Adaptive Firewall

User Manual

Sun Microsystems, Inc.
555 Ellis street
Mountain View, CA 94043
www.cobalt.com

In the U.S.A.:
Phone (888) 70-COBALT
(650) 623-2500
Fax (650) 623-2501

Outside the U.S.A.:
Phone +1 (650) 623-2500
Fax +1 (650) 623-2501

Contents

1 Introduction 1

Using this Manual 1

Features of the Sun Cobalt Adaptive Firewall 2

Packet Firewall 2

Secure Remote Management 2

Access Logging and Monitoring 3

Authentication of IP Packets 3

Adaptive Firewall Requirements 3

Customer Service and Technical Support 4

General Cobalt information 4

Cobalt Technical Support and Service 4

2 General Network Security Concerns 5

Firewall Basics 7

What is a Firewall? (Scope and purpose of firewall) 7

Firewall design principles 7

Packet Filtering 8

Proxying 8

A Short Tutorial on Packet Filtering 8

3 The Sun Cobalt Adaptive Firewall 11

Server Components 12

pafserver 12

paflogd 12

thttpd-phoenix 12

pafnanny 12

e-conduit 13

Phoenix kernel Module 13

Firewall Policy File 13

Firewall Template File 13

User Components 15

Secure Management System (SMS) 15

The Adaptive Firewall Menu Bar Options 15

File 15

Firewall 16
Admin 17
Help 17

4 Adaptive Firewall Administration 19

Installation 19
Pre-Installation Issues 19
Obtaining & Installing Adaptive Firewall (standard method) 19
Obtaining & Installing Adaptive Firewall (manual method) 22
Starting the Secure Management System 23
Licensing the Adaptive Firewall 24
Obtaining and Installing a License Key 24
Adding an Upgrade Key 25
Transferring the Adaptive Firewall to Another Qube 3 26
Consequences of Installing the Adaptive Firewall 26
System Component Interaction 26
DHCP 27
Basic Firewall 27
User Interface 27
Resetting the SMS passphrase 29
LCD Panel Interface 30
Using the Adaptive Firewal Option 30
Backup and Restore of the Adaptive Firewall Configuration 32
Backing Up Your Adaptive Firewall Configuration 32
Restoring an Adaptive Firewall Configuration 33
Uninstalling the Adaptive Firewall 33
Upgrading the Adaptive Firewall 34

5 Configuring the Adaptive Firewall 35

The Secure Management System 35
Symbolic Addresses in Firewall Files 39
Host Addresses versus Network Addresses 40
Use of Wildcards 41
Creating the Initial Firewall 41
Protocol and Application Windows 41
Global Options 41

Common Internet Applications 43
Mail Services Options 46
Unix Applications 48
Multimedia 50
VPN 50
Network Management 51
Remote Management 53
Log 54
Custom Protocols 54
Configuring Custom Protocols 55

6 Troubleshooting 57

Common Problems 57
Debugging the Active Firewall 61
Understanding the Adaptive Firewall Log File 61

A Recommended Further Reading 63

B Manual Backup & Restore 65

Manual Backup 65
Manual Restore 65

C Glossary 67

Introduction

This user manual is for Qube 3 administrators who are implementing the Sun Cobalt Adaptive Firewall to increase the level of security of a Qube 3. The administrator should be familiar with networking, routing and internet security basics. Additionally they should be comfortable with the Cobalt administration interface and Netscape Navigator or Microsoft Internet Explorer Web browsers.

The manual assumes some familiarity with network security issues. Appendix A provides an overview of these issues and Appendix B includes suggestions for further reading concerning security topics.

Using this Manual

The chapters of this user guide are as follows.

Chapter 1 the present chapter, gives a brief introduction to the Adaptive Firewall as well as abstracts of the subsequent chapters.

Chapter 2 contains a broad overview of network security and basic firewall design philosophies. It also includes a short tutorial on packet filtering firewalls.

Chapter 3 describes the implementation of the firewall, discussing its components and their functions and interworking. These include the server components as well those that are accessed by the administrator via the Secure Management System (SMS) user interface.

Chapter 4 discusses pre-installation concerns and prerequisites, including instructions on the installation, removal and licensing of the firewall software on the Qube 3.

Chapter 5 provides detailed instructions for using the Secure Management System user interface to configure the firewall to meet the needs of the network and users. It also includes descriptions of the default protocols and applications that the Adaptive Firewall supports.

Chapter 6 describes how to troubleshoot potential or suspected problems with the Adaptive Firewall. It provides details about the collection of log and system data, tips on interpreting the data, and also points to other resources for getting help.

Appendix A provides a reading list where more in-depth discussions of firewalls and security can be obtained.

Appendix B describes how to perform manual backup and restore operations if these operations cannot be accomplished with a web browser.

Features of the Sun Cobalt Adaptive Firewall

The following features are described in this section:

- Packet Firewall
- Secure Remote Management
- Access Logging and Monitoring
- Authentication of IP Packets

Packet Firewall

Conventional static packet filtering is typically used to either limit traffic between specific source and destination network addresses, or to define specific applications that are allowed to traverse the network. Although static filtering has long been available in router and bridge products, the filtering rules used are placed in a specific order. This can leave significant vulnerabilities because the firewall rules are unable to adjust for unforeseen circumstances. The Adaptive Firewall solves this problem by adapting to the specific traffic on the network and can open, lock, and limit connections on an on-demand basis between authorized hosts for authorized applications.

Secure Remote Management

The Sun Cobalt Adaptive Firewall utilizes an administration user interface written in Java. Transactions between the Adaptive Firewall Secure Management System client and the Adaptive Firewall Server have been designed to be secure

from outside intervention. This means that, when properly configured, you can have control over your firewall from any location that has Internet access and a supported web browser[1]. Table 1 lists the supported browsers.

Table 1: Supported Web Browsers[a]

Operating System	Java enabled Web Browser
Windows 2000, NT, 98 & 95	Microsoft Internet Explorer 5.0, 5.5 Netscape 4.07 thru 4.75
Linux	Netscape 4.07 thru 4.75

a. Backup and Restore operations cannot be accomplished via Microsoft Internet Explorer..

Access Logging and Monitoring

While many networking devices provide logging facilities, the Adaptive Firewall not only tracks access attempts, it also provides real-time status information indicating both the inbound and outbound network traffic.

Authentication of IP Packets

When the corporate network is attached to public networks like the Internet, it is never reasonable to assume that every system accurately represents itself. A common cracker technique is to learn the network address of a trusted system inside a corporate network, and to then create packets that appear to be from the trusted host. The Adaptive Firewall can detect and prevent these types of attacks.

Adaptive Firewall Requirements

To use the Sun Cobalt Adaptive Firewall, you need:

- A Cobalt Qube 3 Internet server appliance
- Knowledge of the local area network that the Qube 3 is attached to. This includes the major TCP/IP parameters of that network: the Qube 3's assigned IP addresses and the associated network masks.

1. Some non-supported Java enabled browsers may work in limited or full capacity. Use non-supported browsers at your own risk. Supported browser and OS combinations have been tested and are known to function properly.

- Knowledge of what services (www, mail, etc.) the Qube 3 is providing to the Internet or network that it is attached to.

Customer Service and Technical Support

For further information on the Sun Cobalt Adaptive Firewall and other Cobalt products, visit the Cobalt website at `www.cobalt.com/support`. The site includes a Knowledge Base that customers can query as well as a list of Frequently Asked Questions (FAQs) that may provide additional help, insights or answers about the use and configuration of Cobalt products.

General Cobalt information

In the U.S.A., call (888) 70-COBALT or (888) 702-6225, or send email to info@cobalt.com.

Outside the U.S.A., call +1 650 623-2500, or send email to info@cobalt.com.

In Europe, call +31 70 517 6375, or send email to info-europe@cobalt.com.

In Japan, send email to info-japan@cobalt.com.

Cobalt Technical Support and Service

In the U.S.A., call (888) 70-COBALT or (888) 702-6225, or send email to support@cobalt.com.

Outside the U.S.A., call +1 650 623-2679, or send email to support@cobalt.com.

In Europe, send email to support-europe@cobalt.com.

In Japan, send email to support-japan@cobalt.com.

Updates and corrections for this User Manual can be found on the Sun Microsystems, Inc. Cobalt website at http://www.cobalt.com.

General Network Security Concerns

In order to take full advantage of the unique and powerful features of the Sun Cobalt Adaptive Firewall, the user must understand the importance of network security and the problems that a network administrator faces. Understanding these issues will help the user implement solutions to meet the security needs of the given network.

Note: *This is a brief introduction. We suggest you to do further reading on your own. A list of suggested sources is given in Appendix A*

In almost every case there is data on your Local Area Network (LAN) that is private or sensitive in some way. This might be a customer database, financial or medical information, etc. and it needs to be protected from those who would, by accident or intent, gain access to the data.

The first step in protecting this data is to compose a security policy that takes into account what data on your LAN ***should*** and ***should NOT*** be available to which users (both local and remote), and the ease with which they can gain that information. Who is allowed to administer the machines and network? Other components of a good security policy will also take into account the physical security and access of the network and machines on your LAN.

The world is full of people who will try to compromise your LAN, this is why a security policy is fundamental if your company is to have any level of interconnection with other networks or the Internet at large.

These people are broadly referred to as hackers and sometimes crackers. The latter term is generally applied to hackers who are malicious in nature and seek to do unsavory things to your LAN or networked hosts.

The various types of attackers can be generalized into the following groups:

1. Core or old-time hackers
2. Professional hackers
3. Intelligence/Counter Intelligence
4. Script Kiddies

The core group consists of people who hack at the kernel and machine levels and mainly do so in order to discover how things really work. Knowledge gained here can be used to refine or expand current computing technologies, or develop new ones. Many security holes are discovered and fixed at this level. Knowledge gained here is generally used for profit in developing new technologies and for making current products more secure.

The Professional hackers are individuals who make their living at discovering security problems for their clients. Some will also develop exploits of known security holes. It is at this level that the majority of the detailed programming work goes on. They are generally employed as security consultants being used to make a given company's network more secure.

The Intelligence/Counter Intelligence are professionals who have been employed to break into specific targets. They may be employed by individuals, small to large corporations, and governments. Their main task is to compromise networks or hosts and retrieve sensitive data that their employers have charged them with.

The last group is commonly referred to as script kiddies. This is likely to be the largest and least knowledgeable group of hackers. They use tools and scripts developed by more advanced groups of hackers to try to compromise networks for their own enjoyment. It is from this group that the majority of visible attacks are made. The attacks tend towards persistence and are generally easily observed.

There are several underlying reasons that will persuade people to hack a network or machine that is not their own:

1. To discover how things work
2. To retrieve specific information or data
3. Out of boredom, to gain glory or praise at being able to thwart someone else's security measures.

With these dangers in the world a security policy is mandatory.

Firewall Basics

What is a Firewall? (Scope and purpose of firewall)

A firewall, stated in the simplest terms, is a set of applications and hardware that are used to allow or deny traffic from networks outside the firewall host to networks or hosts inside the firewall.

The firewall host is designed to stand as your first line of defense between the Internet and your internal network or LAN. Its primary function is to act as a gatekeeper or guard that only allows System Administrator authorized traffic to reach your machines and thus keep any sensitive data from being seen by unwanted eyes. It may also be used to keep internal users from reaching the Internet or specified sites on the Internet at large.

The primary purpose of a firewall is to provide a singular check point into your network.

Firewall design principles

There are two basic philosophical models for firewalls, **permissive** and **restrictive**.

