Gauntlet™ for IRIX™ Administrator's Guide

Document Number 007-2826-001

Gauntlet™ for IRIX™ Administrator's Guide
Document Number 007-2826-001

Contents

List of Examples

List of Figures

List of Tables

About This Guide

The *Gauntlet for IRIX Administrator's Guide* is intended for the person(s) responsible for network security at your site. Knowledge of UNIX® and network administration is assumed. The guide provides detailed information on how to configure the IRIX™ operating system to prevent unwanted access to your internal, trusted network hosts.

Gauntlet Documentation

This guide supplements, and in many cases overlaps, information provided by the user interface as you configure Gauntlet™ with forms which you access and modify using Netscape Navigator™. You may wish to look at this guide first to orient yourself, especially Chapter 1, "Firewall Basics,", which provides an overview of the product. If you are familiar with firewalls and wish to begin configuration immediately, refer to your software release notes for information on installing the software with Inst, and follow the instructions provided in the browser forms. Note that the forms provide links to additional information during each step of the configuration process.

This document does not address how to first connect to the Internet (see the WebFORCE™ Welcome page for the local link *Connecting to the Internet*). Also, it does not provide details on general system and network administration, but instead should be used in conjunction with the *IRIX Advanced Site and Server Administration Guide.*

The *Gauntlet for IRIX Administrator's Guide* is primarily concerned with helping you to construct a firewall—a system that separates your internal, trusted network from the external world, such as that represented by the Internet. Information is also provided to help you locate additional information sources and security tools, as well as vendors that supply various security-related products.

Caution: The *Gauntlet for IRIX Administrator's Guide* contains suggestions only, and Silicon Graphics can accept no liability for use or misuse of it. No document can be expected to address all details of security issues at your site. By understanding the underlying issues and making informed decisions regarding the degree of security you want to provide, you can create the kind of environment that best suits your needs. By monitoring your site and keeping up-to-date with developments in network security, you should be able to adjust and tailor your environment to ensure security while responding to user demands. This document and the Gauntlet software can go a long way in helping you establish secure network access, but you remain responsible for actively maintaining and refining network security.

What This Guide Contains

This guide contains the following chapters and appendixes:

- Chapter 1, "Firewall Basics"—Describes the role of a firewall—what it is, what it can do for you, and what it can't do for you. This chapter also provides a basic description of Gauntlet functionality and design considerations.
- Chapter 2, "Initial Configuration"—Discusses network hardware configuration (that is, how to situate your firewall in your network design), and provides a checklist to help you address areas of concern when implementing your firewall.
- Chapter 3, "Management Interface"—Covers the actual step-by-step configuration of the Gauntlet firewall host by use of a forms-based browser. Also provides information and pointers for those who prefer to edit system files and use the command line interface directly.
- Chapter 4, "Daily Operation and Maintenance"—Provides information on using reports and log files to monitor Gauntlet operation. Also provides pointers to additional documentation and network resources related to security issues.
- Appendix A, "Gauntlet and IRIX"—Provides a few notes on how the Gauntlet installation is integrated into the base IRIX operating system
- Appendix B, "Sample Reports"—Contains a few samples of the reports that the Gauntlet host can generate.

- Appendix C, “Configuring World Wide Web Clients”—Describes use of some popular World Wide Web browsers with the Gauntlet firewall.

Conventions Used in This Guide

In this document, text that appears on the screen, for example in an editing session, is shown in a typewriter-style font:

```
This is on the screen
```

Filenames, IRIX commands, and browser buttons are shown in italics; for example, the file and pathname */var/adm/SYSLOG* is printed *like this*.

When user input is shown, for example at a system prompt, the text is in bold:

```
# passwd gauntlet
```

The prompt is always shown as the superuser prompt (#) because use of the instructions in this document requires superuser privileges.

Additional Resources

This section provides pointers to various existing resources to help you secure your network.

Note: The lists of references, vendors, and so on is necessarily incomplete, and no mention should be construed as an endorsement by Silicon Graphics.

Books

The following books provide additional information on network configuration and network security.

- *Firewalls and Internet Security*, Steven Bellovin and William Cheswick, 1994. Addison-Wesley. ISBN 0-201-63357-4.
- *Internetworking with TCP/IP*, Douglas Comer, second edition, 1991. Prentice-Hall, Inc. ISBN 0-13-468505-9.

- *UNIX System Security*, David A. Curry, 1992 Addison-Wesley. ISBN 0-201-56327-4.
- *Practical Unix Security*, Simson Garfinkle and Eugene Spafford, 1991. O-Reilly & Associates, Inc. ISBN 0-937175-72-2.

Internet Resources

Internet resources relating to system and network security include answers to frequently asked questions (FAQs) from various newsgroups; documents concerning the history, practice, and theory of security; bulletins on new security issues; interactive mailing lists discussing security issues; and so on. World Wide Web pointers (URLs) are provided here rather than including the material in full as it is frequently updated.

Network Security and Firewall URLs

- *http://www.telstra.com.au/info/security.html*—many links to general network security information including security-related mailing lists.
- *http://www.sei.cmu.edu/SEI/programs/cert.html*—The Computer Emergency Response Team (CERT) Coordination Center was established by the Advanced Research Projects Agency to coordinate information regarding security threats for Internet users.
- *http://ciac.llnl.gov/*—The U.S. Department of Energy Computer Incident Advisory Capability page has links to advisory bulletins, mailing lists, documents and more.
- *ftp://ftp.tis.com/pub/firewalls/faq.current*—Firewall FAQ - Frequently Asked Questions and answers concerning firewalls.
- *ftp://ftp.uni-paderborn.de/doc/FAQ/comp.security.unix/*—General UNIX security FAQ.
- *http://www.alw.nih.gov/Security*—Links to a wide variety of security-related resources including multiple FAQs.
- *http://www-ns.rutgers.edu/www-security/index.html*—A home page for security issues related to the World Wide Web.
- *ftp://thumper.bellcore.com:/pub/nmh/skey*—Documentation and source code for S/Key authentication software.

- *ftp://ftp.nrl.navy.mil/pub/security/nrl-opie/*—source code for any POSIX-compliant UNIX system for OPIE (One-Time Passwords In Everything). OPIE is downward-compatible with the S/Key authentication software described in Chapter 3.

Note that URLs change and some of these may already be out of date. Use a good WWW search tool and search for various key words such as “network security” and “firewall” to find others.

Connecting to the Internet

The issues can be complex and confusing when trying to find the best way to connect to the Internet. The WebFORCE Welcome page includes a local link “Connecting to the Internet” which provides basic information and pointers to help you if you have yet to establish an Internet connection.

Contact your Silicon Graphics sales representative for information on the Netscape Proxy Server™ for IRIX and other Internet-related hardware and software tools.

Chapter 1

Firewall Basics

This chapter provides an overview of some of the basic features and terminology of the Internet, and introduces the Gauntlet Firewall and its basic features. This chapter contains the following sections:

- “The Internet” on page 1 summarizes the Internet—the major reason for interest in creating firewalls today.
- “Network Security Issues” on page 2 describes the role of firewalls in establishing and maintaining network security.
- “Gauntlet Firewall Functional Description” on page 4 summarizes the specific Gauntlet firewall functions which implement network security on an IRIX host.

The Internet

The Internet is a vast, connected network of heterogeneous computer resources, spanning the globe and growing daily. Increasingly, individuals and organizations are finding access to the Internet to be important for a wide variety of services pertinent to their businesses and other interests, including electronic mail, access to vast information archives, and keeping abreast of current developments in a host of areas.

Undoubtedly the most recent spur to the growth of interest in Internet access is the development of the World Wide Web, which provides both a “friendly” graphical interface to Internet resources and a standardized means of presenting and accessing them. Products designed for this market, such as WebFORCE, allow their users to establish an Internet presence that can be accessed around the world.

The Internet presents ways to share data that you want to share, but you must take measures to protect data that you want protected. The Gauntlet system presents one of the best ways to protect your internal, trusted

network from the Internet (or any untrusted network), while still allowing you easy access to the resources that are out there.

Network Security Issues

If you are connecting to any untrusted network such as the Internet, you should configure your connection so that you do not unwittingly risk the exposure or corruption of important data. You should know exactly which (if any) data you are making publicly accessible, and you should guard against the possibility of unwanted intruders gaining access to your site. The Internet has many known (and some famous) instances of unwanted intrusions, vandalism, and so on, and acknowledging and acting on such possibilities is the best way to ensure that your Internet presence is a pleasurable and profitable one.

While it is beyond the scope of this document to detail particular instances of malicious or criminal activity on computer networks, a great deal of such information is available on the Internet itself, and makes for useful reading for those responsible for computer security (refer to “Additional Resources” on page xv for pointers to additional information).

In general, you need to establish a line of defense between your trusted computer resources (your *internal* network) and the computer resources publicly accessible through the Internet (the *external* network). This line of defense should shield you from direct, external accesses, and it may be as simple as a single router or computer host or as complex as multiple routers and an entire computer network. (This document is concerned with establishing the secure firewalls possible with a computer host or network, not with the limited firewall protection of a router-only configuration.) Behind this line, you choose the degree to which you want to allow internal, trusted users access to the Internet, and the degree to which external users can access your internal resources. Your choices constitute your security policy.

What Is a Firewall?

One way of establishing the line between the external world of untrusted hosts and the internal world of trusted hosts is by creating a firewall. A

firewall is a combination of computer hardware and software that allows you to restrict interactions with the Internet to the degree you desire. The simple formula is the more access you allow, the greater the security concerns; the greater the restrictions you place on access, the easier it is to monitor and maintain security. The trade-off is one of ease of use versus peace of mind. For system and network administrators, this often translates as balancing the wishes of users with the needs and capacities of the administrator(s). The balance achieved must be determined individually for each site.

An example of a simple firewall is shown in Figure 1-1. In this illustration, a single computer host is configured with two network interfaces to become what is known as a dual-homed host—a host with a presence on each of two different networks. When it is configured as described in this document, it represents a single, controlled barrier between your internal network and the Internet where you can focus your security efforts.

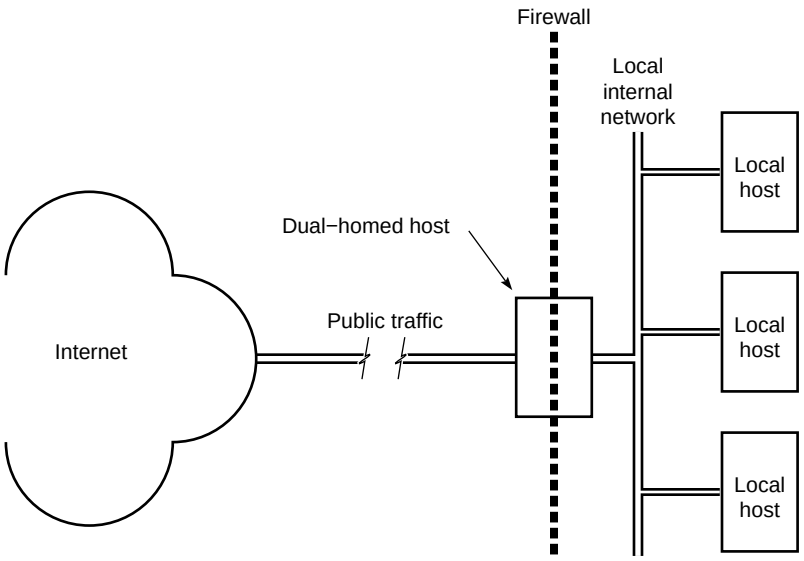

Figure 1-1 Firewall Environment

Gauntlet Firewall Functional Description

The Gauntlet firewall system is a standard IRIX system that has been modified to serve as a secure and flexible firewall. While firewall hardware can be implemented in one of several ways, the most secure and the one Silicon Graphics recommends is the dual-homed host configuration depicted in Figure 1-1. This configuration forces all traffic to go through the firewall and thereby eliminates some of the common holes in network security.

The Gauntlet firewall is designed to enforce security on connections between networks that are in different administrative domains, or which do not trust each other. In addition to enforcing security via access controls, Gauntlet firewalls provide detailed traffic reports and complete audit trails for information passing through the firewall. The Gauntlet firewall is implemented with a conservative design philosophy, placing security and assurance of correctness as the primary design objective for all services it provides.

To provide connectivity, the Gauntlet firewall does not rely on network-level filtering or traffic control as do many firewalls. Gauntlet firewalls act as a complete traffic block and transport all traffic through application layer service software (known as “proxies”) that act as a gateway to each service on behalf of the user. The basic services supported through a Gauntlet firewall are: TELNET, rlogin, FTP, NNTP (USENET NetNews), Gopher+, HTTP (World-Wide Web), the X-Window System, and SMTP-based electronic mail. For each service provided, there is a separate secure forwarding proxy server that performs protocol-specific access control and auditing. While this approach is less direct than simply using a router or packet-screening system that operates at the network layer, it is the only approach that provides a high degree of assurance and traffic control.

The default configuration of the Gauntlet firewall is that all networks other than the Gauntlet system itself are untrusted. Since the Gauntlet firewall starts with an empty user authentication database, no interactive traffic is permitted to cross it until either trusted networks are added, or until users are added to the authentication database.

Transparency and Encryption

Gauntlet V3.0 supports two additional functions that make it a superior application-level firewall: transparent proxies and IP- level encryption. Proxy transparency means that the firewall automatically “intercepts” outgoing connections and automatically invokes a proxy server on behalf of the user. Transparent proxies make it possible for the user never to have to explicitly interact with the firewall at all, while the administrator is still provided with precise access control and auditing information.

When the Gauntlet firewall is configured in transparent mode (see Figure 1-2), the network interfaces are labelled to the operating system as “internal” or “external.” Traffic originating from the internal interface is a candidate for transparent proxies, while traffic from the external interface is not. Internal workstations must be configured to route traffic through the firewall as if it were a router. Routes to the network are not advertised to the Internet by the Gauntlet firewall.

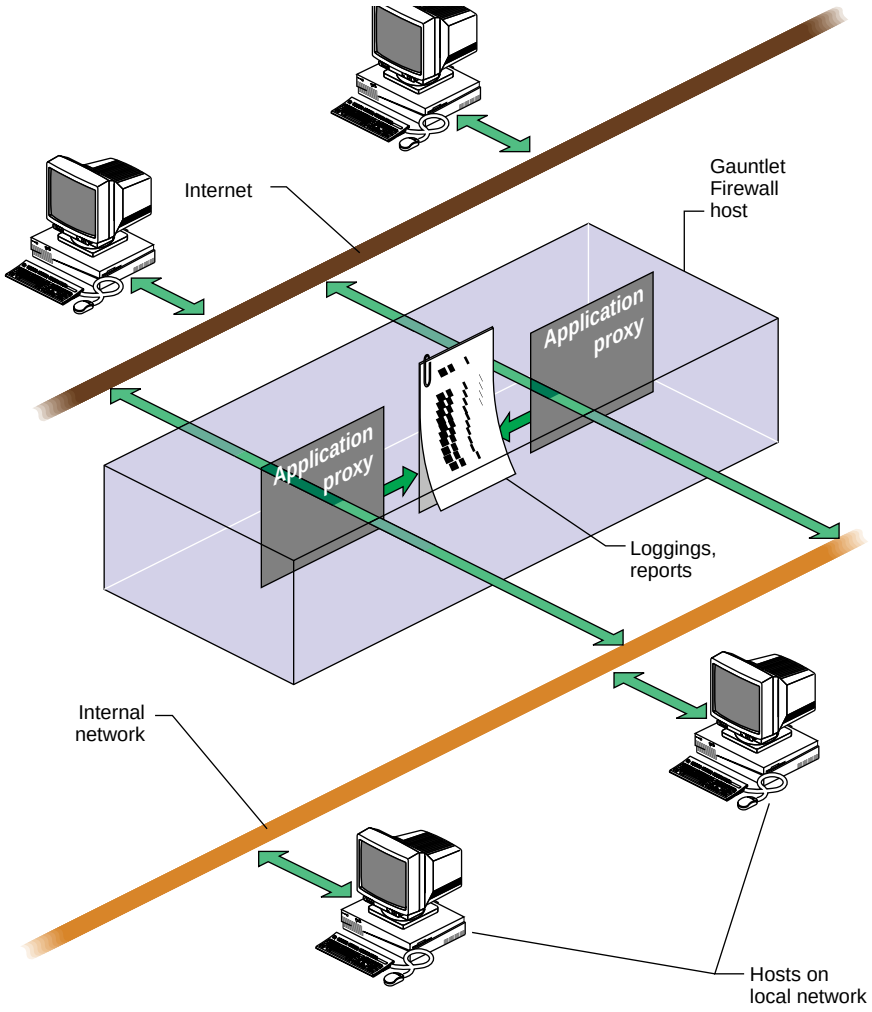

Figure 1-2 Transparent Proxies

IP-level encryption can be used to build Virtual Network Perimeters ("VNPs", as shown in Figure 1-3) between remote facilities operating with an untrusted network between them.[1] All traffic between the networks forming a VNP must be routed through the firewalls, which encapsulates and transmits the traffic encrypted using DES. When operating in this manner, the firewalls gateway, at an IP level, all traffic destined for the local

networks—proxies, therefore, are not required and any protocol and application may be used. An interloper who was monitoring traffic between the two firewalls would only see a single multiplexed stream of encrypted data between the firewalls, and would be unable to determine anything about the contents, source, or protocol of the traffic. The process used also "authenticates" traffic at a network layer, such that an attacker would have to mount a sophisticated cryptologic attack in order to be able to produce traffic that would decrypt as valid traffic at each firewall.

