

WebFORCE™ Firewall Administrator's Guide

Document Number 007-2613-001

CONTRIBUTORS

Written by John Raithel

Production by Chris Everett

Engineering contributions by Nelson Bolyard, Andrew Chersonson, Tina Darmohray,
Eliot Lear.

Cover design and illustration by Rob Aguilar, Rikk Carey, Dean Hodgkinson,
Erik Lindholm, and Kay Maitz

© Copyright 1995, Silicon Graphics, Inc.— All Rights Reserved

This document contains proprietary and confidential information of Silicon Graphics, Inc. The contents of this document may not be disclosed to third parties, copied, or duplicated in any form, in whole or in part, without the prior written permission of Silicon Graphics, Inc.

RESTRICTED RIGHTS LEGEND

Use, duplication, or disclosure of the technical data contained in this document by the Government is subject to restrictions as set forth in subdivision (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 52.227-7013 and/or in similar or successor clauses in the FAR, or in the DOD or NASA FAR Supplement. Unpublished rights reserved under the Copyright Laws of the United States. Contractor/manufacturer is Silicon Graphics, Inc., 2011 N. Shoreline Blvd., Mountain View, CA 94043-1389.

Silicon Graphics, the Silicon Graphics logo, and IRIS are registered trademarks and IRIX, WebFORCE, and IRIS Insight are trademarks of Silicon Graphics, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd. Netsite and Netscape Navigator are trademarks of Netscape Communications Corporation. PostScript is a registered trademark of Adobe Systems, Inc.

Contents

	List of Figures	v
	About This Guide	vii
	Style Conventions	viii
1.	Introduction	1
	The Internet Today	1
	Network Security and Firewalls	1
	Network Security Issues	2
	What Is a Firewall?	3
	Firewall Design Philosophy	4
	World Wide Web Issues	5
2.	Controlling Internet Access With a Firewall	7
	Hardware Configuration	7
	Routers and Firewalls	7
	Configuring SGI Hardware for Use as a Firewall	8
	Dual-Homed Host Firewall	8
	Screened Host Gateway	9

- IRIX Configuration 11
 - Network Software Setup on a Dual-Homed Host 11
 - Tightening Security in IRIX 11
 - Disable Forwarding of IP Packets 11
 - Limiting *inetd* Services 12
 - Password Protection 15
 - Limiting *rpc* Services Access 16
 - Disabling NIS (YP) 16
 - Limiting NFS access 17
 - Limiting X11 Access 17
 - Setting Up a Proper Anonymous FTP Account 18
 - Setting up a Proper Log File 18
 - Checking Software Integrity 18
 - Educating Users 19
 - Network Configuration 19
 - Domain Name System (DNS) 19
 - Mail Configuration 20
 - sendmail* Configuration and Mail Aliases 20
 - Spool Isolation 21
 - Using Proxy Servers 21
- 3. Additional Resources 23**
 - Books 23
 - Internet Resources 24
 - Network Security and Firewalls 24
 - Proxy Servers 24
 - Commercial Products 25
 - Software 25
 - Connecting to the Internet 25

List of Figures

Figure 1-1	A Simple Firewall Environment	4
Figure 2-1	Screened Host	9
Figure 2-2	Screened Subnet	10

About This Guide

The *WebFORCE Firewall 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.

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 should be used in conjunction with the *IRIX Advanced Site and Server Administration Guide*.

The *WebFORCE Firewall Administrator's Guide* is primarily concerned with helping you to construct a firewall—a system that separates your internal 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.

This document contains the following chapters:

- Chapter 1, “Introduction,” provides an overview of the internetworked environment. Key concepts such as the Internet, World Wide Web, and firewalls are discussed.
- Chapter 2, “Controlling Internet Access With a Firewall,” provides details on how to configure the IRIX operating system to prevent unwanted intrusions into your internal network.
- Chapter 3, “Additional Resources,” is a list of references and pointers that provide additional information and contacts with which you can further develop a secure installation.

Caution: The WebFORCE Firewall 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 needs.

Style Conventions

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 and UNIX commands are shown in italics for example, the file and pathname */var/sysgen/master.d/bsd* is printed *like that*.

