Global Information Assurance Certification Paper

Securing a Solaris Check Point Firewall
Lee R. Baker
March 11, 2001

Introduction

A firewall is usually the first line of defense protecting your internal network from the Internet. Being the first line of defense all traffic from the Internet, both malicious and desired, will be seen by the firewall and it will be the first point of attack for any malicious traffic. Because it is the entry point to your internal network it should be made as secure as possible. This paper will outline the steps require to build a secure firewall using the Sun Solaris operating system and Check Point FireWall-1 firewall software.

The steps required to accomplish this are:

- Install the Solaris operating system
- Install patches to the operating system
- Remove any unnecessary packages
- Add packages required for firewall software
- Add optional operating system packages for additional functionality
- Secure the operating system
- Secure the network
- Install the firewall software

The safest method of performing the above steps is with the system connected to an isolated network. To get patches and other files to this system use a second system that can be connect to the Internet for downloading files and than disconnected and connect to the isolated network.

Install the Operating System

When installing an operating system for a firewall you want minimize the operating environment as much as possible. The Solaris operating environment can be loaded from the Solaris operating system CD with one of the following four installation clusters:

- Core
- End User
- Developer
- Entire Distribution

The Core cluster is the one that you want to install. This will install the minimum packages possible.

During the installation, you will be asked to partition the system disk. There are many different opinions about how to partition a system disk, this is recommended as a minimum:

/	- all software
/var	- for operating system logs
swap	- will contain both swap and /tmp
/logs	- if your firewall will be logging to this system

With this configuration, you are protecting the root partition from filling up with either operating system or firewall logs.

Install Operating System Patches

Next, you need to install the operating system Recommended, Security and Kernel Update patches. All of these patches can be obtained from the SunSolve Web site at http://sunsolve.sun.com. These patches are free for downloading from this site and don't require a service contract. It is important that these patches be applied before any changes are made to minimize or secure the operating system because some of these patches could install new versions of the files that you will be modifying to secure the operating system.

It is important to keep the system updated with the most current patches. The following note is from a Sun BluePrints [2] paper and cautions about installing patches after the operating system has been minimized and secured.

> **Note** – Once package removal and system configuration has begun, patch installation should *only* be done after the README and pkgmap of the package is reviewed for possible conflicts.

Remove Unnecessary Packages

Now that the operating system has been installed and patched, you can remove unnecessary packages. Since different packages are required depending on the operating system version and the hardware that the system is running the package removal example below is for a headless Sun Enterprise Ultra with Solaris 2.7 installed. In this case, the Core cluster will have installed 39 packages of which 20 are not required to run Check Point FireWall-1 version 4.0. The following packages can be removed using the *pkrm* command:

```
SUNWsndmr       Sendmail root
SUNWsndmu       Sendmail user
SUNWftpr        FTP Server, (Root)
SUNWftpu        FTP Server, (Usr)
SUNWpcelx       3COM EtherLink III PCMCIA Ethernet Driver
SUNWpcmci       PCMCIA Card Services, (Root)
SUNWpcmcu       PCMCIA Card Services, (Usr)
SUNWpcmem       PCMCIA memory card driver
SUNWpcser       PCMCIA serial card driver
SUNWpsdpr       PCMCIA ATA card driver
SUNWxwdv        X Windows System Window Drivers
SUNWxwmod       OpenWindows kernel modules
```

```
SUNWnisr        Network Information System, (Root)
SUNWnisu        Network Information System, (Usr)
SUNWcg6         GX (cg6) Device Driver
SUNWadmr        System & Network Administration Root
SUNWdtcor       Solaris Desktop /usr/dt filesystem anchor
SUNWsolnm       Solaris Naming Enabler
SUNWatfsr       AutoFS, (Root)
SUNWatfsu       AutoFS, (Usr)
```

Add Packages Required by Firewall

The Check Point FireWall-1 software requires three packages that were not in the Core cluster. These packages are on the Solaris 2.7 CD that must be mount. Use the following commands to install the packages:

```
mount -F hsfs -o ro /dev/dsk/c0t2d0s0 /cdrom
cd /cdrom/Solaris_2.7/Product
pkgadd -d . packagename
```

The three packages that need to be installed are:

```
SUNWlibC        Sun Workshop Compilers Bundled libC
SUNWter         Terminal Information
SUNWscpu        Source Compatibility, (Usr)
```

Add Optional Packages

The operating system now has everything that is required to run the Check Point FireWall-1 software, but to make management and trouble shooting of the system easier some of the following packages could be added.

Manpages:

```
SUNWdoc         Documentation Tools
SUNWman         On-Line Manual Pages
```

Snoop for tracking down networking problems:

```
SUNWfns         Federated Naming System
```

Secure Operating System

The operating system now has the minimum number of packages. The next thing needed is to secure the operating system by turning on certain security features, disabling unneeded services and turning on additional logging.

The first thing to do is to turn on console security. This is done by setting the OpenBoot PROM Security Mode; the following commands will set the security mode that will prevent EEPROM changes and hardware command execution while at the OpenBoot PROM prompt.

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

The next thing to do is to eliminate unnecessary accounts from the /etc/passwd and /etc/shadow files. The *smtp, nuucp, uucp,* and *listen* accounts can be eliminated using the following command for each account:

```
# passmgmt –d smtp
```

The *cron* and *at* commands are used to execute commands at sometime in the future and access to these commands can be controlled with the files in the /usr/lib/cron directory. This directory can contain at.deny, at.allow, cron.deny, and cron.allow files; these files control access to the *cron* and *at* commands. If none of these files exist than only root can use these commands, which on most firewalls is desired, so these files should be removed from the above directory.