The permissive model states that all traffic will be passed through the firewall unless it is coming from sites that have been specifically blocked. This is an inherently dangerous method and should never be used as an exterior firewall. With this method there can be many unknown or unquantified and thus invisible security threats. As new security holes are found and used in different protocols this type of firewall becomes unmanageable. To be properly maintained, the system administrator would have to know of security holes as soon as they were discovered and then modify the firewall appropriately. In the real world this is an unrealistic expectation. It is a reasonable assumption that any given security hole will be known and exploited by a few hackers before the hole is known broadly enough that it can be patched or locked out via a firewall. Thus ,using this method as your primary defense is questionable at best.

The Adaptive Firewall is designed to operate under the restrictive philosophy of a firewall, namely: “That which is not expressly permitted is prohibited”. Or said another way, the only traffic that is allowed to pass through the firewall are those that the administrator explicitly configures. The reasoning here is that the given system administrator should know what applications and protocols are allowed to pass through the firewall. Tighter security is the natural result of using the

restrictive model. The policies that are developed in this manner are thoroughly defined and only allow traffic that the administrator knows should be coming in or out of the firewall.

There are two basic types of firewalls, packet filtering and proxying.

Packet Filtering

Packet filtering is the means by which traffic is checked and regulated when it attempts to pass through the firewall. If a given packet meets a defined set of parameters it will be passed or blocked as the policy dictates.

Proxying

Proxying is used when you want to hand traffic that is tied to a specific application such as email or web traffic to a specific host that is located behind the firewall.

NOTE: The Adaptive Firewall firewall only supports packet filtering

A Short Tutorial on Packet Filtering

The term “filtering”, when applied to networks, derives its origin from the similarity of a packet filter to a filter used in physical processes. In an aquarium, for instance, a continuous stream of water flows through a filter. There are sometimes contaminants in the water in the form of floating dirt and debris. The filter extracts those unwanted elements, allowing only the desired water to pass.

Packet filtering rules (instructions by which a packet filter operates) provide ways to control inbound and outbound packets. These rules operate outside the network protocols and are transparent to the user. Generally, the rules are generated by a filter because the filter acts as a gateway between networks, passing packets from LAN to LAN or between a LAN and an external network.

The packet filter’s rules implement the System Administrator’s policies for network traffic. The policies develop from one of these extremes:

A. That which is not expressly prohibited is permitted.

B. That which is not expressly permitted is prohibited.

Obviously, premise B is less permissive than premise A. It is more secure to block packets than to pass them if they don’t match a rule. And approach A requires constant attention. It requires advance planning to add rules when new services are added to the network if filtering is to successfully recognize every packet that should be blocked.

Whether the basic premise of one's security policy is to permit or prohibit access, packet filtering rules are invariably static rather than adaptive. That is, they are established before, rather than during, their execution. A static packet filter operates using premise A.

Adaptive Firewall Technology is superior to any type of packet filtering because it adapts rules based on information in the packets that pass through the firewall server. It monitors packets and their headers, looks for triggers, then edits prepared templates that temporarily allow network accessibility.

Adaptive Firewall Technology provides an alternative to traditional packet filtering.

Recognize information in the packet data as a special trigger. Use the trigger to generate a new set of rules to be inserted into the firewall process for some period of time.

Each step of the firewall can take one of five actions for each datagram in the "input" stream:

1. If the datagram matches the requirements of the current firewall rule, go on to the next step.

2. If the datagram doesn't match the requirements of the current firewall rule, skip ahead to a later point in the firewall.

3. Allow the datagram to pass and do no further processing on it.

4. Reject (discard) the datagram and do no further processing on it, except to optionally return an ICMP Unreachable message to the sender. Logging of rejected packets is optionally available.

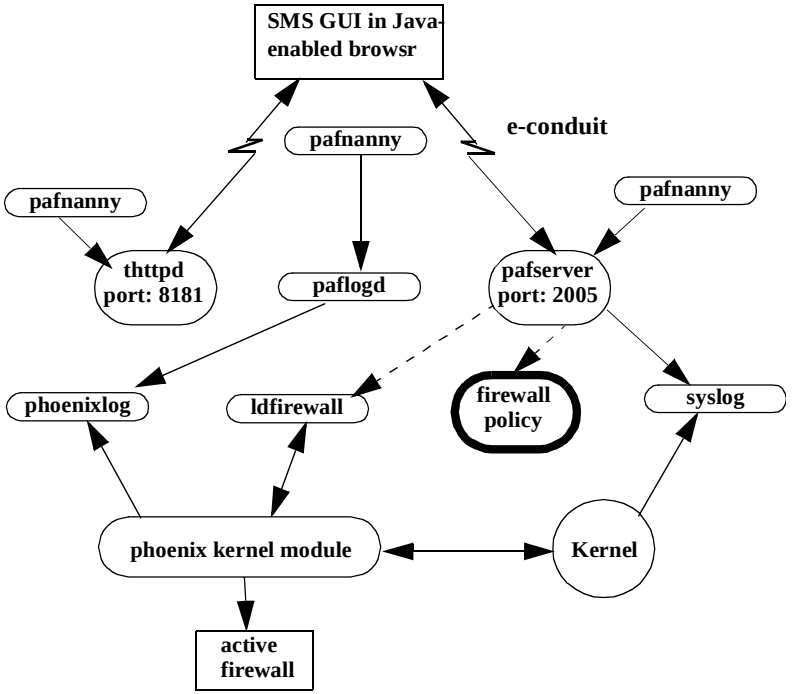
5. Recognize this datagram as a special triggering datagram. Instead of merely passing or blocking this triggering datagram from or into the output stream, generate a new set of firewall rules to be inserted into the firewall process for some period of time.

The first four options in the above list describe the functionality of a traditional static packet firewall. The fifth makes the Adaptive Firewall unique, because unlike conventional packet firewalls, the Adaptive Firewall uses a state-inspecting technology and can respond to its input stream with on-the-fly changes in the way it processes the datagram input stream.

The Sun Cobalt Adaptive Firewall can respond to a packet by setting up a limited session, specific to two endpoints, that would pass only specific application packets and do so for a specific time. The Adaptive Firewall, for the first time, allows users to maintain complete security over their data transmissions while maintaining the flexibility that modern businesses need in communicating over public networks like the Internet.

The Sun Cobalt Adaptive Firewall

The Sun Cobalt Adaptive Firewall is actually a group of programs that function interdependently in order to protect your network. The following figure illustrates each of the firewall components. The sections that follow provide a brief description of how they all fit and function together.



Server Components

Each of the server components is described in the sections that follow.

pafserver

This is the main server component and it responds to requests sent from the SMS interface. Using e-conduit to create an encrypted tunnel, the pafserver allows the Secure Management System to control the firewall remotely from a Java enabled web browser. By default, it listens on port 2005.

paflogd

Messages from the active firewall are logged to `/var/log/phoenix.log` via the `paflogd` component. When log files get too large, `paflogd` rotates them to make sure the host's hard drive does not fill up. Care is taken that the firewall keeps functioning correctly if `paflogd` can't keep up with the load. If the load does get too intensive, the kernel module will print a warning message in the file `/var/log/phoenix.log` to notify the user about any messages lost by the daemon. By default, all packets that are rejected by the firewall are logged.

thttpd-phoenix

The Adaptive Firewall includes a modified version of Jef Poskanzer's `thttpd`(C). The modified version has added the "-N" option to allow for interaction with the `pafnanny`. This is a specialized webserver that listens for connections from the Secure Management System. It listens for connections on port 8181. When a connection is seen the `pafserver` responds to the SMS via port 2005.

pafnanny

It is unlikely, but possible, that one of the `pafserver`, `paflogd` or `thttpd-phoenix` may crash. One instance of `pafnanny` is started for each process to be monitored. These three programs are needed for the SMS user interface to function. To ensure that all trhee programs are operating, `pafnanny` continually monitors those processes and if one crashes or quits unexpectedly it is restarted immediately. The active firewall will continue to function regardless of the state of the SMS components. If one segment of SMS were to crash, remote management of the firewall would not be possible.

e-conduit

The e-conduit layer provides a secure tunnel through which SMS communicates with the `pafserver`. Separate keys for encryption and authentication are generated to facilitate this interaction and they are generated in such a manner that none of the known secret tokens are used in the data stream. The tunnel is encrypted with a 56-bit DES with 90 bits of SHA1 authentication. Thus the e-conduit layer creates perfect forward secrecy with reasonably strong encryption and very strong authentication.

Phoenix kernel Module

This user-loadable module contains the actual firewall that is integrated into the operating system kernel when the system boots. It does not run as a separate program. After creating the active firewall, its task is to keep track of all the traffic going through the firewall system, and it decides whether this traffic is allowed to pass, depending on the rules defined in the firewall policy file.

Firewall Policy File

This file contains the firewall rules that are used to build the active firewall that is running in the phoenix kernel module. The file is generated based upon the selections made in the firewall template file in SMS. It is sometimes referred to as a firewall filter file.

Firewall Template File

This file defines the user configurable applications and protocols that the Sun Cobalt Adaptive Firewall recognizes. These supported applications are displayed in the left-most column of SMS. There are similar sets of parameters for most common applications that run over IP-based networks, such as the Internet. The firewall currently recognizes the following list of pre-defined applications. Details of each application and their uses are given later in Chapter 4.

- Cracking prevention, which provides protection against intrusion programs like `nmap` and the various port scanning packages, anti-spoofing, and lockout against source routing.
- A restricted site list. No communications will be allowed with the identified sites. Placing a site into this list will override any reference to that same site within a protocol or application specific selection.
- A trusted site list, allowing traffic to pass to another completely trusted site
- File Transfer Protocol (FTP)

- Telnet
- World Wide Web (mosaic, Netscape, gopher, WAIS)
- News (nntp)
- SMTP mail (Simple Mail Transfer Protocol)
- Pop mail (Post Office Protocol)
- IMAP Mail (Internet Mail Access Protocol)
- Domain Name Service (DNS)
- Dynamic Host configuration Protocol (DHCP)
- UUCP (UNIX to UNIX Copy)
- Whois
- Finger
- Talk/chat
- Archie
- UNIX Utilities “r” commands (rsh, rlogin, rcp)
- Multimedia
- Secure Shell
- X11
- Lan Manager (NetBIOS)
- Time Services (Network Time Protocol, or NTP)
- TFTP (Trivial File Transfer Protocol)
- IPsec (IP Security)
- PPP Tunnels
- Ident
- Routing information (RIP, OSPF, BGP, EGP)
- Syslog
- SNMP (Simple Network Management Protocol)
- Ping/Traceroute
- ICMP (Internet Control Message Protocol)
- Log

User Components

Secure Management System (SMS)

Firewall configuration is handled primarily through the Java-based graphical user interface. This section gives an overview of the available menu commands provided via that interface. Specific details on using SMS are discussed in Chapter 4.

The Adaptive Firewall Menu Bar Options

The menu bar at the top of the Sun Cobalt Adaptive Firewall window provides the options described in the paragraphs that follow.

File

The File option allows the user to create new firewalls, open existing firewall files, save a new or updated firewall definition to a file, save an edited firewall definition to a new file name, delete a firewall, backup or restore a configuration, or log off the Adaptive Firewall user interface

Table 2: File Menu

Menu Item	Key Sequence	Description
New Firewall	Ctrl+N	Create new firewall policy/file from blank template. Note: In keeping with the “restrictive” model of firewalls a blank template prohibits any traffic from traversing the interface on which it is installed.
Open Firewall file...	Ctrl+O	Open existing firewall policy/file
Save Firewall File...	Ctrl+S	Save currently loaded firewall file. If the current firewall is pre-existent, a backup copy of that original file will be saved under the original name with the suffix .bak.
Save Firewall File As...	No key sequence	Save currently loaded firewall file under a different name.
Delete Firewall File...	Ctrl+D	Delete firewall file.

