Check Point Software Technologies Ltd.

Minimum OS Installation Guidelines
for
Linux VPN-1/FireWall-1 Appliance

CHECK POINT™
Software Technologies Ltd.
We Secure the Internet.

Date: Apr/10/2002
Version 1.4
Updated for
Check Point VPN-1/FireWall-1 NG FP2
And
Linux Red Hat 7.2

Table of Contents

1 Overview

This document is intended to guide Check Point Appliance partners in their development of Linux based VPN-1/FireWall-1 devices. The material outlined here helps to prepare Linux appliances for OPSEC certification. However, not all of the security tests run against the appliance are outlined. All appliance vendors are expected to take steps to harden their product. This document should only be used as a guide.

This document is created under the assumption that the appliance will be running VPN-1/FireWall-1 and some form of management software (ssh and/or an HTTPS based UI).

- Strictly control and monitor an HTTPS based UI. There must be a documented way to disable all remote management features if the client desires. Complete steps to secure Apache are not included within this document. More information can be found here: http://httpd.apache.org/docs/misc/security_tips.html.

Remote management features of the appliance represent the greatest security risk to the device. It is crucial that all possible steps are taken to avoid compromising the VPN-1/FireWall-1 through a partner management feature. Special attention will be given to this area during OPSEC certification.

As in any software based security procedure it is crucial to track the known vulnerabilities. Patches and updates should be applied prudently.

Additional Linux security references:

http://www.bastille-linux.org
http://www.linuxsecurity.com
http://www.securityfocus.com
http://www.linuxdoc.org/LDP/solrhe/Securing-Optimizing-Linux-RH-Edition-v1.3.pdf
http://xforce.iss.net/

2 Version Information

This information is used to correlate the minimum OS installation recommendations with Linux options: Please check the latest product release notes to determine which versions of the following should be used. In general, it is best to apply the latest patches. The security patches should be applied prior to installation of VPN-1/FireWall-1. This guide is applicable for Check Point VPN-1/FireWall-1 version NG FP-2.
Version of Red Hat Linux: 7.2 (nothing beyond 7.2 is currently supported by Check Point)
Version of Linux Kernel: RH 7.2 distribution comes with 2.4.7-10. Currently Check Point supports only 2.4.9-13.

Check here for latest information:
http://www.redhat.com/support/errata/rh72-errata.html
ftp://updates.redhat.com/7.2/en/os/i386

