# Secure Access Manager User's Guide

*Ascend Communications*

Part Number 7820-0429-001 June 17, 1996

# Product warranty

**1** Ascend warrants that the MAX will be free from defects in material and workmanship for a period of twelve (12) months from date of shipment.

**2** Ascend shall incur no liability under this warranty if

- the allegedly defective goods are not returned prepaid to Ascend within thirty (30) days of the discovery of the alleged defect and in accordance with Ascend's repair procedures; or
- Ascend's tests disclose that the alleged defect is not due to defects in material or workmanship.

**3** Ascend's liability shall be limited to either repair or replacement of the defective goods, at Ascend's option.

**4** Ascend MAKES NO EXPRESS OR IMPLIED WARRANTIES REGARDING THE QUALITY, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE BEYOND THOSE THAT APPEAR IN THE APPLICABLE Ascend USER'S DOCUMENTATION. Ascend SHALL NOT BE RESPONSIBLE FOR CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGE, INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR DAMAGES TO BUSINESS OR BUSINESS RELATIONS. THIS WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES.

## Warranty repair

**1** During the first three (3) months of ownership, Ascend will repair or replace a defective product covered under warranty within twenty-four (24) hours of receipt of the product. During the fourth (4th) through twelfth (12th) months of ownership, Ascend will repair or replace a defective product covered under warranty within ten (10) days of receipt of the product. The warranty period for the replaced product shall be ninety (90) days or the remainder of the warranty period of the original unit, whichever is greater. Ascend will ship surface freight. Expedited freight is at customer's expense.

**2** The customer must return the defective product to Ascend within fourteen (14) days after the request for replacement. If the defective product is not returned within this time period, Ascend will bill the customer for the product at list price.

### Out-of warranty repair

Ascend will either repair or, at its option, replace a defective product not covered under warranty within ten (10) working days of its receipt. Repair charges are available from the Repair Facility upon request. The warranty on a serviced product is thirty (30) days measured from date of service. Out-of-warranty repair charges are based upon the prices in effect at the time of return.

# Ascend Customer Service

When you contact Ascend Customer Service, make sure you have this information:

- The product name and model
- The software and hardware options
- The software version
- The SPIDs (Service Profile Identifiers) associated with your product
- Your local telephone company 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
- The type of computer you are using
- A description of the problem

## How to contact Ascend Customer Service

| Ways to contact Ascend Customer Service | Telephone number or address |
|---|---|
| Telephone in the United States | 800-ASCEND-4 800-272-3634 |
| Telephone outside the United States | 510-769-8027 |
| E-mail | support@ascend.com |
| Facsimile (FAX) | 510-814-2300 |

You can also contact the Ascend main office by dialing 510-769-6001, or you can write to Ascend at the following address:

Ascend Communications
1275 Harbor Bay Parkway
Alameda, CA 94502

## Need information on new features and products?

We are committed to constantly improving our products. You can find out about new features and product improvement as follows:

- For the latest information on the Ascend product line, visit our site on the World Wide Web:
  `http://www.ascend.com/`
- For software upgrades and release notes visit our FTP site:
  `ftp.ascend.com`

# Contents

# About this guide

This guide explains Ascend Secure Access Manager (SAM), the router tool for building dynamic firewalls.

# What is in this guide

These topics are covered in this guide:

- Secure Access Manager overview
- Installing Secure Access Manager on a workstation running Windows
- Navigating Secure Access Manager
- Understanding packet filtering
- Building Secure Access firewalls
- Sending Secure Access firewalls to your routers

This manual includes these chapters:

- Chapter 1, “Introducing Secure Access Firewall”

  This chapter describes Secure Access Firewall, Secure Access Manager, and the system requirements to install Secure Access Manager.
- Chapter 2, “Enabling Secure Access Firewall”

  This chapter explains what you need to do to install and enable Secure Access Firewall on your Ascend router.
- Chapter 3, “Starting SAM”

  This chapter explains how to open Secure Access Manager.
- Chapter 4, “Exploring the SAM Interface”

  This chapter explains the Secure Access Manager screen.

- Chapter 5, “Building Firewalls”
  This chapter introduces packet filtering and Secure Access firewalls and provides an example of how to create a firewall.
- Chapter 6, “Sending Firewall Configurations to an Ascend Unit”
  This chapter explains how to send firewalls from the Secure Access Manager to your Ascend router.
- Chapter 7, “Adding Firewalls to Profiles”
  This chapter explains add firewalls you create using Secure Access Manager to your Ascend router’s profiles.
- Chapter 8, “Troubleshooting”
  This chapter contains answers to some frequently asked user questions.
- Appendix A, “Reference”
  The Reference section contains thumbnail descriptions of the services in the category box.

In addition to this manual, Secure Access Manager has extensive online context-sensitive help.

# This guide assumes you know

- Your company’s network security policies
- Ascend router configuration using the VT 100 emulation menu system
- Features of Windows-based applications including point-and-click selection methods
- TCP/IP Protocol architecture
- IP addresses
- Common TCP-based services such as Telnet, FTP, and HTTP
- Other common services and protocols used on the Internet

# Documentation conventions

This section shows the documentation conventions used in this guide.

| Convention | Meaning |
|---|---|
| **`Monospace text`** | Monospace text represents information that you enter exactly as shown, and it identifies onscreen text, such as, statistical information. |
| [] | Square brackets indicate an optional attribute that you append to a command. To include an attribute, type only the information inside the brackets. Do not type the brackets unless they appear in bold type. |
| *italics* | Italics represent variable information. Do not enter the words themselves in the command; enter the information they represent. |
| Key1-Key2 | Keys displayed next to each other represent combination keystrokes. To enter combination keystrokes, press one key and hold it down while you press one or more other keys. Release all the keys at the same time. |
| \| | The \| symbol separates command choices that are mutually exclusive. |
| **Note:** | A note signifies important additional information. |
|  **Caution:** | A caution means that a failure to follow the recommended procedure could result in a loss of data or damage to equipment. |
|  **Warning:** | A warning means that a failure to take appropriate safety precautions could result in physical injury. |

# Introducing Secure Access Firewall 1

This chapter introduces Secure Access Firewall and Secure Access Manager, its graphical user interface. It includes these sections:

# What is Secure Access Firewall?

Secure Access Firewall is a tool for creating dynamic firewalls. Secure Access Firewalls control network access at the router level. These firewalls monitor Internet Protocol (IP) data traffic arriving at the router and compare the packets to well-defined descriptions of acceptable and non-acceptable packets. You enable Secure Access Firewalls by adding them as filters to Connection Profiles and Mod Config Profiles. The firewalls are dynamic, responding to triggers in packet traffic. The dynamic, temporary changes resulting from the packet triggers make the firewalls more secure than static packet filtering.

# What is Secure Access Manager?

Secure Access Manager, or SAM, is a graphical user interface for configuring Secure Access Firewalls. SAM is a Windows-based point-and-click utility you install on a network-connected workstation external to the Ascend unit. From SAM you can send the firewall's configuration to your Ascend MAX or Pipeline. These firewalls are installed in the Telnet menu system where they can be assigned to Profiles.

# PC requirements for Secure Access Manager

The Secure Access Manager software will operate on any network-connected workstation meeting the requirements listed below:

- 1.2 MB hard drive disk space.
- Windows 3.x, Windows 95 or Windows NT operating system.

# Enabling Secure Access Firewall 2

This chapter explains what you need to do to install Secure Access Manager on a workstation and how to enable Secure Access Firewall on your Ascend MAX or Pipeline unit. It covers these topics:

# Installing Secure Access Manager

This section explains how to install Secure Access Manager (SAM) in these ways:

- from a diskette
- from the Ascend FTP server

## Installing SAM from a diskette

### Windows 3.x or Windows NT system

**Note:** This information is also in the Readme file on the diskette.

**1** Insert the diskette in the appropriate floppy drive

**2** Select File>Run from the Program Manager menu

**3** Enter A:setup in the text box if the diskette is in the A drive.

Substitute the correct letter to identify the drive if the diskette is not in drive A.

The SAM setup program will automatically install SAM. During setup you have the opportunity to designate where you would like SAM installed. The default directory is C:\ASCEND\SAM. The setup program also creates a program group for SAM in Windows' Program Manager.

### Windows 95 system

The procedure is essentially the same as described for a Windows system. In place of the Program Manager, run the setup program from the Windows Explorer application.

## Upgrading SAM from the Ascend FTP server

The Ascend FTP server address is ftp.ascend.com. You can download a zipped version of the latest SAM program and an unzip utility from these directories at the FTP site.

Secure Access Manager at /pub/Software-Releases/secure-access.

Unzip utility at /pub/Utilities directory.

Follow these directions when you have downloaded the file sam.zip and an unzip utility, if necessary, to your workstation's hard drive

**1** Create a staging directory such as C:\SAM.

**2** Unzip, or extract, the compressed files from sam.zip, placing the uncompressed files in the staging directory

**3** Run the setup program from Program Manager or Windows Explorer, depending on your version of Windows, as described in "Installing SAM from a diskette" on page 2-2.

# Enabling Secure Access Firewall

You must contact Ascend support to enable Secure Access Firewall, whether you load the SAM software from a diskette or download it from the Ascend FTP server at ftp.ascend.com.

Your Ascend support contact person will need your unit's serial number and may ask you for information about its configuration. You will receive hash codes that allow you to enable Secure Access Firewall. Contact Ascend support via one of the methods explained in "Ascend Customer Service" on page iv.

