Global Information Assurance Certification Paper

Firewalls are only as secure as you make them: Hardening Solaris 8 and Windows 2000 for CheckPoint NG

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 2 - Case Study in
Information Security

Submitted by: Jason Pong on 15 November 2004
Location: SANS Downunder 2004, Melbourne Australia

Table of Contents

1 Abstract

If you were to ask the average Joe Blow on the street, what is IT security? Chances are they will say Firewalls or maybe Anti Virus products. These seem to be the buzzwords around. A lot of people will think that just because they have a firewall or maybe anti virus on their PC, that these are the silver bullets that will protect them from the big bad world of the Internet.

Any good technical security practitioner knows that a firewall is not a silver bullet that will protect your organisation from the "bad" people out on the Internet. Whilst it is one of the layers of security that should be in your organisation, by no means is it the one and only. In my experience as an IT security engineer, the most common mistake most people make when building their firewall is a bad security policy. What is a bad policy you might ask? Well, I have seen some firewalls out there configured default allow vs. default deny or the most common is the firewall administrator opening up ports that they normally wouldn't for their mates (for example, "Hey Fred, can you please open up port *xyz* so I can get my webcam going to check up on my cats"). This paper will describe how to harden a CheckPoint Firewall-1 running Solaris 8 and Windows 2000 as a manager.

2 Before

This paper is to tell you how I have hardened my firewall Operating Systems (Solaris 8 and Windows 2000). It is not meant to be a hand holding exercise with step-by-step commands. It assumes the reader has administrative skills in Solaris 8 and Windows 2000 to carry out the process of hardening.

You might ask "but why do I need to harden the Operating System when my firewall policy should be protecting itself from non-authorised connections?" A firewall that isn't harden is only as secure as the policy, and once a firewall has been "owned", you are in a world of pain. I'm sure we all have seen firewall policies out there that are not as secure as they can be (for example, the one that I gave above where the firewall rules default allow all vs. default deny all).

The risk is that if we do not harden the basic Operating System, we are leaving the firewall itself vulnerable to being hacked and owned. There are generic security holes as with every operating system and we want to minimize these holes. This means that we want to install only the minimum core operating system components, disable any non-essential services that the firewall does not require and also encrypt any remote administration connections just to name a few steps we can take as precaution. We will go into more details later.

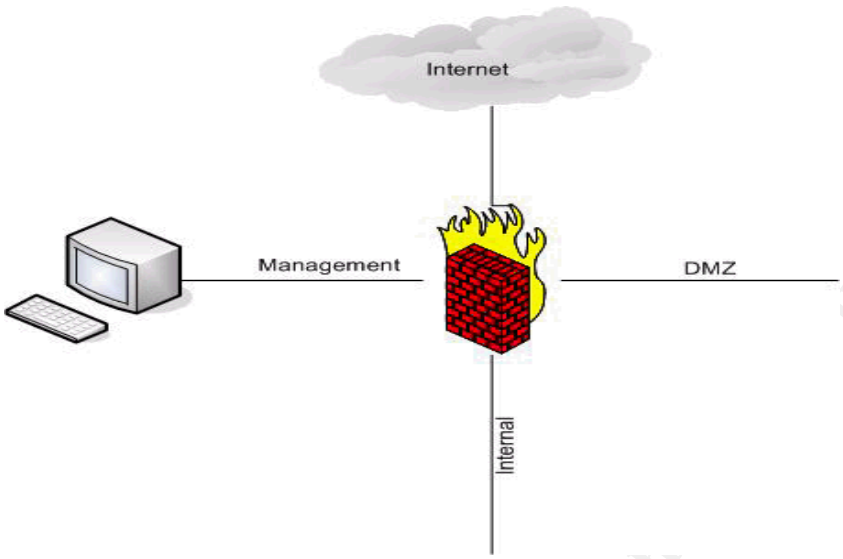
3 During

3.1 The Firewall Design

The last company I worked for prior to my course at SANS Downunder 2004 was a

consulting firm that used to design and customize build firewalls for the customer's requirement. For the purpose of this documentation, we shall refer to this company as RDT.