Table 2: File Menu

Menu Item	Key Sequence	Description
Backup Configuration...	No key sequence	Backup the Adaptive Firewall configuration and policies to the machine running SMS.
Restore Configuration...	No key sequence	Restore the Adaptive Firewall configuration and policies from the machine running SMS.
Log off	Ctrl+Q	End firewall administration session and close GUI

Firewall

The Firewall option allows users to Save and Activate the Current Firewall, Activate and Deactivate Firewalls, Set and Remove the Startup Firewall and configure any custom protocols.

Table 3: Firewall Menu

Menu Item	Key Sequence	Description
System Status	No key sequence	Displays version information, currently active firewall(s), firewall(s) installed at system startup, and licensing information.
Save and Activate Current...	Ctrl+C	Save firewall file currently loaded in the GUI and install it on a particular network interface.
Activate Current Firewall...	Ctrl+F	Choose firewall file to install on a particular network interface.
Deactivate Active Firewall...	Ctrl+X	Uninstall current firewall file from a particular interface.
Set Startup Firewall...	Ctrl+T	Install chosen firewall file on to network interface at system startup time.
Remove Startup Firewall...	Ctrl+R	Unset installation of startup firewall file.
Custom Protocols...	No key sequence	Add rules for ports/protocols that are not included in the standard firewall template.

Admin

The Admin menu provides the user access to change the user interface passphrase, install/delete and confirm licensing information.

Table 4: Admin Menu

Menu Item	Key Sequence	Description
Change Passphrase...	None	Change passphrase used to login to the user interface.
Licenses		
Modify Firewall License	None	Display or add license file for Adaptive Firewall
Purchase License	None	Opens a new web browser directly to a page where licenses can be purchased.
Logging		
View Log	None	View firewall log in pop-up window.
Download Log	None	Download firewall log to text file.

Help

The **Help** menu provides the user with information about the version of the Adaptive Firewall client, server, and firewall, as well as the operating system it is currently running on.

Table 5: Help Menu

Menu Item	Key Sequence	Description
Documentation...	None	Opens a new web browser which leads to the Adaptive Firewall documentation.
About...	None	Opens a window that displays the version information for the Adaptive Firewall.

Adaptive Firewall Administration

This chapter discusses how to install, upgrade and remove the Sun Cobalt Adaptive Firewall software. Details on the administration and licensing of the Adaptive Firewall are also described. Additionally the major effects of having the Adaptive Firewall installed on a Qube 3 are also explained.

Installation

The Adaptive Firewall is delivered as a standard Cobalt PKG and the installation is quite straightforward. The configuration of the firewall policy for an installation requires careful thought, however. Take the time to think through your security needs before installing a policy. For pointers on where to start, consult , “General Network Security Concerns,” on page 5.

Pre-Installation Issues

Sun Cobalt Adaptive Firewall has been designed as add-on software for the Cobalt Qube 3. It is currently not available for other Cobalt Server platforms.

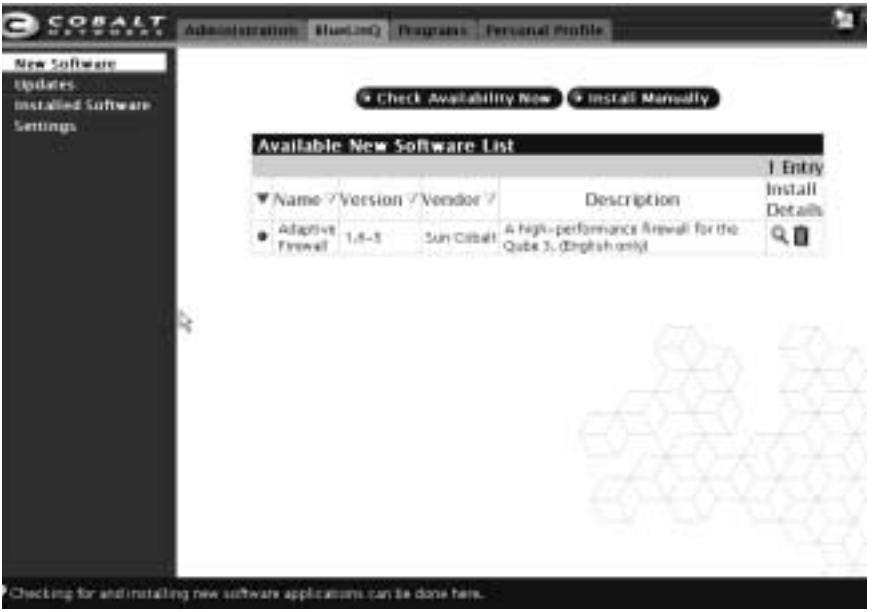
Obtaining and Installing the Adaptive Firewall (standard method)

In most cases the installation of the Adaptive Firewall pkg follows the default method of adding any additional/3rd party software to your Qube 3. These steps are as follows:

1. Login to the Qube 3 via the administrator website.

2. From the top menu click on the **BlueLinQ** menu tab.

3. Click **New Software** from the menu on the left.
4. Click **Check Availability Now** from the menu at the top of the screen.



5. Click **Install Details** for the Adaptive Firewall package.

6. Click **Install** to automatically install the Adaptive Firewall pkg on the Qube 3.

7. You will now see information about obtaining licensing for the Adaptive Firewall. Click **Accept** to finish the installation or **Decline** to abort.

Note: *Once the the Adaptive Firewall pkg has been successfully installed the browser will refresh and the Adaptive Firewall will appear under the Network Services menu.*

Obtaining and Installing the Adaptive Firewall (manual method)

1. In some instances you may be instructed to download the Adaptive Firewall pkg from a site other than the common Cobalt distribution site. After you have downloaded the appropriate pkg follow the instructions below.

Note: *The pkg must be located on the host that is running the administration UI.*

2. Login to the Qube 3 via the administrator website.
3. From the top menu click on the **BlueLinQ** menu tab.
4. Next click **New Software** from the menu at the left.

5. Click **Manual Install** from the menu at the top of the screen.

6. Click the **Upload** button.
7. Click **Browse** to locate the package that you downloaded to your computer. Once found, click **Open** to select the package.
8. Click **Prepare** to examine the pkg. This will give you a chance to review the function of the software.
9. Click **Install** to automatically install the Adaptive Firewall pkg on the Qube 3.

Note: *Once the Adaptive Firewall pkg has been sucessfully installed the browser will refresh and the Adaptive Firewall will appear under the Network Services menu.*

Starting the Secure Management System

There are two ways to start SMS. You can login to the Qube's standard admin user interface and then select Adaptive Firewall from the Network Services menu. This will load a page shown in Figure 2 that gives a brief description of the Adaptive Firewall and a Start Adaptive Firewall button. Clicking that button will start SMS and display the screen shown in Figure 1

Figure 1. Adaptive Firewall Start Page

You may also access SMS directly by pointing it to `http://myhostname:8181` where “myhostname” is the hostname of the machine running the firewall[2].

Once this has been done you will be able to configure the parameters for the active firewall.

Licensing the Adaptive Firewall

Use of the Adaptive Firewall is governed by means of a license key. This key not only enables the software to be used but it also dictates the number of user transactions that can occur. A user transaction is defined by an IP address and the number of concurrent tcp connections that are in use by that particular IP.

There are two types of keys: base and upgrade. The base key is the primary license and must be present for the Adaptive Firewall to operate. Upgrade keys are available for adding additional users.

Obtaining and Installing a License Key

License keys can be obtained on-line using the following procedure:

2. You can use the IP address of the firewall host instead of the hostname if desired.

1. When you start the SMS user interface, it looks to see if there is a license installed. If it doesn't find one, then it displays a dialog box that asks if you want to open a new browser window to https://licenses.cobalt.com.
2. When you get to that URL, you must specify what kind of license you would like to purchase. The MAC address of eth0 will already be filled in for you in the appropriate field.
3. After your purchase has been approved, a confirmation page is displayed that will contain your license key (you will also receive a copy via e-mail).
4. Copy the license key from this page.
5. In the SMS GUI, go to the **Admin** menu and select the **Licenses** item.
6. Under **Licenses** select **Modify Firewall License**. A new window with a dialogue box will appear.
7. Paste the license from the confirmation page into the dialogue box. You must paste every line from "Product:" through "=== END LICENSE ===".
8. Click the **Confirm** button. Your license has now been installed.

Adding an Upgrade Key

This process is essentially the same as adding a base key except that there is an extra line in this license that denotes it as an upgrade. The Adaptive Firewall must have a base key to operate: the software will not run if an upgrade key is installed but a base key is not already installed.

Follow these steps to upgrade a license key:

1. In the SMS user interface, go to the **Admin** menu and select the **Licenses** item.
2. Under **Licenses** select **Purchase License**. A new window is started that sends you to https://licenses.cobalt.com. Follow the steps 2 through 8 in the preceding section..

Caution: Once a license has been added or modified you must reactivate any currently active firewalls. The new license will not be utilized until this occurs. You should also do a backup, so that there is a backup copy of the new license.

Transferring the Adaptive Firewall to Another Qube 3

The license keys that allow the Adaptive Firewall to activate a policy are tied to the hardware of the given Qube 3. Specifically, they are based on the hardware address of the primary ethernet interface (eth0).

Caution: **You must contact support in order to transfer your old license key to the new host. Without a valid license you cannot activate any firewall policies.**

If it becomes necessary to transfer the Adaptive Firewall installation to another host, simply backup your current configuration and then download the Adaptive Firewall pkg from BlueLinQ and install it on the new hardware. See “Backup and Restore of the Adaptive Firewall Configuration” on page 32. Once this is done restore your configuration to the new Qube. After restoring your configuration, you will need to erase the original license and add your new license key. If you install your new license key before doing the restore, the new key will get overwritten with the old key and you will have to reinstall the new key.

Consequences of Installing the Adaptive Firewall

Installing the Adaptive Firewall on to your Qube 3 adds an additional layer of security. Once configured, traffic to and from the Qube 3 will be tightly controlled. If there are errors in the configuration of your security policy, some or all traffic may not be transmitted in the manner that you may be expecting. It is possible to configure a policy that will not allow any traffic to pass through the Qube. Be sure that you have thoroughly familiarized yourself with the Adaptive Firewall before using it in a production environment.

The following sections discuss the changes that will be most readily seen by the Administrator. Chapter 3 discusses the component pieces of software that comprise the Adaptive Firewall.

Chapter 4 details the configuration of the Adaptive Firewall and the building of a security policy.

System Component Interaction

The section that follows describes the interaction between the primary Adaptive Firewall components and the base components built into the Qube 3.

DHCP

DHCP can be used to set the IP address of the interface. However the Adaptive Firewall will **not** dynamically re-assign IP addresses within the firewall policy. You must use the wildcard character (*) to specify all local addresses within the configuration of the firewall policy in order to ensure an enforceable policy when DHCP is used.

Basic Firewall

The Adaptive Firewall can be run alone or in conjunction with the basic IP Chains based firewall. Unlike IP Chains, the Adaptive Firewall will dynamically toggle the open/closed status of various ports dependent upon usage and the configuration of the firewall policy. If the Adaptive Firewall has been installed and is enforcing a policy the Basic Firewall is redundant.

Any active Adaptive Firewall policy will examine all packets before the Basic Firewall. This is true for all traffic, inbound or outbound. If there is also a Basic Firewall installed then it must be configured to allow the same traffic that the Adaptive Firewall is configured to allow. Otherwise traffic that is passed by the Adaptive Firewall would be blocked by the Basic Firewall.

It is highly recommended that the Adaptive Firewall be run alone. This will keep potentially confusing cross-firewall mis-configuration issues from occurring.

Note: *Unless you are running web caching, which requires IPChains, the Adaptive Firewall should be used as the sole firewall.*

User Interface

After the Adaptive Firewall installation is complete, a new menu item, **Adaptive Firewall** will appear under the **Network Services** menu of the **Administration Screen** in the user interface. When clicked, this will display a short description of the Adaptive Firewall and a button that can launch the Adaptive Firewall user interface, the Secure Management System (SMS). The SMS is used to create and modify the security policy that will be invoked as the active firewall. The first time you log into SMS, a blank policy will be loaded. After configuring this you will need to save it. In subsequent uses of SMS, the policy that was most recently edited will load automatically.

