



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

**Securing UNIX
GCUX Practical Assignment
Securing Unix Step By Step –
Securing & Deploying Checkpoint Firewall-1
Enforcement Gateway**

Elias Rawadi
Version 1.9 April 8, 2002

© SANS Institute 2000 - 2002, Author retains full rights.

The Challenge

The IT engineering department in a multinational company with offices in over one hundred worldwide cities, most in third world countries, has the challenge of delivering a secure high bandwidth (10-100Mbps) data services from its offices to its customers' sites through the use of firewall protected private point-to-point connections.

The company is well aware of the implications and risks of leaving the task of building secure firewall servers to each location. As a result, it has decided to centralize the process by entrusting its IT engineering department with the task of delivering a simple, automated, easily deployable, secure Solaris and CheckPoint Firewall-1 gateway installation, (a cookie cutter solution if you will).

The intention of this paper is to deliver a procedure for building and delivering a secure "canned" CheckPoint Firewall-1 enforcement gateway distribution archive that requires minimal installation input, deployment time and technical knowledge. It is not the goal of this paper to configure the firewall for any particular deployment, or install/configure/secure a CheckPoint centralized management server that controls these enforcement gateways. However, we will cover in details the interaction between the firewalls and the management station during the testing process.

System Description

One way to describe the system is to go through the steps of a deployment scenario. The process gets started when a need for a firewall/VPN enforcement gateway installation arises at a certain site that could be located anywhere in the world. A Netra T1 SUN server is procured from a local or regional supplier and then directly shipped to that site. At that point, the onsite engineer or technician who does not need to have great understanding of firewalls or be a Unix/security guru will setup the system using the standard procedure and distribution archive specified and built by this writing. This process results in a standard tested CheckPoint firewall enforcement gateway image deployed at all the locations, reducing support cost and maintenance, while minimizing security risks.

Once the distribution archive is installed on the target system and IP connectivity is established, a security engineer sitting at a Checkpoint Enterprise Management station (centralized management) establishes SSL encrypted communication with the deployed firewall gateway. Then, he or she possibly pushes a license if central licensing is used, configure static routes, installs a security policy customized for that site, checks the logs (if centralized logging is configured), or monitor OS and firewall health/status.

To satisfy requirements like high bandwidth, global availability and support, price/performance ratio, ruggedness, reliability, modularity, rack size, manageability, and IT staff expertise, the company went through the process of evaluating and testing numerous security products. At the end, CheckPoint Firewall-1 and SUN's Netra T1(500MHz UltraSPARC IIe CPU, 18 GB hard drive, and 256 MB of memory) running Solaris 8 were the products of choice. A list of hardware and software required to build the system is described in the hardware and software section.

In order to properly maintain a distribution archive without affecting the critical operation of deployed firewalls, a staging system identical to the one to be deployed systems is required. All testing, OS and application patching, and upgrading will first be performed on the staging firewall which has identical setup as the production firewalls. When the changes are tested and approved they become a part of the distribution archive.

Audience

This document assumes that the reader possesses some Solaris system administration and checkpoint Firewall-1 operational knowledge as the OS installation process will be abbreviated a bit and not every screenshot and prompt pertaining to the Solaris OS installation will be displayed in full. For detailed Solaris OS installation, please refer to Sun's product documentation site (<http://docs.sun.com>).

Risk

The firewall will protect the network infrastructure services at deployed locations. While the company understands that it takes risk whenever valuable resources are connected to the corporate network and made available to customers and partners, it also understands that it must strike a balance between security and providing needed services. To mitigate the risks, one has to identify them and then try to prevent any damage.

The primary security concerns to the firewall are:

Un-secured / Mis-configured Systems

Installing a firewall on a system without proper hardening and patching may leave the firewall vulnerable to the underlying operating system security shortcomings. Since this deployment consists of multiple locations and firewalls,

the company has tasked one group to build and maintain an easily deployable secured Solaris based CheckPoint firewall image. This will remove all guesswork and personal interpretations out of building a secure firewall Enforcement gateway system. The end result is a standard tested image deployed at all the locations, reducing support cost and maintenance. The securing process involves minimizing the operating system, applying the latest recommended security patches, hardening the system by disabling unnecessary services, adding secure access and troubleshooting software like SSH and lsof, and finally specifying necessary ongoing maintenance.

Mis-configuration by the Firewall Administrator

Mis-configuration of a firewall rulebase is always a possibility since humans can and will make mistakes. Depending on the gravity of a mishap, the corporate network could become vulnerable to attacks. To alleviate this problem the company has put in a place a robust and well-documented change management procedure that details the steps administrators must follow before and after changes are made to the firewall rulebase, OS settings, upgrades, or patches.

Physical Security Compromise

The physical security of any server is critical. As gaining physical access may lead to the compromise of a system by using one of two methods:

1. Taking the boot hard drive and installing on another system as a second non bootable disk
2. Booting from portable media (CDROM) and then mounting the boot disk

Both situations can lead to read/write access to the /etc/shadow file where the root password can be modified or better cracked using programs like Crack or John the Ripper. To safeguard against these threats, the EEPROM security functionality will be turned on so a password is required before any PROM level command can be executed. Also, the server is placed in a lockable cabinet with tightly controlled key access along with an appropriately sized un-interruptible Power Supply (UPS) and air conditioning.

Downtime Due to Hardware Failure

Computer Hardware does break down at one point or another otherwise no one would need expensive service and maintenance contracts. To remedy this situation one must address the issues of backup and redundancy. During the planning process, the Netra T1 was picked as the platform of choice since it is a ruggedized box with carrier-grade packaging for a higher level of system

reliability. The Netra T1 also features a modular design with easily swappable components, an affordable price tag and a rack size (1U) that allows for keeping spare units or components at each site without heavily taxing a deployment budget.

Remote Firewall Administration

Administering multiple firewalls from a central management server and keeping the underlying operating system security patches up to date exposes the firewall to vulnerabilities like password sniffing. To alleviate this risk, we will harden the system by removing all access services that uses clear text passwords and data load and replaced them with OpenSSH. OpenSSH provides all the necessary services to securely access and copy patches to the system. Also, CheckPoint uses SIC (Secure Internal Communications), a certificate-based SSL (Secure Socket Layer) encrypted channel for communications between CheckPoint Modules (Management Server, VPN/FireWall...).

Methodology

Hundreds of papers, articles and checklists have been written about securing Solaris and other Unix flavors. Most of these publications deal with running Solaris hardening scripts as YASSP or Titan and generally follow this process:

1. Install the Core Solaris cluster plus any additional required packages.
2. Install the latest Solaris patch clusters.
3. Minimize the system by removing all unnecessary packages.
4. Harden/armor the OS and configure it for the intended application environment, CheckPoint Firewall-1 in this case.
5. Install and configure Checkpoint Firewall-1 NG package.

We will follow the same methodology, using SUN's framework of the *JumpStart Architecture and Security Scripts* (JASS) Toolkit to automate and simplify building secured Solaris systems. In addition, we will perform the following:

1. Create distribution archive using SUN "flar" utility
2. Demonstrate the deployment of the "flar" archive using CDROM or Web server
3. Perform a security check on the system using scanners and Center for Internet Security (CIS) Solaris benchmarking script.

Required Hardware & Software

1. Netra T1, Operating power 90-264V AC, sun4u, 256 Megabytes memory, single 18 GB hard-drive (expandable to two drives), terminal console access, Quad Fast Ethernet card. The disk and memory specifications exceed CheckPoint Firewall-1 requirements.
2. Access to a Unix system with C compiler, to build and compile various source codes and as a temporary storage platform.
3. Solaris 8 Revision 04/01 or later CDs.
4. Solaris 8 Recommended Solaris Patch Clusters (<http://sunsolve.sun.com>)
5. The Solaris Security Toolkit JASS, (<http://www.sun.com/security/jass/>)
6. The fix-modes package must first be acquired (<http://www.sun.com/blueprints/tools> or <ftp://ftp.wins.uva.nl/pub/solaris/fix-modes.tar.gz>).
7. The Isof package ([sof-4.49-sol8-sparc-64-local.gz](http://www.sun.com/blueprints/tools/sof-4.49-sol8-sparc-64-local.gz)).
8. The pre-built openSSH and its required packages may be downloaded from www.sunfreeware.com, make sure you get the 3.4 version as vulnerabilities have been discovered in previous versions.
 - openssh, [openssh-3.4p1-sol8-sparc-local.gz](http://www.sun.com/blueprints/tools/openssh-3.4p1-sol8-sparc-local.gz)
 - openssl, [openssl-0.9.6d-sol8-sparc-local.gz](http://www.sun.com/blueprints/tools/openssl-0.9.6d-sol8-sparc-local.gz)
 - tcp wrappers, [tcp_wrappers-7.6-sol8-sparc-local.gz](http://www.sun.com/blueprints/tools/tcp_wrappers-7.6-sol8-sparc-local.gz)
 - prngd, [prngd-0.9.25-sol8-sparc-local.gz](http://www.sun.com/blueprints/tools/prngd-0.9.25-sol8-sparc-local.gz)
9. A Web server running on any platform.
10. The benchmark document and scoring tools, [The Solaris Tools archive](#) .
11. CheckPoint Firewall-1 NG FP1 CD.

SUN's Flash Installation Facility

One of the obvious solutions to the task at hand is to build a full Jumpstart server along with the JASS toolkit. This scenario would be perfect in a data center environment with dedicated qualified staff and infrastructure. Since we are dealing with highly autonomous installations spread around the world with minimal or non-existing infrastructure (bandwidth, dedicated servers), let alone technical expertise, it makes more sense to provide a “canned” solution that requires minimal user input, deployment time and knowledge. To achieve this we will use Sun’s Flash facility, which extends the use of the traditional JumpStart installation framework by adding the mechanism to archive a snapshot of a master image. In a Windows environment this is called a “ghosted” (after Symmantec Ghost software) image and is used to deploy to other systems. Using the Flash facility, systems, may be “ghosted” using a CDROM, NFS, HTTP, or JumpStart servers. Another advantage of the Flash archive is that it is

faster than other mechanisms since Flash installation does not individually install software packages and does not update the installed package database. The archive Flash is essentially written to the installation disk as fast as the data can be taken off the network or the local CDROM/Tape.

Installation

Environment

The installation environment must be clean. The target system (Netra-T1) must not be connected to the Company's general network or the Internet at any time. The hardening toolkit (JASS, <http://www.sun.com/security/jass/>) and Solaris 8 Recommended patches (<http://sunsolve.sun.com>) must be downloaded from none other than SUN's official site before hand ,unzipped/extracted, and stored on a separate system or CDROM since the target system disk will be wiped out by a new OS installation. Never trust any previous installation. If connectivity from the target machine to a storage system or a web server is needed, a crossover cable or a small hub may be used.

Core OS Installation

The Core Solaris option performs minimal system installation. The number of packages is platform dependent and ranges between 60-120. However, in a CheckPoint Firewall-1 as well as other servers environment, where the graphical interface and other drivers are not required, the number of required packages can be normally further reduced to a number around 20-35. For the CheckPoint Firewall-1 server the absolute minimum number is 30. To install Solaris Core option, insert Solaris 8 Installation Disk at the OpenBoot PROM and type the following:

```
ok boot cdrom
```

Select Initial Install option if you get prompted:

```
Your system appears to be upgrade-able.  
Do you want to do a Initial Install or Upgrade?
```

```
1) Initial Install  
2) Upgrade  
Please Enter 1 or 2 >
```


The next issue is the swap size, which according to industry standard should be 2-3 times the memory size. Since Checkpoint is not a swap heavy application, and disk space availability is no longer as high a commodity as it used to be (the entire system disk used to be 512 MB), using the default (512MB) is acceptable.