3 Minimum OS Installation Guidelines

3.1 Installed Packages / Service Configurations

A basic installation of Red Hat Linux without any “pre-defined package collections” should be done. In order to do such installation, one should select “Custom” installation, and deselect all pre-defined package collections when asked. Make sure the packages are distributed from a reliable source (RH cd) or checked via rpm -k and/or gnupg. The restricted install results in the following 127 packages:

```
Base RH-packages:

Anacron-2.3-17
apmd-3.0final-34
ash-0.3.7-2
at-3.1.8-20
Authconfig-4.1.19-1
Basesystem-7.0-2
bash-2.05-8
bdflush-1.5-17
bzip2-1.0.1-4
bzip2-libs-1.0.1-4
chkconfig-1.2.24-1
console-tools-19990829-36
cpio-2.4.2-23
cracklib-2.7-12
cracklib-dicts-2.7-12
crontabs-1.10-1
cyrus-sasl-1.5.24-20
cyrus-sasl-md5-1.5.24-20
cyrus-sasl-plain-1.5.24-20
db1-1.85-7
db2-2.4.14-7
db3-3.2.9-4
dev-3.2-5
dhcpcd-1.3.18pl8-13
diffutils-2.7.2-2
dosfstools-2.7-1
e2fsprogs-1.23-2
ed-0.2-21
eject-2.0.9-2
file-3.35-2
filesystem-2.1.6-2
fileutils-4.1-4
findutils-4.1.7-1
gawk-3.1.0-3
```

```
gdbm-1.8.0-10
glib-1.2.10-5
glibc-2.2.4-13
glibc-common-2.2.4-13
gpm-1.19.3-20
grep-2.4.2-7
groff-1.17.2-3
grub-0.90-11
gzip-1.3-15
hdparm-4.1-2
hotplug-2001_04_24-11
indexhtml-7.2-1
info-4.0b-3
initscripts-6.40-1
ipchains-1.3.10-10
iproute-2.2.4-14
iptables-1.2.3-1
iputils-20001110-6
kbdconfig-1.9.14-1
kernel-2.4.7-10
krb5-libs-1.2.2-13
ksymoops-2.4.1-1
kudzu-0.99.23-1
less-358-21
libstdc++-2.96-98
libtermcap-2.0.8-28
lilo-21.4.4-14
logrotate-3.5.9-1
lokkit-0.50-6
losetup-2.11g-5
mailcap-2.1.6-1
mailx-8.1.1-22
MAKEDEV-3.2-5
man-1.5i2-6
mingetty-0.9.4-18
mkbootdisk-1.4.2-3
mkinitrd-3.2.6-1
mktemp-1.5-11
modutils-2.4.6-4
mount-2.11g-5
mouseconfig-4.23-1
ncurses-5.2-12
net-tools-1.60-3
netconfig-0.8.11-7
newt-0.50.33-1
ntsysv-1.2.24-1
openldap-2.0.11-13
openssl-0.9.6b-8
pam-0.75-14
parted-1.4.16-8
passwd-0.64.1-7
pciutils-2.1.8-23
pcre-3.4-2
popt-1.6.3-1.03
procmail-3.21-1
procps-2.0.7-11
psmisc-20.1-2
```

```
pwdb-0.61.1-3
quota-3.01pre9-3
Raidtools-0.90-23
Readline-4.2-2
redhat-logos-1.1.3-1
redhat-release-7.2-1
reiserfs-utils-3.x.0j-2
Rootfiles-7.2-1
rpm-4.0.3-1.03
sed-3.02-10
sendmail-8.11.6-3
setserial-2.17-4
setup-2.5.7-1
setuptool-1.8-2
sh-utils-2.0.11-5
Shadow-utils-20000902-4
slang-1.4.4-4
slocate-2.6-1
sysklogd-1.4.1-4
Syslinux-1.52-2
SysVinit-2.78-19
tar-1.13.19-6
tcsh-6.10-6
Termcap-11.0.1-10
Textutils-2.0.14-2
time-1.7-14
timeconfig-3.2.2-1
tmpwatch-2.8-2
utempter-0.5.2-6
util-linux-2.11f-9
vim-common-5.8-7
vim-minimal-5.8-7
vixie-cron-3.0.1-63
which-2.12-3
words-2-17
zlib-1.1.3-24
```

The removal of the following unnecessary packages should then be done via “rpm -e”:

```
apmd-3.0final-30
ash-0.3.7-2
gpm-1.19.3-20
sendmail-8.11.6-3
dhcpcd-1.3.18pl8-13
mouseconfig-4.23-1
procmail-3.21-1
openldap-2.0.11-13
cyrus-sasl-md5-1.5.24-20
cyrus-sasl-plain-1.5.24-20
indexhtml-7.2-1
iptables-1.2.3-1
netconfig-0.8.11-7
parted-1.4.16-8
pcre-3.4-2
```

Note: Do not remove the dhcpcd package if installing a DAIP module.

The following packages must be installed for Check Point NG FP-2:
(Not installed by the basic packaging installation)

```
shareutils-4.2.1-8
perl-5.6.0-17
compat-libstdc++-6.2-2.9.0.16
```

All relevant security updates should be applied:
http://www.redhat.com/support/errata/rh72-errata-security.html
More information available on RH security
http://linuxdocs.org/HOWTOs/Security-HOWTO.html

The resulting operating system provides the necessary foundation to correctly run Check Point VPN-1/FireWall-1 software. No other software should be installed on the appliance. However, as a VPN-1/FireWall-1 appliance there may be justifiable cause for installing additional software. Additional software installations should be strictly controlled and sufficiently documented. Justify all additions in the OPSEC submission document and provide a method for disabling them if a customer chooses). Listed below are the categories and required secure configurations for additional software:

1. *System Management*

   - Secure Shell Access is allowed on an appliance with restrictions – SCP use is encouraged in all appliance documentation. (/etc/ssh/sshd_config and ssh_config)