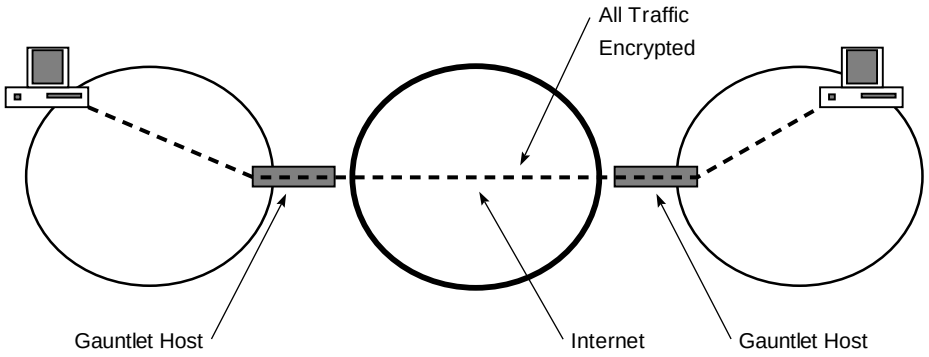

Figure 1-3 Virtual Network Perimeters over Untrusted Networks

Base Policy

To simplify installation and configuration, the Gauntlet firewall implements an access control policy based on the originating network. For general use, the Gauntlet Internet Firewall's configuration system supports a notion of "trusted networks" and "untrusted networks." Trusted networks are networks that are inside the security perimeter and from which access is permitted without an authentication step being required. Untrusted networks are outside the security perimeter and require authentication prior to being permitted access. Individual components of the Gauntlet software

[1] The IP Encryption option is available only within the US and Canada, due to US Government export regulations.

can be configured to further restrict or more precisely control traffic through the firewall.

In addition to the core security services provided, the Gauntlet firewall includes a forms-based systems management interface, which provides easy-to-use control over configuration and daily operation. (See Chapter 3, “Management Interface,” for details.) The Gauntlet platform is a truly open platform, and includes complete source code and documentation for its software.

Chapter 2

Initial Configuration

Introduction

This chapter contains the following sections:

- "Choosing Your Network Configuration" on page 9—describes the preferred network configuration in which the Gauntlet firewall is most effective.
- "Installation Procedure" on page 12—lists the steps you should follow to install a Gauntlet firewall host on your network.
- "Before You Begin" on page 14—provides a checklist designed to help you prepare for installation and configuration of the Gauntlet firewall.

The Gauntlet system is designed to connect between two networks, with a network interface connected to each. This documentation refers to "internal" and "external" network connections. The internal network is a trusted network (or networks), while the external network (or networks) is any untrusted network you want to connect to, for example, the Internet. The Internet is considered untrusted because anybody can try to access your network from it.

Choosing Your Network Configuration

Silicon Graphics recommends that you install the firewall using two network interfaces. In this way, routers are not a security-critical component of your network. If you are connecting a Gauntlet system to an existing subnet in which screening is already being performed by routers, your situation may require that you connect the firewall with only one network interface. Doing so requires care, since the security of the system then relies on a combination of the Gauntlet firewall and the screening routers; if the router is configured improperly, a security breach might result.

Figure 2-1 represents the standard, recommended configuration of a Gauntlet system. In this configuration, one interface is connected to each network, and traffic does not automatically flow across the firewall system (IP packet forwarding is disabled). Routers should be configured to maintain their own security and may optionally be configured to provide additional filtering as desired.

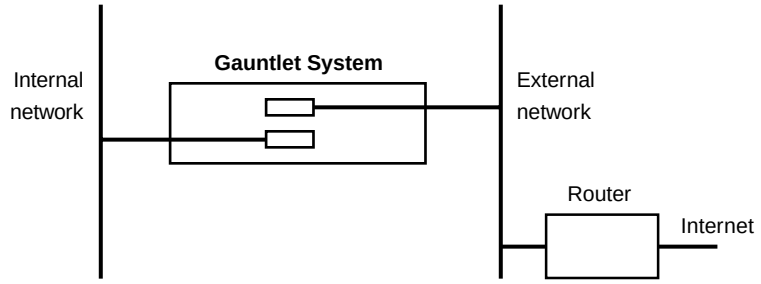

Figure 2-1 Recommended Gauntlet Installation

Figure 2-2 represents a Gauntlet system connected between networks that are screened using routers. Only a single interface is attached to the network. In this configuration, the security of the network depends not only on the Gauntlet system, but on the router(s) screening rules. Care must be exhibited when setting up the routers. Note that the router between the internal network and the external network in Figure 2-2 may be omitted at your discretion. If so, use extreme care to ensure that traffic is only permitted from the untrusted network to the Gauntlet system and not to any other hosts on the protected network.

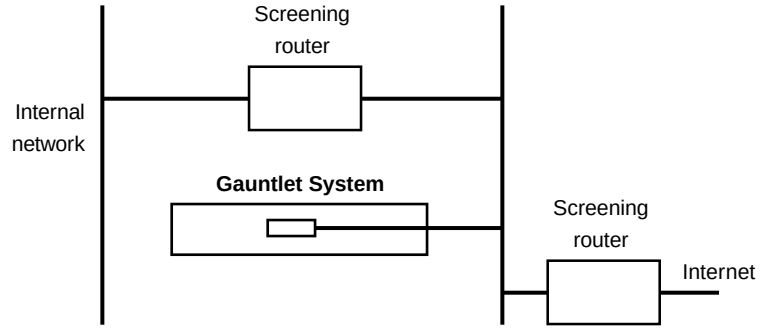

Figure 2-2 Less Secure Configuration Relying on Screening Routers

Using the configuration in Figure 2-2 is not recommended unless a particular environment absolutely mandates it.

Figure 2-3 illustrates a full-scale Gauntlet architecture in which two local area networks are protected by dual-homed Gauntlet hosts and connected via the Internet.

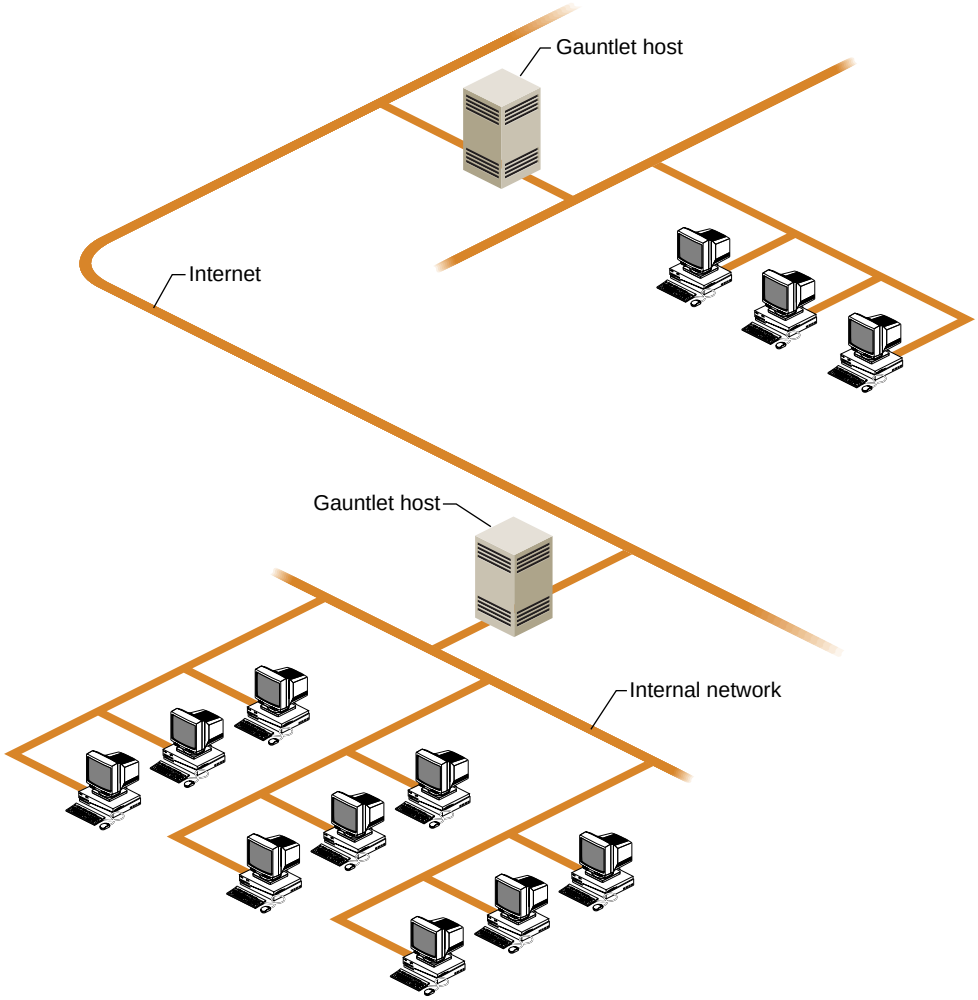

Figure 2-3 Example Gauntlet Network Architecture

Installation Procedure

This section is a list of steps we recommend you follow in sequence to install a Gauntlet firewall. Read through this list before proceeding.

Caution: The host should not be connected in the firewall position until specifically noted, and that is not until the last step of this procedure.

1. Read the section “Choosing Your Network Configuration” on page 9
2. Fill out the preparation checklist in the section “Before You Begin” on page 14.
3. Install a new release of IRIX on the host you plan to use as the Gauntlet firewall.

   Note: We recommend you install a completely new release so that you are starting with a known configuration. It is possible to install the firewall software on an established system, but we do not recommended it unless you must and are confident of your administrative expertise.
4. Add any additional network hardware that you are using. (Do not connect the Gauntlet host to the external connection until the final step.)
5. Install Gauntlet and Encrypt (U.S. only) from the installation media. Refer to your software release notes for details on software installation.
6. Click on *Network Setup (*and *ISDN Setup* and *PPP Setup* if you need them). Also click on *Minimize Exposure* under About Firewall Administration.
7. Step through the configuration forms (described in Chapter 3), and enter the information according to your setup and security policy as defined in the preparation checklist.
8. Once you have filled out the forms to your satisfaction, click on *Configure All* (on the introductory form). Any obvious problems are reported, so fix them, and run *Configure All* again until no major problems are reported.
9. You may now physically connect your Gauntlet host to the external network connection.

Chapter 3, “Management Interface,” describes the management interface (referred to in Step 7) you use to configure the Gauntlet firewall environment.

Before You Begin

Use the following checklist to help you establish your basic firewall implementation philosophy. You should have the information requested here (as appropriate for your design) before attempting to initialize the Gauntlet software.

Preparation Checklist

Follow the steps in this section to collect the necessary information before beginning the Gauntlet configuration.

1. Assign a designated system administrator and a backup administrator for the gauntlet system:
   - System administrator:_____

     Phone: _____

     E-mail: _____

     Beeper / Pager: _____
   - Backup administrator:_____

     Phone: _____

     E-mail: _____

     Beeper / Pager: _____
2. Is your network currently operational where the firewall is to be installed?

   When installing the Gauntlet host, be sure it is not connected to the external network until the configuration procedure as described in Chapter 3 is completed.
3. What is the contact information for your network service provider (for example, your Internet service provider)?

   Phone: _____

   E-mail: _____

   Beeper / Pager: _____
4. What is the speed / type of your network connection?

__ PPP / SLIP at _____

__ 56 KB

__ 218 KB

__ 512 KB

__ T1

__ Ethernet

5. What are the network hardware connections in use at your site?

   __ AUI—Location: _____

   __ 10BaseT—Location: _____

   __ BNC—Location: _____

   __ Other (describe)—Location: _____

6. Do you have administrative control of internetwork routers at the point where the firewall is to be connected?

   __ Yes

   __ No

   - If “No”, who has control?
   - Name: _____
   - Phone: _____
   - E-mail: _____
   - Beeper / Pager: _____

7. What is the network address of the internetwork router(s) where the firewall is to be connected?

   Router IP address: _____

8. What is the registered DNS domain for your network (if the firewall is to be connected to the Internet)?

   Your DNS domain name: _____

9. Is DNS currently administered by you or by a third party?

   __ By us

__ By third party:

- Name: _____
- Phone: _____
- E-mail: _____
- Beeper / Pager: _____

10. If you serve DNS for your domain, do you have an external system (such as your service provider) that is to act as a secondary server?

    __ No

    __ Yes

    - IP Address: _____
    - Name: _____
    - Phone: _____
    - E-mail: _____
    - Beeper / Pager: _____

11. Do you want to hide internal DNS information from external networks?

    __ No

    __ Yes

    - If so, you must have an internal DNS server:
    - Hostname: _____
    - IP address: _____
    - Administrator: _____

      Phone: _____

      E-mail: _____

      Beeper / Pager: _____

12. What is the internal address of the firewall (for dual-homed hosts only)?

    Hostname: _____

    IP address: _____

13. If the internal and external addresses are both part of the same network number, please ensure that you are using the subnet routing on your internal network. For example, if the external address is 192.33.112.55 and the internal address is 192.33.112.99. the firewall must be correctly configured with a subnet mask to enable it to determine if the hosts are on internal or external networks.
14. For each of the following protocols, determine access privileges, that is, whether access is permitted from inside out, and / or from outside in.

Table 2-1 Network Protocol Access Privileges

Protocol	External to Internal	Internal to External
Telnet		
FTP		
finger		
rlogin		
NNTP (USENET)		
http (World Wide Web)		

15. For each of the following services, describe whether strong authentication is required to access the network. (Strong authentication refers to the use of hardware or software means to provide single-use passwords.)

Table 2-2 Protocol Authentication Required

Protocol	External to Internal	Internal to External
Telnet		
rlogin		
FTP		

16. If the firewall host is physically accessible to the system administrator(s), should access be limited only to the console, or is network access (for example, Telnet) to be allowed?

__ Console access only

__ Network access allowed

17. Do you have a central e-mail hub that should receive all e-mail for *user@yourdomain.domain*?

    __ No

    __ Yes

    - Hostname: _____
    - IP address: _____

    If you do not have a central e-mail hub for your organization, describe where e-mail should go when entering or leaving your network (see Table 2-3).

Table 2-3 E-mail Routing

E-mail Address	Entering Network	Leaving Network
user@host.yourdomain.domain		
user@yourdomain.domain		

18. Should all outgoing e-mail from your domain have an address of *user@yourdomain.domain*? (This option makes sense only if there is a central hub for *user@domain.domain*.)

19. Are there any special mail gateway systems internally that the firewall should know about? For example, if you wish to set up virtual e-mail domains such as *user@MSmail.yourdomain.domain*, list special domains or interconnections that you may require.

    Special requirements: _____

20. Are you currently running USENET on your network?

    __ No

    __ Yes

    - Do you plan to gateway USENET NNTP traffic through the firewall?

      __ No

__ Yes

Internal news server:

Hostname: _____

IP Address: _____

External news server:

Hostname: _____

IP Address: _____

21. Do you plan to provide an anonymous FTP server?

__ No

__ Yes

22. Draw a diagram of your network including all connectivity points with the firewall, routers, and external networks, including dial-in[1], SLIP / PPP, frame relay, remote bridges, and so on.

[1] A dial-in line to the internal network is a weak point in security as the firewall (or even a router) does not control traffic through it in any way.

Chapter 3

Management Interface

Gauntlet Management Interface Overview

The Gauntlet system includes a network browser-based interface (“forms-based”) designed to make it easy for you to quickly configure and run the system. The Gauntlet management interface supports all common Gauntlet administrative functions and is organized (like this chapter) into the following browser forms:

Note: In addition to the use of the browser interface, you may, if you prefer, directly modify some of the files that this interface configures. Refer to “Viewing the Gauntlet File List” on page 26 for more information.

For initial configuration, you may prefer to simply step through the forms in order by selecting the *Continue* button at the bottom of each form as you finish with each form. Return to the previous form by clicking on *Back*. As you become more familiar with the interface and your configuration, you may prefer to go directly to any form by clicking on the appropriate form name in the bars at the top and bottom of a form.

You can view additional information on many subjects by selecting any linked word or phrase on the form. You can “unclutter” forms by hiding sections that you are already familiar with or that do not concern you. To hide a section of a form, click on the *Hide* button, shown in Figure 3-1.

Figure 3-1 Hide Button

The selected area is hidden from view and is represented by an *Unhide* button, shown in Figure 3-2.

Figure 3-2 Unhide Button

Click on the *Unhide* button to display more detailed configuration information on the corresponding section.

Caution: Clicking on *Hide* or *Unhide* buttons causes any unsaved changes *on that page* to be thrown away.

