



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.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at <http://www.giac.org/registration/gsec>

**Upgrading Corporate Firewalls from
Checkpoint Firewall-1™ v 4.1 to
Checkpoint Firewall-1™ NG**

**GIAC Security Essentials Certification
Version 1.4b - Option 2**

**Brian Foster
June 2003**

Abstract

This paper will examine how my organisation, a large Australian based international law firm, met the challenge to upgrade our 6 corporate firewalls from Checkpoint Firewall-1™ v4.1 (referred to as 4.1 from hereon) to Checkpoint Firewall-1 NG™ (referred to as NG from hereon). Checkpoint had declared their intention to drop the support of v4.1 in favour of NG and notwithstanding this declaration, there were advances in NG which we were keen to exploit to make our overall perimeter defence solution more manageable. My role in the project was of project initiator and project manager with a high-level view of what was expected, not the guy who knows the commands to type in at the console.

The extensive planning phase actually spawned a better solution than we had first envisaged (detailed in the next section) and the result was a set of firewalls and management console which catered solely to our remote solution, totally self contained and independent of the main corporate firewalls which control internet access, email flow, VPNs etc. The firewall count has subsequently increased from 6 to 8 with an additional Management console but the benefit to our client base, and the flexibility it has given to the overall solution far outweighs the extra cost. The overall security of our remote access service has taken another giant step forward with the project which has followed the firewall upgrade. All our remote clients are now equipped with a Checkpoint module which contains a personal firewall, the rules base of which can be set and controlled from the (new) Management console. The benefits derived from this follow-on project are discussed in a later section. (The details of this second project are not included in this paper, merely an overview and an outcome analysis)

The Before view

The firm has Australian offices in Sydney, Melbourne, Perth and Brisbane ; offices in Ho Chi Minh City and Hanoi in Vietnam and an office in Singapore. All offices with the exception of Brisbane have a firewall (Brisbane connects via the corporate WAN) through Sydney).

The firewalls in Singapore, Hanoi and Ho Chi Minh City are all Nokia IP 120 devices whilst those in Sydney Melbourne and Perth are all Intel based. At the start of the project, only Hanoi and Ho Chi Minh City are running NG.

Figure 1 overleaf shows a diagram of the firewall network at the commencement of the project.

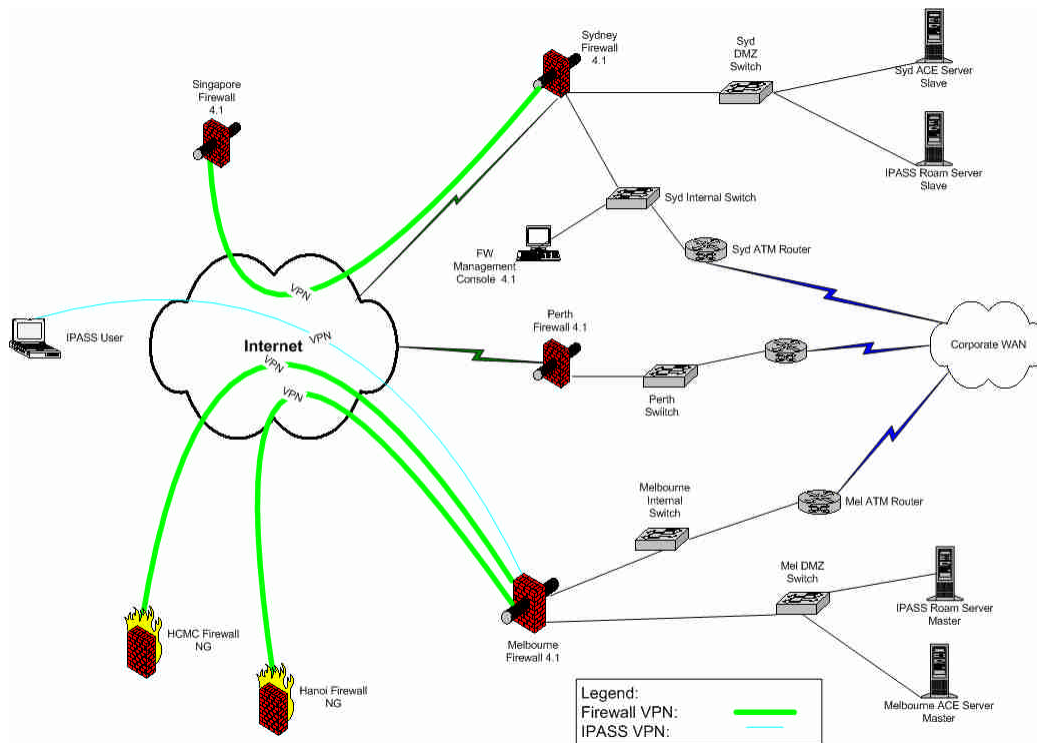


Figure 1 – The Firewall network – Before

Firewall technology was first introduced into the Firm in 1997 and the following year, our remote and travelling clients were changed from using RAS as a means to connect to the corporate network to a combination of iPass™ and Checkpoint SecuRemote™. In order to clarify the situation, iPass™ is a global roaming service that provides internet access to authorised clients just about anywhere in the world simply by calling a local telephone number (http://www.ipass.com/services/services_corpaccess.html). Once the client has access to the internet, then Checkpoint SecuRemote™ is used to authenticate with the corporate network.

Between 1998 and early 2003, whenever a service pack had to be applied or substantial changes made to any of the firewalls, there had always been a major impact on these remote clients. With such a large and well spread client base we would not know if we had notified or updated all the clients of the need to make a change to their laptop. By and large, the remote clients are the senior partners and fee earners within the Firm meaning any adverse impact on the part of the solution which services these people is felt right across the firm (not a desirable outcome).

More than 12 months previously, I had raised a request to have the corporate firewalls upgraded and was the sponsor of that project but not strictly involved in the planning. The team came up with a plan which would have resulted in a massive impact on the remote client base which numbers more than 700 people and the risk of making the remote solution unusable for some if not all these people was very real. I rejected the plan. The team were obviously struggling and the IT director was on the verge of outsourcing the complete

project, to which I was opposed. I had been involved with the firewalls since they were installed and had a thorough understanding of how they work and convinced him that I should lead the team. I had an idea which would make our firewall defences more versatile, better able to service our remote clients and still maintain the defence in depth required of a large corporate site.

The answer was to install a second set of firewalls and management console, totally self-contained and separate from the main corporate firewalls and configured to service only the remote clients and nothing else. Of course there were quite considerable costs involved, but minimal risk. The subsequent benefits to our remote clients, 700+ and growing all the time, were proven to outweigh the additional cost burden. The increased security posture achieved from such a solution finally swung the decision pendulum in my direction (although he did make it clear that certain parts of my anatomy were at risk of being re-arranged if the project did not succeed as I had prescribed!!)

The first task was to write a thorough business case to prove to the firm that an upgrade was essential and moreover, that we had the necessary expertise to see the project through to a satisfactory conclusion. The director of IT was sceptical that the team I was assembling was capable of implementing the solution I had put forward having suffered a number of high profile (relative) failures in the recent past whilst working under other project managers. However, I had a clear picture of the outcome we would achieve and along with my network planner, worked out a full and complete project and implementation plan and sold this to the director. In reality the actual firewall upgrade itself, changing the operating system and installing the new software, whilst being a task for a skilled operator is a relatively routine operation and Checkpoint have developed a whole suite of tools to assist in the process. On this basis, I had every confidence in the ultimate success of the project.

It was essential to upgrade to NG as Checkpoint were about to cease supporting v4.1 (this decision has been overturned and 4.1 support is continuing – but its days are numbered). The second overriding reason to upgrade was to satisfy the increasing use of ADSL and other broadband connections. These “always on” types of connection pose a real threat to the corporate network if the computer is connected to the internet without the security of a personal firewall or some other perimeter device. However, with up to 700 potential “always on” connections to my corporate network (the number of remote users) and the possibility of everyone using a different device (or no device at all) and the endless different configurations, the remote solution was rapidly turning into an administrative nightmare not to mention a security hotspot. Although not the focus of this project, once the NG upgrade is complete the follow up project (as mentioned in the Abstract section) is to roll out Checkpoint SecureClient NG™ to all the remote users. This product includes a personal firewall which can be configured and locked down by the administrator at the corporate Firewall Management Console. This allows us to set and maintain a consistent set of firewall rules to protect the laptop computer and therefore by extension, the corporate network. (<http://www.checkpoint.com/techsupport/ngupgrade/top10/2.html>)

The centrepiece of the business case and “sale” to the director of IT was to state that throughout the whole upgrade process, there would be no adverse client impact and that, in all but a handful of cases, the upgrade would be fully automated. That is not to say that the clients would not see the upgrade process was happening, as it was necessary to install a new version of the client software and that process is not transparent, but we would not be faced with a scenario which would state for instance that on May 1 you as the client would have to change over to version xx of the software – (follow these instructions, load this do that and if all fails ring the Help Desk) . The project plan catered for the staging of the upgrade over 3 weeks, during which time the majority of clients would have been into the office and their SecuRemote software would be upgraded with the automatic process via the login script and only the “stragglers” would require manual intervention.

The complete exercise was simulated in a lab environment and every facet of the plan (including roll-back) was thoroughly tested to a test plan prior to giving the go-ahead and signing off on the project timeline and implementation plan.

Here is a short description of figure 1, the “Before” Firewall network diagram which is shown here again for ease of viewing .

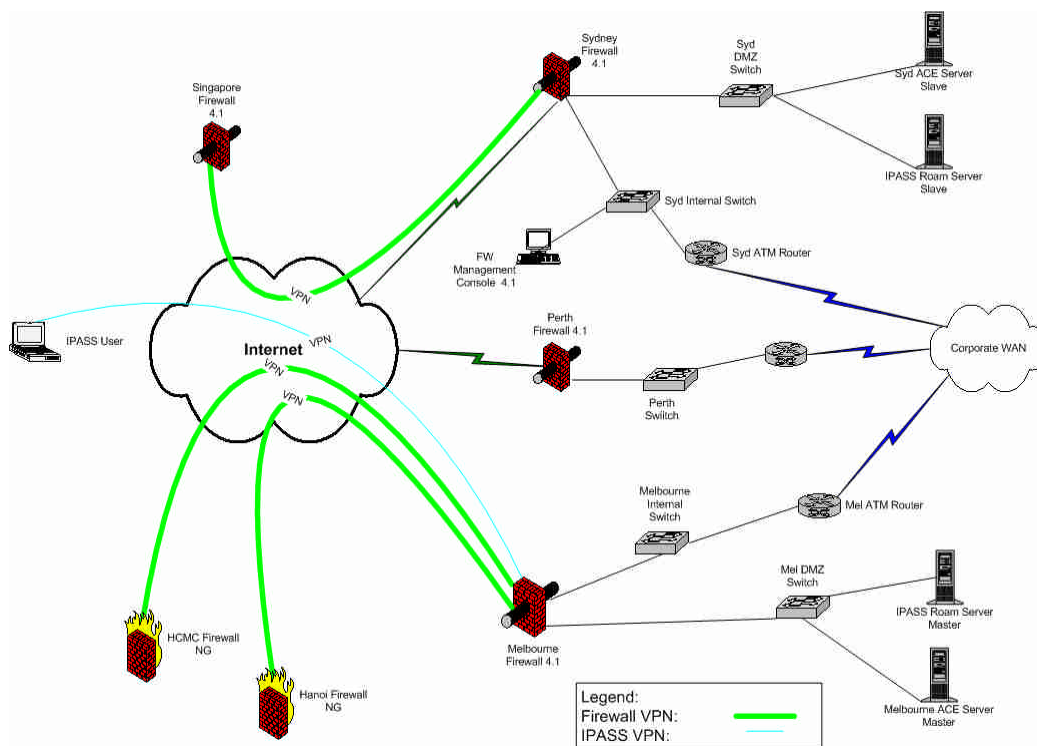


Figure 1 – The Firewall network – Before

- Our remote offices in Vietnam (Ho Chi Minh City and Hanoi) are each connected to our Melbourne firewall via a VPN which provides a path for email and data replication as well as services from our centrally located Support Services (Help) desk.

- Our Singapore office connects via a similarly configured VPN to our Sydney firewall and receives the same services .
- The three corporate firewalls in Australia (Sydney, Melbourne and Perth) are all controlled from a central Management console situated in Sydney. Each of the corporate firewalls has a path to the internet to allow clients in each office access to the internet. External email flows into the organisation via Sydney and flows outbound through Melbourne.
- Finally, any of our remote clients, from anywhere in the world, connect (via iPass) to our Melbourne firewall for authentication.

The configuration does provide full redundancy and fail-over. If the Melbourne firewall is down for any reason, then Sydney automatically takes over the role of iPass™ authentication, the Melbourne proxy server has the Sydney firewall in its secondary path and email will flow out through Sydney. In case of failure of the Melbourne firewall the VPNs need to be manually reconfigured in order to reach Sydney from Vietnam

The During phase

(Note: This procedural document describes how the project progressed to a satisfactory conclusion, it is not a “how to” document showing the commands to use, how to run the tools which assist in the upgrade process etc. The tools to use are sourced from Checkpoint but the actual description and support assistance requires a user name and password login to a secure part of the Checkpoint site. My organisation has a valid account and it was the actual Checkpoint tools and instructions which were used, but the url is useless without such an account and login credentials. A hard copy with screen shots and sample commands are attached as Appendix A, B & C to the document for completeness – and noted as such)

As with any large organisation with multiple administrators, the rules base in the existing firewall had grown as new requirements were catered for, and some of the network objects became out of date, no longer in use and potentially clogging the system. Within our organisation, there is no 1 person allowed to make firewall changes, any modifications being presented to a committee of 4, all qualified to give a proposed rule change/addition the third degree before allowing or denying the request. A consensus is required before any rules changes are authorised. Therefore in the lead up to the commencement of the project, the committee met to check each of the existing rules, make sure each of them were still required and also fully commented as to the role of each individual rule. Unnecessary rules were disabled for some weeks prior to being deleted and an independent audit was commissioned.

Each phase of the project (it was easy to split into distinct phases) was modularised as far as possible with definite end points to each module with its own milestone on the overall project plan.

Three new servers were ordered (2 to be firewalls and 1 Management console) and the software and licence keys obtained. My organisation has an up to date and independently audited process for hardening a WIN2000 server and the new firewalls were built side by side and hardened in the same way with all unnecessary services turned off. The NG software with the latest FP (feature pack) was installed, and as these new firewalls were to be employed to look after just the remote access solution, only the portion of the rules base which pertain to the remote access solution of iPass™ and SecuRemote were applied to the new firewalls. They were lab tested and then shipped to their final destination. The new management console, which resides in Melbourne, was built and functionally tested with the new firewalls.

The new management console was brought into operation, followed by the Sydney NG firewall. At this juncture, the NG firewall was doing nothing as the rules were set only for the remote access or to drop the packets and as no clients were set-up to access this box, no traffic could get through. The old 4.1 firewall was still handling all remote access traffic. The iPass™ organisation were given the ip addresses of the new firewalls to add to their authentication databases to permit authentication via this path.

A pilot group had been identified and their section of the login script was modified to install the NG client and make the necessary configuration changes to their laptops. The modifications ensured they would authenticate against the new Sydney NG firewall. An information email had been circulated throughout the pilot group beforehand and a request was issued asking them to use the remote solution as soon as was practical once the modification had been applied. All were able to authenticate to the corporate network without any problem and an investigation of the logs revealed they were authenticating against the NG firewall in Sydney.

The team who set up and support our laptop fleet now swung into action and all new laptops were supplied with the NG client installed, and when tested in the field, these client machines were seen to be correctly authenticating against the Sydney NG firewall.

Following this successful pilot the Melbourne NG firewall was installed.

After a week of problem free operation, the next group were upgraded via the login script, and the logs closely scrutinised to ensure everyone had been able to login to the network from a remote location. This was an imperative since with 700+ remote users, not everyone would have been into the office during the client phase and if they had not run the login script, which was responsible for making the configuration changes as well as installing the new client, we ran the risk of leaving these people in limbo. The list of successful logins was maintained and the stragglers identified for later manual update. It took 3 weeks to upgrade the bulk of the clients (689) using the login script and a relatively simple manual procedure communicated to those who had not been to the office.