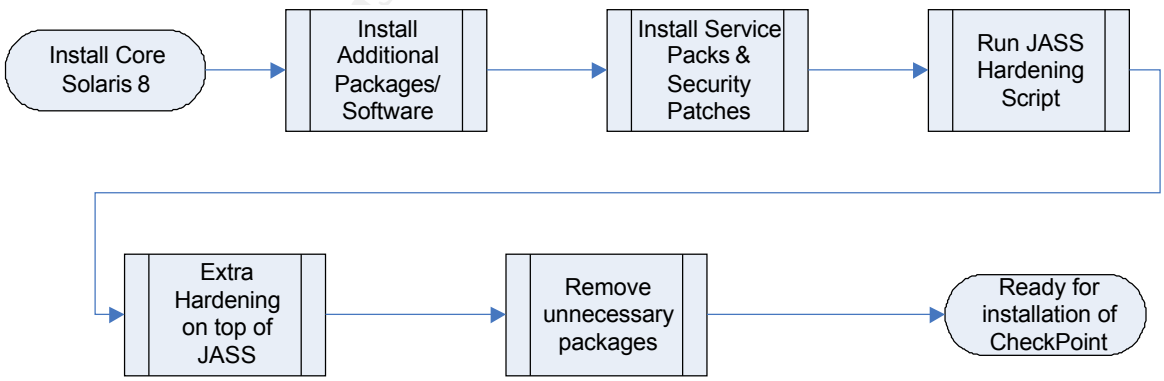
One of the projects that I was on was to design a firewall infrastructure for a customer at a small site. Their requirements are your classic firewall design with one DMZ and one segment for management.

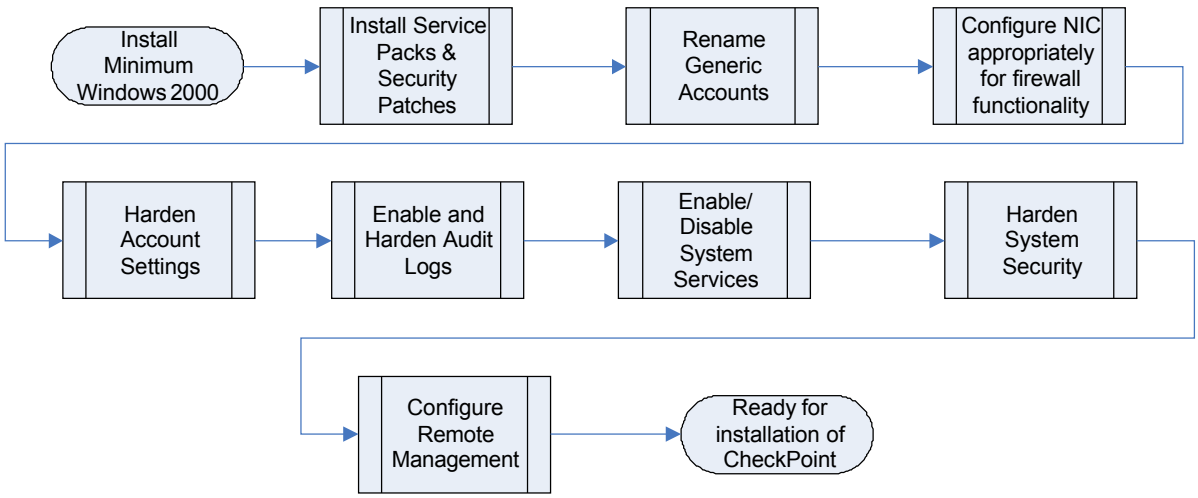


The hardware I used for this project was a Sun Fire 280R (with quad card) for the firewall and a Compaq DL380G3 for the firewall management.

3.2 Overview of Operating System hardening

The following is an overview of the hardening processes:





3.3 Solaris hardening

After the arrival of the hardware, rack, switches etc I was ready to start my installation. The first thing I did was to build my firewall module with Solaris 8. I chose to install just the core operating system. The reason for doing this is that you do not want to have unnecessary packages/services running on your firewall that you don't need. Because I'm going to be running CheckPoint Firewall-1 NG, I can install it with the 64-bit operating system. But if you were to run an older version say 4.1 (unsupported now), it can only operate on 32-bit operating systems. Be sure to pick the right one otherwise your installation of CheckPoint will not work.

Because we have only installed the core operating system, we still require a few extra packages on Solaris to run CheckPoint. Some of these packages are required to run CheckPoint; some are to make life easier for the system administrator:

Here are the 5 packages required to run CheckPoint Firewall-1 NG:

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

Here are some packages that I have installed to make life easier for the administrator (optional):

- SUNWbash (GNU Bourne-Again shell)
- SUNWbzip (The bzip compression utility)

- SUNWbzipx (The bzip compression library (64-bit))
- SUNWauaox (Australasia 64-bit OS Support)
- SUNWesxu (Extended System Utilities (64-bit))
- SUNWntpr (NTP (Root))
- SUNWntpu (NTP (Usr))
- SUNWmdr (Solstice DiskSuite Drivers)
- SUNWmdu (Solstice DiskSuite Commands)
- SUNWmdx (Solstice DiskSuite Drivers(64-bit))