When you are satisfied with your configuration of a form, select *Save* at the bottom of the form. (In some forms, separate portions are added to databases when you select the *Add* button, and there is no general *Save* button for those forms.) Any known error in your configuration of the form is reported at this time, and you are given the opportunity to fix the error. You must save the configuration of each form you modify while you are still in the form for your modifications to be remembered. Note that clicking *Add* or *Save* does not cause any actual system configuration to take place—you can still exit or change any of the fields on any of the forms until you select the *Configure All* button at the bottom of the initial introductory form.

Do not select *Configure All* until you are sure that all of the forms are set up as you want them. Many (but not all) forms provide defaults which may suit your situation; the defaults are conservatively chosen so that network services are disabled until you specifically enable them.

Accessing the Gauntlet Management Interface

To access the management interface, you must be logged in as root. The command to start the management interface is *gauntlet-admin*. In a few seconds, a browser form requesting the Gauntlet administrative password should appear on your display. (If this is the first time you have run *gauntlet-admin*, you are prompted to create a Gauntlet administrative password. Also, if there is no root password on the Gauntlet host, you are prompted to enter a root password.) Refer to “Remote (Network) Connections” on page 35 for information on remote access to the administrative interface.

The following sections describe each of the Gauntlet management forms. Note that the forms-based interface is designed to be self-sufficient, and it may present enough information for you to make all appropriate configuration decisions. This documentation is intended to provide additional background information and may considerably overlap the information available through the forms.

Introductory Management Form

Figure 3-3 and Figure 3-4 illustrate the Gauntlet introductory management form. This form is both the entry point and the exit point of the forms-based management interface. From this form, you can go directly to any of the other management forms, or begin a sequential configuration sequence. When you have configured all the forms as desired, you must return to this form and select *Configure All* for the actual Gauntlet system configuration to occur.

Caution: Do not select *Configure All* until you have configured all the other forms appropriately.

The introductory management form describes how to use the forms-based interface, and then contains a list of form names at the bottom of the page that allow you to access another form, go to the next form, or configure your system.

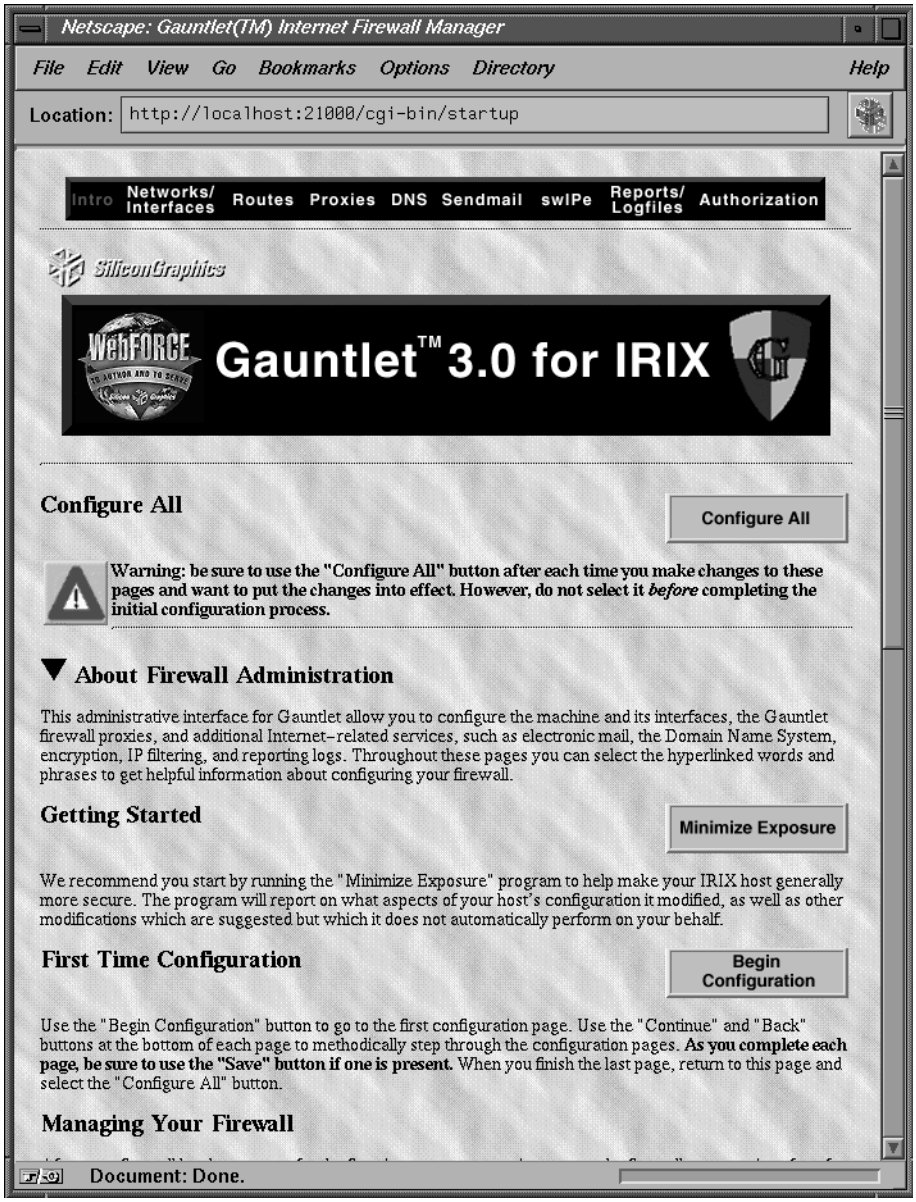

Figure 3-3 Gauntlet Introductory Management Form (1 of 2)

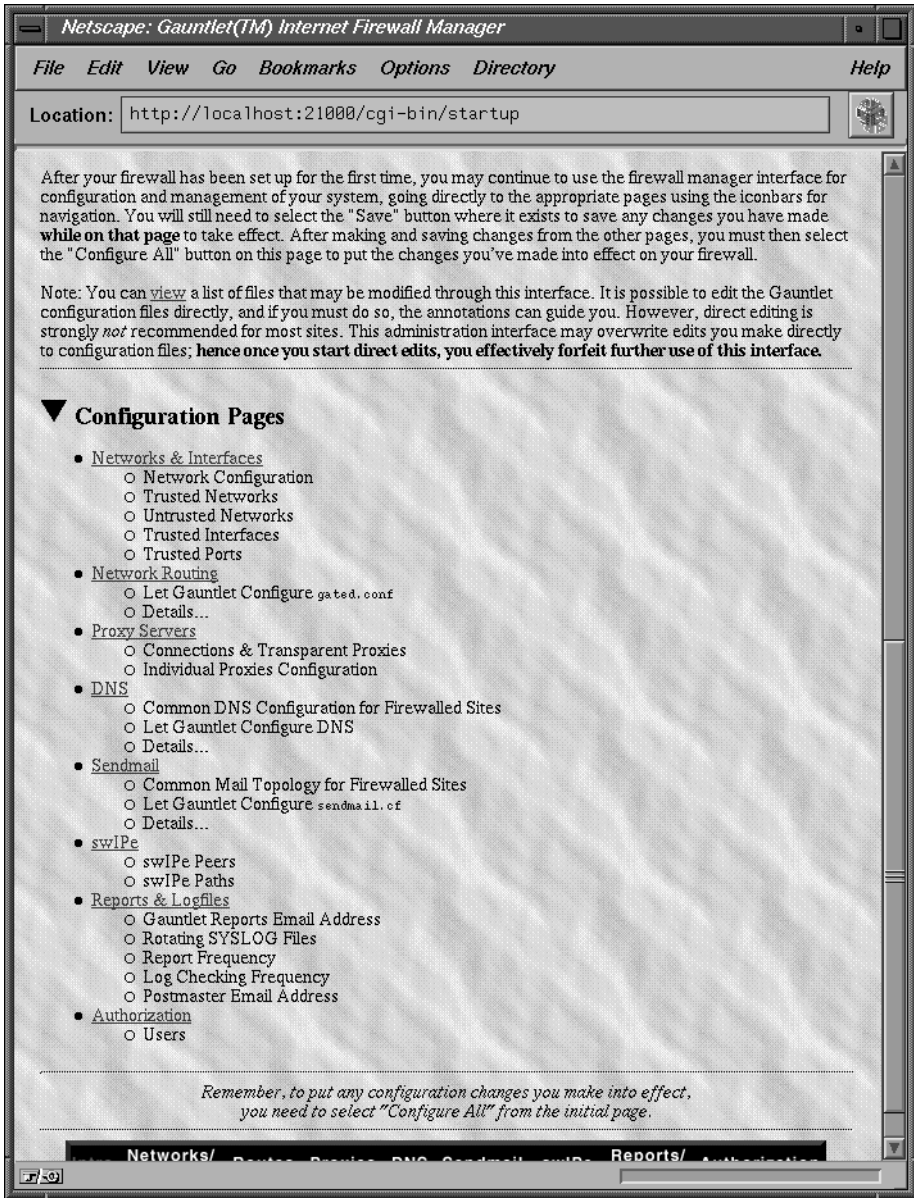

Figure 3-4 Gauntlet Introductory Management Form (2 of 2)

The section of the form called “Getting Started” provides a *Minimize Exposure* button which you can click to reduce possible security risks. If you click *Minimize Exposure*, the system reports on what it looks for and on any changes made. If there are areas where it cannot make changes but changes are considered desirable, those are reported too.

You begin configuring your firewall in the “First Time Configuration” section by clicking *Begin Configuration*, but first read “Managing Your Firewall” for some issues regarding direct file editing.

The last part of the introductory management form displays the sections covered by each of the other browser forms, and a list of links to those other forms is in the bar on the bottom if you wish to go directly to any of them. This document follows the sequential procedure you will follow if you click *Begin Configuration* on this form and each *Continue* button on the following forms.

Viewing the Gauntlet File List

If you want to see a list of the files that the Gauntlet configuration manipulates, click on the *view* link in the “Managing Your Firewall” portion of the introductory form. If you do not want to use the forms-based interface, you can directly edit these files although we do not recommend doing so. Refer to Table 3-1 for reference page information on the command line interface.

Table 3-1 Gauntlet File and Command Line Documentation

Reference Page	Description
authmgr(1M)	network authentication client program
authsrv(1M)	network authentication daemon
ftp-gw(1M)	FTP proxy server
http-gw(1M)	Gopher / HTTP proxy
netacl(1M)	TCP network access control
plug-gw(1M)	generic TCP plugboard proxy
rlogin-gw(1M)	rlogin proxy server

Table 3-1 Gauntlet File and Command Line Documentation

Reference Page	Description
rsh-gw(1M)	rsh proxy server
tn-gw(1M)	Telnet gateway proxy
smap(1M)	sendmail wrapper client
smapd(1M)	sendmail wrapper daemon
tn-gw(1M)	TELNET proxy server
x-gw(1M)	X gateway service
netperm-table(4)	configuration and permissions database

Networks and Interfaces Configuration Form

The Gauntlet networks and interfaces configuration form (Figure 3-5 and Figure 3-6) uses the standard Silicon Graphics Network Setup tools to configure the firewall's network interfaces. If you have not already configured your network setup with these tools, click *Network Setup* to configure the firewall hostname, network interfaces, and IP addresses; click *ISDN Setup* to configure ISDN; and click *PPP Setup* to configure PPP.

Note: If you directly run the Network Setup tools from the Gauntlet forms-based interface, you must be physically at the Gauntlet host console. Of course, you can also use the Network Setup tools independently of the Gauntlet interface from any location.

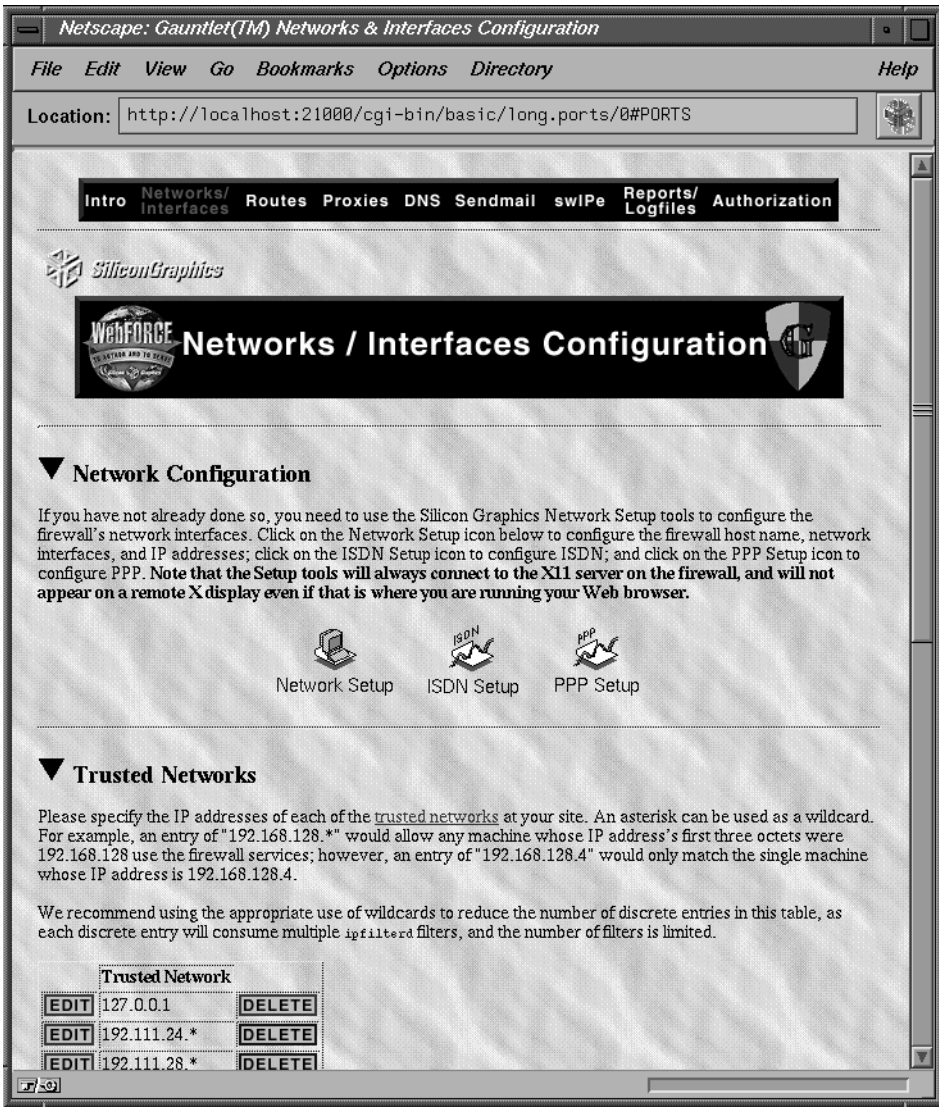

Figure 3-5 Networks and Interfaces Configuration Form (1 of 2)

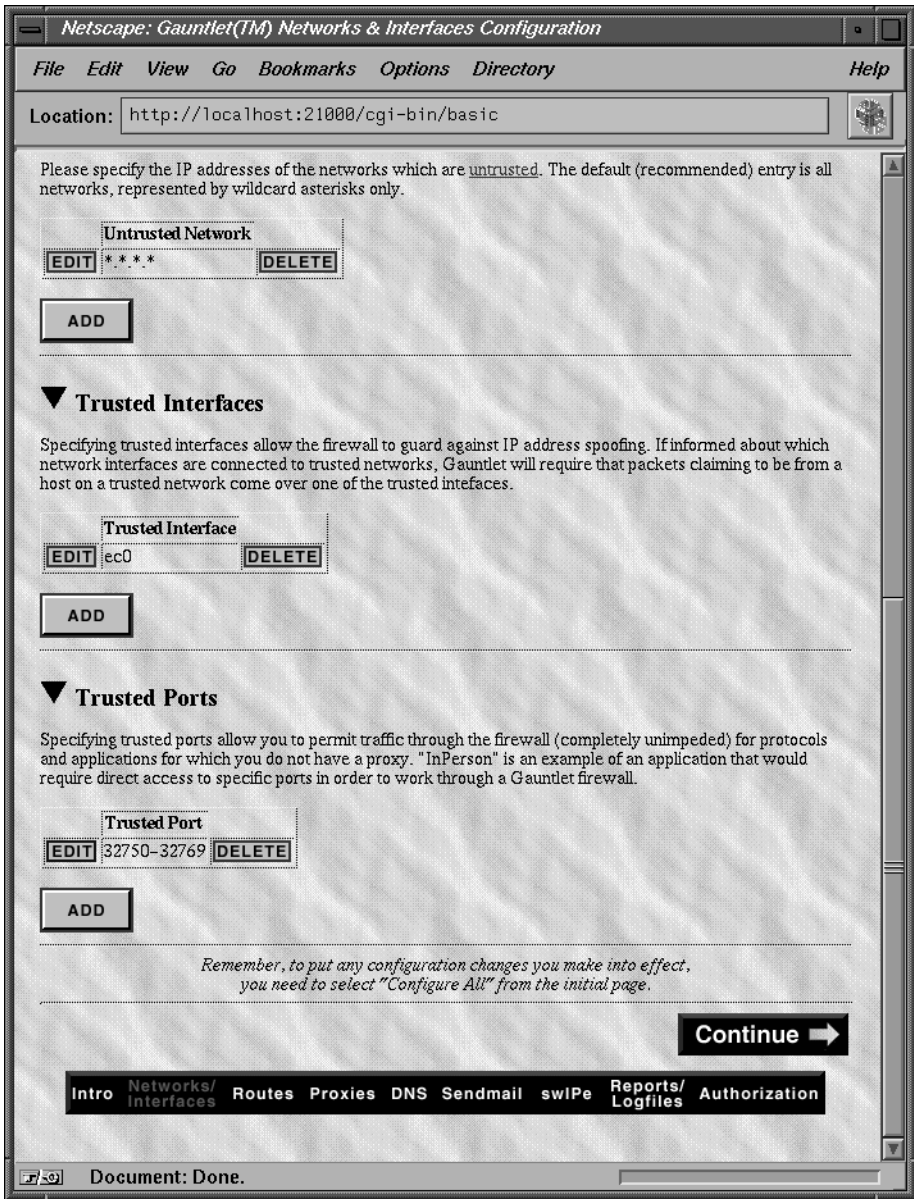

Figure 3-6 Networks and Interfaces Configuration Form (2 of 2)

The Gauntlet networks and interfaces configuration form allows you to specify trusted and untrusted networks (see “Base Policy” on page 7). Until you make changes on this form, all networks are considered untrusted, and only the Gauntlet system itself is trusted.