At this point it was considered that the remote access module of the project, installing the new NG firewalls and Management console and ensuring the clients authenticate against the new firewalls was complete.

Figure 2 shows a diagram of the project when the initial pilot group and the new iPass™ clients are authenticating against the new NG firewalls. It shows that most of the iPass™ clients are still authenticating against the Melbourne Firewall 4.1. N.B. The FW Management Console NG in Melbourne controls only the 2 new Sydney and Melbourne NG firewalls.

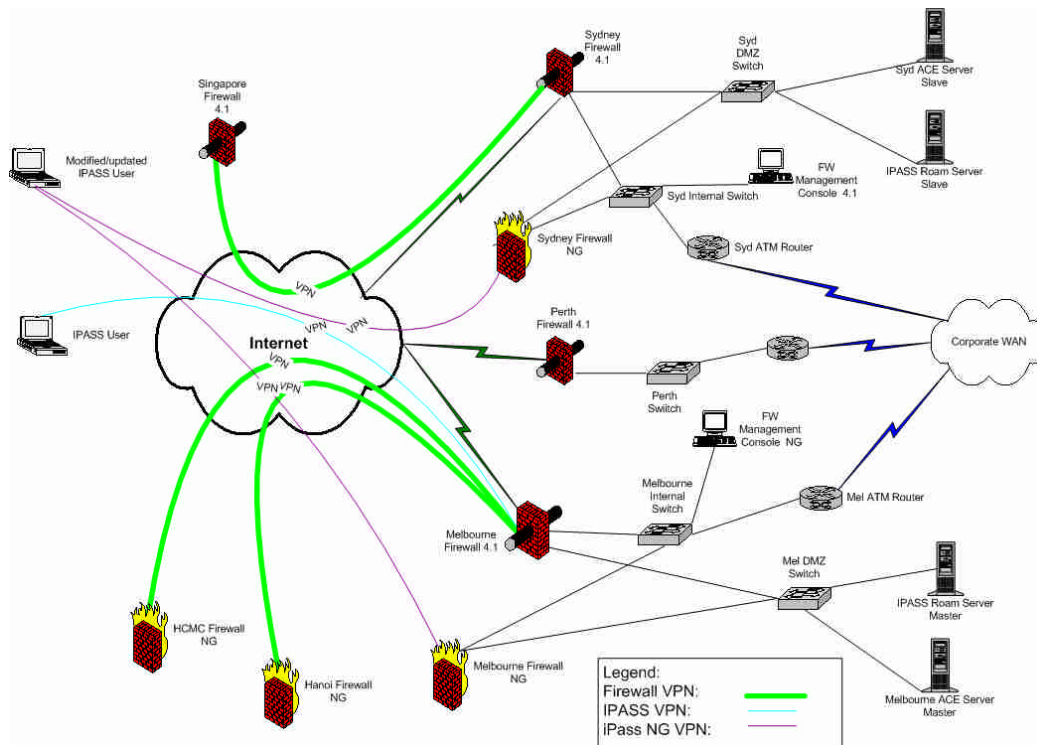


Figure 2 – The Firewall Network – mid phase

It was now time to upgrade the existing 4.1 Sydney Management Console machine. The Management console must be upgraded first as an NG console can control 4.1 firewalls but a 4.1 console cannot control an NG firewall.

To expedite this process, a high-end desktop machine was configured to take the place of the Management console whilst the actual console machine was being upgraded to NG. It was given the same IP address, rules base, configuration, OS level. There is no problem in turning off the existing console and bringing up this replacement as no attempt was being made to modify rules/objects etc within the firewalls during this change over period. Whilst the “surrogate” was in place, the real console machine was being reinstalled with WIN2000 (hardened to current corporate specification -

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/Windows/Win2kHG/06Tmplts.asp>) and the relevant Checkpoint module.

The firewall administrators' workstations which are permitted to access the Management console remotely via the Checkpoint GUI were also updated to the NG version. Before progressing to the next step, the actual upgraded Management Console machine was returned to production and the “surrogate” removed.

Next the focus changed to the upgrade process for the existing 4.1 firewalls following the official Checkpoint procedures attached in Appendix B.

The Sydney firewall was upgraded first of all. All the mail functions and web browsing were redirected across the corporate WAN to our Melbourne office. Our client base did not have to do anything, and didn't even know there was

such a major event happening in the background. We took a commercial decision to terminate the VPN to our Singapore office and a couple of other VPNs to some of our external clients for the 6 hour window required to upgrade the 4.1 firewall to NG.

The same hardening process was followed for the OS, the relevant Checkpoint modules were added and most important, the existing rules base was applied to the upgraded unit (going through the exercise of changing the rules and upgrading the software in the same phase was considered an unacceptable risk). The firewall was brought back up, the VPNs reinitialised (required a person on site in Singapore) and early on the first day the VPNs were reinitialised with our external clients. The mail flow and internet service was redirected back to this 4.1 firewall which had now been upgraded to NG and all this happened without the bulk of the 750 people in our Sydney office being any the wiser.

Melbourne was next, and this time all traffic was redirected across the WAN to Sydney and in/out through the Sydney gateway. Again, it was acceptable to the business to take the VPNs to Hanoi and Ho Chi Minh City off the air for the duration of the upgrade downtime (less than 6 hours in this case), the same process performed (hardening, services stopped, software installed) and once again the existing rules base applied to the now NG firewall and the VPNs in Hanoi and Ho Chi Minh City re-established.

Perth was next, relatively simple as Perth's role is solely an internet gateway to the Perth staff (about 450 people) – it has no mail function and no VPNs. Simply re-routing the internet traffic across the WAN to Sydney for the duration of the upgrade process is all that was required.

The final upgrade was to the Singapore firewall, which is a Nokia IP120 device. It was considered safer to employ the local supplier of Nokia devices to send one of their engineers to the site to act in tandem with our firewall engineer in Melbourne to go through the upgrade process in Singapore and re-establish the VPN to the Sydney office.

The final part of the upgrade phase was to reappraise the rules in the firewalls which had been upgraded from 4.1 to NG. One of the clearly stated objectives of the project was to divorce the remote access solution from the overall corporate firewall solution in order to create an environment where each "module" was independent of the other. The rules base in the upgraded firewalls were now modified to disable all those rules which were associated with the remote solution, thereby isolating our remote clients to the new firewalls only. This was a critical point, because if we had missed anyone out, or misconfigured their computer in any way, there was now only one way into the corporate network, via a whole new firewall structure. I am delighted to report that not one of our clients has experienced any problem, all are authenticating to the correct firewall and the project hailed as a major success.

The After Phase

To gain a better understanding of the firewall network within my organisation post upgrade, please read the following in conjunction with the diagram in Figure 3 below.

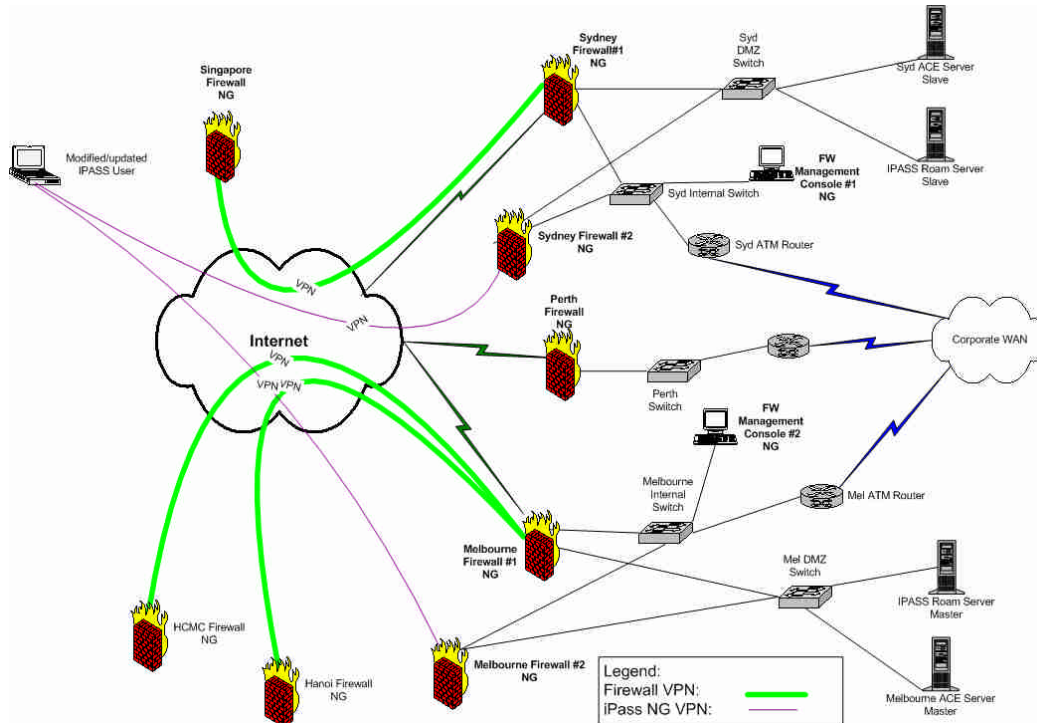


Figure 3 – The Firewall Network – Completed

- The new firewalls introduced as part of this project are depicted as **Firewall #2 NG** in the Sydney and Melbourne offices .
- The **FW Management Console#2 NG** is the new console device for these 2 firewalls. These machines (in conjunction with the Room servers and ACE servers in the two offices) form the “module” which is the basis for the remote access solution for the whole organisation. All our iPass/SecuRemote™ clients authenticate to either one of these two firewalls and this solution is wholly “self contained”.
- What had been the existing corporate 4.1 firewalls in Sydney, Melbourne and Perth, now identified as **OfficeName#1NG** are under the control of the Management console in Sydney (**FW Management Console #1NG**) and continue to control internet access, mail flow and VPN access .

The separation of the functions to two distinct firewall groupings has without any doubt increased the security of our perimeter defences as a whole. The move to NG has given birth to the subsequent project (not covered here) of applying Checkpoint SecurClient to the remote computers which has a feature

of a personal firewall with a rules base which is maintained from the FW Management Console #2NG. This has reduced the risk posed from the remote computers being attached to “always on” connections and therefore vulnerable to attack and subsequent infection/compromise of the corporate network.

The second benefit gained from separating the functions is from this point onward, any firewall modifications/software upgrade need not upset the remote solution, nor does it have to wait until a suitable window of opportunity opens before the modifications can be applied. The risk of compromise due to an unpatched system is therefore minimised.

The perimeter defence system has become slightly more complex with the introduction of 2 more firewalls and a new management console, but clear and concise drawings and documentation help to minimise the complexity and explain each and every scenario to mitigate the risk.

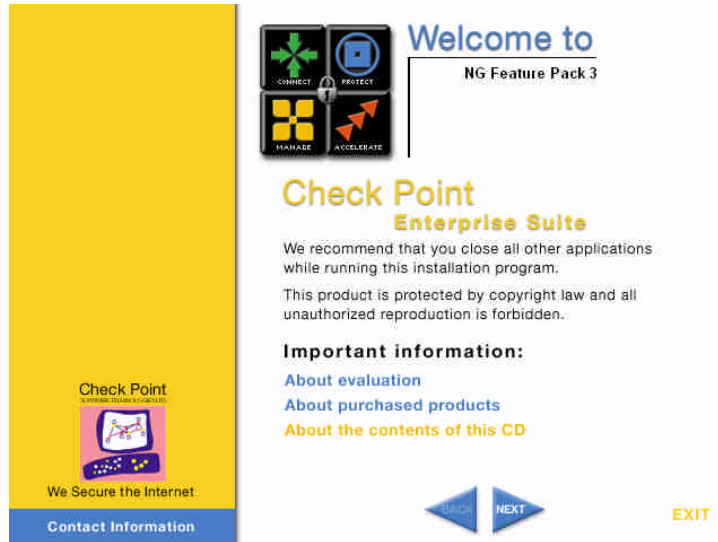
Collectively my team examined, defined and overcame the risks one by one in the planning stages of the project, and the result clearly indicates that we were correct in our thinking and implementation. Indeed, but for the fact that installing the new client is not transparent and requires user acknowledgement of reboot, our client base would have been transferred to a totally new method of remote authentication without them even knowing – which is a good result for 700 clients spread not just across this continent, but in other parts of the world.

Appendix A

Installing Firewall NG Management Server

This entire appendix sourced from Checkpoint Technical Services Department, NG Upgrade Centre

Insert the Check Point (Internet Security Solutions) CD.
Once the CD starts Click next.



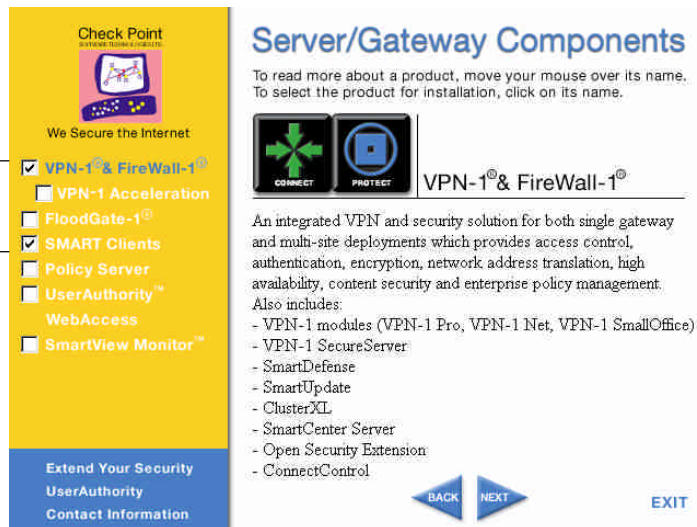
Click Yes



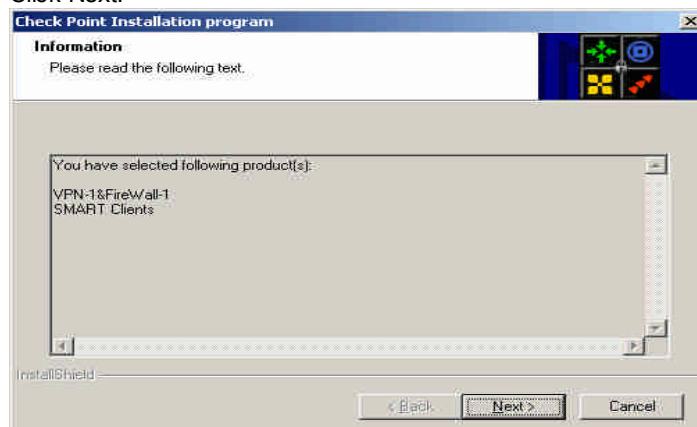
Select Server/Gateway Components and click Next.



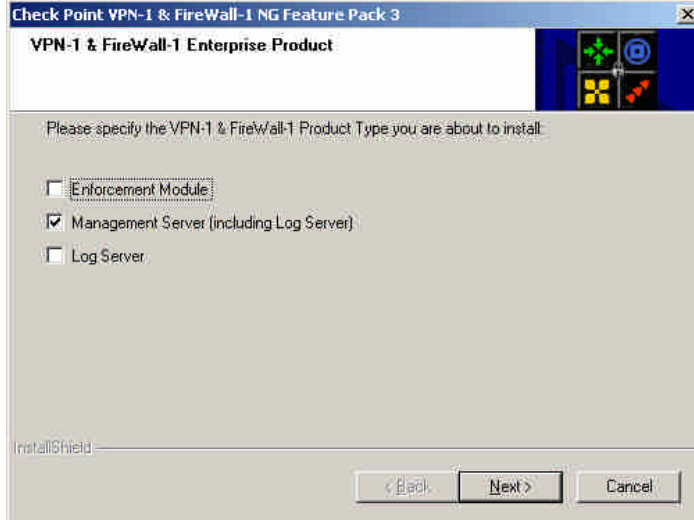
Select VPN-1 & Firewall-1
Select Smart Clients
Click Next.