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

```
# autoconfig -f
```

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

In some cases, screen output of a line of text must be broken to fit on the page of the printed copy. When this is done, a backslash (\) is placed in the far right column of the broken line to indicate that the line continues, for example:

```
tftp dgram udp wait guest /usr/etc/tftpd tftpd -s \  
/usr/local/boot /usr/etc/boot
```

This is actually all one line of text.

Introduction

This chapter provides an overview of some of the basic features and terminology of the Internet, and introduces various issues discussed in greater detail throughout this document.

The Internet Today

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 of importance 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 for 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 seen and accessed around the world.

Network Security and Firewalls

This document addresses an important aspect of this internetworked accessibility: the need to establish and maintain the security of local computers and computer networks. Specifically, computer sites have a need and a right to determine the privacy and safety of their data from

competitive interests as well as outright software vandalism. The Internet presents ways to share data that you want to share, but you must take measures to protect data that you want protected.

Network Security Issues

If you are connecting to 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 Chapter 3 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 router¹ or computer host or as complex as multiple routers and an entire computer network. 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 internal resources.

¹This 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.

What Is a Firewall?

The line between the external world of untrusted hosts and the internal world of trusted hosts is established 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 really one of ease of use vs. 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. Silicon Graphics can only present the issues here and point to other resources for additional information and services to help you establish your policies.

An example of a simple firewall is shown in Figure 1-1. In this illustration, a single computer host such as an Indy 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 obstruction between your internal network and the Internet where you can focus your security efforts. In this document, the term firewall host refers to an IRIX host configured for network security.

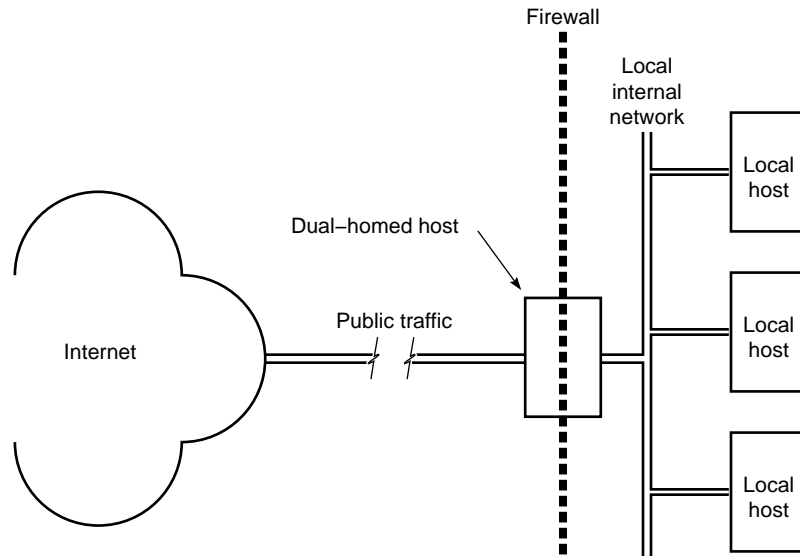


Figure 1-1 A Simple Firewall Environment

The firewall does not in any way restrict interactions on your internal network. Local hosts may share resources in the same way they did before connecting to the firewall. What is different is that now, to the extent determined by your site policy, these hosts may interact with external sites as well. Chapter 2 presents some scenarios of how you might configure a network with a dual-homed host.

Firewall Design Philosophy

The key to administering network security is the firewall. While there are important issues concerning internal security, those issues are the same regardless of whether or not you are connected to the Internet (for references on UNIX system security, refer to Chapter 3, “Additional Resources”).

Regarding the firewall itself, you should:

- limit users—if possible, limit users to the sole administrator of the system. If additional users are necessary, refer to Chapter 2,

“Controlling Internet Access With a Firewall,” for a discussion of issues regarding password protection and educating users.

- limit services—the more services you allow, the more possible security holes you present. In addition and in general, the more complex the software providing these services the more chance for compromise, and the newer the software, the less chance it has been well tested in the “real world.”
- monitor the system—this document helps you configure the IRIX software of your firewall to maintain log files that can provide information on accesses to your firewall host, including time of access and unsuccessful access attempts. Also, make use of the many standard UNIX tools such as *w(1)*, *ps(1)*, and so on that give you snapshots of current system activities.