Figure 2. Adaptive Firewall Start Page

Clicking the Configure Adaptive Firewall button will start SMS in a JAVA window and present the SMS login screen requiring you to enter your password. **Use the randomly generated initial license passphrase that has been emailed to the Qube administrator account**.

If this the first time you have logged into SMS you will see a notice about not having a valid license and you will be required to change the initial, random passphrase. This will also occur if the passphrase has been reset manually.

To change the passphrase you must re-enter the initial passphrase once and the new one twice.

.

Details on the Menu functions of SMS can be found in the section “The Adaptive Firewall Menu Bar Options” on page 15. Instructions on the use of SMS are in the section “The Secure Management System” on page 35.

Resetting the SMS passphrase

If necessary, the SMS passphrase can be reset via the **Admin** menu in the SMS user interface. It can also be changed from the LCD panel as described in the next section.

Note: *To insure security integrity, you will be required to change the passphrase the next time you login to SMS.*

LCD Panel Interface

After the Adaptive Firewall software is installed, the LCD panel interface will have one new option, **Adaptive Firewal**. This is used to remove any active firewall policy in the case that:

1. You have accidently firewalled yourself out of the Qube 3 via misconfiguration of a firewall policy.
2. You want to test the current policy and see what is being blocked.

To reinstate the firewall policy you will need to use the **Activate Firewall** from the **Firewall** menu of the SMS user interface.

The new **Adaptive Firewal** option also lets you reset the passphrase.

Using the Adaptive Firewal Option

You can reset the Adaptive Firewall policy settings including the passphrase by using the following procedure:

1. Hold in the **S** key until the LCD displays:

   ```
   SELECT:
   SETUP NETWORK
   ```

2. Press the **S** key repeatedtly until you see:

   ```
   SELECT:
   ADAPTIVE FIREWAL
   ```

3. Then press the **E** key. The `ADAPTIVE FIREWAL` option actually has two submenus within it: `DROP FIREWALLS` and `RESET PASSPHRASE.` The LCD first displays the message:

   ```
   SELECT:
   DROP FIREWALLS
   ```

   If you press the **E** key, you will a message asking you to confirm or reject the dropping of the firewall.

   ```
   DROP FIREWALLS
     [Y]ES  [N]O
   ```

   By default the cursor will have "**No**" selected. To proceed with the reset, use the left arrow or **S** button to select "**Yes**" and then press **E**.

   If you enter a "yes" reply, any active firewall policy will be removed from all interfaces and the Adaptive Firewall will not be filtering the traffic from any interface.

   ```
   DROPPING FIREWALLS
   ```

If you enter a “no” reply the LCD will return to displaying the hostname and IP address of the Qube 3’s primary ethernet interface.

Caution: When the Adaptive Firewall is reset there is no active firewall policy in effect and all traffic from the network will be passed through the Qube 3. Any desired firewall policy must be reactivated from SMS.

4. If, when the LCD displayed the message:

```
SELECT:
DROP FIREWALLS
```

You press the **S** key, the second choice within the `ADAPTIVE FIREWAL` opton is displayed:

```
SELECT:
RESET PASSPHRASE
```

If you press the **E** key, you will a message asking you to confirm or reject the resetting of the firewall.

```
RESET PASSPHRASE?
  [Y]ES  [N]O
```

By default the cursor will have “**No**” selected. To proceed with the reset, use the left arrow or **S** button to select “**Yes**” and then press **E**.

If you enter a “yes” reply, you will see the message:

```
RESETTING PASSPHRASE
```

IFollowed by the message:

```
NEW PASSPHRASE
XXXX YYYY ZZZZ
```

The new passphrase is three four-letter words separated by spaces. All 14 characters (including the spaces) are part of the passphrase. The next time you login to the SMS interface, you will be asked to change the passphrase.

If you enter a “no” reply the LCD will return to displaying the hostname and IP address of the Qube 3’s primary ethernet interface

Backup and Restore of the Adaptive Firewall Configuration

The backup process can only be executed from a Java enabled Netscape browser (version 4.0.7 or higher). The process will create a backup file on the host where the browser is running.

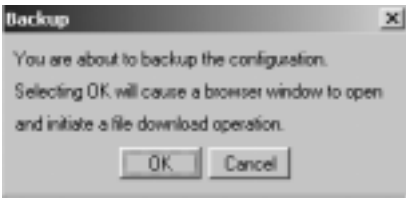
Backing Up Your Adaptive Firewall Configuration

1. Connect to the Qube 3 by using one of the SMS mechanisms described in “Starting the Secure Management System” on page 23.

   Caution: Microsoft Explorer CANNOT be used for this backup procedure.

2. From the "File" menu, select "Backup Configuration...". A popup window will ask you to confirm the backup:

3. The new browser window will prompt you for the location to which you would like to save the backup file. By default, this file will be named "backup.cgi". It is recommended that this file be renamed using a scheme that includes the date of the backup. Additionally if you have more than one Qube 3 you may want to include the hostname or IP address of the unit within the file name. This lets you more easily determine what backup files belong to which machines and when they were backed up. Such a file name might look like this: dorothy.092400.backup.

   The resultant backup file is saved to the host on which SMS is running. It is saved to the location that you specified earlier in this step.

   The following information is included in the backup file:

   - All firewall and startup firewall filter files/policies.
   - Any Adaptive Firewall licenses.

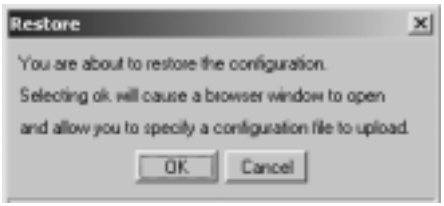
Restoring an Adaptive Firewall Configuration

The restore process can only be executed from a Java enabled Netscape browser (version 4.0.7 or higher) and must be done from a machine that contains a previously saved backup tar file.

1. Connect to the Qube 3 by using one of the SMS mechanisms described in “Starting the Secure Management System” on page 23.

Note: Microsoft Explorer CANNOT be used for this restore procedure.

2. From the "File" menu, select "Restore Configuration...". A popup window will ask you to locate the backup file::



3. When the restore has completed, your license file and any firewall policy files will have been placed in their respective locations as follows:
   - All firewall policies will be restored.
   - Any startup firewall policies will be restored.
   - All Adaptive Firewall licenses will be restored.
4. After a restore you must manually reactivate any given firewall policy. If a startup policy has been selected you may also reboot the Qube 3. In most cases a manual reactivation from SMS can be used.

Uninstalling the Adaptive Firewall

To remove the Adaptive Firewall software from your Qube 3, follow these steps:

1. Login to the Qube 3 via the administrator website.
2. From the top menu click on the **BlueLinQ** menu tab
3. Click **Installed Software** from the left hand menu.

4. Locate the entry for Adaptive Firewall and click the **Uninstall icon** found at the far right of that line.

Note: *After the Adaptive Firewall pkg has successfully uninstalled, the admin session will be automatically refreshed. This will remove the Adaptive Firewall option from the Network Services menu. The* `/etc/phoenix` *directory and all of its subdirectories are* <u>not</u> *deleted from the Qube 3 after the uninstall is completed.*

Upgrading the Adaptive Firewall

To upgrade your Adaptive Firewall installation, follow the instructions below.

1. Make a backup of your current configuration.
2. Go to the BlueLinQ site and install the latest release of the Adaptive Firewall. If you wish you can simply download the pkg and follow the instructions for manual installation.

Configuring the Adaptive Firewall

This chapter details the use of the Secure Management System (SMS) user interface to configure the Adapative Firewall.

For instructions on logging into SMS See “Starting the Secure Management System” on page 23.

The Secure Management System

The initial SMS user interface screen is shown in Figure 3. The top of the SMS window contains the menu bar with the items: File, Firewall, Admin and Help. Under the menus is a column on the left that lists the application sets that are listed in the filter template. To the right of the column is a splash screen that contains contact information for Sun Microsystems Inc.

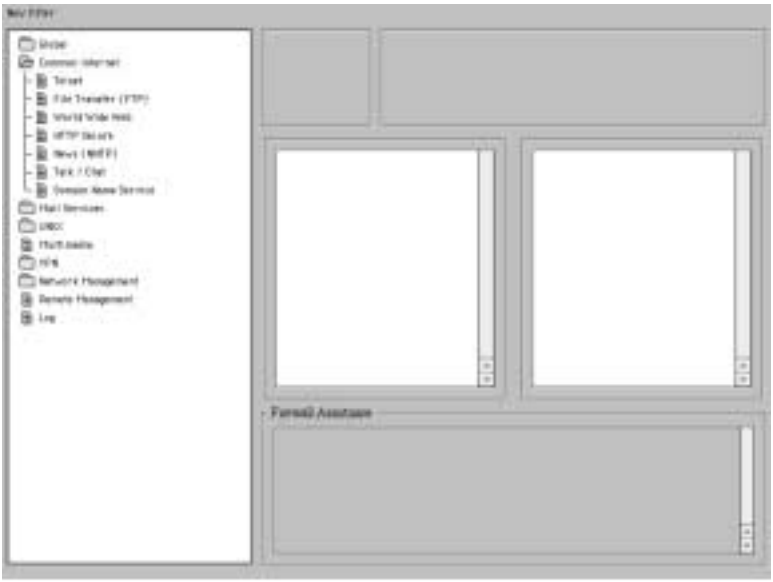
Figure 3. The Initial SMS Screen

Double click on the folder named “Common Internet”.

Note: *Some browser OS combinations may have problems using mouse clicks to expand folders. Highlighting the folder and pressing return will expand the folder. Also note that you can use the arrow keys on your keyboard to move between folders*

The folder expands to list the available applications and protocols that are defined in the filter template. The splash screen has been replaced by three rows containing additional windows as shown in Figure 4: two in the top row, two input fields (with scrollbars) in the second row and a single window in the bottom row that is marked “Firewall Assistance”. Collectively these comprise the Application/Protocol Configuration Area.

Figure 4. Application/Protocol Configuration Screen



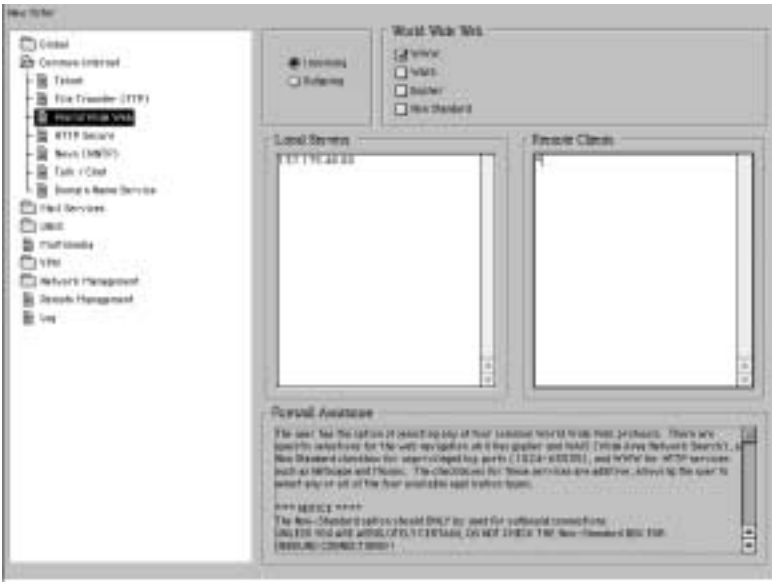
Single click on the file marked “World Wide Web”. You will note that the Configuration Area is now fully loaded. When any Application/Protocol is chosen from the left-most column, the initial configuration screen for that selection will be loaded. By default it will load the screen for configuring the allowable inbound traffic for that Application/Protocol. (Remember the Sun Cobalt Adaptive Firewall uses the “restrictive” firewall philosophy: that which is not expressly permitted is prohibited.) The Incoming check box in the top, left most field is the indication that inbound traffic is being configured. The next field to the right is now labelled with the name of the loaded Application/Protocol, in this case “World Wide Web”. Listed in this field are the protocols that can be enabled.