Make sure you have the latest Pipeline or MAX operating system before you contact Customer Support to enable Secure Access Firewall. Earlier versions may not support the firewall feature. You can get latest Pipeline or MAX system software from the following directories on the Ascend FTP site:

- For Pipeline products: /pub/Software-Releases/Pipeline/
- For MAX products: /pub/Software-Releases/MAX/

*Table 2-1. Secure Access Firewall model numbers*

| Model # | Description |
|---|---|
| P50-SO-ASA | Secure Access Firewall for P50 |
| P75-SO-ASA | Secure Access Firewall for P75 |

*Table 2-1. Secure Access Firewall model numbers*

| Model # | Description |
|---|---|
| P130-SO-ASA | Secure Access Firewall for P130 |
| M201-SO-ASA | Secure Access Firewall for MAX 200Plus |
| MX18-SO-ASA | Secure Access Firewall for MAX 1800 |
| MX20-SO-ASA | Secure Access Firewall for MAX 2000 |
| MXHP-SO-ASA | Secure Access Firewall for the MAX 4000, MAX 4002, MAX 4004 |

# Starting SAM

# 3

This chapter explains how to open Secure Access Manager and describes the layout of the graphical user interface. It covers these topics:

# Opening Secure Access Manager

Secure Access Manager (SAM) runs on either Windows 3.1, Windows 95, or Windows NT. This section explains how to open SAM on these platforms.

## Opening SAM from Windows 3.1 or Windows NT

If your system runs Windows 3.x or Windows for Workgroups, either of these two procedures will open Secure Access Manager from Windows' Program Manager.

### Program group icon

1. Select the SAM program group icon.
2. Double click on the sam.exe icon in the program group.
   This icon looks like the Ascend logo.

### File menu

1. Select File>Run from the Program Manager menu.
2. Enter the path and filename for SAM in the textbox.
   If you choose the default location during installation the entry is C:\ASCEND\SAM\sam.exe.
3. Select the OK button.

## Opening SAM from Windows 95

If your system runs Windows 95, this procedure will open Secure Access Manager:

1. Select the Start button at the bottom of the Windows 95 screen
2. Select Run
3. Enter the path and filename for SAM in the textbox of the dialog box.
   If you choose the default location during installation the entry is C:\ASCEND\SAM\sam.exe.
4. Select the OK button.

# Exploring the SAM Interface

# 4

This chapter explains the Secure Access Manager screen. The information includes the layout of the screen's options and how to select them. It covers these topics:

# SAM Menu and toolbar

The SAM screen is a Windows-style interface (Figure 4-1).

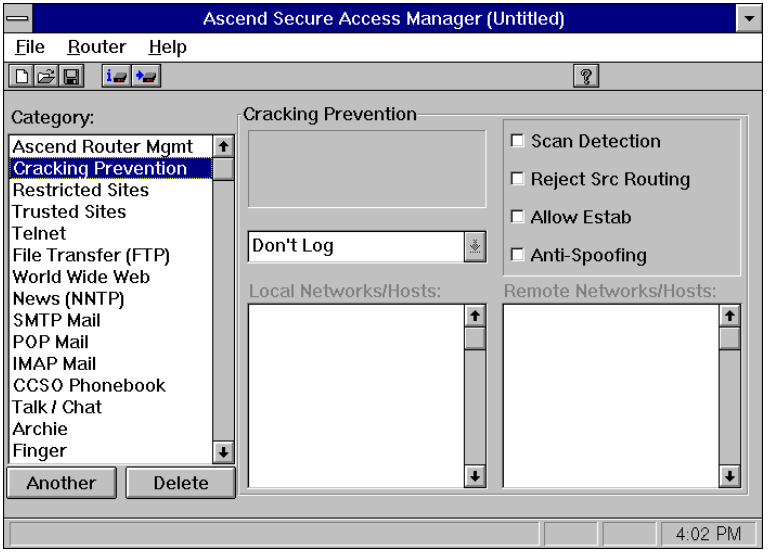


*Figure 4-1. SAM main screen*

At the top, below the title bar, are two areas called the menu bar and the toolbar. You select any item on either bar by moving your mouse cursor to an item and clicking your left mouse button. When you select a menu bar command a drop down list of associated commands appears. The toolbar buttons are shortcuts to performing the menu commands. When you become familiar with the menu commands you can select toolbar buttons to reduce keystrokes or mouse clicks.

## Menu bar

The menu bar contains three menu commands:

- File
- Router
- Help

# File menu

Select File to perform common tasks like opening and saving files. The drop down list that appears after selecting file includes these submenu commands:

## New

The New command provides a clean slate for building a new firewall. After completing one firewall, you may wish to create another one. Select the File>New menu commands to erase the options you selected for your first firewall.

**Warning:** When you select File>New you will not be prompted to save any previous selections. Remember to save firewalls or send them to your Ascend unit before selecting File>New.

## Open

The Open command brings up a dialog box from which you select the drive, directory and filename of a firewall file saved on your PC. The saved firewall's selections populate SAM. Use File>Open to edit an existing firewall file.

## Save

The Save command brings up a dialog box from which you select the drive, directory and filename for a firewall you wish to store on your workstation.

**Note:** All firewall configurations should be saved before sending them to your Ascend unit.

## Save As

The Save As command displays a dialog box from which you can save a firewall under a different name or file type. The two files types available are .FW and .PRF. You can read .FW files because they are ASCII-based. .PRF files are compiled and cannot be read or edited by SAM.

### Exit

The Exit command shuts down the Secure Access Manager program and returns you to the Windows Program Manager or the Windows 95 screen.

## Router menu

The Router menu contains two submenu items:

- Options
- Router Name/Address

### Options

The Options command brings up the Target Router Information dialog box. Target Router Information includes the following textboxes and checkboxes:

- **Router Name/Address:** A place to type the Ascend unit name or its IP address.
- **Firewall Name textbox:** A place to enter the name for the firewall options currently selected.

  **Note:** Until you change them, the Ascend unit and firewall names you enter in the textboxes are the default router and firewall names for the current SAM session.
- **Internal and External interface radio buttons:** Choices for the location of the firewall.
- **Auto Save to Disk checkbox:** Toggle switch that, when turned on, automatically saves the firewall in .FW format which can be read as an ASCII file or parsed by SAM.
- **Debug Log in sam.log:** Select this checkbox to record information about the establishment of a link between your workstation and your Ascend unit. Recording link information is only necessary if you experience difficulties when sending your firewall to the Ascend unit.

### Send

The Send command also brings up the Target Router Information dialog box. If you already used the Options command to enter router and firewall information in Target Router Information, a link to that router is established and the current firewall is sent automatically to the Ascend unit when you press the dialog box OK button.

**Note:** Change the router information before selecting the OK button if you wish to send the current firewall to a different Ascend unit.

- **Debug Log in sam.log:** Select this checkbox to record information about the establishment of a link between your workstation and your Ascend unit. Recording link information is only necessary if you experience difficulties when sending your firewall to the Ascend unit.

If you contact Ascend support for assistance, send your contact the sam.log file for analysis.

## Help menu

The Help menu has five submenu commands.

### This Screen

The This Screen command changes the mouse cursor to a help pointer. Move the pointer to any object on the SAM screen and click your left mouse button to receive information on that object.

### Help On

The Help On command opens the help Search dialog box.

### Contents

The Contents command displays a list of general topics covered by the SAM Help feature. Each listing is preceded by a colored bullet marker. A green marker means the listed item is session oriented. Items with blue bullets are not session oriented. Only the Cracking Prevention listing is preceded by a red bullet.

### Index

The Index command displays the complete list of topics covered by the SAM Help feature.

### About

The About command displays a dialog box with information about your version of SAM. If you seek help from the Ascend Technical Assistance Center, you may be asked for information from the "Template" line of the dialog box.


*Figure 4-2. The Help>About window with Template line information*

# Category box

The Category box is located on the left side of the SAM screen. The Category box contains a scrollable list of protocols, services and applications you select to build your firewall. Some of the options, such as Cracking Prevention, are highly recommended components for all firewalls. Others are very site dependent, such as Multimedia, which is the basis for blocking or allowing real time audio and video protocols.

**Note:** The Reference section contains short profiles about each security feature selection. You can also obtain this information by selecting Help from the menu bar or toolbar.

# Category options

To the right of the Category box are option radio buttons. The radio buttons usually include the options Incoming, Outgoing, and Enable, although different buttons may appear when you select a few of the security features in the Category box. If you select IP Address Resolution, for example, the options are ARP and RARP.

Click on the standard options to define a selected category's packets. Other options enable packet logging or refine the firewall's filtering granularity.

## Custom Categories

SAM includes the means to create firewall components for protocols that are not included in the Category box. Select Custom IP Protocol if you need to enable incoming or outgoing TCP or UDP traffic by via 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.

### Custom IP Protocol

In addition to the standard category options discussed in the next section, a drop down list and a textbox labeled Port Number appear in the SAM window when you select the Custom IP Protocol category. These are descriptions of the Custom IP Protocol options:

- **Port Number**: This option identifies the port where the Custom IP Protocol connection takes place. The port number may identify the protocol if the port number is well known, such as ports 20 and 23, which are reserved for FTP and Telnet. 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.
- Drop down list options:
  - **Inactive**: This option retains the incoming /outgoing designation, the port number, and the location textbox information for the selected Cus-

tom IP Protocol category, but deactivates the firewall defined by the category's entries.

- **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.

## 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 reference section includes a table of hexadecimal equivalents for common Ethernet types.

