Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst (GCFW) Practical

Assignment Version 3.0 Option C

"Perimeter Security for an on-line business in today's treacherous world of e-business …"

Submitted By

Seamus Hetherton
Date: 17th August 2004

Abstract

GIAC Enterprises is a medium sized company in the fortune cookie business for the last 10 years. The company has a number of groups one of which sells fortune cookie sayings online. GIAC has a niche in the market to supply other fortune cookie companies with saying's and is predicted to grow significantly over the next 2 – 3 quarters. GIAC sales employee's are in the process of signing a number of large contracts with other fortune cookie companies around the world for the supply of fortune cookie sayings.

The current network setup for their online business is a rudimentary packet filtering device that is connected to the local ISP. GIAC have experienced numerous violations to their Internal Network ranging from their company Web Server being compromised and de-faced to virus outbreaks severely impacting their normal business operations. GIAC are totally reviewing their IT security policy's and procedures to protect their business so that they can obtain acceptable levels of availability appropriate to the business process needs.

H-Secure Solutions (Hetherton-Secure Solutions) have been engaged to define an appropriate network architecture protect the Company's expanding business operations. Although considerable growth is predicted, margins are low in this business and there are of course budgetary constraints for equipment purchase – the total cost of ownership including ongoing maintenance of the IT systems must also be considered when recommending a solution.

Assignment 1 – Security Architecture

Clarification of Requirements/Business Process

The initial requirements were to define a network security architecture for GIAC Enterprises online cookie business with access requirements (and restrictions) for:

- Customers (Companies or individuals that purchase bulk online fortunes)
- Suppliers (Companies that supply GIAC Enterprises with their fortune cookie sayings)
- Partners (International companies that translate and resell fortunes)
- GIAC Enterprises employees located on GIAC Enterprises internal network
- GIAC Enterprises mobile sales force and telecommuters
- The general public

A number of discovery meetings were scheduled with GIAC personnel and the following additional requirements/business process information were documented so that where relevant they were comprehended as part of the design in terms of components selected etc.

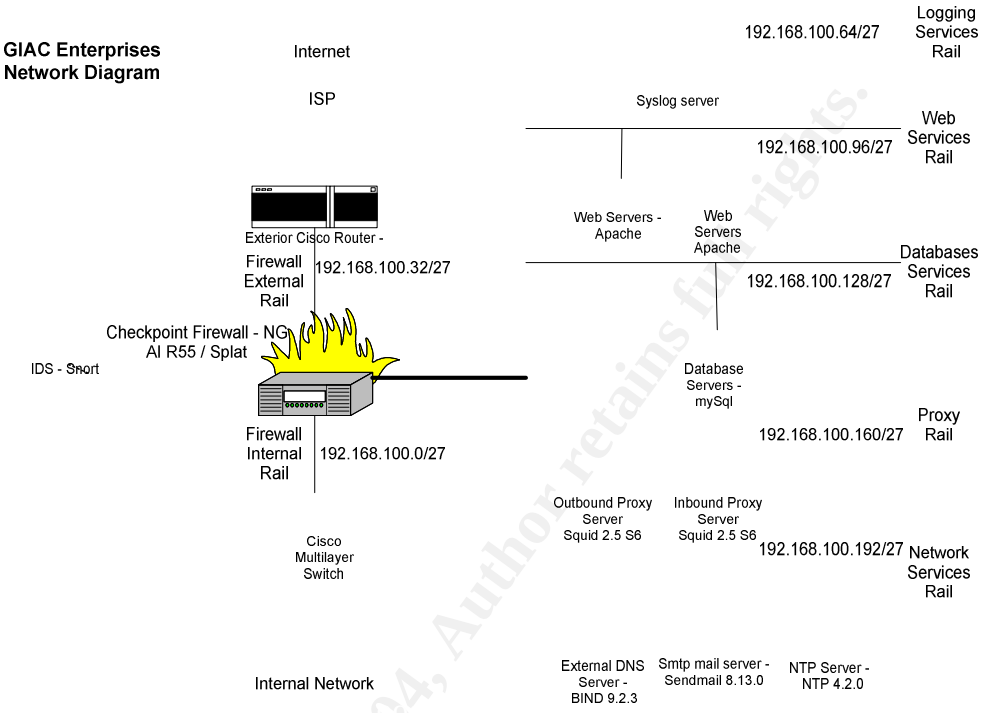
- GIAC currently has 60 employees, 20 of which are Sales personnel located in different Regions around the World
- GIAC have a MS windows based environment internally using Microsoft products for general office applications – Outlook for internal email, MS Word, Excel etc
- GIAC use Intel based HP Servers for their applications / database's which they purchase directly with required Operating System and associated maintenance contract – they standardize on 2 models – a low end DL320 and a mid-range DL380-G3 Server for high performance applications such as Database Servers etc
- GIAC currently use Cisco Network Equipment for both Layer2 and Layer 3 Connectivity which support personnel are familiar with – any additional Routers / Switch's should also be Cisco unless there is a compelling reason to use another vendor …
- GIAC Employee's require Internet access for business purposes – this includes www access to Supplier's/Partner's websites and more generally for normal business use. ftp access is also a requirement.
- GIAC Sales personnel will require secure remote access to GIAC Internal Network to access email, internal database applications etc …
- Most GIAC employees will require secure remote access to GIAC Internal Network to support employee's working from home as per the GIAC's telecommuting policy which allows employee's to work from home 1 day per week as per agreement with their Manager – GIAC management has found this flexibility has improved employee

satisfaction/ productivity and wants to roll the capability out without compromising security.

- GIAC Suppliers must be able to upload fortune cookie sayings online when stock levels reach minimum quantities – GIAC need to operate Just In Time methodology to reduce stock inventory levels so as to maximize profits in a competitive market
- GIAC Partners need to be able to download batch's of fortune cookie sayings when required for translation and re-sale subject to credit limit checks
- Ease of Management/Maintenance of the environment is a key requirement – support personnel that have expertise in different areas ie Server/Operating System, Database/Applications and Network and will be expected to support the environment in 7x24 Hour rotations through cross-training – hence ease of management is crucial.
- Network Redundancy is not a requirement – recovery of any system within 2 Hours is a requirement – the business process will ensure that Large Customers have stock levels adjusted to appropriate levels so that unforeseen service interruption has minimal impact to revenue.
- GIAC estimate that they will reach Sales of 1,500,000 fortune online cookie sayings per week

Design Proposal/Components

Attached is a network diagram of the Design we recommend GIAC implement ;



The following table outlines the addressing scheme used – Private non-routable addressing as per RFC 1718 are used for the firewall and associated components in the DMZ. The ISP has allocated a pool of public routable addresses – initial allocation is for 30 addresses which are represented by a.b.c.0/27 for the purposes of this proposal. The Router will connect to the ISP on a Subnet w.x.y.0/27 which the ISP has allocated to GIAC…

We have used Variable Length Subnet Masks to subnet a single private Class C Subnet ie 192.168.100.0 into smaller subnets for each of the rails required in the DMZ – a standard /27 mask is used for all subnets to be consistent and for ease of maintenance.

GIAC also use private addressing from the 192.168.0.0 Class B Subnet. Subnets 192.168.0.0 – 192.168.63.0 are reserved for GIAC Internal Networks.

GIAC have reserved 192.168.1.0/24 as an Internal Management Network.

IP Addressing Scheme

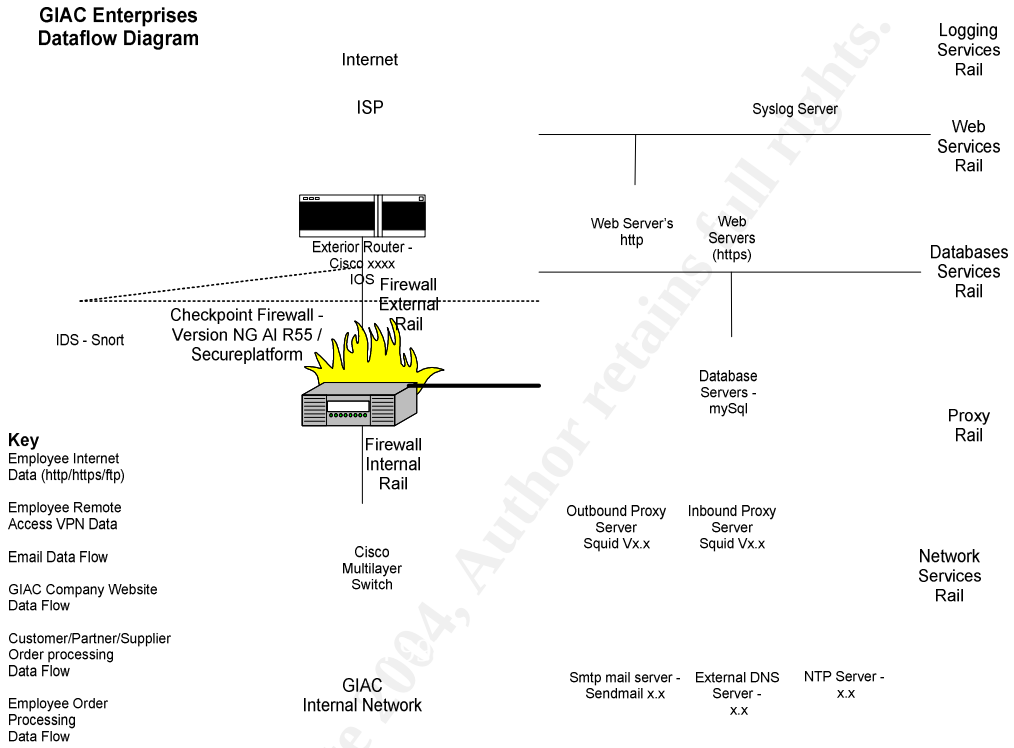
Private IP Address	Device	Public Address	Comments
192.168.100.0/27	Internal Rail - VLAN 2 (Connection to Multilayer Switch)		
192.168.100.1	lan-router-ir		IP Range 1 - 30
192.168.100.2	Reserved		
192.168.100.3	Reserved		
192.168.100.4	abaddon-ir		
192.168.100.5	Reserved		
192.168.100.6	Reserved		SM
192.168.100.31	Broadcast		255.255.255.224
192.168.100.32/27	External Rail - VLAN 3 (Connection to External Router)		
192.168.100.33	isp-router-er		IP Range 33 - 62
192.168.100.34	reserved		
192.168.100.35	reserved		
192.168.100.36	abaddon-er	a.b.c.1	
192.168.100.37	reserved		
192.168.100.38	reserved		SM
192.168.100.63	Broadcast		255.255.255.224
192.168.100.64/27	Logging Services Rail - VLAN 4 (syslog server)		
192.168.100.65	abaddon-lsr		IP Range 65 - 94
192.168.100.66	giac-syslog		SM
192.168.100.95	Broadcast		255.255.255.224
192.168.100.96/27	Web Services Rail - VLAN 5		
192.168.100.97	abaddon-wsr		IP Range 97-126
192.168.100.98	Web_Server1_static	a.b.c.2	
192.168.100.99	Web_Server1_Dynamic	a.b.c.3	
192.168.100.100	Next Available IP		SM
192.168.100.127	Broadcast		255.255.255.224
192.168.100.128/27	Database Services Rail - VLAN6		
192.168.100.129	abaddon-dsr		IP Range 129 - 158
192.168.100.130	Database_Server1	a.b.c.4	
192.168.100.131	Database_Server2	a.b.c.5	SM
192.168.100.159	Broadcast		255.255.255.224
192.168.100.160/27	Proxy Services Rail - VLAN7		
192.168.100.161	abaddon-psr		IP Range 160 - 190
192.168.100.162	Inbound_proxy1	a.b.c.6	
192.168.100.163	Outbound_proxy1	a.b.c.7	SM
192.168.100.159	Broadcast		255.255.255.224
192.168.100.192/27	Network Services Rail - VLAN8		
192.168.100.193	abaddon-er		IP Range 193 - 222
192.168.100.194	smtp_relay_server	a.b.c.8	
192.168.100.195	external_dns_server	a.b.c.9	
192.168.100.196	ntp_server	a.b.c.10	SM
192.168.100.223	Broadcast		255.255.255.224

The following table outlines the Components selected ;

Component	Vendor/ Application Name / Website	Software Version	Hardware/OS
Exterior (ISP) Router	Cisco Router www.cisco.com	IOS 12.3	Cisco 1721/ Cisco IOS 12.3
Stateful Firewall	Checkpoint Software www.checkpoint.com	Checkpoint NG AI R55	HP DL380 G3 www.hp.com Secureplatform
Proxy Firewall	Squid http://www.squid-cache.org/	Squid 2.5 STABLE6	HP DL320 G2 www.hp.com Red Hat Linux ES 3
DNS Server	Information Systems Consortium - BIND http://www.isc.org/	Version 9.2.3	HP DL320 G2 www.hp.com Red Hat Linux ES 3
SMTP Relay Mail Server	Sendmail www.sendmail.org	8.13.0	HP DL320 G2 www.hp.com Red Hat Linux ES 3
NTP Server	NTP.ORG - NTP www.ntp.org	4.2.0	HP DL 320 G2 Red Hat Linux ES 3
Syslog server	syslog is included in linux distribution	As per OS Revision	HP DL320 G2 www.hp.com Red Hat Linux ES 3
IDS	Sourcefire www.sourcefire.com	Linux Appliance (Based on Snort)	Sourcefire NS500 Intrusion Sensor
Interior Router/ Lan Router	Cisco Multilayer Switch www.cisco.com	IOS 12.3 (EMI Image)	Cisco 3550
Layer 2 DMZ Switch	Cisco Layer2 Switch	IOS 12.3 (SMI Image)	Cisco 3550
Web Server(s)	Apache Web Server http://www.apache.org/	2.0.50	HP DL380 G3 Red Hat Linux ES 2.1
Database Servers	Mysql http://www.mysql.com/	4.0	HP DL380 G3 Red Hat Linux ES 2.1

Dataflow – Services/Protocols/Applications

Below is our network diagram with the Dataflow in GIAC Enterprises illustrated ;



Internal employees access the Internet using HTTP/HTTPS/FTP through the Proxy Servers located on the Proxy Rail in the DMZ – the IE Browsers on the Client machines are configured to connect to the proxy server on a non standard port that the proxy Server is listening on. This prevents Trojans on machines that have been infected connecting out to the Internet and compromising the perimeter. The proxy servers will also be used to block access to sites as required by the company. HR/Information Security personnel will define/maintain the list in line with company policy.

Mail from employees to external sites is sent from the Internal Exchange Server to the Sendmail Mail server in the DMZ via SMTP. Mail from external users is also forwarded from the Sendmail Mail server to the Internal Exchange Server using SMTP after it is virus scanned.

A Web Server on the Web Services Rail provides all Company Product Information using HTTP – files are uploaded to the Web Server as required using the ssh protocol to update content.
Ordering is done on a Web Server using HTTPS Protocol – the web server communicates to a backend SQL Database to retrieve fortune cookie sayings and order processing using stored procedures run with the relevant customer privileges. Smaller customers can order and download directly using HTTPS once credit card details are verified.
Larger Customers will order by accessing the HTTPS Server but have the option of getting the batch file encrypted and emailed to them using pgp software - they can specify this in their user profile once they get a licence to use it in the country where they are based. Once the order is submitted, scripts running on the Web Server will perform credit checks, extract fortune cookie sayings into a batch file, encrypt using pgp and email the file to the customer.
Partners will use the same mechanism as Large customers.
Suppliers will receive automatic email notification when GIAC stock levels reach certain thresholds set by the purchasing group – in response to this they will email batch files which will extracted, de-crypted and uploaded into the fortune cookie database.

GIAC employees manage orders using applications/tools that perform sql query's/update's to the external database – external databases are also copied and backed up to internal Database servers for disaster recovery purposes.

The DNS Server in the DMZ provides hostname to IP Address lookup services to the Outbound Proxy and Sendmail Server using the DNS protocol – IP Address's are resolved and cached for sites accessed on the Internet – no DNS Entries for internal hostnames are stored on this Server – this prevents hacker's on the Internet from mapping the Internal Network using the DNS Server - a DNS Server on GIAC's internal Network is used for internal hostname resolution.

Most of GIAC's employee's will have secure remote VPN access to GIAC's Internal Network using the IPSEC Protocol ie Client machines running Checkpoint SecureClient VPN establish an encrypted connection to the Firewall using the IPSEC Protocol using a defined authentication scheme. An internal IP Address is assigned to the Client and decrypted traffic will traverse GIAC's Internal Network. Access can be restricted to specific services, networks for different groups etc as required.

The NTP protocol is used to synchronize the clocks on the Server's in the DMZ. The NTP Server itself synchronizes its clock off a Server on the Internet – NTP uses UDP/123 to communicate.

All systems in the DMZ send their logs to a logging host using the syslog protocol – The syslog Server is used to consolidate logs from all systems to correlate events.

Defence In Depth

All components in the design are leveraged to provide defence in depth by using a range of technologies, multiple vendor's, hardening of systems so that only required services are enabled and dedicated systems for specific services. Also in addition to implementing and configuring the components as designed the system needs to be tested, audited and maintained to meets the goals of the business.

Where possible additional levels of defence in depth without adding additional cost was implemented so that we have maximized the capabilities of all of the components used.

Filtering Routers:

We are using the static filtering on the Router's. Static filtering has a number of security weaknesses/limitations – firstly all packets are processed individually and there is no method of maintaining "state" hence attackers can craft packets that will be allowed through. Static filters cannot inspect payload and have problems dealing with some of the more complex protocols such as FTP ie all tcp traffic with destination port of >1023 must be permitted (for passive ftp) which would allow any service above 1023 e.g. X-Windows to be accessed.
However, static filtering is extremely useful for high level filtering of unwanted traffic which provides defence in depth and also takes the load off other components such as the Firewall.
In order to mitigate the weaknesses/limitations of static filtering we are using a Stateful Firewall which provides stateful filtering and inspection for some protocols for granular control of traffic – more recent version of Cisco IOS S/W support stateful filtering ie reflexive ACL's. This is a relatively new capability on Cisco Router's – although it is an added feature we get at no additional cost it would require further evaluation e.g. the impact on memory resources which is used to store connection information and is limited on Router's – also as it is new support personnel are less familiar with it so it could be difficult to maintain/troubleshoot – hence we have not included it as part of this proposal.

The Routing configuration of the External and Internal Routers is another important security consideration – EIGRP which is a Cisco proprietary dynamic routing protocol is used on the GIAC's Internal Network – static routes are used in the DMZ to route traffic and of course BGP Routing is used on the Internet.
GIAC uses private non-routable addresses internally as per (RFC 1918) and routable address's from an ISP allocated pool for externally facing systems – static NAT is configured on the firewall to for 1:1 mapping of relevant dmz server address's to public address's on the Internet.

External Router

The external router is used to land the connection to the ISP – This is our first line of defence against the Internet at large and we will leverage its use as a security device by applying appropriate ACL's to filter traffic both inbound and outbound.