You can use a terminating asterisk as a wildcard to represent “all” in network addresses, for example:

- 192.168.128.*—all IP addresses beginning with “192.168.128”
- 192.168.*—all IP addresses beginning with “192.168”
- *—all IP addresses

Note: Something like 192.*.128.* won’t work; only a terminating asterisk is allowed.

Trusted/Untrusted Networks

The Gauntlet Firewall supports the concept of “trusted networks.” These are the networks that are permitted to use firewall services without user authentication (see “Authorizing Users Form” on page 51). Typically, the trusted networks are your internal, local networks.

Click on the *ADD* button and then specify the IP address of each network you want to add to the list of trusted networks.

If a network is neither trusted nor untrusted, users from that network will not be permitted to use the firewall services nor even attempt authentication. For this reason, the typical default entry for untrusted networks is *all* networks (other than those indicated configured as trusted), represented as a single asterisk. This means that users from any network other than an explicitly trusted one must pass authentication.

You can add to the list of untrusted hosts by clicking on the *ADD* button. If you list only specific network addresses as untrusted, that means that those networks may access your network if they pass authentication, but no other networks (except explicitly trusted networks) may even attempt authentication (access is immediately refused). If you leave the list of untrusted hosts blank, that means that no network access (other than from

specifically trusted networks) is allowed to attempt authentication. All such access is immediately refused.

User Authentication and Untrusted Networks

Users from an untrusted network can still access firewall resources if they have an entry in the authentication database of the firewall, that is, they are specifically allowed to use the services. Refer to “Authorizing Users Form” on page 51 for information on how to establish user authentication.

Trusted Interfaces

Specifying trusted interfaces allows the firewall to guard against IP address spoofing. If informed about which network interfaces are connected to trusted networks, Gauntlet will require that packets claiming to be from a host on a trusted network come over one of the trusted interfaces.

Specifying trusted interfaces is required—you cannot have trusted networks without trusted interfaces.

Trusted Ports

Specifying trusted ports allows you to permit traffic through the firewall (completely unimpeded) for protocols and applications for which you do not have a proxy. InPerson™ is an example of an application that requires direct access to specific ports in order to work through a Gauntlet firewall. Note that this is only relevant when the Gauntlet firewall is positioned to be the router between internal and external networks.

Routing Configuration Form

Use the routing configuration form (Figure 3-7) to specify your routing implementation.

If you already have a customized routing configuration file for *gated* on the Gauntlet host and want to keep using it, check the box for “Preserve the gated.conf file if it exists?”

If you are going to let Gauntlet generate a new *gated.conf* file, click on *ADD* under *Explicit Routes* and then add the network, gateway, and “hop” metric to each network you add. (Use a metric of “0” if the gateway is an interface on the Gauntlet host, and a “1” if it is anywhere else.)

Entering a destination network as “default” sets the default route.

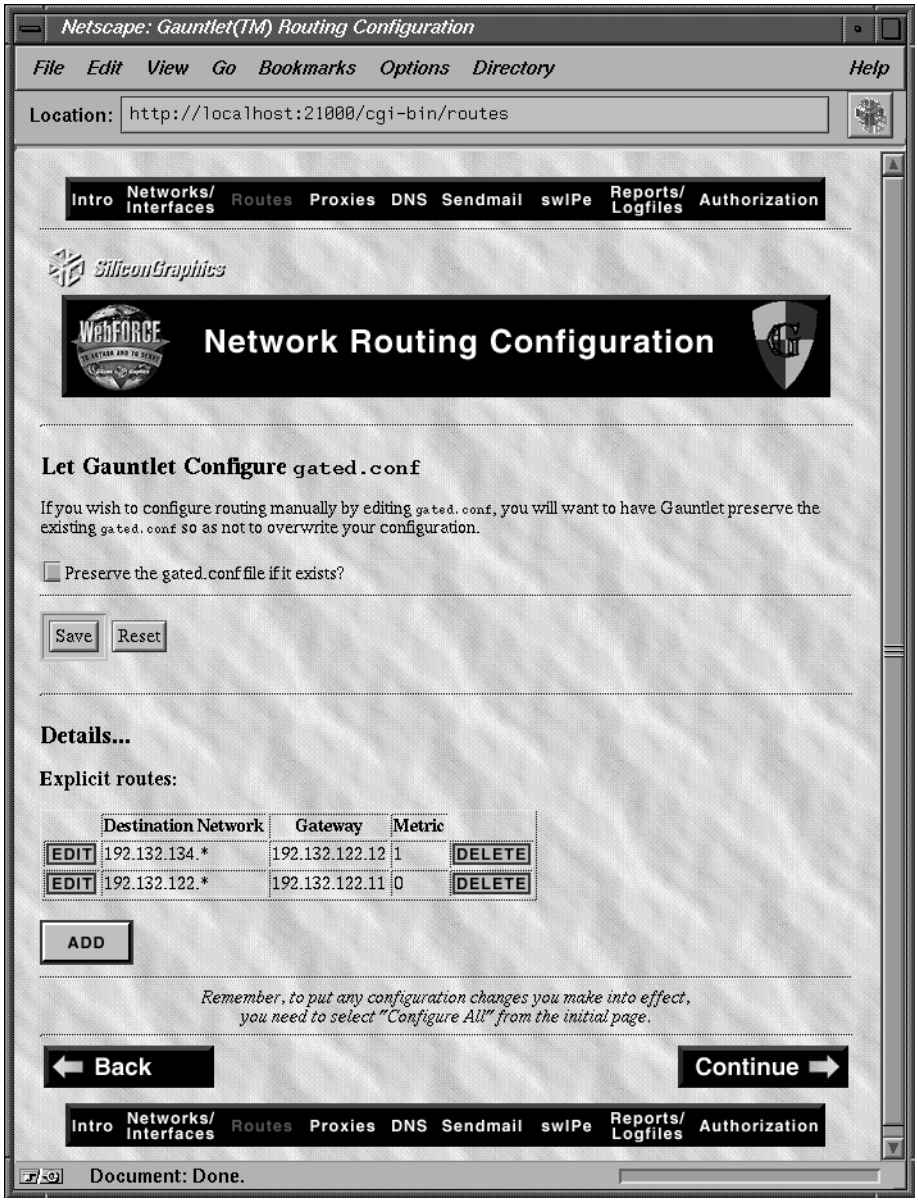

Figure 3-7 Routing Configuration Form

Figure 3-8 illustrates an example routing configuration.

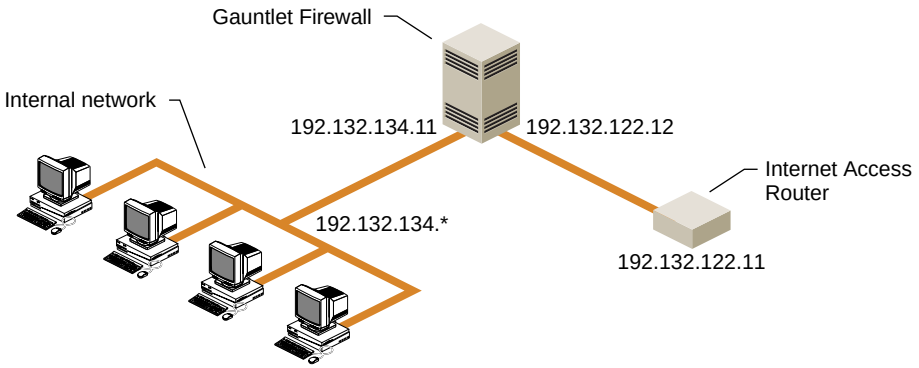

Figure 3-8 Example Gauntlet Host Routing Configuration

If hosts on your internal network are running a routing daemon, they should eventually acquire the default route from the Gauntlet host, or the route can be explicitly added to those hosts by their administrators.

Additional Routing Information

If you want more general information about routing, or routing using the command line interface to IRIX, refer to the section “Setting Up a Router” in Chapter 17 of the *IRIX Advanced Site And Server Administration Guide* and the reference page for gated(1M).

Proxy Servers Configuration Form

The proxy server configuration form (Figure 3-7 and Figure 3-11) allows you to control network services through the Gauntlet firewall. You can enable and disable particular services, specify timeout values and port numbers, and so on. Each service can be configured separately.

Remote (Network) Connections

If you want to allow network logins to the firewall, specify this by checking the box for "Do you want connections allowed TO the firewall?" If this box is not checked, you must configure the firewall at the system console—not from a network login. Network logins are convenient, but could lessen the security of the firewall.

When logins are enabled, administrators can connect to the firewall by accessing the *rlogin* or *telnet* proxies. Example 3-1 illustrates a sample Telnet session.

Example 3-1 Administrative Telnet Connection to Firewall

```
magnolia-% telnet fwall
Trying 127.0.0.1 port 23...
Connected to localhost.

IRIX System V.4 (rfwall)

login: root
Password:
IRIX Release 5.3 IP22 rfwall
Copyright 1987-1994 Silicon Graphics, Inc. All Rights
Reserved.
Last login: Wed Aug 16 14:05:49 PDT 1995 by UNKNOWN@localhost
You have mail.
rfwall 1# setenv DISPLAY magnolia.abc.sgi.com:0
rfwall 2# gauntlet-admin
```

Note: If you log in from the network (you must have enabled network logins) to the firewall host, you may need to set the DISPLAY environment variable to your host to be able to use *gauntlet-admin*.

Caution: Network logins should only be used over secure links when absolutely necessary. Another option for remote access to the firewall is to connect a modem to one of the serial ports to enable controlled dial-in access for administrators only.

Enabling Transparent Proxies

You must also specify if you want to enable transparent proxies. With transparent proxies, user requests to connect to a particular service on an external host using a supported application protocol, pass through the proxy server as if the user were communicating directly with the network host. If you do not enable transparent proxies, the user must first connect to the proxy server, and then from the proxy server, connect to the desired network host. Transparent and non-transparent connections are illustrated in Figure 3-9.

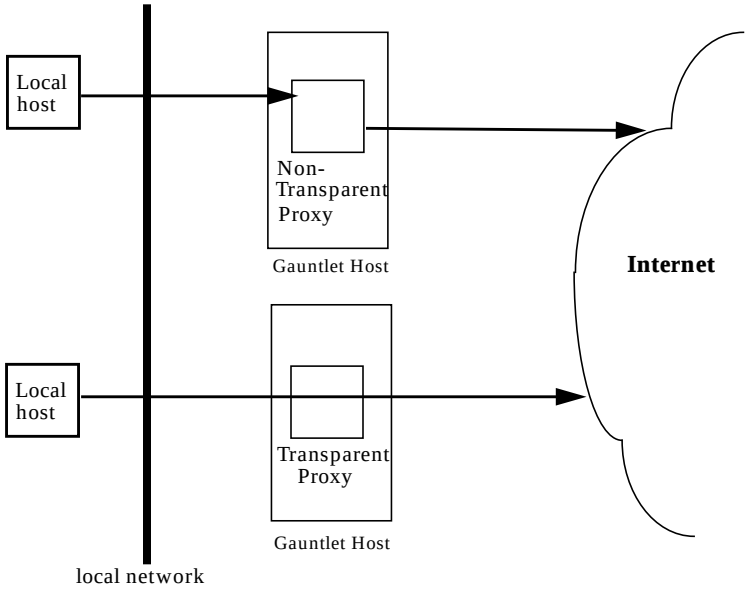

Figure 3-9 Transparent and Non-Transparent Proxy Servers

Enabling Individual Proxy Services

Next, specify which services you want to enable. Many of the services allow you to specify a timeout value (click the *Unhide* button if you don't see it) so change the default timeout value of any service if it does not suit your needs. (The timeout value is the number of seconds the server maintains a connection before it times out due to inactivity.)

If you enable a service, it means the firewall will run a daemon supporting that service. For example, enabling Telnet means that a proxy Telnet server will run on the Gauntlet firewall to mediate and enable Telnet connections. It will be a transparent Telnet proxy if you have enabled transparent proxies. Note that you must also have configured the Networks/Interfaces Configuration Form correctly for the service to work.

FTP Server Configuration

If you enable FTP on the firewall, you can specify a timeout value and also specify if you want to enable anonymous FTP. The Gauntlet configuration sets up anonymous FTP according to the recommendations in "Setting Up Anonymous FTP" in the *IRIX Advanced Site and Server Administration Guide*. Also, if enabled, anonymous FTP prevents users from untrusted networks from using the FTP application proxy.

Telnet

If you enable the Telnet proxy, enter a number of seconds for it to timeout when idle (or accept the default of 3600 seconds—one hour).

rlogin

If you enable the rlogin proxy, enter a number of seconds for it to timeout when idle (or accept the default of 3600 seconds—one hour).

X Windows, finger, gopher, and whois

Check these boxes to enable the corresponding proxy server. No further configuration is required. X Windows is for use in conjunction with telnet and rlogin proxies only. See x-gw(1M) for an example session.

HTTP Proxy Server Configuration

If you enable HTTP (Hypertext Transfer Protocol for World Wide Web access), you must also specify the following:

- which port the HTTP server should use—the default is "8080".
- which user ID the HTTP server should use—the default is "uucp".

- which group ID the HTTP server should use—the default is “6”.
- which default URL the HTTP server should provide—the default is “” (none).

NNTP Proxy Server Configuration

Enable NNTP for USENET News access. If configured with the addresses of an internal and external news server, the firewall gateways NNTP traffic bidirectionally between the two systems. Host IP addresses or DNS names may be used. When configuring news on the internal and external servers, both systems should be set to feed news to the firewall, rather than attempting to exchange it directly. For example, if the internal news server is “nntp.sgi.com” with IP address 192.33.112.100 and the external news feed is “news.uu.net” with IP address 11.11.11.11, configure the proxy with the appropriate names and addresses, and then configure the news software on “nntp.sgi.com” to transfer articles to the firewall. The upstream news feed “news.uu.net” would also transfer articles to the firewall.

SMAP Proxy Server Configuration

If you enable SMAP (for *sendmail*), you should specify the following:

- an idle timeout for SMTP connections—”3600”.
- which user ID the SMTP server should use—the default is “uucp”.
- which directory the SMTP server should use—*/var/spool/smap*.
- an address to send bad e-mail to—the default is “root.”