There are another two packages that I would never go anywhere without when I build a firewall. The first one is a TCP wrapper. For those that don't know this software, it will let you to have the ability to monitor and filter incoming requests to FTP, TELNET, RSH, RLOGIN, SYSTAT and other network services. This is another layer of protection on your firewall. To download the source or document for TCP Wrappers, you can find it at ftp://ftp.porcupine.org/pub/security/index.html. The second piece of software that I would install is Openssh. Openssh is a free version of ssh which will let you replace rlogin, telnet, ftp, and rcp. You might ask why use it if you already have programs like telnet, ftp etc that come with the core operating system. Well, the answer is that all communications via ssh are encrypted, unlike telnet, ftp etc where it's all in clear text so someone can sniff for your username/password. For more information and source code download, you can download it from http://www.openssh.com. Of course with these pieces of software, you will have to compile the source code yourself. But if you don't know how to compile or are not having any luck compiling them, you can always download the binaries from http://www.sunfreeware.com. But because we are paranoid by nature being good security practitioners, we would rather compile our own code than rely on someone else's, right?

After the operating system and extra packages have been installed, the next step would be to install all the Solaris Recommended Security Patches. These can be found on (http://sunsolve.sun.com). Once the patches are installed, reboot the server and you have your core operating system ready to install CheckPoint.

Before you install CheckPoint on the server, you might be interested in hardening the operating system. As with anything, a firewall is only as secure as you make it. So it is always a good idea to harden the operating system. You might ask, "where do I start?" Well, I'm glad you asked. I for one don't believe in re-inventing the wheel. Sun already has a Solaris Security Toolkit (JASS) that has been developed for securing Solaris Systems. For more information about the product or download a copy of JASS, you can go to http://www.sun.com/software/security/jass.

Once you have run JASS over your operating system to harden it, I would still go

further in hardening the operating system. Don't get me wrong, JASS does a great job, but there are still a couple of things we can do to further harden the system. Here are some of the things that I would do to harden a Solaris system.

- */etc/default/kbd*, I would disable the KEYBOARD_ABORT variable. This is so that the abort sequence cannot be used to bring the firewall down
- */etc/default/login*, I would make sure that only root can login on the console directly plus I would make the umask value to 022. This is so that for any new files that are created, only the owner of the file has write access.
- */etc/default/passwd*, I would enable password aging on. Min weeks are 1 and Max weeks are 8. Also have a password length of 8
- */etc/default/su*, I would make sure the SULOG is set to /var/adm/sulog and that SYSLOG is set to "YES". This option is required so that all su attempts are logged
- */etc/default/sys-syspend*, make sure the variable PERMS has "-". This is so that the operating system cannot be suspended with the *sys-suspend* command.
- */etc/dfs/dfstab*, make sure there's nothing in the file. This file is used to share local directories over the network
- */etc/init.d/inetsvc*, to make extra TCP logging, add the "-t" variable to inetd so it reads inetd –s –t
- */etc/nsswitch.conf*, I have set all the attributes to files.
- */etc/syslog.conf*, make sure there are entries in the file that logs TCP Wrapper, Inetd, and SSH. For example, add in the following:

```
### Log all TCP Wrapper connections here
local3.info                     /var/adm/tcpdlog


### Log all inetd connections here
daemon.notice                   /var/adm/inetdlog


### Log all ssh connections here
daemon.info                     /var/adm/sshlog
```

- Make sure under */etc/init.d/nddconfig* (that was created with JASS) has the following values set for the parameters

Variable	Value	Description
arp_cleanup_interval	60000	Period that ARP remains in cache
ip_forward_directed_broadcasts	0	Should the server forward boardcasts to networks or hosts
ip_forward_src_routed	0	Should the server forward source routing
ip_ignore_redirect	1	Should the server ignore ICMP packets that defines new routes. The architect around the firewall infrastructure is static so this option is no required
ip_ire_flush_interval	60000	Period that a specific route will be kept for
ip_respond_to_address_mask_broadcast	0	Should the server respond to ICMP requests for netmasks
ip_respond_to_echo_broadcast	0	Should the server respond to broadcast pings
ip_respond_to_timestamp	0	Should the server respond to ICMP timestamp
ip_respond_to_timestamp_broadcast	0	Should the server respond to ICMP timestamp broadcast
ip_send_redirects	0	Should the server respond to ICMP redirect
ip_strict_dst_multihoming	1	Enable Strict Destination Multihoming
tcp_conn_req_max_q0	8192	Queue that is used for unestablished connections
tcp_conn_req_max_q	2048	Queue that is used for fully established connections
tcp_rev_src_routes	0	Should the server reverse IP source routing
tcp_extra_priv_ports_add	“”	No extra privilege ports beside 1-1023
udp_extra_priv_ports_add	“”	No extra privilege ports beside 1-1023
tcp_smallest_anon_port	32768	Setting lowest ephemeral ports
udp_smallest_anon_por	32768	Setting lowest ephemeral ports

tcp_largest_anon_port	65535	Setting upper bounds of the ephemeral ports
udp_largest_anon_port	65535	Setting upper bounds of the ephemeral ports
tcp_smallest_nonpriv_port	1024	Define where the non privilege port starts
udp_smallest_nonpriv_port	1024	Define where the non privilege port starts
Ip_forwarding	0	Switch off IP forwarding

- Users *lp* and *adm* should not be using cron on the firewall. There are no reasons for them for the role of a firewall. Disable their cron jobs by removing their files from /var/spool/cron/crontabs directory.