World Wide Web Issues

There is the same security issue inherent in accessing software on the World Wide Web that has always been an issue when acquiring software from any unknown or untrusted source. When a user clicks on a browser button for a network resource, what is invoked is unknown. A click, for example, could download an executable PostScript™ file with a potential for damage. Users should be aware of this issue. If this is a serious concern at your site, you may consider isolating and limiting those hosts with World Wide Web access.

If you are setting up the Netsite™ server for your World Wide Web site, refer to Appendix B of the *Netsite Communications Server Administrator's Guide*, particularly the sections on “HTTP User Access Control” and “Make Your Server Safe”.

Refer to “Internet Resources” on page 24 for a pointer (URL) to additional information on security issues related to the World Wide Web.

Controlling Internet Access With a Firewall

This chapter discusses how to set up a “firewall”—a configuration that stands between your local network and your Internet service provider. The types of firewalls discussed are those in which an IRIX host is configured as part of the firewall. A general overview of some possible hardware configurations is presented, and the rest of the chapter presents detailed information on configuring IRIX software.

Hardware Configuration

This section discusses how to configure network hardware to serve as the hardware portion of a firewall solution. (For information on how to configure Silicon Graphics software in a firewall solution, refer to “IRIX Configuration” on page 11.) Only setups that include an IRIX host as part of the solution are discussed, as router-only solutions tend to be too limited. The use of a firewall host has the advantages of permitting and restricting specific applications, maintaining log files, and adding authentication to network access.

Routers and Firewalls

The firewall host is typically combined with a router, whether provided as part of your connection to your Internet service provider (referred to as an ISP router in this document) or added by you to your private configuration. Many routers can be configured to provide IP packet-level security, but do not support such features as proxies and authentication (See “Using Proxy Servers” on page 21). To add these features, you must have a system such as the IRIX host setups described in the rest of this chapter.

When using a router with a firewall host, configure it to allow traffic only to the firewall host. You should filter out:

- ICMP¹ redirects not from the router
- IP packets specifying the loose source routing option
- external packets claiming to be from the internal network (known as “spoofing”)

Consult with your Internet service provider to determine the packet filtering options available for your Internet connection. You can also add routers to your firewall configuration as described in the next section, and then configure your routers with additional filtering options (refer to the router vendor documentation for details). (See also “Packet Filtering Gateways,” in *Firewalls and Internet Security*, by Cheswick and Bellovin, referenced in “Books” on page 23.)

Refer to *ipfilterd*(1M) for information on IP packet filtering with IRIX.

Configuring SGI Hardware for Use as a Firewall

This section discusses general hardware configuration issues for the basic setup of a dual-homed host acting as the firewall, and then presents the “screened host” and “screened subnet” firewall configurations.

Dual-Homed Host Firewall

You can configure your Silicon Graphics host hardware for use in a firewall by making it a dual-homed gateway—that is, giving it two network connections. Figure 1-1 illustrates the general idea of using a dual-homed host as the firewall.

Creating a dual-homed host may involve, for example, adding an additional Ethernet controller board, or you may already have two Ethernet connections. For specific information on the network hardware in your system, refer to your system documentation. For information on configuring

¹Internet Control Message Protocol

network hardware, refer to “Networking Hardware” in the *IRIX Advanced Site and Server Administration Guide*.

Screened Host Gateway

A screened host scenario uses a router to screen traffic between the Internet and the external network connection of the firewall host. It can further limit traffic to a few ports of the firewall host. No traffic is allowed from the outside to any other host on the internal network. This is the typical connection to the Internet in which the router is provided by the Internet service provider. Figure 2-1 illustrates the basic screened host scenario.

