SGI™ Internet Server Start Here

007–4261–002

CONTRIBUTORS

Written by Lori Johnson

Edited by Rick Thompson

Production by Susan Gorski

Engineering contributions by Bao Phac Do, Anietie Ekanem, Kirk Erickson, Rafael Seidl, Ken Trant

COPYRIGHT

© 2000 Silicon Graphics, Inc.; provided, copyright in certain portions may be held by third parties, as indicated elsewhere herein. All rights reserved.

LIMITED AND RESTRICTED RIGHTS LEGEND

The electronic (software) version of this document was developed at private expense; if acquired under an agreement with the USA government or any contractor thereto, it is acquired as "commercial computer software" subject to the provisions of its applicable license agreement, as specified in (a) 48 CFR 12.212 of the FAR; or, if acquired for Department of Defense units, (b) 48 CFR 227-7202 of the DoD FAR Supplement; or sections succeeding thereto. Contractor/manufacturer is Silicon Graphics, Inc., 1600 Amphitheatre Pkwy., Mountain View, CA 94043-1351.

TRADEMARKS

Silicon Graphics is a registered trademark and SGI and the SGI logo are trademarks of Silicon Graphics, Inc.

Adobe, Acrobat, and PostScript are registered trademarks of Adobe Systems Incorporated. Linux is a trademark of Linus Torvalds. Microsoft and Windows are trademarks of Microsoft Corporation. NFS is a trademark of Sun Microsystems, Inc. Tripwire is a trademark of the Purdue Research Foundation and is licensed exclusively to Tripwire, Inc.

Cover design by Sarah Bolles, Sarah Bolles Design, and Dany Galgani, SGI Technical Publications.

Record of Revision

Version	Description
001	February 2000 Original publication
002	April 2000 Corrections to the ISE 1.0 released version

Contents

Tables

About This Guide

This publication documents the SGI Internet Server for Linux.

Related Publications

The following contain related information:

- *SGI 1200-Family of Servers Quick Start Guide*
- *SGI 1200-Family of Servers Errata*
- *SGI 1200-Family of Servers User's Guide*
- *SGI Internet Server Administrator's Guide*
- *SGI ProPack 1.3 for Linux Start Here*
- SGI Linux Web site: `http://oss.sgi.com/projects/sgilinux`

Obtaining Publications

The *SGI Internet Server Administrator's Guide* (`ISE_AG`) and *SGI Internet Server Start Here* (`ISE_SH`) are found in the following locations on an installed system:

- HTML in:

  `/usr/doc/sgi/ise-`*Version*`/ISE_AG-`*Revision*`/html`
  `/usr/doc/sgi/ise-`*Version*`/ISE_SH-`*Revision*`/html`

- PDF in:

  `/usr/doc/sgi/ise-`*Version*`/ISE_AG-`*Revision*`/pdf`
  `/usr/doc/sgi/ace-`*Version*`/ISE_SH-`*Revision*`/pdf`

- Compressed PostScript in:

  `/usr/doc/sgi/ise-`*Version*`/ISE_AG-`*Revision*`/ps`
  `/usr/doc/sgi/ise-`*Version*`/ISE_SH-`*Revision*`/ps`

For example:

```
/usr/doc/sgi/ise-1.0/ISE_AG-001/html
```

Note: Documentation is available on the CD-ROM in `/mnt/cdrom`, rather than `/usr`.

To download a free copy of the Acrobat PDF reader, go to the `http://www.adobe.com/products/acrobat/readstep.html` Web site.

The *SGI 1200-Family of Servers Quick Start Guide* is not preinstalled, but is available in hardcopy and on the *SGI 1200-Family of Servers Hardware Documents CD*.

To obtain the latest SGI documentation, go to the SGI Technical Publications Library at `http://techpubs.sgi.com`.

Conventions

The following conventions are used throughout this document:

Convention	Meaning
`command`	This fixed-space font denotes literal items such as commands, files, routines, path names, signals, messages, and programming language structures.
variable	Italic typeface denotes variable entries and words or concepts being defined.
`user input`	This bold, fixed-space font denotes literal items that the user enters in interactive sessions. Output is shown in nonbold, fixed-space font.

[ ]	Brackets enclose optional portions of a command or directive line.
...	Ellipses indicate that a preceding element can be repeated.

Reader Comments

If you have comments about the technical accuracy, content, or organization of this document, please tell us. Be sure to include the title and document number of the manual with your comments. (Online, the document number is located in the front matter of the manual. In printed manuals, the document number can be found on the back cover.)

You can contact us in any of the following ways:

- Send e-mail to the following address:

  `techpubs@sgi.com`

- Use the Feedback option on the Technical Publications Library World Wide Web page:

  `http://techpubs.sgi.com`

- Contact your customer service representative and ask that an incident be filed in the SGI incident tracking system.

- Send mail to the following address:

  Technical Publications
  SGI
  1600 Amphitheatre Pkwy., M/S 535
  Mountain View, California 94043–1351

- Send a fax to the attention of “Technical Publications” at +1 650 932 0801.

We value your comments and will respond to them promptly.

Configuring the SGI Internet Server

Note: You should read through this document **first** before completing the steps in the *SGI 1200-Family of Servers Quick Start Guide.*

This chapter covers the following:

What Do I Need to Do?

The following is an **overview** of the tasks required to use your SGI Internet Server.

Note: Steps 8 and 10 below, Bastille Linux and Linuxconf HTTP access, are optional but recommended.

1. Unpack the hardware. Check for damage and completeness.
2. Read through this *SGI Internet Server Start Here* and the *SGI 1200-Family of Servers Quick Start Guide* to understand the hardware requirements.

   The *SGI 1200-Family of Servers Quick Start Guide* is not preinstalled, but is available in hardcopy and on the *SGI 1200-Family of Servers Hardware Documents CD*
3. Understand the vendor recommendations:
   - "Security Policies", page 3
   - "Network Port Use Security Policy", page 4

   Note: The port naming conventions applied by Linux for single-port FastEthernet PCI adapters (PCI 00010) are **not** what most users would expect. See *SGI 1200-Family of Servers Errata.*

   Dual-port FastEthernet PCI adapters (PCI 00011) have normal port naming conventions.

4. Install the hardware according to the directions in the *SGI 1200-Family of Servers Quick Start Guide*:
   - If you want to use a keyboard, video, and mouse during the preproduction phase, follow the directions in the *Quick Start*. Additional information is found in "Local Console Access", page 9, in this *Start Here.*
   - If you want to use a serial console, see "Serial Console Access", page 7.
5. Fill out the following worksheets:
   - "Password Worksheet", page 47
   - "Network Connectivity Worksheet", page 49
6. Power on the server and log in as `root` using the SGI factory password `sgisgi`.

   Note: You will be asked to change the password.

7. The system will boot to multiuser mode and Linuxconf will be automatically invoked. You will supply the information from "Network Connectivity Worksheet", page 49. For more information, see Chapter 3, "Configuring the Network", page 11.

   Note: You must enter all of the information for this step or the Bastille Linux step will fail.

8. Use the Bastille Linux hardening script to lock down the server. See Chapter 4, "Server Lockdown Using Bastille Linux", page 15. This step is optional but recommended.
9. Reboot the server.
10. Enable Linuxconf HTTP access. See Chapter 5, "Enabling HTTP Access for Linuxconf Administration", page 35. This step is optional but recommended for ease of use only if you restrict access to a private network port.
11. Connect serial consoles if not already done in step 4. See "Serial Console Access", page 7.
12. Log on using the serial console and the new `root` password.

13. Ensure that your server is accessible on the preproduction network (but not yet in production).
14. Point your browser to the SGI Internet Server Web administration graphical user interface (GUI) using the following URL, where *hostname* is the name of the server:

    `http://`*hostname*`/sgi-iserver/`

    Use user `iseadmin` and password `iseadmin`. For more information, see Chapter 6, "SGI Internet Server Web Administration GUI", page 45
15. Use the GUI to configure additional features, such as setting up E-mail accounts and using Tripwire intrusion detection software. For information about these tasks, see the *SGI Internet Server Administrator's Guide*.
16. Connect the server into your production environment.