- Disable the nscd service from starting up. Name Service Caching Daemon is used for caching most common name service requests like passwd, hosts, group etc. This function is not required for our design. Disable it from starting up by removing */etc/rc2.d S76nscd*

- Disable super user trust between our server and other servers on the network. Because of the nature of this server, any trust between the super user and other servers should not take place. Remove the files */.rhosts*, */.netrc*, and */etc/hosts.equiv* (if they exists). I would also go as far as re-creating those files (using the *touch* command and then set the permissions to deny all access to the files (*chmod 0*).

- Disable core dumps on the system. Some might argue that when a program crashes, a core dump might be useful because it let's you analyst what happened. But the reasons why we want to disable core dumps are because the core files contains sensitive information. You can disable core dump by setting "*set sys:coredumpsize=0*" to /etc/system

- Since we have setup that only root can login directly from the console, the only way to get a root login is for a user to ssh into the firewall (no generic accounts, all user accounts on the firewall must belong to a user for audit and ownership purposes) and use the command *su* into root. Because we want to add in another layer of security, we will now create a special group called the *wheel* group (using groupadd command). After that, we want to set user as *root* and group as *wheel* to files (*chown root:wheel /sbin/su.static /usr/bin/su*). The last step is to make sure only the user and group owners can run those commands (after all, it would defeat the purpose of what we're trying to achieve here if we let anybody have access to those commands). You can achieve that by running this command (*chmod 4550 /sbin/su.static /usr/bin/su*)

- Do you remember how I said earlier that only have the basic core operating systems because we do not want unnecessary files or services running on

our firewall? Well now it's time to remove some unnecessary packages from our system that the firewall does not require to run. They are:

- SUNWadmr (System & Network Administration Root)
- SUNWatfsr (AutoFS (Root))
- SUNWatfsu (AutoFS, (Usr))
- SUNWauda (Audio Applications)
- SUNWaudd (Audio Drivers)
- SUNWauddx (Audio Drivers (64-bit))
- SUNWdtcor (Solaris Desktop /usr/dt filesystem anchor)
- SUNWftpr (FTP Server (Root))
- SUNWftpu (FTP Server (Usr))
- SUNWi1cs (X11 ISO8859-1 Codeset Support)
- SUNWigsr (IGS CyberPro2010 Device Driver (Root))
- SUNWigsu (IGS CyberPro2010 DDX (OW) Driver)
- SUNWigsx (IGS CyberPro2010 64-bit Device Driver (Root))
- SUNWkey (Keyboard configuration tables)
- SUNWluxdx (Sun Enterprise Network Array sf Device Driver (64-bit))
- SUNWluxop (Sun Enterprise Network Array firmware and utilities)
- SUNWluxox (Sun Enterprise Network Array libraries (64-bit))
- SUNWmdi (Sun Multipath I/O Drivers)
- SUNWmdix (Sun Multipath I/O Drivers (64-bit))
- SUNWnisr (Network Information System, (Root))
- SUNWnisu (Network Information System, (Usr))
- SUNWpl5u (Perl 5.6.1 (core))
- SUNWrmodu (Realmode Modules, (Usr))
- SUNWsolnm (Solaris Naming Enabler)
- SUNWuaud (USB Audio Device Drivers)

- SUNWuaudx (USB Audio Device Drivers (64-bit))
- SUNWwsr2 (Solaris Product Registry & Web Start runtime support)
- SUNWxwdv (X Windows System Window Drivers)
- SUNWxwdvx (X Windows System Window Drivers (64-bit))
- SUNWxwkey (X Windows software, PC keytables)
- SUNWxwmod (X Window System kernel modules)
- SUNWxwmox (X Window System kernel modules (64-bit))
- SMEvplr (SME platform links)
- SMEvplu (SME usr/platform links)
- SUNWcg6 (GX (cg6) Device Driver)
- SUNWcg6x (GX (cg6) Device Driver (64-bit))
- SUNWdfb (Dumb Frame Buffer Device Drivers)
- SUNWensqr (Audio Device Driver (32-bit))
- SUNWensqx (Audio Device Driver (64-bit))
- SUNWauaow (Australasia OW Support)