## Standard category options

**Incoming:** Select Incoming if you want the firewall to pass packets from a remote source to a local destination.

**Outgoing:** Select Outgoing if you want the firewall to pass packets from a local source to a remote destination.

**Enable:** Click on the Enable option to allow the selected service's packets to cross the firewall. Selecting the Enable radio button activates the Local and Remote textboxes. Textbox label changes in this chapter explains how the

selection of the Incoming or the Outgoing option affects the labels above these textboxes.

**Note:** SAM 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.

**Non standard options:** Non standard options may appear when you select certain protocols, services, or applications from the security features box. The Reference section contains detailed information on all supported services and service options.

**Protocol versions:** SAM supports different versions of some protocols and applications. You can refine the selection of IMAP Mail, for example, by selecting the v2/v4 and v3 options. The v2/v4 and v3 options may be selected separately, or at the same time. This is true whenever a category has version options. Notice that when a category may be defined by version, there is no Enable option. Selecting a version is the same as selecting Enable.

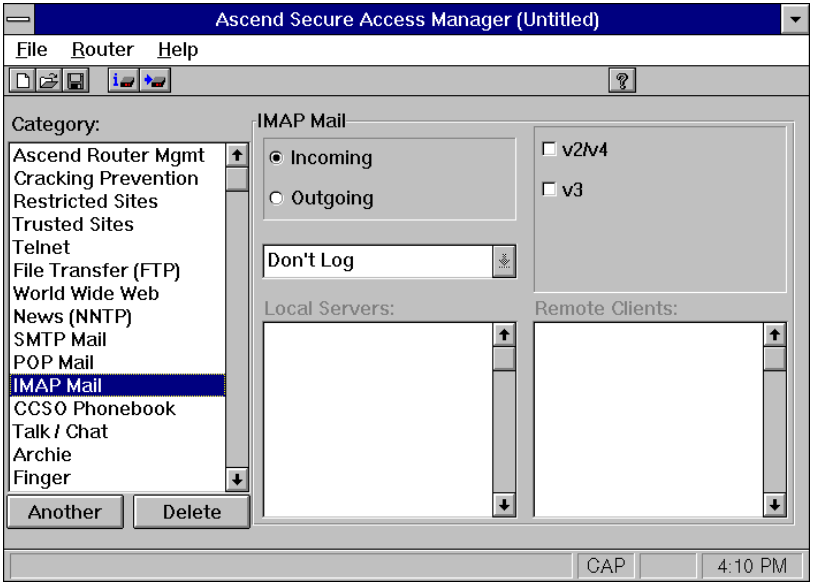


*Figure 4-3. The IMAP Mail service with version options v2/v4 and v3.*

- **Grouped services:** Some service selections such as Routing Information, Ping/Traceroute and Unix Utilities, group similar or related options under a single feature heading. For example, as Figure 4-4 shows, Routing Information's options include four different routing protocols, RIP, OSPF, EGP and BGP.

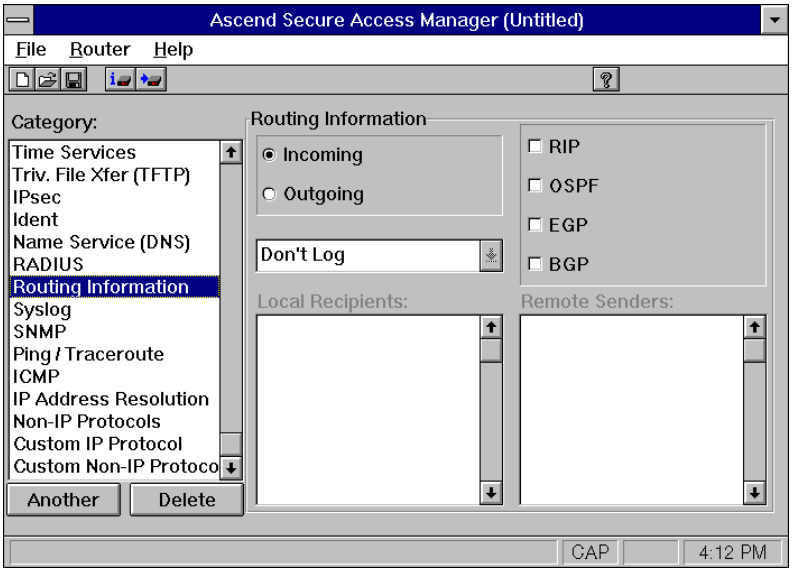


*Figure 4-4. The Routing Information service with RIP, OSPF, EGP and BGP.*

# Location textboxes

Two location textboxes, Local and Remote, occupy the lower portion of the SAM window. Location textbox entries identify the sources and destinations of the packets defined in the firewall.

**Note:** You must make an entry in each location textbox when you create a firewall. The firewall will not function if you leave the local or remote location textbox blank.

## Textbox label changes

If your firewall allows incoming packets, the local textbox is labeled “Local Clients” and the remote textbox is labeled “Remote Servers.” If your firewall enables outgoing packets the labels are “Local Servers” and “Remote Clients.” There are a few exceptions to this, but the exceptions are logically related to the actions of particular firewall security features. For example, if you choose Restricted Sites from the list of security features, the location textboxes are labeled “Grounded Locals” and “Undesirable Outsiders.”

### Location textbox entries

IP addresses are always acceptable in location textboxes, but fully qualified domain names are preferable for these reasons:

- Domain names are not affected by changes in domain IP addresses.
- SAM attempts to resolve all domain names in the firewall. You will receive an error message if SAM cannot resolve a domain name and SAM will not allow you to send the firewall to the router, although it will allow you to save the firewall as an .FW file.
- 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 the workstation running SAM can access a Domain Name Server (DNS) to resolve IP addresses and hostnames.

## IP addresses

IP addresses in the dotted quad format are acceptable textbox entries. You can also enter netmask addresses using either of these formats.

xxx.xxx.xxx.xxx/255.255.255.0

xxx.xxx.xxx.xxx/24

### Asterisks as wildcards

An asterisk character (*) entered in a location textbox functions as a wildcard. For example, if you enter an asterisk in the remote textbox of an incoming FTP firewall, the client(s) in the local textbox can receive FTP packets from any remote server. The asterisk is very useful for indicating that all addresses are enabled in the local or remote location textboxes. However, use it wisely.

### Multiple location entries

Each location textbox is large enough to accept multiple domain names, hostnames and IP addresses, in any combination. You can use the scroll bars at the right of each box if you require more space for entries.

**Note:** Separating the sites in each location textbox by hitting the Enter key does not create a one-to-one relationship between the local entry and the remote entry that appears on the same line. Therefore, when your SAM window looks like the one in Figure 4-5, each of the four remote clients can send telnet packets to each of the four local servers.

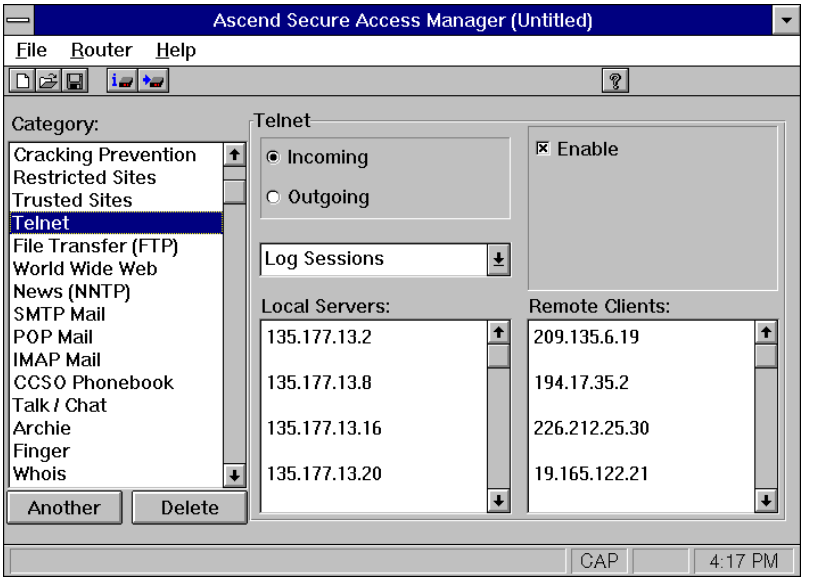


*Figure 4-5. Creating a firewall enabling four remote clients to telnet to all four local servers.*

### Creating multiple firewalls for a single security category

Near the bottom of the SAM window is a button labeled Another. When you click on Another you create a second appearance of the currently highlighted security category. The second appearance is preceded by an asterisk. Figure 4-6 illustrates the creation of a second telnet entry.

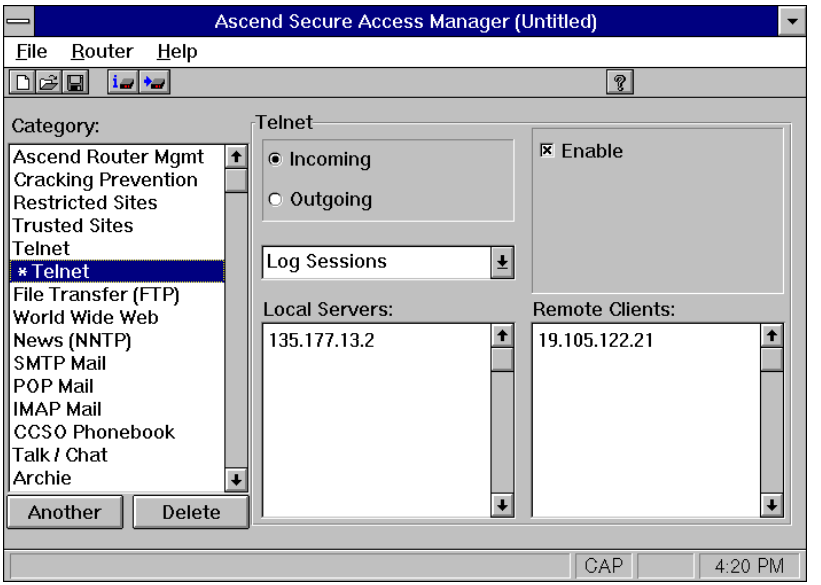


*Figure 4-6. Creating a second telnet entry in a firewall.*

### Deleting a Category box selection

You can remove firewall security selections from the Category box by selecting the feature and clicking on the Delete button located next to Another. SAM will not let you delete the last entry of a category box security selection. If you attempt to do so you will be instructed to disable the entry instead.