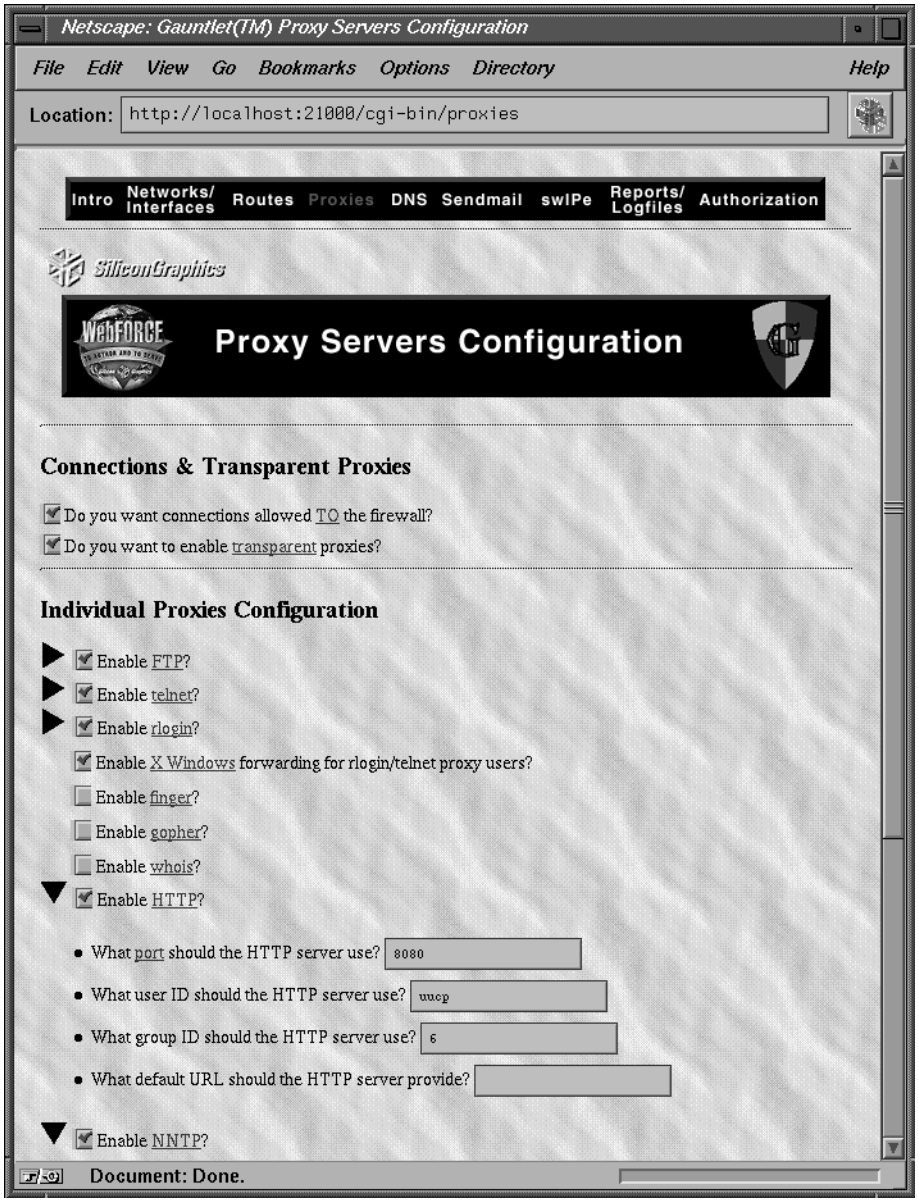

Figure 3-10 Proxy Servers Configuration Form (1 of 2)

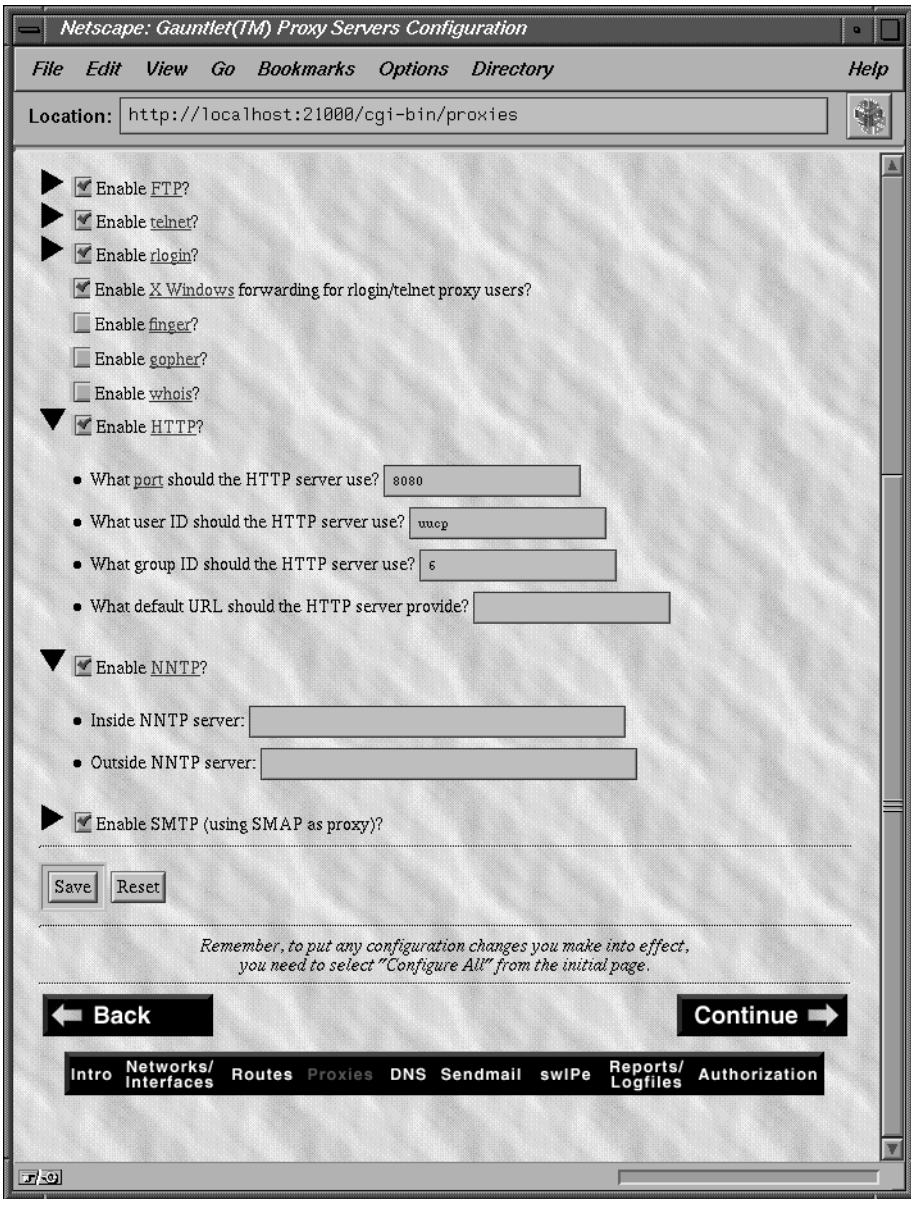

Figure 3-11 Proxy Servers Configuration Form (2 of 2)

Domain Name Service (DNS) Configuration Form

The DNS configuration form (Figure 3-12) helps you configure the files necessary to run a minimal DNS master server configuration for your site. This configuration is enough to function as the external server in a dual-DNS configuration, or as the basis for a site-wide server or other site-specific server. If you are the site-wide DNS server, add appropriate entries for each of the hosts on your network. If you prefer to preserve your existing DNS configuration, be sure that the "Preserve the current DNS configuration?" box at the top of this form is checked, because the default is to not preserve the current configuration.

Domain Name Service and Gauntlet

When you join the Internet, you will need to participate in the Internet-wide DNS hierarchy. There are several popular methods of having your site's DNS information available on the Internet. Some sites have their service provider serve the information for them. For sites that choose to run their own DNS server, there are two common firewall configurations. One involves running two DNS servers, an internal and an external server. This is often referred to as a split-DNS or dual-DNS configuration. The other involves running a fully-populated DNS server on the external host. In either case, the GAUNTLET host would be a common choice to run a DNS server on, either as the external part of a dual-DNS configuration, or as the single DNS server for the site.

DNS, the name service used on the Internet, should be configured for your site to give out the addresses that other sites need to contact you. This might include the address of your router, your firewall host, and any other machines you want others to be able to communicate with. In the case of a simple firewall comprised of a dual-homed host, the dual-homed host would be a DNS server, providing the address of the Internet side of its network connection. In the case of a screened subnet, the DNS server could be any of the "public" hosts in the subnet, and it could provide addresses for all of these hosts and the router.

You should also set up the DNS Mail eXchanger (MX) record to advertise the name of the host(s) responsible for mail at your site. This may be the firewall host or another host. Do not publish internal hostnames and addresses on the firewall host. If you have a single firewall host performing multiple

services, say FTP and WWW serving, use CNAME records to “alias” the services to the hostname. This makes it easy to move these services to different hosts if you want to separate them later.

Configuring DNS is a task that is very difficult to automate reliably, as many sites’ DNS configurations vary widely. The purpose of the DNS configuration tools included with the Gauntlet firewall is to give the administrator a quick means of setting up a basic, working DNS. More advanced DNS management will require manual operation and familiarity with the DNS software.

Gauntlet uses the Silicon Graphics example DNS configuration files to configure DNS for your firewall. If you are not sure how to fill in the DNS configuration form, refer to the chapter on “The BIND Name Server” in the *IRIX Advanced Site and Server Administration Guide*.

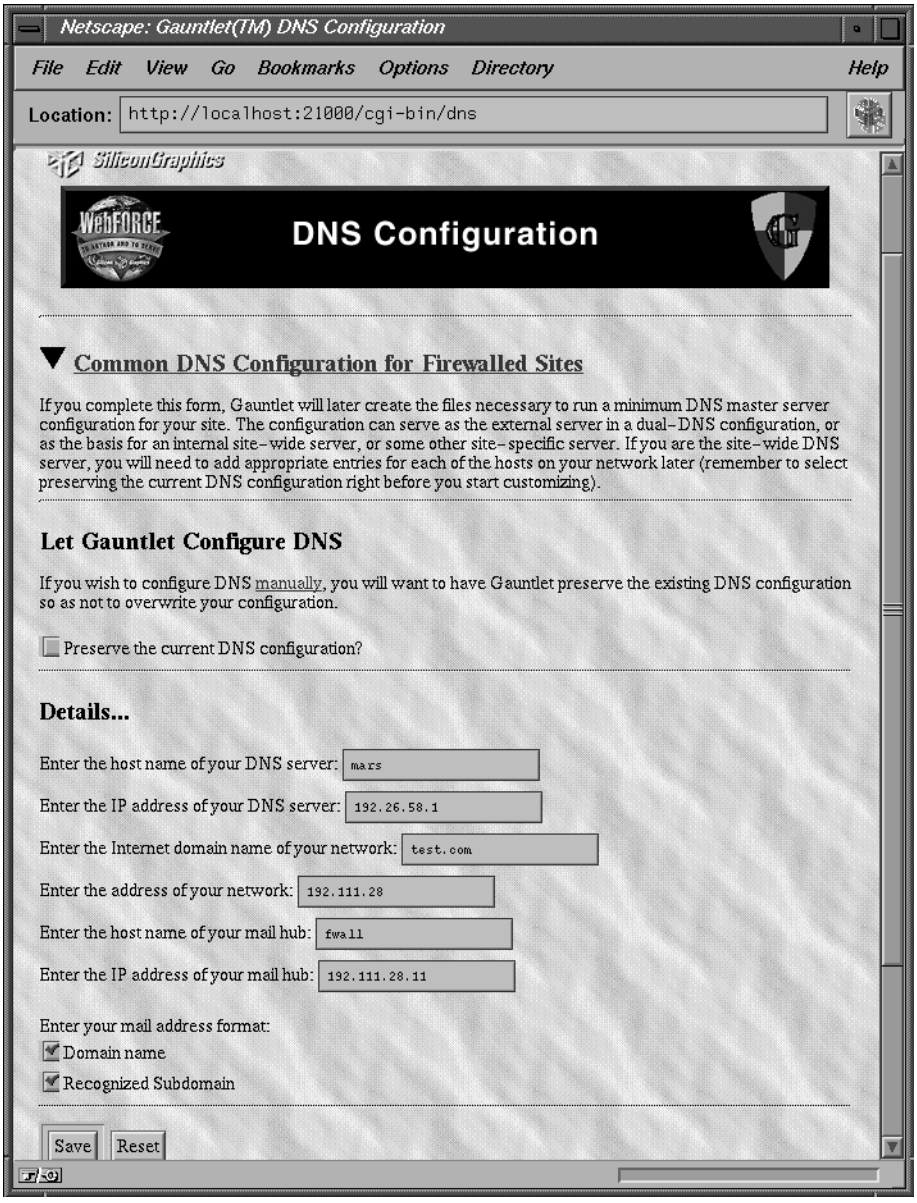

Figure 3-12 DNS Configuration Form

Sendmail Configuration Form

Use the Sendmail configuration form (Figure 3-13) if you want to use the Gauntlet browser-based interface to modify the Gauntlet firewall's Sendmail configuration. If you prefer, you can use the IRIX *configmail* tool, or edit the */etc/sendmail.cf* file directly. Be sure to check the *Preserve the current sendmail.cf file?* button if you do this, because the default is to not preserve the current configuration.

Refer to sendmail(1M), configmail(1M) and IRIX sendmail" in the *IRIX Advanced Site and Server Administration Guide.*

Sendmail and DNS

Your mail system should be configured cooperatively with your DNS configuration. That is, whichever machine your DNS server is advertising as your Mail eXchanger (MX) host, must have its *endmail.cf* configured to accept mail for your network and to do the appropriate thing with it once it is received. Usually that means to forward the mail to a master mail machine on the internal network, which knows users' internal addresses, and how to deliver the mail to them.

Note: The convention is to use the domain name of your network as your electronic mail address. For example, user "harry" at company XYZ corporation, whose domain name is XYZ.com would have the electronic mail address of "harry@XYZ.com". To reinforce the electronic mail address of your site, and to make it easy for others to reply to your users' mail, we recommend that you configure your *sendmail.cf* to rewrite all your addresses to conform to this convention.

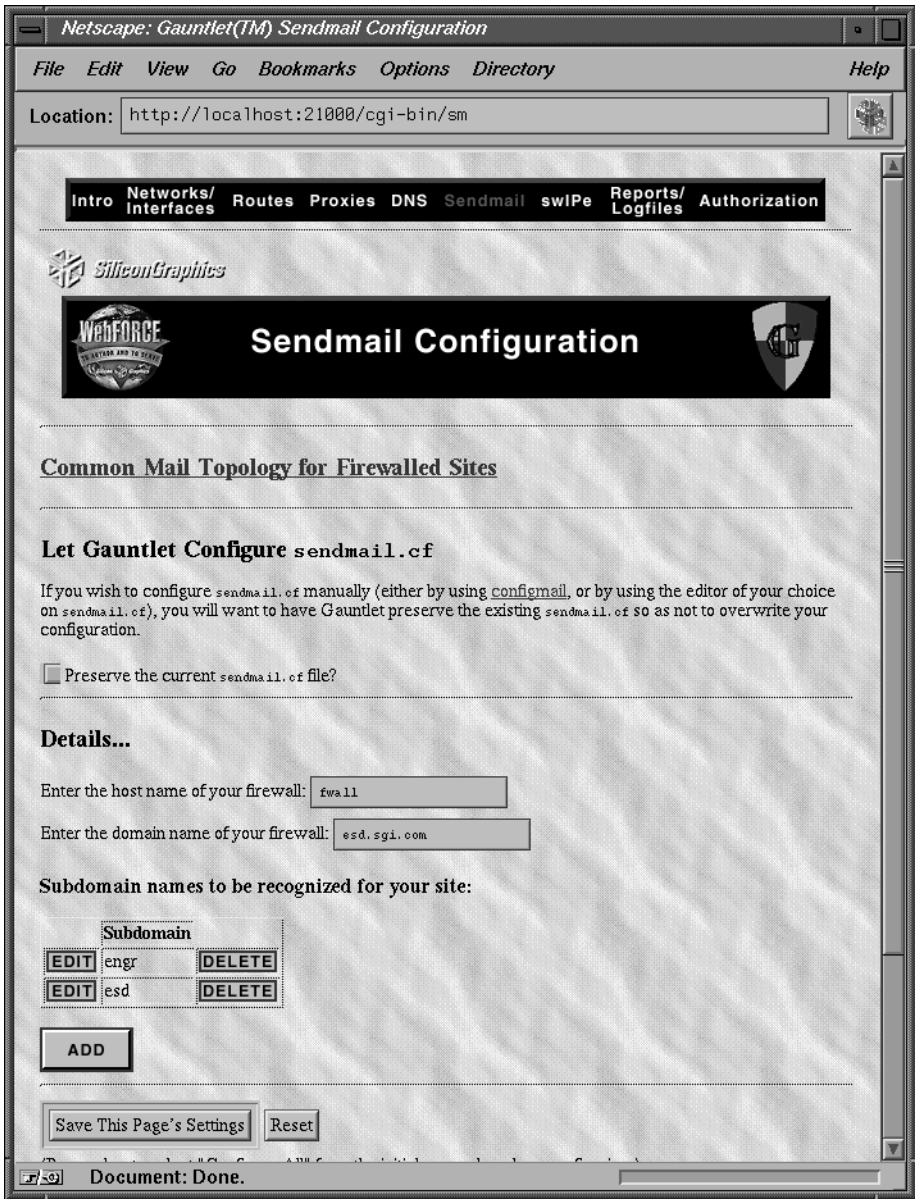

Figure 3-13 Sendmail Configuration Form

swIPe Configuration Form

Figure 3-14 illustrates the swIPe configuration form. swIPe provides IP network address authentication, that is, it ensures that the IP packets are coming from who they say they are, protecting against IP address spoofing. IP address authentication could be used in conjunction with permission sets to guarantee that interaction is only occurring between confirmed entities. Encryption protects against unauthorized access to data. Use encryption for data that crosses over untrusted networks and that must be kept secret and be protected against alteration.

swIPe Peers and Paths

Peers are two Gauntlet firewalls configured to support authentication or encryption between them. There must be a Gauntlet host at each end of any session that is secured in this fashion. Refer to Figure 3-15 for an illustration of two Gauntlet hosts acting as peers in a network path that passes through the Internet.