If you click the “WWW” check box, you can enter the pertinent host information that will allow traffic to reach your webserver. Note that no traffic will cross the firewall until the host addresses are entered into the Local Servers and Remote Clients input fields. It is not enough to enable the protocol, you must tell it what the endpoints of the connection will be.

In the **Local Servers** field (second row, left) enter the IP address of your webserver. The **Remote Clients** field (second row, right) must contain the IP address of the host that needs access to the webserver listed in the **Local Servers** field. Assuming that the webserver should be visible from all hosts on the external network, usually the Internet, you may be wondering how you can list every possible IP address. This can be accomplished by entering an asterisk (*) in

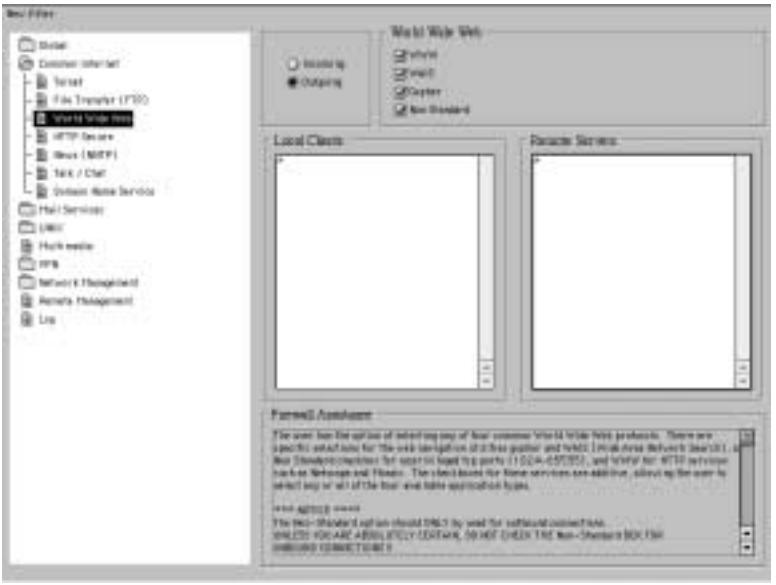
the **Remote Clients** field. Our example (Figure 5), therefore, shows a **Local Server** address of 137.175.48.80, which is our webserver behind the firewall. In the **Remote Clients** field we find an *, thus allowing any host outside the firewall to access 137.175.48.80.

Figure 5. Example WWW Incoming Configuration



Now click the Outgoing checkbox. Notice that the input fields have now changed to Local Clients and Remote Servers and are empty. Additionally, none of the protocol options are selected. In most cases you'll want to allow outbound web traffic from all of the machines inside the firewall to any webserver outside the firewall. We do this by entering asterisks in both the Local Clients and Remote Servers fields. We have also checked the WAIS and Gopher checkboxes so that anyone behind the firewall who needs to use those services can access them. Figure 6 shows the choices we've made.

Figure 6. Example Outgoing Configuration



Notice that the Firewall Assistance window at the bottom of the screen displays general information and tips on configuration as well as specific information about the loaded application/protocol. In this case there is a notice that points out that the use of the Non Standard option should be limited to outbound connections. Be certain to read the information in the Firewall Assistance window before you configure a given protocol option. It may contain caveats or notices of the consequences of mis-understanding or mis-configuring the protocol.

Symbolic Addresses in Firewall Files

It is particularly important to note that the filter files should be constructed using IP addresses and not hostnames because name resolution may require the use of a protocol such as the Domain Name System (DNS) or NIS (Network Information Service). If the connection being firewalled is also required for DNS to work, firewall definitions containing hostnames can never be properly resolved. For security reasons, the firewall must be fully compiled and installed before any information (including DNS queries) can traverse the interface. It is safest to always use addresses, rather than hostnames, when defining firewall rule sets.

Note: If DHCP is being used to assign the interface that is being firewalled, you must be careful how you specify addresses for the local servers: use wildcards or network addresses rather than host addresses for local servers.

Host Addresses versus Network Addresses

In some cases you will want to limit traffic to or from a particular network instead of a single host. You do this by adding the network address followed by the netmask in the appropriate Client or Server input field. This would take the form of `<network_address;netmask>`. Possible Class C netmask configurations are found in Table 6.

Table 6. Possible Class C Subnets

Shorthand Notation	Dotted Quad Notation	Number of Networks	Number of Hosts per Network
24	255.255.255.0	1	254
25	255.255.255.128	2	126
26	255.255.255.192	4	62
27	255.255.255.224	8	30
28	255.255.255.240	16	14
29	255.255.255.248	32	6
30	255.255.255.252	64	2

Example: to allow telnet access from machines on the Class C network 137.175.48.0 to any machine outside the firewall, enter 137.175.48.0;24 in the Local Clients field and * in the Remote Servers field of the Outgoing Telnet Configuration Area.

Use of Wildcards

To allow any and all hosts or networks to use or connect to a particular application or protocol, place the asterisk (*) character in the appropriate field for the given protocol. Those instances wherein the use of an * is dangerous or disallowed will be noted in the relevant section of the user guide and the SMS Firewall Assistance window.

The * character should always be used alone: addresses of the form a.b.c.* or a.b.* are not valid. The proper manner to define a network address is as described in section above. Thus the networks 137.175.48.0 and 192.168.0.0 would be entered in SMS as 137.175.48.0;24 and 192.168.0.0;16 respectively.

Creating the Initial Firewall

When opening up SMS you may note that there is a firewall/filter file named `outgoingonly`. This file a good base from which to generate your first firewall. It allows for outbound connections for most of the standard Internet protocols and services. It can be modified to enable any inbound services that your network requires or to specify additional outbound needs.

Note: If you do use the `outgoingonly` file as a base, be sure to save your changes to a different file so that the original remains intact, having only outbound rules configured.

Protocol and Application Windows

The current application and protocol types for which the Sun Cobalt Adaptive Firewall can generate firewall files are described in the sections that follow. A description of the options available within each window is included. Click on the checkbox beside the desired name to select the protocol or application type.

Global Options

Caution: Never use an "*" under any of the global categories because this would specify that **ALL** traffic be allowed to pass through the firewall or that **ALL** traffic be denied.

Cracking Prevention

This is provided to help prevent unwanted incursions into the user's network or systems. Three options are provided:

Port Scanning

This prevents entities from outside the user network from performing automated scans of the address space. These scans are used by various scripts and tools to locate and probe systems on a network.

Anti-Spoofing

This is used to thwart the common cracker technique of pretending to be a trusted internal system in order to gain access to resources. These types of attacks can be recognized because the source addresses of spoofed hosts will originate outside the network, but will carry an address which appears to be inside the network. When the Anti-Spoofing option is selected, the generated firewall file will prevent any packets having source addresses on an internal network from entering through the firewalled connection, thus thwarting spoofed packets. Spoofing cannot be prevented if any of the protected computer systems trust machines outside the firewall. Activating this feature will enable the Local Networks box. This field is used to define a list of network addresses which are internal to the user site. These network addresses are used in anti-spoofing firewalls to identify trusted internal networks. The box is a scrollable region, so long lists of networks may be entered.

Source Routing

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

Allow Estab

Enabling this feature will allow any established connections to remain active when an edited firewall is activated. If it is not enabled all connections will be reset when the edited firewall is activated. Those connections will need to be restarted.

Caution: Use of the Allow Estab feature is not usually recommended because it defeats the Stateful Packet Inspection mechanism for TCP connections. Since the inspection occurs on the establishment of the session, letting established sessions continue means that they will not be inspected to see if they violate the new firewall rules that were activated.

Restricted Sites

The **Restricted Sites** list gives the user a way to totally lock out certain internal hosts from all communication with the outside, and certain external hosts from all communication with the inside. When a host is restricted, it cannot communicate with hosts on the other side of the firewall, and hosts on the other side of the firewall cannot communicate with it. The **Enforce** checkbox must be selected in order to make this list take effect. When the **Enforce** checkbox is selected, the **Undesirable Outsiders** and **Grounded Locals** fields becomes active, allowing IP addresses to be added, modified, or deleted. These fields are scrollable regions, allowing the entry of long lists of sites.

Trusted Sites

The Trusted Sites option box allows the user to pass all traffic between this site and another completely trusted site. Generally, this is not a recommended configuration, but can be useful with an Intranet.

Note: Restricted and Trusted site rules take precedence over any subsequent rules. Once enabled **all** traffic between the specified hosts will be affected. Restricted will be blocked and Trusted will be allowed through the firewall. Use this option with caution.

Note: Note that the use of an asterisk in either the Local Networks/ Hosts or Remote Networks/Hosts fields will result in blocking ALL traffic from passing through the firewall. DO NOT use an asterisk (*, the wildcard character) under this Protocol/Application set.

Common Internet Applications

Telnet

Allows telnet connections to be configured. Due to inherent security issues with telnet, it is not advisable to allow inbound telnet connections to machines on your network.

- Telnet opens port 23 for tcp connections.

File Transfer Protocol

The File Transfer Protocol options are used to control the ability of users to transfer files into or out of the local network. Selecting the **Incoming** checkbox with the **Enable** checkbox allows external clients to make connections to local FTP servers. Areas are provided to specify **Local Servers** and **Remote Clients**. Only IP addresses may be entered. Entering a network address allows all hosts from that network. The asterisk character * is a wildcard, so entering a * in the **Remote Clients** area will allow all remote clients to reach the specified ftp server(s).

It is possible to permit internal sites to make FTP connections to external hosts by selecting the **Outgoing** checkbox. Selecting the **Outgoing** and **Enable** checkboxes causes the names on the scrollable boxes on the right to change from **Local Server** to **Local Client** and from **Remote Client** to **Remote Server**. Again, only IP addresses may be entered.

- FTP opens ports 20/tcp and 21/tcp for ftp-data and ftp command channels respectively.

World Wide Web Protocols

The user can select any of four common World Wide Web protocols. There are specific selections for the web navigation utilities gopher and WAIS (Wide Area Index Search), a Non Standard checkbox for custom protocols, and WWW for the standard HTTP services. The user can select any or all of the four available application types.

Selecting any of the four protocols and the **Outgoing** checkbox enables the **Local Clients** and **Remote Servers** fields, allowing the user to specify a list of available servers or networks which can be accessed by internal clients. The **Restricted Sites** facility is better suited to preventing local users from accessing external web sites that may be considered objectionable by management, while still allowing users to have access to other areas of the Web.

When configuring for inbound connections, be aware that the Non Standard option, if selected, will open ports 1024-65535 for all tcp-based traffic. Because this would leave a rather large hole in your firewall, it is strongly recommended that Custom Protocols be utilized in those cases where non-standard inbound ports are used.

The following port/protocol pairs can be opened under World Wide Web:

- 80/tcp for standard http/web traffic (WWW)
- wais
- gopher
- non standard

Caution: Never enable **non standard** for **inbound** traffic because this will enable **ALL** tcp based traffic to pass the firewall on all unprivileged ports (1024-65535).

HTTP Secure

Secure Hyper Text Transmission Protocol is a variant of the HTTP developed by Netscape to process secure transactions. Browsers that support the “https://” access method can connect to servers using Secure Socket Layer (SSL) when this service is enabled.

- HTTP Secure opens port 443 for tcp connections.