Inbound Filtering – Internet traffic should never use Source IP Address's that are private – this can be as a result of a device leaking out packets, incorrectly configured hardware or someone spoofing our address – if this reaches the target machine it will try and respond and get a Destination unreachable message which can be an effective DoS technique – the Loopback Address and Broadcast Address should also not be used. An inbound filter will be applied to filter out this traffic. We could also filter out un-used address's as per IANA but have decided not to as the maintenance overhead does not justify the benefit – we could also filter out IP Addresses from countries where a lot of attacks are originating recently eg China – however as we are doing business there this is not feasible.

Outbound Filtering – The Firewall will use static NAT address's for the Proxy Server(s), DNS Server(s), SMTP Server from allocated ISP Pool – so the ISP allocated pool should be the only valid source IP address's outbound – An outbound filter will be applied to the external Router ISP Interface to filter out any other address's – this will prevent the Firewall leaking out internal address's giving hacker's clues to the structure of GIAC's internal network.

Internal Router

The Internal Router is an existing Multilayer Switch (LAN Router) in our Design which we are leveraging to apply filtering to enhance our defence in depth strategy. The same functionality is available in terms of ACL capabilities on the Multilayer switch except performance is much better as ACL's can be processed in hardware if logging is not required.

Outbound Filtering – Only valid Source IP address's on GIAC's Internal Network's should be destined for the DMZ – an outbound filter will be applied to the Firewall Interface to block other IP Address's – this will prevent an attacker located on our internal network or running a tool on a compromised system can no longer spoof their source IP address while attacking hosts on the Internet – this will help us become a good Internet neighbour, avoid any legal issues from other users/companies or disconnection by the ISP as a result of a DoS attach being launched from our systems.
Critical Services used on our Internal Network will also be blocked using the outbound filter – this is to prevent critical service/network information reaching the DMZ/Internet which could be used by hacker's to compromise our systems.

Firewall - Stateful Checkpoint Firewall

As discussed with regards to the Filtering Routers, the use of static filtering has a number of weaknesses. The provision of the Checkpoint firewall gives us stateful filtering and stateful inspection of a number of protocols including ftp, http, CIFS. The most recent version of Checkpoint Software (Checkpoint NG AI R55) which we have recommended also has Intrusion Protection System capabilities. This does have an additional licence fee but gives us another technology for our defence in depth strategy.
DMZ Networks: We have separated the dmz into a number of different functions including Logging Services, Web Services, Database Services, Proxy Services, and Network Services – this provides us an extra level of isolation and defence in depth. If for example the static web server is compromised there is no direct access to any of the other service rails - this is easily implemented with components we selected without adding multiple interfaces which are not very expensive but the number of PCI slots in the Server are limited – to implement it we use 802.q trunking technology – both the Checkpoint Secureplatform Firewall and Cisco Switch's support 802.1q trunking – we can add additional Service Network's at point in the future as additional servers/functions are added. It also makes the policy management more logical and easy to understand so that mistakes are less likely.

Remote Access VPN

Remote Access to GIAC's Internal Network is a requirement and will be implemented using Checkpoint's SecureClient VPN solution using IPSEC Protocol.

The Firewall is being used as a VPN Device for remote users to login to the GIAC Internal Network. We have recommended this for a number of reason's ;

- Ease of Management including Personnel Firewall – GIAC sales employee's are located around the globe in all sorts of hostile environments – Personnel Firewall's are a must and the easy of Management of using the checkpoint Firewall GUI to manage and enforce the company's security policy down to the Client level is an advantage – personnel firewall settings can be verified and logs monitored centrally …

- The Firewall H/W has more than enough performance to handle the additional load / overhead of encryption/de-crypt ion – there are also additional options in the future of increasing the performance by purchasing a software performance pack licence and/or a pci vpn encryption card although we do not see any that this will be necessary in the short/medium term.

Note: Although Checkpoint's SecureClient Application allows a centrally managed policy to be downloaded to Client's , there is no local file integrity checking which is a weakness.

Site to site VPN

This proposal does not currently include Site to Site VPN with Customer's / Partner's as it depends on the ability of the Customer/Partner to install/support a VPN device on their end or alternatively GIAC could spec a standard solution and deploy it – the business process does not currently require it but it is an additional step that can be taken in the future if required – the VPN capability of the Checkpoint Firewall can be leveraged – one point to note is that you can have interoperability/reliability issues with different vendor's implementation of IPSEC / Interpretation of the RFC – this consultant has experienced such issues whereby additional hardware had to be deployed to resolve the problem such that a device from the same vendor was used at each end. This would of course increase deployment costs and management overhead. If a site to site VPN becomes a requirement at a future date it will be investigated further and a proposal developed based on a better understanding of Customer's/ Partner's infrastructure etc.

Proxy Server Firewall(s)

The Squid Proxy Server is an application aware firewalls and performs payload inspection on http requests – we are using one proxy server for normal user http traffic requests to the Internet and a 2nd proxy server as a reverse proxy for http requests from the Internet to our Web Server(s) as an extra layer of protection – proxy'ing gives us a level of protection over and above static filtering and stateful filtering and squid also provides filtering capabilities which we can use to provide defence in depth. Also there are caching facilities to improve performance. The outbound proxy server is also used to provide ftp access for users to the Internet.

An additional and very powerful security measure that we have recommended is to perform content filtering on the reverse proxy server using a plug-in tool for squid called "Jeanne". This tool allows you to specify exactly what files and directories are accessible on the Web server and will hide a lot of vulnerabilities that may be present on the Web Server due to lack of maintenance, incorrect configuration etc. and is another defence in depth strategy.

A useful tool for analyzing the squid logs is Calamaris which we also recommend.

EMAIL

All email to/from GIAC Enterprises is routed through an SMTP mail relay in the DMZ – The SMTP Server will be built so that outbound Mail headers that would reveal information about the internal network will be stripped out. GFiMailEssentials and GFiMailSecurity from GFi Security and Messaging software http://www/gfi.com/mes/ will be installed on the SMTP Gateway to filter spam mail and protect against viruses, exploits & Trojans.

SMTP will be configured on both the Windows 2003 Internal Exchange Server and the Sendmail Linux Server in the DMZ – the use of two different implementations of the same applications on two different OS's is an extremely powerful security defence in depth measure. A hacker would have to compromise two different vulnerabilities in the same timeframe to compromise our perimeter through the email infrastructure.

DNS

We are using a split DNS model with separation of our IP Address space as a defence in depth strategy – a DNS Server in the DMZ will provide information that is required by the Internet. The version of BIND we are using allows us to configure the external DNS Server recursively for hosts in the DMZ and non-recursively for Internet hosts to prevent any cache poisoning attacks. Zone transfers will not be allowed initially but may be required later with the ISP to provide DNS redundancy – before we allow that we will need to validate that the ISP restricts zone transfers by source IP Address. DNS configuration will be validated to ensure it is configured correctly after installation using tools such as nslookup.

Intrusion Detection System

An IDS device is added to as another layer of security to detect any attacks that may get through the security provided by other components such as the Firewall(s) and Proxy Server(s). The IDS device selected is a low end appliance based on snort – new signatures from the vendor will be updated regularly - although the appliance is only has 2 ports all rails will be monitored using the SPAN feature of the Cisco Switch ie the span feature allows us to send traffic from any number of ports/vlans to a specified port on the switch where the IDS device is attached – also, the span port can be configured to disable traffic from the connected device thus making the IDS undetectable to hacker's etc. Tuning will be required on the IDS rule base to decrease the number of false positive's which can be one of the major drawbacks of IDS's ie too many incorrect alerts for legitimate traffic can mask the real attacker's traffic – also IDS's based on packet analysis can only detect attacks for which it has signatures so zero day attacks will go undetected – to reduce the number of false positives one option is that monitoring of the external interface to the Internet can be eliminated – the downside of this is that we will

not have the same visibility and thus may not be able to mitigate attacks before our perimeter is compromised. The other weakness is that IDS's only detect and alert but do not block traffic – blocking of traffic can be done by Intrusion Protection Systems which latest Checkpoint Firewall software versions have integrated – this feature known as Smartdefence can be used by purchasing an additional licence and yet another defence in depth strategy we can leverage either initially or as an improvement later after the project is implemented when resources are available.

NTP

NTP is installed on 2 Server's for redundancy and is used to synchronize the clocks on all the Server's in the DMZ. This ensures accurate correlation of any log file entries to help identify any attacks etc on the perimeter that may occur ie synchronization of times will help to clearly identify the sequence of events.

Syslog Server

The syslog server is a host where logs from all systems are centralized – this is one of the important aspects of defence in depth and ties all systems together so that trends can be spotted ie "The Big Picture" – this system will only run syslogd and sshd for login by administrators. It will also reside on its own segment in the dmz – the logging services rail.

The Checkpoint Firewall will also be configured to send its logs to the syslog firewall so that its easier to correlate all events. This can be done by running a backround process on the firewall to send its logs to the syslog server as follows;
- fw log –ft | logger –p local0.info –t hostname &

We will also log DNS zone transfers which can be indicative of a hacker attacking our network.

DMZ Servers Operating System Security

ALL Servers located in the DMZ must be hardened – for GIAC systems who will be using Linux, the process can be automated using Bastille Linux scripts which can be downloaded from http://www.bastille-linux.org.

DMZ Servers Application Security

Apache Web Server – the apache web server application which runs as the httpd daemon will be run as user nobody so that permissions are restricted. All web server files will be owned by root and only root will have write

permission. The directories that the that can be accessed through the web server will be limited by specifying them in the httpd.conf file which the httpd daemon reads on start up. The config file will also be modified so that banner information is not given out using the “Servertokens” directive.All scripts will be fully tested including boundary testing.

Internal Servers Operating System Security

For Windows systems, SANS provides checklists which can be purchased/ downloaded and used to harden and lockdown – we recommend this on Internal systems.
The Centre for Internet Security has a number of auditing tools that can check the configuration and make recommendations to locking down also.
http://www.cisecurity.org/

End User Operating System Security

All end user systems should be patched regularly and should have anti-virus software installed and centrally controlled updates to .dat files for the latest virus signatures.

Baseline Host Auditing

Tripwire will be used frequently for baseline auditing to detect unauthorized changes to systems.

Physical Security

All Servers and Network Equipment will be installed in a secure area with restricted access only to personnel that require it for maintenance on the systems.

Operations Review

Ongoing maintenance of the security policy will be required to keep up with new threats which are released daily – a daily operations review should be setup to cover the following ;

- Any alerts from IDS / Log files – assessment and follow-up assigned and tracked until closed
- New Threats/Vulnerabilities – Many threats will not affect GIAC as they may be related to other products or specific configurations – an assessment is required to rate them – if it is critical to GIAC’s

operations then options to mitigate the threat until patches are available need to be explored.

- Any new service requirements should go through a extensive technical review before approval – if approved they should be tracked and implementation validated – also the security policy should be tested to validate that it is functioning as expected.

Performance/Cost

The table below outline's the cost of all of the infrastructure components including hardware costs, software costs and maintenance costs. These are the maximum costs and can be further reduced by any discounting arrangements GIAC may be able to negotiate or re-use of existing hardware.

Function	**Vendor/ Description**	**Part Number**	**Cost ($)**	**Annual Maintenance Year 1-3**	**Comments**
Stateful Firewall	Checkpoint Express S/W – incl FW-1, VPN-1	CPXP-SC3-100-NG	6500	2925 (975x3)	100 User Licence
SecureClient VPN Remote Access	Checkpoint VPN-1 SecureClient	CPVP-VSC-100-NG	7000	3150 (1050x3)	100 User Licence
Checkpoint Firewall /Management Server	HP Server	HP DL380-G3	4500	700	
DNS Server	HP Server	HP DL320-G2	2500	450	
SMTP Server	HP Server	HP DL320-G2	2500	450	
Outbound Proxy Server	HP Server	HP DL320-G2	2500	450	
Inbound Proxy Server	HP Server	HP DL320-G2	2500	450	
Web Server's X 2	HP Server	HP DL380-G3	9000	1400	
Database Server's X 2	HP Server	HP DL380-G3	9000	1400	
NTP Server	HP Desktop X 2	N/A	0	0	Existing Hardware
Syslog Server	HP Server	HP DL320-G2	2500	450	
IDS	Sourcefire	NS500	3995	740	

	Intrusion Sensor				
Router	Cisco 3600	CISCO3631-CO-AC	7500	2070 (3 x 690) 6000 (3x2000)	
Router	Cisco 1721	CISCO1721	3800 (1900 x2)	1952 (292 x 3 x 2)	X2 incl Spare Router in case of h/w failure
Switch	Cisco 3550 Switch X 2	WS-C3550-24-SMI	6000	714 (238 x 3)	Spare required
			$62295	**$15250** **(approx $5000 per Year Annual Maintenance Costs)**	
ISP Connectivity	As per local ISP	N/A	TBD	TBD	

The first component we should consider is the traffic levels we expect on the ISP connection and the resultant capacity of the link we require – the fortune cookie sayings themselves which is the business critical data which is transferred between Customer's, Supplier's and Partner's. GIAC estimate that they will sell 1,400,000 sayings per week = approximately 100,000 per day – assuming an average of 100 character's per saying this equates to 10,000Mbytes per day = 500Mb per Hour which a T1 line will easily be able to handle.

The traffic for all the business support process's is more difficult to predict ie Internet access, email etc. However, we do know that we have 20 Sales personnel and a percentage of other employees using remote access VPN (50 people working on average of 1 day remotely => average of 10) so total number is average of 30 per day. Initially we will recommend a T1/E1 connection which based on previous experience and should be adequate for current predications allowing for growth but can be easily upgraded if required in the future. As we are not using redundant ISP's in this phase of the implementation a highly reputable ISP with a proven track record of high availability should be selected.

GIAC already uses Cisco equipment for Layer 2 and Layer 3 connectivity and so this dictated the vendor for Network equipment – the existing LAN Router/Multilayer Switch already in place was leveraged to provide connectivity to the DMZ and appropriate ACL's applied to the interface. The 3550 process's ACL's in hardware with little or no impact to the cpu provided

they are not logged - if logging is required it will be enabled initially and cpu monitored – if excessive cpu utilization occurs logging on some of all of the ACL's applied will be removed.

The Cisco 1721 exterior router was selected for connection to the ISP – we need a spare in case of hardware failure to meet our 2 hour SLA of recovery of any hardware component so the 1721 is quite cost effective – when we purchase hardware we have to consider the ongoing maintenance costs which can really add up so it's a balance between performance required and cost – ACL's can consume a lot of cpu and the larger the ACL is and where in the ACL a match occurs will impact performance ie the ACL is processed from top down until a match occurs so the larger the ACL and the line where the traffic match's will have an impact of the router cpu – for this reason the ACL should be designed to minimize the impact on the router ie permit statements for the highest volume of traffic should be placed as near to the start of the ACL as possible – we will only be applying a small number of high level ACL's to the interface – we will not log most of the traffic to save cpu cycles on the router but will need to log some traffic which we would want to know about and may alert us to malicious activity. If the Router needs to be upgraded in the future due to growth we will not have invested a hugh amount and will recommend and a new higher end platform – this could be justified in terms of additional revenue etc.

The fact that GIAC use HP Servers already for their applications in order to leverage existing Spare Servers we selected Secureplatform from Checkpoint as the operating system running on a HP Server – this has the benefit of being able to use an Open Server with the security of an appliance ie Checkpoint pre-harden the OS and disable all services not required – the installation is extremely quick and can be restored in less than 30 minutes – the performance of the Firewall is much greater than we expect to use even with significant growth – however it is also been used as the Management Server which stores the Logs and as a VPN device so the cost of this hardware compared to other vendor's appliance's is easily justified on the basis of standardizing on the Server hardware and using a common spare for numerous applications. A number of options are available to increasing the Firewall's performance in the future

- Purchase a performance pack licence – this enables software acceleration techniques to boost performance
- Purchase a PCI VPN Acceleration Card to offload encryption from the Server CPU

A redundant firewall configuration was not part of this proposal but can easily be added later if required – business process's will be adjusted to comprehend outages as a result of hardware failures of any component and recovery time including on-call policy for support personnel which currently is a 1 hour 7x24 hour response.
In terms of Remote Access VPN we also recommended the use of Checkpoints personnel firewall for the additional security and ease of management – the cost for this item is quite substantial but justified as its one of the main threats – if the cost is prohibitive GIAC could use another vendors

product which may be cheaper but would lose the ease of management and control.

Services – Proxy, DNS, NTP and Sendmail were all implemented on different hardware servers for additional security – other than Sendmail add-on software from Gfi the software is free – to reduce hardware costs existing hardware could be leveraged to avoid cost of new purchases – however different aspects of hardware specification is more critical for certain applications and must be comprehended as part of hardware selection – Squid Proxy Servers will consume large amounts of memory due to the nature of HTTP whereby a user accessing a single web page can download multiple web pages – this can also have a knock-on affect to the cpu which may start process's for each page – depending on level of utilization Server resources can be quickly consumed so don't use a PC for this application. However, with a workforce of 60 employees the outbound proxy should not be overly burdened.

IDS – Although Snort is a free application which can be installed on an open server, we have recommended the sourcefire appliance for ease of maintenance/management – GIAC will be paying a premium for a pre-hardened appliance, with vendor supplied signature updates and helpdesk support – failure of this component will not immediately impact business operations so a spare is not absolutely necessary – a support contract which supports GIAC's requirements will be purchased.

Assignment 2 – Security Policy and Component Configuration

Router Hardening

The External router is our first line of defence against the Internet where we will deploy high level filters to filter out traffic which we know is not legitimate or required as part of GIAC's business. Before applying any policy, the Router should be configured and hardened to ensure that the device itself is not the subject of a compromise ie

- Password Encryption

All passwords stored in the configuration should be encrypted – this is done by specifying ;
service password encryption
This is to prevent someone looking over your shoulder and seeing the password – if someone actually has the encrypted password its easily broken with programs from that can be downloaded from the Internet so caution is required here.

- Administrative access

Limit the hosts or networks that can connect to the router – in GIAC's case access will be limited from the Internal Management Network (192.168.1.0/24) using ssh;

Access-list 10 permit 192.168.1.0 0.0.0.255

Line vty 0 4
Access-class 10 in
Transport input ssh

Note: Cisco only support ssh v1 which is not as secure as ssh v2 but its better than telnet which uses clear text passwords.

- Disable SNMP Access

Snmp will be disabled on the External Router – once configured we will manage it locally if any changes are required – disabling snmp means that we will not receive any traps for interfaces going down etc but we will use other mechanisms to alert us for these types of failures – command required ;
no snmp

- Disable Source routing

Loose source routing can be used by attackers that have knowledge of the network to route packets to required destinations possibly by-passing

access level controls. To prevent this possibility source routing is disabled as follows ;
no ip source-route

- Disable un-used Services

Any services that are not required should be disabled so that even is a vulnerability is discovered, GIAC will not be exposed to it ie
no service tcp-small-servers
no service udp-small-servers
no service finger
no ip http
no ip bootp

- Limit ICMP

Layer 3 to Layer 2 broadcast should be disabled to prevent malicious directed broadcasts from causing denial of service problems with is the basis of Smurf attacks. Also ICMP unreachable error messages which give out network information should be stopped ie
no ip direct-broadcast
no ip unreachables

- Warning Banner

A "warning banner" should be provided indicating that it is unlawful to enter without proper authorization. This is a legal requirement.

banner motd # Use of this system by unauthorized persons or in an unauthorized manner is prohibited

- Syslog

The syslog information should be send to our syslog server on the Logging Services Rail so that we can monitor events on the Router
logging 192.168.100.65

Router Policy

External Router

The policy applied to the **External Router** is to filter out traffic. To do this we create access-lists – enter global configuration mode on the router by typing **config t** and create the access lists as follows ;

ip access-list extended inbound_to_GIAC
deny ip 192.168.0.0 0.0.255.255 any
deny ip 10.0.0.0 0.255.255.255 any
deny ip 172.16.0.0 0.15.255.255
deny ip 127.0.0.1 0.0.0.0 any

permit ip any any

This access list prevents any private ip source addresses entering our network which may be someone spoofing our address incorrectly configured systems or leaky NAT devices. We also prevent loopback addresses which can be used as part of an attack.