Supply input as follows to these prompts:

Networked: Yes
Use DHCP: No
Primary network interface: eri0
Host name: fw1
IP address: 10.1.1.2
System part of a subnet: Yes
Netmask: 255.255.255.0
Enable IPv6: No
Configure Kerberos Security: No
Name service: None
Region: offset from GMT, Hours offset: 0
Date and time: 2002-03-26 16:43:00
Geographic region: North America, U.S.A. (en_US.ISO8859-1)
Install Type (Standard/Flash): Initial "Standard"
install Software group: Core System Support 64-bit .. 268.00 MB
Disk: c1t0d0 (17269 MB) boot disk 17269 MB
Preserve Data : No

Note that eri0 is not supported by CheckPoint yet, but our internal tests found no problem with its operation. If you need Checkpoint support in case you have problems, I recommend using one the four QFE interfaces instead.

Next is the file system and disk layout. By default the firewall sends its log files to the management station, which may resides on the same machine or on a separate dedicated server. In either case, since we have no other good use for the space, it is a good idea to make the /var partition as large as possible in order to accommodate the large amount of log storage a busy CheckPoint firewall requires.

Automatically Layout File Systems?: Manual Layout as follows

File System and Disk Layout:

/	c1t0d0s0 1026 MB
swap	c1t0d0s1 501 MB
/usr	c1t0d0s3 1000 MB
/var	c1t0d0s4 14741 MB

Mount Remote File Systems?: No

After completing above tasks, a summary of your selections is displayed, followed by the prompt:

There are two ways to install your Solaris software:

- "Standard" installs your system from a standard Solaris Distribution.
- "Flash" installs your system from one or more Flash Archives.

Choose the standard install and make sure you set the root password once the system finishes installation. The default core packages are listed in appendix A.

Install Packages Required for Checkpoint FW-1 NG

Checkpoint Firewall-1 requires five additional packages that are not part of the Solaris Core installation. The following four packages reside on the Solaris 8.0 Software CDROM 1/2:

```
system SUNWlibC Sun Workshop Compilers Bundled libC
system SUNWlibCx Sun WorkShop Bundled 64-bit libC
system SUNWadmc System administration core libraries
system SUNWadmfw System & Network Administration
Framework
```

The fifth package resides on the Solaris 8.0 Software CDROM 2/2:

```
system SUNWter Terminal Information
```

These packages have to be manually added by first mounting the Solaris Software CDROM 1/2, then using the pkgadd command as follows:

```
# mount -F hsfs -o ro /dev/dsk/c0t0d0s0 /cdrom
# cd /cdrom/Solaris_8/Product
# pkgadd -d . SUNWlibC
# pkgadd -d . SUNWlibCx
# pkgadd -d . SUNWadmc
# pkgadd -d . SUNWadmfw
```

Next you need to install the SUNWter package which is on the Solaris 8.0 Software CDROM 2/2, which requires unmounting the currently mounted CDROM

```
# cd /
# umount /dev/dsk/c0t0d0s0
```

Eject the drive and replace with the correct CDROM and install the SUNWter package:

```
# mount -F hsfs -o ro /dev/dsk/c0t0d0s0 /cdrom
# cd /cdrom/Solaris_8/Product
# pkgadd -d . SUNWter
```

Checking the number of installed packages using the `pkginfo | wc -l` commands. The `pkginfo` displays information about packages and the `wc -l` command displays the number of lines, in this case from the output of the `pkginfo` command.

```
# pkginfo |wc -l
107
```

Install Infrastructure Packages

The following packages are infrastructure support packages needed to do tasks ranging from keeping the system time synchronized, and unzipping files, to supporting packages like Perl, which is required by the Open SSH package. These packages may be installed using the same procedure listed in the previous paragraph.

SUNWntpr	NTP, (Root)
SUNWntpu	NTP, (Usr)
SUNWsndmu	Sendmail user
SUNWsndmr	Sendmail root
SUNWtoolx	programming Tools (64-bit)
SUNWgzip	GNU Zip (gzip) compression utility (1/2 OS CDROM)
SUNWzlib	The Zip compression library (2/2 CDROM)
SUNWpl5u	Perl 5.005_03 (1/2 CDROM)

Install Patch Cluster

The latest patch cluster `8_Recommended.zip` should be downloaded via a web browser or an ftp client from <http://sunsolve.sun.com> and applied. Once you start this process, you may want to take a break, since this operation may take a few hours:

```
# unzip 8_Recommended.zip
```

```
# cd 8_Recommended
# ./install_cluster
# Patch cluster install script for Solaris 8 Recommended
[...]
Are you ready to continue with install? [y/n]: y
Determining if sufficient save space exists...
Sufficient save space exists, continuing...
Installing patches located in /space/8_Recommended
Using patch_order file for patch installation sequence
Installing 112396-02...
Installing 108987-09...
Installing 111293-04...
[...]
```

Messages of failed installation with return code 2 or 8 may be safely ignored. Return code 8 implies that this patch is for a package that is not installed on this system while return code 2 implies that this patch or a newer patch for this software package as already been applied:

```
Installation of 110075-01 failed. Return code 2.
Installation of 108528-14 failed. Return code 8.
```

It is important to note that the patch application must be done before minimization and hardening since applying patches afterward may reverse work performed by the minimization and hardening process by reinstalling or enabling services or files.

Minimizing the System

Minimizing a system is the process of removing unnecessary packages and applications. The purpose of minimizing the system is to improve its security. As security vulnerabilities get regularly discovered, the fewer software packages a system has, the less likely that system will be affected by these vulnerabilities and the less work one has to do finding and patching them. As previously mentioned the Core Solaris installation on a Netra T1 takes one hundred and two packages. To this we added five Checkpoint software packages, and nine infrastructure packages needed for maintenance and troubleshooting purposes:

```
# pkginfo | wc -l
116
```

The following is a list of the minimum packages¹ required to run CheckPoint Firewall-1 on Solaris 8 in a 32 and 64 bit environment:

32 Bit Packages

SUNWcar	Core Architecture, (Root)
SUNWcsd	Core Solaris Devices
SUNWcsl	Core Solaris, (Shared Libs)
SUNWcsr	Core Solaris, (Root)
SUNWcsu	Core Solaris, (Usr)
SUNWesu	Extended System Utilities
SUNWhmd	SunSwift SBus Adapter Drivers
SUNWkvm	Core Architecture, (Kvm)
SUNWlibms	Sun WorkShop Bundled shared libm
SUNWloc	System Localization
SUNWnamos	Northern America OS Support
SUNWpd	PCI Drivers
SUNWswmt	Install and Patch Utilities

Netra T1 Specific Packages

The following is a list of Netra T1 hardware specific packages:

SMEvplr	SME platform links
SMEvplu	SME usr/platform links
SUNWensqr	Ensoniq ES1370/1371/1373 Audio Device Driver (32-bit), (Root)
SUNWglmr	Symbios 875/876 SCSI device driver, (Root)
SUNWidecr	IDE device drivers
SUNWider	IDE Device Driver, (Root)

64 Bit Packages

The following is a list of 64-bit packages required to run 64-bit mode software, which is the mode that will be used to run the CheckPoint firewall:

SUNWcarx	Core Architecture, (Root) (64-bit)
SUNWcslx	Core Solaris Libraries (64-bit)
SUNWcsxu	Core Solaris (Usr) (64-bit)
SUNWesxu	Extended System Utilities (64-bit)

¹ Solaris Operating Environment Minimization for Security
<http://www.sun.com/blueprints/1299/minimization.pdf>

SUNWhmdx	SunSwift SBus Adapter Drivers (64-bit)
SUNWkvmx	Core Architecture (Kvm) (64-bit)
SUNWlmsx	Sun WorkShop Bundled 64-bit shared libm
SUNWlocx	System Localization (64-bit)
SUNWnamox	Northern America 64-bit OS Support
SUNWpdx	PCI Drivers (64-bit)

Infrastructure Packages

The following is a list of packages needed to ensure better and easier operation of the firewall. For example, even though we could have skipped installing the compression utility SUNWgzip, we opted to keep it just in case we need to compress logfiles, uncompress and install a needed utility that ships in a gzipped format.

SUNWntpr	NTP, (Root)
SUNWntpu	NTP, (Usr)
SUNWsndmu	Sendmail user
SUNWsndmr	Sendmail root
SUNWtoolx	programming Tools (64-bit)
SUNWgzip	GNU Zip (gzip) compression utility
SUNWzlib	The Zip compression library
SUNWinst	Contains the FLAR utility used to "ghost" the system

Checkpoint Required Packages

The following is a list of checkpoint required packages. The Firewall-1 software will abort installation or not properly run if any of these packages² are missing:

SUNWlibC	Sun Workshop Compilers Bundled libC
SUNWlibCx	Sun WorkShop Bundled 64-bit libC
SUNWadmc	System administration core libraries
SUNWadmfw	System & Network Administration Framework
SUNWter	Terminal Information

Other Packages

Packages not listed in above sections (see appendix C for complete list) may be removed using the pkgm command, for example the command:

```
# pkgm SUNWatfsr
```

² Spitzner, Armoring Solaris II, <http://www.enteract.com/~lspitz/pubs.html>

would remove the AutoFS user package. You may use a script to automate the process:

```
#!/bin/sh
cat del | \
while read line
do
    pkgm -n -A $line
done
```

where del is a text file containing a list (one per line) of packages that need to be deleted. You may have to do some of the packages by hand depending on your installation, as some of them require user interaction even when you employ the `-n` option.

Hardening the System

Running The JASS Script

Download the source file JASS 0.3.5.tar.Z from <http://www.sun.com/blueprints/tools/license.html>. The zipped file contains Solaris documents that are great reference materials for Solaris security and network performance. Copy the previously extracted files into a directory on the server using the `zcat` and `tar` commands as follows:

```
# zcat jass-0.3.5.tar.Z | tar -xvf -
# cp jass-0.3.5 /usr/local
# cd /usr/local/jass-0.3.5
```

The JASS toolkit has the capability to run in both standalone and Jumpstart environment. Since our installation is a one time operation, it makes more sense to use the standalone method and skip customization. To implement all of the hardening scripts as defined in the `secure.driver` script file, change to the `jass-0.3.5` directory and issue the `jass-execute` command with `secure.driver` file located in the `drivers` directory as an argument:

```
./jass-execute -d secure.driver
```

Discussing the internal working of the JASS toolkit is beyond the scope of this paper, but we will when possible, display the command that accomplished discussed task just in case the reader wants to perform the hardening manually. Detailed information about customization may be found in the [Solaris™ Security Toolkit-Internals](#) article. The `jass-execute` process will take about a minute or two and perform the following:

Tighten User Access Control and Increase Logging:

Solaris ships pre-configured with accounts and services whose access must be tightened to improve system access security. These accounts may be safely disabled or in some cases deleted without affecting the operation of the system in most cases. Access to services like FTP, "at", and "cron" should also be tightly controlled. Since the end system is a firewall, most of these services are not needed for proper operations.