Vendor Recommendations

This section contains information about hardware that is specific to ISE:

- "Security Policies"
- "Network Port Use Security Policy", page 4

Security Policies

You must know the corporate security policy for systems and applications. If you do not have a policy, you should consider establishing one. See "Network Port Use Security Policy", page 4.

You should establish a security policy that specifies how domain name service (DNS) names for secondary network interfaces are derived from the basic hostname. In particular, private network interfaces should be readily identified as such by a standard prefix or suffix.

The basic hostname should be associated with the public interface on which incoming requests are received. If you have multiple public interfaces, your network architecture may call for giving the default gateway interface a derived name.

Network Port Use Security Policy

To simplify the integration of new systems into your network architecture, you should do the following before plugging in any network cables:

- Establish a security policy that defines how port names should be mapped to untrusted (public) and trusted (private) networks.

  Apply the policy consistently when cabling up all of your servers — regardless of vendor — to your network equipment (this equipment is not included in the SGI Internet Server). Doing so greatly reduces the risk of accidental misconfiguration, including the opening up of security holes in your production environment.

- If you have only one interface, it will be named `eth0`. If your architecture calls for a private network, you should reserve the name `eth1` for that private network, irrespective of its physical location. Ports `eth0`, `eth2`, and so on, may be used for public networks.

  For a front-end server, the outbound traffic will typically be to an untrusted network like the Internet; therefore, you should use port `eth0` as your default gateway interface.

- If you must use `eth1` for a public interface, you should mark the exception clearly in the following places:

  – Affected name tag

  – `/etc/motd` file on that system

  – Diagrams of your production network operations center network architecture

  Alternatively, you can choose to purchase network adapters such that `eth1` need not be used at all. If the port physically exists but there are security reasons why it should not be used on that system, the port should be covered up with tape (not included).

Note: An SGI Internet Server that has a connection to a public network, or communicates with systems or applications that run on a public network, should implement an IP filtering tool to increase security. Therefore, you should run the Bastille Linux script when prompted.

You may also wish to lockdown other systems at your site using Bastille Linux. You can copy the Bastille Linux software from the ISE package or download the latest copy from the Bastille Web site. However, your license does not permit you to copy the entire ISE software package to a non SGI Internet Server.

Support

For SGI Linux support services, see `http://support.sgi.com/linux`.

General Product Feedback

For general feedback (not support) about the SGI Internet Server, see:

`http://www.sgi.com/cgi-bin/feedback/`

For marketing information, see:

`http://www.sgi.com/solutions/broadband/sgi_internet.html`

Setting Up Console Access

This chapter discusses the following:

Serial Console Access

This section discusses the following:

Requirements for Additional Hardware

Requirements for additional hardware (not included):

- A suitable serial cable (that is, a null modem cable) and connector type for attaching to `COM1` on the back of the 1200 box (DB9 female)
- One of the following:
  - A serial RS-232 console device
  - A workstation running terminal emulation software
  - A port on an already deployed serial concentrator or terminal server

Setting Up a Serial Console

To set up the serial console, do the following:

1. Connect one end of your serial cable to your SGI Internet Server on `COM1`.
2. Connect the other end directly to one of the following:
   a. A console device (such as a terminal).
   b. A free port on a terminal server you have already deployed. This may be based on cat-5 cabling and RJ-45 jacks, so you may need an RJ-45 to DB9 female adapter. The combination of all these elements should produce an RS-232 null modem connection.
3. Use your console device to gain shell access or use terminal emulator software running on a workstation (connected to your terminal server or serial concentrator equipment).

Note: By default, Linux does not allow `telnet` login for `root`. Therefore, there must be a regular user account already set up even if Bastille was not run.

For security purposes, you should deny access to the `telnet` daemon from all public networks, using both `ipchains`(8) and `tcp_wrappers` for redundancy. You will perform this step as part of using the Bastille Linux script. See Chapter 4, "Server Lockdown Using Bastille Linux", page 15.

Uses for a Serial Console

Using a serial console access for preproduction tasks has the following advantages:

- It allows you to place your server in your network operations center while still performing preproduction tasks
- You can move your server into production mode without recabling

You will also want a remote console during production mode. In a production environment, you would typically have multiple server systems and use either a serial concentrator or a serial terminal server to access them all from a workstation in your network operations center.

Local Console Access

This section discusses the following:

- "Requirements for Additional Hardware"
- "Setting Up a Local Console"
- "Uses for a Local Console", page 10

Requirements for Additional Hardware

Requirements for additional hardware (not included) are one of the following:

- Cabling and a free port on a keyboard, video, and mouse (KVM) switch already connected to an administration workstation

or:

- Standard set of hardware:
  - A generic multisync SVGA monitor and cabling
  - A standard PC PS/2 keyboard
  - A PS/2 mouse

Setting Up a Local Console

To set up the local console, do the following:

1. Plug the SVGA monitor into the video connector
2. Plug the standard PC PS/2 keyboard into the keyboard connector
3. Plug the PS/2 mouse into the mouse connector

For a diagram showing the SGI 1200 server rear connectors, see the *SGI 1200-Family of Servers Quick Start Guide*.

Uses for a Local Console

You may want to use local console access while you are setting up your server before placing it in production mode, especially if you are performing preproduction tasks in an area outside your network operations center. This method is simple, but may require you to physically move and recable your system later on.

Configuring the Network

Before you power up for the first time, you should you fill out the information required for the "Network Connectivity Worksheet", page 49.

Immediately after you power up for the first time, you will be asked if you want to run Linuxconf to set up your networking. You should answer `Yes`. The `curses`-based interface to Linuxconf will be invoked.

To use Linuxconf to enter the network connectivity information, do the following:

1. Press the `Tab` and `Enter` keys to quit out of the initial help screen.
2. Using the arrow keys and the `Enter` key, open the following tabs in succession:

   Config
   Networking
   Client tasks
   Basic host configuration

3. Enter in the appropriate information from your "Network Connectivity Worksheet", page 49.

   The following is an **example** for a system with two network interfaces, `eth0` and `eth1`. The latter will be used for private networking. The example shows user input in bold; when performing your own configuration, please remember to substitute your own names and IP addresses.

Note: If you have decided to mount and cable up the system in your production rack, ensure that no one can access `eth0` until you are ready to bring the system into full production. The safest ways to do that are as follows:

- Do not to plug in `eth0`
- Do not enable the interface at this time. You can enable `eth0` later on when you are ready for it.

```
+-------------------------------------------------+
|                      -------- Host Name -------- |
|Host Name             foo.bar.com                |
|                      -------- Adapter 1 -------- |
|                      [ ] Enabled                |
|Config mode           (o)Manual ( )Dhcp ( )Bootp |
|Primary name + domain foo-eth0.bar.com           |
|Aliases (opt)         www.yourcorp.com foo-pub   |
|IP address            1.2.3.4                    |
|Netmask (opt)         255.255.255.0              |
|Net device            eth0                       |
|Kernel module         eepro100                   |
|                      -------- Adapter 2 -------- |
|                      [X] Enabled                |
|Config mode           (o)Manual ( )Dhcp ( )Bootp |
|Primary name + domain foo-eth1.bar.com           |
|Aliases (opt)         foo-priv foo               |
|IP address            1.2.100.4                  |
|Netmask (opt)         255.255.255.0              |
|Net device            eth1                       |
|Kernel module         eepro100                   |
+-------------------------------------------------+
```

4. Press the `Tab` key to navigate to the `Accept` button and then press the `Enter` key.
5. Specify the plain host name (up to but not including the first ".") as an alias to your private interface `eth1`. This enables you to launch the Linuxconf HTTP interface directly from the SGI Internet Server Web administration graphical user interface (GUI).
6. Open the following tabs:

   Config
   Networking
   Client tasks
   Name server specification (DNS)

7. Enter in the server IP addresses from your "Network Connectivity Worksheet", page 49.

For example:

```
+-------------------------------------------------+
|DNS usage             [X] DNS is required ...    |
|Default domain                                   |
|Nameserver 1          1.2.3.254                  |
|Nameserver 2          1.2.10.254                 |
+-------------------------------------------------+
```

8. Accept your settings by pressing `Tab` to move to the **Accept** button and then pressing `Enter`.

9. Open the following tabs:

   Config
   Networking
   Client tasks
   Routing and gateways
   Defaults

10. Enter in the gateway IP address from your "Network Connectivity Worksheet", page 49. Do not enable routing; there is normally no reason for a front-end production system to route or forward packets.