# Log options

Secure Access Manager automatically logs all packets rejected by a firewall. You can also select one of these four log options from the drop down Log box located

above the location textboxes. Like the location textboxes, the log box is not activated until you click on the Enable checkbox.

- **Don't Log**
- **Log Sessions:** Select this option to log the packets that start a session
- **Log All Packets:** Select this option to log all packets in a session
- **Trace All Packets**: Select this option to trace the route of packets that are not rejected

## Storing and retrieving log information

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

Syslog messages appear in the following format. The <message> portion may include one or more fields which are described in detail in Appendix A, "Reference."

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

The following table describes the fields in this syslog message. The message 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  194.70.42.65;21  156.150.203.9
```

*Table 4-1. Example syslog entries*

| Entry | Field | Description |
|---|---|---|
| Mar 22 | date | The date the message was logged by syslog |
| 17:02:06 | time | The time the message was logged by syslog |
| redfish | router name | The router which sent this message |
| ASCEND: | | |

*Table 4-1. Example syslog entries*

| Entry | Field | Description |
|---|---|---|
| wan0 | interface | The name of the interface where the firewall is installed. |
| tcp | message field <protocol> | the protocol of the packet traversing the firewall |
| 194.70.42.65;21 | message field <local> | the IP destination address of the received packet: port number for ftp command session |
| | message field <direction> | the direction in which the packet was traveling |
| 156.150.203.90 | message field <remote> | the IP source address of the received packet |
| 84 | message field <length> | the length of the packet in 8-bit bytes (octets) |
| !pass | message field <log> | the log label indicating the firewall blocked the packet |

# Building Firewalls

# 5

This chapter introduces packet filtering and Secure Access Firewalls. It covers these topics:

# Overview

Secure Access Firewalls are special kinds of packet filters. The following section briefly explains packets and packet filtering.

Data sent across an IP network is broken into small pieces called packets. Many different streams of IP network data may pass through the same router interface. Some may be from an outgoing Telnet session, for example, while others may be incoming packets from a remote World Wide Web server. Each packet travels separately and it must be identifiable so that it can be reassembled with its counterparts at its destination. Packets handled by the TCP protocol must also be identifiable so the protocol's transmission error checking can determine if all the packets from a session have arrived.

Packets are identifiable because of the headers attached to them as they pass through different layers of the TCP/IP stack. Each of the four layers adds its own header in front of the data being transmitted. Some information important to the packet filtering process is included in these headers.

*Table 5-1. Packet headers*

| Header Information | Description |
|---|---|
| Ethernet source and destination addresses | The Ethernet source, or the router that delivered the packet to the Ethernet. The Ethernet destination, or the router where the packet will be sent. |
| 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. |
| TCP source and destination ports | A two byte number associated with client and server processes, such as 21 for ftp and 23 for telnet |

*Table 5-1. Packet headers (continued)*

| Header Information | Description |
|---|---|
| TCP flags | SYN, which identifies the first packet in a TCP session. ACK, which, if set, identifies all session packets other than the initial packet.RST, the TCP RESET header bit FIN, the close connection header bit |

Most packet filtering implementations pass or deny packets based on packet header information. Secure Access Firewalls are one of the few implementations that also look into the data itself to make that determination.

Essentially, packet filters are rules. The rules include specific information about destinations, sources or protocols. One of the packet's headers must contain information that matches the information in the rules or the packet filter will discard it.

To simply illustrate this process, 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. This is known to be a server which contains sexually explicit material which can easily be downloaded across the Internet. Each outgoing packet is scrutinized and all packets that contain the IP destination address of the prohibited WWW server are discarded.

If you are familiar with the concept of packet filters, you are probably aware of their common implementation, described as static. Static packet filters are carefully arranged stacks of rules that determine what data enters and leaves the network through a router. The rules remain fixed, or static, after they are installed. The rules do not adapt to network traffic, but they do monitor it and control it like a sentry at a guard post. Static packet filtering is a standard feature of Ascend routers and filter rules are part of Connection Profiles and Answer Profiles. Consult your user guide chapter on using filters for more information.

Secure Access Firewall is a dynamic implementation. It is flexible, self-adjusting and temporal, meaning Secure Access Firewalls control not only what passes in and out of your network, but when it can pass, and for how long it can pass.

Secure Access Firewall uses templates which are edited on the fly in response to IP packet traffic. The templates are not packet filtering rules in the same sense that static packet filters are carefully constructed stacks of rules. When packet header information matches the requirements of a Secure Access Firewall the packets are allowed to pass. Triggers in the packet traffic, like a port number used by an ftp data channel, cause the templates to temporarily incorporate information about the session into the template specifications. The firewall then includes information that only relates to that session. Network access is shut down at the network destination port when the final packet of the session is received.

Secure Access Firewall templates are configured by choices you select in SAM, the Secure Access Manager. Secure Access Manager supports filtering 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 protocols, service and applications.

# Preparing to build firewalls

This section explains what you need to know about remote access to your network and the types of services you should consider filtering.

## Identifying your needs

### Network access and filtered services

Before you begin creating Secure Access Firewalls, you should gather some necessary information about your local network and the remote clients and servers that you will incorporate into the firewalls. Essentially, you need to decide which services you should permit and which you should deny. You should also decide where to permit the services and where to deny them. The reference section is an alphabetical list of the services, protocols and applications supported by Secure Access Firewall. The short descriptions included with the entries may be helpful when you are sifting through your firewall options.

Also consider whether any packets are required to maintain your network connections to outside networks. Some Internet Service Providers (ISPs) require

a routing protocol and will mark your link inactive if they receive no routing packets because your firewall blocks outgoing routing packets.

### Locations

When you have decided where you will allow access and where you will deny it, record the domain names, hostnames, or IP addresses of those locations. For reasons described under the heading Location textbox entries in Chapter 4, "Exploring the SAM Interface," domain names are the recommended form of entry in location textboxes.

# Building Firewalls

This section explains the process of building firewalls with Secure Access Manager. It contains these sections:

- Before you begin
- Selecting options
- Saving firewalls

## Before you begin

Keep the following information in mind before you begin building firewalls with Secure Access Manager.

### Router support for firewalls

- Different models of Ascend routers support different numbers of firewalls. The range of support is from 3 to 12 firewalls. Refer to your router's users guide to see how many firewalls your router supports.