- Sun by default will use the same MAC address for all it's multiple Ethernet interfaces. To switch off this feature and enable unique MAC address per interface, you will need to set *local-mac-address?=true* on eeprom (command *eeprom local-mac-address?=true*)
- As a habit I usually set the boot up sequence as disk, CDROM and lastly network. You can achieve this by using the command *eeprom "boot-device=disk cdrom net"*
- Hard code speed and duplex for all NICs. As a consultant for RDT, I have seen performance issues when both firewall and switches are set to auto negotiation. Don't take the chance with auto negotiation.
- I would also follow CheckPoint performance tuning recommendations as outlined by CheckPoint (http://www.checkpoint.com/techsupport/documentation/FW-1_VPN-1_performance.html#solaris)

After you have done all of the above, reboot the server and you should be in a

position to start your installation of the CheckPoint firewall module. At this stage, we have hardened your Solaris 8 operating system and now all there is left to do is to install the firewall software.

3.4 Windows 2000 Hardening

Now that we have got the Solaris hardening completed and the firewall module built, it's time to move onto the firewall management server. This server was a Compaq DL380G3 and the operating system was Windows 2000. As before, when you install Windows 2000 on the server, only install it with the minimum. What I have done is to customise my applications so that only the required components are installed. I do not install the applications below:

- Calculator
- Character Map
- Clipboard Viewer
- Desktop Wallpaper
- Document Templates
- Mouse Pointers
- Object Packager
- Paint
- WordPad
- Communication
- Games
- Multimedia
- Indexing Service
- IIS
- Management and Monitoring Tools
- Message Queuing Services
- Networking Services
- Other Network File and Print Services
- Script Debugger

Once the server is installed with your fresh installation of Windows 2000, you should update all the service packs and security patches on it immediately. I would put the server onto a trusted network (ie a network that you know is safe and virus free, eg RDT's internal network. I would not plug this server straight out to the Internet for example without some sort of security parameter setup, eg firewall, anti virus etc) and go to http://windowsupdate.microsoft.com/ to update all my service packs and security patches. If I cannot plug this server into a network that is relatively safe, I would download the service packs and patches onto a CD and install it this way.

Now that you have installed the basic Operating Systems and it has been patched up, it's now time to do some hardening. What I normally do is to rename the local Administrator account. I would then create a dummy account called Administrator, give it the same access as your guest account (i.e. none), set a password (containing special characters and numerical keys) and disable the account. The reason for this is that if anyone should try to login as a local Administrator account, it will be logged. I would also rename the guest account to nobody, remove all privileges it had, set a password and disable the account. Remove *TSInternet* User account should it exists.

Because the server does not require being on a domain, I would create a workgroup name for it (usually random characters eg *LIJU85J65GH*). I would also go into Network Connections and unbind everything except for TCP/IP (eg Client for Microsoft Networks). Disable NetBIOS over TCP/IP and disable all unused adapters. As before with Solaris, I would also hard code the speed and duplex of the NIC to avoid any issues with auto-negotiation.

User Accounts

I would configure the local System Account Policy and accounts as follows:

Account Settings

Property	Value
Enforce Password History (passwords remembered)	12
Maximum Password Age	56
Minimum Password Age	0
Minimum Password Length	8
Enforce Password Complexity	Enabled
Store password using reversible encryption for all users in the domain	Disabled
Account Lockout Threshold (invalid logins)	5

Account Lockout Reset	30 mins

Accounts Auditing

Action	Success	Failure
Account Login Events	enabled	enabled
Account Management	enabled	enabled
Directory Service Access	disabled	disabled
Login Events	enabled	enabled
Object Access	disabled	enabled
Policy Access	enabled	enabled
Privilege Access	enabled	disabled
Process Tracking	disabled	disabled
System Events	enabled	disabled

User Rights

User Right	Settings
Access this computer from network	Administrators
Act as part of the operating system	(no one)
Add workstations to domain	(no one)
Back up files and directories	Administrators
Bypass traverse checking	Authenticated Users
Change the system time	Administrators
Create a pagefile	Administrators
Create a token object	(no one)
Create permanent shared objects	(no one)
Debug programs	(no one)
Deny Access to this computer from the Network	(no one)
Deny logon as a batch job	(no one)

Deny logon as a service	(no one)
Deny logon locally	(no one)
Enable computer and user accounts to be trusted for delegation	(no one)
Force shutdown from a remote system	(no one)
Generate security audits	(no one)
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	(no one)
Log on as a batch job	(no one)
Log on as a service	Administrators
Log on locally	Administrators
Manage auditing and security log	Administrators
Modify firmware environment values	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove Computer from docking station	(no one)
Replace a process level token	(no one)
Restore files and directories	Administrators
Shut down the system	Administrators
Synchronize directory service data	(no one)
Take ownership of files or other objects	Administrators

