

# **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 permited 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<sup>™</sup> v 4.1 to Checkpoint Firewall-1<sup>™</sup> 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<sup>™</sup> v4.1(referred to as 4.1 from hereon) to Checkpoint Firewall -1 NG<sup>™</sup> (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 in itiator 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 then 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) Mana gement 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.

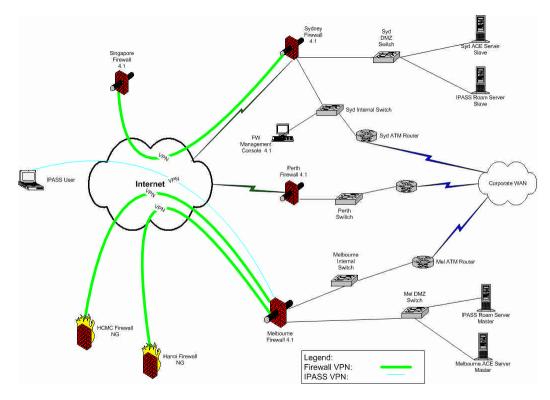


Figure 1 – The Firewall network – Before

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 <sup>™</sup> and Checkpoint SecuRemote <sup>™</sup>. In order to clarify the situation, iPass <sup>™</sup> 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 (<u>http://www.ipass.com/services/services corpaccess.html</u>). Once the client has access to the internet, then Checkpoint SecuRemote <sup>™</sup> is used to authenticate with the corporate network.

Between 1998 and early 2003, whenever a service pack had to be applied or substantial chang es 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 re sulted 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 d irector 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 a natomy were at risk of being re-arranged if the project did not succeed as I had prescribed!!)

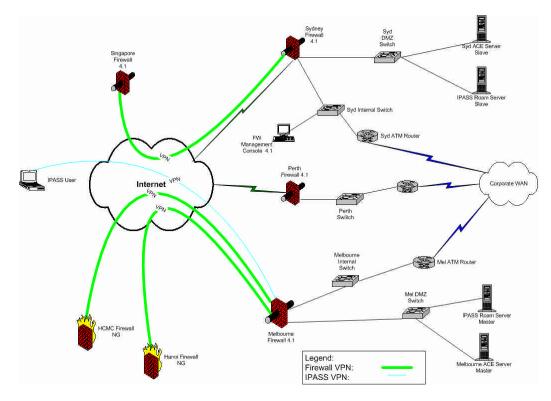
The first task was to write a thorough business case to prove to the firm that an upgrade was essential and moreover, that we had the necessary expertise to see the project through to a satisfactory conclusion. The director of IT was sceptical that the team I was assembling was capable of implementing 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 endl ess 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 Abs tract section) is to roll out Checkpoint SecureClient NG<sup>™</sup> 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/t\_op10/2.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 prov ides 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 corporat e 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 emai I 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 redundanc y and fail-over. If the Melbourne firewall is down for any reason, then Sydney automatically takes over the role of iPass<sup>™</sup> 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 "ho w 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 a re 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 r ule 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 sof tware 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<sup>™</sup> and SecuRemote were applied to the se 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 traf fic could get through. The old 4.1 firewall was still handling all remote access traffic. The iPass<sup>™</sup> organisation were given the ip address es 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 cl ient 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 issue d asking them to use the remote solution a s 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 Managem ent 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<sup>™</sup> clients are authenticating against the new NG firewalls . It shows that most of the iPass<sup>™</sup> clients are still authenticating aga inst the Melbourne Firewall 4.1. N.B. The FW Management Console NG in Melbourne controls only the 2 new Sydney and Melbourne NG firewalls.

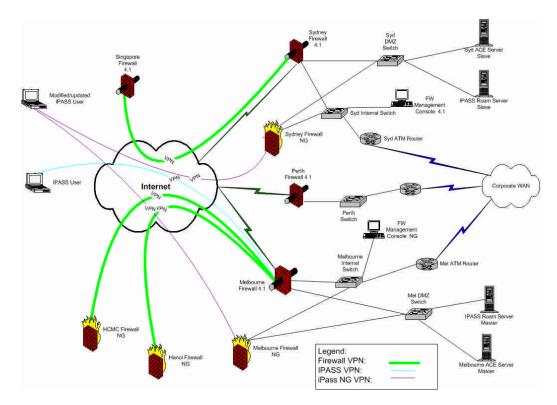


Figure 2 – The Firewall Network – mid phase

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 rea I console machine was being reinstalled with WIN2000 (hardened to current corporate specification -

http://www.microsoft.com/t echnet/treeview/default.asp?url=/technet/security/pr odtech/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 an ything, 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 cli ents. The mail flow and internet ser vice was redirected back to this 4.1 firewall which had now been upgraded to NG and all this happened without the bulk of the 75 0 people in our Sydney office being any the wiser.

Melbourne was next, and this time all tr affic 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 cas e), 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 u pgrade 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 corpor ate 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 conjunct ion with the diagram in Figure 3 below.