- Contact Ascend Technical Assistance Center via the means listed in the front of this User Guide if you cannot find information about the number of firewalls your router can support.

### Default firewalls

- The Secure Access Manager has a default security philosophy.

**"That which is not permitted is denied."**

This means that, by default, no packets will pass through the firewall unless you specifically allow them to pass.

## Firewall sources and destinations

- You must select the Enable checkbox to activate the Local and Remote location textboxes.
- With one exception, your firewall will allow designated packets to pass between the sources and the destinations you enter in the location textboxes.

  The only exception occurs when you choose the Restricted Sites category. Your Ascend router's firewall will not pass any packets to or from Restricted Sites. As a reminder, the location textboxes are labeled Grounded Locals and Undesirables Sites when you choose Restricted Sites.
- Location textboxes accept fully qualified domain names, hostnames, and IP addresses. Qualified domain names are recommended. Reasons for this recommendation are explained in Location textbox entries.
- Source and destination information must be entered for each category of your firewall.
- Labels above location textboxes change according to packet direction.
- You may enter one or many sites in each location textbox.
- Wildcard entries represented by the asterisk character (*) are acceptable in either or both location textboxes.

## Firewall size

- You are not limited to any number of categories you may select for your firewalls. You may also choose to enable incoming and outgoing packets for most of these options.

**Note:** Some services such as telnet and ftp are bi-directional. A request to issue a command or to get a file must engender a response. SAM automatically enables response packets for features like ftp and telnet. You do not need to enable incoming from specific sites if you enable outgoing from a local client.

## Firewall location and direction

- SAM 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.
- Address Resolution Protocol (ARP) is necessary on Ethernet interfaces.
- Domain Name Service (DNS) is required if users access the Internet.
- Terms that describe the location and direction of firewalls, interfaces and packets are very similar, but they are not interchangeable. This table explains the distinctions among these sets of terms.

*Table 5-2. Firewall terminology*

| Terms… | Relationship Defined… | Description… |
|---|---|---|
| local/remote | Host to firewall | Describe a host's location as it relates to a firewall:<br>• a local client/server is inside the firewall<br>• a remote client/server is outside the firewall.<br>Use:<br>entering sources and destinations in local and remote textboxes |
| external/internal | Firewall to router | Describe a firewall's location as it relates to a router's interfaces:<br>• an external firewall is generally on the WAN interface<br>• an internal firewall is generally on the LAN interface.<br>Use:<br>Selecting a router interface in the Target Router Information dialog box |

*Table 5-2. Firewall terminology*

| Terms… | Relationship Defined… | Description… |
|---|---|---|
| incoming/outgoing | Session to firewall | Describe a session's direction at the firewall:<br>• enabled incoming sessions enter a firewall-protected network<br>• enabled outgoing sessions leave the firewall-protected network<br>Use:<br>Selecting security feature options that define the types of packets affected by a firewall. |

### Incomplete firewalls

- You can save firewalls on a local hard drive or diskette before sending them to the router. For example, if you lack important source or destination information you can always open the saved file and add the information later. In fact, if you can't wait to obtain a source or destination location, leave the category out of the firewall and send the firewall to the router. Later you can replace the firewall with a new, edited version.

**Note:** Although you can save firewalls and reopen them with a text editor, you should not attempt to manually edit them. If you open a firewall to see its contents the first words you will see are a warning to refrain from manually editing the file.

## Selecting Options

This section explains how you select firewall options. Screen shots of the Secure Access Manager illustrate the steps you take to make your selections.

This demonstration firewall includes three options from the list of protocols, services and applications in the Category box at the left of the Secure Access Manager screen. Although a firewall that includes the following items might

never be sent to a real router, this firewall does demonstrate many of the features you can incorporate into your firewalls.

During three phases of selecting security categories and options for your demonstration firewall you will:

- turn on Cracking Prevention for a network.
- enable outgoing ftp service from a single host and turn on the SAM logging feature.
- enable remote clients' access a local WWW server and turn on the logging feature.

## Phase 1 Cracking Prevention

The SAM window in Figure 5-1 shows that the firewall's Cracking Prevention is enabled by clicking in three checkboxes and entering destination and source information in the location textboxes.

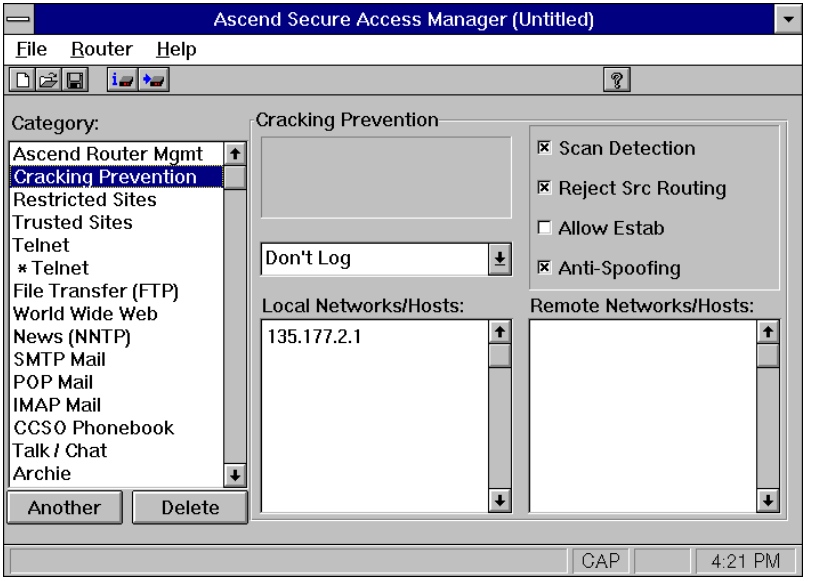


*Figure 5-1. Cracking Prevention turned on for network 135.177.2.1*

Follow these steps to create this portion of the firewall. Use your mouse to maneuver through the SAM window or tab from selection to selection.

**1** Select the Cracking Prevention security category.

**2** Next, select Scan Detection, Anti-Spoofing, and Reject Src Routing, three options visible in the screen's upper right hand corner.

- In this example, Allow Estab. has not been selected. Allow Estab. is a useful tool in some instances, but not necessary for blocking attackers. See Appendix A, "Reference," for more information on Allow Estab. and all the selections that make up this firewall.
- The local and remote textboxes only activate when you select the Anti-Spoofing feature. Scan Detection and Reject Src Routing do not require location address information. Anti-Spoofing, however, does require either a local or remote location textbox entry.

**Note:** Scan Detection, Reject Src Routing and Anti-Spoofing are different than other security category options, most of which require both local and remote location textbox entries. As noted in Step 2, the location textboxes are not even activated when you select Scan Detection or Reject Src Routing. Anti-Spoofing is unique because it only works if one or the other of the text-boxes contains location information. See the entry for Anti-Spoofing under the heading Cracking Prevention in the Appendix A, "Reference," for more information about using location information to define Anti-spoofing fire-walls.

**3** Enter 135.177.2.1 in the Local location textbox.

## Phase 2 Outgoing FTP

Switch from Cracking Prevention in Figure 5-1 to FTP in Figure 5-2 by clicking on FTP in the list of security categories.

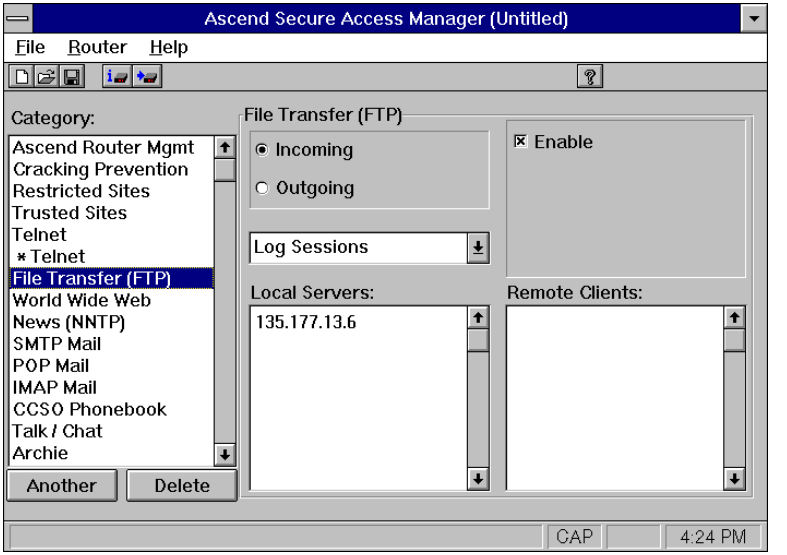


*Figure 5-2. Outgoing FTP enabled for host 135.177.13.6*

The choices you made for Cracking Prevention are retained. You do not need to save the firewall before selecting FTP.

The steps to create the FTP section of the firewall are similar to those you used in Phase 1 to turn on Cracking Prevention. Move through the selections by clicking on them or tabbing to them.

**1** Select FTP.

**2** Click on the Outgoing radio button.

**3** Click on the Enable radio button and activate the local and remote textboxes.

**4** Enter IP address 135.177.13.6 in the Local textbox to indicate the single internal host this firewall will allow to receive incoming FTP packets.

**5** Enter an asterisk (*) in the Remote textbox to indicate the firewall should allow outgoing packets from 137.177.13.6 to any remote server.

**6** Select the Log Sessions option to save information about the outgoing ftp sessions.

Remember that FTP is bi-directional and SAM automatically allows remote FTP servers' response packets for 135.177.13.2 through the firewall.

## Phase 3 World Wide Web

Switch from FTP in Figure 5-2 to World Wide Web in Figure 5-2 by clicking on FTP in the list of security categories.

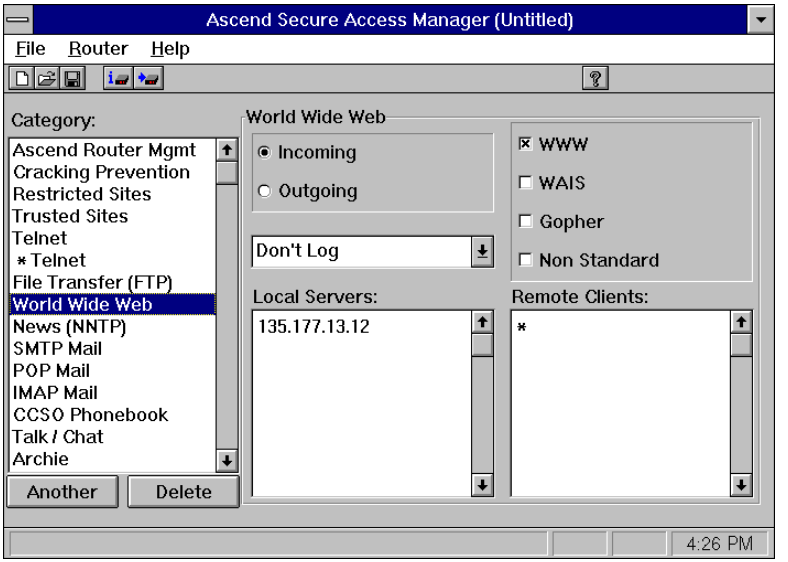


*Figure 5-3. Access to 135.177.13.2, a local WWW server, is enabled for any remote client.*

To complete your firewall:

**1** Select World Wide Web from the security categories list.

**2** Click on the WWW radio button to enable that option.

**3** Enter 135.177.13.2 in the Local textbox to indicate the IP address of the local WWW server.

**4** Enter an asterisk (*) in the Remote textbox.

5 WWW packets from all remote clients pass through the firewall to 135.177.13.2.

6 Select the Log Sessions option.

All WWW sessions to 135.177.13.2. will be logged.

## Building custom protocol firewalls

Although SAM includes many protocols and applications in its list of categories, you may need to consider how to handle UDP protocol packets or TCP packets for less common TCP protocols. The Custom IP Protocol selection offers options with which you can describe these packets and build a firewall that enables them to pass.

Building a firewall based on user defined IP protocols is very similar to building a firewall base on SAM's other category selections. The standard options are present and necessary, including Incoming, Outgoing, Enable and remote and local IP addresses. After choosing the direction of the packets and enabling their passage through the router firewall, you must also inform SAM of the type of protocol the firewall is for and the workstation port where the packets will be sent or received.

Unlike TCP packets, UDP packets do not contain flags, like SYN, which marks a TCP packet as the initial packet transmitted. If your firewall enables UDP traffic, you may select a general UDP session option or one of three other UDP options that identify the specific packets you want to pass the firewall. These specific options allow UDP query/response packet exchange or limit the enabled packets to those which are sent or those which are received.

The example firewall built by the procedure explained in this section allows SNMP query and response packets to pass between a local workstation and a remote server.

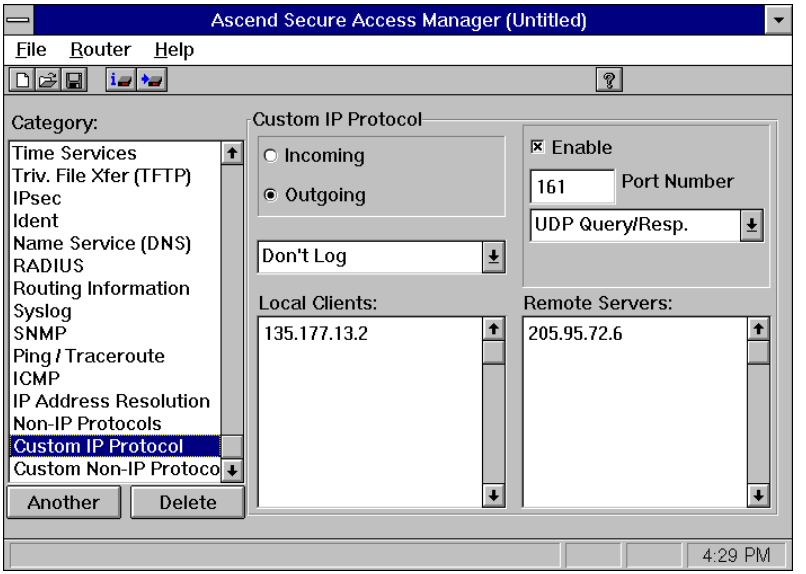


*Figure 5-4. SAM Custom IP Protocol window enabling SNMP query/response session.*

To build a UDP firewall:

**1** Select Custom IP Protocol from the Category list.

**2** Click on the Outgoing radio button.

**3** Click on the Enable radio button.

**4** Type 161, the well known port number for the UDP SNMP protocol, in the Port Number textbox.

**Note:** You can enter a range of port numbers in the Port Number textbox by separating the beginning and ending numbers with a hyphen. You cannot enter two ranges at a time. For example, “1-1024” is an acceptable entry. “1-1024, 4025-6500” is not an acceptable entry.

**5** Click on the word Inactive or the arrow beside it in the drop down list box below the Port Number textbox.

**6** Select UDP Query/Resp. from the drop down list.

**7** Type the IP address 135.177.13.2 in the Local Clients textbox.

**8** Type the IP address 205. 95.72.6 in the Remote Servers textbox.

**9** Select the appropriate Logging option from the Logging drop down menu.

**10** Save the firewall as an .FW file on your workstation or send it to your router.

## Building custom TCP session firewalls

Custom TCP session and custom UDP session firewalls are built the same way. The protocols of general TCP and UDP sessions are identified by the number in the Port Number textbox. The number will usually be a well known port number like 53, which in both TCP and UDP sessions is reserved for Domain Name Service.

All appropriate information concerning IP addresses and other category options should be entered or selected as described in the example under “Building custom protocol firewalls” on page 5-13.

## Deactivating a custom IP protocol firewall

You can disable a Custom IP Protocol firewall by deactivating the firewall. When you deactivate the firewall all of its entries are retained so you do not need to recreate it when the need to enable the packets arrives. This option is not available for Custom Non-IP Protocols.

To deactivate a custom IP protocol firewall:

**1** Select the Custom IP Protocol firewall you want to deactivate from the category list. If you have used the Another button to create more than one Custom IP Protocol firewall all but one of the Custom IP Protocol selections will be preceded by an asterisk.

**2** Click on the arrow in the drop down list box.

**3** Select Inactive from the drop down list.

**4** Send the firewall to the router.

## Building a firewall for bridged packets

You can control Ethernet traffic between network nodes by building a Custom Non-IP Protocol firewall that enables bridging of specific types of Ethernet

packets. The SAM window in the figure below illustrates how bridging of incoming Banyan Systems protocol packets is enabled on an Ethernet network.

**Note:** Enabling incoming Non-IP protocol packets does not automatically enable outgoing packets of the same protocol type. In the example, incoming Banyan System packets will pass the firewall, but outgoing Banyan System packets will not.

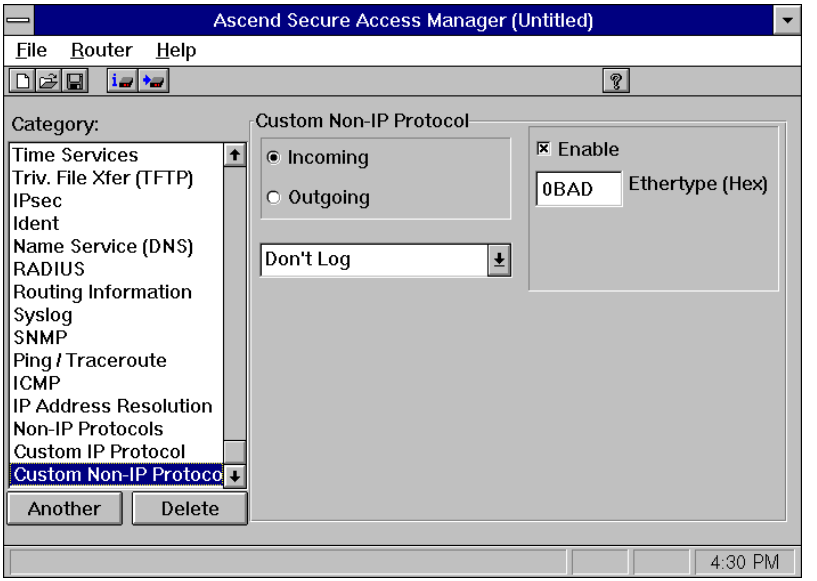


*Figure 5-5. Building a custom non-IP protocol firewall*

To build a custom non-IP protocol firewall:

1. Select Custom Non-IP Protocol from the list in Category.
2. Click on the Incoming radio button.
3. Click on the Enable radio button.
4. Enter 0(zero)BAD in the Ethertype (Hex) textbox.

   Refer to Table A-1 in Appendix A, “Reference,” for hexadecimal values for common non-IP protocols.
5. Select the appropriate Logging option from the Logging drop down menu.
6. Save the firewall as an .FW file on your workstation or send it to your router.

# Sending Firewall Configurations to an Ascend Unit

# 6

This chapter explains how to send firewall configurations from the Secure Access Manager to your Ascend Pipeline or MAX. It covers these topics:

# Before you begin

Before you begin the process of sending a completed firewall configuration to your Ascend unit you need the following information.

- The name or IP address of your default router
- The name of your firewall
- The names or IP addresses of any other routers you will send firewall
- The security level that is authorized to change or add firewalls on these routers
- The passwords for the authorized security levels

Also, verify your access to your Ascend unit.

**Note:** Refer to Chapter 8, "Troubleshooting," before you load a firewall on a network interface sitting between you and your Ascend unit. The tips in that chapter explain how to avoid closing your network access from your workstation to the Ascend unit.

# Target Router Information dialog box

The Target Router Information dialog box shown in Figure 6-1 is accessible from the Router menu or the Router Information button on the toolbar. The

information you enter in this box describes where you want to place your firewall.

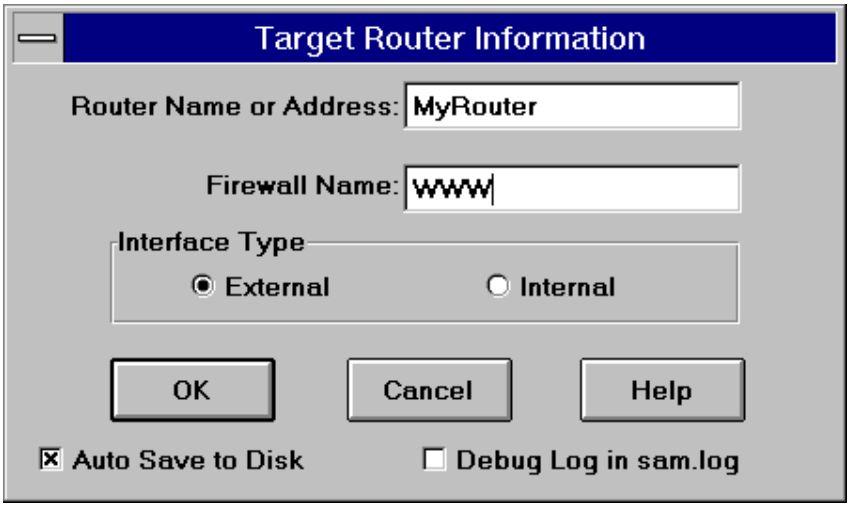


*Figure 6-1. Target Router Information dialog box.*

# Identifying a default router

The following section explains how to identify your default router for SAM. You can easily do this from the menu or toolbar. Because the toolbar is really a shortcut to the menu, both methods are discussed simultaneously.

There a five steps in the process of identifying a default router.

1. Select the Router>Options menu or the fourth toolbar button, Router Information, which displays a router and the letter “i”. The Target Router Information dialog box appears.
2. Enter the router’s name or IP address in the Router Name/Address textbox.
3. Enter the firewall's name in the second textbox.
4. Select the router interface on which to place the firewall.

The Internal interface is generally the Ascend unit's Ethernet connection, although Figure 6-2 illustrates a situation where the Ascend unit's Ethernet interface is external.

**5** Click on the dialog box's OK button.

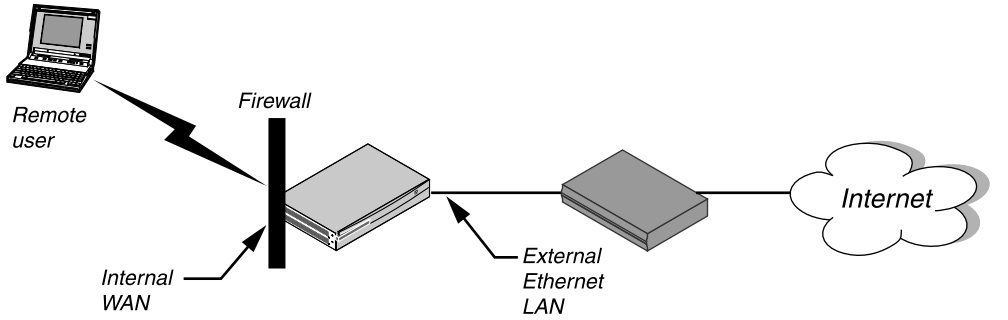


*Figure 6-2. The Ascend unit's Ethernet interface as external*

Figure 6-2 illustrates a configuration in which the Ascend unit's Ethernet interface is considered external because it is the remote user's means to a second router that provides access to the Internet.

# Sending your firewall to the default router

The five step procedure for sending a firewall to a default router is easy if you have verified a trouble-free connection to your router.

**1** Select the Router>Send menu or the fifth toolbar button, which depicts a router and an arrow.

The Target Router Information dialog box appears again. The names and addresses you entered for a default router are in the textboxes.

**2** Select the OK button

A box labeled 'Sending to Router' appears. The messages in the box are progress reports about the connection between your workstation and the Ascend unit. These messages are typical of what appears in the box.