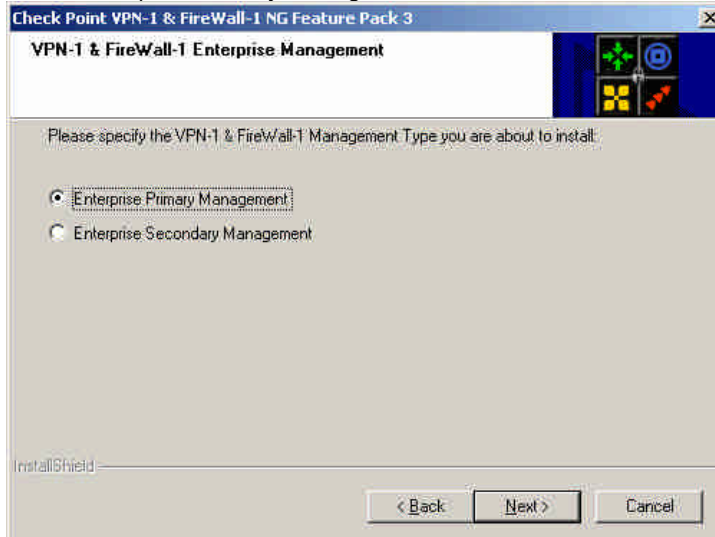
Click Next.



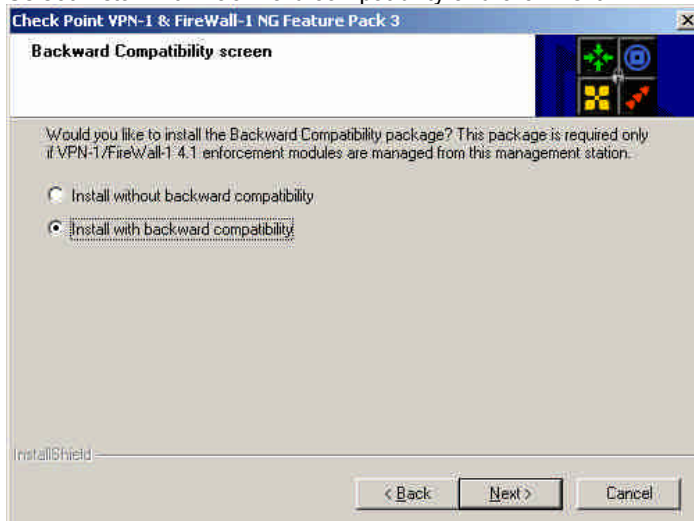
Select Management Server (Including Log Server) and click Next.



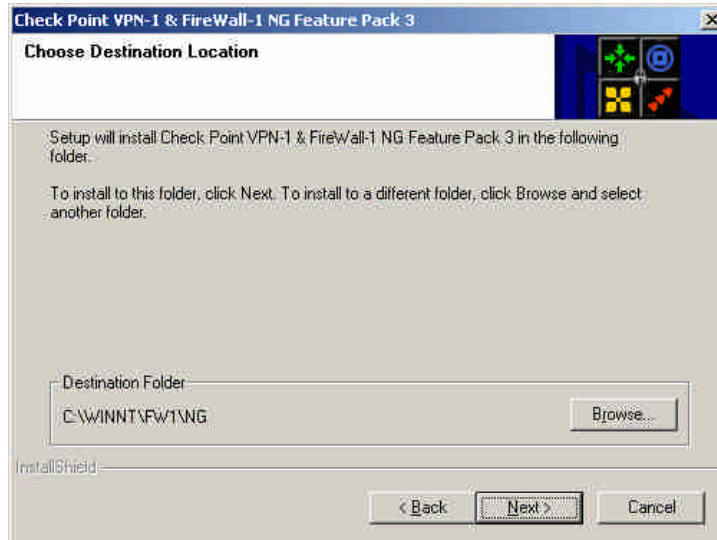
Select Enterprise Primary Management and click Next.



Select Install with Backward compatibility and click Next.



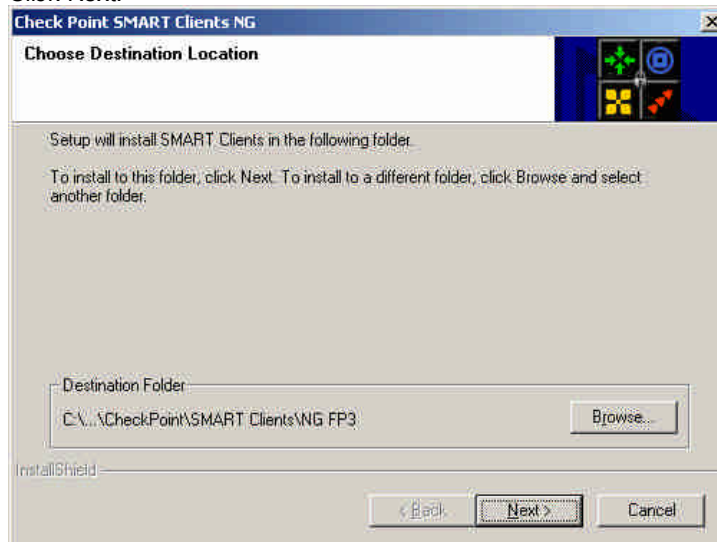
Select Next



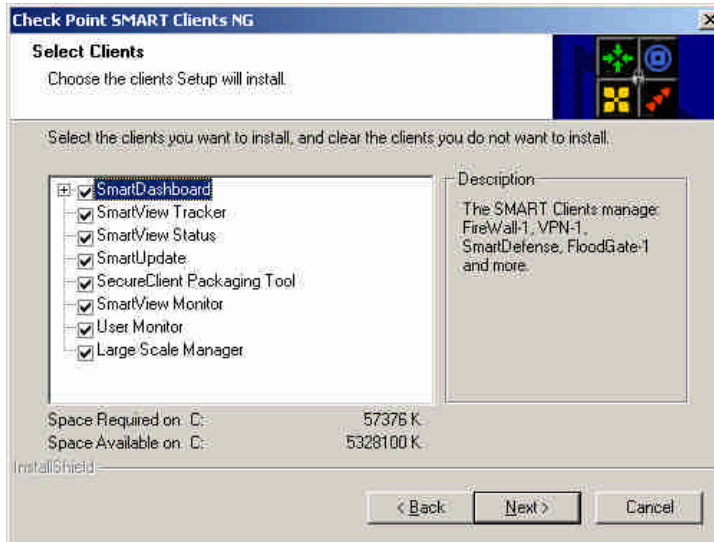
Click OK



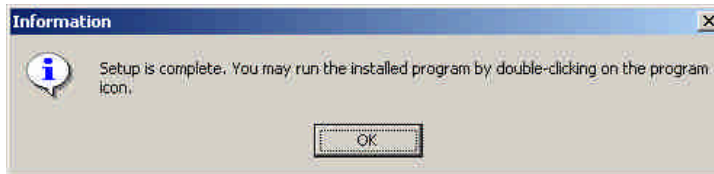
Click Next.



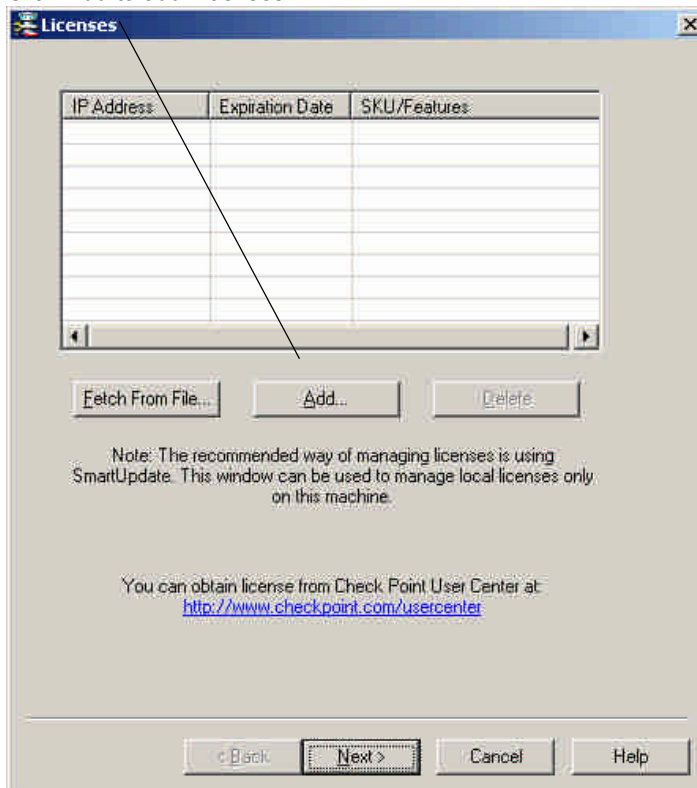
Select all and click Next.



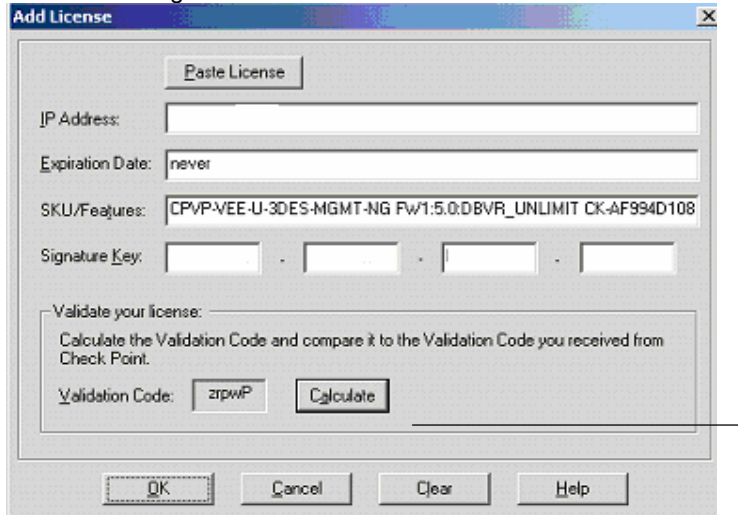
Click OK.



Click Add to add Licenses.



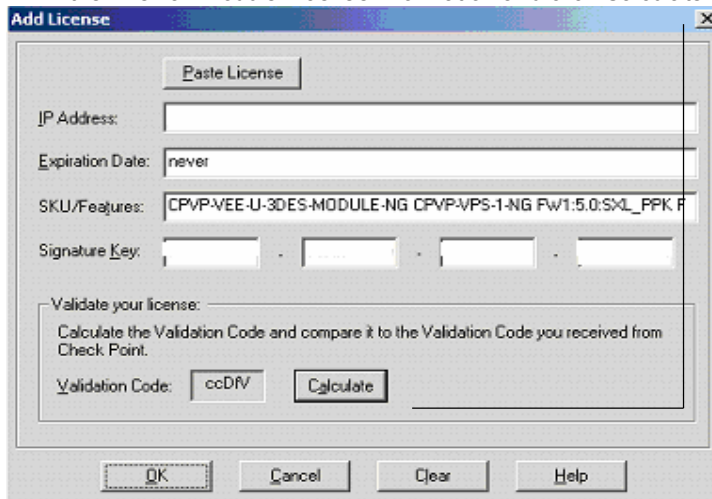
Fill in the Management Server License information and click Calculate then OK,



The 'Add License' dialog box contains the following fields and controls:

- Paste License** button
- IP Address:** text field
- Expiration Date:** dropdown menu showing 'never'
- SKU/Features:** text field containing 'CPVP-VEE-U-3DES-MGMT-NG Fw1:5.0:DBVR_UNLIMIT CK-AF994D108'
- Signature Key:** four text fields separated by hyphens
- Validate your license:** section with instructions: 'Calculate the Validation Code and compare it to the Validation Code you received from Check Point.'
- Validation Code:** text field containing 'zrpwP'
- Calculate** button
- OK**, **Cancel**, **Clear**, and **Help** buttons at the bottom.

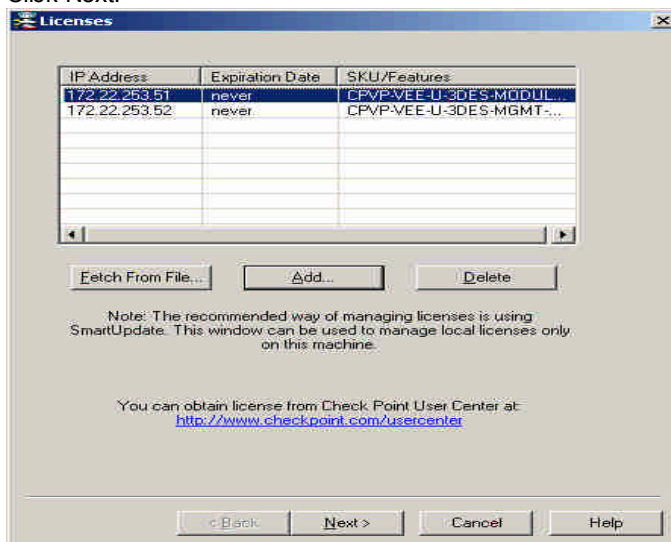
Fill in the Firewall Module License information and click Calculate then click OK.



The 'Add License' dialog box contains the following fields and controls:

- Paste License** button
- IP Address:** text field
- Expiration Date:** dropdown menu showing 'never'
- SKU/Features:** text field containing 'CPVP-VEE-U-3DES-MODULE-NG CPVP-VPS-1-NG Fw1:5.0:SKL_PPK F'
- Signature Key:** four text fields separated by hyphens
- Validate your license:** section with instructions: 'Calculate the Validation Code and compare it to the Validation Code you received from Check Point.'
- Validation Code:** text field containing 'ccDM'
- Calculate** button
- OK**, **Cancel**, **Clear**, and **Help** buttons at the bottom.

Click Next.



The 'Licenses' window displays a table of installed licenses:

IP Address	Expiration Date	SKU/Features
172.22.253.51	never	CPVP-VEE-U-3DES-MODUL
172.22.253.52	never	CPVP-VEE-U-3DES-MGMT...

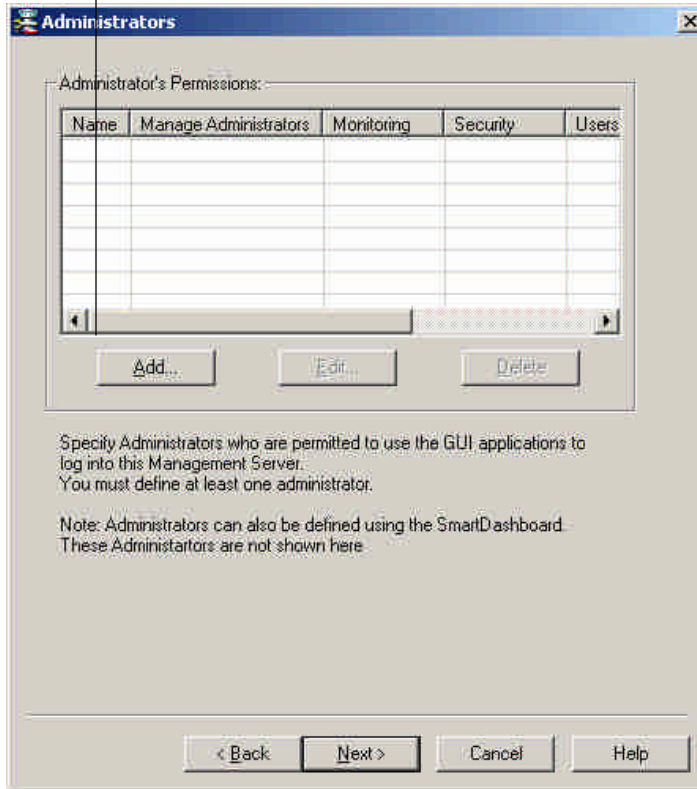
Below the table are buttons: **Fetch From File...**, **Add...**, and **Delete**.

Note: The recommended way of managing licenses is using SmartUpdate. This window can be used to manage local licenses only on this machine.