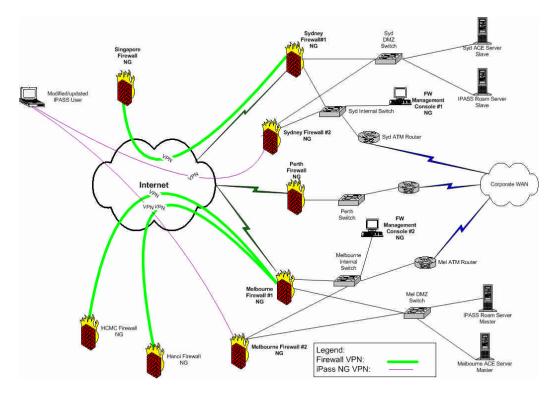


Figure 3 – The Firewall Network – Completed

- The new firewalls introduced as part of this projec t 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 Roam 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 Manag ement 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.

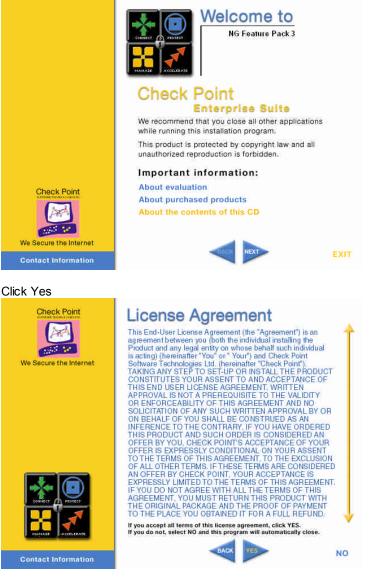
The perimeter defence system has become slightly more complex with the introduction of 2 more firewalls and a new management console, but clear and concise drawings and documentation help to minimise the com plexity and explain each and every scenario to mitigate the risk .

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 imp lementation. 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.



Check Point	Product Menu important: before you continue, please be sure to review the most up-to-date information about the products on this CD www.checkpoint.com/NG/FP3
	Server/Gateway Components
	C Mobile/Desktop Components
Extend Your Security	BACK NEXT
Contact Information	BACK NEXT EXIT
Select VPN-1 & Fire Select Smart Clients Click Next.	
Select Smart Clients	Server/Gateway Components To read more about a product, move your mouse over its name.
Select Smart Clients Click Next.	Server/Gateway Components To read more about a product, move your mouse over its name. To select the product for installation, click on its name.
Select Smart Clients Click Next.	Server/Gateway Components To read more about a product, move your mouse over its name. To select the product for installation, click on its name.
Select Smart Clients Click Next.	Server/Gateway Components To read more about a product, move your mouse over its name. To select the product for installation, click on its name.
Select Smart Clients Click Next.	Server/Gateway Components To read more about a product, move your mouse over its name. To select the product for installation, click on its name. WPN-1 <sup>®</sup> & FireWall-1 <sup>®</sup> An integrated VPN and security solution for both single gateway and multi-site deployments which provides access control, authentication, encryption, network address translation, ligh availability, content security and enterprise policy management Also includes • VPN-1 modules (VPN-1 Pro, VPN-1 Net, VPN-1 SmallOffice) • VPN-1 modules (VPN-1 Pro, VPN-1 Net, VPN-1 SmallOffice) • VPN-1 SecureServer • SmartDefense • SmartUpdate • ClusterXL • SmartCenter Server
Select Smart Clients Click Next.	Server/Gateway Components To read more about a product, move your mouse over its name. To select the product for installation, click on its name.
Select Smart Clients Click Next.	<section-header>Server/Gateway Components To read more about a product, move your mouse over its name, to select the product for installation, click on its name.</section-header>

You have selected following product(s):

VPN-1&FireWall-1 SMART Clients

3 InstallShield -

-

Cancel

Next >

< Back

eck Point VPN-1 & FireWall-1 NG Featur VPN-1 & FireWall-1 Enterprise Product			× (0) (1) (1) (1) (1) (1) (1) (1) (1
Please specify the VPN-1 & FireWall-1 Prod	uct Type you are a	bout to install	
Enforcement Module			
I Management Server (including Log Serv	ver)		
Log Server			
italiShield	2	(a	
	< Back	<u>N</u> ext>	Cancel

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

Select Enterprise Primary Management and click Next.

Check Point VPN-1 & FireWall-1 NG Feature Pack 3	×
VPN-1 & FireWall-1 Enterprise Management	
Please specify the VPN-1 & FireWall-1 Management Type you are a	bout to install
Enterprise Primary Management	
C Enterprise Secondary Management	
Install6hield	
< <u>B</u> ack	Next> Cancel

Select Install with Backward compatibility and click Next.