News (NNTP)

News applications such as `rn` are used to access a wide variety of information on diverse topics ranging from technical information to art. News is distributed in a relay fashion: sites receive news, then feed it to other sites, whch in turn feed it further up the line. The News options allow the network administrator to control which sites send news into the internal network and which sites may receive news from the internal network.

- NNTP opens port 119 for tcp connections.

Talk and Chat

The talk and chat protocols provide users with the ability to interactively communicate through the network. Users can type messages which are displayed in near real-time on the screen of another user. There are several applications and protocols available for this purpose. The options in the Talk / Chat window allow firewalling of packets for any or all of the `talk`, `ntalk` (New Talk), and `irc` (Internet Relay Chat) applications. In the `talk` and `ntalk` services, client refers to the host that initiates the talk session, and server refers to the host that answers. After the session is in progress, both hosts are effectively clients.

The following port/protocol pairs can be opened under Talk and Chat:

- 517/udp for Talk
- 518/udp for Ntalk
- 194/tcp for IRC

Domain Name Service (DNS)

DNS is a facility for providing name-to-address translations for TCP/IP systems. DNS is a hierarchical service: IP naming conventions segment hostnames using the period “.” character. Thus, ftp.Cobalt.com indicates that a host called “ftp” can be found in the “Cobalt” domain of a larger domain called “com”. Within each domain there are one or more name servers. The name server for a domain maintains a set of maps for resolving host name lookups. The name server uses these maps to translate between the names of hosts within its domain and their corresponding IP addresses. If the name server is queried for a name or address outside the scope of its domain, it uses a list of contact information to find another name server to query that contains the appropriate information.

In general, most name servers act as both clients and servers, since they must resolve both the names and addresses of outside entities for local clients and the names and addresses of internal entities for remote clients.

Generally, you want to allow internal hosts to query external name servers. To enable this, select the **Outgoing** checkbox, both **Queries** checkboxes and put an asterisk (*) in both location boxes.To limit **Outgoing** queries to only originate from your local nameserver, only put its address in the **Local Servers** box.

To allow external hosts to query your nameserver(s), select the **Incoming** checkbox, the **Queries** checkbox and enter your nameserver(s) in the **Local Servers** box and an asterisk (*) under the **Remote Clients** box. (Read the following paragraphs before selecting the **TCP Queries** checkbox.)

There are two cases when you may want to select the **TCP Queries** checkbox for Incoming packets. The first case, which is extremely rare, is when you have DNS records that exceed 512 bytes. In this case, the truncated bit would be set on the reply and another query would be sent from your nameserver using TCP. These TCP queries would need to pass through the firewall.

The second case is when there are external secondary servers doing zone transfers of your domain. If there is an asterisk (*) in the **Remote Clients** box, then both your secondary servers and anyone else can do zone transfers of your domain. If you wish to restrict incoming zone transfers to come only from your secondary servers, then you will need to configure this in your DNS software. With BIND 8, you can use the “allow-transfer” option to restrict zone transfers from certain sites.

If your DNS software doesn’t have the ability to restrict zone transfers, then don’t check the **TCP Queries** checkbox. Instead, create a custom port to allow zone transfers (incoming) from your secondary servers to your DNS server.

The following port/protocol pairs can be opened under DNS:

- 53/udp for Queries
- 53/tcp for TCP Queries (Zone Transfers)

Mail Services Options

The following mail services can be configured:

- SMTP mail
- POP mail
- IMAP

- CCMail P.O.
- CCSO Phonebook

SMTP Mail

The SMTP Mail firewall options allow the network administrator to control the flow of one of the most common mail protocols into and out of the network. SMTP, or Simple Mail Transfer Protocol, is the primary protocol used by sendmail and many other popular mail transport agents. Separate controls are provided for **Incoming** and **Outgoing** mail. Controls operate much like those described for options already discussed. When the **Enable** checkbox is selected, the network administrator may enter lists of local and remote clients and servers, as appropriate. Generally, for inbound mail the **Local Servers** field would contain the IP address of the machine running your mailserver. The **Remote Clients** field would contain the IP address of the machine from which your site receives its mail.

- SMTP opens port 25 for tcp connections.

POP Mail

POP (Post Office Protocol) is a client-server mail protocol. Separate controls are provided for incoming and outgoing POP traffic. There are also separate checkboxes for selecting the POP-2 and POP-3 protocols. Selecting the **Incoming** and **Enable** checkboxes will allow incoming POP messages between the specified **Local Servers** and **Remote Clients**. Selecting the **Outgoing** and **Enable** checkboxes will allow outgoing POP messages between the specified **Local Clients** and **Remote Servers**.

The following port/protocol pairs can be opened under IMAP Mail:

- 110/tcp for Pop-3
- 109/tcp for Pop-2

IMAP Mail

IMAP (Internet Mail Access Protocol) mail is a client-server mail protocol that offers the user the advantage of manipulating the mail on the remote server before downloading the entire mailbox. Separate controls are provided for incoming and outgoing IMAP traffic. There are separate checkboxes for selecting the versions 2/4 or version 3 of the protocol.

The following port/protocol pairs can be opened under POP Mail:

- 143/tcp for v2/v4
- 220/tcp for v3

CCMail P.O.

cc:Mail is a file-based, multi-protocol mail system that can be installed on networks that permit users' workstations to mount the cc:Mail server's directory as if it were a local hard disk.

- cc:Mail opens port 3264 for tcp connections.

CCSO Phonebook

CCSO Phonebook is a distributed database protocol that keeps track of personal and account information.

- CCSO Phonebook opens port 105 for tcp connections.

Unix Applications

Archie

`Archie` is a service that locates files on the Internet using ftp.

- `Archie` opens port 1525 for udp connections.

Finger

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

- `finger` opens port 79 for tcp connections.

Whois

The `whois` application allows users to query databases of user and host ID information. Many U.S. government organizations, including the Department of Defense, maintain `whois` servers. The `whois` application can also be used to query the Internet Registry at `rs.internic.net` for identifying information on users and hosts.

- `whois` opens port 43 for tcp connections.

UNIX Utilities

The UNIX utilities are a set of commands that allow remote operations on other hosts. They are both extremely powerful and extremely dangerous, since they represent one of the more significant potential security hazards on UNIX systems. The `rexec` command, in particular, is very insecure. The `rlogin` command allows users to remotely log into other machines. The `rexec` and `rsh` facilities are both used to execute commands on remote systems without establishing an interactive login session. While there are

system level security measures that are designed to protect against unauthorized intrusions via UNIX utilities, any system which has been improperly configured can be at risk of external attack. For inbound connections it is recommended that only known, trustworthy sites be enabled to use these protocols.

The following port/protocol pairs can be opened under Unix Utilities:

- 512-1023/tcp for `rsh`
- 512/tcp for `rexec`
- 512-1023/tcp `rlogin`
- 515/tcp printer (lpr)

X11

X11 is a windowing system that provides the user with remote graphics access. Unfortunately, it gives the remote user the same capabilities as the user at the terminal and can therefore be dangerous.

UUCP

UUCP is the UNI- to-UNIX copy program. The UUCP protocols allow file transfer, mail transfer, and remote program execution via either TCP/IP connections or through the use of point-to-point dialup modem connections.

- UUCP opens port 540 for tcp connections.

TFTP

Trivial File Transfer Protocol is a simpler version of FTP that doesn't support authentication. For that reason, it is not recommended that TFTP be used outside of your own network.

- TFTP opens port 69 for udp connections.

Rsync

Rsync is a program used to push or pull files across networks.

- Rsync opens port 873 for tcp connections.

SOCKS

SOCKS proxy TCP application data. Enable this service if you have a SOCKS based server running on a host behind the firewall or if you connect to a remote SOCKS server.

- SOCKS opens port 1080 for tcp connections.

CVS

CVS (Concurrent Versions System) is a version control system.

- CVS opens port 2401 for tcp connections.

Multimedia

The multimedia options box allows the user to pass or block multimedia packets from RealAudio and Streamworks.

The following port/protocol pairs can be opened under Multimedia:

- 7070/tcp for RealAudio
- 1558/udp for Streamworks

VPN

Virtual Private Networks (VPN) options are described in the paragraphs that follow.

Secure Shell

Secure Shell (SSH) is an Internet protocol intended to replace the functionality of the UNIX r-commands with a more secure application. SSH offers security measures such as encryption and authentication and can help a user create a Virtual Private Network (VPN).

- SSH opens port 22 for tcp connections.

IPSec

IP Security (IPSec) is a standard that provides authentication and encryption of data across networks. IPSec options allow the user to select ESP (Encrypted Security Payload) and/or AH (Authentication Header) to meet their security needs.

IKE

The Internet Key Exchange service is used in conjunction with IPSec to negotiate security associations for use in IP.

- IKE opens port 500 for udp connections.

PPP Tunnels

The PPP Tunnels option box allows the creation of PPP tunnels between source and destination addresses.

- PPP Tunnels opens port 57 for udp connections.

V-One SmartPass

V-ONE SmartPass is a component of V-ONE's SmartGate VPN product. Enabling this service allows SmartPass clients to connect to a V-ONE SmartGate server and establish a virtual private network.

- V-One SmartPass opens port 3845 for tcp connections.

L2TP

Level-Two Transport Protocol.

- L2TP opens port 1701 for tcp connections.

PPTP

Point-to-Point Tunneling Protocol.

- PPTP opens port 1723 for tcp connections.

Network Management

LAN Manager (NetBIOS)

NetBIOS (Network Basic Input/Output System) is a service that manages Microsoft Networking. The Lan Manager (NetBIOS) options box allows file/printer information as well as name service to be passed from machines running this tool.

- LAN Manager opens port 137 for udp connections.

Time Services

Time Services include NTP (Network Time Protocol), rdate, daytime, and timed. NTP can set the time on your machine using both internal and external sources.

The following port/protocol pairs can be opened under Time Services:

- 123/udp for NTP
- 37/tcp for rdate
- 13/tcp for daytime
- 525/udp for timed

Ident

Ident is a protocol that queries a sending host for the login name of the user sending mail to the receiving host.

- Ident opens port 113 for tcp connections.

Routing Information

Routing information protocols are used by standalone routers and by systems acting as IP routers to identify possible routes between networks and hosts. When multiple routes are available, it is possible for routers to dynamically adapt to changing network conditions. It is also possible to use routing information protocols to help to identify aspects of a network's topology or to mislead a host into mis-routing packets.

The following ports are opened for the various routing protocols:

- 179/tcp for BGP

- 89 for OSPF
- 8 for EGP
- 520/udp for RIP

Syslog

Syslog allows the user to log messages generated by machines and devices on the network. Flooding the syslog with messages is a common method of attack by intruders. Once the disk space on a syslog server is filled, no more messages will be recorded and thus no evidence will be left of the break-in.

SNMP

SNMP (Simple Network Management Protocol) allows the user to manage the equipment on the network, such as routers, hubs, servers, etc.

- SNMP opens port 161 for udp connections.

LDAP

Lightweight Directory Access Protocol.

- LDAP opens port 389 for tcp connections.

RADIUS

RADIUS (Remote Authentication Dial In User Service) servers provide user authentication and authorization services. RADIUS can also send accounting information to its clients.

- The RADIUS protocol uses UDP packets on port 1812
- RADIUS accounting uses UDP packets on port 1813.

TACACS

Terminal Access Controller Access Control System - provides user authentication for users trying to gain access to a router or an access server.

- TACACS opens port 49 for udp connections.

DHCP

DHCP (Dynamic Host Configuration Protocol) is a protocol for assigning dynamic IP addresses to devices on a network. Select DHCP Client if the IP address of the interface that is being firewalled is set via DHCP. Select DHCP Server if this host is acting as a DHCP server for a network. .