- Removes the following accounts: smtp listen nobody4. This is accomplished by editing the /etc/passwd file and deleting the lines that starts with these names. Once the password file is saved, the pwconv needs to be run so the /etc/shadow file is also updated.
- Disables the following accounts: daemon bin adm lp uucp nuucp nobody noaccess, by changing their shell to /sbin/noshell in the /etc/passwd file.
- Sets account aging to 1 Minweeks and 8 for Maxweeks, password length to 8. Edit the /etc/default/passwd file and set these entries.
- Sets "at", "cron" and ftp (Solaris 8 default) deny list to all the accounts, and cron log size. Even though the FTP service is not running, a second line of defense is always a good idea, just in case the service gets somehow re-enabled.
- Sets telnetd banners by editing the /etc/motd and /etc/issue files. See appendix D for their contents.
- Sets ftpd banner and default umask to 022, taking away world and group write permissions from newly created files. Create an /etc/default/ftpd file containing the lines
BANNER="Authorized users only, All access may be logged"
UMASK=022
- Creates /var/adm/sulog' file to track the use or attempted use of 'su'
- Creates the log file /var/adm/loginlog to track failed login attempts
- Customizes syslog file to allow for more extensive logging as Solaris by default does not capture some syslog events, i.e, events sent to LOG_AUTH.
- Sets login 'RETRIES' to '3' in /etc/default/login. This set the number of failed logins that will be allowed to 3 before login exits.
- Customizes /etc/.login and /etc/profile files.
- Sets the 'root' user's primary group to 0, so all created files and directory will have root group ownership, instead of other thus tightening access. This is accomplished by editing the /etc/passwd file and changing the fourth column from 1 to 0
- Disables direct remote 'root' login to the system, protecting against brute force password attack on the root account. This is the default in Solaris 8.
- Disables the ability to use 'rhosts' authentication. ".rhosts" files are used for network based authentication and are insecure and should be disabled.
grep -v rhosts_auth /etc/pam.conf > /etc/pam.new
mv /etc/pam.new /etc/pam.conf

- Resets the current number of EEPROM 'badlogins' to 0. This allows for monitoring of the number of failed EEPROM logins
eeprom security-#badlogins=0

In order to avoid a self-inflicted denial of service the JASS script instructs the user to execute the EEPROM security manually from the operating system at the root prompt:

```
# eeprom security-mode=command
Changing PROM password:
New password:xxxxxxx
Retype new password:xxxxxxx
```

Boot and Network Services:

Even though a well-configured firewall will prohibit access to the following services, we will disable the ones that are not needed for the operation of the firewall as an in depth multi-layered defense is always a good idea. Some of these services may not exist on the system as we chose the Solaris OS minimal installation.

- Disables all services in the /etc/inetd.conf file. The startup script for this file has already been disabled, but again, in depth defense is the guiding principal. This task is accomplished by inserting the # character at the beginning of each line defining a service
- Disables AnswerBook 2 service
mv /etc/rc2.d/S96ab2mgr /etc/rc2.d/_S96ab2mgr
- Creates S00set-tmp-permissions which sets the correct permissions on the /tmp and /var/tmp directories when the system is rebooted
- Creates the S70noddconfig script that makes the network interface less susceptible to various attacks. The script uses the ndd command and does the followings³:
 - Decreases ARP cleanup interval to 30000 from 600000 milliseconds reducing the effectiveness of an ARP attack.
 - Disables the forwarding of directed broadcasts to prevent broadcast based attacks.
 - Disables forwarding of source routed packets, which may be used for hacking purposes.
 - Ignores ICMP packets that define new routes foiling attempts to poison the routing table.

³ The Solaris Security Toolkit JASS, <http://www.sun.com/security/jass/>

- Shortens the time interval to 60000 from 1200000 milliseconds a specific route will be kept to help reduce the effectiveness of attacks.
 - Disables response to ICMP netmask requests to prevent access to netmask information.
 - Disables response to ICMP broadcast echo requests (ping). Ping could be used to map the network or as a denial of service attacks.
 - Disables response to ICMP timestamp requests. Any information given out may help a hacker. Do not make easy for them.
 - Disables the capability to send ICMP redirect messages, which can alter routing behavior.
 - Increases the size of the queue containing un-established connections from 1024 to 4096
 - Enables strict destination multi-homing. A packet is dropped when it is sent to an interface from which it did not arrive.
 - Increases the size of fully established connection queue providing some limited protection against resource consumption attacks.
 - Disables reverse route packets.
 - Defines the upper (65535) and lower (32768) bounds of short-lived ports.
- Disables Apache web service
mv /etc/rc3.d/S50apaha /etc/rc3.d/_S50apache
 - Disables the Asynchronous Point-to-Point Protocol (ASPPP) service
mv /etc/rc2.d/S47asppp /etc/rc2.d/_S47asppp
 - Disables the sysid and autoinstall functions
mv /etc/rc2.d/S72autoinstall /etc/rc2.d/_S72autoinstall
mv /etc/rc2.d/S30sysid.net /etc/rc2.d/_S30sysid.net
 - Disables the automount service
mv /etc/rc2.d/S74autofs /etc/rc2.d/_S74autofs
 - Disables the Desktop Management Interface (DMI) service
mv /etc/rc3.d/S77dmi /etc/rc3.d/_S77dmi
 - Disables the Common Desktop Environment (CDE) service
mv /etc/rc2.d/S99dtlogin /etc/rc2.d/_S99dtlogin
 - Disables the Lightweight Directory Access Protocol (LDAP) client
mv /etc/rc2.d/S71ldap.client /etc/rc2.d/_S71ldap.client
 - Disables the line printer (LP) service
mv /etc/rc2.d/S80lp /etc/rc2.d/_S80lp
 - Disables Networked File System (NFS) client service
mv /etc/rc2.d/S73nfs.client /etc/rc2.d/_S73nfs.client
 - Disables the Networked File System (NFS) server service
mv /etc/rc3.d/S15nfs.server /etc/rc3.d/_S15nfs.server
 - Disables the file PRESERVE functionality, which has historical security problems, which may have already been fixed.
mv /etc/rc2.d/S80preserve /etc/rc2.d/_S80preserve
 - Disables the Power Management service. The system is a firewall server and needs to stay up, so no power management is necessary
mv /etc/rc2.d/S85power /etc/rc2.d/_S85power

- Disables the Remote Procedure Call (RPC) service
mv /etc/rc2.d/S71rpc /etc/rc2.d/_S71rpc
- Disables the Service Location Protocol (SLP) service
mv /etc/rc2.d/S72slpd /etc/rc2.d/_S72slpd
- Disables the SunSoft Print Service (SPC) service
mv /etc/rc2.d/S80spc /etc/rc2.d/_S80spc
- Disables the Unix-to-Unix Copy (UUCP) service
mv /etc/rc2.d/S70uucp /etc/rc2.d/_S70uucp
- Disables the Volume Management (VOLD) service
mv /etc/rc2.d/S92volmgt /etc/rc2.d/_S92volmgt
- Disables the Web-based Enterprise Management (WBEM) service
mv /etc/rc2.d/S90wbem /etc/rc2.d/_S90wbem

Other Kernel Configuration:

- Configures the NFS server service to accept connections/requests originating from privileged ports only. Again, the NFS daemon has previously been disabled and this step is part of the multi-layer defense, just in case someone has accidentally re-enabled it.
- Enables kernel-level stack protections and logging. This setting helps prevent and log the system against certain types of buffer overflow hacks. The JASS script accomplish that by adding the following to the /etc/system

```
set noexec_user_stack = 1
set noexec_user_stack_log = 1
```

Fix-Modes Script

The Fix-Modes script tightens the security on otherwise lax permissions on many of the Solaris files. It makes the file system modes more secure by removing group and world write permissions on all files, devices, and directories listed in /var/sadm/install/contents, with the exception of those files and directories that are supposed to be group/world writable. The files and directories are OS and release dependent and are listed in the Fix-Modes distribution file exceptions.h. The JASS tool is highly customizable and has the capability to run the fix-modes script provided that the script is placed in the JASS specified directory. Since the JASS tool was run without any modification, the fix-mode scripts will have to be run manually.

Unpack the downloaded package and run the fix-modes script:

```
# zcat fix-modes.tar.Z | tar -xvf -
# cd Fix-Modes
# ./fix-modes
```

```
secure-modes: WARNING: Can't find required uid/gid smmsp
secure-modes: WARNING: Can't find required uid/gid smmsp
touch: var/lp/logs/lpNet cannot create
touch: var/lp/logs/lpsched cannot create
chown: var/lp/logs/lpNet*: No such file or directory
chown: var/lp/logs/lpsched*: No such file or directory
chgrp: var/lp/logs/lpNet*: No such file or directory
chgrp: var/lp/logs/lpsched*: No such file or directory
chmod: WARNING: can't access var/lp/logs/lpNet*
chmod: WARNING: can't access var/lp/logs/lpsched*
[...]
```

The error and warning messages may be safely ignored as they result from the script trying to access non existing files or create files in non existing directories. These directories and files were deleted by the system minimizing process.

Beyond JASS Customization

Since we chose not to do any customization on the JASS scripts we will have to perform further hardening and in some cases undo certain JASS enabled settings by hand:

Miscellaneous

- Delete the newly created `/etc/notrouter` file. The presence of this file causes the system not to act as a router. Since this is a firewall box and routing is fundamental to a firewall operation, this file needs to be removed.
- Reset the `ip_strict_dst_multihoming` parameter to 0 in the `/etc/S70niddconfig` file. In a firewall environment cross-interface traffic needs to occur in order for IP traffic to cross from one interface to another provided the firewall rules permit that traffic.
- Disable the `inetd` script in `/etc/rc2.d`, as an extra precaution as all services in listed the `inetd.conf` file have been disabled already. Users will no longer be able to telnet, ftp, rlogin, and tcp/udp small services.

```
# mv S72inetsvc _S72inetsvc
```

- Disable the `sendmail` script in `/etc/rc2.d/`, since the `sendmail` daemon does not need to run as a daemon in order to send mail and this host does not need to act as a mail server. `Sendmail` historically has been plagued by vulnerabilities and it is a always a good idea to disable it when possible.

```
# mv S88sendmail _S88sendmail
```

- Disable the caching script in /etc/rc2.d/. nscd provides a cache for the most common name service requests. This caching service is not required for a firewall operation and thus need to be turned off.

```
# mv S76nscd _S76nscd
```

- Limit user resource consumption by limiting the number of processes to 128 per user, and disable core file system creation by adding these lines to /etc/system. Core dumps may contain sensitive information like passwords, file contents and path... and are usually world readable.

```
set maxuprc = 128
set sys:coredumpsize = 0
```

- Remove the following line from /etc/inittab to disable the login prompt on serial devices. Note that the console serial device is not affected:

```
sc:234:respawn:/usr/lib/saf/sac -t 300
```

- Force the system to use a stronger TCP sequence number generation algorithm to counter TCP session hijacking programs. Edit /etc/default/inetinit and change TCP_STRONG_ISS value to 2.

File System Configuration

Solaris file systems may be protected by employing the logging, nosuid and ro mount options. The logging option stores changes to the file system into a log before they are applied to the UFS file system, thus keeping it from ever becoming inconsistent. This process allows for fsck to be bypassed, which reduces the time to reboot a system if it crashes, or is uncleanly halted. The logging feature may be applied to all writable UFS file systems. It is important to note that the remount keyword must be employed along with the logging option so other options to the file system take effect.

The nosuid option disallows set-UID execution and thus keeps would be hackers from executing rogue set-UID programs mounted from removable media or copied to an existing file system. A good candidate for this option is the /var file system since you cannot turn off set-UID on the root file systems.

The ro option mounts the file system in read-only mode protecting the system binaries from being replaced with trojan horse programs. The /usr file system is where Solaris binaries reside and should be mounted read-only.

The following are the changes that need to be made to the /etc/vfstab file. A system reboot is required for these changes to take effect.

- Mount root file system in /etc/vfstab with logging option :

```
/dev/dsk/c1t0d0s0 /dev/rdisk/c1t0d0s0 / ufs 1 no remount,logging
```

- Mount /usr read-only mode in /etc/vfstab :

```
/dev/dsk/c1t0d0s3 /dev/rdisk/c1t0d0s3 /usr ufs 1 no ro
```

- Mount non-root ufs file system *nosuid* to prevent set-UID program execution:

```
/dev/dsk/c1t0d0s4 /dev/rdisk/c1t0d0s4 /var ufs 1 no nosuid
```

SSH & TCP Wrappers Installation

SSH provides protection against eavesdropping, session hijacking, and other network-level attacks by encrypting all traffic including passwords. Users of telnet, rlogin, ftp, and other programs such as X are vulnerable since passwords and data are transmitted in clear text over the network.

In this section, we will summarize the steps taken to install and configure OpenSSH, an open source version of the SSH secure shell system. More detailed installation and configuration information may be obtained from www.sunfreeware.com/openssh.html, or www.sun.com/blueprint.