    For example:

```
+-------------------------------------------------+
|Default gateway       1.2.3.1                    |
|Enable routing        [ ]                        |
+-------------------------------------------------+
```

Note: The default gateway device used by Linux is `eth0`, which is fine in this case.

However, if you have three or more interfaces, there might be circumstances in which you would want to designate a different physical network port to be the default gateway device. To do this, specify the appropriate value for `GATEWAYDEV` in the `/etc/sysconfig/network` file after you have shell access.

---

11. Accept your settings.
12. Quit Linuxconf by using the `Tab` key to navigate to the `Quit` button.

Server Lockdown Using Bastille Linux

Using Bastille Linux is optional but recommended. This chapter discusses the following:

Note: You must have access to the information listed in "Network Connectivity Worksheet", page 49.

What is Bastille Linux?

Bastille Linux is a product that will provide increased security for your SGI Internet Server. It is an open-source development effort to which SGI has contributed hardware , enhancements, and bugfixes. For the latest licensing, versioning, and security education information, see the official project Web site:

`http://www.bastille-linux.org`

This chapter provides additional documentation intended to make Bastille Linux easier to use as part of the deployment process of your SGI Internet Server.

The purpose of Bastille Linux is to make it harder for someone to gain unauthorized access and/or `root` privileges to your system. It provides an interactive universal hardening program intended to be run immediately after installing Red Hat software. Because your SGI Internet Server is preinstalled, you will be given the option to run it during your first boot-up.

When prompted to run the Bastille Linux hardening script, you should answer YES if you intend to put your system into production on an untrusted network such as the Internet.

Caution: Using Bastille Linux does **not** mean your system is impregnable; the only certain way to safeguard your system is to disconnect it from any network and put it behind a locked and guarded door. The point of using Bastille Linux is to make your network system so hard to break into that intruders will move on to easier systems.

Bastille Linux has verbose and nonverbose options, so it is useful for both security savvy administrators and those who are inexperienced. The extensive online help in the verbose mode makes it an excellent instructional tool for those wishing to learn more about how to secure a Linux operating system. In addition, most tasks are optional, providing the flexibility required to provide the security appropriate to your site.

Products Secured by Bastille Linux

Bastille provides secure operations for the following products (in alphabetical order):

- Account security
- Apache Web server configuration
- Berkeley Internet name domain (BIND) domain name service (DNS) server configuration
- Boot (physical) security
- File permission tightening / set user ID (SUID) audit
- File transfer protocol (FTP) server configuration
- Firewalling / network address translation
- `inetd`(8) and `tcpdchk`(8) configuration
- Linux loader (LILO) security module
- Logging
- Miscellaneous system daemon security
- Pluggable Authentication Modules (PAM) configuration
- Print server security

- `sendmail`(8) mail server configuration
- `ssh`(1) secure shell configuration

Bastille Linux Log Files

Bastille Linux keeps the following plain-text log files of each session:

- `/root/bastille-action-log`, a complete transcript of the session
- `/root/bastille-input-log`, a listing of all the answers given by the user
- `/root/bastille-error-log`, a record of any errors that may have occurred

It is important to prevent a unauthorized access to these files. They should be accessed only over a strongly encrypted channel, a private network, a serial connection, or a local console.

Bastille Linux Recommendations

The Bastille Linux script will ask you a series of questions. Each answer you give is immediately processed, with no opportunity to skip questions or revise the answers. Therefore, it is important that you know the following information prior to running the Bastille Linux script:

- Which interfaces are public and which (if any) are private.
- IP addresses associated with each interface.
- Which services should be available on each interface (everything else should **not** be available).
- For each network port, a list of specific ports for which the kernel should allow connections. Instead of port numbers, you may also list service names as they appear in `/etc/services`, or a combination of both. For example, `192.82.208.21:80` is the `HTTP` port for the `reality.sgi.com` Web site. In Bastille you could refer to either the port number (`80` in this case) or its popular name (`HTTP`), which can be found in the `/etc/services` file.
- IP addresses of primary DNS co-master and secondary DNS servers.

- IP address of the network time protocol (NTP) co-master (to keep system clocks synchronized).
- Hostname or IP address of a host for remote system logging (*syslogging*), if available. Ideally, this loghost should be accessible only on your private network. In a pinch, you can have production servers on a public network perform syslogging for each other.

Also see "What You Must Know Before Answering IPCHAINS Questions", page 19.

Note: A complete log of your session is kept in the `/root/bastille-action-log` file. This is useful if you have multiple servers.

How you answer the Bastille Linux questions depends upon your own situation. The rest of this chapter shows an example of the answers applicable to systems that are running a Web server or other front-end application on the Internet, and who are therefore at substantial risk of attack by hackers:

- The server to be locked down has one or more network interfaces. Zero or one of these are connected to a private subnet; all others are connected to public subnets. If a private subnet is to be used, the system acts as a secondary firewall (also known as a *firewall perforation*). It therefore must be configured with great care.
- The private network is either completely disjoint from all public subnets or else connected to one of them via a primary firewall.
- The server will be used as a web hosting platform, with content updates by means of FTP uploads, and a low number of E-mail accounts for use by the hosted customers.

The following subsections show the Bastille questions and the recommended answer (in bold). The reason for choosing the recommended answer follows the question when necessary; if no reason is given, the default reason is to plug a security hole.

IPCHAINS

One of the key components of Linux Bastille is the `IPCHAINS` module. This module helps you build a configuration file for the `ipchains`(8)tool,. This tool allows you to control the following at the IP packet level, based on the IP address and port number on each side of the connection:

- Those systems that can establish a connection to your server

- Those systems to which your server can connect

Packets are filtered based on any combination of the following:

- Source or destination IP address
- Network interface they arrived on
- IP protocol number
- Source or destination TCP/UDP port number

That is, IP filtering allows you to specify exactly what network connections are allowed by evaluating the following parameters:

source_machine_IP#:Port# - destination_machine_IP#:Port#

Supported IP protocols include TCP, UDP, and ICMP.

What You Must Know Before Answering IPCHAINS Questions

In order to correctly configure `IPCHAINS`, you must know the following:

- What systems should be allowed to connect to your server
- What protocols they will be allowed to use
- Who your system is allowed to connect to
- What protocol it is allowed to use

You can review the list of protocols by looking in the `/etc/services` file.

Structure of the `IPCHAINS` Configuration

The `IPCHAINS` configuration has the following chains:

- `INPUT` chain, which lists the systems that can connect to your server
- `OUTPUT` chain, which lists the systems to which your server is allowed to connect
- `FORWARDING` chain, which is used for firewall systems

Each part functions the same way but must be configured separately; if you have a server with multiple network interfaces, each interface must be configured independently as well. Unless you are configuring a firewall, you should not need to

configure forwarding other than to set the policy to DENY. SGI recommends that you use the DENY policy on all three chains.

The DENY policy has the following benefits:

- It returns no information or error codes to the remote system, giving them no help in cracking your system's security.
- If you didn't explicitly allow a packet, it is blocked.

Example of a Single Network

The following example is for a system with one network interface: eth0 is connected to a public network (that is, non-trusted).