The above access list will be applied to the ISP interface in interface configuration mode with the following command ;
ip access-group inbound_to_GIAC in

Another access list is created for the outbound direction – all source addresses leaving our network should be from the allocated ISP range a.b.c.d/24 so the access-list can simply allow those addresses and deny everything else – however as a defence in depth strategy firstly we block any Microsoft traffic from passing out to the internet which could reveal valuable information about our internal network. – we should never see this traffic in the dmz as we are blocking it at the LAN Router also but its good to be paranoid in cases like this.

ip access-list extended Outbound_to_ISP
deny tcp any any range 135 139
deny tcp any any eq 445
deny udp any any range 135 139
deny udp any any eq 445
permit ip a.b.c.d 0.0.0.255 any
deny ip any any

Now this access list will be applied to the ISP interface in interface configuration mode with the following command ;
ip access-group Outbound_to_ISP out

Note : A common mistake is to apply the access-list in the wrong direction – care should be taken as the result could be at best downtime or at worst exposure of your network to malicious activity.

Mutlilayer Switch / LAN Router

Similarily, apply the following access lists to the LAN Router interface leading to the DMZ to provide high level filtering at that point.

ip access-list extended inbound_from_dmz
permit ip 192.168.100.0 0.0.0.255 any
permit ip 192.168.50.0 0.0.0.255 any
deny ip any any log

Now this access list will be applied to the inner rail interface in interface configuration mode with the following command ;

ip access-group inbound_from_dmz in

ip access-list extended outbound_to_dmz
deny tcp any any range 135 139
deny tcp any any eq 445
deny udp any any range 135 139
deny udp any any eq 445
permit ip 192.168.0.0 0.0.63.255 192.168.100.0 0.0.0.255
deny any any log

Now this access list will be applied to the inner rail interface in interface configuration mode with the following command ;
ip access-group outbound_to_dmz out

Building/Hardening the Checkpoint Firewall

As discussed in Section 1, we are using Secureplatform as the Operating System on which to run the Checkpoint Application – Secureplatform is a linux based (Linux 7.3) operating system pre-hardened by Checkpoint so that all services not required are disabled. No further hardening is required, other than to apply the latest Hotfix Accumulator to for the most up to date bug fixes and/or vulnerability fixes.

The Firewall should be build using the Checkpoint bootable CD – the following steps should be completed from the console of the Firewall Server - configuration of the policy itself will be done using the checkpoint gui.

Note: In order to save additional cost of a Server the Checkpoint Firewall Enforcement Module (Firewall-1 / VPN-1) and the Management are on the same Server – these functions can be separated if required but as GIAC only have one Firewall so one server will be used for both functions.

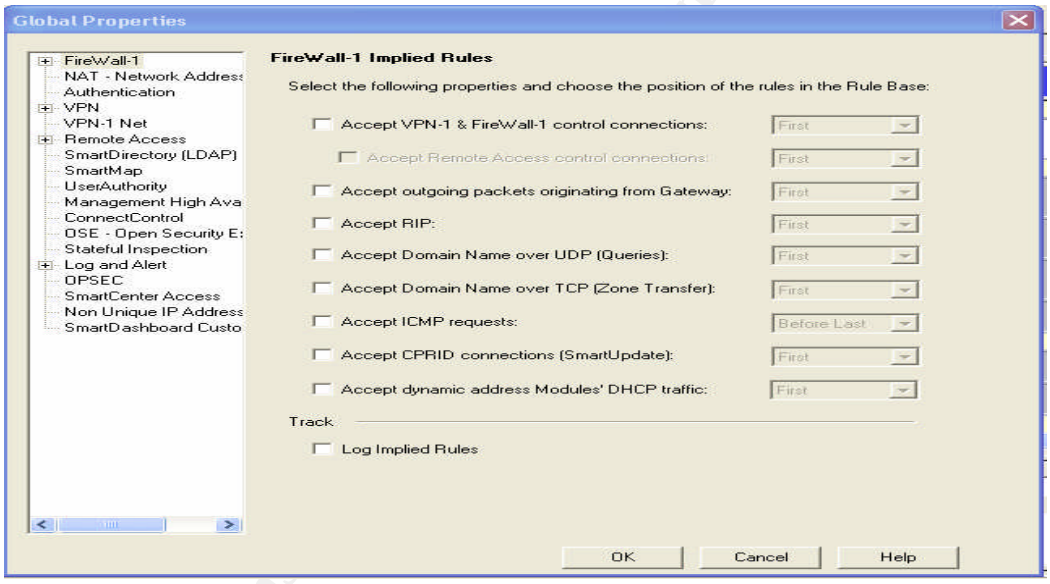
	Checkpoint NG AI Secure Platform OS/Product Installation

Step 1- Insert CD in Firewall Server	Insert the Checkpoint NG AI Secure Platform bootable CD in the Drive and reboot the Server
Step 2- Install Checkpoint Secure OS on Firewall	a) You will be prompted to Press <Enter> Key with 90 Seconds or Installation will be aborted – Press **<Enter>** immediately to proceed Install will start as follows ; Loading kernel, ramdesk, Starting installation process b) A scan on the hardware will be performed and You will be prompted to select **OK** to proceed with Checkpoint Secure Platform OS – **Note :** All data on the disk will be erased as part of this install … Select **OK** to proceed c) Select Keyboard Type and **OK** to proceed d) You will be prompted to select network device to use – Select one of the Interfaces and Select **OK** to proceed . e) You will be prompted for IP Address/Subnet Mask - Enter IPAddress/Subnet Mask and Default Gateway configuration. Select **OK** to proceed f) You will be prompted for HTTPS Server Configuration – default is to enable https web based configuration on port 443 – Allow default – Select **OK** to proceed g) You will be prompted that next stage will format the Hard drive and erase all data Select **OK** to proceed Hard drive will be formatted , OS installed and Checkpoint S/W installed … f) After install is complete you will be prompted to press <Enter> to reboot system and remove CD from drive … Press **<Enter >** to reboot system …
Step 3- Set Passwords on Firewall	a) Login to system with default password – login : admin, password : admin. You will be prompted to Change the admin password Also change expert password by typing expert at the command line (expert password will initially be set to admin password)

Step 4- Complete Network configuration	a) Configure Network Parameters - using sysconfig utility. (hostname, ip address etc) Type sysconfig on the command line and type n ; Set the Network Configuration Parameters by selecting the options ie 1) Hostname 2) Domain Name 3) Domain Name Servers 4) Network Connections Note1: Use Configure Connection Option to configure Interface IP Address / Subnet Mask. Note2: Use Add New Connection Option to create/configure vlan interfaces 5) Routing When complete Press "n" for Next c) Configure Time and Date by selecting the following options ; 1) Set time zone 2) Set date 3) Set local time When complete Press "n" for Next d) Skip "Import Check Point Products configuration" section - Press "n" for Next

Step 5- Complete Installation of Checkpoint Products	e) You are now at the Checkpoint Product Installation stage At the "Welcome to Checkpoint Suite" screen Press "n" for Next and Press "y" to accept the terms of the licence agreement and select the following options ; 1.( ) Check Point Enterprise/Pro 2.( )Check Point Express **Select 2 and N (Next) to continue** 1 ( ) New Installation 2 ( ) Advanced Upgrade **Select 1 and N (Next) to continue** You will be prompted with a list of Products 1.( ) VPN-1 Express 2.( ) SmartCenter Express 6.( ) SmartView Monitor 7.( ) SmartView Reporter Express **Select 1 and 2 and N to continue** Note: VPN-1 Express is selected for Firewall -1/ VPN-1 Gateway Functionality Smart Center is selected as the Management is local on the Firewall Validation – You have selected the following products for installation ; * VPN-1 Express and SmartCenter * Backward Compatibility module for VPN-1 Express **Select N to continue** Installing VPN-1 Express and SmartCenter Express R55… After install you will be prompted "Welcome to Checkpoint Configuration Program" You will now be prompted Do you want to install licences (y/n) [y] ? **Type n and <enter>** (Licenses can be installed later – automatically defaults to 15 day evaluation licence) You will now be prompted to Configure Administrators … Do you want to add administrators (y/n) [y] ? **y** Define Administrator name/password/privilege level ie Read/Write, Read or Customized Next define GUI Clients ie Next, you are asked to type random keystrokes that will be used in cryptographic operations to make it unique The Internal Cerfificate Authority is initialized and the Certificate's Fingerprint is created – take note of this so that when you connect you can validate you are connecting to the correct system .. Now Re-boot sytem by typing **reboot** to complete installation **…**

With regards to hardening the Checkpoint Application itself the main thing to be aware is that the Checkpoint Firewall in its default configuration will pass certain traffic un-logged – these are referred to as implicit rules which make the configuration easier in that you do not have to configure rules to allow Management of the Firewall itself. Traffic including DNS and icmp are also allowed through – In older versions of Checkpoint software this traffic was not even logged - the current version does allow logging of implicit rules however the 1st step we recommend is that all this traffic is disabled by default and specifically allowed by specifying appropriate rules as part of the policy - this will prevent support personnel not familiar with Checkpoint having to discover this the hard way in the future – the implied traffic is disabled by selecting the policy general properties and under Firewall-1 Implied Rules de-select all options so that traffic must be explicitly allowed as part of the policy ie



Implementing the Policy on the Checkpoint Firewall

To support the business the security policy required on the Firewall will be as follows;

- Allow WWW Traffic outbound to Internet via Outbound Proxy Server
- Allow WWW Traffic inbound to Web Servers via Inbound Proxy Server
- Allow SQL traffic from Web Servers to Database Servers
- Allow SQL traffic from GIAC Employees to Database Servers
- Allow email traffic from GIAC Employees to Internet via SMTP Server
- Allow email traffic from Internet to GIAC Employees via SMTP Server
- Allow DNS traffic from our external DNS Server to the Internet

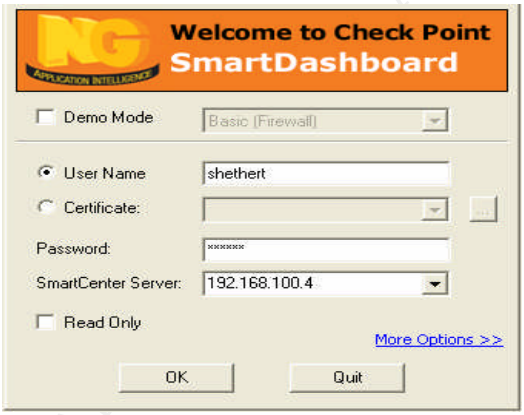
- Allow NTP traffic from external NTP Server to GIAC NTP Servers and from GIAC NTP Server to all other Servers in the DMZ
- Allow ssh traffic to all DMZ devices for Management – also CPMI traffic is required for firewall management
- Allow FTP traffic from GIAC employees to Internet via Outbound Proxy Server(s)

VPN Policy

- Allow IPSEC Encrypted traffic inbound from Internet to the Firewall using a minimum of 3DES for encryption and SHA1 for Integrity.

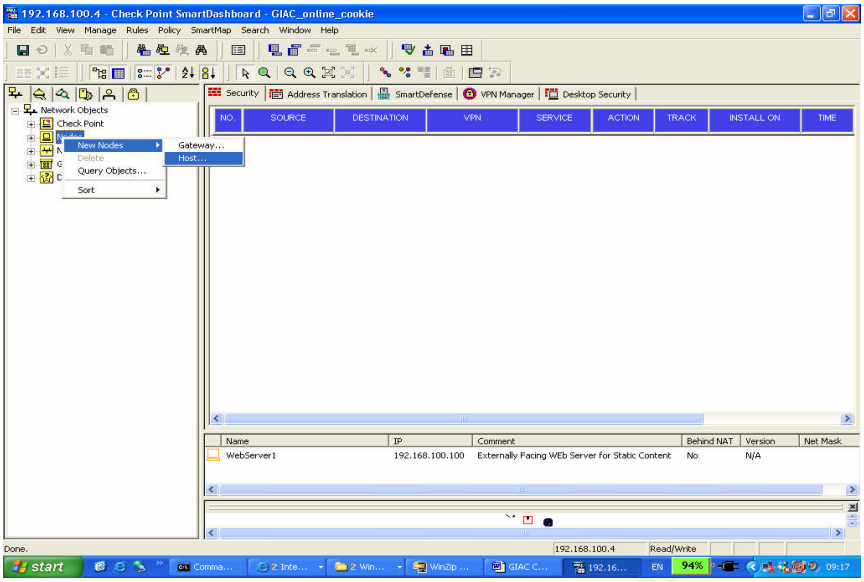
Configuring the Policy on the Checkpoint Firewall

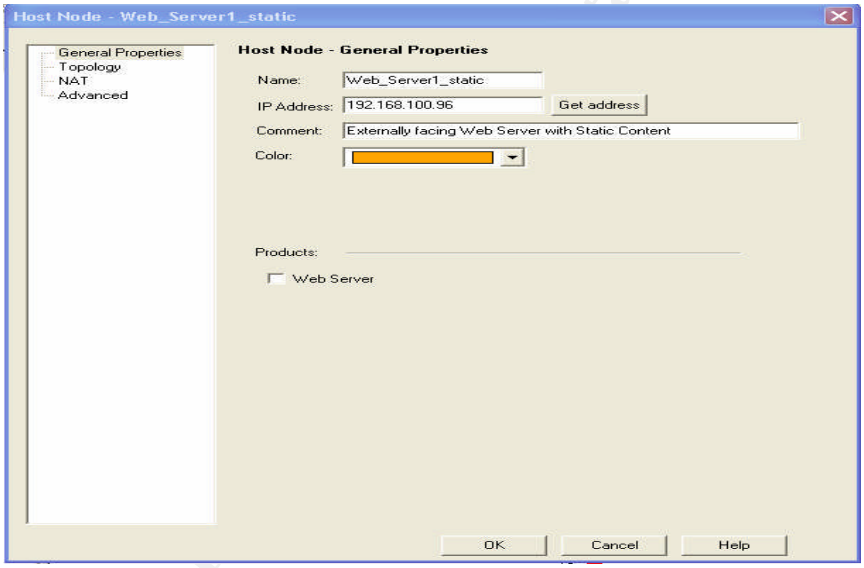
After the Firewall installation is completed, you can connect to the Firewall Management using the Checkpoint gui client which can be installed on a Windows or Solaris machine – in GIAC's case the gui client will be installed on a windows management server that is located on an internal management network – the administrators will connect to the management system using Windows Terminal Server. The gui clients can be installed from the CD or downloaded from Checkpoint's website. Connect to the SmartCenter Management Server (Firewall) using Smartdashboard. After initial login the rule base will be empty.



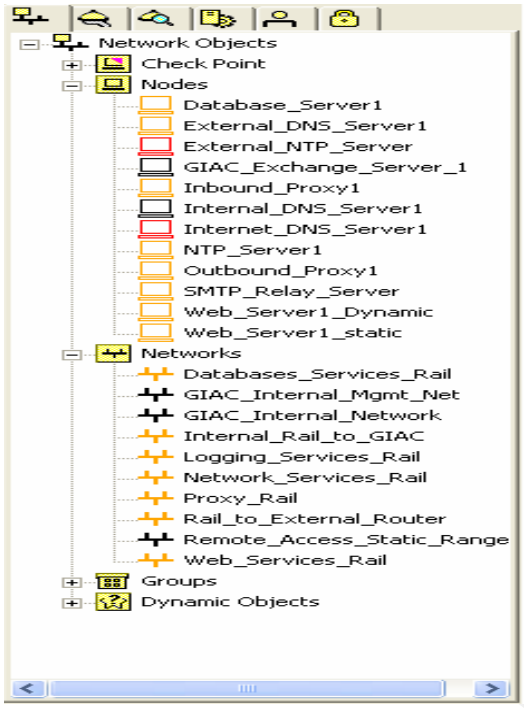
The firewall policy is configured using the following steps ;

1. The 1st step is to create objects for everything required in the Design - Everything in the Checkpoint Firewall is an object including the firewall, networks, hosts and services. Highlight the required object type and select New eg Host. Enter the name, IP Address Information, a comment and select a colour for the object. In our network we have selected Red as the colour for objects on the Internet, Orange for objects in the DMZ and Black for objects in the Internal GIAC Network. Below is an example to creating the Web_Server object – repeat for other's;

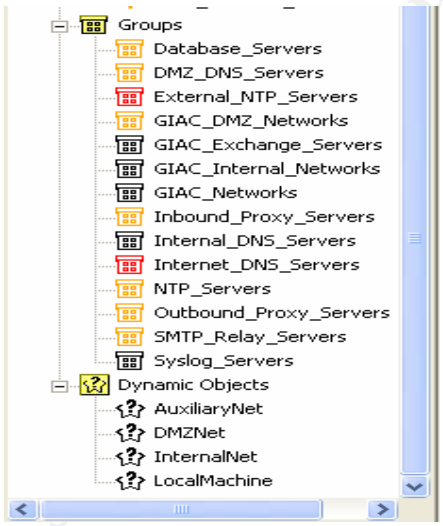




Repeat until all objects are created as shown below …



2. Now create the following groups and add the relevant objects to each group



Note: Groups are used to minimize changes to the rule base for ease of maintenance eg if a New Web Server is added, the object should be created, added to the Web Server Group and the policy installed ie no change is required to the rulebase itself thus simplifying updates.