Note: Even if you do not enable Client or Server, DHCP will still work (though not optimally). By selecting either Client or Server, you are allowing traffic to flow over ports 67 and 68. If you block this traffic, the DHCP protocol can still work by using raw IP on the interface, which bypasses the firewall filter. By blocking this traffic over ports 67 and 68, you will cause the firewall to be unnecessarily unloaded and reloaded when the DHCP lease is renewed.

Ping and Traceroute

Ping and traceroute are applications that use ICMP (Internet Control Message Protocol). Ping gives the user information about whether or not a host can be reached and how long it takes a packet to get to that host. Traceroute tests whether or not a host is reachable and also gives information about the route used to reach the host.

- Ping allows icmp type 8 and 0 packets
- Traceroute opens ports 33410-33524 for udp connections.

ICMP

ICMP (Internet Control Message Protocol) messages give a user information about a network status such as service availability, as well as requests from the receiving machine for the host machine to slow down the rate of delivery exchange or to redirect a route. The ICMP option box breaks these messages down into three categories: Errors, Information Requests, and Redirects.

The following ICMP packet types are enabled for the specified check box:

- Errors: 3, 4, 11 & 12
- Info Requests: 10, 13, 15 & 17
- Redirect: 5

Remote Management

Enabling the Secure Management System (SMS) allows you to administer the Adaptive Firewall remotely. If you will be administering the firewall through an interface that the firewall is installed on, you MUST configure this service. If not, the activated firewall will prevent you from administering the Adaptive Firewall.

The ports available here are:

- 8181/tcp and 2005/tcp for the Secure Management System
- 444/tcp and 81/tcp for Cobalt Administration functions
- (Port 2323/tcp is a legacy from a previous system and should not be used).

Log

The Log options box allows the user to select what packets are recorded in the Adaptive Firewall log. The user can specify Incoming or Outgoing packets to be logged. The default behavior logs all rejected packets, but this option can be turned off by checking the No Rejects checkbox.

Checking the Start checkbox allows the user to log only the first of the packet stream while checking the End checkbox logs the last of the packet stream for those packets matching the IP address(es) in the **Log Sessions** box.

Selecting **All Packets** logs all packets whose IP address matches the address(es) listed in the **Log Packets** box. If you wish to log all packets for all machines, then put an asterisk (*) in the **Log Packets** box.

Custom Protocols

The Custom Protocol menu lets you allow a specific port or protocol through your firewall that is not in the template list. Although custom protocols cannot handle a complex protocol that uses a combination of dynamic TCP and UDP rules, it does handle the majority of cases.

Custom protocols are based on a port number and a protocol type. Here are the most common protocol types:

- TCP Session
- UDP Session
- UDP Query/Response
- UDP Packet Dst Spec
- UDP Packet Src Spec
- Raw IP Packet

TCP Session The firewall will pass TCP packets that contain the specified destination port if the packets are transmitted between the locations entered in the Local and Remote boxes.

UDP Session The firewall will pass UDP packets that contain the specified destination port if the packets are transmitted between the locations entered in the Local and Remote boxes. The source port can be any port. After the initial packet has passed, subsequent UDP packets in a UDP session are passed if the client side port is the original source port and the server side port is the source port of the initial UDP response packet.

UDP Query/Response This is similar to a UDP session, but the destination that receives the source's packet usually only responds with one or two packets and then the session ends.

UDP Packet Dst Spec This permits the firewall to pass UDP packets in one direction between the locations listed in the Local and Remote text boxes if the destination port matches what is specified.

UDP Packet Src Spec Same as above except the source port must match what is specified in the Port/Protocol box.

Raw IP Packet This is used to allow IP packets that are not defined by the TCP, UDP or ICMP protocols. When you select this option, the Port/Protocol box implies that a protocol will be entered. When one of the other options are selected, the Port/Protocol box implies that a port will be entered.

Configuring Custom Protocols

The following steps illustrate how you might add SSH using custom protocols. (Although Secure Shell is already in the template, we use it here as a simple example.) SSH uses TCP and runs on port 22.

1. Select **Custom Protocols** from the **Firewall** menu
2. Press **Add**
3. Check **Incoming**
4. Check **Enable**
5. Select **TCP Session** in the pull down list
6. Enter `22` in the **Port/Protocol** field
7. Enter `SSH` in the **Name** field
8. Enter the **Local Server** address and the **Remote Client** address(es) in the respective fields.
9. Click **OK**

To activate your changes, select **Save and Activate...** from the **File** menu in SMS

Troubleshooting

This chapter discusses common problems that may be encountered when using the Adaptive Firewall and possible solutions to those problems. The second section of the chapter describes how to debug an active firewall.

Common Problems

Problem: The Adaptive Firewall has been installed and a firewall policy has been activated and now the Qube 3 cannot be reached.

Explanation: Generally this is a result of an improperly configured firewall policy. The Adaptive Firewall operates on a restrictive principle. If a certain type of packet has not been enabled within the firewall policy it will be blocked by the active firewall.

If you are using the Secure Management System through the interface that the active firewall is installed on and you have not configured the firewall policy to allow SMS traffic, then after the initial activation of the firewall SMS will no longer be able to connect.

Solution:

1. Go to the LCD configuration panel of the Qube 3 and press the S button until **Adaptive Firewal** appears.
2. Press the **E** button and you will see **Drop Firewalls**. When given the choice, select **[Y]es**. Once **Drop Firewalls** has been confirmed, the active firewall will be dropped from all interfaces. This will allow you to get back into the host and fix the firewall policy to allow SMS to function when there is an active firewall.
3. Login to SMS. Once you are logged in the firewall policy that was most recently edited will be automatically loaded. If this is **not** the policy that was activated, open that one instead.
4. From the left hand column of services select **Remote Management**
5. Click the **Incoming** check box
6. Click the **Enable SMS** checkbox.

7. In the Local Servers field insert the IP address of the Qube 3. This is the IP of the interface that the active firewall will be run on. In the Remote Clients field insert the IP address of the host(s) you will be running SMS from. You may also enter "*" to allow a connection from any host.
8. From the **Firewall** menu select **Save and Activate**.

Note: *It is most secure to enter the actual IP address(es) of the machines you will be using for remote administration.*

Problem: Every time the firewall policy is saved and activated (or just activated) the current SMS session hangs.

Explanation: Unless configured otherwise, the Adaptive Firewall will terminate all active connections when a firewall policy is activated. This behavior is usually noticed by the admin via SMS not responding after a change has been made and activated.

Solution:

The **Allow Estab**. checkbox (under **Global**/**Cracking Prevention**) can be enabled to avoid this situation. This will allow active connections to continue normally when the active firewall is modified and re-initialized.

Caution: This is NOT recommended except under extraordinary conditions since such established connections are vulnerable to spoofing attacks.

Problem: Forgotten or corrupt SMS passphrase.

Explanation: In some cases you may have forgotten or never received the initial Adaptive Firewall passphrase. This is the password that is used to login to SMS and administer the firewall.

Solution:
1. Reset the passphrase as described in "Using the Adaptive Firewal Option" on page 30.
2. When you login into SMS using the new passphrase you will be prompted to change the passphrase a second time. This is done to ensure proper security.

Problem: Packets of a given protocol are not getting sent to the network or not being replied to.

Explanation: In most cases this is the result of an active firewall that has not been properly configured.

Solution:

1. Read through **Debugging the Active Firewall** in the section that follows and check the Adaptive Firewall log files to see if that protocol is being blocked.
2. If it is being blocked, locate the configuration screen within SMS for that protocol and ensure that it is properly configured.
3. If you can find no evidence of blocked packets but still suspect the active policy try de-activating and send traffic of the protocol in question.

   If it does pass, then there is a mis-configuration of the policy. Reactivate it and look at the logs again.

   If it still does not pass, the problem is not related to the Adaptive Firewall policy. Be sure that all related servers and clients are properly configured.

4. If there are still problems after checking the Adaptive Firewall's configuration, double check the settings for the IP Chains firewall to ensure there is no conflict between them.

Problem: Traffic that is configured to pass the firewall is being dropped.

Explanation: In most cases this will be the result of reaching or exceeding the connection or user transaction limit. The solution depends on whether the problem is caused by exceeding the connection limit or user transactio limit.

Connection Limit Exceeded: For each new outgoing connection that is made, a connection counter is incremented. This counter tracks the approximate number of outgoing tcp connections. When the connection counter exceeds the limit set in the license file, then the real number of connections is counted. If the number of real connections is still in excess of the limit then subsequent connections will be denied.

This methodology is used to avoid having to constantly count the real number of connections. Doing so would take too much time and connections are generally too volatile. It is possible that some of the connections have timed out and although you might observe that the connection counter exceeds the limit, the real number of connections might not. The connection counter is incremented each time a tcp connection is requested.

Solution - Connection Limit Exceeded:

1. This situation can be verified by checking the Adaptive Firewall log for the following messages:

```
1/26-16:14:22 connection request rejected
1/29-15:11:13 connection counter: 2
1/29-15:11:13 real connection #: 5
1/29-15:11:13 connection request rejected; number of connections reached
limit.
```

~~Another method to check the number of connections is to run the command 'cat /proc/net/phoenix_version'. This will display the list of IPs and the total number of current connections.~~

2. If you are seeing this error consistently, you will need to upgrade your license to allow for more connections.

User Limit Exceeded: User transactions are determined by the firewall counting the number of unique outgoing source IP addresses. When the number of addresses exceeds the user limit, packets are dropped.

Solution - User Limit Exceeded:

1. This situation can be verified by checking the Adaptive Firewall log for the following messages:

   ```
   1/26-16:14:22 reaching user limit, connection request rejected
   ```

   ~~Another method to check the number of connections is to run the command 'cat /proc/net/phoenix_version'. This will display the list of IPs and the total number of current connections.~~

2. If you are seeing this error consistently, you will need to upgrade your license to allow for more connections.

Problem: The Qube 3 has been rebooted and now no traffic is being passed.

Explanation: If the startup firewall does not load at boot time, the Adaptive Firewall will fail to a closed state. As a result no traffic will be passed.

This situation can be verified by checking in `/var/log/messages` for the following message that indicates that a failclose firewall has been installed:

```
1/29-15:11:13 ldfirewall: firewall license error, installing default
firewall /etc/phoenix/failclose.
```

Solution: Use the **Drop Firewal** option on the LCD control panel of the Qube 3 .

1. Use the LCD panel to drop the firewall as described in “Using the Adaptive Firewal Option” on page 30.

2. When the firewall has been dropped, any active firewall policy will be removed from all interfaces and the Adaptive Firewall will not be filtering the traffic from any interface.

Caution: When the Adaptive Firewall is reset there is no active firewall policy in effect. As such all traffic from the network will be passed through the Qube. Any given policy must be reactivated from SMS.

Debugging the Active Firewall

If you suspect that a given application or protocol should be passing through the firewall but are uncertain that it is, the following information should help you determine if the firewall is functioning as expected.

Understanding the Adaptive Firewall Log File

Below are examples of some typical entries from the Adaptive Firewall log. They will assist you in reading the log files to determine where problems or unexpected blockages may be occurring.

```
1/2-15:55:36 eth1:: tcp 209.41.220.250/13223 <- 209.186.246.198/3765 48 syn !pass (769)
```

Using the example above, the meaning of the fields of a given log entry are as follows:

Table 7. Example log File

Field Contents	Meaning
`1/2-15:55:36`	Timestamp, indicating when the entry was made.
`eth1::`	Indicates which interface is being filtered.
`tcp`	Indicates what transport protocol was used.
`209.41.220.250/13223`	Shows the IP address and port number of the local machine.
`<-`	Indicates the direction of traffic flow.
`209.186.246.198/3765`	Shows the IP address and port number of the remote host.
`48`	Indicates the size of the packet that was transmitted, in bytes.
`syn`	Shows any relevant bits set on packet. In this case the “syn” bit shows a request for a tcp session.
`!pass`	Indicates that the packet was denied access and was blocked (pass) at the firewall.
`(769)`	The line number within the firewall file where the rule that was triggered was based on.