Unzip the previously downloaded packages and install them:

```
#gunzip tcp_wrappers-7.6-sol8-sparc-local.gz
#gunzip openssl-0.9.6d-sol8-sparc-local.gz
#gunzip openssh-3.4p1-sol8-sparc-local.gz
#gunzip prngd-0.9.25-sol8-sparc-local.gz
#pkgadd -d tcp_wrappers-7.6-sol8-sparc-local
#pkgadd -d prngd-0.9.25-sol8-sparc-local
#pkgadd -d openssl-0.9.6d-sol8-sparc-local
[...]
#pkgadd -d openssh-3.4p1-sol8-sparc-local
[...]
# mkdir /var/empty
# chown root:sys /var/empty
# chmod 755 /var/empty
# groupadd sshd
# useradd -g sshd -c 'sshd privsep' -d /var/empty -s /bin/false sshd
```

Create the files that control access to the services (ssh in this case) and hosts: /etc/hosts.allow and /etc/hosts.deny, and populate as follows:

```
# echo sshd: ALL > /etc/hosts.deny
# echo sshd:x.x.x.x > /etc/hosts.allow
```

Where x.x.x.x is the ip address of the firewall management station. This will limit access to the sshd service to the firewall management station.

Create startup scripts for SSH and prngd as specified in appendix E, set permission and create link to startup script

```
# chown root /etc/init.d/prngd
# chgrp sys /etc/init.d/prngd
# chmod 555 /etc/init.d/prngd
# ln -s /etc/init.d/prngd /etc/rc2.d/S98prngd
# /etc/rc2.d/S98prngd start
# chown root /etc/init.d/sshd
# chgrp sys /etc/init.d/sshd
# chmod 555 /etc/init.d/sshd
# ln -s /etc/init.d/sshd /etc/rc2.d/S98sshd
# /etc/rc2.d/S98sshd start
```

Configure the /usr/local/etc/sshd_config as specified in appendix F.

Generate server key files:

```
# cd /usr/local/bin
# ./ssh-keygen -t rsa1 -f /usr/local/etc/ssh_host_key -N ""
Generating public/private rsa1 key pair.
[...]
# ./ssh-keygen -t dsa -f /usr/local/etc/ssh_host_dsa_key -N ""
Generating public/private dsa key pair.
[...]
# ./ssh-keygen -t rsa -f /usr/local/etc/ssh_host_rsa_key -N ""
Generating public/private rsa key pair
[...]
```

Note that SUN now provides a patch for Solaris 8 that enables /dev/random on the system. This patch would have saved us the installation of the prngd package had the OpenSSH been compiled with the options to take advantage of it.

Install lsof

Simply put, lsof lists information about files and ports that are opened by the processes running on a UNIX system. But since pretty much everything in Unix is a file, lsof becomes a very versatile tool that can report on files, active network sockets, and device files, pipes.... lsof combines many features of tools like fuser, netstat, and ps, which makes it an indispensable forensic analysis tool, thus earns it the right to be included in the distribution archive.

The package installs in /usr/local/bin.

```
# gunzip lsof-4.49-sol8-sparc-64-local.gz
# pkgadd -d lsof-4.49-sol8-sparc-64-local
[...]
The following packages are available:
1 SMClsf lsof
  (sparc) 4.49
[...]
```

Configure the Firewall Network Interfaces

Edit the /etc/hosts files and enter the ip addresses for the interfaces and create the files /etc/hostame.qfe0, /etc/hostname.qfe1, /etc/hostname.qfe2. Set the eeprom variable local-mac-address? to true so that each interface will get a unique MAC address, otherwise all interfaces will have the same MAC which may create problems if the two interfaces get connected to the same switch/hub.

```
# echo "172.16.1.1 <tab> qfe0" >> /etc/hosts
# echo "172.17.1.1 <tab> qfe1" >> /etc/hosts
# echo "172.18.1.1 <tab> qfe2" >> /etc/hosts
# echo qfe0 > /etc/hostname.qfe0
# echo qfe1 > /etc/hostname.qfe1
# echo qfe2 > /etc/hostname.qfe2
# init 0
[...]
ok setenv local-mac-address? True
# boot
```

To verify the MAC Addresses,

```
# /usr/sbin/ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu
8232 index 1
inet 127.0.0.1 netmask ffffffff
eri0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
index 2
inet 10.1.1.2 netmask fffffff0 broadcast 163.185.19.255
```



```
ether 0:3:ba:8:74:7d
qfe0: flags=1000842<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
index 3
inet 172.16.1.1netmask 0
ether 0:60:5b:b:20:9c
[...]
```

Configure NTP

Computer internal clocks are notoriously inaccurate. It is essential to use an external clock source for computer time synchronization to accurately time-tag logged events as these logs may be used for incidents handling and forensics. Correlation of events is made easier by a synchronized time source.

The NTP software is installed as a recommended infrastructure package. This system will be configured as a client that retrieves the time from one or more of the internal timeservers. Edit the configuration file `/etc/inet/ntp.conf` and specify the following:

```
driftfile /etc/inet/ntp.drift
server 10.11.1.1
server 10.12.2.2
server 10.13.3.3
restrict default nomodify
```

The `/etc/rc2.d/S74xntpd` startup script ensures that NTP daemon starts up and synchronizes the clock automatically with specified time servers on the network.

Installing and Configuring Checkpoint FW-1 NG

Before attempting to install the Checkpoint Firewall, ensure that patches 108434 and 108435 have been installed. The Checkpoint installation will abort without them.

```
#patchadd -p |grep 108434
108434-06
#patchadd -p |grep 108435
108435-06
```

Earlier versions of the [Recommended and Security patch cluster](#) did not include these patches, so make sure that you get the latest release.

Insert the CheckPoint NG CD-ROM into the drive and mount it,

```
# mount -F hsfs -o ro /dev/dsk/c0t0d0s0 /cdrom
```

```
# cd /cdrom
# ./UnixInstallScript
Check Point Software Technologies Ltd.
We recommend that you close all other applications while running Suite!
This installation program.
[...]
```

Enter "N" to go to the next screen and enter "y" if you agree with the software license agreement. Next CheckPoint SVN foundation installs and the following displays:

The following products are included on this CD.
Select Product(s)

- 1.[*] VPN-1 & FireWall-1.
- 2.[] FloodGate-1.
- [...]

Enter "1" for the VPN-1 & FireWall-1 option followed by "N" for the next display. Once the next screen displays, enter "2" for the enforcement module since the management server will reside on a centralized management station:

Installation Type

- 1. () Enterprise Primary Management and Enforcement Module.
- 2. (*) Enforcement Module.
- [...]

Enter N and the enforcement module will start installing. During the boot process, a default filter is generated and applied so the OS is protected during that vulnerable time when the policy is not being enforced. IP forwarding is also disabled. The above is achieved by adding two boot scripts "/etc/fw.boot/S25fw1boot" and "/etc/fw.boot/S00fw1bootd".

Answer the prompt as specified in bold below:

```
***** VPN-1 & FireWall-1 kernel module installation*****
```

```
installing VPN-1 & FireWall-1 kernel module...
May 6 18:38:17 station1 vpn: VPN-1: driver installed Done.
***** Interface Configuration *****
```

```
Scanning for unknown interfaces...
Would you like to install the High Availability product ? (y/n) [y] ? n
IP forwarding disabled
Hardening OS Security: IP forwarding will be disabled during boot.
Generating default filter
Default Filter installed
Hardening OS Security: Default filter will be applied during boot.
```

This program will guide you through several steps where you will define your VPN-1 & FireWall-1 configuration. At any later time, you can reconfigure these parameters by running cpconfig

The next step is to enter a license, enter "n" if you do not have a license handy at the moment or if you plan on using a centralized license which is a newly available feature in Firewall-1 NG. Otherwise enter y and manually enter the license or specify a license file:

Do you want to add licenses (y/n) [n] ? n

There is no need for group permission so just press "Enter" at the prompt:

[...]

Please specify group name [<RET> for no group permissions]: **"Enter"**

No group permissions will be granted. Is this ok (y/n) [y] ? y

[...]

Randomly press keys to fill up the bar between brackets:

Configuring Random Pool...

You are now asked to perform a short random keystroke session. The random data collected in this session will be used in various cryptographic operations.

[...]

Please keep typing until you hear the beep and the bar is full.

[.....] *

Thank you.

Enter the one time password required to set up secure communication with the management station

Configuring Secure Internal Communication...

The Secure Internal Communication is used for authentication between Check Point components:

Trust State: Uninitialized

Enter One Time Password:

Again One Time Password:

The Secure Internal Communication was successfully initialized

initial_module:

Compiled OK.

Hardening OS Security: Initial policy will be applied until the first policy is installed

Check Point Software Technologies Ltd.

Would You like to reboot the machine [y/n]: y

Security Benchmark and Scanning

After the minimizing and hardening process, the system is ready to be tested for functionality and audited for vulnerabilities. The testing consists of the following:

Host based Scan

To do this we will use the “Cis-scan” package, which is a non-invasive tool that scores the security of a system against the [Center of Information Security](#) developed level-1 Solaris BenchMark.

```
# zcat cis-san.tar.Z | tar -xvf -
# cd cis
# pkgadd -d CISscan
[...]
# cd /opt/CIS
# ./cis-scan
*** CIS Ruler v1.2.1 ***
Copyright 2001, 2002, The Center for Internet Security
```

Placing logs in /opt/CIS/cis-ruler-log.20020509-18:59:27.1797

```
Investigating system...this will take a few minutes...
...Found Solaris kernel version 5.8...
...Reading and caching /etc/passwd and /etc/shadow...
...Reading and caching /etc/shells...
...Reading and parsing /etc/vfstab for later use...
...Reading and caching /etc/system...
...Cataloging rc scripts...
[...]
Rating = 9.33 / 10.00
[...]
```

This is not a bad score, but when it comes to computer security overlooking anything is a dangerous bet. Digging into the items we find that we were penalized against:

```
# egrep “^Negative” /opt/CIS/cis-ruler-log.20020509-19:12:38.1842
Negative: 4.4 ip_forwarding not deactivated.
Negative: 4.4 ip6_strict_dst_multihoming isn’t activated.
Negative: 4.4 ip6_ignore_redirect isn’t set to 1.
Negative: 4.4 ip6 source routing (ip6_forward_src_routed) should be
deactivated
```

Negative: 4.4 tcp_ip_abort_cinterval should be at most 60,000 to avoid TCP flood problems.

Negative: 5.4 Couldn't read the /etc/rc2.d/S21perf file to check for system acctg.

Negative: 5.4 Couldn't open /var/spool/cron/crontabs/sys to look for sa1 and sa2
no system accounting.

We notice that most of the issues have to deal with IPV6 and accounting. These services were intentionally not enabled on the system. We could have turned off checking for these issues in cis-scan but we preferred to keep it there just in case someone inadvertently enabled IPV6.

Vulnerability Scan

Nessus, one of the best security scanners on the market (<http://www.nessus.org>), is used to scan for vulnerabilities on all TCP and UDP ports (1-65535). No vulnerabilities were reported which was expected since the firewall drops all incoming traffic except for ports permitted by the security policy between the firewall and the management station.

Firewall Policy/ Modules Communication Test

Since there is no policy that will fit every environment the firewall will be deployed in, we will create and test a base policy that should be used as the starting point for every deployment.

Communication Setup

A firewall has the task of enforcing a security policy defined by the security administrators. The Management server through the configuration of security rules conveys a security policy to the firewall. In order to test the firewall policy communication between the management server and module must be established. CheckPoint uses SIC (Secure Internal Communications), a certificate-based SSL (Secure Socket Layer) encrypted channel for communications between CheckPoint Modules (Management Server, VPN/FireWall...). The ICA (Internal Certificate authority) that resides on the management server generates the certificates used for authentication.

The Secure Internal Communication one time password entered at each end (during the installation process of the firewall) is used to secure a one-time link between the Management Server and this firewall. A certificate for this firewall is then delivered across this link. Once the certificate arrives at this machine, it can then communicate with other CheckPoint communicating components.