3. Now we can start creating the Rule base – firstly we will create section headers so that rules are logically grouped again for ease of maintenance ie

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
	Firewall Management (Rule 1)								
	WWW Access (+ftp) (Rules 2-5)								
	Database Access (Rules 6-7)								
	email Access (Rules 8-11)								
	Network Services - DNS, NTP, syslog (Rules 12-17)								
	Remote Access VPN - SecureClient (Rules 18-19)								
	DMZ Network / Server Management (Rule 20)								
	Default Deny (Rule 21)								

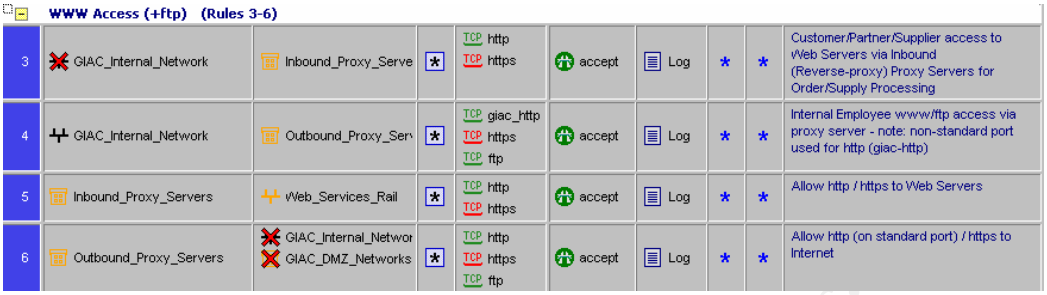
In terms of rule positions the positioning is important to achieve the correct results – as with the Cisco acl's the rulebase is checked from top down until a match is found. Rules that conflict or hide other rules will be flagged by the policy verification process. More granular rules for a specific service will normally be placed at the start followed by more general rules eg if we want only certain hosts to connect to the firewall for management we can allow that and then follow it with a rule to drop everything else – logging this allows us to see attempted access to the firewall.

In terms of performance, the position of the rules will have some impact but it is not nearly as critical as that of the packet filtering router ie the Checkpoint Firewall match's the initial communication of a session against the rule base and once established, the session is added to the connection table which subsequent packets are checked against as opposed to the packet filtering router in which all packets are matched against an acl. For this reason we will group rules together logically for ease of Maintenance but we will put the www access rules to the top of the rule base as this is likely to be utilized the most.

4. The 1st Rule we create is the stealth rule which restricts access to the Firewall itself – we select the management network as the source, the firewall as the destination and CPMI / ssh as the services – CPMI is the service the Checkpoint GUI Clients use to connect to the Management Server – ssh is used to logon to the firewall itself for troubleshooting tasks etc eg to run tcpdump - all other traffic to the firewall will be dropped as per rule 2 ie

	Firewall Management (Rules 1-2)								
1	GIAC_Internal_Mgmt_Net	abbadon	*	TCP ssh_vers TCP CPMI	accept	Log	*	*	Allow management of the Firewall from restricted Management Network
2	* Any	abbadon	*	* Any	drop	Log	*	*	Drop all other traffic to the Firewall and log

5. Next we add WWW Access Rules – Rule 3 allows users on the Internet access to our Inbound Proxy Server (Note: Source is X GIAC_Internal_Network which means Not GIAC Internal Network – this is done by negating the cell)
   Rule 5 allows the inbound proxy server access to the Web Servers which it requires to pass on requests.
   Rule 4 allows GIAC Internal Employees Internet access via the Outbound Proxy Server. Notice that a new service named giac_http is defined which is http on an alternative port other that port 80.
   Rule 6 allows Outbound Proxy Servers http/https/ftp access to the Internet.



WWW Access (+ftp) (Rules 3-6)									
3	GIAC_Internal_Network	Inbound_Proxy_Serve	*	TCP http TCP https	accept	Log	*	*	Customer/Partner/Supplier access to Web Servers via Inbound (Reverse-proxy) Proxy Servers for Order/Supply Processing
4	GIAC_Internal_Network	Outbound_Proxy_Ser	*	TCP giac_http TCP https TCP ftp	accept	Log	*	*	Internal Employee www/ftp access via proxy server - note: non-standard port used for http (giac-http)
5	Inbound_Proxy_Servers	Web_Services_Rail	*	TCP http TCP https	accept	Log	*	*	Allow http / https to Web Servers
6	Outbound_Proxy_Servers	GIAC_Internal_Networ GIAC_DMZ_Networks	*	TCP http TCP https TCP ftp	accept	Log	*	*	Allow http (on standard port) / https to Internet

Tip1: The source object or destination object can be dragged from the list of objects to the rule where its required.

Tip2: The Source/Destination can be Negated (meaning anything except the listed object) by Selecting RMB / Negate Cell option while placing the mouse over the cell

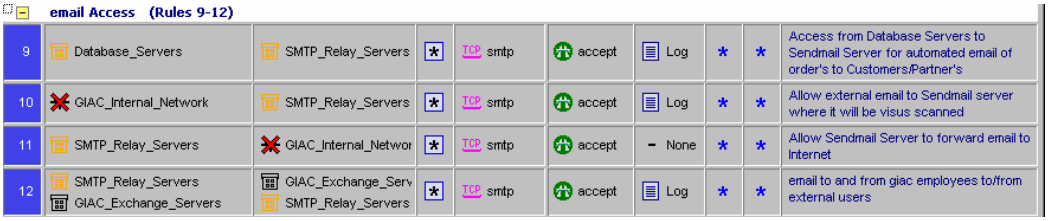
Tip3: Rules can be changed around by selecting the rule and dragging it to the required position

Tip4: Select a service, right click and select “Where used” to get a list of rules that uses this service.

6. Next, create the Database Access Rules – Rule 7 allows Web Servers to execute sql scripts to the backend database for order processing.
Rule 8 allows Internal GIAC Employess to access the Database Servers using applications that execute sql queries/updates.

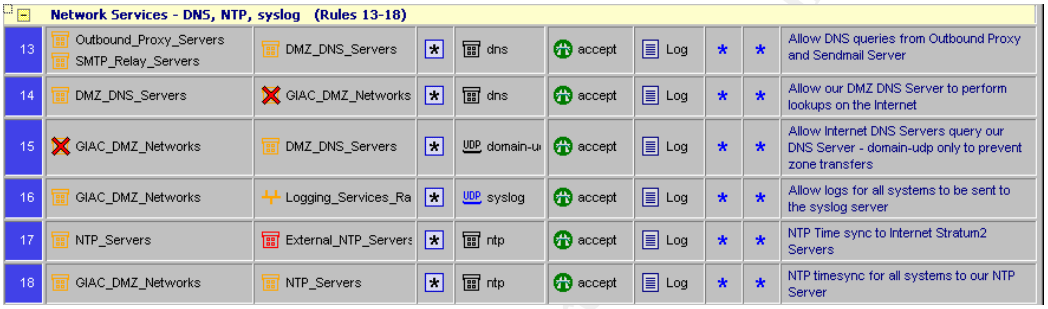
Database Access (Rules 7-8)									
7	Web_Services_Rail	Database_Servers	*	mysql	accept	Log	*	*	Web Server access to Backend sql database for query's/updates for Order processing
8	GIAC_Internal_Networks	Database_Servers	*	mysql	accept	Log	*	*	GIAC employees access to sql database for query's/updates for Order processing

7. Next create email access rules. Rule 9 allows Database Servers that execute stored procedures to email orders to Customers and Partners. Rule 10 allows external users including Suppliers to send email to the GIAC SMTP mail server where it is virus scanned. Rule 11 allows outbound email from the SMTP Server to the Internet and Rule 12 allows email in both directions between the SMTP Mail Relay and the GIAC Internal Exchange Server.



email Access (Rules 9-12)									
9	Database_Servers	SMTP_Relay_Servers	*	TCP smtp	accept	Log	*	*	Access from Database Servers to Sendmail Server for automated email of order's to Customers/Partner's
10	GIAC_Internal_Network	SMTP_Relay_Servers	*	TCP smtp	accept	Log	*	*	Allow external email to Sendmail server where it will be visus scanned
11	SMTP_Relay_Servers	GIAC_Internal_Networ	*	TCP smtp	accept	None	*	*	Allow Sendmail Server to forward email to Internet
12	SMTP_Relay_Servers GIAC_Exchange_Servers	GIAC_Exchange_Serv SMTP_Relay_Servers	*	TCP smtp	accept	Log	*	*	email to and from giac employees to/from external users

8. Next, create Network Services – DNS, NTP and syslog. Rule 13 allows DNS queries from the Outbound Proxy Server and Sendmail Server. Rule 14 allows our external DNS Server to perform DNS Lookups on the Internet. Rule 15 allows the Internet DNS Servers to query our external DNS Server but only on domain-udp so that zone transfers cannot occur. Rule 16 Allows logs from all systems to be forwarded to the syslog server. Rule 17 allows the NTP Server to sync up with a Stratum 2 Server which we have selected and received authorization from the owner to use – Rule 18 in turn allows all devices on our DMZ Networks to sync time from GIAC NTP Server



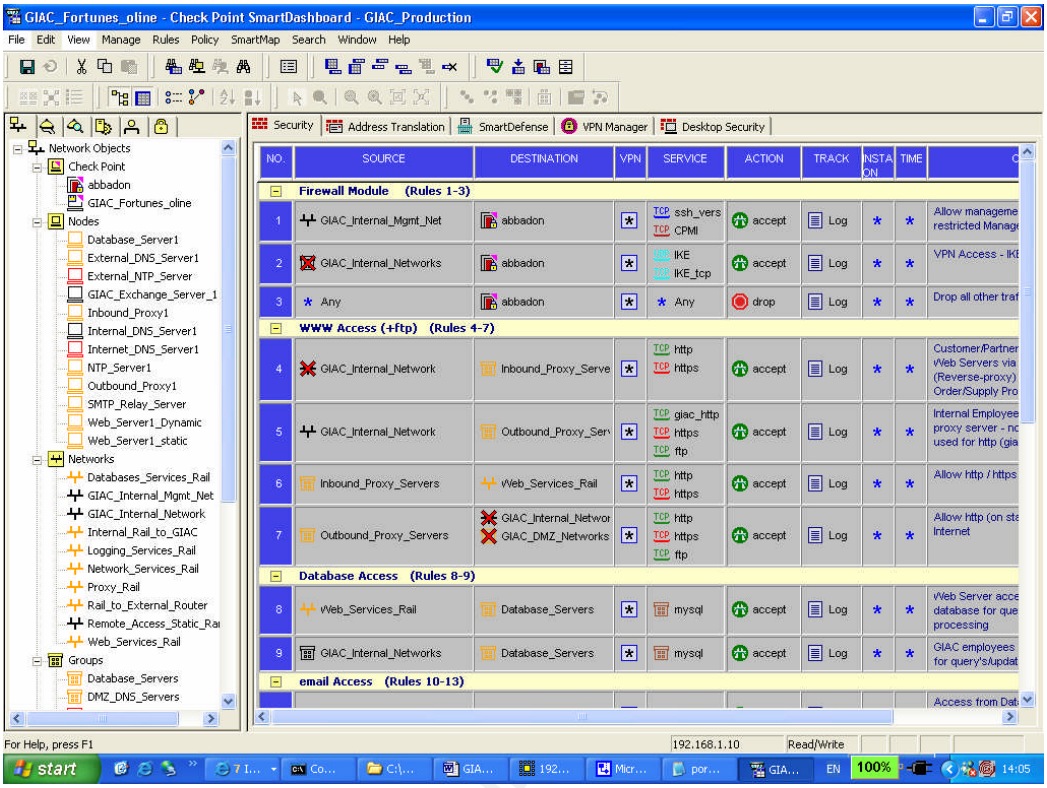
Network Services - DNS, NTP, syslog (Rules 13-18)									
13	Outbound_Proxy_Servers SMTP_Relay_Servers	DMZ_DNS_Servers	*	dns	accept	Log	*	*	Allow DNS queries from Outbound Proxy and Sendmail Server
14	DMZ_DNS_Servers	GIAC_DMZ_Networks	*	dns	accept	Log	*	*	Allow our DMZ DNS Server to perform lookups on the Internet
15	GIAC_DMZ_Networks	DMZ_DNS_Servers	*	UDP domain-u	accept	Log	*	*	Allow Internet DNS Servers query our DNS Server - domain-udp only to prevent zone transfers
16	GIAC_DMZ_Networks	Logging_Services_Ra	*	UDP syslog	accept	Log	*	*	Allow logs for all systems to be sent to the syslog server
17	NTP_Servers	External_NTP_Servers	*	ntp	accept	Log	*	*	NTP Time sync to Internet Stratum2 Servers
18	GIAC_DMZ_Networks	NTP_Servers	*	ntp	accept	Log	*	*	NTP timesync for all systems to our NTP Server

Note: Another Rule is required above to allow DNS queries from our Internal DNS Server to our external DNS Server to resolve Internet host IP Addresses. We found this in our auditing/testing and will apply it as part of the installation.

9. Next create a rule to allow management of the systems in the DMZ – Rule 21 allows ssh access to all Networks in the DMZ. Ssh can be used not only to connect to the device but also to upload files securely.

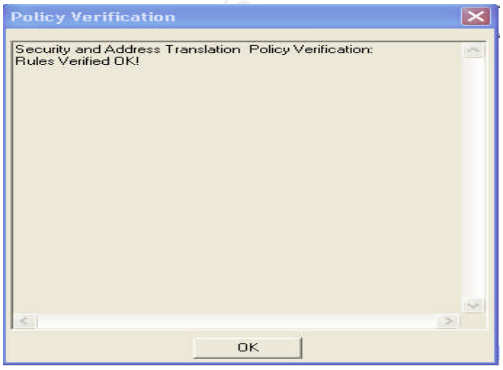
DMZ Network / Server Management (Rule 21)									
21	GIAC_Internal_Network	GIAC_DMZ_Networks	*	TCP ssh_vers TCP ssh	accept	Log	*	*	Allow login to dmz systems via ssh for management

10. The completed Rulebase (truncated) looks as follows ;



11. Once the policy is completed it should be verified for inconsistencies and installed. This can be done by selecting Policy/Verify and Policy/Install from the menu or clicking the icons on the toolbar

Note: The policy cannot be installed until successfully verified as shown below ;



12. Test Connectivity …

VPN Configuration

We are using the Checkpoint Firewall as a Remote Access VPN for GIAC Employees. GIAC Employees will access GIAC's Internal Network using Checkpoints SecureClient VPN – before configuring the VPN a number of decisions are required in terms of how users will be managed and how they will be authenticated to gain access. The required IPSEC Parameters for Encryption Algorithm, Data Integrity and IKE also need to be finalized.

For GIAC's implementation we are recommending managing the users on the Checkpoint gateway and authenticating users using certificates generated by the Checkpoint gateway's Internal Certificate Authority.

The IPSEC Parameters recommended are as follows ;

Encryption algorithm : Use default of 3DES

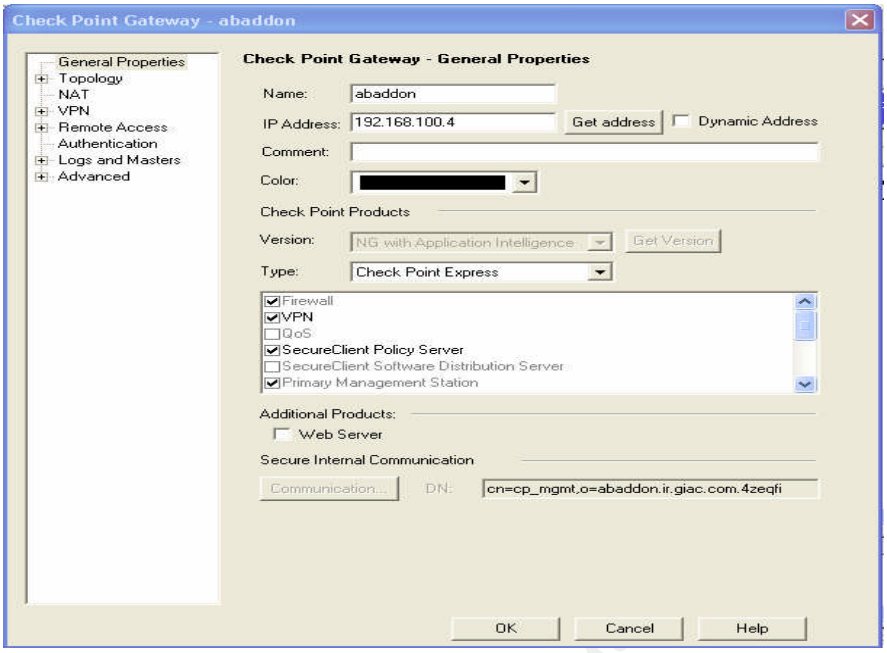
Data Integrity : Use default of SHA1

IKE Security Associations Properties : Use Default - Diffie Hellman Group 2 (1024 Bit)

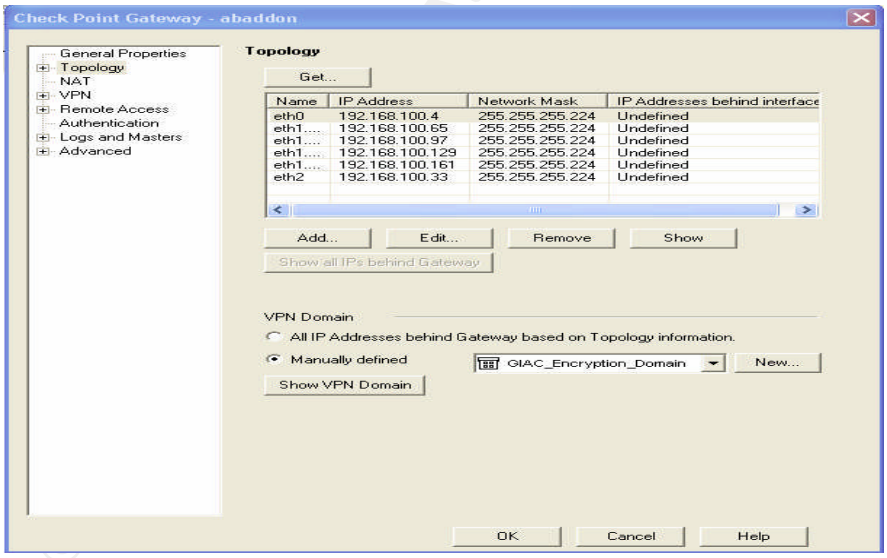
We will also allocate an Internal IP Address to Remote Access Users for traceability and equivalent network access to internal users.

The following configuration steps are required to configure the Checkpoint Firewall for Remote Access VPN as per guidelines above …

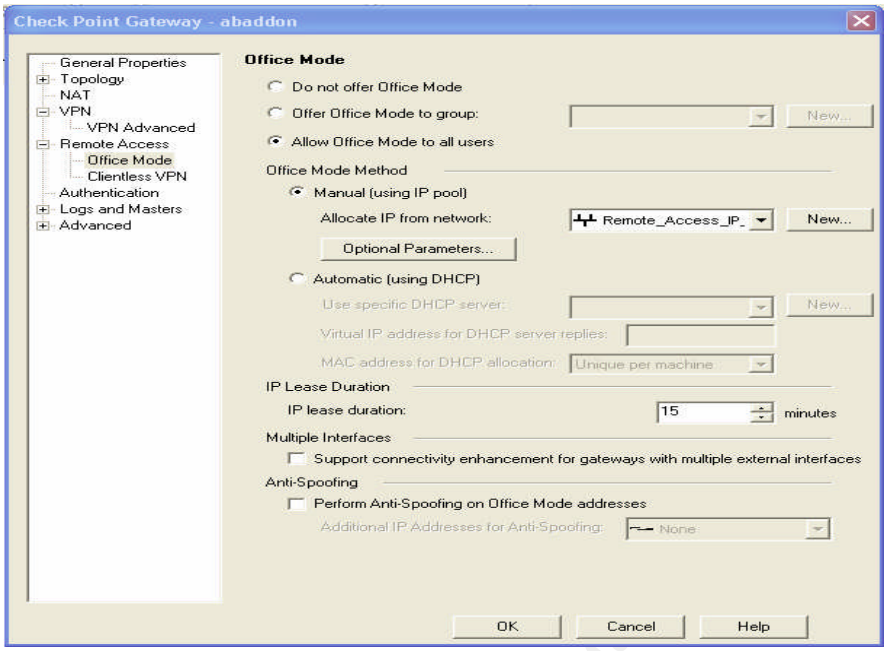
1. Firstly configure the VPN parameters on the gateway itself – this is done by highlighting the firewall object itself which is abaddon in GIAC's case – Using RMB select edit to open the object general properties – the VPN checkbox must be selected for this gateway to support VPN connections as shown below .