Backward Compatibility screen			
Would you like to install the Backward Com if VPN-1/FireWall-1 4.1 enforcement module			
	es are managea non	r mis management su	auonee
C Install without backward compatibility			
Install with backward compatibility			
tall6hield			
	52	0211	

#### Select Next

oose Destination Location			
Setup will install Check Point VPI folder.	N-1 & FireWall-1 NG Feature	Pack 3 in the fo	llowing
To install to this folder, click Next another folder.	t. To install to a different fold	er, click Browse	and select
Destination Folder			
Destination Folder			Biowse.

### Click OK

Informat	ion 🔀
٩	End of Check Point VPN-1 & FireWall-1 NG Feature Pack 3 installation.

#### Click Next.

Check Point SMART Clients NG			×
Choose Destination Location			
Setup will install SMART Clients in the following	folder		
To install to this folder, click Next. To install to a another folder.	different folder, clic	k Biowse and select	
Destination Folder C:\\CheckPoint\SMART Clients\NG FP3		Browse.	
Install6hield			
	(Back	Next> Cancel	-

#### Select all and click Nex t.

neck Point SMART Clients NG	
Select Clients Choose the clients Setup will install.	
Select the clients you want to install, and clear the clients	you do not want to install. Description The SMART Clients manage: FireWall-1, VPN-1, SmarDefense, FloodGate-1 and more.
Space Required on C: 57376 K Space Available on C: 5328100 K stallChield	
space Available on L: 5320100 K	ck <u>N</u> ext > Cancel

### Click OK.

Informat	ion 🗵
٩	Setup is complete. You may run the installed program by double-clicking on the program icon.
	OK.

#### Click Add to add Licenses.

Licenses			2
IP Address	Expiration Date	SKU/Features	
1 Y			
	$\land$		
4			
Tarranteeronatio	-14 F (2008)	- C 5	
Eetch From File	<u>A</u> dd	Delete	
		f managing licenses is using	
SmattUpdate, H	us window can be u on this ma	sed to manage local licenses only chine.	
		heck Point User Center at	
h	tp://www.checkpoi	nt.com/usercenter	
	C Back	ext> Cancel Ha	de
22			

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

	Paste Lic	crise			
P Address:					
xpiration Date:	never				
SKU/Features:	CPVP-VEE	-U-3DES-MGM	T-NG FW1:5.0:DB	VR_UNLIMIT CK-AF9	94D108
Signature <u>K</u> ey:				•	
-Validate your lice Calculate the V Check Point		de and compar	re it to the Validatio	n Code you received f	rom
⊻alidation Code	2rpwF	Calcul	ate		

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

	Paste L	1001100					
IP Address:							
Expiration Date:	never						
SKU/Feaţures:	CPVP-VE	E-U-3DES	MODUL	E-NG CPVP-	VPS-1-NG	FW1:5.0:S	<pre>K</pre>
Signature <u>K</u> ey:							
-Validate your lid	ense:						
Calculate the Check Point.	/alidation (	Code and c	ompare i	to the Valid	ation Code	you receive	ed from
⊻alidation Cod	e: ccD	fV	Calculate				

## Click Next.

172.22.253.51         never         CPVP-VEE-U-3DES-MODUL           172.22.253.52         never         CPVP-VEE-U-3DES-MGMT
(I)
Eetch From File,         Add         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.check.point.com/usercenter

Click Add to add A	dministrator Account.
--------------------	-----------------------

Add

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

Add Administrator		? ×
Administrator Name:		
Password:		
Confirm Password:		
Permissions		
Read/ <u>W</u> rite All		
Manage Administrators		
C Read Only All		
C Customized:		
✓ SmartUpdate	Read/Write	-
✓ Objects Database:	Read/Write	¥
Check Point Users Database:	Read/Write	<b>-</b>
DAP Users Database:	Read/Write	-
Security Policy:	Read/Write	-
🗖 QoS Policy:		-
🗖 Log Consolidator:		-
Smart <u>V</u> iew Reporter:		<b>Y</b>
Monitoring:	Read/Write	<b>_</b>
OK Cancel	Help	

<u>Add</u> <u>Edt</u> <u>Delete</u> pecify Administrators who are permitted to use the GUI applications to	Name	Manage Administrators Yes	Monitoring Al	All	All
necify administrators who are nermitted to use the GLU applications to	•1	<u>A</u> dd		Delete	<u>,</u>
you must define at least one administrator.	ig into t	Administrators who are peri his Management Server.	mitted to use the		ns to

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

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

Remote holstname	Add>	172.17.43.254	
In certain configuratic Security Policy before Clients settings can a See Help for details.	the Management pply.		
ipecity remote clients Nanagement Server.	from which an Admini	strator can log to this	

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

😤 Key Hit Session	×
The random data will be used as a seed for cryptographic operations.	
Please enter some random text until you hear the beep and the bar is full:	
<u>R</u> andom Characters:	
🔲 🍎	
Note: Strokes that are too fast or too similar to the predecessor strokes, are ignored.	
<u></u> ],	
KBack Nexts Cancel Hel	_
Ligadik Mexico Candel Hei	