Event Log

Auditing is important part of the hardening process as this will allows us to view the health/troubleshooting of our system. Because of the nature of the logs, I would normally disable any non-privilege users from looking at the log files.The settings for Windows Event Logging that I normally set are as follows:

Property	Value
Maximum application log size	49152 Kb
Maximum security log size	49152 Kb
Maximum system log size	49152 Kb
Restrict guest access to application log	enabled
Restrict guest access to security log	enabled
Restrict guest access to system log	enabled
Retain application log	disabled
Retain security log	disabled
Retain system log	disabled
Retention method for application log	As needed
Retention method for security log	Manually
Retention method for system log	As needed
Shut down the computer when the security audit log is full	disabled

Windows Subsystems

The Posix and OS/2 subsystems are not required for the firewall functionality so they are removed from the system.

System Services

There are many services that comes default with Windows that are not required to run a firewall. As part of the hardening, any service that is not required is to be disabled. The list below shows the list of services and it's start-up status after the hardening.

Some of the services that have been disabled may be enabled, should they be required i.e. Windows Time Service (NTP Time Sync), Removable Storage (Windows Backup). It is highly recommended to configure all servers for NTP as this helps auditing.

Service	Setting	Description

Alerter	disabled	Used to automatically send administrative alerts to a predefined list of NetBIOS names.
Clipbook	disabled	Permits cutting and pasting over the network. It uses Network DDE
Computer Browser	disabled	Builds and maintains the list of computers and domains that is displayed in the Network Neighborhood. It can also provide other applications with this information.
DHCP Client	disabled	Manages network configuration by registering and updating IP addresses and DNS names.
Distributed File System	disabled	Manages logical volumes distributed across a WAN or LAN. Requires Server Service
Distributed Link Tracking Client	disabled	Send notification of files moving between NTFS volumes in a network domain
Distributed Link Tracking Server	disabled	Stores information so that files moved between volumes can be tracked for each volume in the domain.
Distributed Transaction Coordinator	disabled	Coordinates transactions that are distributed across two or more databases, message queues, file systems, or other transaction protected resource managers.
Directory Replicator	disabled	Provides a very basic file replication mechanism. It is mainly used to replicate the contents of the NETLOGON share between domain controllers.
Fax Service	disabled	Help send and receive faxes
File Replication	disabled	Maintains file synchronisation of file directory contents among multiple servers
Indexing Service	disabled	Indexing
Internet Connection Sharing	disabled	Provides Network Address Translation, addressing and name resolution for computers on a dial up network
Intersite Messaging	disabled	Allows sending messages between Windows Advanced Servers.
IPSEC Policy Agent	disabled	Manages IP security policy and starts the ISAKMP/Oakley (IKE) and the IP security driver.
Infrared Monitor	disabled	Supports infrared devices installed on the computer and detects other devices that are in range.

Kerberos Key Distribution Center	disabled	Generates session keys and grants service tickets for mutual client/server authentication.
Messenger	disabled	Receives NetBIOS datagram pop-up messages sent with the net send command
Net Logon	disabled	Required when running a computer in a domain environment. It passes authentication requests to the domain controller from domain member computers that are not domain controllers themselves. It finds a domain controller and provides a secure communication channel to it. On a domain controller, the Net Logon service authenticates users and facilitates synchronisation of the Systems Account Manager (SAM) database between domain controllers.
Network DDE	disabled	Makes it possible to use Dynamic Data Exchange (DDE) over the network. DDE is used to send messages and data between applications.
Network DDE DSDM	disabled	Network DDE Service Data Manager (DSDM) service maintains a database of the DDE shares on a system.
NT LM Security Support Provider	disabled	Provides security to remote procedure call (RPC) programs that use transports other than named pipes.
Print Spooler	disabled	Loads files to memory for later printing. NOTE: This service may be required to install Windows Service Packs
QoS RSVP	disabled	Provides network signalling and local traffic control setup functionality for QoS-aware programs and control applets.
Remote Access Auto Connection Manager	disabled	Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address.
Remote Access Connections Manager	disabled	Creates a network connection.
Remote Registry Service	disabled	Allows remote registry manipulation.
Removable Storage	manual	Manages removable media, drives, and libraries.