To set up communication,

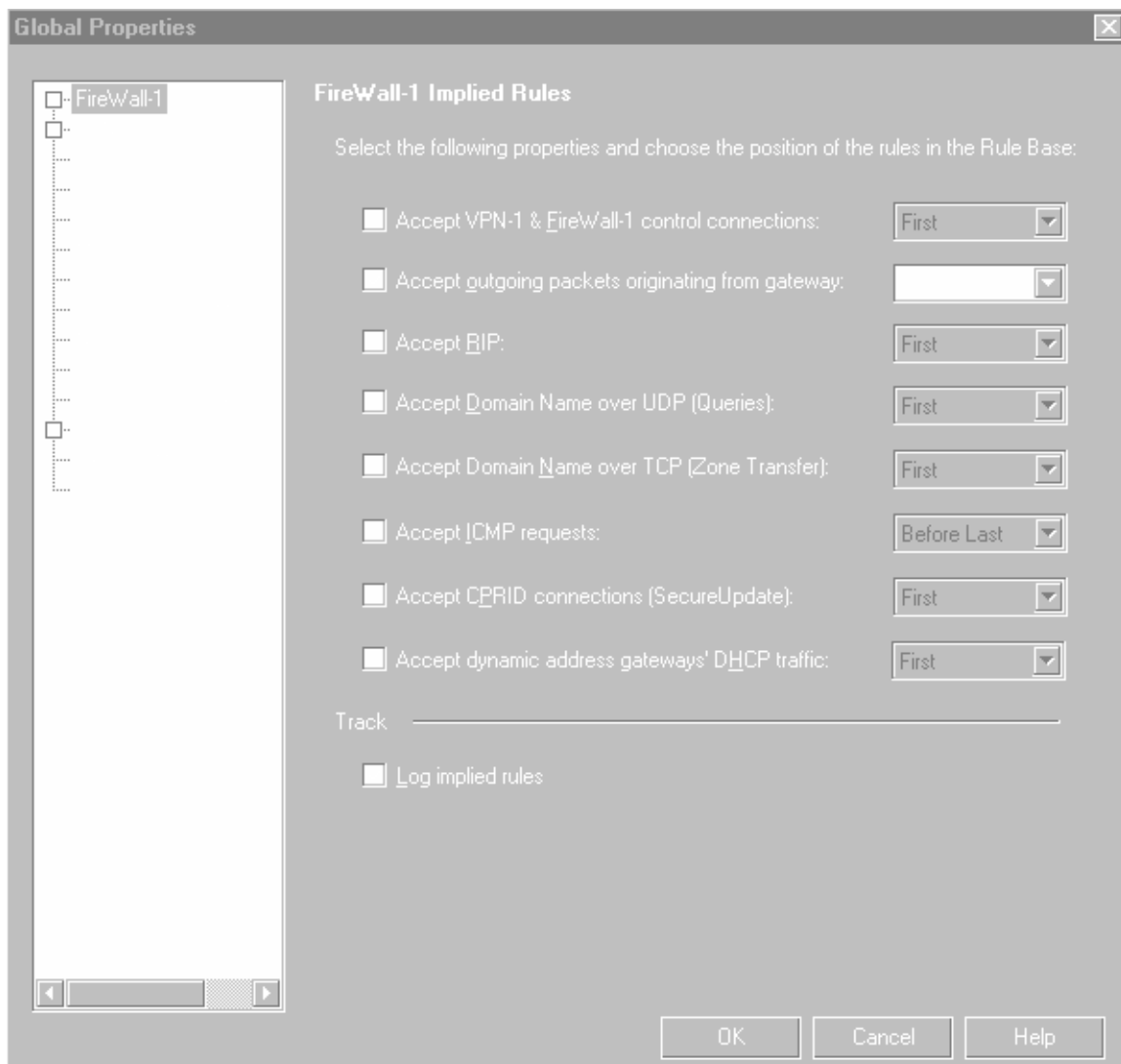
- Connect to the Management Server using the Policy Editor GUI by entering an administrator username/ password (created when the management server is installed or later added), and the IP address of the management station.
- Create an object for the Module, and give it a name and an IP address:
 - Choose Network Objects from the Manage menu, and click on New Workstation...
 - In the Workstation Properties — General page fill in the Module name and IP address, click on Topology and add all the firewall interfaces and their IP addresses.
 - Check the Check Point Products Installed box, and check the appropriate product.
 - Leave Managed by this Management Server radio button selected
 - Click Communications...The Communication window will open
 - Enter the one-time password — the SAME password entered when installation the firewall.
 - Confirm this password in the Verify Password field.
 - Click Initialize to start the Module initialization process.

At this point a certificate is issued to the Module. It is signed and securely transferred to the Module. For more detailed information consult CheckPoint's Getting Started manual.

Security Policy Setup

Checkpoint Firewall-1 by default ships with certain potentially vulnerable services open to the world. The appropriate measure to take is to disable all default services and explicitly enable the particular ones you need in the rulebase with appropriate restrictions, and source and destination addresses.

From the Policy Editor GUI policy menu item, click on Global Properties and set up the properties as the following image shows,



Next we need to create the rulebase. First we specify a stealth rule which blocks all direct access to the firewall. Only the firewall administration management stations need to have direct access to the firewall. The services allowed for that rule should be limited to the CheckPoint defined service group "Firewall1" and SSH traffic. SSH traffic is needed for troubleshooting and copying files like OS patches, service packs, and utilities to the firewall. Finally we install an explicit deny all rule in order to log any denied traffic. These logs will be sent to the management station for storage and possible analysis and report generation.

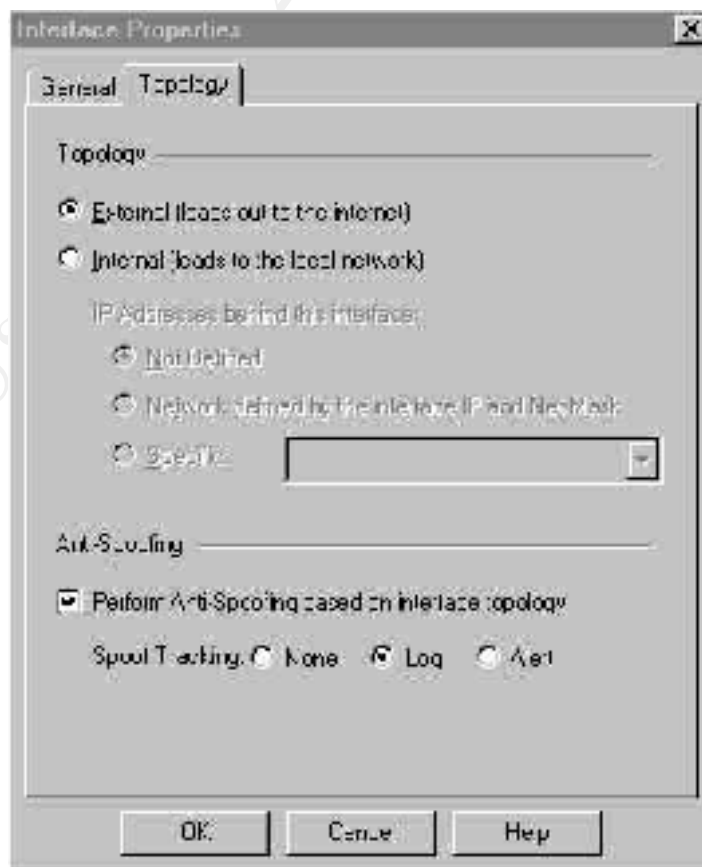
The above rules are created by clicking on add below in the Policy Editor Rules menu and then going to each file in the rule base and right clicking to add the components specified in the following image:

ID	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALLATION	TIME	COMMENT
1	Any	Local_3Network	Firewall1 SSH	Accept	Log	Policy Targets	Any	Administrative access only
2	Any	Local_3Network	Any	Deny	Log	Policy Targets	Any	Blocked Traffic
3	Any	Any	Any	Deny	Log	Policy Targets	Any	Blocked Traffic

Note that the Firewall1 service group includes the following ports: TCP ports 256, 257, 258, 259, 900 and UDP port 256 and 500. These ports may be further tightened (258 is for backward compatibility with version 4.x, UDP 256 is for FWZ encryption which is about to be phased out). In some situations more ports need to be added depending on the functionality of the firewall. The best way to determine what ports one needs to open between the management station and the firewall is to monitor the log files. With new releases and feature packs, Checkpoint keeps adding more functionality requiring more ports to be opened.

The last item to do is setting up antispoofing, which specifies that each incoming packet will be examined to ensure that its source IP address is consistent with the interface through which it entered the machine.

To accomplish this, click on the firewall object created earlier in the Policy Editor, click on topology, click on each defined interface, click on topology, and finally specify external for the outside interface and inside for all other interfaces. If more than one subnet exists on the internal network, a group encompassing all these subnets needs to be defined and assigned to the "Specific" option which needs to be checked.



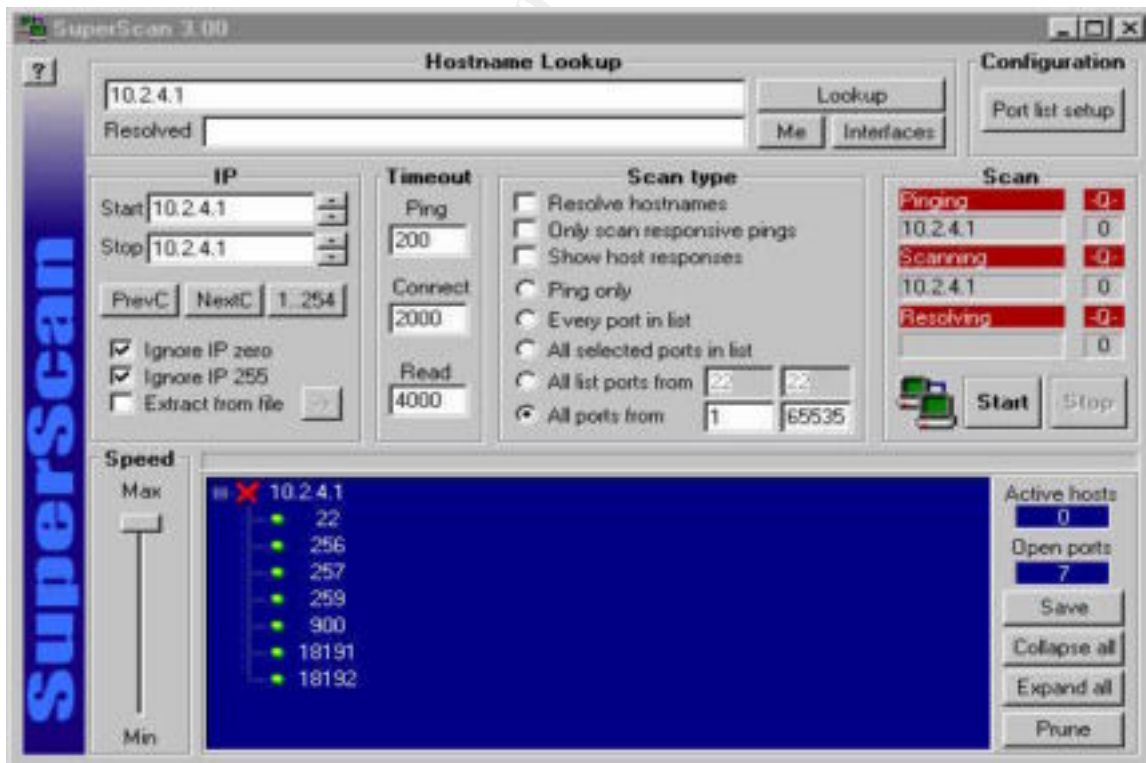
Once the policy is defined on the management station, it needs to be installed on the firewall. Clicking the install option in the Policy Editor policy menu will accomplish this task.

Testing the Policy

The default deployment firewall rulebase is tested in both directions: inbound and outbound. To do so, we generate traffic (just try to scan any address on the internal or external subnet from the opposite side) from the inside of the network destined to outside addresses and vice versa. As expected, the firewall correctly drops all connection attempts.