     - No X11 forwarding (X11Forwarding no)
     - No Version 1 connections allowed (Protocol 2)
     - No fallback to rsh (FallBackToRsh no)
     - No root access via ssh

   - Apache Web Server Access is allowed so that a partner can develop a web based User Interface for configuring the appliance. All Apache security fixes should be applied see http://httpd.apache.org

     - HTTPS access required
     - Limit the interface which responds to requests (i.e. edit httpd.conf "Listen" line)
     - Disable access to the filesystem (<Directory /> Order deny, allow Deny from all </Directory>)
     - Edit access.conf to control the IP's which are allowed to connect
     - Authentication Required

- Additional RAID or other fault tolerant packages can be installed but will require documentation.

2. Security Enhancements

- The appliance should automatically logout idle users (idled v.1.16 or Higher) -

  ```
  /usr/local/sbin/idled
  /usr/local/lib/idled.cf
  /usr/local/man/man5/idled.cf.5
  /usr/local/man/man8/idled.8
  /etc/rc.d/init.d/idled
  /etc/rc.d/rc3.d/S91idled
  /etc/rc.d/rc3.d/K91idled
  ```

  idled can be downloaded from:
  http://www.rpmfind.net/linux/rpm2html/search.php?query=idled

Install file encryption packages if properly documented.

All unnecessary services should be renamed or removed – Their startup scripts in /etc/rc.d/rc2.d – rc6.d should be altered from ‘S’ to ‘X’ (i.e. #rename S45pcmcia X45pcmcia S45pcmcia). “chkconfig --del” can also be used to remove startup scripts. See below

```
X45pcmcia     (BASE)
X05kudzu      (BASE)
X25netfs      (BASE)
X99linuxconf  (BASE)
X11portmap
X14nfslock
X35identd
X60lpd
X80sendmail
X90xfs
X08iptables
X08ipchains
```

3.2 User/System Accounts

- The root account should not have ssh access. One account should be created to allow secure shell access (For example, “fwssh”). This account will only be used to “su” to root (or sudo can be configured to execute privileged commands as a normal user). It should belong to a specially created restricted group.

- Password checking should be enabled and no “dictionary” based passwords should be allowed. There should be a minimal password length of 5.

- GRUB or LILO should be password protected (add the “password” and “restricted” arguments to /etc/lilo.conf) For example:

```
Image = /boot/vmlinuz-2.4.9-13
          label=linux
          read-only
          restricted
          password = password-here
```

- Autologout via ideld or TMOUT in ~/.bash_profile
- Change the umask of “root” to “027” (in /root/.bash_profile add “umask 027”)
- Root should have a safe search path as in /usr/bin: /sbin :/usr/sbin. It should not include “.”
- No accounts other than root should have the user id (UID) of 0
- The “fwssh” user should have no privileged access - All work must be performed after “su”.
- The use of “nodev” and “noexec” on the "fwssh" home partition should enforced. Also /var which prohibits the execution of programs and creation of character and block devices.

3.3 File System

Although many of the file system security issues are removed by limiting the set of user accounts it is still important to apply the correct permissions and attributes to system files. The file system should also be audited regularly.

- Consider installing Tripwire (this tool monitors key attributes of files including binary signature, size etc.). Tripwire can be downloaded from htttp://www.tripwire.org
- The sticky bit on /tmp should be set to prevent the “fwssh” user from accessing others files “chmod 1777 /tmp”
- “Set-user-ID-root” Issues - Setuid / Setgid programs run as root regardless of who is executing them.

  - Find setuid and setgid programs with the following command “# find / -type f \(-perm -04000 -o -perm -02000 \)”. Remove the setuid and setgid permissions on any suspicious program. For example, “# chmod –s /usr/bin/at /usr/bin/chage /usr/bin/chfn”

  - Remove suid-bit from at least the following:

```
/usr/bin/at
/usr/bin/chage
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/newgrp
```

  - Remove gid-bit from at least the following:

    ```
    /usr/bin/slocate
    /usr/bin/wall
    /usr/bin/write
    /usr/sbin/utempter
    ```

  - Users should not be able to run setuid from their home directory. Use the "nosuid" option in /etc/fstab.