Given that this is a web server, you would allow only the following protocols to connect:

- http on port 80
- https on port 443
- smtp on port 25

Although it is possible to allow access to port 98 over a public network, this is not recommended. Source IP addresses can potentially be spoofed (in which one machine on the network masquerades as another), and passwords transported over a public network in clear text can potentially be viewed by a hacker. See Chapter 5, "Enabling HTTP Access for Linuxconf Administration", page 35.

Even though you are blocking connections to your system, the packets (and the information contained in them) that are traveling to/from your system can still be viewed (snooped) by anyone with a system connected to your network. You must connect to your system for any number of reasons, such as to push content or to administer your server (such as with Linuxconf). Unless you use a tool that encrypts your communications (such as SSH or SSL), your data (such as passwords) can be stolen.

The INPUT chain on a single interface system must combine both eth0 and eth1 input chains from the example above. Because this is a web server, you should onlyallow smtp, http, and https connections from any host. You also want to enable the publishing server to connect (such as by means of ftp), and other protocols you want to allow, such as telnet.

For example:

Target	Interface	Source	Protocol	Port
Input	eth0:	ANY	tcp	http
Input	eth0:	ANY	tcp	https
Input	eth0:	ANY	tcp	smtp
Input	eth0:	192.82.208.21	tcp	linuxconf
Input	eth0:	163.154.38.32	tcp	telnet
Input	eth0:	163.154.38.32	tcp	ftp

The OUTPUT chain is as follows:

Target	Interface	Destination	Protocol	Port
Output	eth1:	*Domain_Name_Server*	udp	domain
Output	eth1:	*Remote_Log_Host*	tcp	syslog
Output	eth1:	*Remote_Backup_host*	tcp	*port_number*

Note: Once a rule is matched, it is acted on; therefore, the order of the rules in your chains can be important.

After you have a good configuration, you can use the following command to save it:

```
# /sbin/ipchains-save > myconfig
```

Bastille Linux will output the `/etc/rc.d/init.d/bastille-firewall` file. This file contains all the IPCHAINS configuration information that you input using the Bastille script. You can edit this file to reflect any future changes or use the following command (via a script) to load in your previously saved configuration:

```
# /sbin/ipchains-restore < myconfig
```

After you have completed the configuration, you can use the following command to review and modify your configuration:

```
# /sbin/ipchains -L -v
```

After you have completed running Bastille, you should review the configuration of IPCHAINS and test your configuration.

Following are the questions and recommended answers for this example.

1. Would you like us to install the ipchains script? (Y or N): **Y**

You will be asked to choose initial settings for the firewall script. The defaults are generally the minimal recommended settings. To accept the default (shown in brackets), press the RETURN key. To change a nonempty default to an empty value, enter some white space before pressing RETURN.

2. `Would you prefer more verbose instructions for each step? (Y or N): **Y**`

   If you are unfamiliar with IP filtering, or security issues in general, you will benefit from the verbose mode.

3. `Advanced networking options? (Y or N): **Y**`

4. `DNS_SERVERS ["0.0.0.0/0"]:` ***(Press the space bar to zero out the defaults)***

   If left empty, the contents of `/etc/resolv.conf` will be used.

5. `TRUSTED_IFACES ["lo"]: **lo**`

6. `PUBLIC_IFACES ["eth+ ppp+ slip+"]: **eth0**`

7. `INTERNAL_IFACES [""]:`

8. `TCP_AUDIT_SERVICES ["telnet ftp imap pop-3 finger sunrpc exec login linuxconf ssh"]: **telnet ftp imap pop-3 finger sunrpc exec login linuxconf ssh**`

9. `UDP_AUDIT_SERVICES ["31337"]: **31337**`

10. `ICMP_AUDIT_TYPES [""]:`

11. `TCP_PUBLIC_SERVICES [""]: **80 443 25**`

    This will allow anyone connecting from the public interface to connect to HTTP, HTTPS, and SENDMAIL ports.

12. `UDP_PUBLIC_SERVICES [""]:`

13. `TCP_INTERNAL_SERVICES [""]:`

14. `UDP_INTERNAL_SERVICES [""]:`

15. `FORCE_PASV_FTP ["N"]: **Y**`

16. `TCP_BLOCKED_SERVICES ["1024 2049 2065:2090 6000:6020 7100"]: **1024 2049 2065:2090 6000:6020 7100**`

17. UDP_BLOCKED_SERVICES ["1066 2049 6770"]: **1066 2049 6770**
18. ICMP_ALLOWED_TYPES ["destination-unreachable echo-reply time-exceeded"]: ***(Press the space bar to zero out the defaults)***
19. ENABLE_SRC_ADDR_VERIFY ["Y"]: **Y**
20. IP_MASQ_NETWORK [""]:
21. IP_MASQ_MODULES ["ftp raudio vdolive"]: ***(Press the space bar to zero out the defaults)***
22. REJECT_METHOD ["DENY"]: **DENY**
23. DHCP_IFACES [""]:
24. NTP_SERVERS [""]:

    If you are using NTP, you must enter the IP address(es) here.

25. ICMP_OUTBOUND_DISABLED_TYPES ["destination-unreachable time-exceeded"]: **destination-unreachable time-exceeded**

Example of Two Network Interfaces

The following example is for a system with two network interfaces:

- `eth0` is connected to a public network (that is, non-trusted)
- `eth1` is connected to a private network

Given that this is a web server, you would allow only the following protocols to connect on the public interface:

- `http` on port 80
- `https` on port 443
- `smtp` on port 25

The `INPUT` chain for the public interface would be as follows:

```
Target  Interface       Source          Protocol        Port
Input   eth0:           ANY             tcp             80
Input   eth0:           ANY             tcp             443
Input   eth0:           ANY             tcp             25
```

However, If you intend to allow your hosted customers to upload content by means of FTP, you must also open up ports 20 and 21 on the `INPUT` chain of your public interface. For POP3 and IMAP4 mail reader services, open up ports 110 and 143, respectively.

You would not enable any protocols on the `OUTPUT` configuration on the public interface. Any attempt to open a connection from your server to a remote server will fail. (Of course, if you had a business need that required you to open a connection to a server on the public network, you must configure it.)

On the private interface `INPUT` chain, you would allow the following protocols:

- `http` on port 80
- `https` on port 443
- `smtp` on port 25
- `telnet` on port 23
- `linuxconf` on port 98
- `ftp` on ports 20 and 21

You must also consider how you will be backing up this system, and what tools you will be using to publish content to your server. Even though this is the private interface (and supposedly safe), it is still a good idea to specify exactly what hosts can open a connection with your server. The `INPUT` chain is as follows:

```
Target  Interface       Source                Protocol        Port
Input   eth1:          ANY                   tcp             80
Input   eth1:          ANY                   tcp             443
Input   eth1:          ANY                   tcp             25
Input   eth1:          192.82.208.21         tcp             98
Input   eth1:          163.154.38.32         tcp             23
Input   eth1:          163.154.38.32         tcp             20
Input   eth1:          163.154.38.32         tcp             21
```

The above example specifies a single host that can connect to the server on port 98 (`Linuxconf`). Even though this is on the private interface, it is still a good idea to control access to this port because it is an administrative tool. SGI strongly recommends that you either apply the same access controls to port 98 as at the application level, or else do not allow any source IP addresses here.

You must also consider who your system can connect to. This is important because it can be used to prevent someone from exploiting a programming or application bug on your system and using it to open a connection out of your box to their system or using your system to attack other servers on your network. You should therefore use the DENY policy.

As a web server, you should have a very limited number of allowable OUTPUT connections, such as for DNS lookups or remote logging. If in your service architecture the DNS co-master is actually on the publi network, you must allow OUTPUT access to it on the public interface eth0 instead of eth1.

On your private interface, you must consider issues such as remote logging (syslog), which allows your server to write out its logs to a remote logging server, and what backup software you are using and how it runs. If your backup solution is designed to push content to the backup server, then your server must create a connection from itself to your backup server. In order to do that, your OUTPUT chain configuration must allow it, as follows:

Target	Interface	Destination	Protocol	Port
Output	eth1:	*Domain_Name_Server*	udp	domain
Output	eth1:	*Remote_Log_Host*	tcp	syslog
Output	eth1:	*Remote_Backup_host*	tcp	*port_number*

Following are the questions and recommended answers for this example.