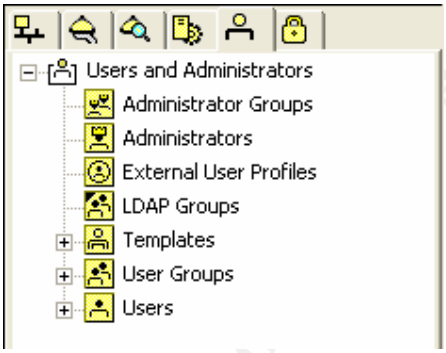
The next step is to define the encryption domain which is essentially any network that users will need to connect to – in GIAC's case we will define a group consisting of GIAC Internal Networks and DMZ Networks which Support personnel will need remote access to …



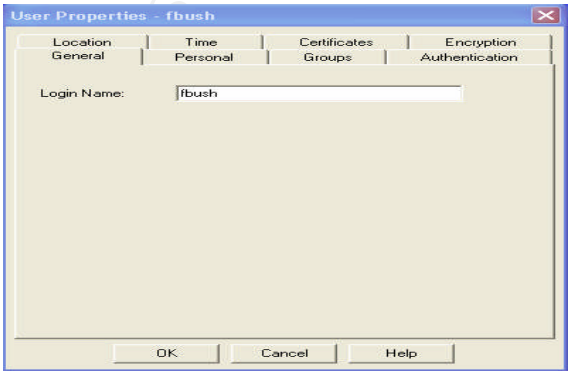
Next select Remote Access/Office Mode, Allow Office Mode with Office Mode Method Manual – Create an object for the GIAC Internal IP Address range that will be used for Remote access users and configure the vpn gateway to allocate IP Addresses from this range as shown below ;



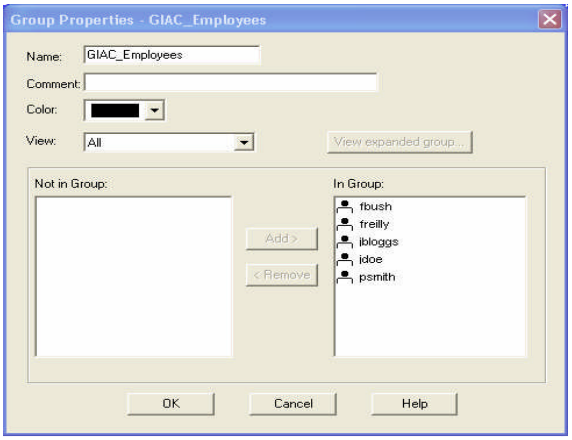
2. Next Create Users / Group by selecting New User / New Group from the Users Tab ie



Enter the login name on the general tab



Select all relevant users into the Group as shown below ;

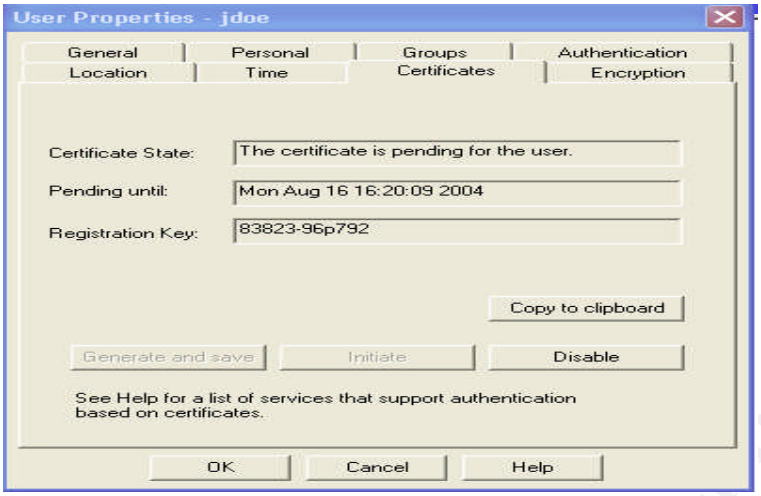


Use the Certificates Tab to initiate the certificate generation

Checkpoints NG AI R55 documentation, VPN-1, Chapter 11, VPN for Remote Clients, "Initiating Certificates for Users", Page 133 gives the following guidelines with regards to creating and transferring certificates ;

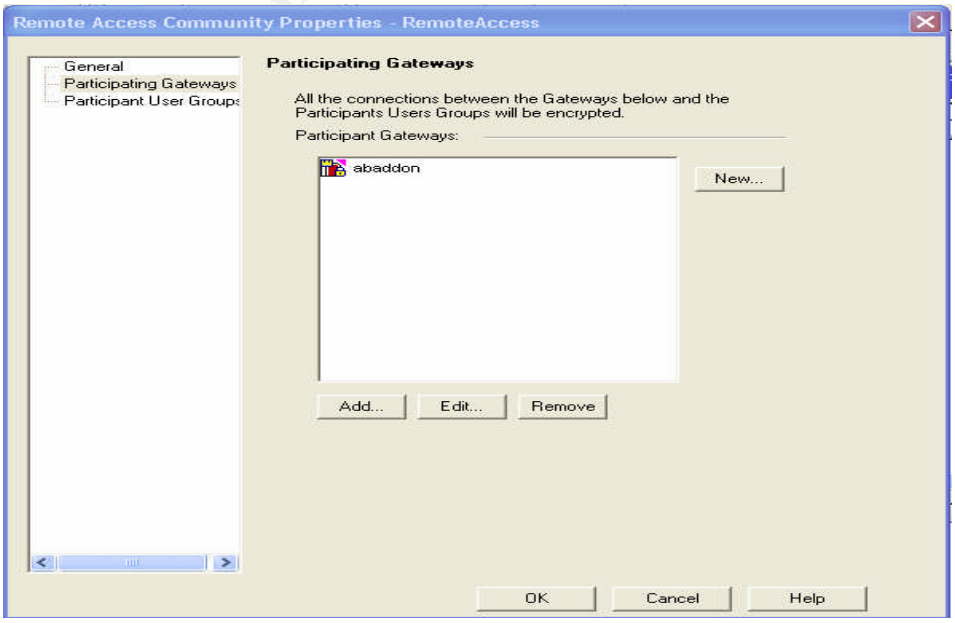
> User Certificate Creation Methods when Using the ICA
> Check Point's Internal Certificate Authority (ICA) offers two ways to create and transfer certificates to remote users:
> 1 The administrator generates a certificate in SmartCenter Server for the remote user, saves it to removable media and transfers it to the client out of band.
> 2 The administrator initiates the certificate process on the SmartCenter Server (or ICA management tool), and is given a registration key. The administrator transfers the registration key to the user "out of band". On receiving the registration key, the user inputs the key to his client. The client establishes an authenticated connection to the ICA (using the CMC protocol) and completes the certificate generation process. In this way:
> • Private keys are generated on the client
> • Hardware tokens can be used for certificates
> This method is especially suitable for geographically spaced-remote users.

With the amount of Sales personnel we have dispersed around the globe we will use the 2nd method which can be completed by the user using the specific registration key that is generated ie

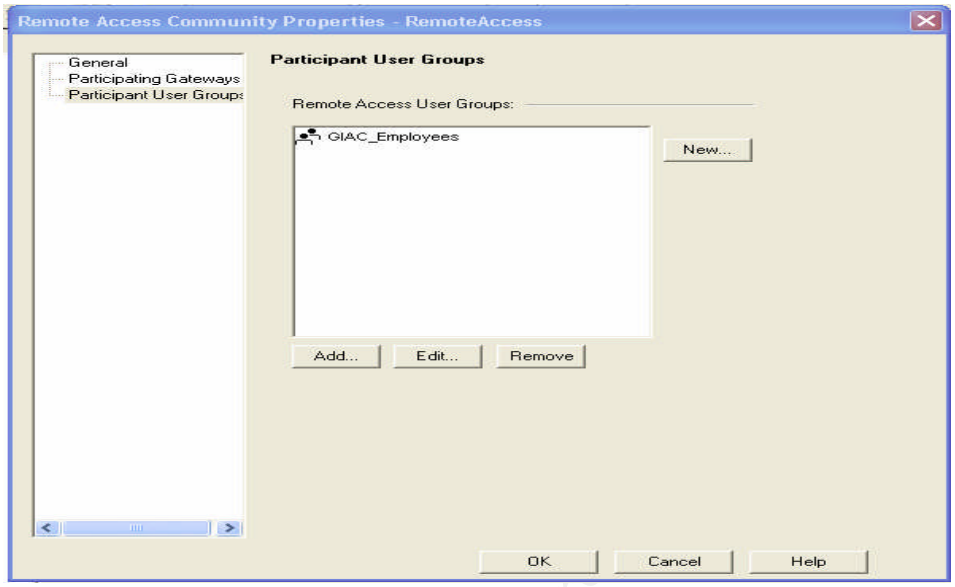


3. Define the VPN Community and its Particapants

   On the VPN Communities tree, double-click **Remote_Access_Community**. The Remote Access Community **Properties** window opens. On the Participating Gateways page, **Add**... Gateways participating in the Remote Access Community.

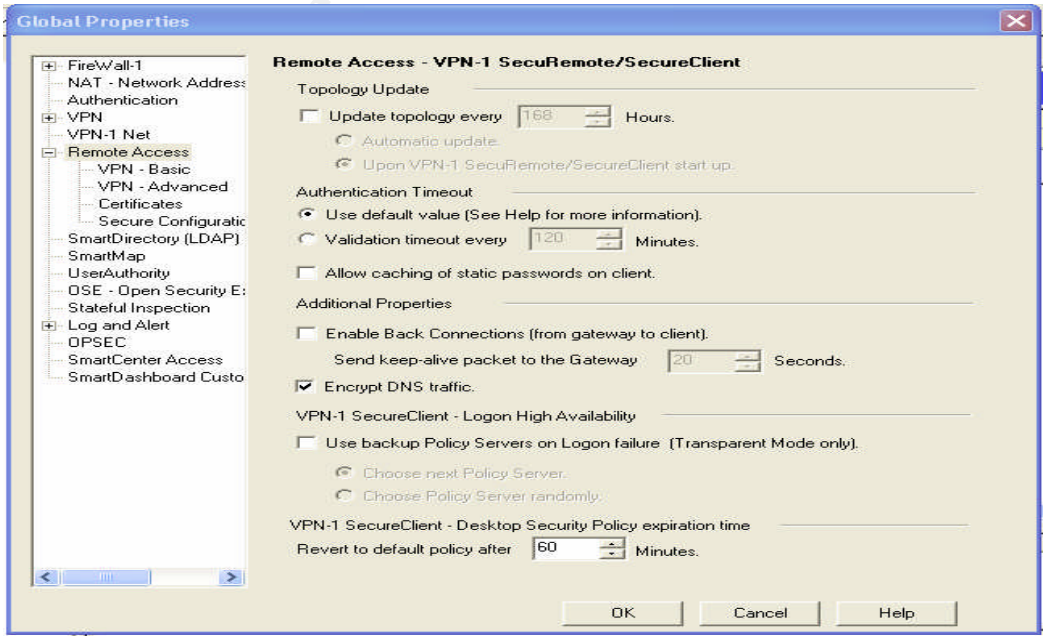


On the **Participating User Groups** page, **Add.**.. the group that contains the remote access users.

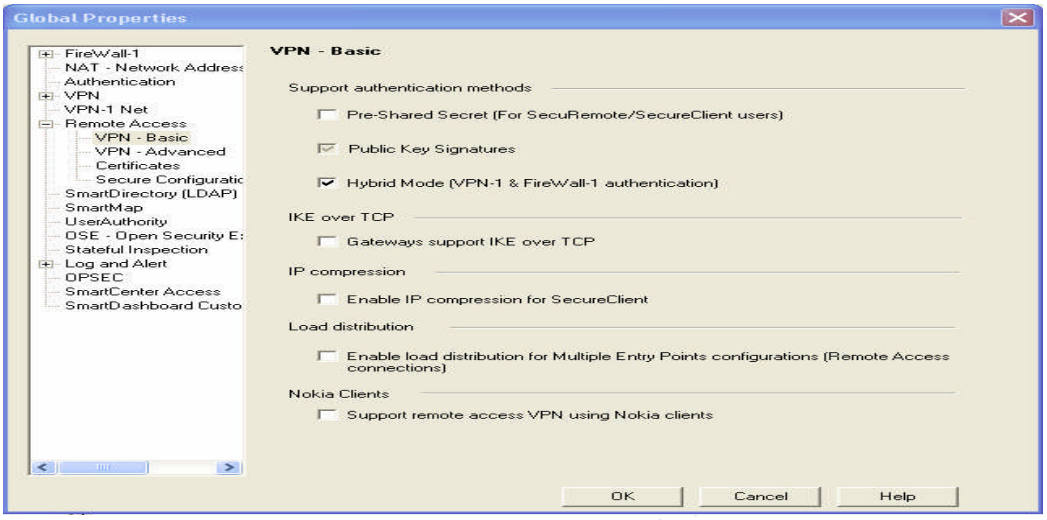


4. Configure Policy VPN Global Properties and add the Rule in the Rulebase to allow Remote Access Users VPN Access

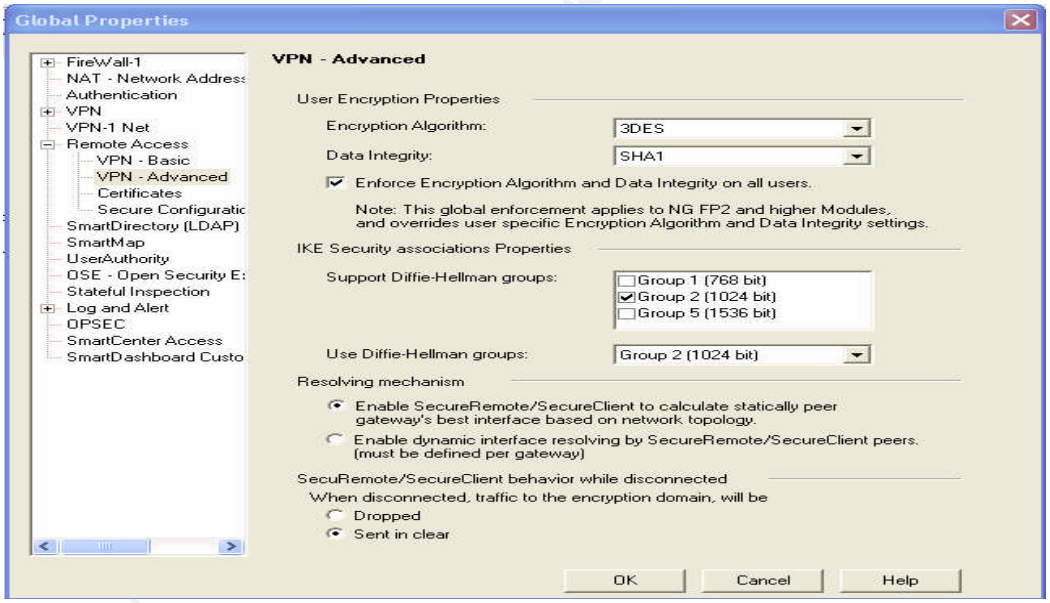
   Under Global Properties there are 4 sections pertaining to Remote Access VPN – Configure as follows. Under Remote Access, de-select high availability as we have only one gateway.



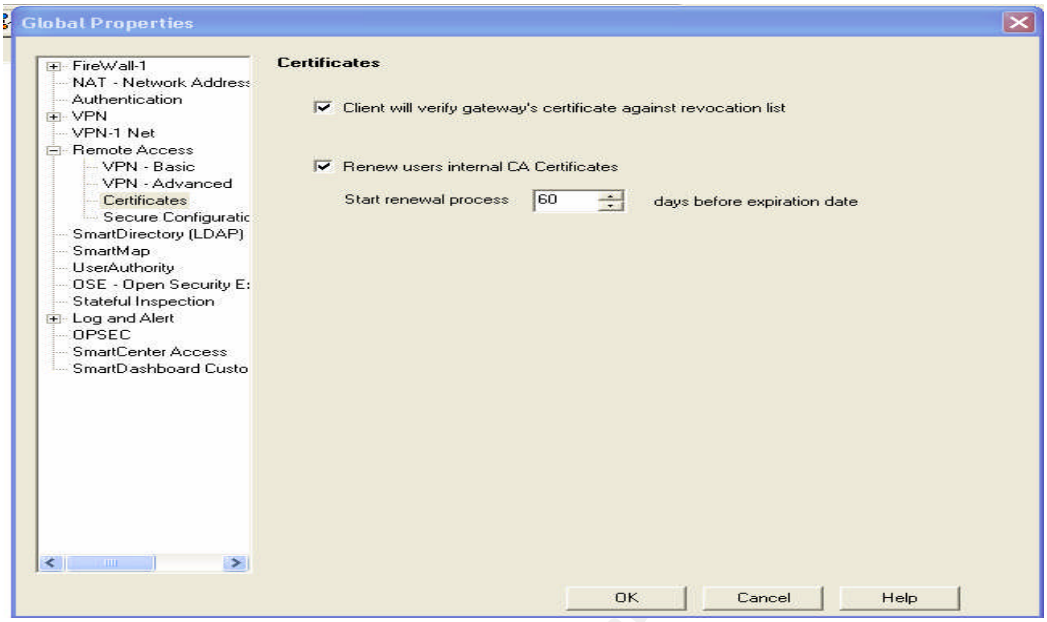
   Under VPN Basic leave defaults …



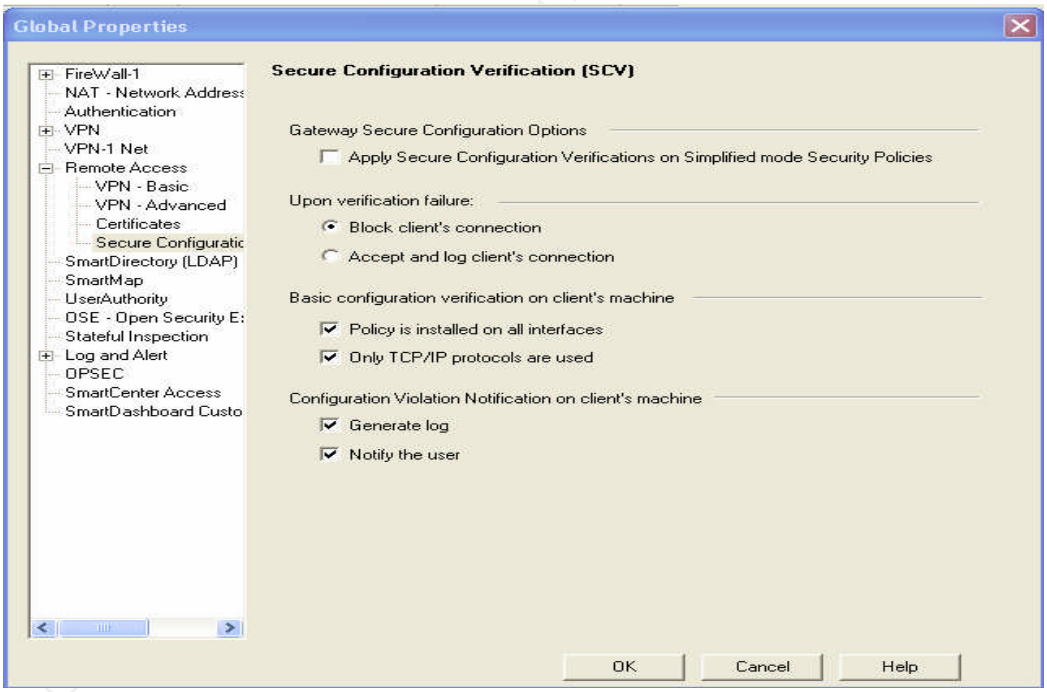
Under VPN Advanced leave as defaults ie Encryption Algorithm 3DES, Data Integrity SHA1 and Diffie-Hellman Group 2