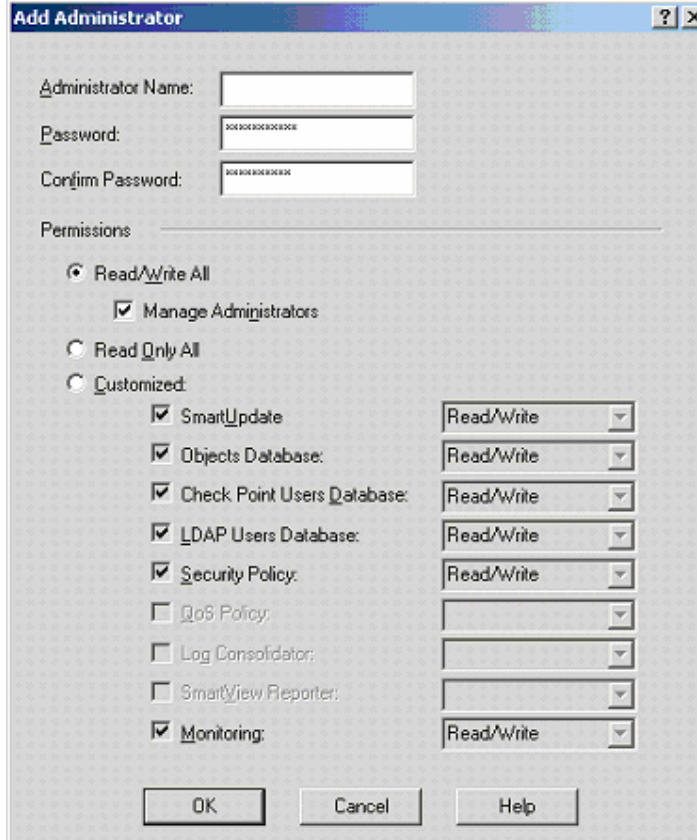
You can obtain license from Check Point User Center at: <http://www.checkpoint.com/usercenter>

At the bottom are buttons: **< Back**, **Next >**, **Cancel**, and **Help**.

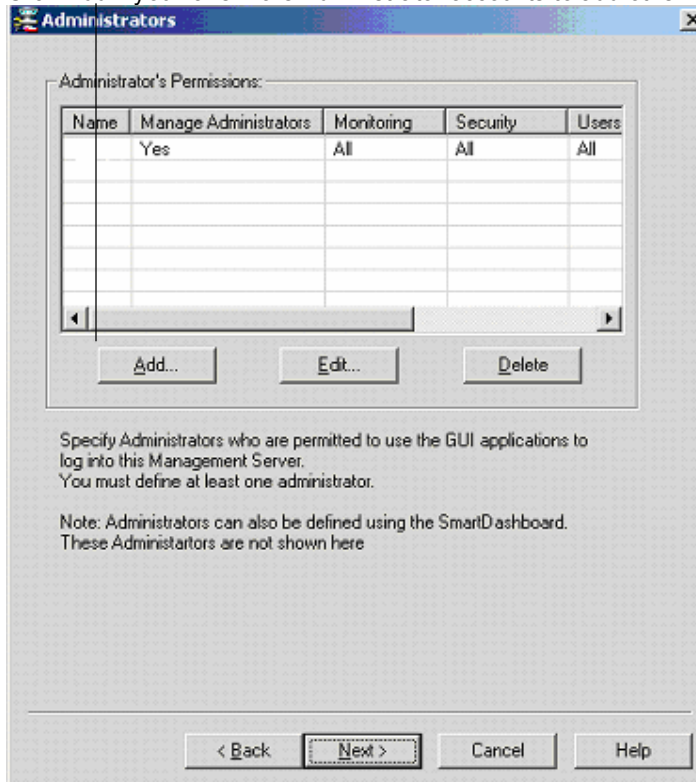
Click Add to add Administrator Account.



Fill in the user id and password and select default settings (as shown below) and click OK.



Click Add if you have more Administrator accounts to add otherwise click Next.



Administrators

Administrator's Permissions:

Name	Manage Administrators	Monitoring	Security	Users
	Yes	All	All	All

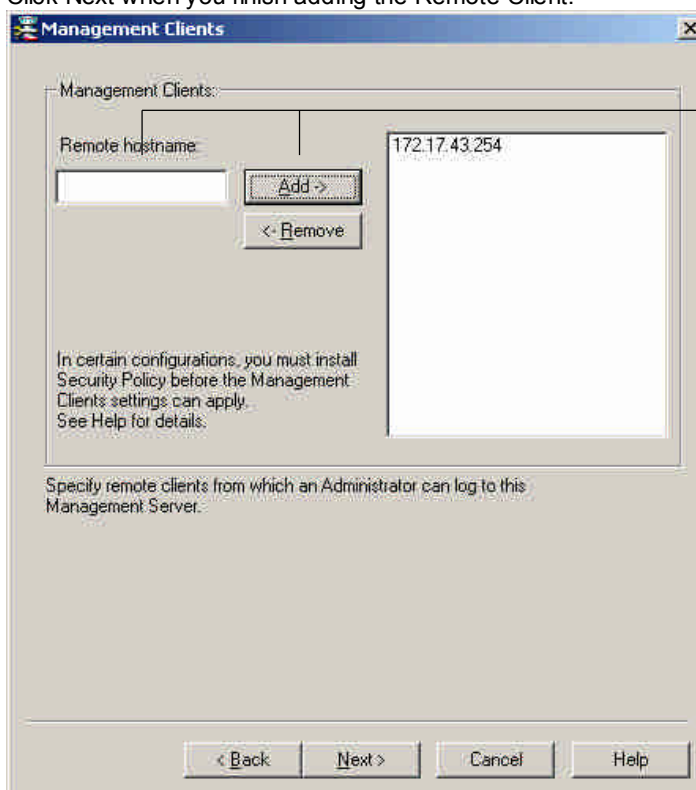
Add... Edit... Delete

Specify Administrators who are permitted to use the GUI applications to log into this Management Server.
You must define at least one administrator.

Note: Administrators can also be defined using the SmartDashboard.
These Administrators are not shown here

< Back Next > Cancel Help

Insert the IP address of the Remote Client into the Remote Hostname then click Add. Click Next when you finish adding the Remote Client.



Management Clients

Management Clients:

Remote hostname: 172.17.43.254

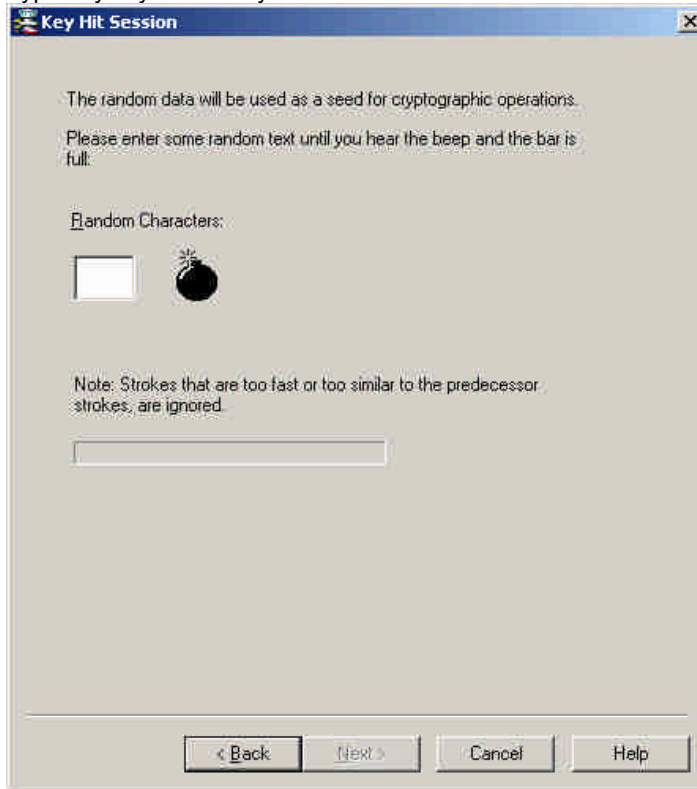
Add-> <- Remove

In certain configurations, you must install Security Policy before the Management Clients settings can apply.
See Help for details.

Specify remote clients from which an Administrator can log to this Management Server.

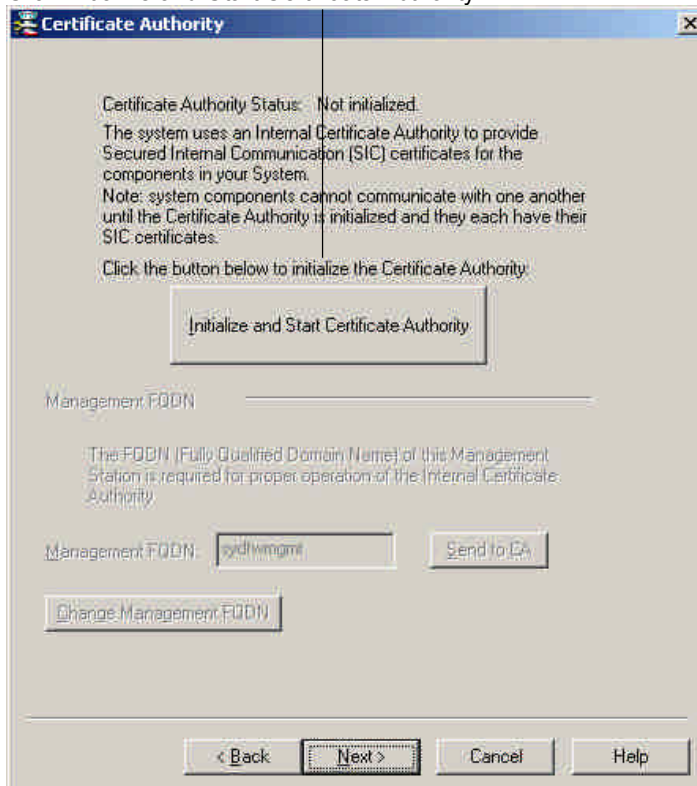
< Back Next > Cancel Help

Type any key on the keyboard until the Next button becomes enabled. Then click Next.



Click Next.

Click Initialize and Start Certificate Authority.



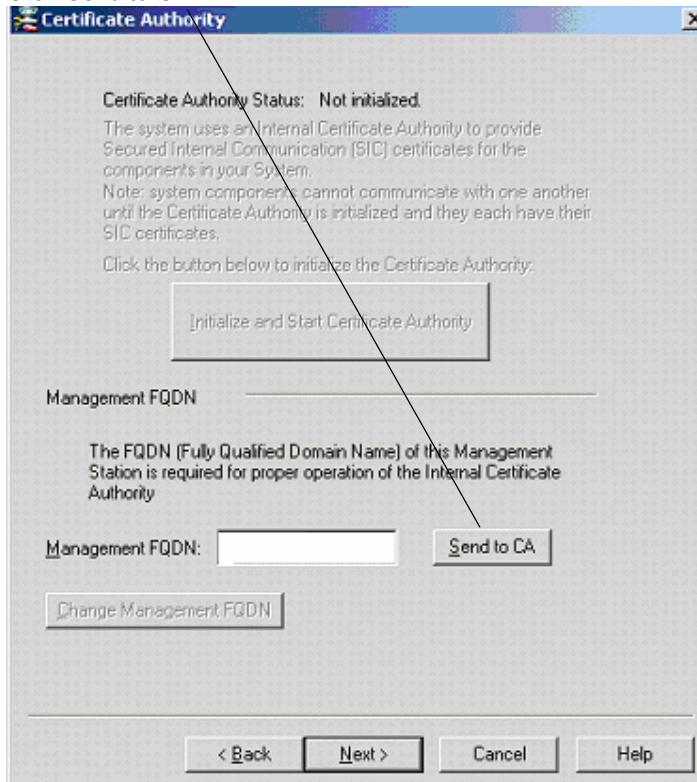
Click OK.



Click OK.



Click Send to CA.



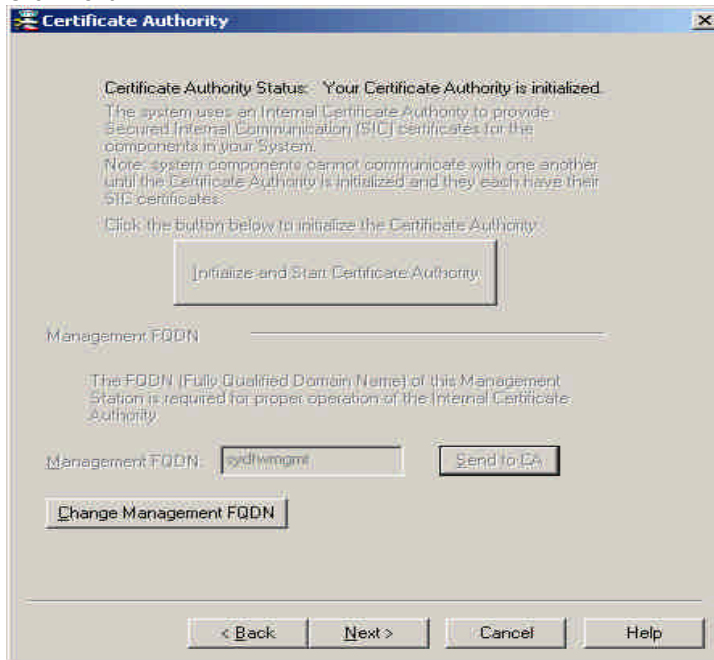
Click OK.



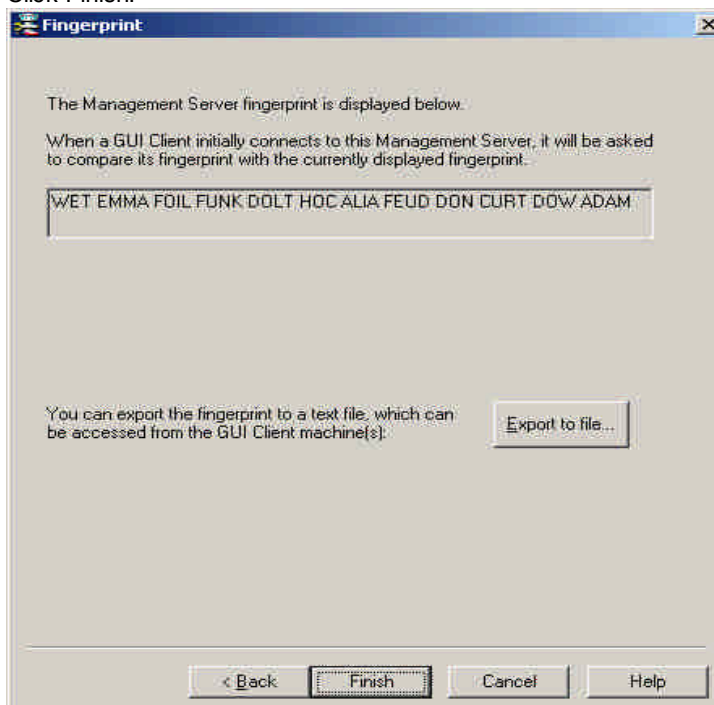
Click OK.



Click Next.



Click Finish.



Appendix B

Upgrade from Checkpoint 4.1 to Checkpoint NG

This entire appendix sourced from Checkpoint Technical Services Department, NG Upgrade Centre

From Firewall NG Management Server

Use the Upgrade Tool to migrate existing Objects and Rules from one machine to another, without having to upgrade the production machine.

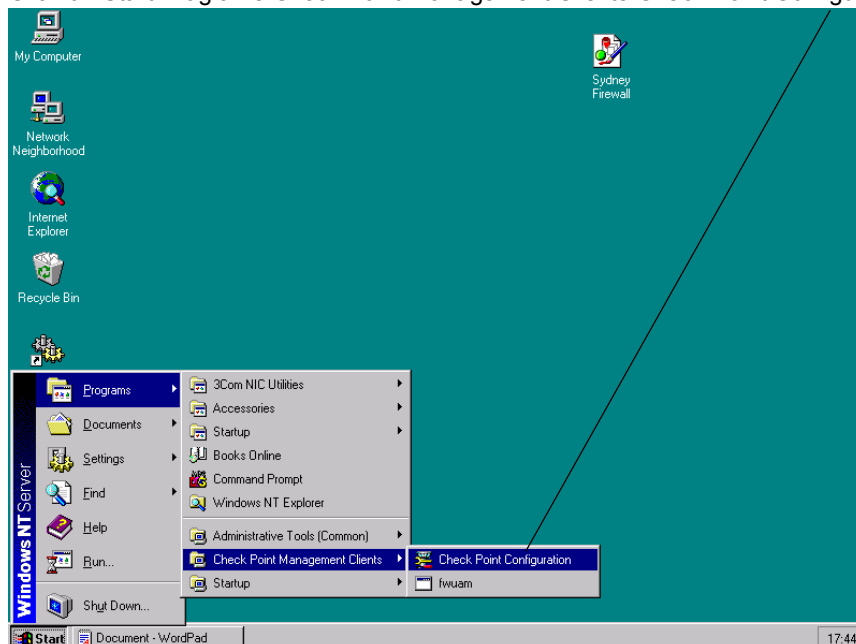
It is recommended to use the Upgrade Verifier Utility prior to the actual upgrade.