Routing and Remote Access	disabled	Offers routing services to businesses in local area and wide area network environments.
Remote Procedure Call (RPC) Locator	Manual	Manages the RPC name service database.
Run As Service	disabled	Enables starting processes under alternate credentials
Task Scheduler	disabled	Makes it possible to Schedule jobs for later execution. Commands can be added to the Schedule Service via the at command.
Server	disabled	The Server Service Provides RPC support and file, print, and named pipe sharing. i.e. it provides the ability for other computers to connect to a host
SNMP	disabled	Provides the ability to release information about a host when requested. The SNMP community string must be supplied and the string have appropriate permissions.
SNMP Trap Service	disabled	Provides the ability to send SNMP traps to an SNMP server.
TCP/IP NetBIOS Helper	disabled	Enables support for NetBIOS over TCP/IP (NetBT) and NetBIOS name resolution.
Telephony Service	disabled	Provides Telephony API (TAPI) support for applications.
Telnet	disabled	Allows a remote user to log on to the system and run console programs using the command line.
UPS	disabled	Manages and handles communication between an Uninterruptible Power Supply (UPS) device and the O/S
Utility Manager	disabled	Starts and configures accessibility tools from one window
Com+ Event System	Manual	Provides automatic distribution of events to subscribing COM components. This service is required to stop DCOM error messages
DNS Client	Automatic	Resolves and caches Domain Name System (DNS) names.
EventLog	Automatic	Provides the interface for reading and writing the three Windows 2000 Event Logs

License Logging Service	Automatic	Manages licensing
Local Disk Manager (LDM)	Automatic	Manages locally attached disks
Local Disk Administrative Service	Manual	Administrative service for disk management requests
Remote Procedure Call (RPC)	Automatic	Provides the endpoint mapper and other miscellaneous RPC services.
Protected Storage	Automatic	Provides Protected Storage for Sensitive data such as private keys.
Plug and Play	Automatic	Provides hardware device installation and configuration
Network Connections	Automatic	Manages network adapters and network settings
Security Accounts Manager	Automatic	Stores security information for local user accounts.
System Event Notification	Automatic	Tracks system events such as Windows logon, network, and power events. Notifies COM+ Event System subscribers of these events.
Windows Management Instrumentation	Automatic	Provides system management information. Required for MMC
Windows Management Instrumentation Driver Extensions	disabled	Provides systems management information to and from drivers. Required for MMC
Workstation	disabled	Allows a host to access resources on a Microsoft network. *Although this service is not required for the running of firewall, it will need to be enabled should a password change be required locally.*
Application Management	Manual	Provides software installation services such as Assign, Publish, and Remove.
Windows Installer	Manual	Installs, repairs and removes software according to instructions contained in .MSI files.

Windows Time	Manual	Sets the computer clock.
DHCP Server	disabled	DHCP Server Service
Windows Terminal Service	disabled	Windows Terminal Service
IrBridge User-Level Interface	disabled	Infrared User Interface
NetMeeting Remote Desktop Sharing	disabled	Allows authorized people to remotely access your Windows desktop using NetMeeting.
Performance Logs and Alerts	disabled	Configures performance logs and alerts.
Smart Card	disabled	Manages and controls access to a smart card inserted into a smart card reader attached to the computer.
Smart Card Helper	disabled	Provides support for legacy smart card readers attached to the computer.
Still Image Service	disabled	Still Image Service
WMDM PMSP Service	disabled	WMDM PMSP Service

System Security Options

System Security will also be required. As part of the hardening process, the following changes to System Security have been made on the system:

Security Option	Setting
Allow server operators to schedule tasks (domain controllers only)	disabled
Allow system to be shut down without having to log on	disabled
Allowed to eject removable NTFS media	Administrators
Audit the access of global system objects	enable
Audit use of Backup and Restore privilege	enable
Automatically log off users when logon time expires (local)	enabled
Amount of idle time required before disconnecting session	5 minutes

Clear virtual memory pagefile when system shuts down	enabled
Digitally sign client communication (always)	enabled
Digitally sign client communication (when possible)	enabled
Digitally sign server communication (always)	disabled
Digitally sign server communication (when possible)	enabled
Disable CTRL+ALT+DEL requirement for logon	disabled
Additional restrictions for anonymous connections	Do not allow enumeration of SAM accounts and shares
Do not display last user name in logon screen	enabled
LAN Manager Authentication Level	Send NTLMv2 response only\refuse LM & NTLM
Message text for users attempting to log on	This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel.
Message title for users attempting to log on	***** This service is for authorised clients only *****
Number of previous logons to cache (in case domain controller is not available)	0
Prevent users from installing printer drivers	enabled
Prevent system maintenance of computer account password	disabled