#### Click Next.

ck Initialize and Start Certificate Authority.	
Certificate Authority	1
Certificate Authority Status: Not initialized. The system uses an Internal Certificate Authority to provide Secured Internal Communication (SIC) certificates for the components in your System. Note: system components cannot communicate with one another until the Certificate Authority is initialized and they each have their SIC certificates. Click the button below to initialize the Certificate Authority.	
Initialize and Start Certificate Authority	
Management FODN	
The FOBM (Fully Gualified Domain Name) of this Management Station is required for proper operation of the Internal Certificate Authority	
Management FODN: Sydtwingint Send to GA	
Dhange Management FUDIN	
< <u>B</u> ack <u>Next&gt;</u> Cancel Help	5

Click OK.						
cpconfig					×	
٩	Your Cer	tificate Au	thority was ir	nitialized suc	cessfully.	
		Lunni				
Click OK.						
cpconfig						×
🕘 us Ci		e Check Point Center at:	l will expire in 15 Product Suite, Ple sercenter			
			OK I			
Click Sen		<b>-</b>				141
itercinca	ate Authori	SY .		X X X X X X X X X X X X X		×
			: Not initialized al Certificate Au		de	
5	Secured Inten	nal Communi	cation (SIC) cer			
N U		component cate Author	n. cannot commu v is initialized ar			
0	Dick the butto	m below to in	nitialize the Cert	ficate Authorit	y.	
	Ini	tialize and S	tart Certificate A	uthority		
			<u> </u>	<u></u>		
Manage	ment FQDN	****		<u></u>		
Sta			omain Name) o operation of the			
<u>M</u> anage	ment FQDN:			Send to C	A	
Change	e Managemer	1 FQDN				
				<u>.</u>		
		< <u>B</u> ack	<u>N</u> ext >	Cance	I H	lelp

### Click OK.



	ie Management FQDN was sent	successibility to the CA
	<u>(                                    </u>	
Next.		
ertificate /	Authority	
Certifi	cate Authority Status: Your Certificat	te Authority is initialized
The	potem uses en Internal Certificate Aut	honty to provide
	red Internal Communication (SIC) Seri onents in your System.	frestes for the
Note:	system componente cannot commun	icate with one another
	he Centicale Authority is initialized en enfroates	a mey each nave men
Clink	the bullon below to minalize the Certifi	idate Authority
	Initialize and Start Certificate Au	
	Thomas and star control and	an and any
anagement	Parana	
	DN (Fully Qualified Domain Name) of is required for proper operation of the	
Station	y	Send to DA

### Click Finish.

ne management solver inge	erprint is displayed below.	
	01. 01. TS	
When a GUI Client initially con o compare its fingerprint with t		
WET EMMA FOIL FUNK DOI	LT HOC ALIA FEUD DON	CURT DOW ADAM
ou can export the fingerprint	to a text file, which can	Lances and L
be accessed from the GUI Clie		Export to file

### 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, wit hout 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 follo wing 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 e xample, fwauth.NDB522. In this case take the real database file (fwauth.NDB522), r ename it to fwauth.NDB and put it in the \upgrade \4.1 directory

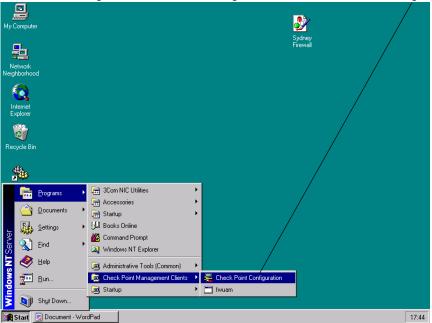
c. rulebases.fws

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 Configur ation.



select the Maste	ISTAD.		
🦉 Check Point C	onfiguration Tool		X
	ecurity Server IP Address	Hi Masters	gh Availability     IP Forwarding
Masters:		172.22.253	.52
hostname:	<u>A</u> dd -> <- <u>R</u> emov	e	Up Down
Specify Managen	ient Servers that can	control this Enforc	ement Module.
	ок с	Cancel Ap	pply Help

#### Select the Masters TAB

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

SMTP Se Licenses	ecurity Server IP Address		igh Availability	
		Masters	IP Forwarding	
Masters:	<u>A</u> dd -> <- <u>R</u> emove	<b>17222225</b>		
Specify Managem	ent Servers that can		ement Module.	

Type the secret password in the Password fiel d eg |\*|&@##\$|~?Type the secret password in the Confirm password field eg |\*|&@##\$|~?Click OK.

Add Master	×
hostname:	172.22.253.52
<u>P</u> assword:	*****
<u>C</u> onfirm password:	******
ОК	Cancel <u>H</u> elp

### Click OK.

🦉 Check Point C	Configuration Tool		×
SMTP S Licenses	Security Server	Hi Masters	gh Availability     IP Forwarding
hostname:	<u>Add</u> →	172.22.253	U52 Up Down
	ок с	ancel Ap	ply Help

Click Yes.