To migrate from Check Point Management Server 4.1 to Check Point Management Server NG FP1 and above using the Upgrade Tool, proceed as follows:

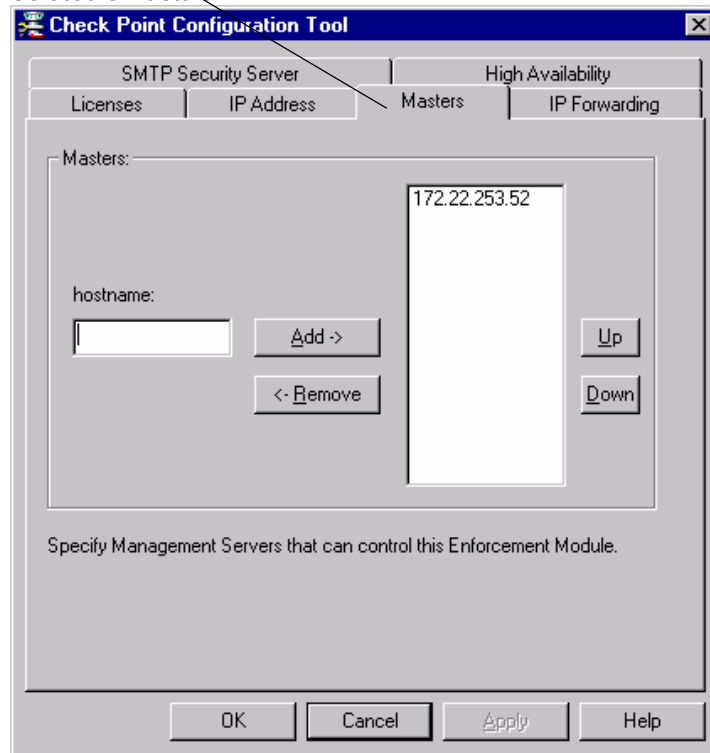
1. Perform a new installation of the desired version (FP1, FP2, etc...) on a new machine.
2. Download and unzip the [upgrade_53008.tgz](#) file (MD5: 57b4180593704265c6187f1674b3deec). It opens into a directory named upgrade. The file "last update" date is December 29, 2002.
3. Unzip the upgrade_53008.tgz into the Firewall management server c: \temp\upgrade
4. Place the following version 4.1 files under the c: \temp\upgrade\4.1 directory:
 - a. objects.C
 - b. fwauth.NDB (on Windows machines this file is only the pointer to the real database file, for example, fwauth.NDB522. In this case take the real database file (fwauth.NDB522), rename it to fwauth.NDB and put it in the \upgrade\4.1 directory
 - c. rulebases.fws
 - d. fgrulebases.fws (if FloodGate -1 is installed)
5. c:\temp\upgrade\upgrade c: \temp\upgrade FP3
6. net start "Check Point Firewall -1" or c:\winnt\fw1\ng\bin\fwstart

From Firewall Module Version 4.1 server

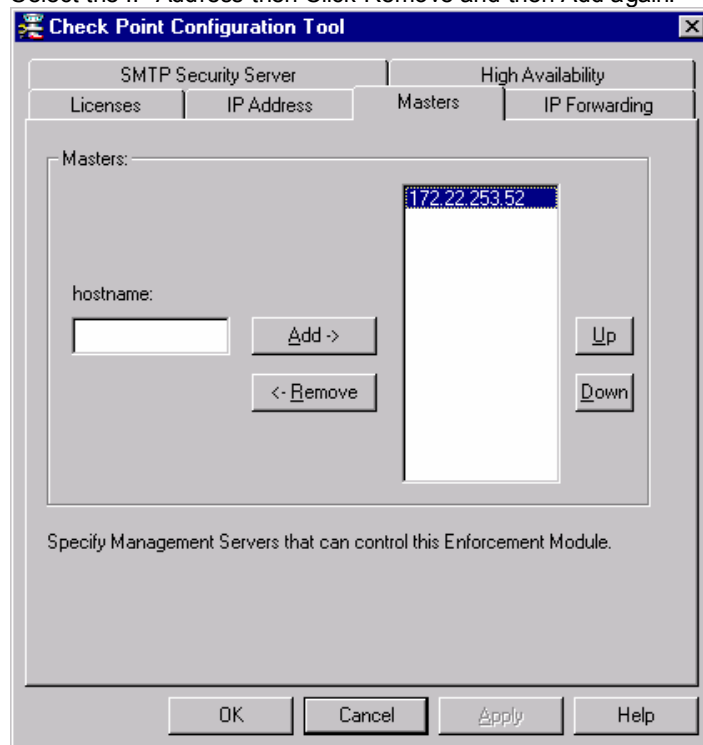
Click on Start/Programs/Check Point Management Clients/Check Point Configuration.



Select the Masters TAB.



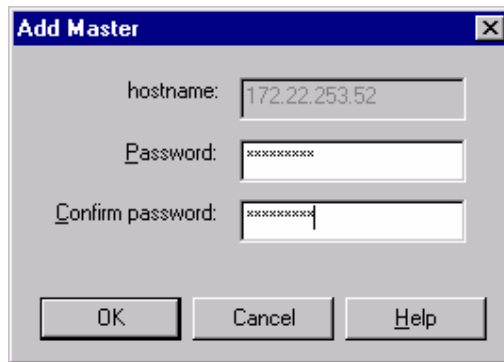
Select the IP Address then Click Remove and then Add again.



Type the secret password in the Password field eg |*|&@##\$|~!?

Type the secret password in the Confirm password field eg |*|&@##\$|~!?

Click OK.



Add Master

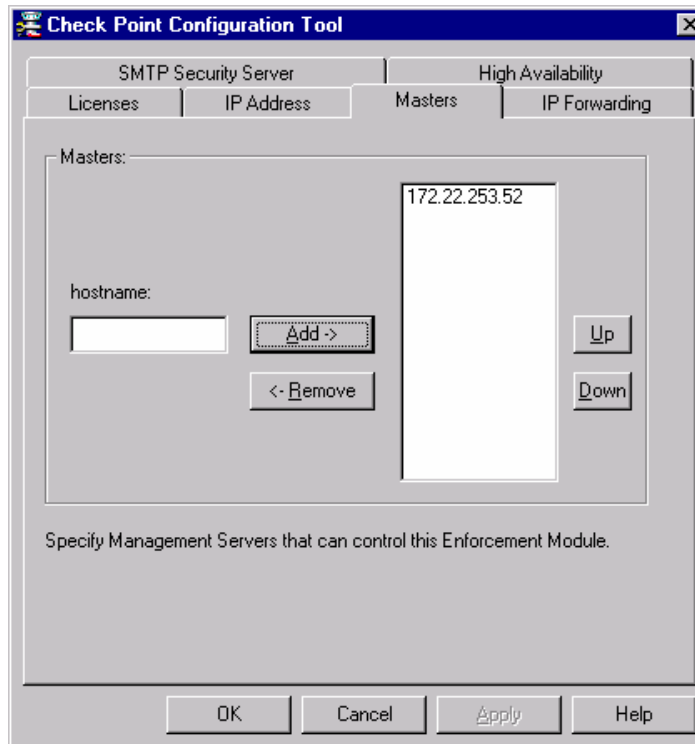
hostname: 172.22.253.52

Password: xxxxxxxx

Confirm password: xxxxxxxx

OK Cancel Help

Click OK.



Check Point Configuration Tool

SMTP Security Server High Availability

Licenses IP Address Masters IP Forwarding

Masters:

hostname: Add -> Up

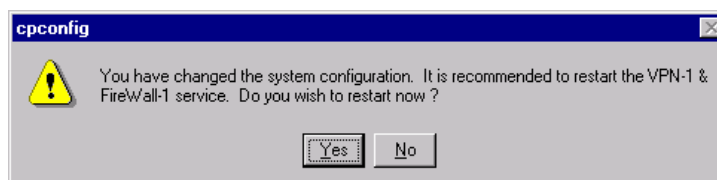
< - Remove Down

172.22.253.52


Specify Management Servers that can control this Enforcement Module.

OK Cancel Apply Help

Click Yes.



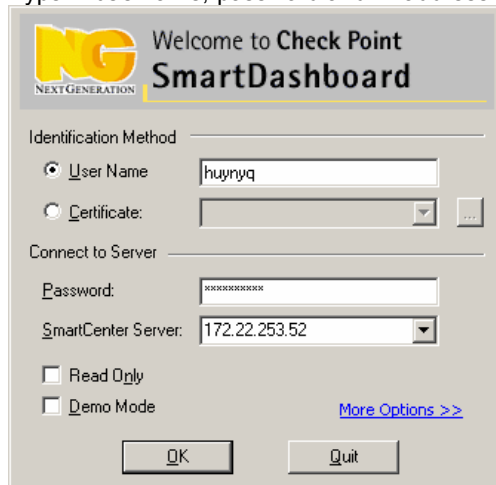
cpconfig

 You have changed the system configuration. It is recommended to restart the VPN-1 & FireWall-1 service. Do you wish to restart now ?

Yes No

From Firewall NG Management Server

Type in username, password and IP address of the Management Server and click OK.



Welcome to Check Point SmartDashboard

Identification Method

☒ User Name:

☐ Certificate:

Connect to Server

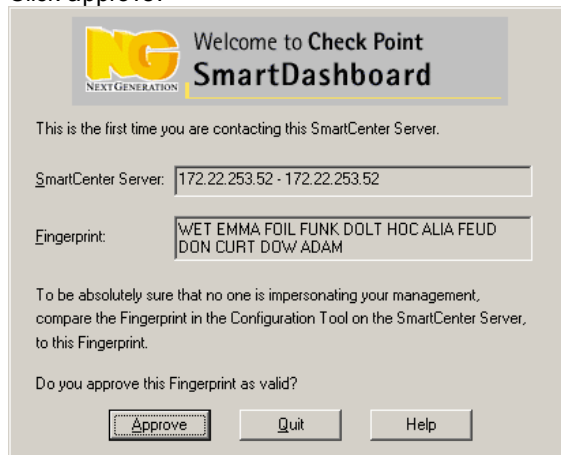
Password:

SmartCenter Server:

☐ Read Only

☐ Demo Mode [More Options >>](#)

Click approve.



Welcome to Check Point SmartDashboard

This is the first time you are contacting this SmartCenter Server.

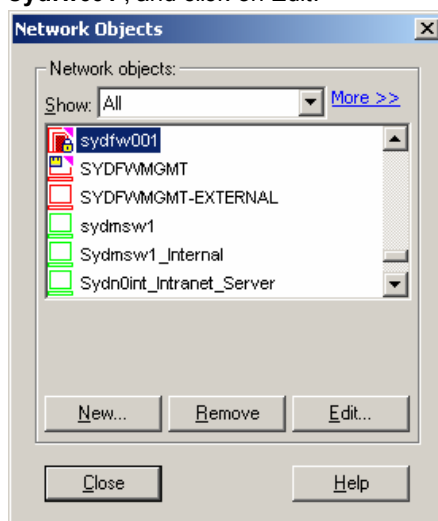
SmartCenter Server:

Fingerprint:

To be absolutely sure that no one is impersonating your management, compare the Fingerprint in the Configuration Tool on the SmartCenter Server, to this Fingerprint.

Do you approve this Fingerprint as valid?

Select the Firewall Object of the Firewall module you want to communicate too eg. **sydfw001**, and click on Edit.



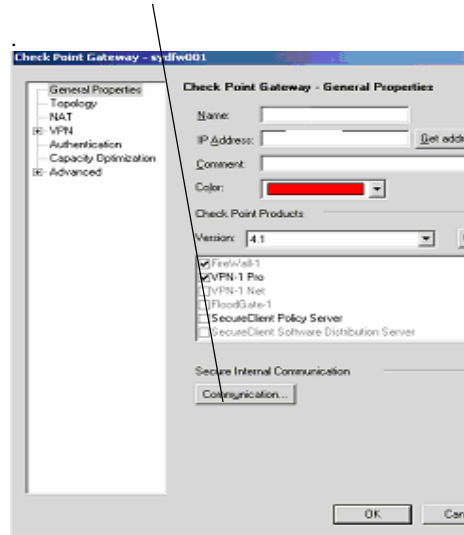
Network Objects

Network objects:

Show: [More >>](#)

- ☒ sydfw001
- ☐ SYDFVMGMT
- ☐ SYDFVMGMT-EXTERNAL
- ☐ sydmw1
- ☐ Sydmw1_Internal
- ☐ Sydn0int_Intranet_Server

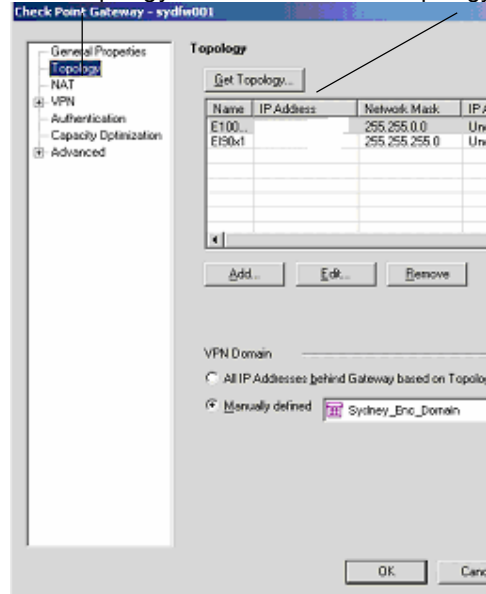
Click Communication



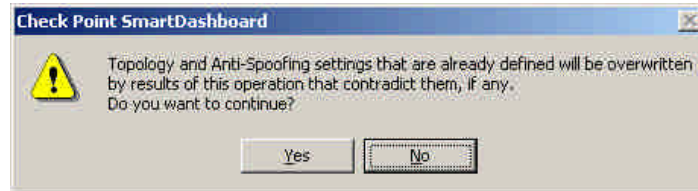
Type the secret password in the Module Activation Key Eg |*|&@##\$|~!?
Type the secret password i n the Confirm Activation Key Eg |*|&@##\$|~!?
Click Initialize.



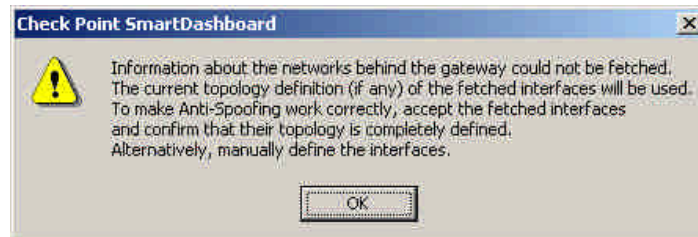
Click Topology and then select Get Topology.



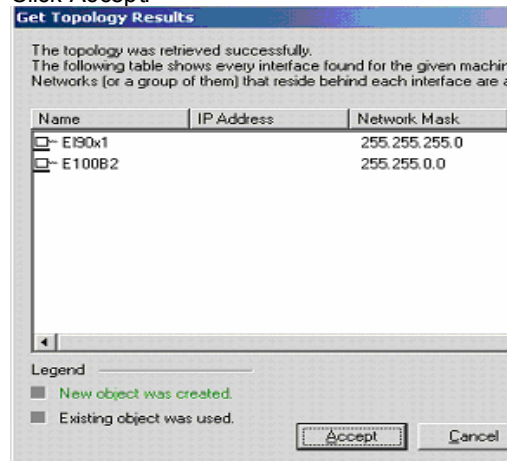
Click Yes.