Bearing the above in mind we see that our first two example entries below are ping requests (`8/0/icmp`) that were bound for the local host 209.41.220.250 from the host 207.243.40.32. They arrived within a second of each other but were not allowed to pass (`!pass`) the firewall due to a ruleset at line 748 ((`748`)) of the current firewall file. They were 1500 bytes long (`1500`).

```
1/2-15:20:25 eth1:: 8/0/icmp 209.41.220.250 <- 207.243.40.32 1500 !pass (748)
1/2-15:20:26 eth1:: 8/0/icmp 209.41.220.250 <- 207.243.40.33 1500 !pass (748)
```

Below is the line from the original example above. It shows that the host 209.186.246.198 requested a tcp session from port 3765 to the host behind the firewall 209.41.220.250. This request was denied (`!pass`) because of a ruleset found at line 769 ((`769`)) in the firewall file.

```
1/2-15:55:36 eth1:: tcp 209.41.220.250/13223 <- 209.186.246.198/3765 48 syn !pass (769)
```

Lastly, here are some examples of a successful connection through the firewall. Here we see that the local host 209.41.220.250 has sent a tcp session request (`syn`) to the remote host 137.175.48.16 from local ports 61435, 61436 and 61437 to port 80 on the remote host. This session was allowed by a ruleset at line 385 (`385`) of the firewall file. As the receiving port is port 80 we can guess that this is a web request.

```
1/2-15:55:37 eth1:: tcp 209.41.220.250/61435 -> 137.175.48.16/80 40 syn (385)
1/2-15:55:37 eth1:: tcp 209.41.220.250/61436 -> 137.175.48.16/80 40 syn (385)
1/2-15:55:38 eth1:: tcp 209.41.220.250/61437 -> 137.175.48.16/80 40 syn (385)
```

Recommended Further Reading

Networking and the TCP/IP Protocols

Computer Networks
by Andrew S. Tannenbaum
(March 1996) Prentice Hall; ISBN: 0133499456

Internetworking with TCP/IP Vol. I: Principles, Protocols, and Architecture
by Douglas E. Comer
(March 1995) Prentice Hall; ISBN: 0132169878

TCP/IP Illustrated, Volume 1: The Protocols (Addison-Wesley Professional Computing Series)
by W. Richard Stevens
(January 1994) Addison-Wesley Pub Co; ISBN: 0201633469

Network Security

Firewalls and Internet Security: Repelling the Wily Hacker
by William R. Cheswick, Steven M. Bellovin
(June 1994) Addison-Wesley Pub Co; ISBN: 0201633574

Building Internet Firewalls
by D. Brent Chapman, Elizabeth D. Zwicky, Deborah Russell (Editor)
(September 1995) O'Reilly & Associates; ISBN: 1565921240

Computer Communications Security: Principles, Standard Protocols and Techniques (Addison-Wesley Professional Computing Series)
by Warwick Ford
(January 1994) Prentice Hall; ISBN: 0137994532

Linux Administration

Maximum Linux Security: A Hacker's Guide to Protecting Your Linux Server and Workstation

(October 1999) Sams; ISBN: 0672316706

Running Linux
by Matt Welsh, Matthias Kalle Dalheimer, Lar Kaufman, Matthew Welsh
(August 1999) O'Reilly & Associates; ISBN: 156592469X

Linux Install and Configuration Little Black Book
by Dee-Ann Leblanc, Isaac Hajime-Yates
(November 1999) The Coriolis Group; ISBN: 1576104893

General Unix Administration

UNIX System Administration Handbook
by Evi Nemeth, Garth Snyder, Scott Seebass, Trent R. Hein
(January 1995) Prentice Hall; ISBN: 0131510517

World Wide Web

CERT: Carnegie Mellon University's Computer Security Task Force
http://www.cert.org

Security Focus: Good source for cross platform vulnerabilities and fixes.
http://www.securityfocus.com

Bruce Schneier: Counterpane: General tips on computer security and encryption
http://www.counterpane.com

Packetstorm: Secure archive site of exploits
http://packetstorm.securify.com

Risks Digest: News group on computer risks
http://catless.ncl.ac.uk/Risks

Antionline: General security news site
http://www.antionline.com

Slashdot: News group on linux and related topics.
http://www.slashdot.org

Manual Backup & Restore

If you are unable to run Netscape to perform a backup or restore you may archive the files manually. This involves logging into your Qube 3 and creating a tar archive that contains the relevant files.

Manual Backup

1. Telnet to your Qube 3 and `su` to the root user.
2. Now `cd` to `/etc/phoenix` and run the following command:

   ```
   tar -cvf <mybackup> license firewalls startup
   ```

   Where `<mybackup>` is the name you have chosen for the file.
3. It is recommended that this file be named using a scheme that includes the date of the backup. Additionally if you have more than one Qube 3 you may want to include the hostname or IP address of the unit within the file name. This lets you more easily determine what backup files belong to which machines and when they were backed up. Such a file name might look like this: dorothy.092400.backup.

   The tar command is used to create compressed archives of files or directories. The options and arguments we are using here are as follows:

   c create a new archive.

   v be verbose about what is being done.

   f use the next argument as the name of the newly created archive.

   license firewalls startup

   the list of files in the current directory that are to be included in the newly created archive.
4. Now you will want to move the tar file to another location and/or host for safe keeping.

Manual Restore

1. Telnet to your Qube 3 and su to the root user.

2. Using ftp place your backup tar file on the Qube 3. It is likely safest to place the tar file in /tmp

3. Now cd to the directory where you placed the tar file and run the command:

   tar -xvf <mybackup>

   Where <mybackup> is the name of the tar file.

   The tar command is used to make compressed archives of files or directories. the options and arguments we are using here are as follows:

   x extract the specified archive.

   v be verbose about what is being done.

   f use the next argument to specify the archive.

   The files will be extracted in the current directory.

4. Now move or copy the needed files to their appropriate places in the Adaptive Firewall home directory (`/etc/phoenix`).

   - `license` should go in the `/etc/phoenix` directory.
   - All firewall policy files under the directory `firewalls` go under the `/etc/phoenix/firewalls` directory.
   - If you have startup firewall policies defined, copy the contents of `startup` to the `/etc/phoenix/startup` directory.

Glossary

DHCP

see Dynamic Host Configuration Protocol (DHCP).

DNS

see Domain Name Service (DNS).

Domain Name

The human-readable equivalent of an IP address that has been assigned to an organization or other entity on the Internet. For example, www.cobalt.com is associated with a particular IP address for a specific host named “www” within the cobalt.com network/domain.

Domain Name System (DNS)

The Internet service responsible for translating a human-readable host name such as bob.com into the numeric IP address (10.1.1.1) for TCP/IP communications.

Dynamic Host Configuration Protocol (DHCP)

A protocol that provides a mechanism for allocating IP addresses dynamically so that an IP address can be reused when a host no longer needs it.

e-conduit

Provides an encrypted tunnel through which the Secure Management System communicates with the Adaptive Firewall server components. Modifications can be made to the firewall/policy configuration securely from external or remote sites.

Ethernet

The most widely used local area network (LAN) technology. Standard Ethernet runs at 10 Mb/s, 100 Mb/s or 1000Mb/s.

firewall filter file

This file contains the firewall rules that are used to build the active firewall that is running in the phoenix kernel module. The file is generated based on the selections made in the firewall template file in SMS. Also referred to as a firewall policy.

firewall template file

This file defines the user configurable applications and protocols that the Sun Cobalt Adaptive Firewall recognizes. These supported applications are displayed in the left most column of the SMS GUI. There are similar sets of parameters for most common applications that run over IP-based networks, such as the Internet.

Gateway

A network device that acts as an entrance to another network. A gateway can also be any device that passes packets from one network to another network across the Internet.

Internet Protocol (IP)

A network-layer protocol in the TCP/IP stack offering services needed for internetworking. IP provides features for addressing, type-of-service specification, fragmentation and reassembly of packets as well as security. IP is defined in RFC 791.

IP Address

A 32-bit address used to identify a host via Transmission Control Protocol/ Internet Protocol (TCP/IP). An IP address belongs to one of five classes (A,B,C,D or E) and is generally written as four octets separated by periods (for example, 192.168.10.10), also called the dotted decimal format.

Each address consists of a network number, an optional subnetwork number and a host number. The network and subnet numbers are used together for routing, while the host number is used to identify an individual host within the network or subnet. A subnet mask is used to delimit the network/subnet portion of an address from the host portion. IP addresses are sometimes also called an Internet address.

LAN

see Local Area Network

Local Area Network

A high-speed, low-error data network covering a relatively small geographic area (up to a few thousand meters). A LAN connects workstations, peripherals, terminals and other devices or hosts in a single building or

geographically limited area. LAN standards specify cabling and signalling at the physical and data link layers of the Open Systems Interconnection (OSI) model. Widely used LAN technologies include Ethernet, fiber distributed data interface (FDDI) and token ring. See also wide area network (WAN).

Media Access control (MAC) address

A standardized data-link-layer address that is required for every port or device that is connected to a LAN. Other devices in the network use these addresses to locate specific ports in the network, and to create and update routing tables and data structures. MAC addresses are six bytes long and their distribution is controlled by the IEEE. Also known as a hardware address, a MAC-layer address or physical address.

Name Server

Programs called name servers constitute the server half of the DNS client-server mechanism. A name server contains information about a segment of the DNS database and makes it available to a client called a resolver. A resolver is often just a library routine that creates queries and sends them across a network to a name server.

Packet

The unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. The packet includes a header containing control information and (usually) user data. Packets are most often used to refer to network layer units of data.

Packet Firewall

A program that filters traffic at the packet level based on source and destination addresses.

pafserver

The main server component of the Sun Cobalt Adaptive Firewall. It is responsible for loading any active firewalls and responding to user commands issued in the Secure Management user interface.

paflogd

The Adaptive Firewall server component that is responsible for logging messages from the active firewall policy. Messages are logged to /var/log/phoenix.log.

pafnanny

The Adaptive Firewall server component that monitors the status of the other major server components (pafserver, paflogd and thttpd).

phoenix kernel module

Loadable module that creates the active firewall. Its task is to keep track of all the traffic going through the firewall system, and it decides whether this traffic is allowed to pass, depending on the rules defined in the firewall filter/policy file.

Secure Management System

The Java-based user interface for the Sun Cobalt Adaptive Firewall. It is used to configure a firewall policy and can be run from Netscape Navigator versions 4.07 and above and Microsoft Internet Explorer 5.0 or 5.5.

Server

A system program that awaits requests from client programs across a network and services those requests. A server can be dedicated, in which case this is its sole function, or non-dedicated, where the system can be used in other ways, such as a workstation

Subnet mask

A number that, in conjunction with an IP address, defines the set of IP addresses that are grouped together as hosts in a given network. Each defined network is divided into a “network address” and a broadcast address, with the remaining addresses used for each individual host on the network. For example, if your IP address is 192.168.25.77 and your subnet mask is 255.255.255.0, then the addresses would be: 192.168.25.0 for the network address, 192.168.25.255 for the broadcast address, and 192.168.25.1 through 192.168.25.254 for the host addresses.

thttpd-phoenix

The Adaptive Firewall server component that provides http content to the Secure Management System user interface.

Transmission Control Protocol (TCP)

A connection-oriented transport-layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

Transmission Control Protocol/Internet Protocol (TCP/IP)

A common name for the suite of protocols developed in the 1970s to support the construction of worldwide internetworks. While there are many protocols in the suite, TCP and IP are the best known and thus have come to be used as the reference name of the entire set.

Wide Area Network (WAN)

A data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Asynchronous transfer mode (ATM), frame relay, Switched Multi megabit Data Service (SMDS) and X.25 are examples of WANs.