### From Firewall NG Management Server

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

	come to Check Point artDashboard
Identification Method	
User Name	huynyq
C <u>C</u> ertificate:	· · · · · · · · · · · · · · · · · · ·
Connect to Server	
Password:	******
<u>S</u> martCenter Server:	172.22.253.52
🗖 Read O <u>n</u> ly	
🔲 <u>D</u> emo Mode	More Options >>
<u> </u>	Quit

Click approve.

Welcome to Check Point SmartDashboard
This is the first time you are contacting this SmartCenter Server.
SmartCenter Server: 172.22.253.52 - 172.22.253.52
Eingerprint: WET EMMA FOIL FUNK DOLT HOC ALIA FEUD DON CURT DOW ADAM
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?
Approve Quit Help

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

Network Objects	×
Network objects:	
Show: All	More >>
SYDFVMGMT	
sydmsw1 Sydmsw1_Internal Sydn0int_Intranet_Server	
New <u>B</u> emove	<u>E</u> dit
	<u>H</u> elp

#### **Click Communication**

General Properties	dfw001
Topology	Check Point Gateway - General Properties
NAT Automication Automication Capacity Opinization E: Advanced	Name: P & ddess: Connent: Caler: Version: 4.1 Version: 4.1 Version

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

Communication		×
Please make sure that the the one entered in the mod		
Module Activation Key:		i*
Confirm Activation Key.	-	
Initialize	Close	Help

### Click Topology and then select Get Topology.

- Topology - NAT	Get Topology	
VPN     Authentication     Capacity Dplinization     Advanced	Name IP Address E100 E190x1	Network Mark IP. 255.255.0.0 Un 255.255.255.0 Un
	VPN Domain	Edt Berrove

Click Yes	3.
Check Poir	it SmartDashboard
⚠	Topology and Anti-Spoofing settings that are already defined will be overwritten by results of this operation that contradict them, if any. Do you want to continue?
_	Yes No
Click OK	
Check Poi	nt SmartDashboard
⚠	Information about the networks behind the gateway could not be fetched. The current topology definition (if any) of the fetched interfaces will be used. To make Anti-Spooling work correctly, accept the fetched interfaces and confirm that their topology is completely defined. Alternatively, manually define the interfaces.
	OK
Networks	ing table shows every interface found for the given machin (or a group of them) that reside behind each interface are a IP Address Network Mask
- E190x	
<u>□</u> ~ E100E	255.255.0.0
•	
Legend	
	bject was created. g object was used.
Click Ye	
Check Po	int SmartDashboard
⚠	At least one interface is defined as internal with undefined topology. Anti-Spoofing cannot be performed.
	Are you sure you want to continue?

### From Firewall Module Version 4.1 server

No

Yes

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.

	come to <b>Check Point</b> nartDashboard
Identification Method	
I User Name	huynyq
C <u>C</u> ertificate:	· · · · · · · · · · · · · · · · · · ·
Connect to Server	
Password:	*****
<u>S</u> martCenter Server:	172.22.253.52
🔲 Read O <u>n</u> ly	
🔲 <u>D</u> emo Mode	More Options >>
<u>0</u> K	Quit

#### Install Rules into the Firewall Module and click Close.

stallation Targets sydtw001	Version 4,1	Advanced Security	
Sarwool	295,0		
			Legend
ogress			
Installation comp	pleted succes	sfully !	
instaliation com	neteu succes	siuny i	

# Configure Firewall NG Management Server to communicate to Firewall NG Module

Select the Firewall Object and click Edit.

Network Objects	×
-Network objects:	
Show: All	
Firewall_Melbourne	
🕞 Firewall_Perth	
📑 Firewall_Singapore	
Freehills_DNS_Server_Group	
Gavin_Richards	
Hacker1	
Melbourne's firewall	
<u>N</u> ew <u>R</u> emove <u>E</u> dit	
<u>C</u> lose <u>H</u> elp	

Flue k Point <b>Fal</b> ieway - Fis	rw.d_Melluneme	×
F General Properties	Check Point Galeway - General Preparties	
iTopology iNAT tit-VPN	Name: Internet Metalante	
- Authentication - Capacity Optimization	IP éddress Get address Dynamic Address	
🗄 - Advanced	Calar:	
	Check Point Products	
	Vesion: 4.1 T Get Vesion	
	FloodGale-1   SecureDiant Policy Server	
	SecureDient Software Distribution Server	
	Secure Internet Communication	
	Communication	
I	OK Cencel Help	

	ewall_Melbourne
Check Point Gateway - Fin  Central Properties  Toplogy -NAT -VPN -Remote Access -Authentication -Logs and Masters -Capacity Optimization -Advanced	ewall Melbourne  Check Point Gateway - General Properties  Nome: Firewal_Melbourne  IP éddress: Comment: Melbourne's line Aal  Cojo: Check Point Products Version: NG Feature Pack 3
	Secure Internal Communication CommunicationDN:
	DK. Cancel