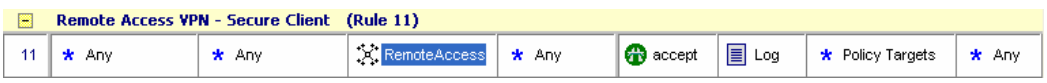
Under Certificates, leave as defaults ;



Under Secure Configuration Verification leave as defaults …

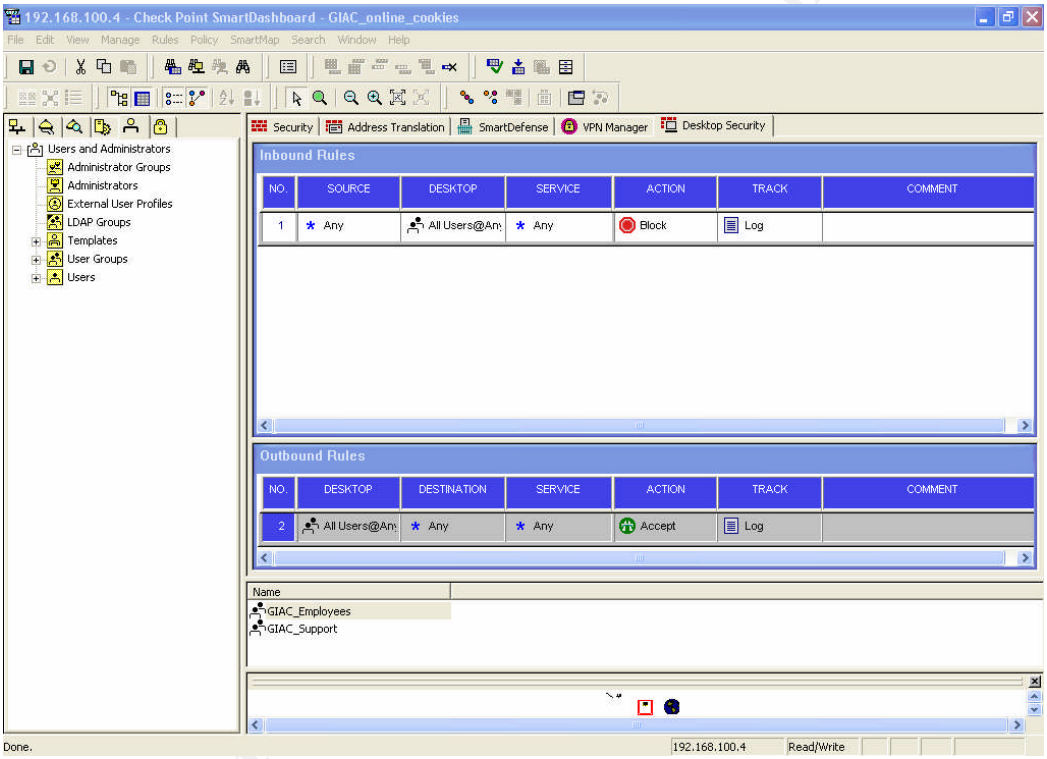


Add the following Rule to the Rulebase to allow Remote Users VPN Access



Initially we are allowing connectivity to all services as employee require access to multiple applications on GIAC Internal Networks. Specific applications/services can be specified for more granular control if required.

5. Configure Desktop Security to protect clients – the default rules will apply to all users – the inbound rule will block any attempt to connect to the laptop and the outbound rule allows the all users to connect to any service – more granular control can be applied at a later date if required …



6. Verify and install the policy by selecting the Policy/Verify and Policy/Install from the menu or clicking the icons on the toolbar

7. Test VPN Connectivity by running the SecureClient Application from the Internet

Squid Proxy Server Configuration

Outbound Proxy Server Configuration

The configuration of the Squid Proxy Server is done using the squid.conf file. For the outbound Proxy Server we will add the following entries ;

Squid.conf

```
http_port     8213
htcp_port     0
acl localnetwork src 192.168.0.0 /18
http_access allow localnetwork
```

We have changed the default port from TCP 3128 to TCP 8213 and only allowed access from our Internal Network range – this could be restricted further to specific client Subnets.

Inbound Proxy Server Configuration

Squid.conf

```
http_port     80
httpd_accel_host web_server
httpd_accel_port 80
htcp_port 0
http_access allow any

httpd_accel_with_proxy on
```

For the inbound Proxy Server the http port will be the standard http port ie TCP 80 – the proxy also uses Port 80 communication to the Web Server although this could be changed if required.

Assignment 3 – Design Under Fire

All is not well at Hackers Fortune Cookies an established and successful business that is starting to feel the affects of competition since the explosion of SANS Graduate's that have started up their online fortune cookie business's. One of the most successful is the GIAC Online Business run by Mr. Brian Rudzonis which is high on our list of targets and we will attempt to infiltrate their network/systems to gain confidential information that we can use to our advantage. Mr. Rudzonis's practical can be located at the following URL – his network diagram has been extracted and is shown below ;

http://www.giac.org/practical/GCFW/Brian_Rudzonis_GCFW.pdf

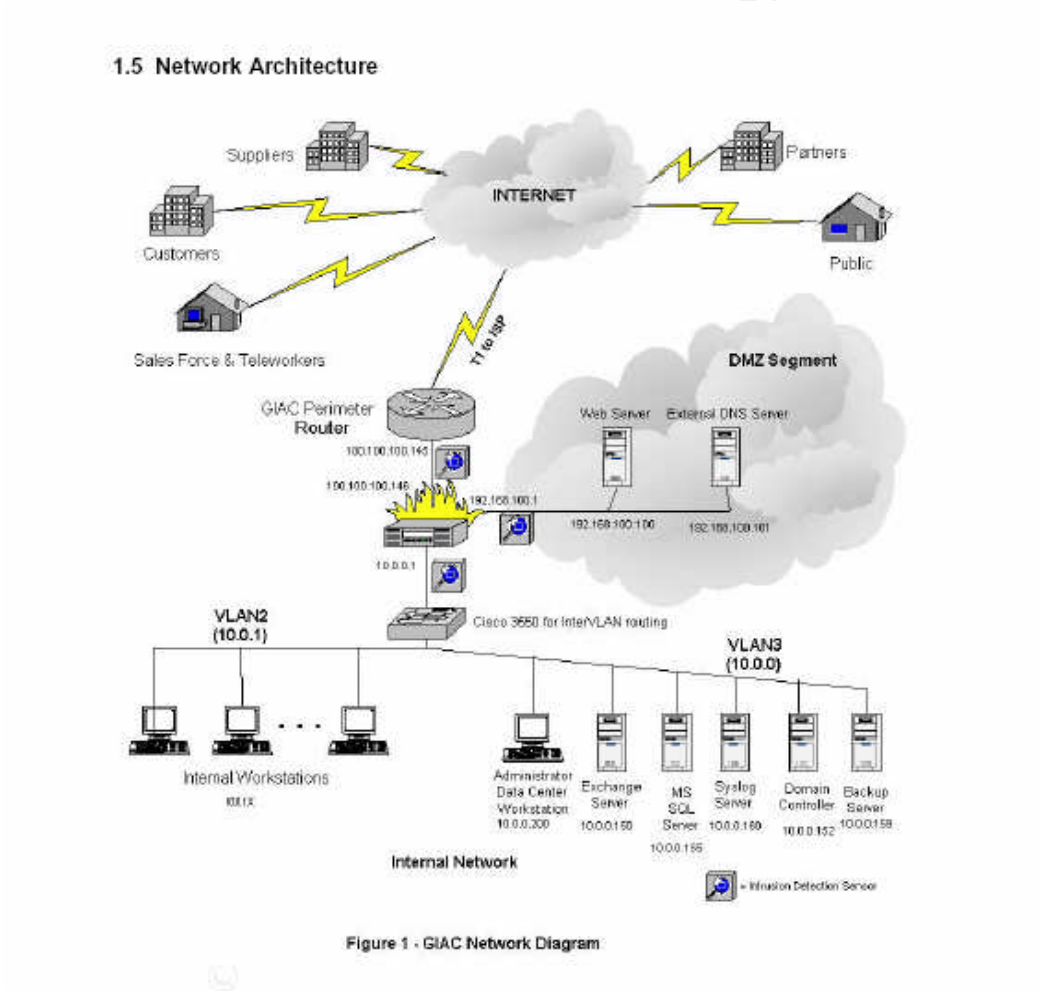


Figure 1 - GIAC Network Diagram

We will plan our attach in a number of stages as follows ;

- Perform Reconnaissance on GIAC Enterprises
- Scan the Network with Active or Passive Probing
- Attempt to Compromise an Internal System
- Retain Access to the system

Perform Reconnaissance on GIAC Enterprises

Initially we know very little about GIAC Enterprises so we need to perform reconnaissance – the best place to start is the InterNIC databases where we can get useful information such as Organization name, domain name, address and phone number etc. At this stage GIAC have no idea we are planning to attack them as we are not directing any traffic at the company itself.

Browse to the internic website http://www.internic.net and access the whois database – With Domain selected Enter giac.org and Submit the query – as there is no specific detail on the DNS configuration in Mr. Rudzonis's paper the record returned will give us the DNS Server(s) IP address's and if we are lucky may give us additional information such as phone number and clues to internal ip addressing – for the purposes of this assignment let us assume the following record is returned ;

G I A C (GIAC-DOM)
12345 Some Road,
Chinatown,
New York,
US

Domain Name: GIAC.COM
Administrative Contact : domain@giac.com

Domain Servers in listed order ;

NS1.GIAC.NET 100.100.100.162

We now have the Domain Server IP Address's – there is only one DNS Server listed – we can try the following dig command to get the BIND Version ie;

Dig @ns1.giac.net version.bind txt chaos

but it will not work for newer versions of BIND which GIAC is using.
We could also try to do a zone transfer to get internal network information as follows;

Hacker-system$ nslookup
Default Server: hacker-ns1.test.com
Address: a.b.c.d

- **server ns1.giac.net**

- **ls –d giac.com > giac.txt**

Received 0 answers (0 records)

but this is not likely to succeed as the design document indicates that GIAC only allow DNS transfers over UDP Port 53. GIAC are not using an ISP DNS Server for redundancy – if they were or they do so in the future we could try performing a zone transfer on the ISP DNS Server instead as this would have a better chance to succeed.

We can also get the Mail Server IP Address from DNS by using the **set q=mx** option. According to Mr. Rudzonis's Assignment, the IP Address of the PIX is used as the MX Record as it is using PIX's Mailguard feature.

In order to discover GIAC Allocated IP Address space, we can perform another whois query on the ARIN database as GIAC is located in the US. We use the DNS Server Public IP Address as follows ;

whois 100.100.100.162 –h whois.arin.net

And we will retrieve the the relevant information which will look something like;

Netname: ISPX123-456
Netblock: 100.100.100.0 – 100.100.100.255

So far we have the following information ;

DNS Server = 100.100.100.162
Mail Server = 100.100.100.146
Web Server = 100.100.100.161

ISP Allocated Address Range = 100.100.100.0/24

Scan the Network with Active or Passive Probing

Okay, in the next stage we want to find out some more detailed information on the type of systems GIAC are using to run the business but we do not want to be traced by GIAC so we will use someone else to do our dirty work for us - http://uptime.netcraft.com is a website we can use to perform probes to GIAC Systems and generate a report which we can view. By simply typing www.giac.com and hitting return the probing will begin. Mr. Rudzonis does not mention changing OS fingerprints as a security measure so the OS and Web Server software returned should be accurate.
We now know that GIAC are using Windows 2003 with IIS6.0 - As vulnerabilities are released and GIAC's Web Server(s) are patched we should be able to get a feel for how long it takes for GIAC to implement patches – that way if a suitable vulnerability is uncovered, we will know how long we have to strike.

We will initially scan the perimeter to access the level of security and access if a firewall is implemented – we will use nmap to perform the scan as follows ;

Nmap –sS –n –v –p 80 –P0 www.giac.com

Nmap –sA –n –v –p 80 –P0 www.giac.com

Depending on the responses we can determine if there is a firewall present ie if neither of the above probes returns a reset then we know there is a stateful firewall protecting the firewall. In GIAC's case we will not get any resets returned due to the implementation of the PIX. In terms of detection two single probes like the above should go un-noticed.

We will scan the systems that we know to determine if additional ports have been left open through mis-configuration etc – we can use nmap in paranoid mode to do this over a long period of time so that scan detection will be more difficult – we will only scan 500 ports to reduce the risk of detection – in case we are detected we will use other systems on the Internet that we have compromised – we will also try and determine the OS on the DNS Server and Mail Server. The nmap commands we will use are as follows ;

Nmap –sS –n –v –P0 –p 500 –TP 100.100.100.161 (Web Server)
Nmap –sS –n –v –P0 –O –p 500 –TP 100.100.100.146 (Mail Server)
Nmap –sS –n –v –P0 –O –p 500 –TP 100.100.100.162 (DNS Server)

Nmap –sU –n –v –P0 –p 500 –TP 100.100.100.161 (Web Server)
Nmap –sU –n –v –P0 –O –p 500 –TP 100.100.100.146 (Mail Server)
Nmap –sU –n –v –P0 –O –p 500 –TP 100.100.100.162 (DNS Server)

Where
-sS = TCP Syn stealth scan
-O = Operating System Detection using Fingerprinting
-n = No DNS resolution
-v = verbose
-p = ports
-P0 = No pings
-TP = Paranoid Mode – 15 minutes between scans

If GIAC have implemented their Network as described in Mr. Rudzonis's design then only the following ports will be open ie

Web Server – TCP 80/443
DNS Server – UDP 53
Mail Server – TCP 25

These ports will be detected by either the Port Scans or the general reconnaissance carried out earlier – see access specified in Appendix B Firewall/VPN Configuration of Mr. Rudzonis's assignment ie

access-list frominternet permit tcp any host 100.100.100.161 eq http
access-list frominternet permit tcp any host 100.100.100.161 eq ssl
access-list frominternet permit udp any host 100.100.100.162 eq dns

access-list frominternet permit tcp any host 100.100.100.163 eq smtp

Compromise an Internal System

The most obvious point of attach for online companies is through the Web Server which will or at least should be closely guarded and monitored system. A compromise of the Web Server can be used as a stepping stone to a backend sql database server which hosts a lot of critical data for the business operations. A lot of sites that use a Microsoft Web Servers will use a Microsoft SQL Database so vulnerabilities in IIS / ASP which is used extensively to develop Database Applications is an option – a search on the Internet for IIS/ASP vulnerabilities can be used as a starting point – advisory's from companies such as eEye Security Digital Security are an example ie http://www.eeye.com/html/research/Advisories/AD20020410.html - see details in appendix - which outline technical details of the issue can be used to develop exploit code. eEye's products can be used to defend such vulnerabilities otherwise vendor patches are required.

Assuming that we can determine the OS / Application running on the SMTP Server is Windows 2003/ Exchange 2003 then the Exchange Server is a very attractive target as traffic is allowed to and from the Internet. Also if we compromised the Exchange Server we would have network access to all of the critical Servers ie Domain Server, Database Server etc. We have searched for any Exchange SMTP vulnerabilities and we found some older ones that Microsoft have released patch's for ie

http://www.microsoft.com/technet/security/bulletin/MS02-037.mspx
http://www.microsoft.com/technet/security/bulletin/MS03-046.mspx

Both of these are fairly difficult to craft attacks for and we could not find any exploit code available from the http://packetstormsecurity.org website. In any case even if we there was this vulnerability is resolved in newer versions of exchange so it probably would not succeed, although its not unknown for old vulnerabilities that were resolved to re-appear in new versions of software so its always worth a try. We will also be on the lookout for any new vulnerabilities that may arise that we can use.

In the meantime its time for a different approach using some social engineering– we work with some of the same partners as GIAC – we have a visit scheduled from one of the Partners who will be visiting GIAC after calling to us as part of a country wide tour – he divulged this information to me after I insisted that he spend more time at Hackers fortune cookies to help us sort out some delivery issues but he assured me he would be contactable at all times via email while at GIAC – like a lot of companies, visitors can plug in to the local network at GIAC, get a DHCP Address and access the company's IT resources to get Internet Access etc.

So, the plan is while he is here in Hacker's fortune cookies we will add some Trojan software to his Labtop so that we will be able to connect to his Laptop through a back door – we will install cryptocat which is an SSL'ized version of ncat – cryptocat will tunnel traffic through HTTPS to a compromised server on the Internet which will allow us to access a command shell – we can test it while he is at Hackers fortune cookie's so that chances of success will be high – while he is at GIAC we will use his laptop to execute scans and compromise additional systems. If these scans are detected, our friendly Partner Sales rep will come under scrutiny – however because of the placement of GIAC's IDS systems, any scanning of the Internal Workstations from a system on the local Subnet (where our Partner Sales person will be connected) or scanning of the Critical Servers on the Internal Server Subnet will not be detected by any of the IDS systems.

Once our friendly Partner Sales Person is in GIAC we will use our backdoor command shell to access GIAC's Network – now that we are connected internally it is much easier – we can use a range of tools to compromise one of GIAC's Laptops or Desktop machines – we can perform port scans to look for open shares, perform sniffing with tools such as dsniff to get user account names which we can attempt to crack with programs such as John the Ripper – its only a matter of time. Once we gain access to one of the Internal systems we will need to install a root kit – as it's a Windows based environment we can install telnet like tools that we can gain access to the system using a password which we have setup so that other hackers don't have access ie iCMD , Tini , RemoteNC or WinShell are examples of tools resembling Telnet.

Reference the following article for more detail …

http://www.windowsecurity.com/articles/Hidden_Backdoors_Trojan_Horses_and_Rootkit_Tools_in_a_Windows_Environment.html

After installation of our tools we will be able to return to our internal system so that we can compromise the Internal Critical Servers over time by sniffing for usernames, cracking passwords, logging on and escalating privileges etc.