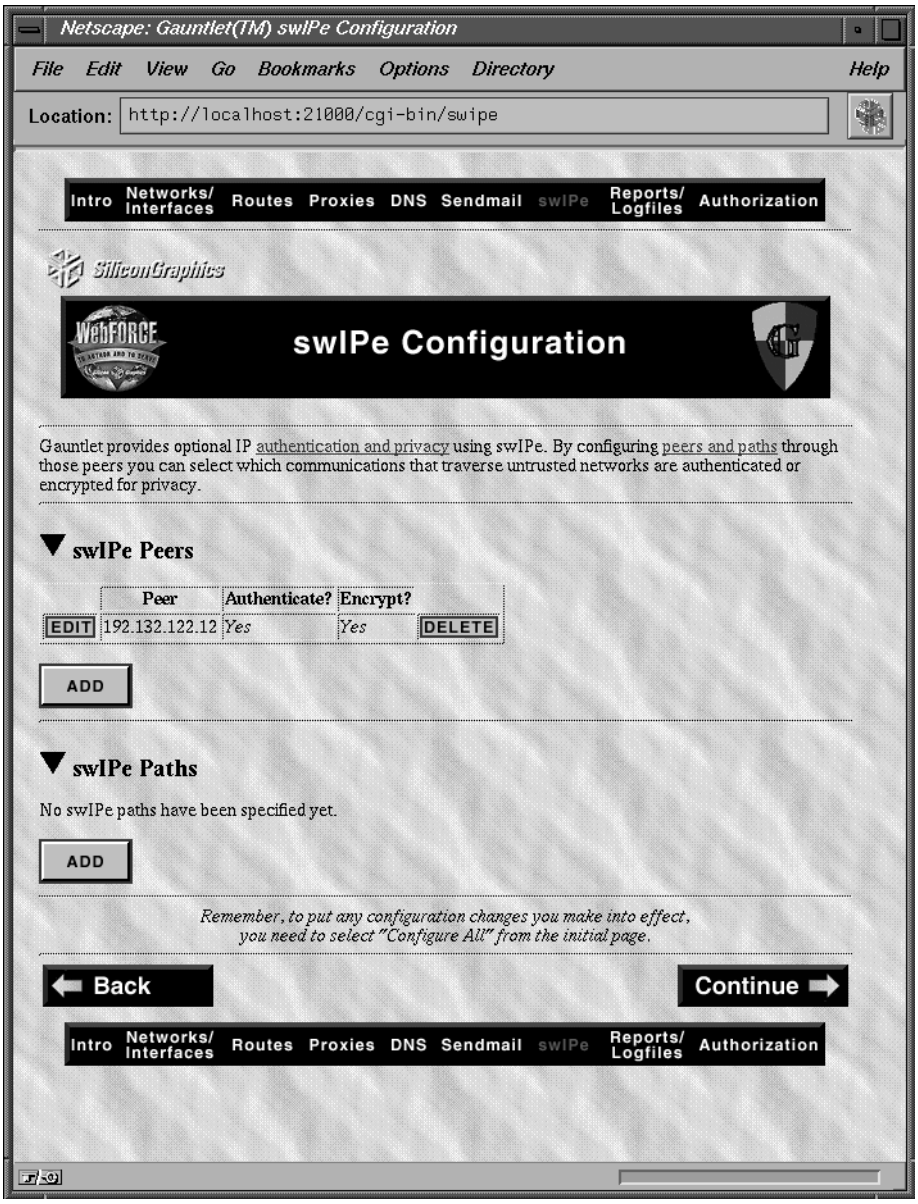

Figure 3-14 swIPe Configuration Form

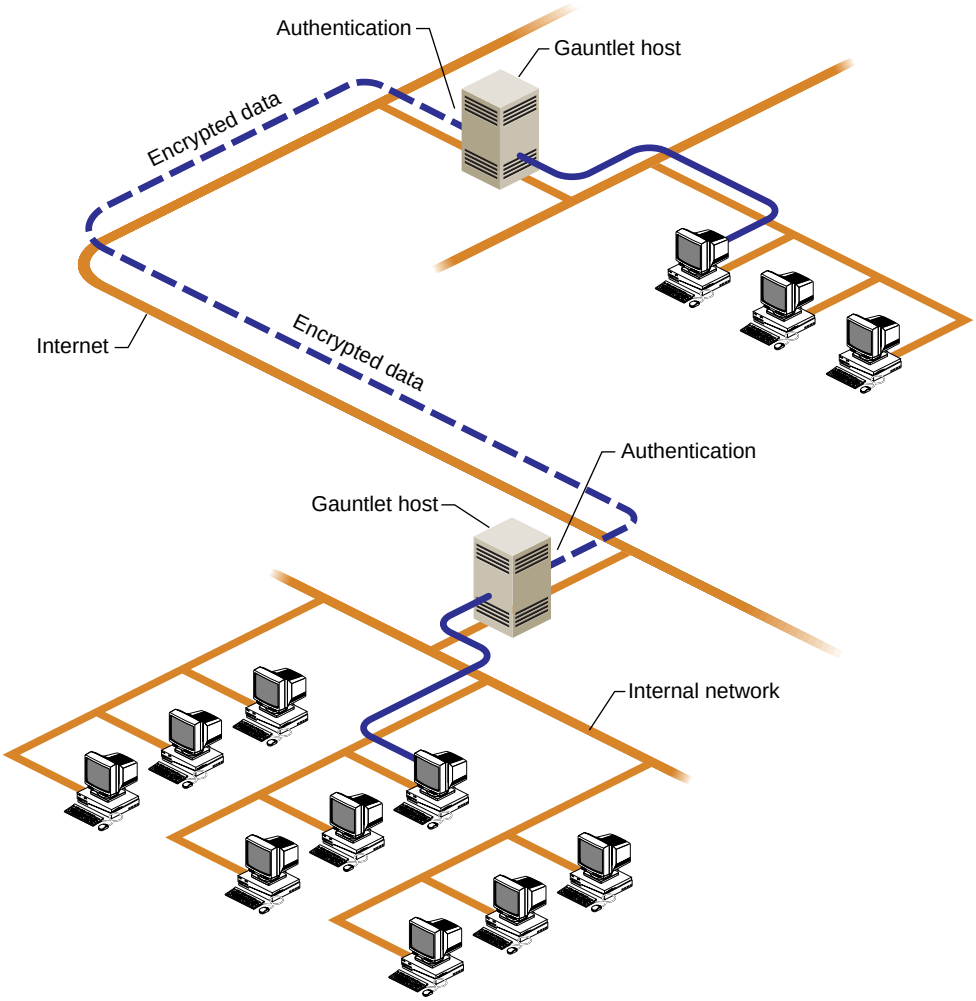

Figure 3-15 Gauntlet Hosts Using swIPe

Logfiles and Reports Configuration Form

You can use the reports and logfiles form (Figure 3-16) to configure some basic reporting mechanisms on the Gauntlet firewall.

The system automatically generates reports, and you can specify yourself (and other users in a comma-separated list) to receive these reports by e-mail.

You may also specify which reports you want to receive (daily, weekly, or both), how often you want the report software to run and how long you want system log files to be saved. Save the files for at least seven days if you want to receive full weekly reports.

You should assign either yourself or another trusted user as the system Postmaster (to receive any generic mail addressed to “Postmaster” at the Gauntlet host).

An example of log file entries generated by the Gauntlet firewall is shown in Example 3-2 (lines have been shortened for readability). If you do not want certain types of entries to be recorded in the log file, you can specify them using *egrep* syntax in the field provided on this form (see egrep(1)). For example, enter “localhost” in the egrep field to keep lines which include the string “localhost” from appearing in the log file output. Be careful not to specify filters which are too broad and that prevent you from seeing warnings and notices you want to see.

Example 3-2 Partial Log File Listing

```
Aug 10 02:00:08 6F:rfwall syslogd: restart
Aug 10 06:56:22 5D:rfwall netacl[1355]: permit host=boston.esd.sgi.com...
Aug 10 06:56:22 5D:rfwall tn-gw[1355]: permit host=boston.esd.sgi.com/...
Aug 10 06:56:32 5D:rfwall tn-gw[1355]: permit host=boston.esd.sgi.com/...
Aug 10 06:56:32 5D:rfwall tn-gw[1355]: connected host=boston.esd.sgi.c...
Aug 10 06:56:32 5D:rfwall netacl[1356]: permit host=localhost/127.0.0....
Aug 10 10:45:41 5D:rfwall authsrv[1893]: BADAUTH smith (tn-gw midas.wp...
Aug 10 10:45:45 5D:rfwall authsrv[1893]: BADAUTH exit (tn-gw midas.wpd...
<etc>
```

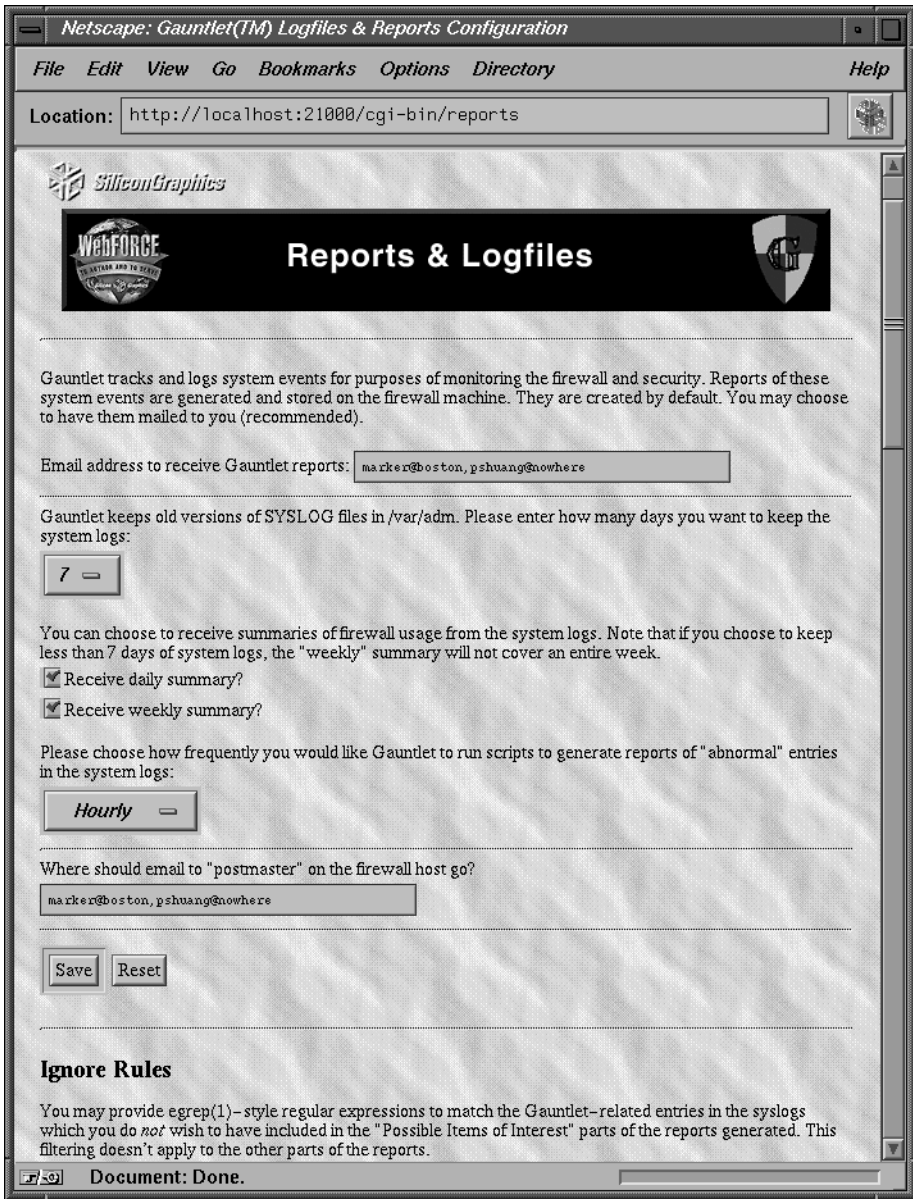

Figure 3-16 Reports and Logfiles Form

Refer to Chapter 4 for command-line and file information on reports.

Authorizing Users Form

The authorizing users form (Figure 3-17) allows you to specify which users can access services from an untrusted network if they successfully authenticate themselves. Several different authentication mechanisms are supported.

Adding a user with the Add Users form (Figure 3-18) means that the user can use all of the enabled services. The group field lets you associate groups of users.

Note: Adding users and groups here does not create IRIX accounts or groups for the users—just proxy server authorization.

Figure 3-19 illustrates user authentication on the Gauntlet host.