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

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

Communication		×
The Activation Key that	you specify must also be used in the module configuration.	1
Activation <u>K</u> ey: Confirm Activation Key:	******	
 ∐rust stale:	Uninitialized	
Initialize	Test DE Storus Beset	
· · · · ·	<u>Close</u> <u>H</u> elp	

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

ctivation Key:	
onfirm Activation	(ey:
rust state:	Trust established

When communication is est	ablished click Close	e.
---------------------------	----------------------	----

C Status for Firewall_Melbourne:	Communicating	
1		-
	Close	

### Click Close.

Communication		×
The Activation Key that	you specify must also be used in the modul	e configuration.
Activation <u>K</u> ey: Confirm Activation Key:		
Linist state:	l Trust established	
Tunnise	Test SIC Status Beset	
	Close <u>H</u> elp	

## Click on the Topology Tab and then select Get Topology.

Image: Second	General Properties	Topology Get Topology		
	- Authentication II- Logs and Masters - Capacity Optimization	E100 E100 MDG All PAddesses behind	255 255 255 240 255 255 255 0 . <u>R</u> emove Gateway based on To Sydney_Enc_Domain	Unde Unde Unde

Select Yes.

Check Po	int Smart	Dashboard		×
⚠	by results		g settings that are already defined that contradict them, if any.	will be overwritten
		Ye	s <u>No</u>	
Click Ac				
11100000	ogy Result			
The follow	wing table sh		e found for the given machi	
Networks	lor a group	of them) that reside	e behind each interface are	
Name		IP Address	Network Mask	
D~ E100			255.255.255.240	
0 - EL90	IBC0		255.255.0.0	
1				
Legend				
· · · · · · · · · · · · ·	object was o	reated.		
🔳 Existi	ng object wa	s used.		
			<u>Accept</u> <u>Cancel</u>	

NAT VPN Remote Access Authentication Logs and Maters - Additional Logging Masters - Log Servers Capacity Optimization Advanced	Use local definitions for Masters     Define Masters Use the following Management Stations for retch and install

Click Yes.

Check Po	int SmartDashboard
	If you select "Define Masters" on this page, "Define Log Servers" will be selected on the Log Servers page.
	Once you click OK on the Masters page, the Masters defined on this page will replace the local definitions for Masters.
	Are you sure you want to continue?
	<u>Yes</u> <u>N</u> o

Select the Management Server object then click Add.

	Selected Management Stations:
gdd >	ſ
< <u>Bi</u> erroye	ſ
	-

### Click OK.

Select Log Servers.

eck Point Gateway - Fire General Properties Topology NAT E VPN Remote Access Authentication Discoge and Master Additional Logging Matter Copacity Optimization B Advanced	Watters             Be local definitions for Masters            Diffine Masters          Be the following Management Stations for fetch and instalt          SYDPVMOMT
**	OK Cancel Help

# Select Define Log Servers.

General Properties Topology NAT VPN Remote Access Authentication Logs and Masters	Log Servers CUse local defin Define Log Se Send logs to the	evers to module (Fire			
Additional Logging Masters	Always send logs Log Server	Logs	Alerts		
Log Servers Capacity Optimization F Advanced					
	Add	Bemove er n unresoneb	Le, send logs to		
	Add	Remove	]	Dawn	

## Click Yes.

Check Po	int SmartDashboard
	If you select "Define Log Servers" on this page, "Define Masters" will be selected on the Masters page.
	Once you click OK on the Log Servers page, the Log Servers defined on this page will replace the local definitions for Log Servers.
	Are you sure you want to continue?
	<u>Yes</u> <u>N</u> o

### Click Add.

General Properties Topology NAT VPN Remote Access Authentication J Logs and Masters	Log Servers Use local defi Define Log So Send logs to the Always send logs	ervers his module (Fires		ne)		
Additional Logging Masters	Log Server	Logs	Alerts			
Log Servers Capacity Optimization Advanced						
Advanced						
	Add	Hemove				
	When a Log Serv	verni unreachab	e, send logs	10	Í	
					13 <u>0</u> 190	
	Adid	Remove				

Add Logging Servers		×
Available Log Servers:	Selected Log Servers:	
	Add >	
	< Bemoye	
L.		
<u>D</u> K	EancelHelp	

Select the Management Server Object then Click Add.