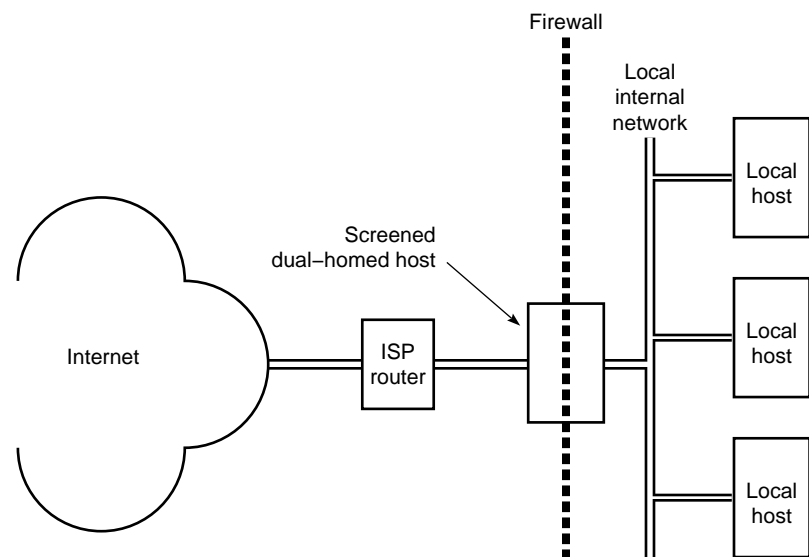


Figure 2-1 Screened Host

An additional level of complexity—and flexibility—is added when you expand the screened host scenario to a screened network scenario. The basic design remains the same, but the screened network receives all external traffic. Both the Internet and the internal network have access to the screened network, but traffic must still pass through the firewall host. This is useful for sites that want to make multiple servers available to the Internet and yet maintain a secure internal network. You could, for example, use one of the

public hosts as your WWW server and another as an FTP server, depending on what you want to make available and the relative CPU loads expected.

Figure 2-2 illustrates a screened subnet¹.

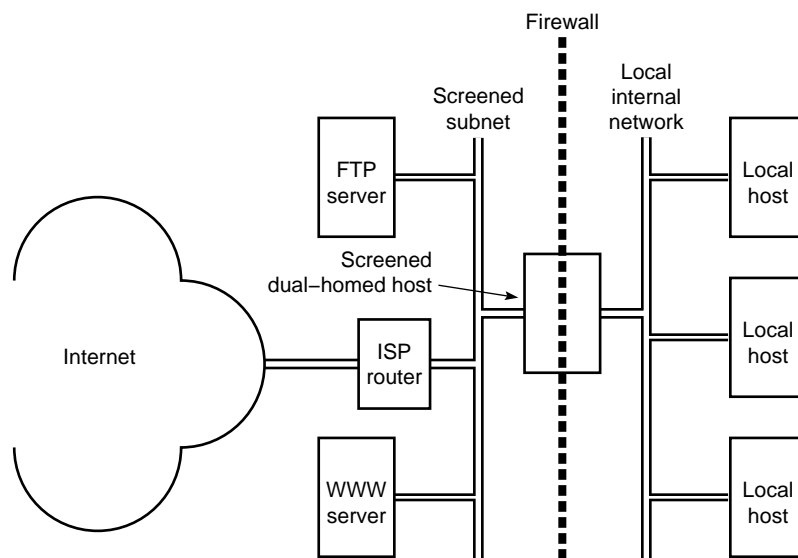


Figure 2-2 Screened Subnet

In the situation shown in the example, you continue to concentrate your security efforts on the single firewall host. Remember though, that your servers outside of the firewall are more easily compromised as they are protected only by a router. Keep your private data on the internal network and forward important data collected on the public servers to an internal host. (Details on software configuration are discussed in the next section.)

¹The “screened subnet” is sometimes called a “demilitarized zone” or “red zone”.

IRIX Configuration

This section discusses the basic network addressing configuration required on a firewall host, and then provides details on configuring IRIX software to tighten security on the host.

Note: Unless specified otherwise, all the software changes discussed in this section are to be performed on the firewall host.

Network Software Setup on a Dual-Homed Host

A dual-homed host is configured in network software as if it is two hosts, each with a different network address and, optionally, a different name. Use separate IP addresses for the two (or more) network interfaces. Refer to “Configuring a Router with Two Interfaces” in the *IRIX Advanced Site and Server Administration Guide*.

Tightening Security in IRIX

This section discusses various modifications you can make to the IRIX operating system software to provide for increased network security. Some of these changes are highly desirable on a firewall; others are more a matter of personal choice depending on the level of security you feel is necessary. The issues discussed include why the changes must or might be made.

The following discussion of changes made to the firewall host software also applies to any host made publicly-accessible, such as the WWW server and FTP server shown in the screened subnet example in Figure 2-2.