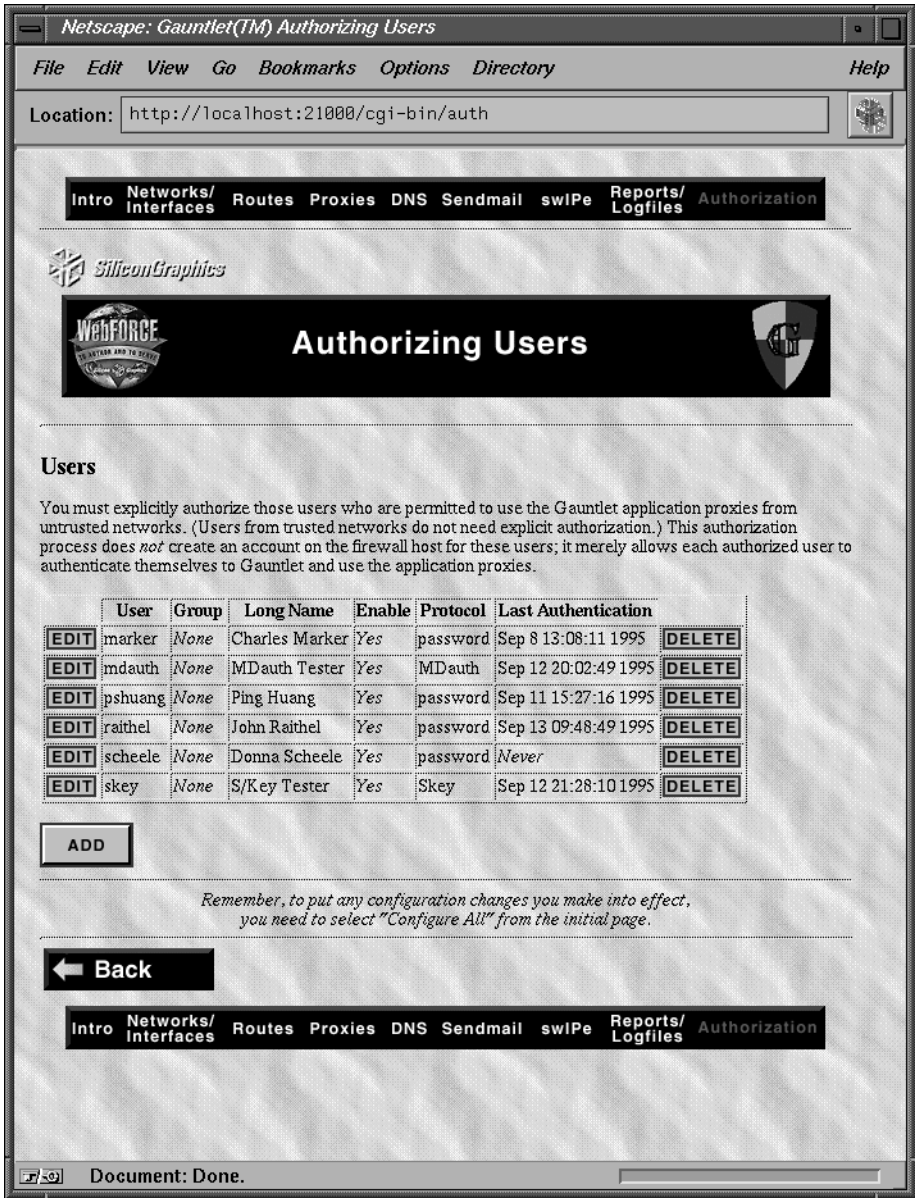

Figure 3-17 Authorizing Users Form

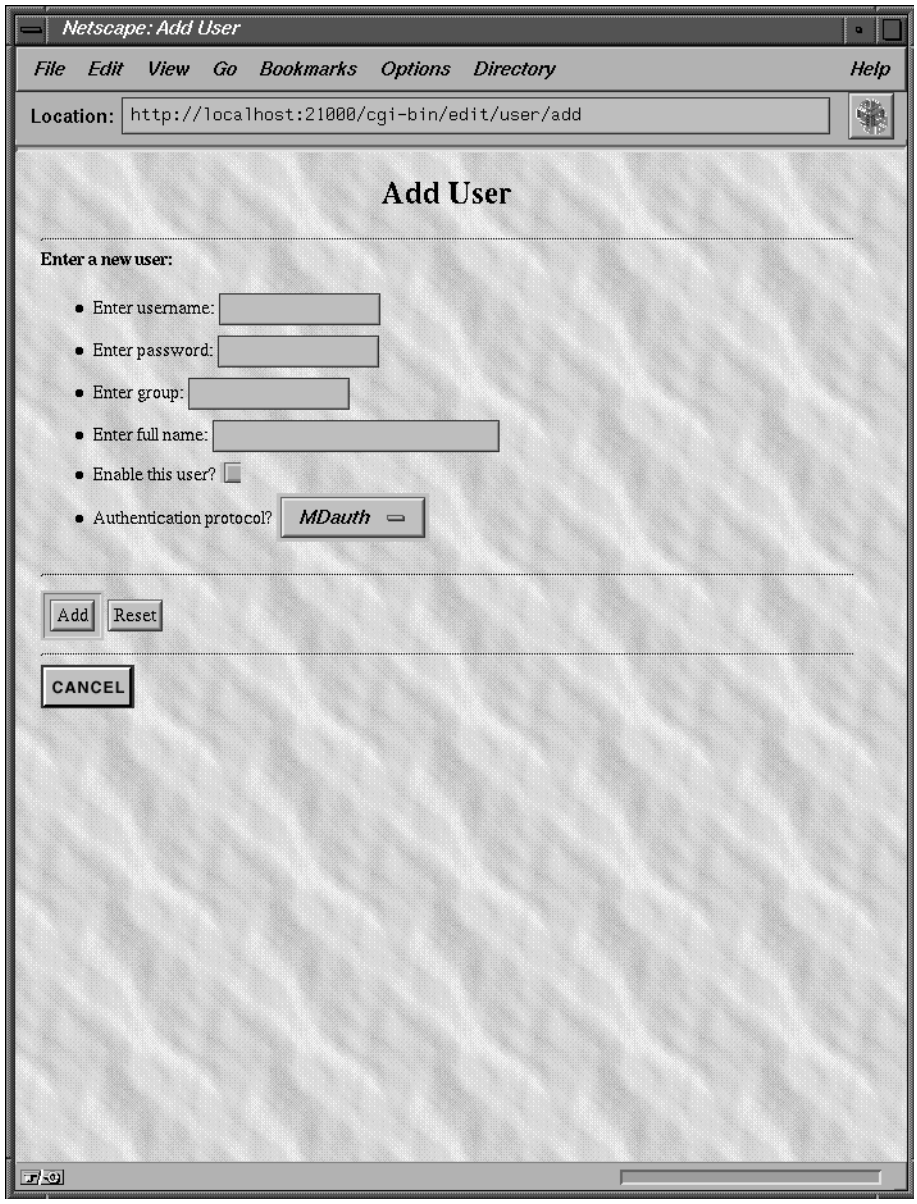

Figure 3-18 Add User Form

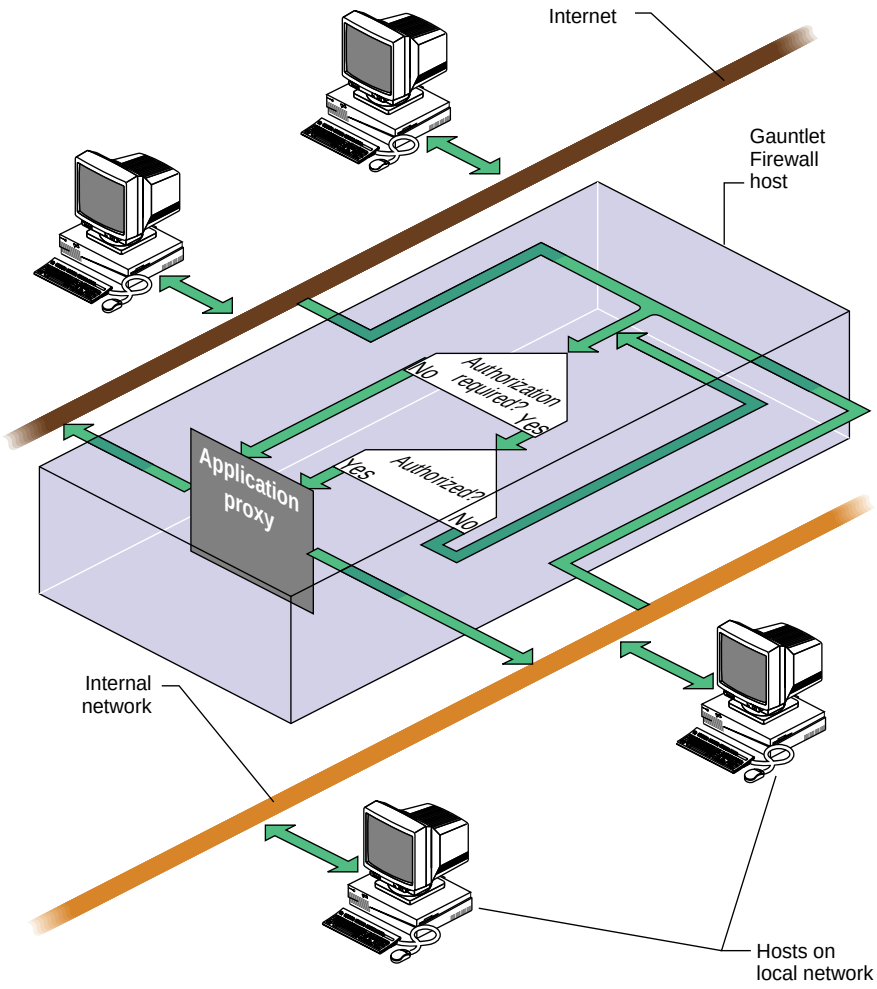

Figure 3-19 User Authentication

User Authentication

You have several choices in setting a user's authentication protocol:

- *password*—Plain text passwords. This is not recommended for use under any circumstances for accessing a network from over an

untrusted network. Plain text passwords are included as an option principally for sites that wish to do chargeback accounting or individual accounting of firewall use.

- *skey*—S/Key software system that uses a challenge-response model to implement authentication. S/Key is a freely available software authentication system from Bellcore. It is included "as is" with the Gauntlet firewall—-the IRIX executable users need to generate responses is */usr/bin/key*. If you want to use S/Key on other systems as well as IRIX, you can download source code from the site listed in "Additional Resources" on page xv. Refer to Example 3-3 for an example of an S/Key authentication session.
- MDauth—another authentication system, but less widely known and available than S/Key. MDauth is also a software-based system that uses challenge response. It is based on MD5 checksums. MDauth is included "as is" with the Gauntlet firewall. Especially in heterogeneous environments, it may be preferable to use S/Key to MDauth. The IRIX executable users need to generate responses is */usr/etc/softmd5*.

When editing a user record, if the *Password:* field is not empty, the new value will be used to reset the user's existing password entry for whatever authentication protocol he or she uses. If you make an error when editing a user record, simply select the *Reset* button, which aborts any changes that were made.

Example 3-3 shows an S/Key authentication session from the point of view of a user on a remote client. Note that this assumes the administrator of the system has already added the user in the authentication database as an S/Key user with a password known to the user, and that the user has access to the */usr/bin/key* program on the client.

Example 3-3 S/Key Authentication Session Example

```
% telnet fwall
Trying 192.111.28.11...
Connected to fwall.esd.sgi.com.
Escape character is '^]'.
Username: jones
Skey Challenge: s/key 662 rf20257:
```

At this point, the user must run the *key* program on the client to generate a response to the server challenge:

```
% key 662 rf20257
Enter secret password: fxdkiux


CHAR BAN SHOT HOP SALT HURT
```

The user then enters the response back at the server prompt:

```
Skey Challenge: s/key 662 rf20257: CHAR BAN SHOT HOP SALT HURT
Login Accepted
tn-gw->
```

Caution: The user client should be secure. Note that S/Key does echo the password to the screen so the user should be sure that no one sees the password.

After a certain number of authentication sessions, a new password must be set for S/Key. The remaining number of authentication sessions for the current password is the first string in the S/Key server challenge (662 in the example).

Chapter 4

Daily Operation and Maintenance

This chapter provides additional information about the Gauntlet software to help you maintain it. The chapter contains the following sections:

- “Daily Operation” on page 57, describes management of reports and logfiles.
- “Firewall Backups” on page 60, discusses issues of backups of the Gauntlet host.

Daily Operation

This section discusses additional aspects of Gauntlet firewall automated reports, system logs, alarms, and user authentication.

Automated Reports

The Gauntlet system includes reporting tools that summarize usage, security-related activity, and types and quantity of traffic. These reports are accessible through the management interface or at the command line. You can request daily reports and weekly reports. The daily report provides traffic and usage statistics from the previous day’s logs. The weekly report provides a summary of traffic during the week that ended on the previous day (see Appendix C). Thus, if the administrator runs it on Sunday, the report will summarize traffic from the previous Sunday through the Saturday that just ended.

To configure the Gauntlet firewall to automatically generate these reports and mail them to you, refer to “Logfiles and Reports Configuration Form” on page 49.

To run the reports at the command line, invoke the report generators as either */usr/gauntlet/bin/weekly-report* or */usr/gauntlet/bin/daily-report*. Running

reports at the command line is not destructive; run them as often as you want. Running the reports does, however, require considerable processing resources and you may prefer to run them during off hours. The report processing scripts are actually a series of shell programs, each of which is responsible for summarizing the behavior of one component of the system. All reporting is implemented using common IRIX tools so that you may modify the reporting in any way you feel necessary.

System Logs

The Gauntlet firewall uses *syslogd* to maintain its logs. The system is preconfigured to maintain its logs automatically in the system area */var/adm*, where one week's worth of active logs is retained. A second set of logs is retained in compressed-format (using gzip(1)) files named after the date on which the log was generated. By default, system logs are retained for 14 days, after which they are automatically removed. Since logs are serviced using the standard logging daemon, administrators have the option of configuring the system to also transmit copies of logging records to other computers over the network. Shadowing the log files on a separate system reduces the chance of logging information being lost, and provides an alternate platform for processing audit records, if desired. If you choose to exclusively shadow the system logs, you must run the report generator on the host that is storing the log information, and set up cron(1M) to rotate the reports on that host as well.

The Gauntlet firewall software uses the system logs as its primary mechanism for alerting you of configuration problems, system errors, or dangerous conditions. When a problem is encountered with the firewall, the first place to check for diagnostic output is the current active system log */var/adm/SYSLOG*.

Alarms

Gauntlet systems incorporate an automated notification system designed to alert administrators of potential problems with the system or attacks against the system's security. Periodically, the system performs a scan of information that has been added to the system log since the last time it checked for noteworthy occurrences. Unlike many systems, which attempt to define a list of noteworthy occurrences to be on the alert for, the Gauntlet system

defines a list of occurrences that are not noteworthy. Events that are not noteworthy are ignored; all others are brought to the systems administrator's attention. Thus, anything new and unforeseen is more likely to be brought to the attention of the system administrator.

System alerts are checked periodically,[1] and any output generated by the alert check is electronically mailed to the firewall administrator immediately (see Appendix C). Sites desiring pager or FAX notification of events can easily take advantage of electronic mail to pager or FAX gateway services, or they may opt to modify the alert processing system. Alerts are processed by a script */usr/gauntlet/bin/frequentcheck*, which relies upon a file listing strings that indicate an unimportant event. If you wish to disable notification of a particular event, add a matching pattern to the file */usr/gauntlet/config/frequentcheck.ignore*.

User Authentication Management

The user authentication database is stored as a set of files in a DBM (hash table) format for quick access. All access to the authentication database is serialized to ensure consistency of the entries in the database; more than one authentication server (*authsrv*) process may access it at a time. The authentication database itself resides in */usr/etc/fw-authdb*. A backup ASCII copy of the database is preserved nightly via *cron*. You can manage the database from the Authorization form. Alternatively, you may prefer to use *authsrv* in command-line mode or the screen-oriented authentication database browser *authedit*. Additional tools for loading and dumping authentication database records are *authload* and *authdump*, which can be used for bulk loading or exporting records. For more information on the operation of *authsrv*, consult the online reference manual.

[1] Alerts are checked using the system *cron*(1M) daemon. See also the manual page for crontab(1)

Firewall Backups

Firewall systems require periodic backups to archival media to minimize downtime in the event of operational error or hardware failure. The Gauntlet system supports all the standard IRIX tape formats and backup tools such as *tar*, *dump*/*restore*, *cpio*, and *bru*. You may prefer to not attach a tape drive to the Gauntlet system and instead perform periodic backups over a network.

System backups may be automated if desired, using conventional UNIX tools for automatic backups. You are cautioned against installing network backup software that runs on the firewall itself if such software permits remote access and command invocation upon the firewall. Many automated network backup programs have been known to contain security flaws. As long as the automated backup technique chosen is entirely invoked with the firewall initiating the connections, the security of the firewall should not be at risk. Generally, once the firewall has been configured, the only parts of the system that will change and require backup are the system logs in */var/adm* and the electronic mail queuing directories in */var/mail* and */var/spool/mqueue*. You may wish to perform a set of archival complete system backups and subsequently resort to incremental backups of the files in */var*.

Once you set up system backups, you may wish to investigate automated checking to see what files have changed on the firewall. This affords additional assurance that your firewall has not been broken into and tampered with.

Appendix A

Gauntlet and IRIX

Gauntlet Administration and IRIX

The Gauntlet software is designed to be easy to set up and operate quickly, even if you are not familiar with the system. If you are an experienced IRIX system administrator, you may prefer to undertake managing the system directly, without using the administrative interface. Remember, though, that once you do so, you effectively give up the use of the browser-based interface for making future changes.

Running a firewall requires a certain amount of expertise. As a firewall system becomes more established, local needs may require its further customization. It is impossible to predict what form local customizations will take, so it is assumed that eventually your Gauntlet system will appear different than the default configuration.

Administrators who wish to move away from relying on the Gauntlet administration tools may use them as a reference, since they are primarily implemented as shell scripts. By convention, modifications against the base IRIX system are retained with the original file renamed to <*file*>*.old.###* where *###* is the process ID. This is to help you determine the differences between a Gauntlet system and a system not yet configured for Gauntlet. You are encouraged to explore the system and to become familiar with its tools and how it operates. The best way to acquire confidence in a security system is to understand its operation and general principles. For that reason, the Gauntlet firewall is designed to be easy to understand as well as operate.

Sample Reports

Sample Alert Report

The report below is a sample of a report generated by a firewall under actual use. Note that the security alerts are sorted separately and presented at the top of the report from the other information. Alerts differentiate between security alerts, system configuration errors, and "other" information. Note the last line in the "other" section; the system disk has overflowed. One advantage of the Gauntlet "tell me what to ignore rather than what to look for" auditing system is that it effectively provides warnings for normal system error messages, such as overflowed disks, disk errors, memory problems, and so on.

Example B-1 Sample Alert Report

```
From root Fri Sep 23 10:30:03 1994
Received: by your.domain; id KAA02230; Fri, 23 Sep 1994 10:30:03 -0400
Date: Fri, 23 Sep 1994 10:30:03 -0400
From: System Administrator <root>
Message-Id: <199409231430.KAA02230@your.domain>
To: firewalladmin
Subject: 09/23/94:10.30 system check
Status: R
Possible Items of Interest
--------------------------
Sep 23 10:16:11 localhost authsrv[2176]: BADAUTH mjr (rlogin-gw unknown/192.33.112.117)
Sep 23 10:16:13 localhost authsrv[2176]: BADAUTH root (rlogin-gw unknown/192.33.112.117)
Sep 23 10:18:12 localhost authedit[2185]: root ENABLED USER mjr
Sep 23 10:18:52 localhost authsrv[2188]: BADAUTH mjr (rlogin-gw unknown/192.33.112.117)
Sep 23 10:18:55 localhost authsrv[2188]: BADAUTH mjr (rlogin-gw unknown/192.33.112.117)
Sep 23 10:19:03 localhost authsrv[2188]: BADAUTH nobody (rlogin- gw unknown/192.33.112.117)
Sep 23 10:19:05 localhost authsrv[2188]: BADAUTH mjr (rlogin-gw unknown/192.33.112.117)
Sep 23 10:19:10 localhost authsrv[2190]: BADAUTH mjr (rlogin-gw unknown/192.33.112.117)
Sep 23 10:19:13 localhost authsrv[2190]: BADAUTH mjr (rlogin-gw unknown/192.33.112.117)
Sep 23 10:19:14 localhost authsrv[2190]: BADAUTH mjr too many tries (rlogin-gw
unknown/192.33.112.117)
Sep 23 10:20:00 gauntlet kernel: uid 0 on /: file system full
```

Sample Weekly Report

The report below is a shortened sample of a report generated by a firewall under actual use. The first section of the report lists electronic mail traffic, decomposed into senders, and recipients sorted in order of greatest usage in terms of data amount and number of messages. Though the system logs contain information cross-referencing sender and recipient, that information is not included in the reports, to protect the privacy of the firewall's users. Summaries of the top users who authenticate to the firewall, as well as FTP traffic and network service access by type, are included.