```
"Contacting Router..."
"Connected to Router..."
"Getting List of Security Profiles..."
```

Secure Access Manager is retrieving information from the Ascend unit. When SAM is finished it displays a dialog box containing a list of security profiles it has received from the Ascend unit.

3 Select one of the security levels offered.

You will likely choose Full Access to obtain the authority to add your firewall to the Ascend unit.

4 Enter the required password if one is required.

5 Select a position for your firewall in the list shown in the Select Firewall dialog box.

**Note:** You will not be shut out for failed attempts if the password you enter isn't appropriate for the security level you choose. However, after four failures you must cancel the attempt to type in the password and select the security level again.

# Positioning firewalls

The number of firewall positions in the Select Firewall dialog box varies according to the model of the Ascend unit. Some Ascend units support three firewalls, others support up to twelve. You may place a new firewall in a position already occupied by another firewall if there are no available positions, or if you want to replace an out of date firewall.

Exercise caution when you do replace a firewall because its position number is used to identify the firewall when it is added to a profile. The packet filtering attributes of the new firewall and the replaced firewall are different. Each connection managed by a profile which included the old firewall will be controlled by the new firewall's filtering.

# Sending the firewall to a different router

You don't have to recreate a firewall to send it to a different Ascend unit. Merely change the router name in the Target Router Information dialog box. The dialog box is accessible from the Router menu or the toolbar buttons.

1. Select the Router>Send menu or the Send toolbar button displaying a router and an arrow.
2. Enter a new router name or IP address in the Target Router Information's Router Name/Address textbox.
3. Select one of the security levels offered.

   You will likely choose Full Access to obtain the authority to add your firewall to the router.
4. Enter the required password if one is required.
5. Select a position for your firewall in the list shown in the Select Firewall dialog box.

The Secure Access Manager sends your firewall to the new router and will continue to send succeeding firewalls there until you again change the router information in the Target Router Information dialog box. Your firewalls will always be sent to the Ascend unit that currently appears in dialog box's Router Name/Address textbox.

# Adding Firewalls to Profiles

# 7

This chapter explains how to add your firewall configuration to a Profile. It covers these topics:

# Before you begin

Before you begin reading this chapter you should review your Pipeline or MAX user guide, particularly the chapter on using filters. You should also verify your connection to your Ascend unit if you decide to follow the steps for adding your firewall to a profile.

# Firewall numbers

Depending on where you look for it, the number associated with a firewall may be 103 or 603. When you send your firewall to the Ascend unit you will assign it to a position identified by a 100 series number. However, when you look for the firewall in the Ascend unit's Firewall menu it will be identified as a 500 or 600 series number.

A 100 series number is an acceptable entry in a profile, but a 500 or 600 series number is not. If you attempt to use 603, for example, when assigning a firewall to a profile, you will receive an error message reminding you that the acceptable number range is 101 to 111, or whatever is appropriate for your MAX or Pipeline.

To avoid this problem, either record firewall's position number when you send it to the Ascend unit or add 100 to the last two digits of the Firewall menu number when you assign it to a profile. For example, if the number is 603 in the Firewall menu, enter it in the profile as 103.

# The Telnet menu system

Your Ascend unit's user guide contains extensive information about the Telnet menu system. This chapter will not duplicate the instructions of that document or describe how to access the Telnet interface.

Firewalls sent to the Ascend unit are stored in the Firewalls menu, level 20-600 in the Telnet interface.

# Assigning firewalls to a Connection Profile

Assuming that you have access to the menu and the authorization to add a firewall to a Connection Profile, the steps are the same you would use to add a Data Filter or Call Filter to a connection Profile. Data Filters control packet traffic on a session. Call Filters determine whether or not a packet will keep a connection up. Firewalls assigned to a Connection Profile filter incoming and outgoing traffic on a WAN connection and activate when a WAN session comes online.

**1** Select Ethernet, Connections, any Connection Profile, Sessions Options

**2** Enter your firewall number in the displayed brackets

**3** Type the Escape key to exit

**4** Select choice number 2 to exit and accept the new firewall

# Assigning firewalls to a Mod Config profile

These steps assume you have access to the menu and the authorization to add a firewall to a Mod Config Profile. Firewalls assigned to a Mod Config Profile filter incoming or outgoing traffic on the Ethernet interface. The firewall is activated when you save the Mod Config Profile changes.

**1** Select Ethernet, Mod Config, Ether options, Filter

**2** Enter your firewall number in the displayed brackets

**3** Type the Escape key to exit

**4** Select choice number 2 to exit and accept the new firewall

# Troubleshooting

# 8

This chapter answers some frequently asked user questions. It covers these topics:

**Note:** Read these tips before you load a firewall on a network interface sitting between you and the Ascend unit. The tips explain how to avoid closing your network access from your workstation to the Ascend unit.

# Assigning firewalls

## Can’t find firewalls on the Ascend unit’s Ethernet menu

I cannot see the “firewalls” menu on the Ascend unit’s Ethernet menu. Why not?

### Answer

There are two possible answers to this question.

1. You have not enabled the secure access feature.
   Contact Ascend Customer Service. The methods for contacting customer service are listed in the front of this User Guide.
2. Your Ascend unit’s software does not support Secure Access Firewall.
   Download a later version of the software from the Ascend FTP server at ftp.ascend.com.

## Invalid range for firewall number

I sent firewalls to the Ascend unit and tried to assign them to some profiles, but I keep getting a message saying I’ve selected a firewall number outside the valid range. I am using the firewall numbers that I see under the firewalls menu. What’s wrong?

### Answer

The numbers in the firewalls menu are not the same as the numbers assigned to the firewalls when you sent them to the Ascend unit via SAM. Appropriate numbers are within the 100-112 range, depending on your product. Those shown in the firewalls menu may be in a 600, or 500, range.

1. Open a firewall file you created and send it to the Ascend unit again. Or create a new firewall and send it to the Ascend unit.
2. When you are asked where you want to place the firewall, make note of the numbers associated with the existing firewalls and use them when assigning the firewalls to profiles.

## Saving firewalls

I saved a firewall before sending it to the Ascend unit and noticed that firewalls can be saved with an .FW or .PRF extension. What's the difference?

### Answer

.PRF and .FW files are very different, and it is important to recognize what happens when you save the firewall in one form or another.

An .FW file is a human-readable and program-parseable ASCII text file saved by SAM. You can open, edit and save an .FW type file using SAM's graphical user interface.

A .PRF file is a compiled filter ready for transfer and installation on the Ascend unit. You cannot open or edit the file with SAM.

# Editing firewalls

## Can't load edited firewall

I loaded a firewall and wanted to change it. However, I can't load another firewall. Why not?

### Answer

Check to see if you have disabled the ability to telnet from the workstation to the Ascend unit.

Your firewall must allow Telnet packets to pass when you want to reload a new version of a firewall. Perform these steps:

**1** Access the Ascend unit via its RS232 port to get to the Telnet interface.

**2** Disable the firewall by changing the "data filter" or "filter" entry in the correct profile to "0".

**3** Reload the firewall.

## Edited firewall not behaving as expected

I had a firewall set up and working, and decided to change something. I sent the modified firewall to the Ascend unit, but it is not behaving according to the new rules. What happened?

### Answer

Currently, a new firewall is not activated for an interface/connection until that interface/connection's profile has been modified, the line has been hung up, or the Ascend unit has been rebooted. Use one of these methods to activate your new firewall.

1. Hangup and redial the connection to activate a new filter for a connection.
2. Edit the Ethernet profile, changing the filter number to 0, then back to the desired number, To activate a new filter on a local interface.

# Routing problems

## Can't route packets from LAN through Ascend unit

I loaded a firewall and now nothing seems to pass from my LAN through the Ascend unit.

### Answer

There are two possible answers to this question.

1. You may have entered an asterisk (*) in one of the address boxes after enabling "Anti-Spoofing", severing all network activity.

   Edit the firewall file and remove the asterisk from the appropriate textbox. Save the firewall under its previous name and send it to the Ascend unit.
2. You may have applied a firewall to the Ethernet interface without enabling Address Resolution Protocol (ARP), which is necessary for the Ethernet interface to work.

   Edit the firewall file and enable ARP. Save the firewall under its previous name and send it to the Ascend unit.

# Telnet problems

## Telnet session freezes after sending a firewall configuration

After sending a firewall to my Ascend unit, I Telnetted to it, set my internal interface to use that firewall, and my Telnet session froze up. What do I do now?

### Answer

The Allow Estab option of the Cracking Prevention feature is not turned on. Exit from your frozen Telnet session then Telnet back into the Ascend unit again.