Note: When you have finished the procedures described in this section, reboot your firewall system to ensure that all changes take effect. *Many of these changes do not take effect until the system is rebooted.*

Disable Forwarding of IP Packets

By default, IRIX forwards IP packets on machines with more than one network hardware interface. You must edit a kernel configuration file, run *autoconfig*, and then reboot to disable this default.

Follow this procedure to turn off automatic IP packet forwarding:

1. Edit the file `/var/sysgen/master.d/bsd`, changing the value of `ipforwarding` to 0:

Change the line:

```
int ipforwarding = 1;
```

to

```
int ipforwarding = 0;
```

2. Save the modified `/var/sysgen/master.d/bsd` file and exit from the editor.
3. Run `autoconfig` with the `-f` option:

```
# autoconfig -f
```

This creates a `/unix.install` file which becomes the new `/unix` after the system is rebooted.

4. Reboot your system.
5. To verify that IP packet forwarding has been disabled after your system comes back up, use the `netstat` command:

```
# netstat -s -p ip | grep forwarding
```

You should see the following:

```
0 packets forwarded (forwarding disabled)
```

If you do not see this message, repeat steps 1 through 5 until you do. (Be sure that your root file system has enough disk space so that the `/unix.install` file is being created correctly. See `autoconfig(1M)` for more information.)

Limiting `inetd` Services

When your system starts up, the `inetd` process reads the `/etc/inetd.conf` file for a list of Internet services to support. Comment out services listed in this file that are not very secure or that you are not using.

Note: These services are being disabled on the firewall only. Services that are commented out in the system files on the firewall may still be available on your internal network—you just can't use them on the firewall host.

1. Edit the file */etc/inetd.conf*, and add the # symbol at the beginning of the following lines to comment them out (some may have already been commented out):

```
exec    stream tcp    nowait root    /usr/etc/rexecd    rexecd
bootp   dgram  udp    wait  root    /usr/etc/bootp     bootp
rstatd/1-3 dgram  rpc/udp wait  root    /usr/etc/rpc.rstatd rstatd
walld/1   dgram  rpc/udp wait  root    /usr/etc/rpc.rwalld rwalld
rusersd/1 dgram  rpc/udp wait  root    /usr/etc/rpc.rusersd rusersd
rquotad/1 dgram  rpc/udp wait  root    /usr/etc/rpc.rquotad rquotad
bootparam/1 dgram  rpc/udp wait  root    /usr/etc/rpc.bootparamd bootparam
ypupdated/1 stream  rpc/tcp wait  root    /usr/etc/rpc.yupdated ypupdated
rexcd/1   stream  rpc/tcp wait  root    /usr/etc/rpc.rexcd  rexcd
```

In other words, they should look like this:

```
#exec    stream tcp    nowait root    /usr/etc/rexecd    rexecd
#bootp   dgram  udp    wait  root    /usr/etc/bootp     bootp
#rstatd/1-3 dgram  rpc/udp wait  root    /usr/etc/rpc.rstatd rstatd
#walld/1   dgram  rpc/udp wait  root    /usr/etc/rpc.rwalld rwalld
#rusersd/1 dgram  rpc/udp wait  root    /usr/etc/rpc.rusersd rusersd
#rquotad/1 dgram  rpc/udp wait  root    /usr/etc/rpc.rquotad rquotad
#bootparam/1 dgram  rpc/udp wait  root    /usr/etc/rpc.bootparamd bootparam
#ypupdated/1 stream  rpc/tcp wait  root    /usr/etc/rpc.yupdated ypupdated
#rexcd/1   stream  rpc/tcp wait  root    /usr/etc/rpc.rexcd  rexcd
```

If you want details on the services you are disabling, refer to their reference pages. For example, refer to *rexecd(1M)* for more information on the *rexecd* daemon.