Example B-2 Sample Weekly Report

```
Electronic Mail Usage
-----------------------------------------------------------------
Total messages: 31955 (173357 Kb)
Top 20 mail recipients (in messages)
Messages
 Count Kb Address
 ----- -- -------
 714 2411.0 avolio@tis.com
 654 1986.8 mjr@tis.com
 180 631.0 fwall-users-request@tis.com
 168 288.5 dave@tis.com
 87 259.6 firewalls@tis.com
Top 20 mail senders (in messages)
Messages
 Count Kb Address
 ----- -- -------
 17146 76358.9 fwall-users-request@tis.com
 1753 4775.3 mjr@tis.com
 567 1368.1 dave@tis.com
 261 778.1 firewalls-owner@greatcircle.com
 154 433.4 avolio@tis.com
Top 20 mail recipients (in kilobytes)
Messages
 Count Kb Address
 ----- -- -------
 714 2411.0 avolio@tis.com
 654 1986.8 mjr@tis.com
 180 631.0 fwall-users-request@tis.com
Top 20 mail senders (in kilobytes)
Messages
 Count Kb Address
```

```
 ----- -- -------
 17146 76358.9 fwall-users-request@tis.com
 1753 4775.3 mjr@tis.com
 567 1368.1 dave@tis.com
 261 778.1 firewalls-owner@greatcircle.com
User Logins
----------------------------------------------------------------
Top 20 permitted user authentications (total: 173)
Logins User ID
------ -------
30 dave
7 avolio
5 mjr_s
Top 20 failed user authentications (total: 77)
Attempts Username
-------- --------
9 anonymous
6 connect
2 tis
2 mjr_s
2 guest
2 dave
2 bob
2 ?
1 whitehousr
1 user
1 system
Authentication Managment Operations
-----------------------------------
administrator PASSWORD mjr
FTP Proxy usage
----------------------------------------------------------------
FTP service users (total: 153)
Connects Host/Address
-------- ------------
120 sol.tis.com/192.33.112.100
6 magellan.tis.com/199.171.39.124
6 kaos.tis.com/192.33.112.218
6 frodo.tis.com/199.171.39.94
4 ziggy.tis.com/192.33.112.161
3 hilo.tis.com/192.33.112.120
2 polaris.tis.com/192.33.112.172
2 hobbs.tis.com/199.171.39.134
1 unknown/150.211.40.151
1 odie.tis.com/199.171.39.132
```

```
FTP service output thruput (total Kbytes: 29568)
KBytes Host/Address
------ ------------
29332 kaos.tis.com/192.33.112.218
235 sol.tis.com/192.33.112.100
FTP service input thruput (total Kbytes: 60875)
KBytes Host/Address
------ ------------
58925 sol.tis.com/192.33.112.100
1133 frodo.tis.com/199.171.39.94
397 magellan.tis.com/199.171.39.124
257 hilo.tis.com/192.33.112.120
128 polaris.tis.com/192.33.112.172
17 kaos.tis.com/192.33.112.218
14 ziggy.tis.com/192.33.112.161
Telnet/Rlogin Proxy Usage
---------------------------------------------------------------
Top 20 telnet gateway clients (total: 330)
Connects Host/Address Input Output Total
-------- ------------ ----- ------ -----
 84 sol.tis.com/192.33.1 782715 11262 793977
 78 socks.tis.com/192.94 7923948 239618 8163566
 36 fred.tis.com/192.94. 18093531 131111 18224642
 12 hilo.tis.com/192.33. 852409 5576 857985
 10 unknown/45.69.0.165 461495 13802 475297
 9 happy.tis.com/192.33 2805 381 3186
 8 otter.tis.com/192.33 449661 1461 451122
 8 magellan.tis.com/199 76980 448 77428
 6 odie.tis.com/199.171 409016 3332 412348
 4 piobmor.tis.com/192. 200561 1430 201991
 4 frodo.tis.com/199.17 503896 5903 509799
 4 eleven.tis.com/192.3 2057 459 2516
Top 20 telnet gateway clients in terms of traffic
Connects Host/Address Input Output Total
-------- ------------ ----- ------ -----
 36 fred.tis.com/192.94. 18093531 131111 18224642
 10 unknown/45.69.0.165 461495 13802 475297
 84 sol.tis.com/192.33.1 782715 11262 793977
 8 otter.tis.com/192.33 449661 1461 451122
 4 piobmor.tis.com/192. 200561 1430 201991
 2 unknown/20.2.1.193 34091 776 34867
 2 kuki.tis.com/192.33. 29699 538 30237
 4 eleven.tis.com/192.3 2057 459 2516
Network Service Connections
---------------------------------------------------------------
```

```
Top 20 network service users (total: 2038)
Connects Host/Address
-------- ------------
946 kaos.tis.com/192.33.112.218
486 sol.tis.com/192.33.112.100
135 hilo.tis.com/192.33.112.120
106 gildor.tis.com/192.33.112.113
79 socks.tis.com/192.94.214.158
57 reddwarf.tis.com/192.33.112.12
36 fred.tis.com/192.94.214.201
30 magellan.tis.com/199.171.39.124
15 otter.tis.com/192.33.112.117
12 happy.tis.com/192.33.112.61
12 frodo.tis.com/199.171.39.94
10 unknown/45.69.0.165
6 ziggy.tis.com/192.33.112.161
6 polaris.tis.com/192.33.112.172
6 localhost.tis.com/127.0.0.1
4 relay.tis.com/192.94.214.100
Top 20 Denied network service users (total: 4)
Connects Host/Address
-------- ------------
3 magellan.tis.com/199.171.39.124
1 sol.tis.com/192.33.112.100
Service Requests
Requests Service
-------- -------
1048 in.fingerd
276 http-gw
194 in.telnetd
189 traceroute-gw
157 in.ftpd
151 in.rlogind
15 whois-gw
8 ping-gw
4 x-gw
```

Configuring World Wide Web Clients

Configuring WWW Clients

Most World Wide Web (WWW) clients support the ability to use a proxy server. Despite the fact that transparency would eliminate the need for proxying WWW traffic, users should configure their clients to use the proxy server if at all possible. This is because many WWW sites run servers on non-standard ports (other than port 80) which the transparency feature of the firewall does not enable access to.

Note: Only the Netscape Navigator browser is supported for running the Gauntlet forms-based administrative interface. Users may, of course, use other browsers to access WWW resources.

UNIX Based clients

Most UNIX-based clients, such as the original NCSA Mosaic, support proxy forwarders via a number of shell environment variables. Setting the environment variables into the process environment is easily done by creating a small shell script that then calls the real executable. Note that the FTP proxy port is port 80, not the normal FTP port 23. When accessing FTP URLs, the HTTP proxy performs FTP commands itself on behalf of the user, bypassing the FTP proxy. This example shell script might be named */usr/local/bin/xmosaic*:

```
#!/bin/sh
http_proxy=http://relay.tis.com:80/
wais_proxy=http://relay.tis.com:8080/
gopher_proxy=http://relay.tis.com:80/
ftp_proxy=http://relay.tis.com:80/
export http_proxy wais_proxy gopher_proxy ftp_proxy
if [ $# != 0 ] ; then
 args=$*
else
 args=http://www.tis.com/
```

```
fi
Mosaic-sun-lresolv $args
rm -f $HOME/.mosaicpid
```

NCSA Mosaic for Windows

Using NCSA Mosaic for Windows, the HTTP proxy values are defined in the *mosaic.ini* file as shown in the example above. Note the attributes for proxy information, which are defined as pointing to the firewall for all services.

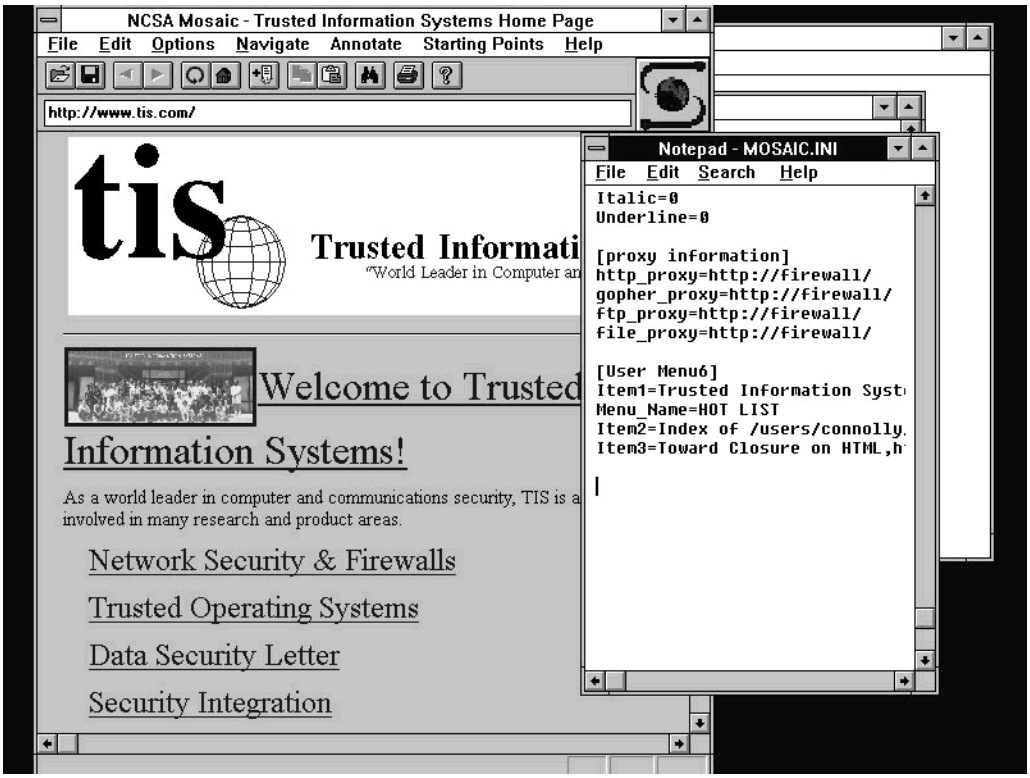

Figure C-1 NCSA Mosaic for Windows

NetScape for UNIX or Windows

Netscape menus directly support defining proxy servers. Select the "Options / Preferences / Mail" and "Proxies" menus and enter the firewall as the proxy server, using the HTTP port 80 as the service port. Netscape also provides an option for "No Proxy On," permitting users to specify a pattern indicating what systems should be contacted directly, rather than via the proxy. This is valuable for organizations that have servers internally that are reachable directly, in addition to servers on the other side of the firewall.

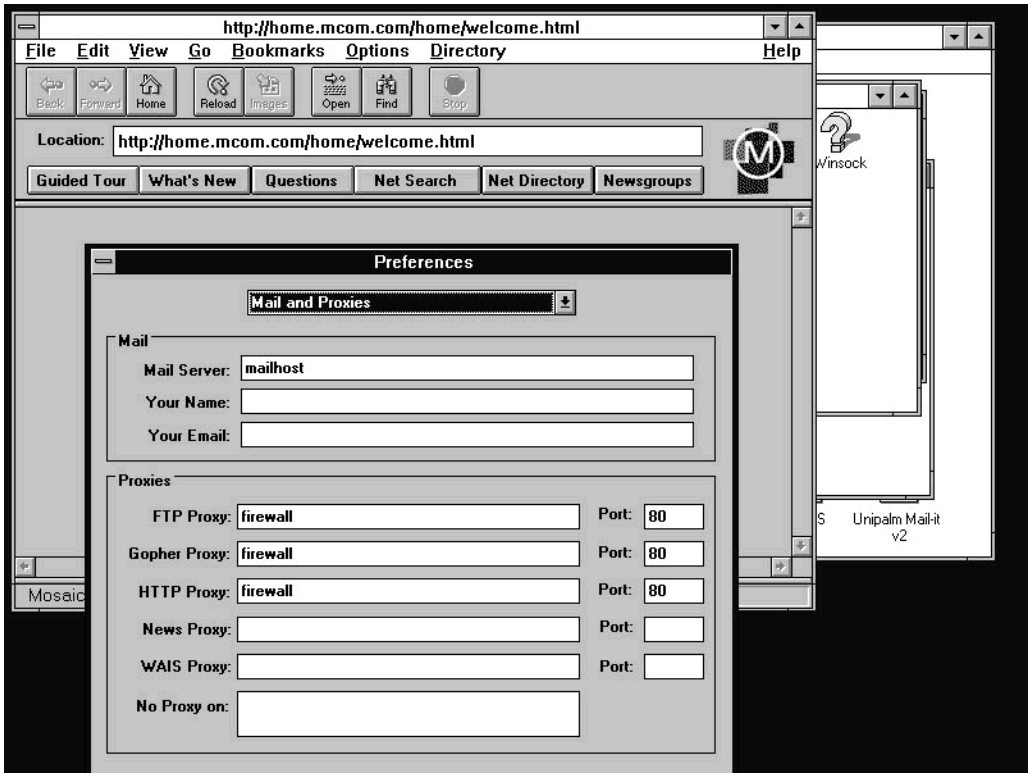

Figure C-2 NetScape for UNIX or Windows

Spry Air Mosaic

Spry Air Mosaic client software supports proxy configuration via the "Options / Configuration / Proxy Servers" menu. The proxy name and port is encoded as a URL in the form of *http://firewall:port/*, where the name of the firewall is the name of the firewall's internal network connection. The *Exclude Domains* option on the proxy menu permits the user to specify which domains should not be accessed via the proxy.

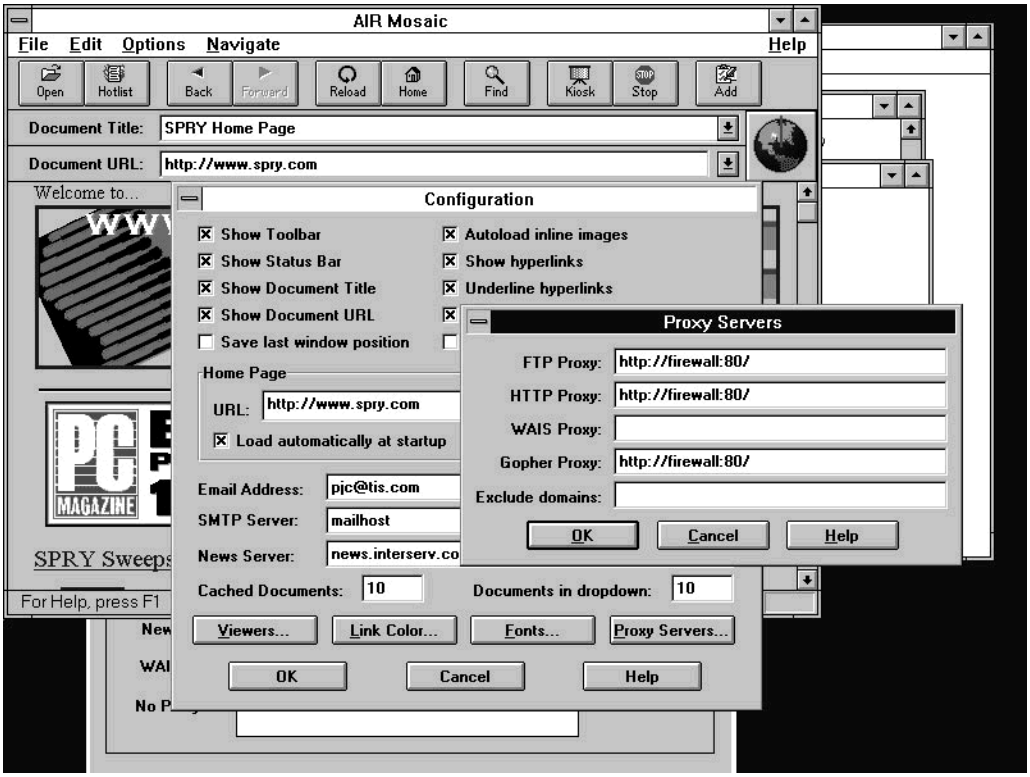

Figure C-3 Spry Air Mosaic

Index

R

S

T

U

V

W

X

We'd Like to Hear From You

As a user of Silicon Graphics documentation, your comments are important to us. They help us to better understand your needs and to improve the quality of our documentation.

Any information that you provide will be useful. Here is a list of suggested topics to comment on:

- General impression of the document
- Omission of material that you expected to find
- Technical errors
- Relevance of the material to the job you had to do
- Quality of the printing and binding

Please include the title and part number of the document you are commenting on. The part number for this document is 007-2826-001.

Thank you!

Three Ways to Reach Us

The **postcard** opposite this page has space for your comments. Write your comments on the postage-paid card for your country, then detach and mail it. If your country is not listed, either use the international card and apply the necessary postage or use electronic mail or FAX for your reply.

If **electronic mail** is available to you, write your comments in an e-mail message and mail it to either of these addresses:

- If you are on the Internet, use this address: techpubs@sgi.com
- For UUCP mail, use this address through any backbone site: *[your_site]*!sgi!techpubs

You can forward your comments (or annotated copies of manual pages) to Technical Publications at this **FAX** number:

415 965-0964