When Allow Estab is on, sessions established before the firewall is implemented can continue after the firewall is loaded. Your Telnet session started before the firewall was activated and the firewall did not recognize your Telnet session as a valid session, so it is blocking all the packets.

## Cannot Telnet after loading a firewall

I loaded a firewall but now I cannot Telnet to the Ascend unit.

### Answer

There are two possible answers.

1. Perhaps the firewall you loaded does not allow Telnet to the Ascend unit from the interface you used to access the Ascend unit. Log in via the Ascend unit's RS232 port and disable the firewall by changing the profile's "data filter" or "filter" entry "0".
2. This situation may also occur if you applied an Anti-Spoofing firewall on an Ethernet interface. Anti-Spoofing does not work as intended when it is enabled on an internal, or Ethernet, interface because traffic from the Ascend unit resembles a spoofing attack. The packets from the Ascend unit appear to be coming from outside your network, but the Ascend unit's IP address is on the same subnet as your internal network. Therefore, Anti-Spoofing stops all Telnet, syslog, route, and other useful traffic from the Ascend unit.

   If you need to put most of your firewall on the internal interface (usually internal interfaces are Ethernet interfaces, but not always), but still want anti-

spoofing protection, build a separate firewall for the external interface(s) that just has:

- Anti-Spoofing turned on, and the address of your internal network (e.g., 192.0.2.0/24) in the Internal Networks list.
- Trusted Sites enabled, and a "*" in the "Remote Clients/Servers" list.

## Cannot use host names to Telnet, but IP addresses work

I enabled Telnet, but I cannot use host names to Telnet between the networks that are connected by the Ascend unit. I can use IP addresses. What is wrong?

### Answer

If your domain name server is across the firewall from you, use SAM to enable DNS queries if you want to use host names with TCP services such as WWW, FTP, and Telnet.

# Logging problems

## Unwanted log messages

Why does the Ascend unit constantly log messages about packets that use UDP port number 520 or 38. Each log entry ends with "!pass (reject)" .

### Answer

You are logging RIP routing updates (UDP port 520) and NetBIOS (LAN Manager) packets (UDP port 138) rejected by the Ascend unit's firewall. These packets are sent out by other hosts on your network. You may also be sending out ICMP error messages in response to each packet.

Currently, the only way to stop logging these is to build a firewall that allows RIP routing updates and NetBIOS packets from internal hosts. Later Secure Access Firewall releases may offer a way to reject packets without logging them, reducing the number of "nuisance" log messages.

# Reference

# A

This chapter contains an alphabetic 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 Secure Access Manager (SAM) 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-4.

### 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 Networks 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 thwarts the common cracker technique of having an external machine impersonate a trusted internal system in order to access resources. These attacks are recognizable because the source addresses of spoofed hosts originate outside the network, but carry what appears to be an internal network address.

**Note:** The purpose of enabling the Anti-Spoofing option is to designate 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 not both.

**Note:** 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.

**Note:** In either case, do not enter an asterisk, address or hostname in the opposite location textbox. SAM would interpret this as an attempt to build a firewall that prevents spoofing of all those locations and the firewall would not work.

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

### Local Networks Box

Enter a list of network addresses internal to the user site in the Local Networks box. Anti-spoofing filters use these network addresses to identify trusted internal networks. Activating any of the Cracking Prevention features enables the Local Networks box. The box is a scrollable region, so long lists of networks may be entered.

### 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 SAM'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.

## Domain Name Service

The Domain Name Service, or DNS, is a facility for providing name to address translations for TCP/IP systems. DNS is a hierarchical service. IP naming

conventions segment host names using the period "." character. Thus, ftp.ascend.com indicates that a host called ftp can be found in the Ascend domain of a larger domain called com.

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 uses a list of contact information 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. Thus, to be able to resolve the names of external entities, select Outgoing Queries.

Selecting the Incoming Queries checkboxes allows the listed External hosts to query the specified Local Servers. The Dumps checkbox allows external systems to act as secondary name servers, and will allow dumps of the Local Servers address maps to be transmitted through the filter to remote name servers.

## 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.

Secure Access 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 may also send error messages when a host or network is unreachable, or a packet's options are malformed (Errors).

### Info Requests

Certain ICMP packets are used to request information like a network address, or an address netmask, from other machines

### Redirect

ICMP Redirect packets inform a host that, in the future, it should use a different route to contact a particular 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 to 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 may want to enable incoming ident as well, to give other mail servers the same courtesy.

## IMAP Mail

Secure Access 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 Encapsulated 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 and understand the security bulletins on Microsoft's WWW site, http://www.microsoft.com.

## Multimedia

Secure Access Firewall supports two options under Multimedia:

- RealAudio
- StreamNet

RealAudio and StreamNet 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 Secure Access News application to control which sites send news into the internal network and which sites may receive news from the internal network.

## 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

Secure Access 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

Secure Access 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, it is possible for routers to dynamically adapt to changing network conditions.

It is also possible to use routing information protocols to help to identify aspects of a network's topology or to mislead a host into mis-routing packets. SAM allows the construction of filters that can block the passage of any of four popular routing information protocols. Selecting any combination of the four protocol checkboxes will activate the Local Routers and Remote Routers areas.

## 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 SAM 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. SAM 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 opens holes for network management stations to gather data and change configurations of SNMP-manageable devices on the internal and external networks.

## 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. SAM 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, currently the most up to date (no pun intended) 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.

## 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 SAM, 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.

SAM 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 supporting graphical browsers such as Netscape, Mosaic, and Microsoft's Explorer.

### WAIS

Wide Area Information Servers that indexes large test databases.

### Gopher

A tool for browsing server directories.

### Non Standard

Custom protocols.

## 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 SAM makes the security considerations of “incoming X11” and “outgoing X11” more consistent with those of other SAM “incoming” and “outgoing” selections.

SAM considers an “outgoing” session to be one where the user (display) is local and the program is remote.

Conversely, a SAM “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 SAM 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 |

*Table A-1. Hexadecimal values for non-IP protocols (continued)*

| Non-IP Protocol | Hexadecimal value |
|---|---|
| AT&T | 8069 |
| Autophon (Switzerland) | 806A |
| 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 |

*Table A-1. Hexadecimal values for non-IP protocols (continued)*

| Non-IP Protocol | Hexadecimal value |
|---|---|
| Counterpoint Computers | 8083 |
| Cronus Direct | 8004 |
| 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 |

*Table A-1. Hexadecimal values for non-IP protocols (continued)*

| Non-IP Protocol | Hexadecimal value |
|---|---|
| DEC Unassigned | 6000 |
| DEC unassigned | 6009 |
| 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 |

*Table A-1. Hexadecimal values for non-IP protocols (continued)*

| Non-IP Protocol | Hexadecimal value |
|---|---|
| Experimental (Conflicts with 802.3 length fields) | 0101-01FF |
| General Dynamics | 8068 |
| 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 |

*Table A-1. Hexadecimal values for non-IP protocols (continued)*

| Non-IP Protocol | Hexadecimal value |
|---|---|
| Loopback (Configuration Test Protocol) | 9000 |
| LRT (England) | 7020-7029 |
| Matra (France) | 807A |
| 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 |

*Table A-1. Hexadecimal values for non-IP protocols (continued)*

| Non-IP Protocol | Hexadecimal value |
|---|---|
| SGI "bounce server" (obsolete) | 8016 |
| SGI diagnostic type (obsolete) | 8013 |
| SGI network games (obsolete) | 8014 |
| 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 |

*Table A-1. Hexadecimal values for non-IP protocols (continued)*

| Non-IP Protocol | Hexadecimal value |
|---|---|
| University of Massachusetts at Amherst | 8066 |
| VALID | 1600 |
| 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 |

*Table A-1. Hexadecimal values for non-IP protocols (continued)*

| Non-IP Protocol | Hexadecimal value |
|---|---|
| XNS Compatibility | 0807 |
| Xyplex | 0888-088A |
| Xyplex | 8088 |
| Xyplex | 8089 |
| Xyplex | 808A |

# Index

## Symbols



## A



## C

## D



## E



## F

## G



## H



## I



## K



## L

## M



## N



## O



## P

## R



## S

## T



## U



## W

## X