1. Would you like us to install the ipchains script? (Y or N): **Y**

   You will be asked to choose initial settings for the firewall script. The defaults are generally the minimal recommended settings. To accept the default (shown in brackets), press the RETURN key. To change a nonempty default to an empty value, enter some white space before pressing RETURN.

2. Would you prefer more verbose instructions for each step? (Y or N): **Y**

   If you are unfamiliar with IP filtering, or security issues in general, you will benefit from the verbose mode.

3. Advanced networking options? (Y or N): **Y**

4. DNS_SERVERS ["0.0.0.0/0"]:***(Press the space bar to zero out the defaults)***

   If left empty, the contents of /etc/resolv.conf will be used.

5. TRUSTED_IFACES ["lo"]: **lo**
6. PUBLIC_IFACES ["eth+ ppp+ slip+"]: **eth0**
7. INTERNAL_IFACES [""]: **eth1**
8. TCP_AUDIT_SERVICES ["telnet ftp imap pop-3 finger sunrpc exec login linuxconf ssh"]: **telnet ftp imap pop-3 finger sunrpc exec login linuxconf ssh**
9. UDP_AUDIT_SERVICES ["31337"]: **31337**
10. ICMP_AUDIT_TYPES [""]:
11. TCP_PUBLIC_SERVICES [""]: **80 443 25**

    This will allow anyone connecting from the public interface to connect to HTTP, HTTPS, and SENDMAIL ports.

12. UDP_PUBLIC_SERVICES [""]:
13. TCP_INTERNAL_SERVICES [""]: **20 21 23 25 80 98 443**

    This will allow anyone connecting from the private interface to connect to FTP, FTP data, TELNET, SENDMAIL, HTTP, LINUXCONF, and HTTPS ports.

14. UDP_INTERNAL_SERVICES [""]:
15. FORCE_PASV_FTP ["N"]: **Y**
16. TCP_BLOCKED_SERVICES ["1024 2049 2065:2090 6000:6020 7100"]: **1024 2049 2065:2090 6000:6020 7100**
17. UDP_BLOCKED_SERVICES ["1066 2049 6770"]: **1066 2049 6770**
18. ICMP_ALLOWED_TYPES ["destination-unreachable echo-reply time-exceeded"]: ***(Press the space bar to zero out the defaults)***
19. ENABLE_SRC_ADDR_VERIFY ["Y"]: **Y**
20. IP_MASQ_NETWORK [""]:
21. IP_MASQ_MODULES ["ftp raudio vdolive"]: ***(Press the space bar to zero out the defaults)***
22. REJECT_METHOD ["DENY"]: **DENY**
23. DHCP_IFACES [""]:

24. `NTP_SERVERS [""]:`

    If you are using NTP, you must enter the IP address(es) here.

25. `ICMP_OUTBOUND_DISABLED_TYPES ["destination-unreachable time-exceeded"]:` **`destination-unreachable time-exceeded`**

For More Information about IPCHAINS

For a more detailed description of how `IPCHAINS` works, see :

`http://www.redhat.com/mirrors/LDP/HOWTO/IPCHAINS-HOWTO-4.html`

File Permissions

1. `Apply new file permissions?` **`YES`**

   It is important to ensure that your system is as secure as possible. If access is gained by intruders, you want to log as much as possible and limit their ability to fully compromise the system.

2. `Disable SUID status for mount/unmount?` **`YES`**
3. `Disable SUID status for ping?` **`YES`**
4. `Disable SUID status for dump and restore?` **`YES`**
5. `Disable SUID status of cardctl? (PCMCIA devices)` **`YES`**

   This is only relevant for laptop systems.

6. `May we remove SUID status form at?` **`YES`**
7. `May we remove SUID status from dosemu (dos emulation)` **`YES`**
8. `May we disable SUID status for inndstart and startinnfeed?` **`YES`**
9. `May we disable SUID status for the printing binaries?` **`YES`**

   A server on the Internet should not be a print server.

10. `May we disable the Berkeley r-tools?` **`YES`**
11. `May we disable SUID root on usrnetctl?` **`YES`**

12. Disable SUID status of traceroute? **YES**

Account Security

1. May we implement shadowing? **YES**

   Various processes running as nonprivileged users must read the /etc/passwd file for information other than passwords. Shadowing ensures the passwords are stored in the /etc/shadow file, which only the superuser may read.

2. May we create a second UID 0 account and apply monitoring on the original root account? **YES**

   There is no liability to doing this.

3. Please enter a name for the admin (UID0) account: ***password***

4. May we modify useradd to do so? (make a root-owned, nonwritable .rhosts file in each account) **YES**

5. May we enforce real password aging? (expire in 180 days) **YES**

   This is a good way to remind yourself to remain vigilant, and reduces the risk of attacks based on derelict accounts.

6. Please enter a name for your account? (ordinary user account) ***account_name***

   This should be done here rather than in linuxconf(8) because Bastille Linux will apply file and directory permission changes to each user later in the script. If you use linuxconf to create these accounts, they will not be secured appropriately.

7. May we restrict cron use to admins only, allowing you to add others one by one? **YES**

Boot Security

1. Should we do this? (password protect LILO) **YES**

   Applying a LILO passwd does not affect reboots (or reboot times) and will not stop a system from rebooting after a failure (such as power failures). The only time the password is required is if parameters are specified on the command line.

2. Please enter a LILO password: ***password***

3. Reduce the LILO delay to zero? (block entry at the LILO prompt) **YES**

   In a production server, you have no need for the option to boot off a test kernel.

4. Do you ever boot Linux from the hard drive? (is LILO on the hard drive)? **YES**

   In a production server, that is the default.

5. Do you want to apply our Linux Loader changes to a boot floppy? **YES**

   If you have approved a change here, you will be asked to insert a boot floppy disk as this point. The changes should be reflected in your boot floppy. If you are skeptical, create a backup copy of your original boot floppy before you proceed.

6. Now, type in the Linux name of the drive device, like so: (floppy drive address fd0 fd1) **fd0**

   The name of the built-in floppy drive.

7. Disable CTRL-ALT-DEL rebooting? **NO**

   The CTRL-ALT-DEL feature should only be disabled if physical access to the system is restricted (that is, someone cannot pull the plug). Using the CTRL-ALT-DEL feature allows the system to shut down cleanly.

8. Password protect single user mode? **YES**

   You must always know the root passwords to your production systems. If you forget one, you will lose access to that system unless you have set up .rhosts access from a secure system on the private network.

Secure inetd

1. May we modify inetd.conf and /etc/hosts.allow to optimize use of wrappers? **YES**

   tcpdchk(8) is a good tool for managing which hosts are given access to various services and for logging access events. It represents a redundant line of defense to the ipchains(8) configuration.

2. `Should we limit this to a particular set of IPs? (limit sshd to accept secure shell connections from only certain IP addresses)` **YES**

   To comply with US export restrictions on cryptography, the ISE product does not include the open source implementation of the `ssh`(1) secure shell package. However, if you are legally allowed to use encryption products in your country, SGI recommends that you obtain this drop-in replacement package for the insecure `rsh`(1) and `rcp`(1) commands.

3. `Enter a set of IP address or networks, delimited by spaces` ***address_or_networks***

   Specify a set of network operations center workstations, or the subnet they are on (which should be your most private).

   Note: The format for a C-class subnet is *x.y.z*.0, netmask 0.0.0.255. You should have multiple systems.

   ---

4. `Should we create "Authorized Use Only" banners for your site? Make default banner set?` **YES**

   Doing so makes it easier to prosecute an attacker and avoid being sued yourself.