## Click OK.

### Click OK.

General Properties	Log Servers	
Topology	C Use local definitions for Log Servers	
- NAT 	Define Log Servers	
- Remote Access	<ul> <li>Denne Log Servers</li> </ul>	
Authentication	Send logs to this module (Firewall_Melbourne)	
Logs and Masters	Always send logs to:	
Additional Logging		
Masters Log Servers	Log Server Logs Alerts	
Capacity Optimization		
Advanced		
	the second	
	Add. Bennye	
	When a Log Server is unreachable, send logs to	
	do:	
	Davin	
	Add Remove	

## Click Close.

Network Objects	x
Network objects:	
Show: All	
Firewall_Melbourne	
🕞 Firewall_Perth	
📑 📑 Firewall_Singapore	
Freehills_DNS_Server_Group	
Gavin Richards	
Hacker1	
Melbourne's firewall	
New Remove	
<u>C</u> lose <u>H</u> elp	

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
Disable rule	> xxx.xxx.xxx -NICS 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.

stallation Targets	Version	Advanced Security	
Frewall_Melbourne	NG FP3	×.	
sydfw001	4.1	~	
			Legend
ogress			2
Installation comple	sted with wa	miner I	

EXIT

NO

# Appendix C Install Firewall Module for NG FP3 This procedure is only for Windows 2000 server.

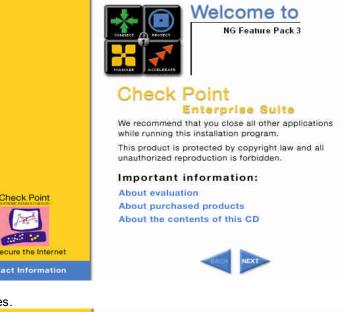
This entire appendix sourced from Checkpoint Technical Services Department, NG Upgrade Centre

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.



# License Agreement

This End-User License Agreement (the "Agreement") is an agreement between you (both the individual installing the Product and any legal entity on whose behalf such individual is acting) (hereinafter "You" or " Your") and Check Point Software Technologies Ltd. (hereinafter "Check Point"). TAKING ANY STEP TO SET-UP OR INSTALL THE PRODUCT CONSTITUTES YOUR ASSENT TO AND ACCEPTANCE OF THIS END USER LICENSE AGREEMENT. WRITTEN APPROVAL IS NOT A PREREQUISITE TO THE VALIDITY OR ENFORCEABILITY OF THIS AGREEMENT AND NO SOLICITATION OF ANY SUCH WRITTEN APPROVAL BY OR ON BEHALF OF YOU SHALL BE CONSTRUED AS AN INFERENCE TO THE CONTRARY, IF YOU HAVE ORDERED THIS PRODUCT AND SUCH ORDER IS CONSIDERED AN OFFER BY YOU, CHECK POINT'S ACCEPTANCE OF YOUR OFFER IS EXPRESSLY CONDITIONAL ON YOUR ASSENT TO THE TERMS OF THIS AGREEMENT. TO THE EXCLUSION OF ALL OTHER TERMS. IF THESE TERMS ARE CONSIDERED AN OFFER BY CHECK POINT, YOUR ACCEPTANCE IS EXPRESSLY LIMITED TO THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE WITH ALL THE TERMS OF THIS AGREEMENT. IF OND DO NOT AGREEW WITH ALL THE TERMS OF THIS AGREEMENT. YOU MUST RETURN THIS PRODUCT WITH THE ORIGINAL PACKAGE AND THE PROOF OF PAYMENT TO THE PLACE YOU OBTAINED IT FOR A FULL REFUND.

If you do not, select NO and this program will automatically close.

Select Server/Gateway Components then Click Next.



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

Check Point	Server/Gateway Comp To read more about a product, move your mouse to select the product for installation, click on its	e over its name.
Extend Your Security UserAuthority Contact Information	BACK	EXIT
Click Next		
Check Point Installation pro	gram	
Information Please read the following tex	et.	
You have selected following	g product(s):	<u></u>
VPN-1&FireWall-1		V V
	< <u>B</u> ack	Cancel

## Select Enforcement Module then click Next.

Check Point VPN-1 & FireWall-1 NG Feature Pack 3	x
VPN-1 & FireWall-1 Enterprise Product	
Please specify the VPN-1 & FireWall-1 Product Type you are about to install:	
<ul> <li>Enforcement Module</li> <li>Management Server (including Log Server)</li> <li>Log Server</li> </ul>	
InstallShield	_
< Back Next > Cancel	

### Select No then click Next.

Check Point ¥PN-1 & FireWall-1 NG Feature P	ack 3	×
Dynamically Assigned IP Address		
Is this a Dynamically Assigned IP Address Modu	e installation?	
C Yes © Na		
InstallShield	< <u>B</u> ack <u>N</u> ext >	Cancel

## Click Next

Check Point VPN-1 & FireWall-1 NG Feature	Pack 3	
Choose Destination Location		
Setup will install Check Point VPN-1 & FireWa folder.	all-1 NG Feature Pack 3 in the fi	ollowing
To install to this folder, click Next. To install to another folder.	a different folder, click Browse	e and select
Destination Folder C:\WINNT\Fw1\NG		Biowse
InstallShield	< <u>B</u> ack	Cancel