Port Scan

We perform a port scan from the management station against the firewall using [FoundStone superscan 3.0](#). The results show only a response from these ports, 256, 257, 259, 900, 18191, 18192, and 22, which are the ports that we have opened between the firewall and the management stations. Ports 18192 and 18191 are used for application status monitoring and the checkpoint daemon which we had running at the time of the scan.

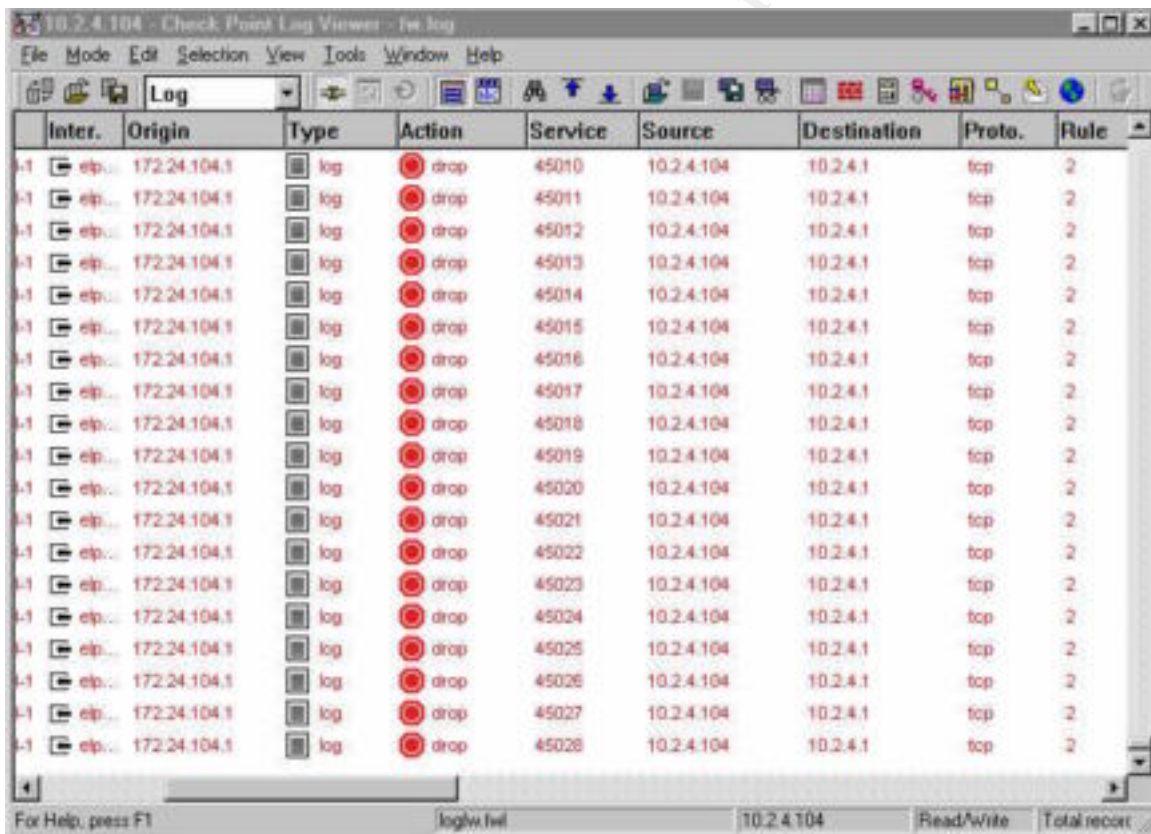


We also perform an Nmap scan sweep of all possible tcp and udp ports on the outside interface of the firewall from an external address and as expected all scan were closed:

```
# nmap -sU -p 1-65535 -sS 10.2.4.1
Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/)
All 131048 ports scanned on (10.2.4.1) are: closed
```

Nmap run completed -- 1 IP address (1 host up) scanned in 3538 seconds

Checking the CheckPoint logs by clicking on log viewer option in the Policy Editor Window menu option, we can clearly see the dropped packets originating from the scans (logs were the results of scanning all 65535 ports). This ensures that logging is properly working.



Inter.	Origin	Type	Action	Service	Source	Destination	Proto.	Rule
4-1	ep... 172.24.104.1	log	drop	45010	10.2.4.104	10.2.4.1	tcp	2
4-1	ep... 172.24.104.1	log	drop	45011	10.2.4.104	10.2.4.1	tcp	2
4-1	ep... 172.24.104.1	log	drop	45012	10.2.4.104	10.2.4.1	tcp	2
4-1	ep... 172.24.104.1	log	drop	45013	10.2.4.104	10.2.4.1	tcp	2
4-1	ep... 172.24.104.1	log	drop	45014	10.2.4.104	10.2.4.1	tcp	2
4-1	ep... 172.24.104.1	log	drop	45015	10.2.4.104	10.2.4.1	tcp	2
4-1	ep... 172.24.104.1	log	drop	45016	10.2.4.104	10.2.4.1	tcp	2
4-1	ep... 172.24.104.1	log	drop	45017	10.2.4.104	10.2.4.1	tcp	2
4-1	ep... 172.24.104.1	log	drop	45018	10.2.4.104	10.2.4.1	tcp	2
4-1	ep... 172.24.104.1	log	drop	45019	10.2.4.104	10.2.4.1	tcp	2
4-1	ep... 172.24.104.1	log	drop	45020	10.2.4.104	10.2.4.1	tcp	2
4-1	ep... 172.24.104.1	log	drop	45021	10.2.4.104	10.2.4.1	tcp	2
4-1	ep... 172.24.104.1	log	drop	45022	10.2.4.104	10.2.4.1	tcp	2
4-1	ep... 172.24.104.1	log	drop	45023	10.2.4.104	10.2.4.1	tcp	2
4-1	ep... 172.24.104.1	log	drop	45024	10.2.4.104	10.2.4.1	tcp	2
4-1	ep... 172.24.104.1	log	drop	45025	10.2.4.104	10.2.4.1	tcp	2
4-1	ep... 172.24.104.1	log	drop	45026	10.2.4.104	10.2.4.1	tcp	2
4-1	ep... 172.24.104.1	log	drop	45027	10.2.4.104	10.2.4.1	tcp	2
4-1	ep... 172.24.104.1	log	drop	45028	10.2.4.104	10.2.4.1	tcp	2

Other Tests

This part of the testing consists of verifying that the system is functioning as we have it configured. The following is a list of the items we test for:

- Verify that /usr partition is mounted as read-only, by trying to create a file.
- Verify that no “suid” program or script will execute on the /var partition
- Verify that logging is functioning correctly by checking the contents of the log files: /var/adm/log, /var/log/syslog, /var/log/authlog, /var/adm/loginlog, /var/adm/sulog, /var/opt/CPfw1-50/log (Checkpoint log files on the management station or locally if setup that way).
- Verify that the “break” sequence has been disabled. Sending the “break” signal should have no effect on the system.
- Verify that EEPROM commands are restricted by password challenge.
- Issue the “ps -ef “ command, you should see less than one screen full of processes running. Go through these processes and verify all the disabled daemons are not running. Mainly besides the Checkpoint daemons, cprid, cpwd, fwd, cpd, and fwboot, you should notice the SSH, prgnd, NTP daemons and some system daemons. The processes inetd, sendmail, nscd must not be running.

Creating Flash Archive

The Solaris Flash facility creates a point-in-time snapshot of Solaris OE, software patches, and applications installed on a system. This snapshot serves as a backup and may be accessed from an NFS server, HTTP, JumpStart, or devices local to the installation client, i.e. CD-ROM or a tape device, where it may be accessed by the Solaris installation client and written to the disk of a target system. After the archive is written to the installation client's disk, necessary customization to local parameters may be performed on that system, i.e. nsswitch.conf, resolv.conf, defaultrouter and so on...

To create an archive, use the “flarcreate” command as follows:

```
# mkdir /var/tmp/FLARIMAGE
#
# flarcreate -n "FW-IMAGE" -a sysadm@mailserver.com -R / \ -x
/var/tmp/FLARIMAGE /var/tmp/FLARIMAGE/FW-IMAGE.flar
[...]
```

Determining which filesystems will be included in the archive...

Determining the size of the archive...

The archive will be approximately 459.12MB.
Creating the archive...

To deploy the archive, the newly created file `/var/tmp/FLARIMAGE/FW-IMAGE.flar` needs to be copied to the deployment platform: CDROM, NFS server, or an HTTP server. To protect the archive against tampering, a checksum or the more reliable MD5 hash signature of the archive is essential. Solaris 8 comes with two checksum commands:

```
# /usr/5bin/sum /var/tmp/FLARIMAGE/FW-IMAGE.flar
28195 112305 /var/tmp/FLARIMAGE/FW-IMAGE.flar
```

or using `cksum`

```
#cksum cksum /var/tmp/FLARIMAGE/FW-IMAGE.flar
1282404939 57500120
```

To perform an MD5 hash, the package md5-6142000-sol8-sparc-local.gz needs to be downloaded, installed, and run over the archive. We will leave this as an exercise to the reader.

Installing a New System from the Flash Archive Using a Web Server

The Flash archive may be installed via NFS, web, CDROM, tape drive. In this section we will describe the web sourced installation procedure. To start the process, put the archive file `/var/tmp/FLARIMAGE/FW-IMAGE.flar` on a web server on the same subnet as the system being built. The web server can reside any http compliant platform ranging from Windows 2000 personal web server, to IIS, Apache....

To install the archive on the target system, follow the same procedure as the Solaris core installation specified above except choose the Flash install option when you are presented with the following screen:

[...]

There are two ways to install your Solaris software:

- "Standard" installs your system from a standard Solaris Distribution.
- "Flash" installs your system from one or more Flash Archives.

Esc-2_Standard F3_Go Back Esc-4_Flash F5_Exit F6_Help

On the following screen you must select a method to retrieve the Flash archive. The retrieval method depends on where the archive is stored. For example, if the archive is stored on a tape, select "Local Tape". In our case, choose HTTP since we will use the web to install.

Available Retrieval Methods

=====

- HTTP
- NFS
- Local File
- Local Tape
- Local Device

F2_Continue F5_Cancel F6_Help

Enter the path to your flash archive using the virtual directory name as in the following example:

First, specify the URL to access the Flash archive. For example:

URL: **http://www.host.com:80/path/to/archive.flar**

Second, specify the Proxy information needed to access the Flash archive. If no proxy is required, leave the "Proxy Host" field blank.

=====

URL: http://10.1.1.100/ FW-IMAGE.flar

Proxy Host:

Proxy Port: 0

F2_Continue F5_Cancel F6_Help

The system will try to locate the archive, and once it finds it, the installation process starts. It will take up to few hours depending on the size of the archive and network speed. Next configure the disk drive partitions and proceed as you would normally with any other installation. The end result should be a mirror copy, as far as content is concerned, of the original system created earlier.

Ongoing Maintenance

A firewall is the first line of defense. It is the gate to the fort and thus must be watched closely. The following is a minimal checklist of what must be done to keep the system security posture up to date:

Join a security site mailing list (www.securityfocus.com) and immediately test and then apply patches that affect the OS and applications installed on the firewall. The Solaris OS can be kept up-to-date by installing Solaris Patch Manager Base Version 1 for Solaris 8 (replaces PatchCheck and is available from <http://sunsolve.sun.com>). In order to use the Patch Manager, you must be registered with SunSolve Online (requires a Sun Support Contract). If used, the Patch Manager should not be part of the distribution archive. One way to accomplish this is to uninstall it before the archive is cut and reinstall afterward. Downloaded patches must first be tested on the staging system before deployment to the production gateways to ensure minimal service interruption. The patch manager can determine the required patches for a system, automatically download them, verify their digital signature, and automatically install most of them if instructed to do so. Since we have a minimal system installed on the firewall gateway and we also have disabled most of the services, a once a week patch check should be sufficient. A new FLAR must be built along with change log documentation describing the changes and what prompted them. Appendix G shows the Patch Manager Base Version 1 installation and setup procedure.