2. Comment out or restrict the following entries in */etc/inetd.conf*:

```
ftp     stream tcp    nowait root    /usr/etc/ftpd    ftpd -la
telnet  stream tcp    nowait root    /usr/etc/telnetd telnetd
shell   stream tcp    nowait root    /usr/etc/rshd    rshd
login   stream tcp    nowait root    /usr/etc/rlogind rlogind
tftp    dgram  udp    wait  guest   /usr/etc/tftpd   tftpd -s \
/usr/local/boot /usr/etc/boot
```

If you comment them out (totally disable them), they should look like this:

```
#ftp     stream tcp    nowait root    /usr/etc/ftpd    ftpd -l
#telnet  stream tcp    nowait root    /usr/etc/telnetd telnetd
#shell   stream tcp    nowait root    /usr/etc/rshd    rshd
#login   stream tcp    nowait root    /usr/etc/rlogind rlogind
```

```
#tftp  dgram  udp    wait  guest  /usr/etc/tftpd  tftpd -s \  
/usr/local/boot /usr/etc/boot
```

To be safe, it is best to disable all those services with the comment character as shown above. If, however, you must include any of these services, change them as indicated below so that they record a log of their use in the file */var/adm/SYSLOG*:

```
ftp    stream  tcp    nowait  root    /usr/etc/ftpd  ftpd -ll  
shell  stream  tcp    nowait  root    /usr/etc/rshd   rshd -lal  
tftp   dgram   udp    wait    guest   /usr/etc/tftpd  tftpd -s -l -h /dev/null
```

Of these, enabling *rshd* is probably the most dangerous, and *tftpd* is almost never required on a firewall. Regarding *ftpd*, refer to the section “Setting Up a Proper Anonymous FTP Account” on page 18. Note the options added to each daemon invocation. (For more information, refer to the reference page for any daemon you modify.)

The *telnetd* and *rlogind* entries have not been included here because remote logins can (and should) be controlled with the use of one-time passwords. One-time passwords are just that—a password can be used once to gain access, but any future use of that same password is disallowed. There are various ways to implement one-time passwords, and how (and if) you use them at your site depends on your need for remote login capability and the degree to which you want to authenticate such logins. Refer to the *Firewalls and Internet Security* book referenced in “Books” on page 23.

3. The *fingerd* service is also a potential security hole because it is a source of account names. You can use the **-S** option to suppress information about login status, home directory, and shell, which might be used to attack security:

```
finger stream tcp    nowait  guest  /usr/etc/fingerd  fingerd -S
```

Or, to be more secure, you can configure *fingerd* with the **-f** option, to return just a message file. In the following example, a message has been placed in */etc/fingerd.message*:

```
finger stream tcp    nowait  guest  /usr/etc/fingerd  fingerd -f \  
/etc/fingerd.message
```

and the contents of */etc/fingerd.message* might say something like:

Thank you for your interest in XYZ company. Please contact us at xyz.email.address or 1-800-XYZ-PHON for more information.

The same message is then returned for any *finger* access.

4. When you have finished making changes to the */etc/inetd.conf* file, write the changes and quit the editor. The changes take effect after a reboot or, if you want to apply them immediately, enter:

```
# killall -HUP inetd
```

5. Test any modified services to be sure they perform as expected.

Password Protection

Limit the number of users with login accounts on the firewall system as much as possible. All accounts in */etc/passwd* should have a password (see *passwd(1)*).

1. Check the */etc/passwd* file to be sure that all accounts have passwords—the second field should not be empty (::).

Use the *passwd* command to add passwords for any accounts that do not have one. Choose long passwords composed of arbitrary ASCII characters—the password should not be in any dictionary.

2. Edit the */etc/default/login* file to include the following lines:

```
SYSLOG=ALL
```

This causes all login attempts—successful or not—to be recorded in the system log (see *syslog(3C)*).

```
MAXTRYS=1
```

This causes login to exit after a single incorrect login. Note that if you set this value to 0, it allows unlimited login attempts.

```
DISABLETIME=5
```

Sleep for 5 seconds after an unsuccessful login attempt before exiting. Make it a longer period if you are experiencing attempts at password guessing.

```
MANDPASS=YES
```

No user is allowed to log in without a password.

For more information on these fields and the */etc/default/login* file, refer to *login(1)*.

3. Check to see if there are any */etc/hosts.equiv* or *\$HOME/.rhosts* files. These files can be configured to allow remote access without password protection, and should not be allowed on a firewall host. Refer to *hosts.equiv(4)* for more information.

Limiting *rpc* Services Access

You can limit access to the firewall host's RPC services by use of the *portmap* command's **-a** option. This allows you to specify the host(s) and/or network(s) within your firewall that are allowed access to RPC-based services. Edit the file */etc/config/portmap.options* to add options to the *portmap* command that is executed at system startup.