Click OK.



Click Accept.



Click Yes.



From Firewall Module Version 4.1 server

From a Dos prompt and type:

```
c:\winnt\fw1\4.1\bin\fw putkey -p <password and ip addr>
```

From Firewall NG Management Server

From a Dos prompt and type:

```
c:\winnt\fw1\ng\bin\fw putkey -p <password and ip addr>
```

```
c:\winnt\fw1\ng\bin\fwstop
```

```
c:\winnt\fw1\ng\bin\fwstart
```


From Firewall Module Version 4.1 server

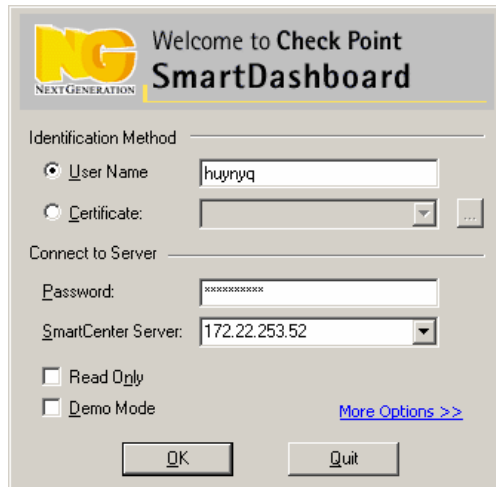
From a Dos prompt and type:

c:\winnt\fw1\ng\bin\fwstop

c:\winnt\fw1\ng\bin\fwstart

From Firewall NG Management Server

Type in username, password and IP address of the Management Server and click OK.



Welcome to Check Point
SmartDashboard

Identification Method

☒ User Name:

☐ Certificate:

Connect to Server

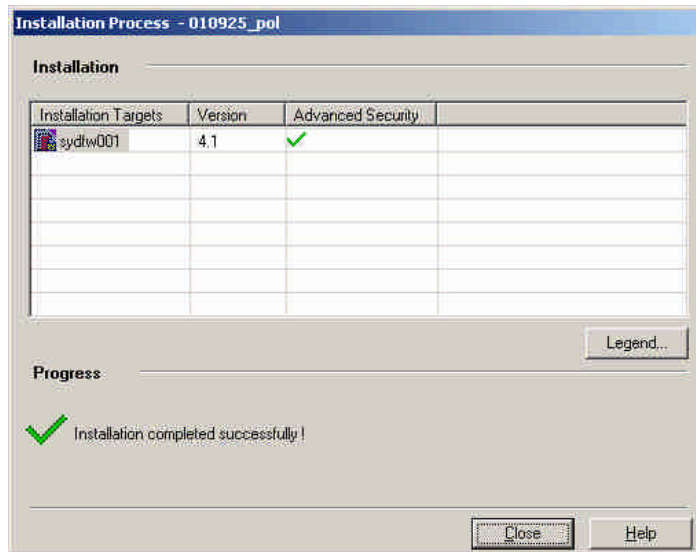
Password:

SmartCenter Server:

☐ Read Only

☐ Demo Mode [More Options >>](#)

Install Rules into the Firewall Module and click Close.



Installation Process - 010925_pol

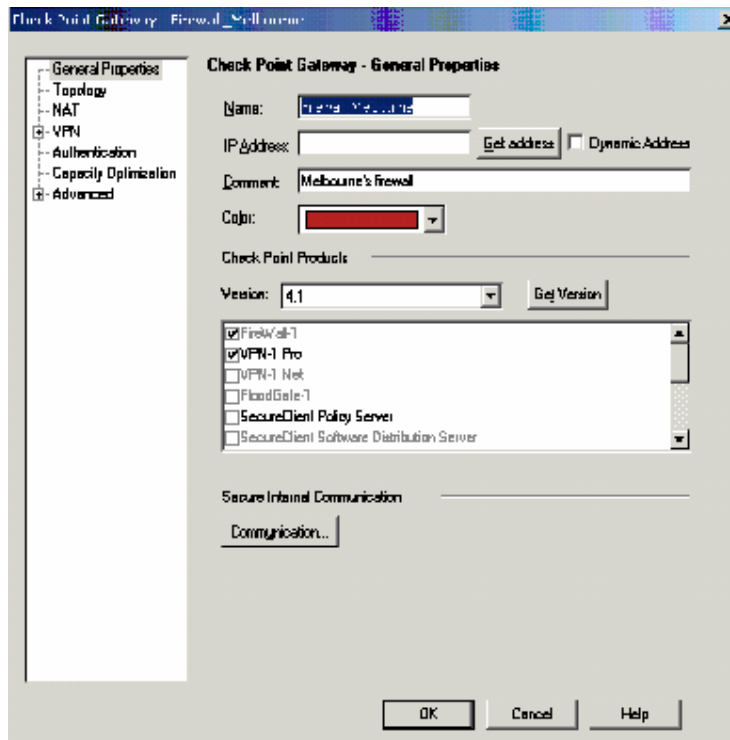
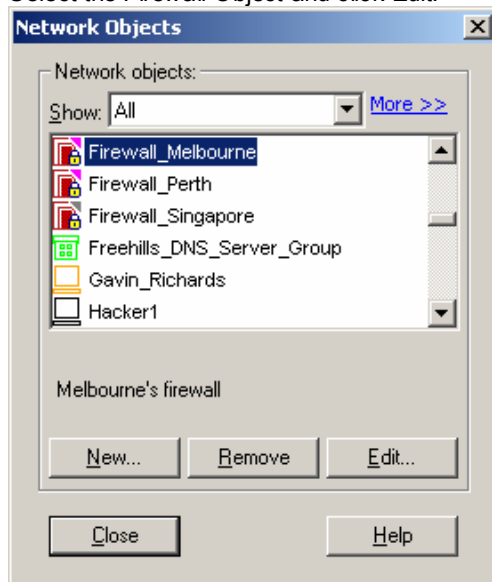
Installation

Installation Targets	Version	Advanced Security
sydlw001	4.1	✓

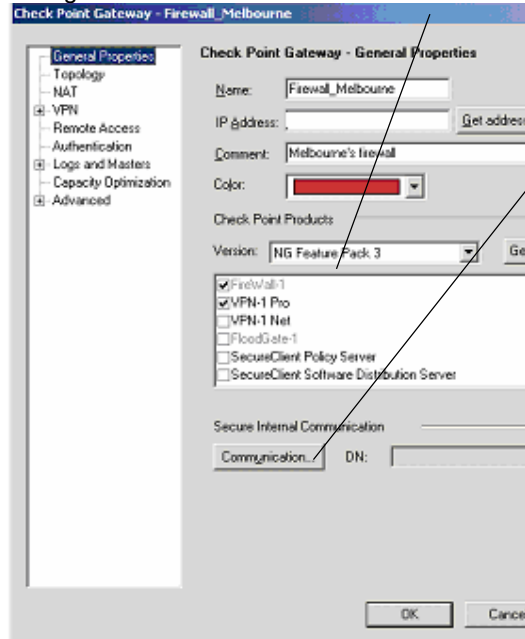
Progress: ☒ Installation completed successfully!

Configure Firewall NG Management Server to communicate to Firewall NG Module

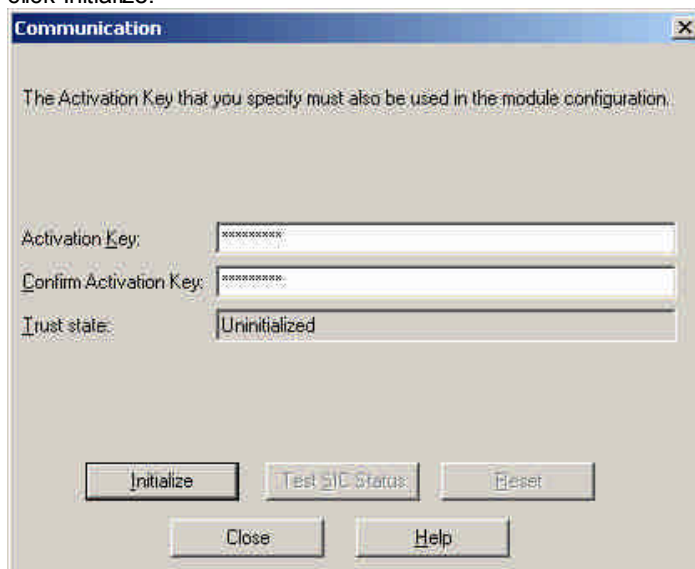
Select the Firewall Object and click Edit.



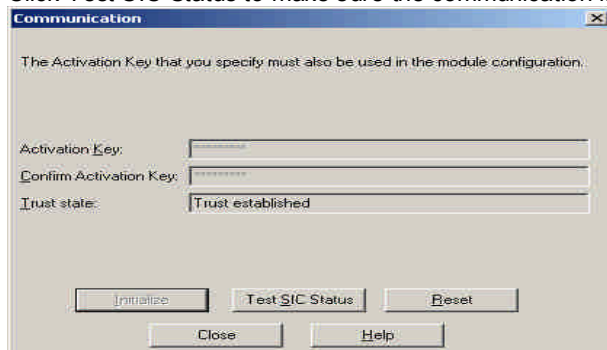
Change version from 4.1 to NG Feature Pack 3 and click Communication.



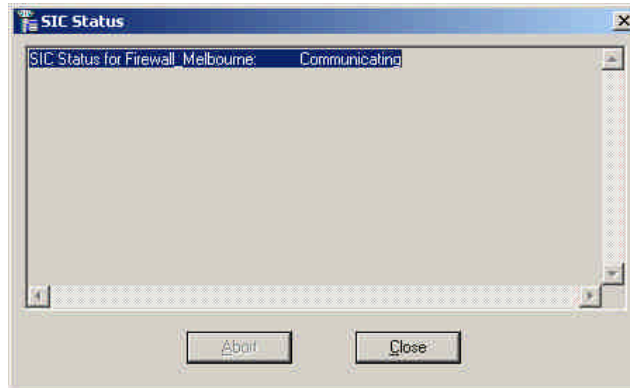
Type in the secret password into the Activation Key and Confirm Activation Key Then click Initialize.



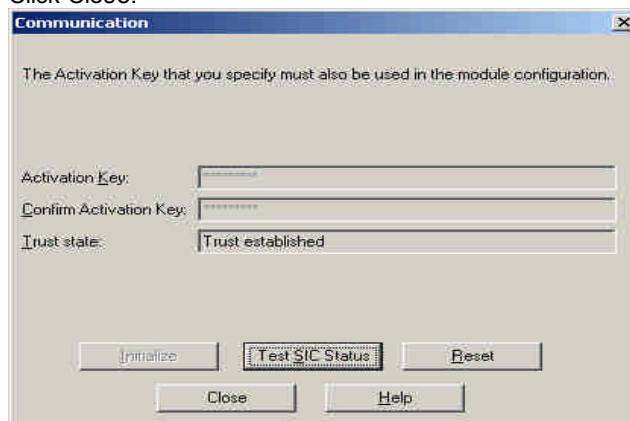
Click Test SIC Status to make sure the communication is established.



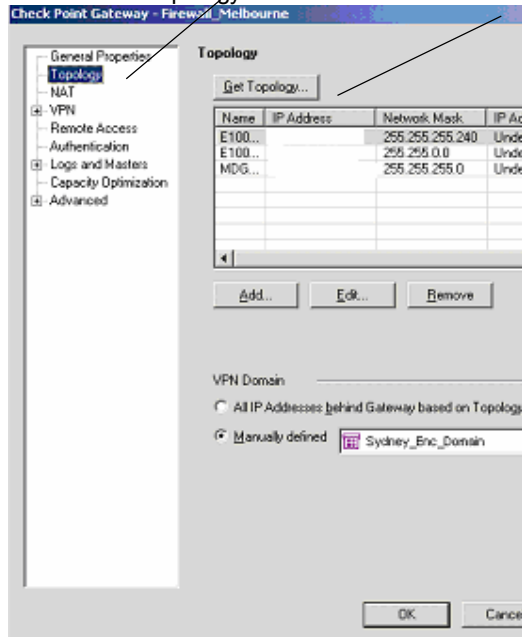
When communication is established click Close.



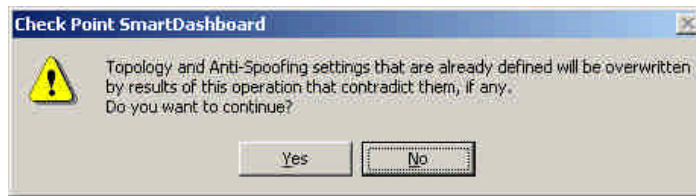
Click Close.



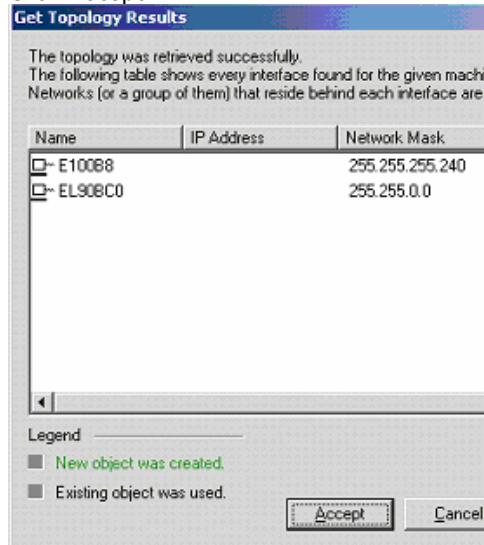
Click on the Topology Tab and then select Get Topology.



Select Yes.

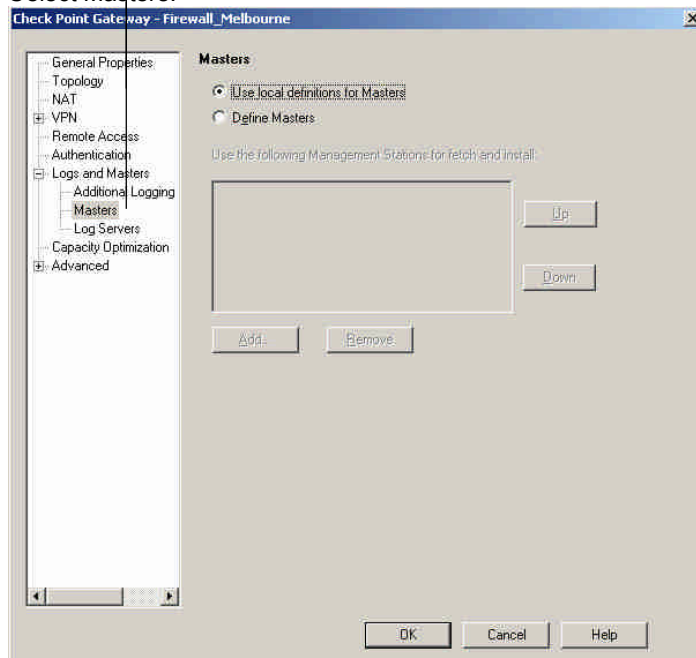


Click Accept.



Select Logs and Masters.

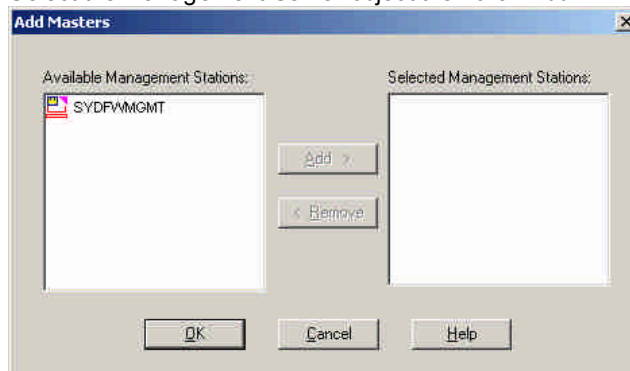
Select Masters.



Click Yes.