Click OK.		
Informati	ion	×
٩	End of Check Point VPN-1 & FireWall-1 NG Feature Pack 3 installa	cion.
	ОК	

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

enses				
IP Address	Expiration Date	SKU/Features		
(			•	I
Eetch From File	<u>A</u> dd		Delete	
	commended way ol window can be us on this ma	ed to manage loc		
You can of	tain license from Ch	neck Point User (	`enter at:	
	tain license from Ch ://www.checkpoir			

Add License	
	Paste License
IP Address:	
Expiration Date:	never
SKU/Features:	CPVP-VFM-U-3DES-NG CPVP-VPS-1-NG FW1:5.0.SXL_PPK FW
Signature Key:	
-Validate your	icense:
Calculate the Check Point	Validation Code and compare it to the Validation Code you received I
⊻alidation Co	de: Pskqo Calculate

Click	Next.			
🚝 Lic	enses			×
[	IP Address	Expiration Date	SKU/Features	
	172.17.1.90	never	CPVP-VFM-U-3DES-NG CPV	
	•			
L				
	Eetch From File	. <u>A</u> dd	Delete	
			managing licenses is using ed to manage local licenses only shine.	
	You can ob	tain license from Ck	neck Point User Center at:	
		://www.checkpoin		
				-
		< <u>B</u> ack	Next > Cancel Help	

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

×

The random data	will be used as a s	seed for cryptogra	aphic operations.	
Please enter som full:	e random text until	you hear the bee	ep and the bar is	
<u>R</u> andom Charact	ers:			
<u> </u>				
	at are too fast or to	oo similar to the pi	redecessor	
Note: Strokes th strokes, are igno		oo similar to the pi	redecessor	
		oo similar to the pi	redecessor	
		oo similar to the pi	redecessor	
		oo similar to the pi	redecessor	
		oo similar to the pi	redecessor	
		bo similar to the p	redecessor	

Click Next.	
🚝 Key Hit Session	×
The random data will be used as a seed for cryptographic operations.	
Please enter some random text until you hear the beep and the bar is full:	
Random Characters:	
v 🍅	
Note: Strokes that are too fast or too similar to the predecessor strokes, are ignored.	
Thank you !	
Thank you :	
< <u>B</u> ack Next> Cancel Help	

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

Secure Internal Con	nmunication		
State			
Trust State:	Uninitializ	ed /	-
Distinguished Name	(DN):	_/	1
Certificate Authority's	IP Address:	/	-
Initialization		/	
The password that yo in the SmartDashboa	ou specify must also be/u rd, which represent this r	ised in the Check Point of machine.	bject
	······································	Reset	1
<u>A</u> ctivation Key:		<u></u> cser	]
Confirm Activation Ke	ay:		

Secure Internal Commu	nication		
State			
Trust State:	Uninitialized	±	
Distinguished Name (DN):			
Certificate Authority's IP A	ddress:		
nitialization			
The password that you sp in the SmartDashboard, wi		ed in the Check Point object achine.	
Activation Key:	******	<u>R</u> eset	
Confirm Activation Key:	*****		
<	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	
<u>Kack</u> Finish Lancel Heip	

## Click OK.

cpconfig	×
⚠	Hardening OS Security: Initial policy will be applied until the first policy is installed
	[OK]

Clic	k OK.	
Inf	ormati	ion X
	ļ	Thank you for using Check Point SVN Integrated installation suite
		OK ]

## Click Finish to reboot the Server.

Check Point Installation program	
	Setup Complete Setup has finished copying the files and setting the components that are needed for installed software operation on this computer. To activate the installed software operation, you must restart your computer. Yes, I want to restart my computer now No, I will restart my computer later. Remove any disks from their drives, and then click Finish to complete setup.
	K Back Finish Cancel

# List of References

- Page 3 Author unknown iPass<sup>™</sup> Technical Services Department. iPass Corp orate Access<sup>™</sup> <u>http://www.ipass.com/services/services\_corpaccess.html</u> (May 31 2003)
- Page 5 Author unknown Checkpoint Technical Services Department. Top 10 Reasons to Upgrade. #2 Mana ging Remote Access VPN users <u>http://www.checkpoint.com/techsupport/ngupgrade/top10/2.html</u> (May 31 2003)
- Page 9 Author unknown Microsoft Technet<sup>™</sup> Windows Security, Windows 200 0<sup>™</sup> Security Hardening Guide Chapter 6 Windows 2000<sup>™</sup> Hardening Guide Configuration Templates <u>http://www.microsoft.com/technet/t reeview/default.asp?url=/technet/sec</u> <u>urity/prodtech/Windows/Win2kHG/06Tmplts.asp</u> (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 Ser vices NG Upgrade Centre Upgrade from Checkpoint 4.1 to Checkpoint NG. February 11 2003
- Appendix C Checkpoint Technical Services NG Upgrade Centre Install Firewall Module for NG FP3. February 11 2003