For example, if you create a */etc/config/portmap.options* file with the following entry:

```
-a 192.0.2.0
```

access to firewall host RPC services are restricted to hosts on the Class C network 192.0.2.

The syntax for the **-a** option allows you to specify multiple network masks, network addresses, and host addresses. As usual, the fewer hosts and/or networks allowed access, the better the security. Refer to the reference page *portmap(1M)* for more information.

Disabling NIS (YP)

Because NIS (formerly called Yellow Pages) has a number of known security holes, remove it from the firewall host as shown in the following steps:

1. Remove the NIS software from the firewall host with the *versions* command:

```
# versions remove nfs.sw.nis
```
2. Certain databases may have been modified to add NIS information by including a **+** symbol in database entry. Use an editor to remove any lines beginning with the **+** symbol from the files */etc/passwd*, */etc/group*, and */etc/aliases*.

3. Remove the */etc/netgroups* file if it exists.

Limiting NFS access

Exporting filesystems and remote mounting external systems on the firewall host can present security problems. You have a few options:

- You can disallow NFS altogether:

```
# chkconfig nfs off
```
- You can edit the */etc/exports* file to limit exported filesystem permissions and access. You can, for example, use the *rw=hostname* option to limit read-write access to a specific host, or you can use the *access=client* option to limit mounting to specified hosts. Refer to the reference page for *exports(4)* for more information.
- If you choose to mount external systems on the firewall host, use the *mount* command with the **nosuid** option to prevent running a trojan horse. Refer to the reference page for *fstab(4)* for details.

Limiting X11 Access

The default configuration allows all hosts access to your display, and this should be disabled. Edit the */var/X11/xdm/Xsession** files to comment out or remove the *xhost +* entries. For example, in */var/X11/xdm/Xsession*, the lines that look like this:

```
# Gives anyone on any host access to this display  
/usr/bin/X11/xhost +
```

should look like this:

```
# Gives anyone on any host access to this display  
# /usr/bin/X11/xhost +
```

Also inform users not to use the *xhost +* command, or simply delete it.

For even better security (just commenting out *xhost +* still allows local programs to connect to the X server), you can enable X authority. To do this, change the *DisplayManager*authorize* entry in */var/X11/xdm/xdm-config* to say:

```
DisplayManager*authorize: on
```

This makes *xdm* generate “magic cookies” (put in each user’s *\$HOME/.Xauthority* file) which are then required for any X client to connect to the X server. This provides a good means of X server access control. (Note that this may already be the default on your system.).

Setting Up a Proper Anonymous FTP Account

If you want to allow anonymous FTP access to the firewall host (or any publicly-accessible host), complete instructions for an anonymous FTP account are given in the reference page for the daemon process, *ftpd(1M)*. Note that if you allow anonymous FTP access, you should enable logging but not disable the *ftpd* process as was described in “Limiting inetd Services” on page 12.

An additional risk is incurred if you allow writes to your anonymous FTP directory. Excessive writes to a crucial system partition could disable the system. It is a good idea to isolate the *ftp* directory to a separate partition or disk (if you allow writes) for this reason.

Setting up a Proper Log File

Log files provide useful information to the firewall administrator, recording specific or all attempts at firewall host login. The various options used to turn on login logging for different daemons have been covered in the discussions on each daemon. Note that the log files must be reviewed periodically to be of use.

Log files are sensitive information and need not be stored on the firewall host. Refer to *syslogd(1M)* for information on how to forward *syslog* messages from the firewall host to a trusted host inside the firewall.

Checking Software Integrity

All software on a firewall host should be watched for modification. A record of checksums of software should be kept and compared periodically to detect unauthorized changes. For this reason too, the less software installed on the firewall host the better.

Educating Users

You can take great pains to make a secure firewall and then have security compromised by users ignorant of the consequences of their actions. If possible, do not allow user accounts on the firewall host. If you do allow user accounts, be sure to tell the account holders:

- Don't use *.rhosts* files (you can add the `-l` option to the *rshd* invocation in */etc/inetd.conf* and thereby disallow these files on the firewall. See *rshd(1M)* for more information.)
- Use passwords with long, non-dictionary, ASCII strings, change them frequently, and don't write them down!
- Don't use the "*xhost +*" command (you can delete the binary, or limit its execution to the superuser as well.).