- Make sure there are no un-necessary world-writeable files (there will be files in /dev and /tmp but all of them should be examined.) Use the command "# find / -perm –2 ! –type l –ls | more"

- Wherever possible "chattr" should be used. This command (and associated command "lsattr") is useful in letting the superuser apply extended attributes over that provided by "chmod".
  - "#chattr +i" results in a non-changeable file - no links can be created
    - Useful against /bin/login, /bin/rpm, and /etc/shadow
  - "#chattr +u" allows for undeletion
  - #chattr +a" results in an append only file
    - System log files can be set to append only (#chattr +a /var/log/messages) - may cause additional changes to log rotation scripts.

- No file in /etc needs to be group writeable
- The utmp and wtmp files should not be world writeable
- The swap file should not be created with world readable permissions (can result in users gaining access to privileged information).
- No programs should be installed which creates lock files in the /tmp directory insecurely (For example, a patched version of "dialog" and "getty" is needed if installed).

3.4 Network configuration

The appliance should not listen on any ports except those used for management. This is crucial for securing network access to the system and deviations will keep the appliance from being OPSEC certified.

Prior to installing VPN-1/FireWall-1 a "# netstat -atun" should look like the one listed below. (only the ssh port should be listed)

```
[root@appliance /]# netstat -atun
Active Internet connections (servers and established)
Proto Recv-Q Send-Q  Local Address  Foreign Address    State
 tcp    0     0      0.0.0.0:7777      0.0.0.0:*          LISTEN
```

- The appliance should not trust any other machines. Remove /etc/hosts.equiv, /.rhosts, /.netrc, and all the “r” commands from /etc/xinetd.d..

- VPN-1/FireWall-1 should be configured to control IP forwarding and be sure to document the restriction of IP forwarding so that no networks are vulnerable when VPN-1/FireWall-1 boots. In general, the appliance should not be forwarding traffic between interfaces until VPN-1/FireWall-1 is installed

```
/etc/sysconfig/network (FORWARD_IPV4=no)
/proc/sys/net/ipv4 (ip_forward 0)
/etc/sysctl.conf (net.ipv4.ip_forward = 0)
```

- Network Time Protocol is used to synchronize time between a system and a time source. Correct time settings are important for Logging of VPN-1/FireWall-1 events and thus some appliance may wish to use NTP. However, if NTP is used it needs to be secured. The NTP implementation should be client based only (the time updates should be requested by the appliance and not pushed through an always up daemon. The appliance needs to offer a way to not use NTP if a customer desires.

3.5 Linux Kernel Issues

The Linux Kernel used on the appliance should be the version listed in the "Version Information" above. This Kernel is the best and most secure version known to work with VPN-1/FireWall-1 at this time.

Linux kernel security options can be configured via the /proc pseudo filesystem (particularly /proc/sys/net/ipv4). Files set to 1 are enabled, 0 disabled

- ip_forwarding 0 (VPN-1/FireWall-1 will control this setting - the Linux system should have this set to 0 by default)
- log_martians
- icmp_echo_ignore_broadcasts
- tcp_syn_retries
- tcp_window_scaling

3.6 Other Appliance Related Items

As mentioned previously, this document serves as a guideline outlining basic security measures that should be taken on the appliance.

- BIOS – Do not configure parameters in the BIOS without providing a password. A password should not be required to boot the appliance, if the appliance crashes it should boot and load VPN-1/FireWall-1 without user intervention, otherwise a temporary loss of power can result in a prolonged downtime).

- The boot order should default to the hard drive.

- By default syslog provides minimal system logging. Modify the /etc/syslog.conf file to have syslog log more information (i.e. add kern.* /var/log/kernel). Enhancements can also be made to /etc/logrotate.conf.

- Modify the start-scripts (including /etc/rc.d/rc.sysinit) to write information to the LCD display if one is available on the appliance.

- No unnecessary cron jobs should be configured. Read the cron file of every system account in:

  ```
        /var/spool/cron
        /etc/crontabs
        /etc/cron.d
  ```