Prompt user to change password before expiration	5 days
Recovery Console: Allow automatic administrative logon	disabled
Recovery Console: Allow floppy copy and access to all drives and all folders	disabled
Restrict CD-ROM access to locally logged-on user only	enabled
Restrict floppy access to locally logged-on user only	enabled
Strengthen default permissions of global system objects (e.g. Symbolic Links)	enabled
Secure channel: Digitally encrypt or sign secure channel data (always)	enabled
Secure channel: Digitally encrypt secure channel data (when possible)	enabled
Secure channel: Digitally sign secure channel data (when possible)	enabled
Secure channel: Require strong (Windows 2000 or later) session key	enabled
Shut down system immediately if unable to log security audits	disabled
Send unencrypted password to connect to third-party SMB servers	disabled
Smart card removal behavior	Lock Workstation
Auto Start Cdrom	disabled
Administrative Shares (Server)	disabled
Administrative Shares (Workstation)	disabled
Secure Additional Base Named Objects	enabled
Disable NTFS 8.3 Name Generation	enabled
Enable NetBT to Open TCP & UDP Ports for Exclusive Access	enabled
DCOM Support	disabled
DCOM Remote Connections	disabled
(TCP/IP) IP Forwarding	disabled
(TCP/IP) ICMP Redirect	disabled
(TCP/IP) SYN (DOS) Protection	Advanced Protection
(TCP/IP) Dead Gateway Detection	disabled

(TCP/IP) Enable Path MTU Discovery	disabled
(TCP/IP) Perform ARP Source Route Requests	disabled
(TCP/IP) IP Auto Configuration	disabled
(TCP/IP) Perform Router Discovery	disabled
(TCP/IP) Disable Dynamic DNS Updates	enabled
(TCP/IP) ICMP address mask request	disabled
(TCP/IP) Disable Interface Media Sense	disabled
(TCP/IP) Disable Source Routed Packets	enabled
IIS Command Shell Exec Support	disabled
Stronger Protection on Base System Objects	enabled
NetBIOS Name Service Conflicts Protection	enabled
Computer Browser Service Reset Protection	enabled
Diable Web Printing	enabled
Restrict NULL Session Access	enabled
Delete Roaming Cache	enabled
DirectDraw Hardware Access	disabled
Unsigned driver installation behaviour	Warn but allow installation
Unsigned non-driver installation behaviour	Warn but allow installation
(TCP/IP) Keep Alive Time	300000

Remote Management

One of the reasons why I choose Compaq DL380G3 was that it comes with integrated Lights-Out (iLO), which is remote management firmware (separate NIC to the operating system). You can configure iLO to use https connections to do your remote management. As with anything, it doesn't come free but it's not expensive to purchase a license for iLO. Of course, you will need to configure it with SSL connections only and make sure any connections that go to iLO has to pass through your firewall. Make sure to lock down access to iLO on your firewall policy (ie not open to everyone)

4 Summary

Now that we have gone through all the steps above, we have a basic platform that is hardened from an Operating System point of view. We have installed only the core operating systems (the theory is that what is not required should not be installed), patched the systems up with the latest patch levels and security patches. We have disabled all non-essential services that are not required by the firewall and we have gone further by hardening the IP stack as well. We have also installed another layer of protection on the firewall module (Solaris) so that any remote management is now done via ssh where all communications are encrypted, plus TCP wrappers to add another layer of filtering. All network speed and duplex settings have been hard coded to avoid any “misunderstanding” when it comes to auto negotiation. We have also set up HP remote management for our Windows box via iLO (https connections only). I would also recommend installing reputable Anti Virus software on the manager and updating it signatures regularly.

All in all, these servers are now locked down from an operating systems point of view and are ready for you to start your installation of CheckPoint. Make sure though that you have implemented a proper firewall policy on it at the end of the day, and don’t let Fred open up any unauthorized ports for his friends! Remember that a firewall is only as secure as you make it.

Appendix A - References

Internet

Spitzner, Lance. “Armoring Solaris: II” 20 July, 2002. URL: http://www.spitzner.net/armoring2.html (2 Feb 2005)

Chouanard, Jean. “How to install Solaris and have a good host security”. 19 November, 2000. URL: http://yassp.parc.xerox.com (2 Feb 2005)

Sun Microsystems. “Solaris Security Toolkit (JASS)” URL: http://www.sun.com/software/security/jass/ (29 January, 2005)

Phoneboy. “Securing Windows 2000 for VPN-1/Firewall-1 Installation” 11 January, 2004. URL: http://www.phoneboy.com/bin/view.pl/FAQs/SecuringWin2k (3 February, 2005)

Cox, Philip. “Hardening Windows 2000” (14 March 2002). URL: http://www.systemexperts.com/win2k/hardenW2K13.pdf (3 February, 2005)

CheckPoint. “Check Point VPN-1 & Firewall-1 NG Performance Tuning Guide”. URL: http://www.checkpoint.com/techsupport/documentation/FW-1_VPN-1_performance.html#solaris (3 February, 2005)

Books

Internet Security Systems. “Windows 2000 Security, Technical Reference” Published by Microsoft Press, 2000

Mulligan, John P. “Solaris Essential Reference” New Riders Publishing, 1999

O’Dea, Michael. “Hack Notes Windows Security Portable Reference”. McGraw-Hill/Osborne, 2003