Even your supposedly protected internal network can be compromised by inappropriate actions of users. If, for example, a user on an internal host attaches a modem and establishes a PPP or SLIP session with an external site, you now have a situation in which the external world has two connections to your internal network—one through the firewall, but the other directly to a non-secure, internal host.

Network Configuration

While it is beyond the scope of this document to describe how to configure your internal network, this section discusses issues of DNS and *sendmail* configuration that relate specifically to firewall security.

Domain Name System (DNS)

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 host names 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 host name. This makes it easy to move these services to different hosts if you want to separate them later.

Mail Configuration

This section presents some suggestions for limiting the susceptibility of your site to an attack through the electronic mail system. Internet electronic mail is based on the Simple Mail Transfer Protocol, or SMTP. The program that implements that protocol is commonly referred to as *sendmail*. *sendmail* is a large and complicated program that is frequently the subject of attack.

***sendmail* Configuration and Mail Aliases**

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 *sendmail* 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.

A note about current convention: It is popular 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, it is recommended that you configure your *sendmail* to rewrite all your addresses to conform to the above convention.

For details on how to configure *sendmail*, refer to the *IRIX Advanced Site and Server Administration Guide*.

Spool Isolation

If a barrage of email is sent to your firewall host, it can fill up the disk and paralyze further operation. If you are concerned about this possibility, isolate the mail spool by putting it on a disk or disk partition of its own. While this does not prevent email from being overwhelmed, it does keep a crucial system disk partition, such as */usr*, from filling up.

Using Proxy Servers

A proxy server is an application that implements security for a particular network service. It is basically an application-level gateway—by “understanding” the particular application protocol, it is able to transparently intercept traffic and so implement protocol-specific security, logging, authentication, and so on.

Proxy servers provided on the firewall can allow, for example, internal users to use Netscape Navigator™ to access the World Wide Web, use *ftp* to transfer files between a host on the internal network and one on the Internet, or to *telnet* to an external host for an interactive session.

Two of the most common proxy server solutions are those supplied in the TIS Firewall Toolkit, and the SOCKS proxy server. The proxy servers available with the TIS Firewall Toolkit implement server-side only applications, in which one proxy server exists for each supported application. The SOCKS approach utilizes a *socksd* process on the server, and then requires any application that communicates with it to be “SOCKSified” that is, compiled with the SOCKS library. The Netscape Navigator, for example, comes already “SOCKSified”.

Refer to “Proxy Servers” on page 24 and the WebFORCE page on Proxy Servers for more information

Additional Resources

This chapter 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.

- *IRIX Advanced Site and Server Administration Guide*, Silicon Graphics, This document is available online and can be viewed by using IRIS InSight™.
- *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

Various resources addressing security are provided on the Internet itself. Pointers (URLs) are provided here rather than including them in full as the material is frequently updated.

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. Listed below are pointers to some of these resources.

Network Security and Firewalls

- <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.
- <http://www-ns.rutgers.edu/www-security/index.html>
Ahome page for security issues related to the World Wide Web.

Proxy Servers

- <http://neptune.tis.com/Home/NetworkSecurity/Toolkit.html>
A toolkit for network security including source code for proxys.
- <ftp://ftp.nec.com/pub/security/socks.cstc/>
Where to begin for looking into SOCKS proxys. A FAQ, the proxys, and other information are accessible from this URL.

Commercial Products

Software

For information, support, and software for implementing firewall security, contact Trusted Information Systems, Inc.(TIS), 3060 Washington Road, Glenwood, MD, 21738 (301) 854-6889, netsec@TIS.COM. (See also the URL referenced for TIS under Proxy Services above).

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.

Tell Us About This Manual

As a user of Silicon Graphics products, you can 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:

- 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 send the title and part number of the document with your comments. The part number for this document is 007-2613-001.

Thank you!

Three Ways to Reach Us

- To send your comments by **electronic mail**, use either of these addresses:
 - On the Internet: techpubs@sgi.com
 - For UUCP mail (through any backbone site): *[your_site]!sgi!techpubs*
- To **fax** your comments (or annotated copies of manual pages), use this fax number: 650-932-0801
- To send your comments by **traditional mail**, use this address:

Technical Publications
Silicon Graphics, Inc.
2011 North Shoreline Boulevard, M/S 535
Mountain View, California 94043-1389

