F.R. 12.212 of the Federal Acquisition Regulations and its successors and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995) of the DoD FAR Supplement and its successors. All U.S. Government end users acquire the Software and the Documentation with only those rights set forth in this agreement.

Export Restrictions

You acknowledge that the laws and regulations of the United States restrict the export and re-export of certain commodities and technical data of United States origin, including the Software and the Documentation, in any medium. You agree that you will not knowingly, without prior authorization if required, export or re-export the Software or the Documentation in any medium without the appropriate United States and foreign government licenses.

Severability

You acknowledge and agree that each provision of this agreement that provides for a disclaimer of warranties or an exclusion or limitation of damages represents an express allocation of risk, and is part of the consideration of this agreement. Invalidity of any provision of this Agreement shall not affect the validity of the remaining provisions of this Agreement.

General

This Agreement is the entire agreement between you and Ascend relative to the Software and Documentation, and supersedes all prior written statements, proposals or agreements relative to its subject matter. It may be modified only by a writing executed by an authorized representative of Ascend. No Ascend dealer or sales representative is authorized to make any modifications, extensions or additions to this agreement. This Agreement is governed by the laws of the State of California as applied to transactions taking place wholly within California between California residents, without application of its conflicts of law

principles. The United Nations Convention on Contracts for the International Sale of Goods is specifically excluded from application to this Agreement.