Disable User Tools

1. `Disable the compiler?` **YES**

   You will still be able to use the compiler as superuser. You should consult your company's security policy document to verify that it is acceptable to have a compiler installed on a production system.

Configure Misc PAM

1. `Modify /etc/security/limits.conf to protect against certain DoS attacks?` **YES**
2. `Should we limit console logins to a small list of users?` **YES**

   Limit your exposure.

3. Please enter the names of the accounts that should be allowed to login, delimited by spaces. ***account_names***

Logging

1. May we add this additional logging? **YES**

   The additional level of detail will probably prove useful one day in troubleshooting a problem.

2. Do you have a remote logging host? **YES**

   The first thing successful attackers will do is attempt to cover their tracks by destroying the `syslog`. Ideally, the remote logging host will be on the private network, out of reach.

   If you answer YES, you must also answer the following question:

   Enter IP address of your remote logging host. ***IP_address***

3. May we configure process accounting? **YES**

   This will enable logging of resource consumption per process run.

Miscellaneous Daemons

1. May we deactivate apmd? **YES**

   APMD is only needed for laptops.

2. Deactivate NFS and samba? **YES**

   There is no reason to run either of these on a server that is connected to the Internet.

3. Disable atd? **YES**

   Use `cron`(8) instead.

4. May we disable pcmcia services? **YES**

   PCMCIA services are only needed for laptops.

5. May we deactivate DHCPD? **YES**

DHCPD is only needed if you intend to use this system for IP address management.

6. Deactivate GPM? (for text mode) **YES**

   However, answer NO if you are using KVM during staging or in production.

7. May we deactivate the news server daemon, innd? **YES**

   innd(8) is only needed if you intend to use this system as a news server.

8. May we deactivate the routing daemons? **YES**

   A production server connected to public and private networks should only route packets if it is a primary firewall.

9. Will you be using gated? **NO**

10. May we deactivate the NIS server and client programs? **YES**

    Use DNS instead.

11. May we deactivate SNMPD? **NO**

    If you followed the suggestions in the earlier sections on ipchains(8) configuration, this will already have been done for you.

sendmail

1. Leave sendmail running in daemon mode? **YES**

   You must provide this service if you are planning to offer Web hosting.

2. Run sendmail via cron? **NO**

3. May we disable these sendmail commands? (vrfy and expn) **YES**

DNS

1. May we confine the name server to a chroot'ed prison? **YES**

2. Deactivate named at least for now? **YES**

   Unless you want to actually provide DNS co-master service from this system.

Apache

1. `Deactivate the web server?` **NO**

   You must provide this service if you are planning to offer Web hosting.

2. `May we bind the web server to the local interface only?` **NO**

   The hosted Web servers must be accessible on the public interfaces.

3. `Bind to a particular interface only?` **NO**

   There is no harm in making a public Web server also accessible from a private network.

   a. `Please enter the IP address for apache to listen to (include the port)` ***IP_address_and_port***

      Use the IP address of the primary interface (incoming requests). Specify port 80.

4. `Deactivate following symbolic links?` **NO**

   You must allow this feature to compete in the Web hosting market.

5. `Deactivate SSI (Server Side Includes)?` **NO**

6. `Disable CGI script execution for now?` **NO**

7. `Disable indices? (disable automatic generated index file)` **YES**

Printing

1. `Deactivate lpr/lpd?` **YES**

   A system connected to the Internet should not be a print server.

FTP

The answers for FTP questions depend on the services you will be providing and other business requirements.

1. `Would you like to disable user privileges on the ftp deamon?` ***yes_or_no***

Providing this service to your Web hosting customers will allow them to manage their content.

2. `Disable anonymous download access?` ***yes_or_no***

   Enter `NO` if you want to use this system as a public FTP server to distribute files.

Completing the Lockdown

You will then be asked if it is OK to reboot the system now for the changes to take effect; you should answer **YES**.

See Chapter 5, "Enabling HTTP Access for Linuxconf Administration", page 35, for the next steps.

Enabling HTTP Access for Linuxconf Administration

This chapter tells you how to enable Linuxconf HTTP access on port 98 to a browser running locally or on a remote workstation. This step is optional but recommended.

You will use the Linuxconf utility to make system administration changes; documentation required for those changes is available online in the SGI Internet Server Web administration graphical user interface (GUI) and in the *SGI Internet Server Administrator's Guide.*

This chapter discusses the following:

Caution: The Linuxconf HTTP interface does not feature SSL encryption, which means that your `root` password could potentially be snooped by a hacker if you allow it to travel over any untrusted network.

If your system cannot be accessed through a private network, you should not use the Linuxconf HTTP interface. You can still use the Web administration GUI to access tutorial documentation and apply it to a separate Linuxconf session, conducted using your KVM access or over your serial console.

Managing Linuxconf HTTP Access Control

By default, only superusers on a system have Linuxconf execution privilege. The application has the following user interfaces:

- `curses`-based interface for use in a local shell or serial console
- Gnome GUI for use in an X Windows environment
- HTTP interface for use in a local or remote browser

Of these, only the first two are available by default. Before you activate the HTTP interface, do the following: in your `ipchains`(8) configuration, ensure that packets directed to port 98 on any of the public interfaces are quietly dropped. If you have followed the SGI recommendations for Bastille Linux, this will already have been done for you.

Local Console

If you have chosen to use a local console for the preproduction environment (as done in "Local Console Access", page 9), do the following:

1. Open a shell by clicking the Gnome footprint logo in the control panel at the bottom of your screen
2. Become superuser and execute the following command to launch the Gnome GUI interface in background mode:

   # **`/bin/linuxconf &`**

Remote Console

If you have chosen to use a remote console for the preproduction environment (as done in "Serial Console Access", page 7), do the following:

1. Open a shell over a private network or your serial console
2. Become superuser
3. Enter the following to launch Linuxconf:

   # **`/bin/linuxconf`**

Configuring Linuxconf for HTTP Access

Note: This section describes using the `curses`-based interface; if using the GUI, you will point and click instead.

1. Use your up and down arrow keys to reach the **Networking** tab. If it has a "+" next to it, press `Enter` to open it up.
2. Open up the **Misc** subtab in the same way. Navigate to the **Linuxconf network access** feature line and press `Enter`.
3. Enable option: press `Space` to allow all users with Linuxconf execution privileges access to the HTTP interface.
4. Log access option: press `Space` to ensure that all Linuxconf HTTP login attempts are logged.
5. Host or network option:

   Note: You must explicitly allow some specific access by filling in this field. If you leave it blank, the HTTP interface remains effectively disabled.

   Linuxconf gives you the following options:

   - To limit access to all hosts on your private network, specify the name of the associated network port (`eth1`).
   - If your network architecture has three tiers, you may instead specify the IP address of your most private subnet. For a typical C-class subnet, this address would take the form *x.x.x*.0. In this case, the netmask (see below) is required.
   - If you prefer, you may specify the hostname or IP address of a specific workstation in your network operations center. Make sure your server can resolve the hostname without having to consult a DNS server on a public network.

   Press `Enter` to move on to the next line.
6. Netmask (optional): if you have restricted access to the private network port, leave this blank. If you specified a C-class subnet, use the value 0.0.0.255. If you specified a host on a C-class subnet, the default value of 255.255.255.0 is fine.

7. Additional entries: if you specify more than one host/network+netmask combination, access will be allowed if any of them are met (that is, a logical `OR`). Mixing restriction types complicates the access control logic. Use this option to ensure that you have access from from multiple network operations center workstations.
8. Press `Tab` to proceed to the `Accept` button.

Note: If you have specified a restriction that cannot be verified when you press `Enter` at this point, it is possible that Linuxconf will hang. If this happens, press `Ctrl-C` to abort the session.

If you actually must apply such a restriction, reenter Linuxconf, provide values that are syntactically equivalent, and then correct them by hand in the `/etc/conf.linuxconf` file.