The ability to of the Solaris operating systems kernel to execute system stack code should be turned off and attempts to execute system stack code should be logged by adding the following two lines to the /etc/system file:

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

The following line should be added to the /etc/system file to make sure that no core files are created when an executing program receives a certain signal and terminates:

```
set sys:coredumpsize = 0
```

Use the following commands from Sun BluePrints [3] to change the root file creation mask from the default of 000 to 022:

```
echo "umask 022" > /etc/init.d/umask.sh
chmod 744 /etc/init.d/umask.sh
chgrp sys /etc/init.d/umask.sh
for d in /etc/rc?.d; do
    ln /etc/init.d/umask.sh $d/S00umask.sh
done
```

Edit the /etc/syslog.conf file and uncomment the following line to enable logging of authentication messages to the /var/log/authlog file.

```
#auth.notice ifdef('LOGHOST', /var/log/authlog, @loghost)
```

Create the /var/adm/loginlog file with the following command to log failed login attempts:

```
touch /var/adm/loginlog
```

Now disable, as many unneeded system services as possible to eliminate the possibility of someone attacking holes in these services. The easiest way to disable a service is to rename the service in the appropriate /etc/rc?.d directory. To disable a service change the capital S at the beginning of the script name with a small s. The following services can be disabled in their respective directories:

/etc/rc2.d
S71rpc – portmapper daemon
S73nfs.client – for mounting NFS remote filesystems

/etc/rc3.d
S15nfs.server – to share a local filesystem

Secure Network

The operating system is minimized and secured; now it is time to secure the network interfaces from attack.

The following commands should be entered into the /etc/init.d/inetinit script:

```
ndd -set /dev/ip ip_respond_to_echo_broadcast 0
ndd -set /dev/ip ip_forward_directed_broadcasts 0
ndd -set /dev/ip ip_respond_to_timestamp 0
ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
ndd -set /dev/ip ip_forward_src_routed 0
ndd -set /dev/ip ip_send_redirects 0
ndd -set /dev/ip ip_ignore_redirect 1
```

These setting will help protect the network interfaces against some problems with broadcasts, timestamp requests, source routed packets, and redirects.

Now edit the /etc/default/inetinit file to turn on truly randomized initial sequence numbers for all TCP connections. This will help protect the network against session hijacking and ip spoofing. Edit the file and change the following line from the default setting of 1 to 2:

```
TCP_STRONG_ISS=1
```

The next thing that needs to be decided is how you are going to connect to the firewall system. The most secure way is to only connect from a terminal connected to a serial port, but this very seldom a practical way to manage a firewall. The next best is to use secure shell from http://www.openssh.com or http://www.ssh.com. The least secure is to use telnet and ftp. If you are using the first two options you can eliminate the inetd daemon by renaming or deleting the /etc/inetd.conf file. If you have to use the third option you will have to edit the /etc/inetd.conf file and comment out everything but the two lines below:

```
ftp     stream  tcp     nowait  root    /usr/sbin/in.ftpd  in.ftpd
telnet  stream  tcp     nowait  root    /usr/sbin/in.telnetd  in.telnetd
```

Using this option it is also a good idea to use TCP Wrappers from the tools section of this site http://www.porcupine.org/wietse to protect and log access via ftp and telnet.

Install Firewall Software

The operating system and network have now been secured and the Check Point FireWall-1 software can be installed. The software comes on a CD as a Solaris package and installs using the *pkgadd* command.

After installing the software, protect your network from IP spoofing by using the anti-spoofing feature of the Check Point FireWall-1 software. If you are using telnet and ftp to access the firewall computer, make sure that you only allow authenticated sessions to protect against password snooping.

Conclusion

The firewall computer can now be considered secure and can be moved from the isolated network to your production network. What has been outline above is a manual method of minimizing and securing a firewall. There are also some more automated methods of doing the same thing. The sites below are some places to look for these automated methods:

http://www.fish.com/~brad/titan/Titan-Docs/TITAN_documentation.html
http://www.yassp.org/
http://www.enteract.com/~lspitz/armoring.html

Sources:

[1] Laggui, Dexter D., "How to Strip Down a Unix OS". URL: http://support.checkpoint.com/kb/docs/public/os/solaris/pdf/strip-sunserver.pdf (9 Feb 01)

[2] Noordergraaf, Alex, "Solaris™ Operating Environment Minimization for Security: A Simple, Reproducible and Secure Application Installation Methodology". Nov 00 URL: http://www.sun.com/blueprints/1100/minimize-updt1.pdf (9 Feb 01)

[3] Noordergraaf, Alex and Watson, Keith, "Solaris™ Operating Environment Security". Jan 00 URL: http://www.sun.com/blueprints/0100/security.pdf (9 Feb 01)

[4] Spitzner, Lance, "Armoring Solaris". 22 Oct 00 URL: http://www.enteract.com/~lspitz/armoring.html (9 Feb 01)

[5] Watson, Keith and Noordergraaf, Alex, “Solaris™ Operating Environment Network Settings for Security”. Dec 00 URL: http://www.sun.com/blueprints/1200/network-updt1.pdf (9 Feb 01)