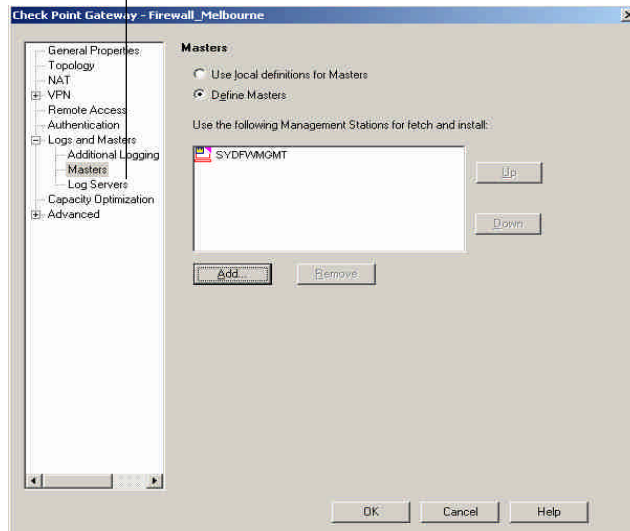


Select the Management Server object then click Add.

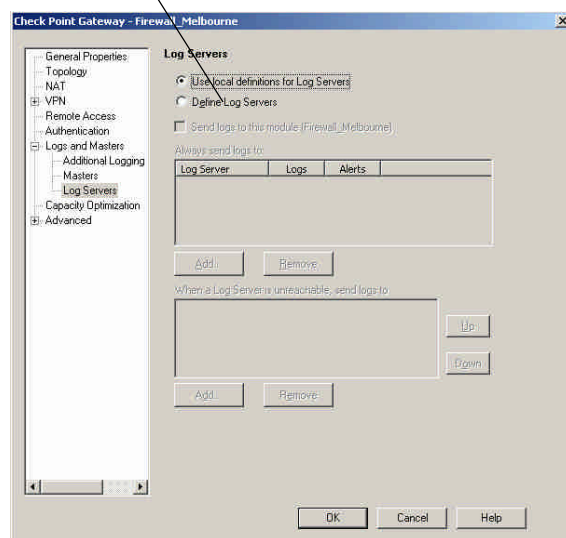


Click OK.

Select Log Servers.



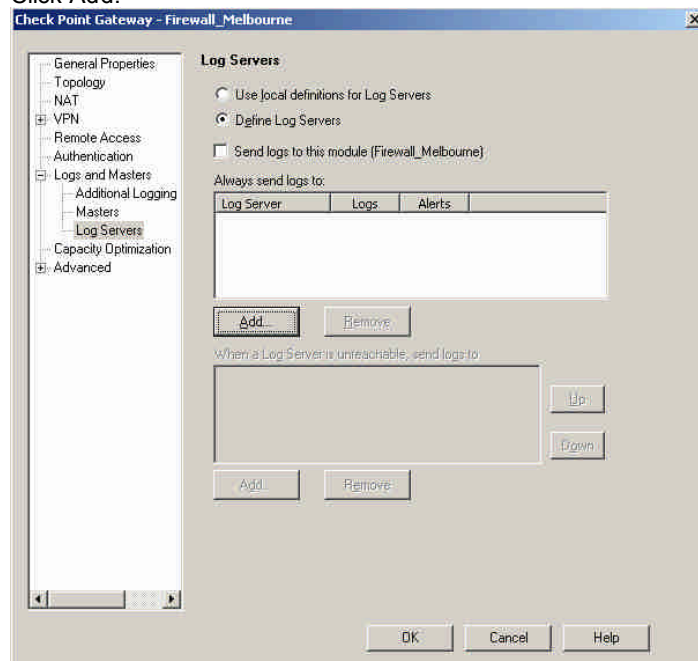
Select Define Log Servers.



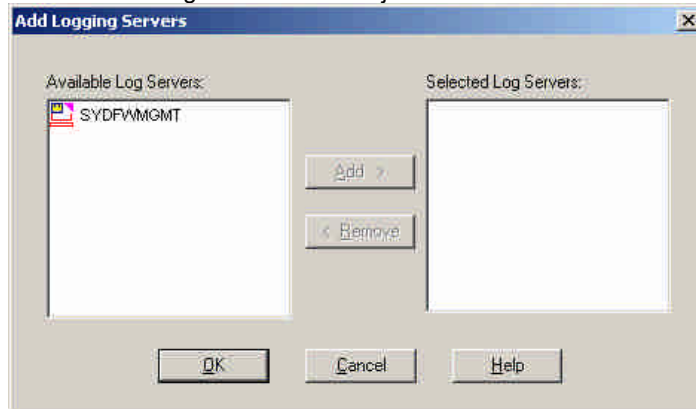
Click Yes.



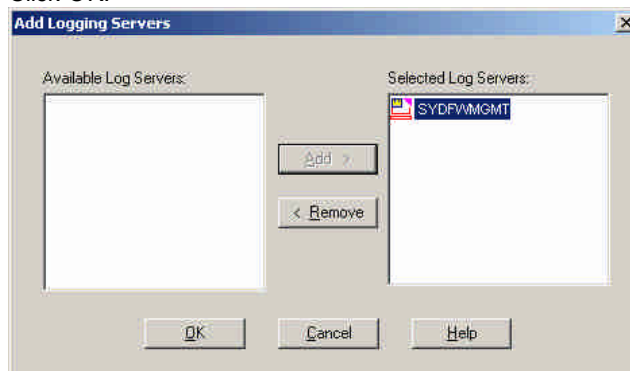
Click Add.



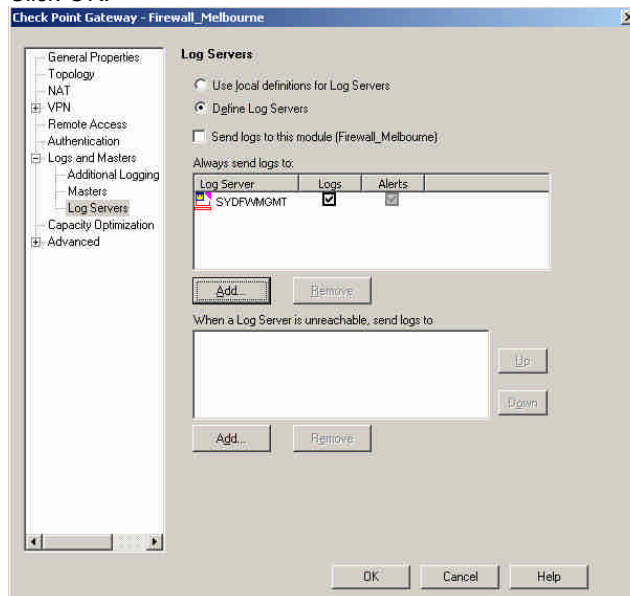
Select the Management Server Object then Click Add.



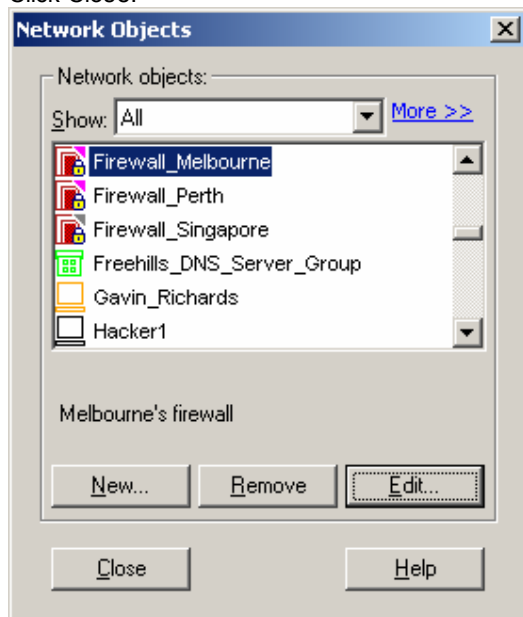
Click OK.



Click OK.



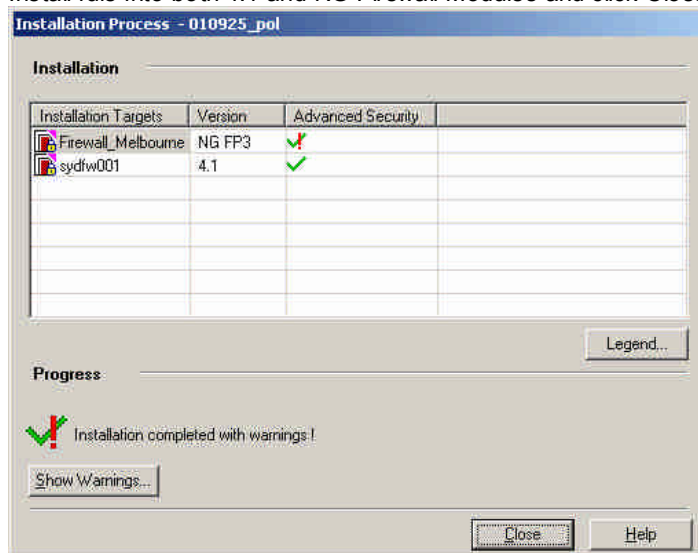
Click Close.



Add the following port to
 Firewall1_Group Object
 FW1_ica_push
 CPD
 CPD_amon
 FW1_ica_service

Disable rule	All_internal_Ne twork	> xxx.xxx.xxx.xxx -NICS
		> xxx.xxx.xxx.xxx -NICS
Disable rule	xxx.xxx.xxx.xxx -NICS	> All_internal_Network
	xxx.xxx.xxx.xxx -NICS	>

Install rule into both 4.1 and NG Firewall Modules and click Close.



Appendix C

Install Firewall Module for NG FP3

This procedure is only for Windows 2000 server.

This entire appendix sourced from Checkpoint Technical Services Department, NG Upgrade Centre

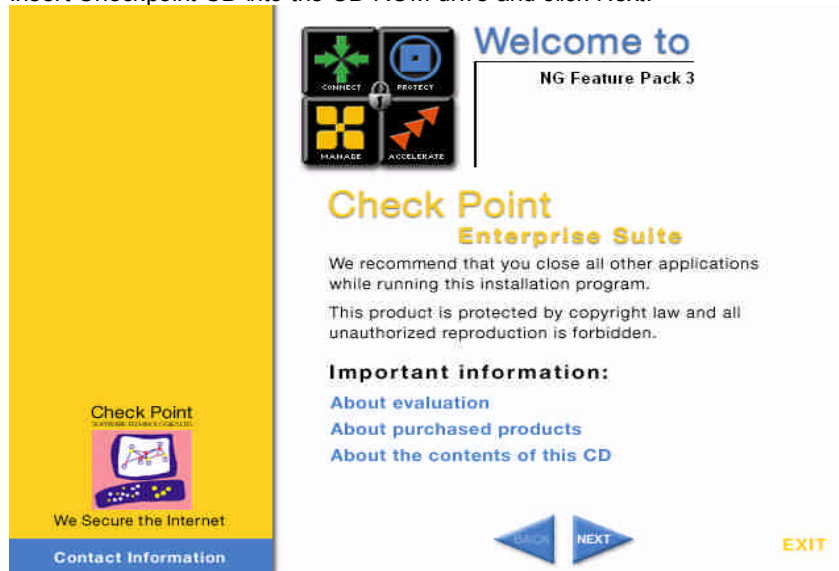
Use Registry Editor to view the following registry key:

HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \Tcpip \Parameters

Set the following registry values:

- Value Name: IPEnableRouter
- Value type: REG_DWORD
- Value Data: 1

Insert Checkpoint CD into the CD ROM drive and click Next.



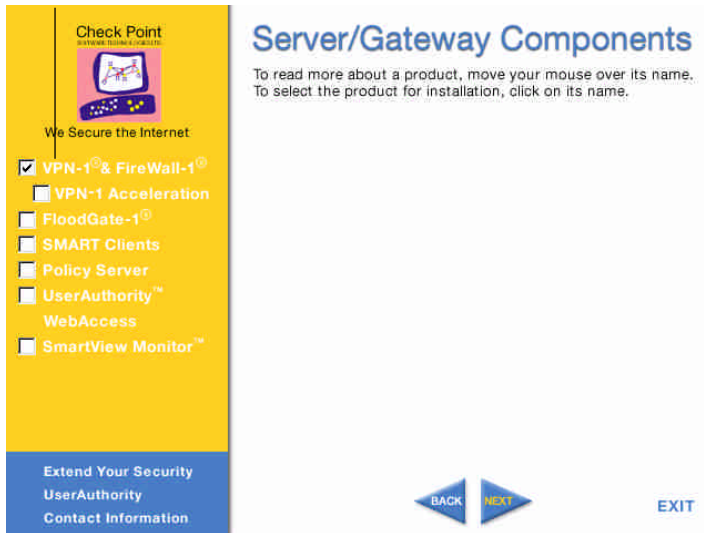
Click Yes.



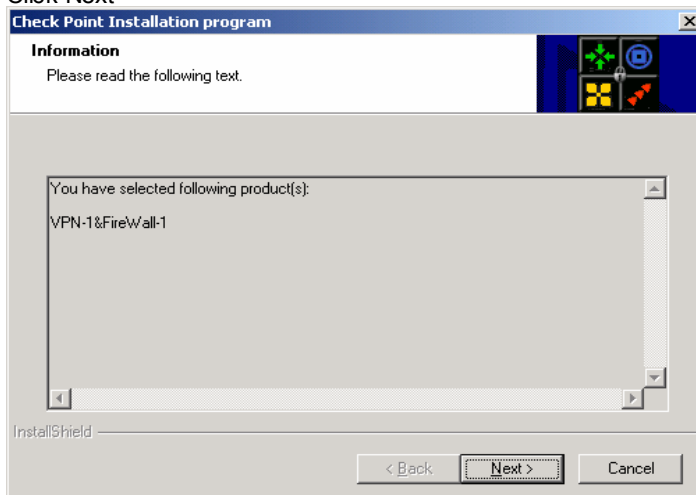
Select Server/Gateway Components then Click Next.



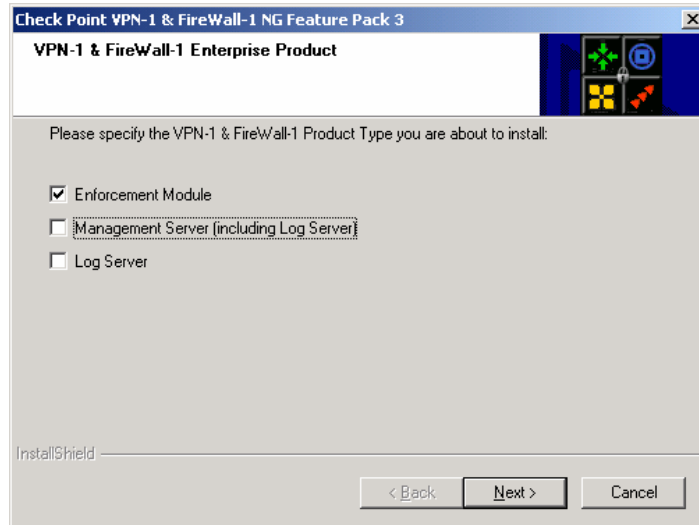
Select VPN-1 & Firewall-1 then click Next.