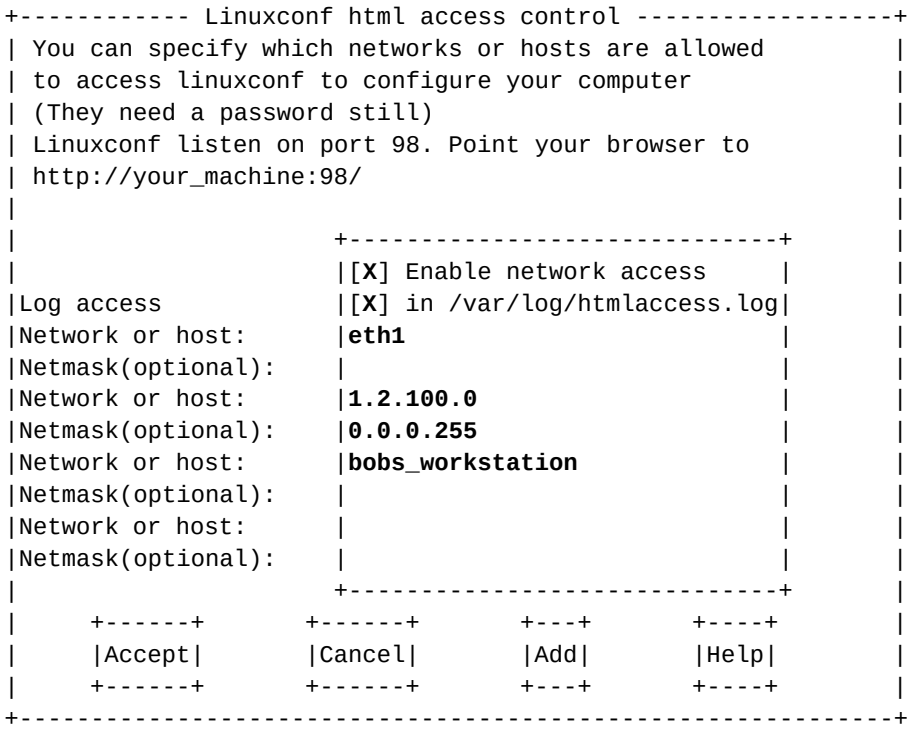
---

9. If you want to allow HTTP access for more than two network operations center workstations, press `Tab` again to reach the `Add` button, then press `Enter`.

The following example demonstrates all three mechanisms for allowing HTTP access to Linuxconf:

- Interface name
- Subnet
- Host

However, to keep things simple, SGI does not recommend actually mixing them. (User input is shown in bold.)



Activating Linuxconf HTTP Invocation Privileges

For security purposes, you should not run `linuxconf --http` from the command line (or from a script); you should launch it from `inetd` as described later in this section.

However, you can use the `inetd`(8) super-daemon to terminate the Linuxconf HTTP process after a configurable interval without activity.

Do the following:

1. Open up a shell as superuser.
2. Verify that the super-daemon is currently running:

   # **/bin/ps -fC inetd**

By default, it is launched at boot time by way of the symbolic link `S50inet` in `/etc/rc.d/rc3.d` or `/etc/rc.d/rc5.d` (depending on your `init` state).

3. Verify that the `/etc/services` file contains the appropriate Linuxconf information:

   # **/bin/grep linuxconf /etc/services**

   The output should read:

   ```
   linuxconf 98/tcp
   ```

   If it does not, edit `/etc/services` and append that line.

4. Verify that the `/etc/inetd.conf` file contains the appropriate Linuxconf information:

   # **/bin/grep linuxconf /etc/inetd.conf**

   By default, the output should read:

   ```
   #linuxconf stream tcp wait root /bin/linuxconf linuxconf --http
   ```

   Edit the file and remove the # character to uncomment the line so that `inetd` will spawn the Linuxconf HTTP interface in response to an incoming TCP request on port 98.

   If the line is missing, edit the `/etc/inetd.conf` file and append the line minus the # character.

5. If you had to make changes to either the `/etc/services` or `/etc/inetd.conf` files, execute the following command to ensure that the `inetd` process rereads its configuration files:

   # **/usr/bin/killall -HUP inetd**

If you want to test this, start a browser on any of the systems for which you earlier allowed Linuxconf HTTP access. Point it at the following URL:

`http://`*hostname*`:98/`

Replace *hostname* with the actual name you have associated with the private interface of your SGI Internet Server in your private DNS server.

Note: The trailing "/" in the URL is required in this case.

If you have a private network interface, and have previously restricted access to port 98 on that interface, the following applies: if you attempt to access the Linuxconf HTTP interface using a name or IP address associated with any of the public interfaces, your request will be quietly dropped by `ipchains`(8). Instead, use the name or IP address associated with your private interface. That interface name or one of its aliases should match the contents of the value of `HOSTNAME` in `/etc/sysconfig/network`, up to but not including the first dot. This is required to use the links from the Web administration GUI to the Linuxconf HTTP interface. See also Chapter 3, "Configuring the Network", page 11.

Managing Linuxconf User Privileges

If you created a second superuser account during the Bastille Linux procedure, that account will be identical to user `root` in every respect except for the account name and password. No further action is required to ensure this account has Linuxconf access.

Do not give any nonprivileged user execution for all Linuxconf features. However, you can choose to delegate selected tasks, such as post office protocol (POP) account management, to a user account.

Caution: By delegating selected tasks, you are providing not just execution permissions for certain sections but also read-only access to the rest of Linuxconf. Therefore, you should only exercise this option on behalf of individuals you trust. In a commercial environment, this should apply to every member of your operations staff.

For example, if you want to delegate POP account management, do the following:

1. Reenter Linuxconf as superuser.
2. In succession, open the tabs for the following:

   Users accounts
   Normal
   User accounts

3. Select the account to which you want to delegate POP account management.

4. Scroll down to the section marked `Privileges`. Grant the user access to Linuxconf, plus POP account management and/or Virtual POP account management.
5. Press `Accept` and `Quit`.

Note: Only superusers are allowed to invoke the `curses`-based interface from a shell due to execution permissions on the `/bin/linuxconf` binary. You should ask them to use the HTTP interface instead, provided you have enabled access to that.

Delegating Selected Linuxconf Privileges to Hosted Customers

In theory, the mechanism described above could be used to delegate tasks such as POP account management to hosted customers. This would alleviate the system administration overhead associated with your SGI Internet Server. However, SGI recommends against delegating any Linuxconf privileges to any hosted customers using either shared or dedicated hosting:

- With shared hosting, Linuxconf privileges are not granular enough for delegation to work as desired.

  Any customer to whom you delegate Linuxconf POP account management privileges would also be able manipulate the POP accounts of all other customers hosted on the same system. Some of them might be competitors. From a business perspective, this ought to represent an unacceptable risk to you.

- With dedicated hosting, you would either have to allow these customers access to a private network (such as through dial-in modems), or else open up Linuxconf HTTP access on a public interface.

You should use another mechanism to implement this type of delegation.

Because the current Linuxconf HTTP interface does not have transport encryption, allowing use by customers introduces the significant risk of having system passwords snooped by a hacker. In addition, you have no control over how carefully a hosted customer would protect any password that you provide.

Separately, if one of your own privileged system administrators were ever to succeed in accessing the Linuxconf HTTP interface by means of the public interface, the system root password could be exposed.

If you open up Linuxconf HTTP access on a public interface, and a hacker is able to obtain a password for a nonprivileged account, your system is instantly compromised. Regardless of whether the transport is encrypted, the hacker could simply access port 98 and perform malicious actions. This is an unacceptable risk.

SGI Internet Server Web Administration GUI

This chapter discusses the following:

- "Accessing the Web Administration GUI"
- "Changing the GUI Password"

Accessing the Web Administration GUI

You will use the SGI Internet Server Web administration graphical user interface (GUI) to configure additional features, such as setting up E-mail accounts and using Tripwire intrusion detection software.

To access the GUI, use the following URL, where *hostname* is the name of the server:

`http://`*hostname*`/sgi-iserver/`

Enter user `iseadmin` and password `iseadmin`.