Improvements/ Countermeasures to Attack

Overall Mr. Rudzonis's design is quite comprehensive and appropriate for the size of GIAC's business operation. However, all designs can be improved and policy's implemented to reduce risks.

The 1st weakness we identified was that Mail was allowed from the Internet to GIAC's most critical Internal Network ie the Server Network which has the Domain Controller and the Database Server – the design does specify that the PIX Mailguard feature is used which includes stateful inspection of the SMTP Protocol which does help but what does that actually mean ? – from cisco's documentation it looks like SMTP is restricted to seven SMTP commands ie

```
!--- To enable the Mail Guard feature
!--- to accept only seven SMTP commands
!--- HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT:
!--- (This may be turned off to permit ESMTP by negating with
!--- the no fixup protocol smtp 25 command):
```

This may be sufficient but if a vulnerability is uncovered that uses the standard commands then the PIX may not catch it – also some security implementations of stateful inspection have proven trivial to break in the past (eg adding a space) so depending on the Firewall to provide this security to your internal critical network may be too risky.

A more robust and secure improvement would be to install a unix Sendmail SMTP Relay server in the DMZ. In this way two vulnerabilities on 2 different OS's/ Applications in the same timeframe would be required for hackers to compromise the perimeter through the mail servers/application.

A second improvement that was not covered in Mr. Rudzonis's assignment was how visitors to the site were handled in terms of access to the Network. One option is to enforce a policy that visitors cannot connect to the Local Network – this may not be realistic or will simply be eroded overtime due to business needs so measures are required – an isolated vlan network on the LAN, or better still on the Firewall if possible with strict access control (eg HTTP/HTTPS) using stateful filtering and Colour coded Telecom Outlets that visitors must attach are examples of measures that could be taken – further measures are to require authentication eg 802.1x before a user can access the network and guest users are assigned to a restricted access vlan – this would not eliminate the trojan on the compromised system working but access would be limited if the users system is compromised through some back door (we have no control over visitors systems in terms of patching etc) . Another improvement would be to install a proxy server for HTTP/HTTPS access eg squid – the proxy server port could be configured to a non standard port number so that Trojans using the standard ports will not work. Finally on this one, an IDS on the Internal Server Subnet would also be worth the investment – as security practices improve that stop the intruder hacking in from outside, there will be more emphasis on attacks from the inside through social engineering or other methods.

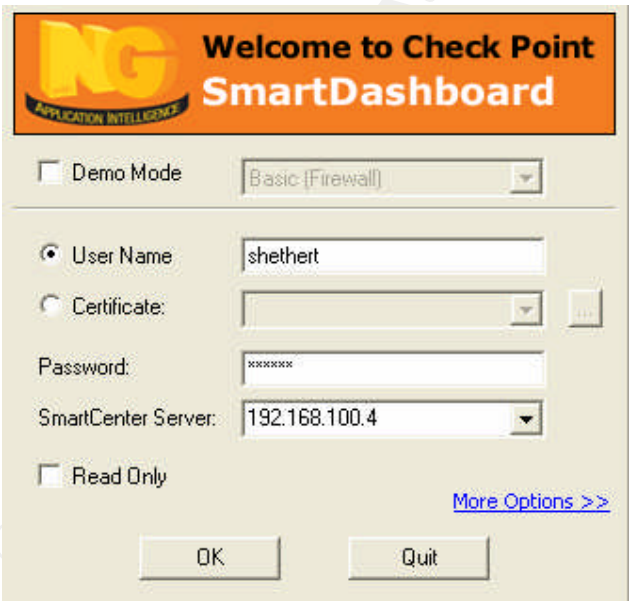
Assignment 4C – Work Procedure

The Firewall Policy will be maintained by a number of Support Personnel within GIAC – as the business grows and expands new servers and applications will be required to support the business – GIAC are very conscious of the need for detailed review, planning and approval of all changes to the Firewall policy to maintain a secure, high availability network for their Customers, Partners, Suppliers and Employees. To help avoid any human errors due to lack of training or familiarity we have been asked to provide GIAC with a work procedure to that will be used by operational personnel in the day-to-day maintenance of the Firewall Policy.

Connecting to the Firewall Management Server

Management of the Firewall is only allowed from a Windows Terminal Server on GIAC Internal Management Network . Once you connect to the WTS using your Windows Domain account, run the SmartDashboard application by selecting the Checkpoint GUI ie

Start/Programs/Checkpoint SmartConsole R55/SmartDashboard



Enter your username, password and IP Address of the GIAC Firewall which is also the SmartCenter Management Server.

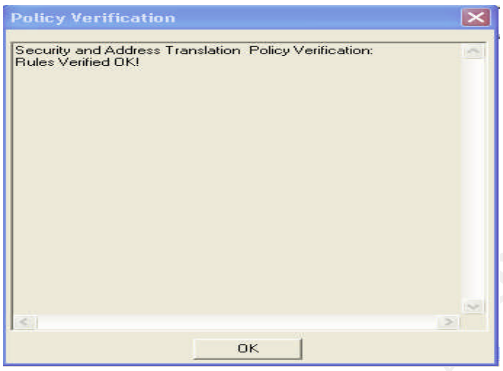
Note: You will need an account on the Firewall Management Server – If you do not have one then complete GIAC Account request form with associated justifications and management signatures …

Policy Installation

Once connected to the Firewall Management Server, changes to the policy should be verified and the policy installed after successful verification.

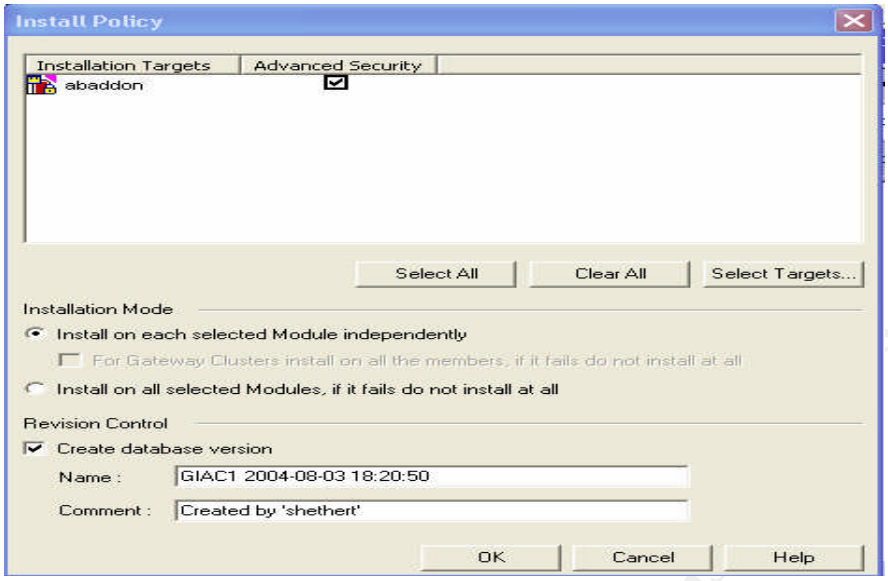
To verify the policy select Policy/Verify the menu or click the icons on the toolbar

Note: The policy cannot be installed until successfully verified as shown below ;

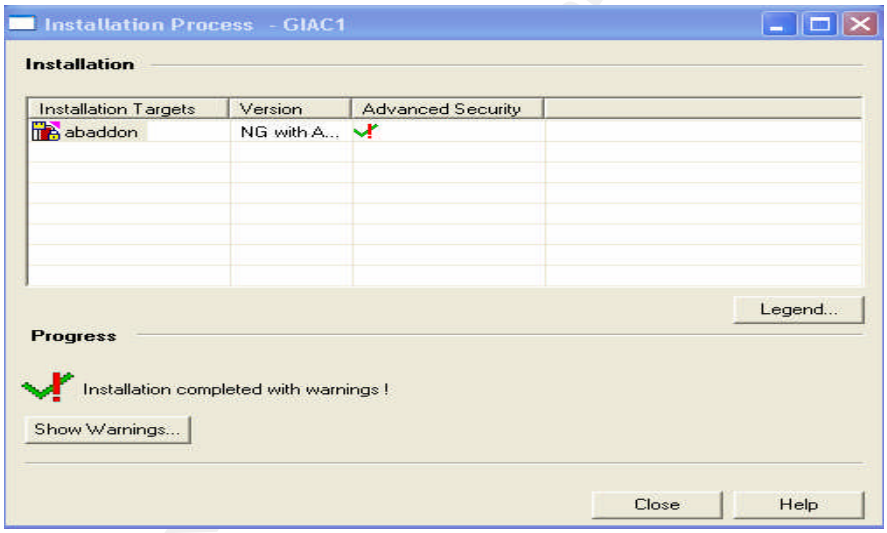


Once the policy is verified it should be installed - This can be done by selecting Policy/Install from the menu or clicking the icon on the toolbar

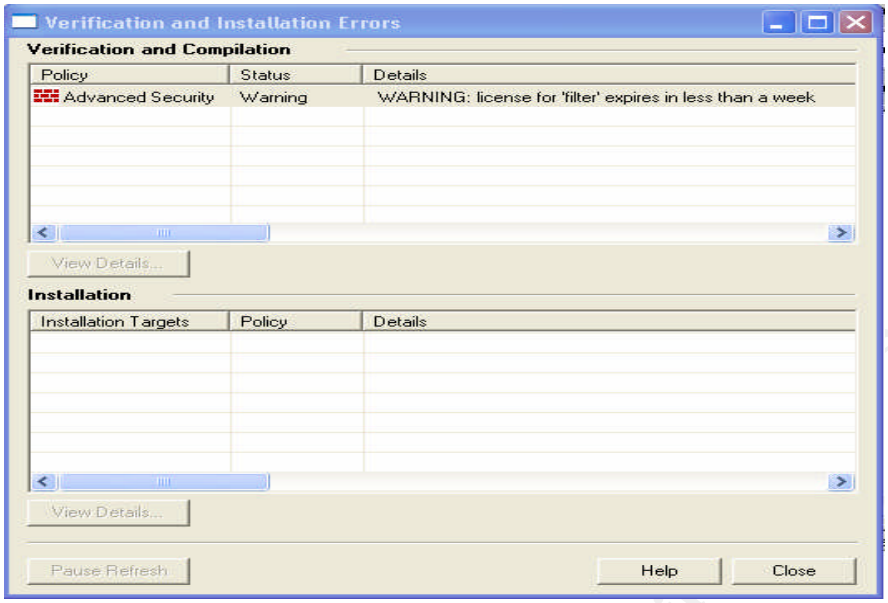
The Install Policy screen will appear as shown below – Click okay to continue ..



A new database version of the policy will be created – select OK to proceed with the installation process.

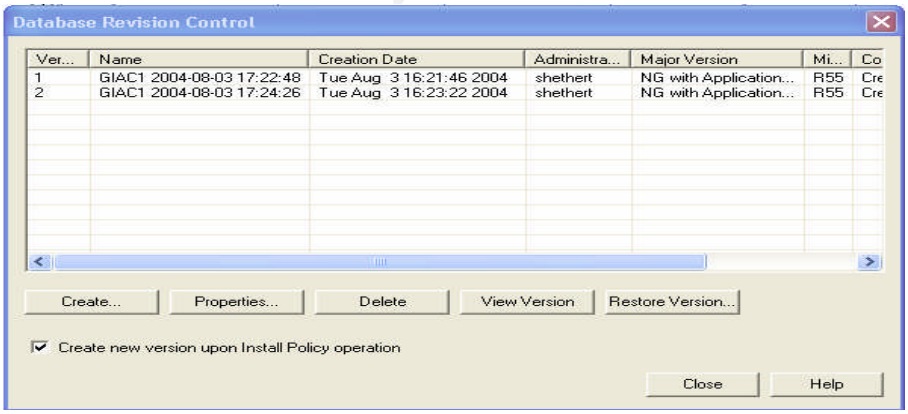


Any errors or warnings show be checked by pressing the “Show Warnings” button – in this case we are receiving a warning that our evaluation licence is about to expire which should not occur on a production system but there are numerous other errors that can be encountered which need to be resolved for policy installation …



Revision Control of Policy / Back-out Procedure

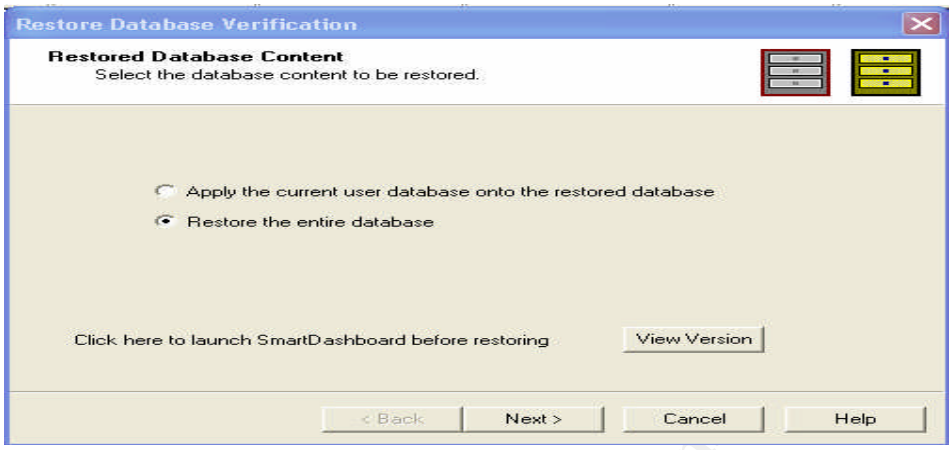
Checkpoint has a nice feature for implementing Revision control of the Firewall Policy. From the **File** Menu Select **Database Revision Control** . The **"Create new version upon Install Policy operation"** checkbox should be ticked so that a new version of the policy will be saved for each update/installation of new policies as shown below …

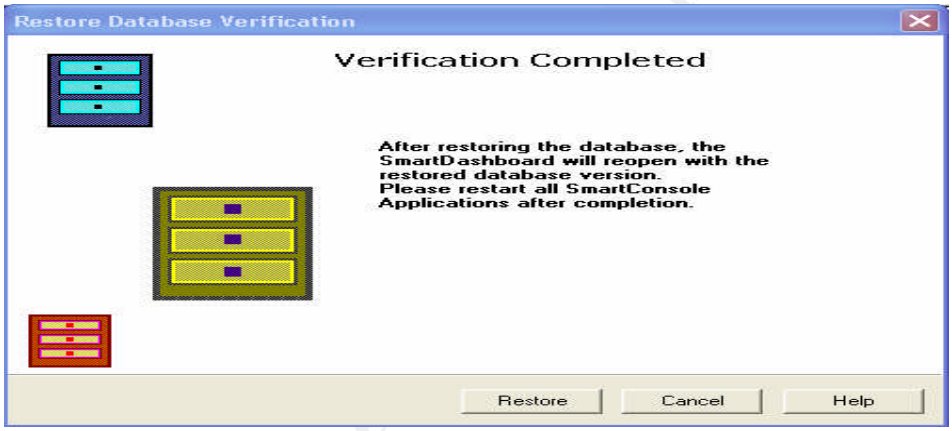


Note: The Administrator that installed the policy is shown so any issues can be directly attributed to individuals – we suggest that tracking of the installation is part of your daily operations review so that all policy installations are tracked and have required approvals.

In the event of an outage due to incorrect configuration etc the previous revision of the policy can be restored - Highlight the required version and select the **Restore Version** button – the Restore Database Verification

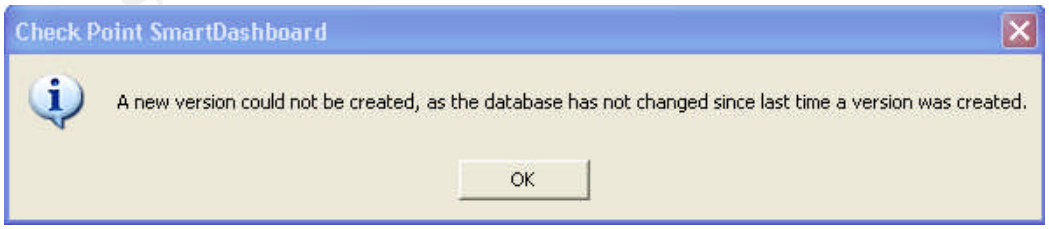
Content will open – Select **Restore the entire database** option so that everything is restored as it was before and select Next …

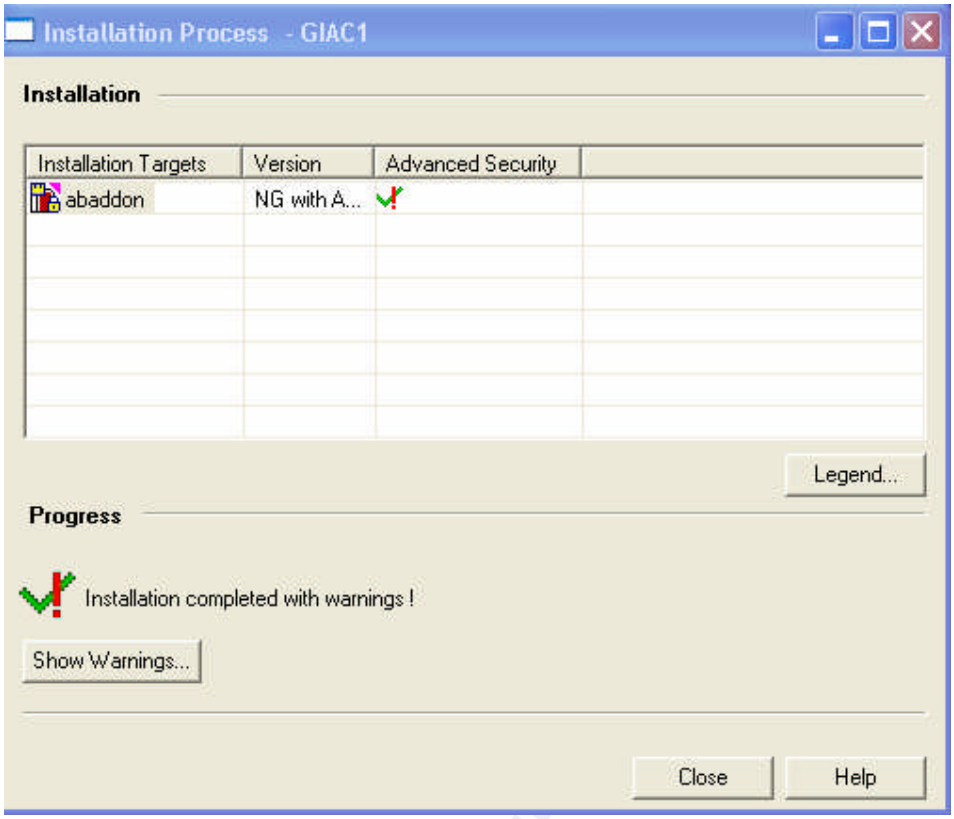




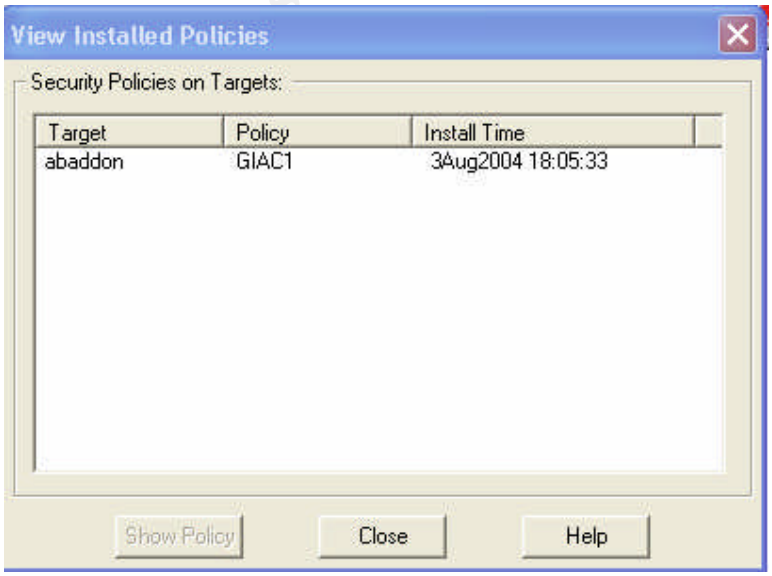
Smartdashboard will re-open with the required policy – Now install the policy as normal.