- Since firewall rule mis-configuration is one of the most common errors, after each change to the firewall policy someone with security expertise other than the administrator who made the change must verify the accuracy of management approved changes. Even though the firewall log files on the management station keep auditing track of these changes, a detailed change log or a change management system should be employed.
- Host and network based scans, similar to the one performed in earlier section, must take place on weekly basis, after each ruleset change, and upon patch application to verify proper security posture of the firewall. The scan results must be reconciled with the installed policies. The scans, their output, the reconciliation reports, and findings must be well documented and kept on file for auditing, incident handling, or forensics.
- The FLAR image must be maintained. Operating systems and application updates and patches must be applied and a new deployable archive must be created and deployed. A change log documenting all the changes from the previous version, and a version control system of the FLAR images should also be maintained along with the FLAR distribution.
- In a distributed CheckPoint firewall environment, all the configuration files, security policies, logs, and possibly licenses are stored on the management station, so daily backup of the firewall directories (`/var/opt/cp/w-1/conf`, `/var/opt/cp/w-1/log` and `/var/opt/cp/w-1/lib`) on the

management station is in order. Log data can get very large and will need to be trimmed. This data is critical since it may be used by Intrusion Detection Systems (IDS) and to correlate and reconstruct events. Going into details on these issues will go beyond the goal of this writing, but they are important enough to forgo mentioning them. Multiple sets of tape should be used and rotated in a round robin fashion allowing for the retention time specified in the site security policy. No regular backup is required on the firewall gateway, since it can be easily reproduced from the FLAR archive. What is required is site specific information like the IP addresses/netmasks of the interfaces, routing information, system name, root password and any other information : phone number/email of engineer at physical location of gateway, location of gateway, description of the firewall connectivity,

Conclusion

In this paper we discussed the process of securing and deploying a secure Solaris 8 based CheckPoint firewall enforcement module using The Solaris Security Toolkit JASS. We intentionally did not do any customization to the JASS script since an investment in this process would have veered us away from our goal. This one time process was captured in a distribution archive with the capability of being easily deployed and accessed from an NFS server, CDROM, tape, or an http server.

© SANS Institute 2000 - 2002
Author retains full rights.

Appendix A

Core Installation Package List

```
# pkginfo |wc -l
  102
# pkginfo
system  SMEvplr      SME platform links
system  SMEvplu      SME usr/platform links
system  SUNWadmr     System & Network Administration
              Root
system  SUNWatfsr   AutoFS, (Root)
system  SUNWatfsu   AutoFS, (Usr)
system  SUNWauda    Audio Applications
system  SUNWaudd    Audio Drivers
system  SUNWauddx   Audio Drivers (64-bit)
system  SUNWcar     Core Architecture, (Root)
system  SUNWcarx    Core Architecture, (Root) (64-
              bit)
system  SUNWcg6     GX (cg6) Device Driver
system  SUNWcg6x    GX (cg6) Device Driver (64-bit)
system  SUNWcsd     Core Solaris Devices
system  SUNWcsl     Core Solaris, (Shared Libs)
system  SUNWcslx    Core Solaris Libraries (64-bit)
system  SUNWcsr     Core Solaris, (Root)
system  SUNWcsu     Core Solaris, (Usr)
system  SUNWcsxu    Core Solaris (Usr) (64-bit)
system  SUNWdfb     Dumb Frame Buffer Device Drivers
system  SUNWdtcor   Solaris Desktop /usr/dt
              filesystem anchor
system  SUNWensqr   Ensoniq ES1370/1371/1373 Audio
              Device Driver (32-bit),(Root)
system  SUNWensqx   Ensoniq ES1370/1371/1373 Audio
              Device Driver (64-bit),(Root)
system  SUNWeridx   Sun RIO 10/100 Mb Ethernet
              Drivers (64-bit)
system  SUNWesu     Extended System Utilities
system  SUNWfcip    Sun FCIP IP/ARP over
              FibreChannel Device Driver
system  SUNWfcipx   Sun FCIP IP/ARP over FibreChannel Device
              Driver (64 bit)
system  SUNWfcp     Sun FCP SCSI Device Driver
system  SUNWfcpx    Sun FCP SCSI Device Driver (64-bit)
```


system	SUNWfctl	Sun Fibre Channel Transport layer
system	SUNWfctlx	Sun Fibre Channel Transport layer (64-bit)
system	SUNWftpr	FTP Server, (Root)
system	SUNWftpu	FTP Server, (Usr)
system	SUNWged	Sun Gigabit Ethernet Adapter Driver
system	SUNWglmr	Symbios 875/876 SCSI device driver, (Root)
system	SUNWglmx	Symbios 875/876 SCSI device driver, (Root)
system	SUNWhmd	SunSwift SBus Adapter Drivers
system	SUNWhmdx	SunSwift SBus Adapter Drivers (64-bit)
system	SUNWi15cs	X11 ISO8859-15 Codeset Support
system	SUNWi1cs	X11 ISO8859-1 Codeset Support
system	SUNWi2cr	Device drivers for I2C devices, (Root, 32-bit)
system	SUNWi2cx	Device drivers for I2C devices, (Root, 64-bit)
system	SUNWidecr	IDE device drivers
system	SUNWidecx	IDE device drivers- 64bit
system	SUNWider	IDE Device Driver, (Root)
system	SUNWigr	IGS CyberPro2010 Device Driver (ROOT)
application	SUNWigsu	IGS CyberPro2010 DDX (OW) Driver and Utilities
system	SUNWigsx	IGS CyberPro2010 64-bit Device Driver (ROOT)
system	SUNWkey	Keyboard configuration tables
system	SUNWkmp2r	PS/2 Keyboard and Mouse Device Drivers, (Root, 32-bit)
system	SUNWkmp2x	PS/2 Keyboard and Mouse Device Drivers, (Root, 64-bit)
system	SUNWkvm	Core Architecture, (Kvm)
system	SUNWkvmx	Core Architecture (Kvm) (64-bit)
system	SUNWlibms	Sun WorkShop Bundled shared libm
system	SUNWlmsx	Sun WorkShop Bundled 64-bit shared libm
system	SUNWloc	System Localization
system	SUNWlocx	System Localization (64-bit)
system	SUNWluxdx	Sun Enterprise Network Array sf Device Driver (64-bit)
system	SUNWluxop	Sun Enterprise Network Array firmware and utilities
system	SUNWluxox	Sun Enterprise Network Array libraries (64-bit)
system	SUNWm64	M64 Graphics System Software/Device Driver
system	SUNWm64x	M64 Graphics System Software/Device Driver (64-bit)
system	SUNWmdi	Sun Multipath I/O Drivers
system	SUNWmdix	Sun Multipath I/O Drivers (64- bit)
system	SUNWnamos	Northern America OS Support
system	SUNWnamow	Northern America OW Support
system	SUNWnistr	Network Information System,(Root)
system	SUNWnisu	Network Information System, (Usr)
system	SUNWpcelx	3COM EtherLink III PCMCIA Ethernet Driver
system	SUNWpcmci	PCMCIA Card Services, (Root)
system	SUNWpcmci	PCMCIA Card Services, (Usr)
system	SUNWpcmci	PCMCIA Card Services (64-bit)

system	SUNWpcm	PCMCIA memory card driver
system	SUNWpcser	PCMCIA serial card driver
system	SUNWpd	PCI Drivers
system	SUNWpdx	PCI Drivers (64-bit)
system	SUNWpl5u	Perl 5.005_03
system	SUNWpsdpr	PCMCIA ATA card driver
system	SUNWqfed	Sun Quad FastEthernet Adapter Driver
system	SUNWqfedx	Sun Quad FastEthernet Adapter Driver (64-bit)
system	SUNWmodu	Realmode Modules, (Usr)
system	SUNWses	SCSI Enclosure Services Device Driver
system	SUNWsesx	SCSI Enclosure Services Device Driver (64-bit)
system	SUNWsior	SuperIO 307 (plug-n-play) device drivers, (Root) (32-bit)
system	SUNWsiox	SuperIO 307 (plug-n-play) device drivers, (Root) (64-bit)
system	SUNWsndmr	Sendmail root
system	SUNWsndmu	Sendmail user
system	SUNWsolnm	Solaris Naming Enabler
system	SUNWssad	SPARCstorage Array Drivers
system	SUNWssadx	SPARCstorage Array Drivers (64-bit)
system	SUNWswmt	Install and Patch Utilities
system	SUNWtleux	Thai Language Environment user files (64-bit)
system	SUNWudf	Universal Disk Format 1.50, (Usr)
system	SUNWudfr	Universal Disk Format 1.50
system	SUNWudfrx	Universal Disk Format 1.50 (64-bit)
system	SUNWusb	USB Device Drivers
system	SUNWusbx	USB Device Drivers (64-bit)
system	SUNWwsr2	Solaris Product Registry & Web Start runtime support
system	SUNWxwdv	X Windows System Window Drivers
system	SUNWxwdvx	X Windows System Window Drivers (64-bit)
system	SUNWxwkey	X Windows software, PC keytables
system	SUNWxwmod	OpenWindows kernel modules
system	SUNWxwmox	X Window System kernel modules (64-bit)

Appendix B

Minimized OS package List (additional packages are needed for Checkpoint Firewall-1 to work)

system	SMEvplr	SME platform links
system	SMEvplu	SME usr/platform links
system	SUNWcar	Core Architecture, (Root)
system	SUNWcarx	Core Architecture, (Root) (64-bit)
system	SUNWcsd	Core Solaris Devices
system	SUNWcsl	Core Solaris, (Shared Libs)
system	SUNWcslx	Core Solaris Libraries (64-bit)
system	SUNWcsr	Core Solaris, (Root)
system	SUNWcsu	Core Solaris, (Usr)
system	SUNWcsxu	Core Solaris (Usr) (64-bit)
system	SUNWensqr	Ensoniq ES1370/1371/1373 Audio Device Driver (32-bit), (Root)
system	SUNWesu	Extended System Utilities
system	SUNWglmr	Symbios 875/876 SCSI device driver, (Root)
system	SUNWhmd	SunSwift SBus Adapter Drivers
system	SUNWhmdx	SunSwift SBus Adapter Drivers (64-bit)
system	SUNWidecr	IDE device drivers
system	SUNWider	IDE Device Driver, (Root)
system	SUNWkvm	Core Architecture, (Kvm)
system	SUNWkvmx	Core Architecture (Kvm) (64-bit)
system	SUNWlibms	Sun WorkShop Bundled shared libm
system	SUNWlmsx	Sun WorkShop Bundled 64-bit shared libm
system	SUNWloc	System Localization
system	SUNWlocx	System Localization (64-bit)
system	SUNWpd	PCI Drivers
system	SUNWpdx	PCI Drivers (64-bit)
system	SUNWqfed	Sun Quad FastEthernet Adapter Driver
system	SUNWqfedx	Sun Quad FastEthernet Adapter Driver (64-bit)