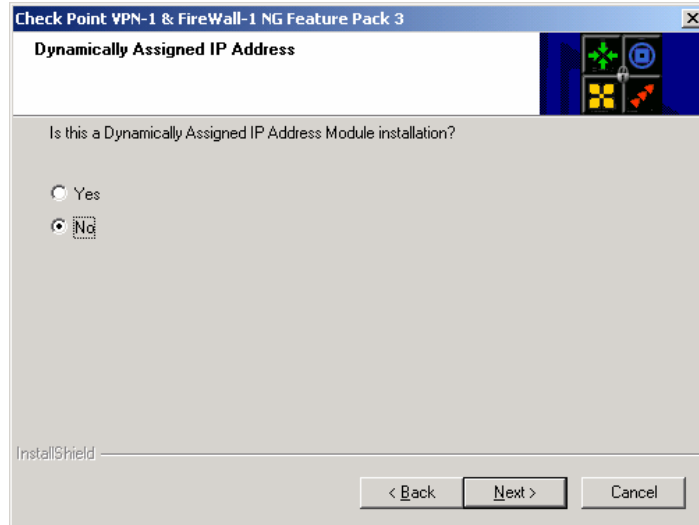
Click Next



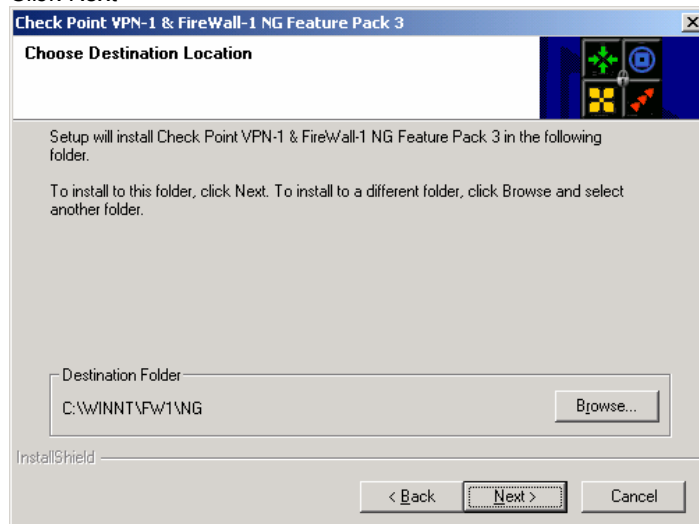
Select Enforcement Module then click Next.



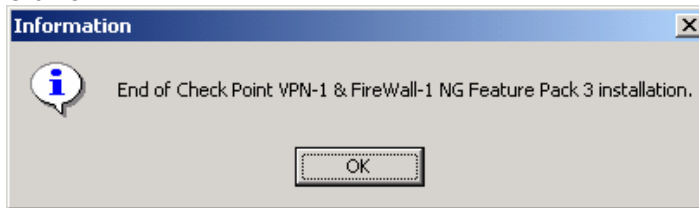
Select No then click Next.



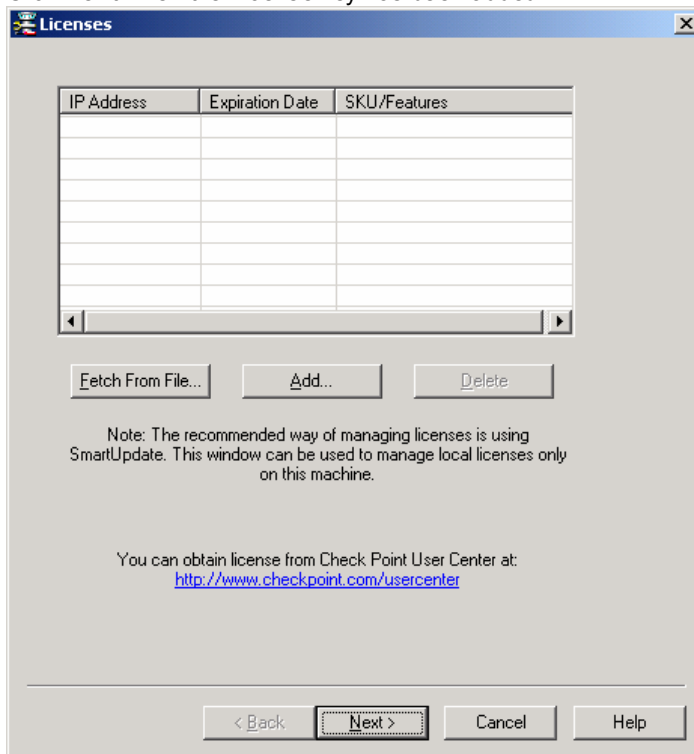
Click Next



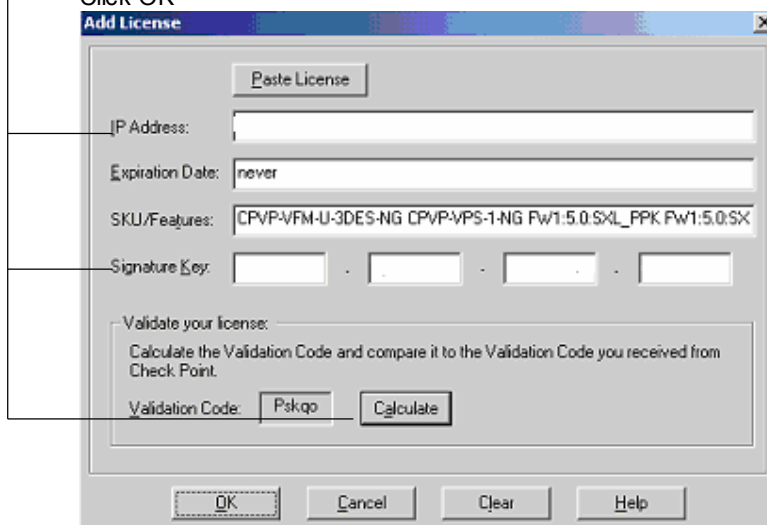
Click OK.



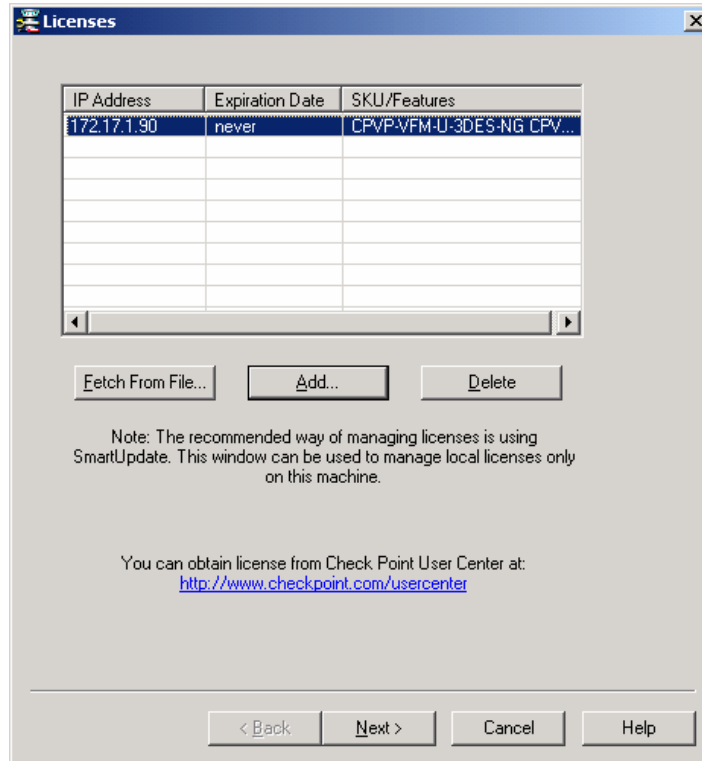
Click Add to add the IP Address and the License number of the Firewall Module.
Click Next when the License key has been added.



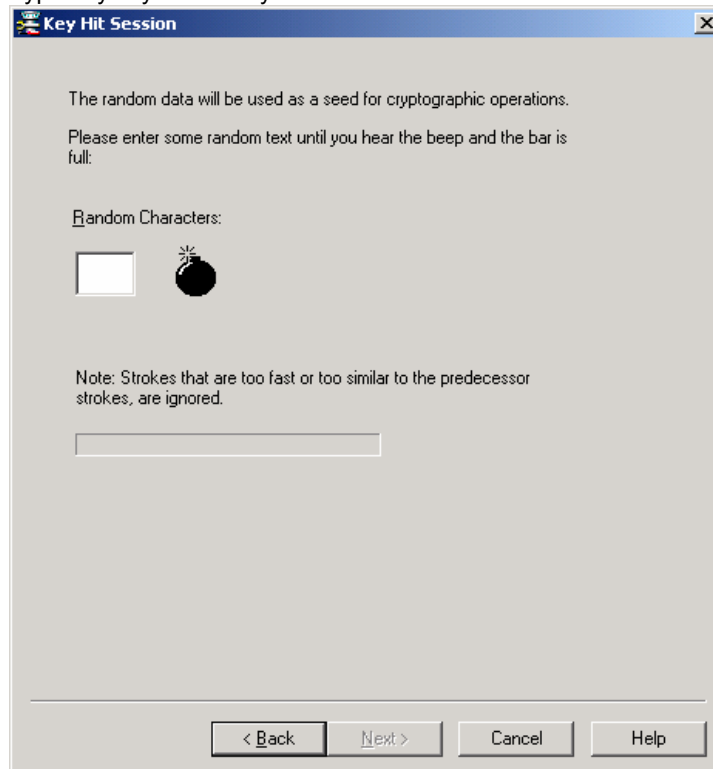
Insert the IP Address and License Key then click Calculate.
Click OK



Click Next.



Type any key on the keyboard until the Next button is enabled.



Click Next.

Type in the secret password in the Activation Key eg ~!@#\$%^&*

Secure Internal Communication

State:

Distinguished Name (DN):

Certificate Authority's IP Address:

Initialization:

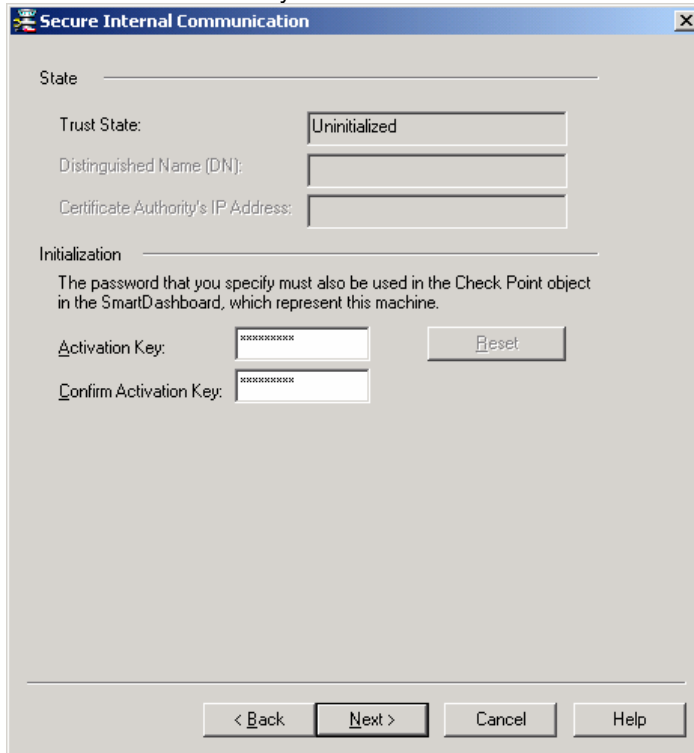
The password that you specify must also be used in the Check Point object in the SmartDashboard, which represent this machine.

Activation Key:

Confirm Activation Key:

< Back Next > Cancel Help

Confirm the Activation Key and click Next.



Secure Internal Communication

State

Trust State: Uninitialized

Distinguished Name (DN):

Certificate Authority's IP Address:

Initialization

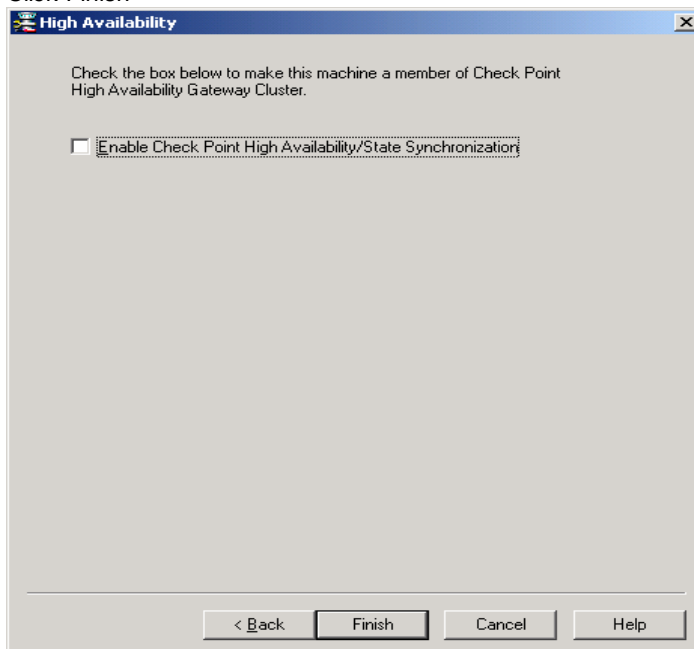
The password that you specify must also be used in the Check Point object in the SmartDashboard, which represent this machine.

Activation Key: [password field] [Reset]

Confirm Activation Key: [password field]

< Back Next > Cancel Help

Click Finish



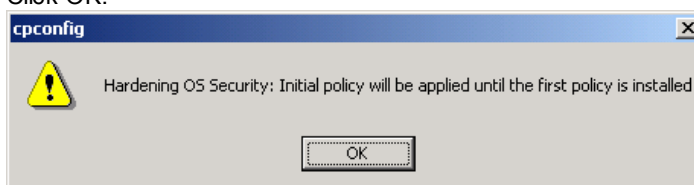
High Availability

Check the box below to make this machine a member of Check Point High Availability Gateway Cluster.


☐ Enable Check Point High Availability/State Synchronization

< Back Finish Cancel Help

Click OK.

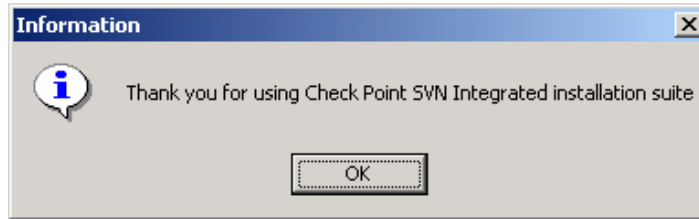


cpconfig

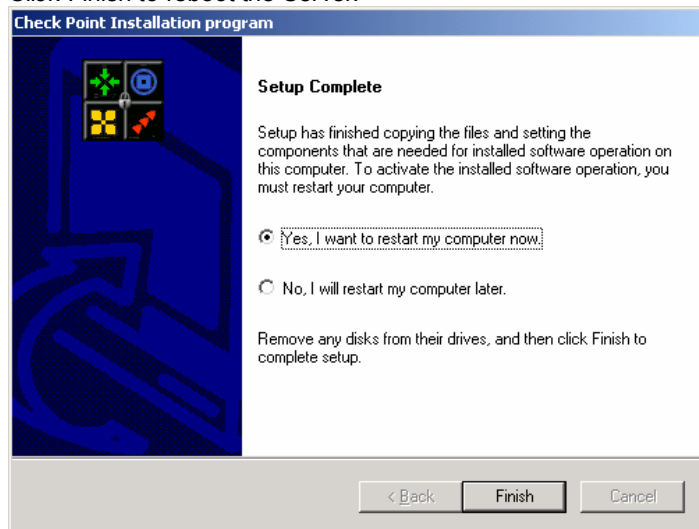
 Hardening OS Security: Initial policy will be applied until the first policy is installed

OK

Click OK.



Click Finish to reboot the Server.



List of References

1. Page 3 Author unknown – iPass™ Technical Services Department.
iPass Corporate Access™
http://www.ipass.com/services/services_corpaccess.html (May 31 2003)
2. Page 5 Author unknown – Checkpoint Technical Services Department.
Top 10 Reasons to Upgrade. #2 Managing Remote Access VPN users
<http://www.checkpoint.com/techsupport/ngupgrade/top10/2.html> (May 31 2003)
3. Page 9 Author unknown – Microsoft Technet™
Windows Security, Windows 2000™ Security Hardening Guide
Chapter 6 Windows 2000™ Hardening Guide Configuration Templates
<http://www.microsoft.com/technet/t r e e v i e w / d e f a u l t . a s p ? u r l = / t e c h n e t / s e c u r i t y / p r o d t e c h / W i n d o w s / W i n 2 k H G / 0 6 T m p l t s . a s p> (May 31 2003)
4. Appendix A – Checkpoint Technical Services – NG Upgrade Centre
Installing Firewall NG Management Server . February 11 2003
5. Appendix B – Checkpoint Technical Services – NG Upgrade Centre
Upgrade from Checkpoint 4.1 to Checkpoint NG. February 11 2003
6. Appendix C – Checkpoint Technical Services – NG Upgrade Centre
Install Firewall Module for NG FP3. February 11 2003