For information about GUI tasks, see the *SGI Internet Server Administrator's Guide.*

Changing the GUI Password

For security reasons, you should change the Web administration GUI password. To do this, use the `htpasswd`(1) command to change the default `iseadmin` user account password, as follows:

```
$ htpasswd /usr/sgi/ise/lib/users iseadmin
New password: new_password
Re-type new password:new_password
$
```

Password Worksheet

This worksheet will help you keep a physical record of your account information. You should shred it after you are done with staging, archive it in a secure place, or elect not to record your passwords in plain text.

Note: The SGI factory preset password for the `root` account is: `sgisgi`

Table A-1 Password Worksheet

Status	User Name	Password
boot-up	`LILO`	
superuser	`root`	
superuser		
regular	`admin` (UID 0)	
regular		
regular		
regular		
regular		
regular		
regular		

Network Connectivity Worksheet

This worksheet will help you to configure your network using Linuxconf.

Note: The hostname and IP addresses are used in the server lockdown and should therefore reflect your production environment rather than your preproduction environment.

Table B-1 Network Connectivity Worksheet

Information Required		**Site-specific Information**
Hostnames:		
Domain names:		
Domain name servers:		
Time server:		
Default gateway IP address:		
Nameserver IP addresses		
	Primary:	
	Secondary:	
Public network		
	Interface	IP Address
	`eth0`	

Information Required		**Site-specific Information**
Private network		
	Interface	IP Address
	`eth1`	
Services accessible from public networks		
	Service	Port
	`http`	
	`ftp`	
	ssh	
Services accessible from private networks		
	Service	Port
	`http`	
	`ftp`	
	`ssh`	
	`telnet`	
IP address of DNS co-masters:		
	Primary:	
	Secondary:	

Information Required		**Site-specific Information**
Apache listening		
	IP address:	
	Port:	

Reinstalling from CD-ROM

For your convenience, the SGI Internet Server ships with all the required software already preinstalled on your system hard drive. However, in certain circumstances, it may be necessary for you to rebuild the system disk image using CD-ROMs.

Warning: The following covers a complete reinstall from scratch. Any data you already have on your system disk will be destroyed. If you are installing a RAID PCI card for the internal drives, all data already on the internal drives will be lost. It is up to you to back up data you cannot afford to lose before you continue.

At the end of this process, your system disk will be functionally equivalent to the state it was in when shipped from the factory. In particular, that means you will have to reassign the hostname, network address(es) and redo the Bastille server lockdown. You will also have to reapply all patches and custom configuration changes to the application(s) included, and reinstall any third-party application(s).

This chapter covers the following:

- "Rebooting the Server", page 58
- "Completing the Configuration", page 59

See the *SGI 1200-Family of Servers Quick Start Guide* and *SGI 1200-Family of Servers Errata* for additional information.

The procedures in this appendix assume that you are the superuser.

When to Reinstall from CD-ROM

You will want to reinstall from CD-ROM in the following circumstances:

- Installing in a country to which SGI may not ship a prebuilt system disk image due to United States export restrictions
- Installing a RAID PCI card for the internal drives
- Upgrading to a faster and/or larger hard drive
- Upgrading the operating system version (if approved by SGI)
- Upgrading the SGI ProPack overlay version (if approved by SGI)
- Customizing the partitioning scheme on your system disk
- Customizing the file systems on your system disk
- Recovering from a break-in
- Replacing a failed system hard drive

Note: The ISE software cannot be installed as a whole on a non-SGI system. Please consult the copyright notice enclosed with your Internet Server Environment CD-ROM if you are considering using this software for any purpose other than the SGI Internet Server.

Required CD-ROMs

To perform the reinstallation, you will need the following CD-ROMs:

- Red Hat 6.2 1/2 (the first of two CD-ROMs)
- SGI ProPack 1.3
- SGI ISE 1.0

The SGI factory basic I/O system (BIOS) settings on your SGI Internet Server allow you to boot your system off the CD-ROM drive. If you experience any problems, press F2 to enter **SETUP** mode during the boot process.

Inspect the **Boot Device Priority** in the **Boot** menu. The CD-ROM should appear higher up on the list than the hard disk. If in doubt, please contact SGI Customer Support.

Note: This may not work from a serial terminal emulator.

Preparing the Hardware

To prepare the hardware for reinstallation, do the following:

1. Shut down the system
2. Power off the system
3. Update your hardware configuration if applicable

Note: Some hardware components may require installation by an SGI support engineer, or your support contract may be void. If in doubt, please contact SGI Customer Support.

Installing the Linux Operating System

Do the following to install the Linux operating system:

1. If you are deploying an SGI RAID controller PCI card, follow the installation instructions shipped with it

2. Power the system back on
3. Immediately after power on, insert the Red Hat 6.2 CD 1/2
4. Select text mode for your installation by entering `text` and pressing the `Enter` key, as documented on the opening screen
5. Follow the directions for Red Hat installation in *Red Hat Linux 6.2 The Official Red Hat Linux Installation Guide*
6. Select the custom installation

The remainder of this section focuses on nonstandard configuration suggestions from SGI.

Partitioning the System Disk or RAID LUN

ISE uses the following partitioning scheme:

- `sda1`: 128 Mbyte Linux native file system, mount point `/boot`
- `sda5`: 128 Mbyte Linux swap
- `sda6`: 1 Mbyte + grow to disk, Linux native file system, mount point `/`

Ideally, the total amount of swap space should be at least equal to real main memory installed in your system; this will ensure that cores can always be completely dumped. If you care about core dumps, you should create additional swap space partitions before creating the final large partition.

On a production server, you generally want to avoid actual swapping to maintain nominal performance. However, the maximum size of a single block of real memory that the operating system will allocate is limited to the total amount of swap space available. For certain applications, you will want to increase the swap space allocation to 2-3 times the amount of real memory.

For more details, please see the following:

`http://metalab.unc.edu/mdw/HOWTO/mini/Partition.html`

`http://metalab.unc.edu/mdw/HOWTO/mini/Partition-3.html#ss3.2`

Selecting Partitions to Reformat

Reformat all partitions and check for bad blocks.

Selecting the Packages to Install

Select `Everything`, that is, all RPM packages.

Selecting a Mouse

The mouse port on the SGI 1200 system is PS/2 style.

Selecting a Time Zone

The clock on the SGI 1200 system implements GMT in hardware. Select the appropriate time zone if you want your time stamps in local time.

Selecting a Monitor

Select **Custom**. Specify the following:

- A resolution of 1024x768 noninterlaced at 8 bits color depth
- 1 Mbyte video RAM
- No special clock chip settings
- 40-150 Hz vertical refresh rate

For more information, see the *SGI 1200-Family of Servers Errata*.

Installing the SGI ProPack Overlay

To install the SGI ProPack overlay, do the following:

1. Insert the SGI ProPack 1.3 CD-ROM
2. Mount the CD-ROM by entering the following:

```
# /bin/mount /dev/cdrom /mnt/cdrom
```

3. Change to the `cdrom` directory:

   # **cd /mnt/cdrom**

4. Execute the `INSTALL` script:

   # **./INSTALL**

5. Select all RPMs

Installing SGI ISE

To install the SGI ISE software, do the following:

1. Insert the SGI ISE 1.0 CD-ROM
2. Mount the CD-ROM by entering the following:

   # **/bin/mount /dev/cdrom /mnt/cdrom**

3. Change to the `cdrom` directory:

   # **cd /mnt/cdrom**

4. Execute the `INSTALL` script:

   # **./INSTALL**

Activate Configuration and Bastille Linux Questions

To activate configuration and Bastille Linux questions upon reboot, enter the following:

touch /root/.SGICONF

Rebooting the Server

Enter the following to reboot the server:

reboot

Completing the Configuration

Follow the steps documented in the *SGI Internet Server Start Here* (this guide) and the *SGI Internet Server Administrator's Guide.*

Index

D

E

F

G

H

I

J