Appendix C

Packages to Be Removed

system	SUNWadmr	System & Network Administration
system	SUNWatfsr	AutoFS, (Root)
system	SUNWatfsu	AutoFS, (Usr)
system	SUNWauda	Audio Applications
system	SUNWaudd	Audio Drivers
system	SUNWauddx	Audio Drivers (64-bit)
system	SUNWcg6	GX (cg6) Device Driver
system	SUNWcg6x	GX (cg6) Device Driver (64-bit)
system	SUNWdfb	Dumb Frame Buffer Device Drivers
system	SUNWdtcor	Solaris Desktop /usr/dt filesystem anchor
system	SUNWensqx	Ensoniq ES1370/1371/1373 Audio Device Driver (64-bit),(Root)
system	SUNWeridx	Sun RIO 10/100 Mb Ethernet Drivers (64-bit)
system	SUNWfcip	Sun FCIP IP/ARP over FibreChannel Device Driver
system	SUNWfcipx	Sun FCIP IP/ARP over FibreChannel Device Driver (64 bit)
system	SUNWfcp	Sun FCP SCSI Device Driver
system	SUNWfcpx	Sun FCP SCSI Device Driver (64-bit)
system	SUNWfctl	Sun Fibre Channel Transport layer
system	SUNWfctlx	Sun Fibre Channel Transport layer (64-bit)
system	SUNWftpr	FTP Server, (Root)
system	SUNWftpu	FTP Server, (Usr)
system	SUNWged	Sun Gigabit Ethernet Adapter Driver
system	SUNWhmd	SunSwift SBus Adapter Drivers
system	SUNWhmdx	SunSwift SBus Adapter Drivers (64-bit)
system	SUNWi15cs	X11 ISO8859-15 Codeset Support
system	SUNWi1cs	X11 ISO8859-1 Codeset Support
system	SUNWi2cr	Device drivers for I2C devices, (Root, 32-bit)
system	SUNWi2cx	Device drivers for I2C devices, (Root, 64-bit)
system	SUNWider	IDE Device Driver, (Root)
system	SUNWigr	IGS CyberPro2010 Device Driver (ROOT)
application	SUNWigsu	IGS CyberPro2010 DDX (OW) Driver and Utilities
system	SUNWigsx	IGS CyberPro2010 64-bit Device Driver (ROOT)
system	SUNWkey	Keyboard configuration tables
system	SUNWkmp2r	PS/2 Keyboard and Mouse Device Drivers, (Root, 32-bit)
system	SUNWkmp2x	PS/2 Keyboard and Mouse Device Drivers, (Root, 64-bit)
system	SUNWluxdx	Sun Enterprise Network Array sf Device Driver (64-bit)

system	SUNWluxop	Sun Enterprise Network Array firmware and utilities
system	SUNWluxox	Sun Enterprise Network Array libraries (64-bit)
system	SUNWm64	M64 Graphics System Software/Device Driver
system	SUNWm64x	M64 Graphics System Software/Device Driver (64-bit)
system	SUNWmdi	Sun Multipath I/O Drivers
system	SUNWmdix	Sun Multipath I/O Drivers (64-bit)
system	SUNWnamos	Northern America OS Support
system	SUNWnamow	Northern America OW Support
system	SUNWnisr	Network Information System,(Root)
system	SUNWnisu	Network Information System, (Usr)
system	SUNWpcelx	3COM EtherLink III PCMCIA Ethernet Driver
system	SUNWpcmci	PCMCIA Card Services, (Root)
system	SUNWpcmcu	PCMCIA Card Services, (Usr)
system	SUNWpcmcx	PCMCIA Card Services (64-bit)
system	SUNWpcmem	PCMCIA memory card driver
system	SUNWpcser	PCMCIA serial card driver
system	SUNWpd	PCI Drivers
system	SUNWpdx	PCI Drivers (64-bit)
system	SUNWpl5u	Perl 5.005_03
system	SUNWpsdpr	PCMCIA ATA card driver
system	SUNWqfed	Sun Quad FastEthernet Adapter Driver
system	SUNWqfedx	Sun Quad FastEthernet Adapter Driver (64-bit)
system	SUNWmodu	Realmode Modules, (Usr)
system	SUNWses	SCSI Enclosure Services Device Driver
system	SUNWsesx	SCSI Enclosure Services Device Driver (64-bit)
system	SUNWsior	SuperIO 307 (plug-n-play) device drivers, (Root) (32-bit)
system	SUNWsiox	SuperIO 307 (plug-n-play) device drivers, (Root) (64-bit)
system	SUNWsndmr	Sendmail root
system	SUNWsndmu	Sendmail user
system	SUNWsolnm	Solaris Naming Enabler
system	SUNWssad	SPARCstorage Array Drivers
system	SUNWssadx	SPARCstorage Array Drivers (64-bit)
system	SUNWswmt	Install and Patch Utilities
system	SUNWtleux	Thai Language Environment user files (64-bit)
system	SUNWudf	Universal Disk Format 1.50, (Usr)
system	SUNWudfr	Universal Disk Format 1.50
system	SUNWudfrx	Universal Disk Format 1.50 (64-bit)
system	SUNWusb	USB Device Drivers
system	SUNWusbx	USB Device Drivers (64-bit)
system	SUNWwsr2	Solaris Product Registry & Web Start runtime support
system	SUNWxwdv	X Windows System Window Drivers
system	SUNWxwdvx	X Windows System Window Drivers (64-bit)
system	SUNWxwkey	X Windows software, PC keytables

system	SUNWxwmod	OpenWindows kernel modules
system	SUNWxwmox	X Window System kernel modules (64-bit)

© SANS Institute 2000 - 2002, Author retains full rights.

Appendix D

Banners

```
#more /etc/issue
```

```
#####
```

```
# This system is for the use of authorized users only. Individuals using this computer system without #authority, or excess of their authority, are subject to having all of their activities on this system #monitored and recorded by system personnel. In the course of monitoring individuals improperly #using this system, or in the course of system maintenance, the activities of authorized users may also be #monitored.
```

```
# Anyone using this system expressly consents to such monitoring and is advised that if such monitoring #reveals possible evidence of criminal activity, system personnel may provide the evidence of such #monitoring to law enforcement officials.
```

```
#####
```

```
#more /etc/motd
```

```
#####
```

```
# This system is for the use of authorized users only. Individuals using this computer system without #authority, or excess of their authority, are subject to having all of their activities on this system #monitored and recorded by system personnel. In the course of monitoring individuals improperly #using this system, or in the course of system maintenance, the activities of authorized users may also be #monitored.
```

```
# Anyone using this system expressly consents to such monitoring and is advised that if such monitoring #reveals possible evidence of criminal activity, system personnel may provide the evidence of such #monitoring to law enforcement officials.
```

```
#####
```

```
# more /etc/default/telnetd  
BANNER="Authorized Use Only"
```

```
# more /etc/default/ftpd  
BANNER="Authorized Use Only"  
UMASK=022
```

Appendix E

/etc/init.d/prngd⁴

```
#!/bin/sh

pid=`/usr/bin/ps -e | /usr/bin/grep prngd | /usr/bin/sed -e 's/^ *//'`
-e 's/ .*//'\`
case $1 in
'start')
    /usr/local/bin/prngd /var/spool/prngd/pool
    ;;
'stop')
    if [ "${pid}" != "" ]
    then
        /usr/bin/kill ${pid}
    fi
    ;;
*)
    echo "usage: /etc/init.d/prngd {start|stop}"
    ;;
esac
```

/etc/init.d/sshd⁵

```
#!/bin/sh

pid=`/usr/bin/ps -e | /usr/bin/grep sshd | /usr/bin/sed -e 's/^ *//'` -
e 's/ .*//'\`
case $1 in
'start')
    /usr/local/sbin/sshd
    ;;
'stop')
    if [ "${pid}" != "" ]
    then
        /usr/bin/kill ${pid}
    fi
    ;;
*)
    echo "usage: /etc/init.d/sshd {start|stop}"
    ;;
esac
```

⁴ Installing OpenSSH Packages, <http://www.sunfreeware.com/openssh.html>

⁵ Installing OpenSSH Packages, <http://www.sunfreeware.com/openssh.html>

Appendix F

SSH server config file

Port 22
Protocol 2,1
ListenAddress 0.0.0.0

HostKey /usr/local/etc/ssh_host_key
HostKey /usr/local/etc/ssh_host_dsa_key
KeyRegenerationInterval 900
ServerKeyBits 1024

SyslogFacility AUTH
LogLevel INFO

LoginGraceTime 600
PermitRootLogin no
StrictModes yes

RhostsAuthentication no
IgnoreRhosts yes
RhostsRSAAuthentication no
HostbasedAuthentication no

PasswordAuthentication yes
PermitEmptyPasswords no

X11Forwarding no

PrintMotd yes
PrintLastLog yes
#KeepAlive no
UseLogin no

© SANS Institute 2000 - 2002, Author retains full rights.

Appendix G

Patch Manager Base 1.0 Install Procedure

To install the Patch manager download the zipped tar file from <http://sunsolve.sun.com/> and copy it to the /usr/local directory

```
# gunzip pproSunOSsparc5.8jre2.1.tar.gz
# tar -xvf pproSunOSsparc5.8jre2.1.tar
# cd pproSunOSsparc5.8jre2.1
# ./setup
```

Update the PATH and MANPATH variables to include the new software and man pages:

```
# PATH="/opt/SUNWppro/bin:/usr/sadm/bin:${PATH}"; export PATH
# MANPATH="/opt/SUNWppro/man:${MANPATH}"; export MANPATH
```

Import Sun root certificates into the Java system keystore. To import the certificates, run the following command:

```
# /usr/j2se/jre/bin/keytool -import -alias smicacert \
-file /etc/certs/SUNW/smicacert.b64 -keystore \
/usr/j2se/jre/lib/security/cacerts
[...]
Trust this certificate? [no]: yes
Certificate was added to keystore
```

```
# /usr/j2se/jre/bin/keytool -import -alias smirootcacert \
-file /etc/certs/SUNW/smirootcacert.b64 -keystore \
/usr/j2se/jre/lib/security/cacerts
[...]
Enter keystore password: xyzhsjsjs
[...]
trust this certificate? [no]: yes
Certificate was added to keystore
```

Import Sun patch signing certificate into the Java system keystore. To import the certificates

```
# /usr/j2se/bin/keytool -import -alias patchsigning -file \
/opt/SUNWppro/etc/certs/patchsigningcert.b64 -keystore \
/usr/j2se/jre/lib/security/cacerts
```

```
[...]  
Enter keystore password: xyzhsjsjs  
[...]  
trust this certificate? [no]: yes  
Certificate was added to keystore
```

Set your SunSolve User ID and password:

```
# pprosetup -u user_id  
# echo your_passwd > /opt/SUNWppro/lib/.sunsolvepw
```

Select your patch server based on your location:

```
Americas (default) https://americas.patchmanager.sun.com/patchmanager/  
Europe https://emea.patchmanager.sun.com/patchmanager/  
Japan https://japan.patchmanager.sun.com/patchmanager/
```

Set the server:

```
# pprosetup -P https://americas.patchmanager.sun.com/patchmanager/
```

Set the Patch Manager to analyze and download the required patches on a weekly basis, beginning on the zeroth day of the week (Sunday) at 11:00pm local time and not to install patches automatically in non-interactive mode:

```
# pprosetup -p none -W 0 -s 23:00:00
```

The default download location for the automated download of patches is set to `var/spool/pkg/patchpro` .

References

Pomerantz, Hal, *Solaris Security Step by Step v. 2.0*, Sans Institute, 2002

Noordergraaf, Alex, and Brunette, Glenn, *Jumpstart Architecture and Security Scripts Toolkit - Part 3 - Updated for version 0.2*, Sun BluePrints OnLine, November 2000.

<http://www.sun.com/blueprints/1100/jssec3-updt1.pdf>

Noordergraaf, Alex and Watson, Keith, *Solaris Operating Environment Minimization for Security*, Sun BluePrints OnLine, December 1999.

<http://www.sun.com/blueprints/1299/minimization.pdf>

Noordergraaf, Alex and Watson, Keith, *Solaris Operating Environment Security*, Sun BluePrints OnLine, January 2000.

<http://www.sun.com/blueprints/0100/security.pdf>

Noordergraaf, Alex and Watson, Keith, *Solaris™ Operating Environment Minimization for Security: A Simple, Reproducible and Secure Application Installation Methodology*, Sun BluePrints OnLine, November 2000

<http://www.sun.com/blueprints/>

Installing OpenSSH Packages, <http://www.sunfreeware.com/openssh.html>

Lance Spitzner, *Armoring Solaris II*, 2001

<http://www.enteract.com/~lspitz/pubs.html>

The Solaris Tools archive (the benchmark document and scoring tools)

<http://www.cisecurity.org>

Solaris man pages