Note : A new version will not be created as it already exists and you will get the following message …



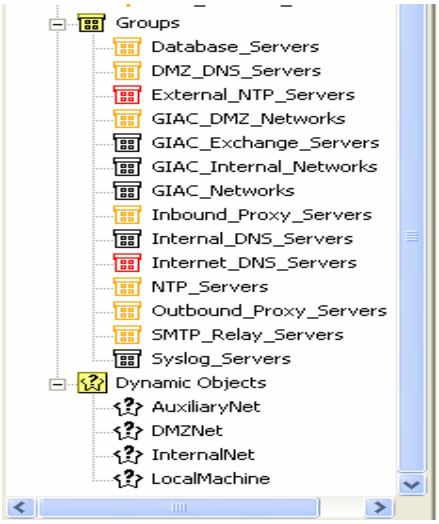


Note : One thing that can be confusing is if you check the installed version it will show the policy installed and the actual install time – there is no way to be sure what revision is actually installed without examining the policy itself – under normal operation, it will be the last revision that was created which is easy to correlate but if you restore a previous revision as in this case its something you need to be aware of – I would have expected to see the revision number in the screen below ;



Adding New Systems to the DMZ

To simplify some of the changes to the Firewall policy we have created groups for all of the existing Server types and Networks as shown below ;



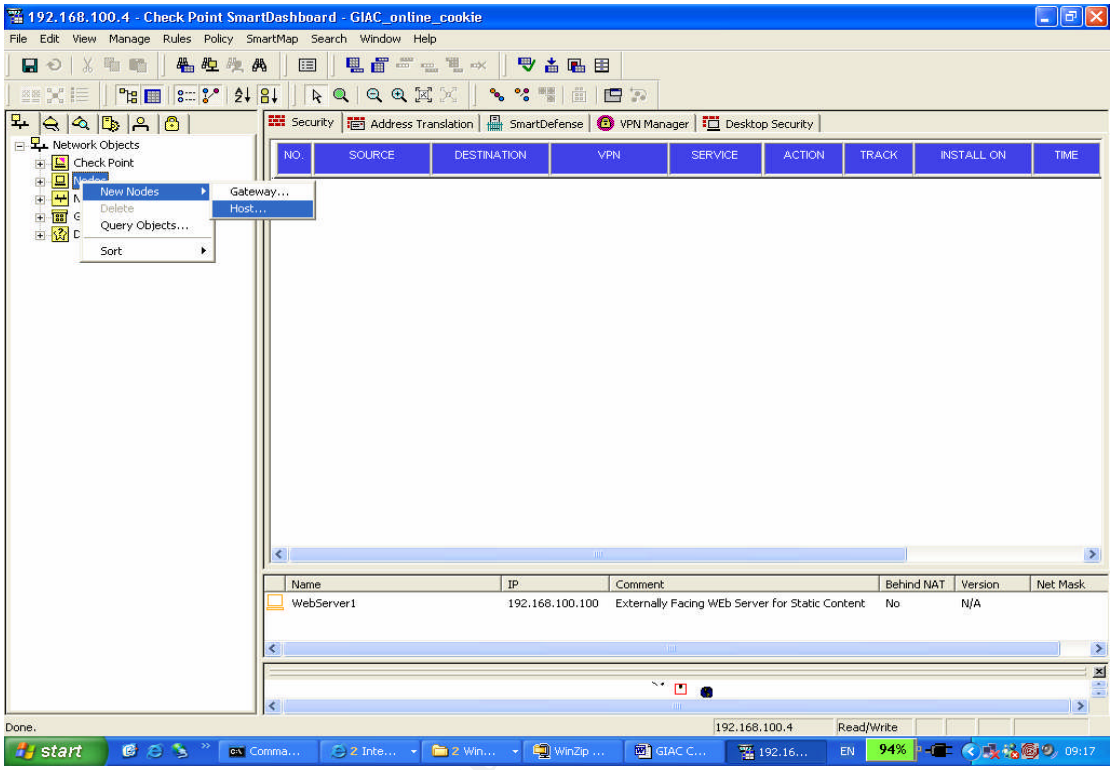
As an example if we wanted to add a new Web Server on the Web Services Rail, then the following steps should be taken;

1) Allocate an IP Address to the Web Server from the IP Address Tracking Sheet attached – for externally facing Servers also allocate an unassigned public IP address from the ISP allocated pool

GIAC_Address_Tracking.xls

2) Add the required entries into DNS

3) Logon to the Firewall and create/configure an object for the Web Server by selecting Nodes / New Nodes / Host as shown below ;

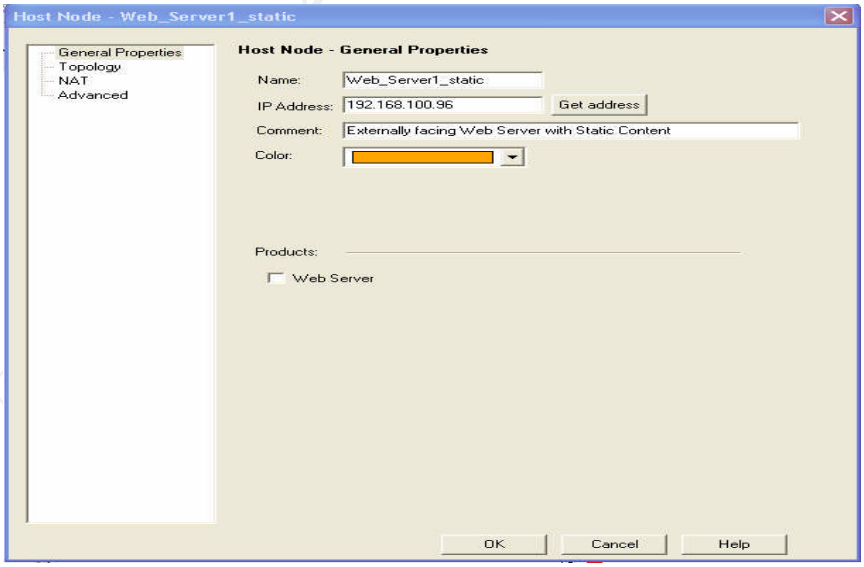


Enter the Name, IP Address, a comment and appropriate colour coding ie

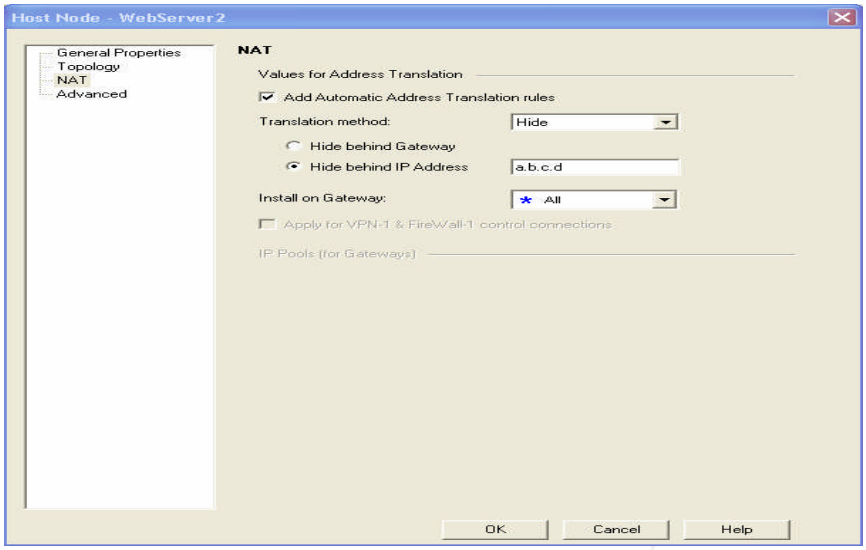
Internal Network = Black

External Network = Red

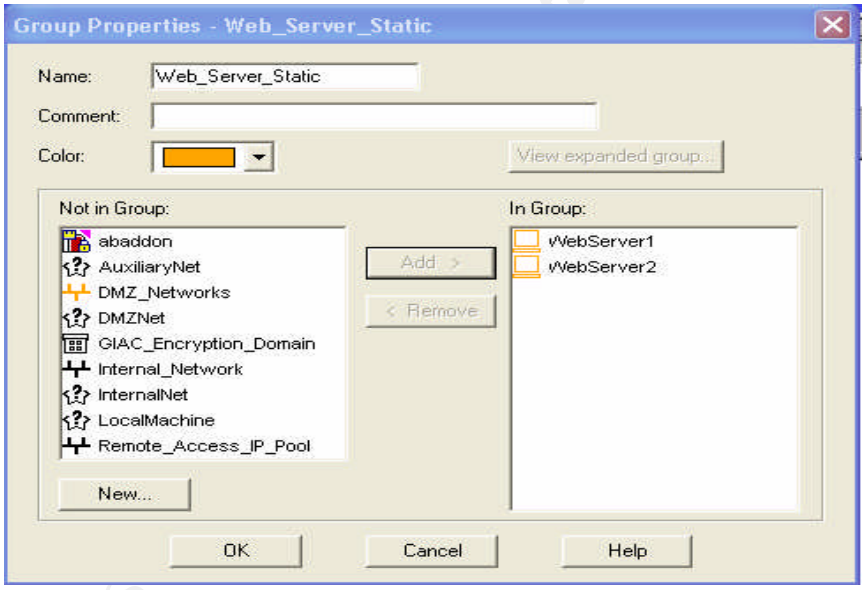
DMZ Network = Orange



For externally facing Servers such as a Web Server, you need to configure NAT for the object – Select Translation Method **"Hide behind IP Address"** and enter the IP Address.



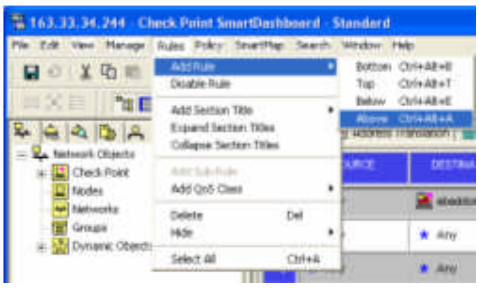
Add the new web Server to the Web Server Group



4) Install the Policy as described above

Addition of New Rules/Services

To insert a new rule in the rulebase, connect to the Firewall as described above, highlight on of the existing rules below where you want to insert the new rule and select Add rule, Above as shown below ;



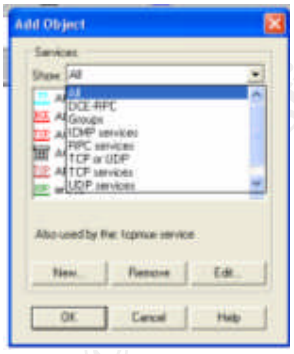
This will add a new rule - it will default to a Source, Destination and Service of Any and DROP – you now need to modify these as required.

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
2	* Any	* Any	Any Traffic	* Any	drop	- None	* Policy Targets	* Any

Everything in the Checkpoint is an object - The Source and Destination fields can be any Node, Network or Group that is already defined or a new one that you define – refer to Configuring the Policy on the Checkpoint Firewall for more detail.

TIP: You can LMB Click on the Any entry, Select Add and the list of available objects will be displayed so that you can select the object required or optionally create a new one – you can alternatively drag the object from the Network Objects pane on the left hand side of the Smartdashboard screen.

To add a service the procedure is similar – LMB Click on the Any entry in the Service section then RMB Click and the Add Object appears for services – the list of services can be narrowed down by selecting TCP, UDP etc as shown below ;



If the intention is to accept the traffic, change the Drop in the Action Column to Accept - the example rule below allows http traffic from a Test network to a test Web Server and traffic will be logged

2	test_net	Test_Web_Serv	Any Traffic	TCP http	accept	Log	* Polic	* Any	Test Rule

Appendix A – ISS Vulnerability / Advisory

http://www.eeye.com/html/Research/Advisories/AD20020410.html

Published Advisories

Windows 2000 and NT4 IIS .ASP Remote Buffer Overflow

Release Date:
April 10, 2002

Severity:
High

Vendor:
Microsoft

Systems Affected:
Microsoft Windows NT 4.0 Internet Information Services 4.0
Microsoft Windows 2000 Internet Information Services 5.0

Overview:
A vulnerability in the ASP (Active Server Pages) ISAPI filter, loaded by default on all NT4 and Windows 2000 server systems (running IIS), can be exploited to remotely execute code of an attackers choice. The fault lies within the decoding and interpretation of form data received by malicious clients. By chunk encoding form data we can force IIS to overwrite 4 bytes of arbitrary memory with data we supply.

This is a very serious vulnerability and eEye suggests that administrators install the Microsoft supplied patch as soon as possible.

The following example will show the vulnerable condition. We will use a default .asp page left after install on a Windows 2000 server with the latest service packs.

Technical Details:
Example:

```
**************Begin Session*****************
POST /iisstart.asp HTTP/1.1
Accept: */*
Host: eeye.com
Content-Type: application/x-www-form-urlencoded
Transfer-Encoding: chunked

10
PADPADPADPADPADP
4
DATA
4
DEST
0
[enter]
[enter]
**************End Session******************
```

Technical Description:

The example session above causes the default exception handler to execute from within the dllhost child process. When the default exception handler executes a window will open with this message:

DLLHOST.EXE - Application error

The instruction at 0x77fcb397 referenced memory at 0x54534544

Notice that 0x54534544 is the hex representation of "TSED", or the value "DEST" in little endian format. The DLLHOST.EXE process is trying to copy "DATA" to "DEST". Because there isn't writeable memory at 0x54534544, an access violation occurs and the structured exception handling (SEH) within the NT kernel catches it and kills the child dllhost.exe process.

The crux of this problem lies in the fact that the memory we overwrite with our data contains Heap Management header structures, in our case being used by AllocateHeap(). Specifically, as we overwrote the header, we control two four byte addresses within it. These addresses are associated with the population and use of lookaside lists. The first four-byte address, which in our example is overwritten by "DATA", is an address that gets copied to the second four-byte address specified in header. We have also overwritten the second address, this time with "DEST". By overwriting these two addresses, we can put four bytes anywhere in memory that the child dllhost.exe has privileges to write to. This allows us to overwrite function pointers, saved instruction pointers, exception handlers, or anything else that will allow us to control the flow of execution into our payload. We have been most successful in exploitation by overwriting a structured exception handler address on the stack. Due to the fact that we supplied addresses that aren't associated with valid lookaside lists, an exception handler will be called, and when it does, it will call our modified routine, which points directly into payload code.

It should be noted that while this vulnerability exists in the .ASP ISAPI, a mechanism is still required to get the malicious request to hit the vulnerable functions within the .ASP ISAPI. Although pages with form submissions make it easier to demonstrate this vulnerability, there are other methods for causing code to execute beyond the form variable referencing. In the above example we used a default .asp file that has script code within it that deals with .ASP Server Variables. When the .ASP ISAPI performs processing on the Server Variables, we are able to cause an overflow and execute code. There are .asp files by default in IIS that allow processing of Server Variables, which make it possible to demonstrate the existence of this vulnerability on default installations.

Like most of the IIS vulnerabilities eEye has discovered in the past, firewalls and intrusion detection systems do not protect from this vulnerability.

SecureIIS - Web Server Protection for Microsoft IIS

It should be noted that clients using SecureIIS 1.2.5 and above are secure from this vulnerability. This vulnerability was discovered by the eEye team while testing a new version of SecureIIS to help further its protection abilities. To learn more visit http://www.eeye.com/SecureIIS

Vendor Status:
Microsoft has released a security bulletin and patch:
http://www.microsoft.com/technet/security/bulletin/MS02-018.asp

Credit:
Discovery: Riley Hassell
Exploitation Research: Riley Hassell and Ryan Permeh

Greetings:
To all the people who continue to make the security industry more exciting with innovative research. Also to the rest of eEye, who help make all this magic possible.

References

Zwicky, Elizabeth D., Cooper, Simon & Chapman, D. Brent -
Building Internet Firewalls, Sebastopol - CA, O'REILLY
June 2000,

Albitz, Paul & Liu, Cricket, DNS and BIND,
Sebastopol - CA , O'REILLY, April 2001

Checkpoint Software Technologies Ltd, Checkpoint NG AI R55
Documentation ;
URL: http://www.checkpoint.com/support/technical/documents/docs_r55.html
(July / Aug 2004)

Cisco Systems Inc, Cisco IOS Software Releases 12.3 Command References
URL:http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_command_reference_list.html
(Jul / Aug 2004)

HP, Server Platforms - Specifications & Pricing
http://welcome.hp.com/country/us/en/prodserv/servers.html
(Jul / Aug 2004)

Rudzonis, Brian "How to Protect a Fortune Cookie Empire: A Secure Perimeter Design for GIAC Enterprises", Feb 12, 2004
URL: http://www.giac.org/practical/GCFW/Brian_Rudzonis_GCFW.pdf
(Jul/Aug, 2004)

Packet Storm, Database of Vulnerabilities and Exploit Code
URL: http://packetstormsecurity.org
(Jul/Aug 2004)

Microsoft Coporation, Technet Security Bulletins – "SMTP Vulnerability"
"Microsoft Security Bulletin MS02-037"
http://www.microsoft.com/technet/security/bulletin/MS02-037.mspx
(Jul/Aug, 2004)

Microsoft Coporation, Technet Security Bulletins – "SMTP Vulnerability"
"Microsoft Security Bulletin MS03-046"
http://www.microsoft.com/technet/security/bulletin/MS03-046.mspx
(Jul/Aug, 2004)

Riley, Hassel , Ryan, Permeh ,
eEye Digital Security Vulnerability Solutions,
"Microsoft IIS /ASP Vulnerability"
http://www.eeye.com/html/Research/Advisories/AD20020410.html
(Jul/Aug, 2004)

SANS Track 2 - Firewalls, Perimeter Protection & Virtual Private Networks
Course Material – www.sans.org