SANS GCFW PRACTICAL ASSIGNMENT
Version 1.8

GIAC ENTERPRISES

By Kah Sing, Chong
Feb 28, 2003

Table of Content **Page**

Assignment 1 Security Architecture

1.1 Introduction

GIAC Enterprises (GIAC) is an e-commerce company incorporated in the year of 1997. Its core business is selling fortunes cookie sayings via Internet.

The company is operating its business with stiff competition from its rivals, which adopt price-cutting measure to attract more customers. To match competitors' pricing, GIAC has to reduce cost. It had resort to reducing staff strength to 20 people from its prime time of 200 staffs. This helps them to save the operating expenses.

However, GIAC's Financial Controller, Mr. Bush felt that the company needs fresh money to fund its operations. He had expressed this in company annual meeting. This intention has fast attracted venture capitalist, Liberal Ventures (LV) interest in investing in its business.

In one of the company visits, LV raised the question as to how GIAC operates its business and how it ensures its network is protected from intruders.

1.2 GIAC Business Operations Overview

To start off, we first reviewed GIAC business operations. This will help LV to understand the network access requirements later on. Based on the natures of business, we classified the business relationships into 2 types i.e.:-

a) internal environment – employees

b) external environment – customers, business partners and suppliers

1.2.1 Employees

GIAC employs 20 staff. There are 2 different types of staff in GIAC i.e. mobile staff (marketing executive) and static staff (office administrator and IT staff). The marketing team, who normally move around in their field, requires to access to GIAC network from remote locations. This is to enable them to check their email and submit monthly report. For secure their access and the GIAC network, all their laptop are protected with Norton Anti-Virus (v7.60) and ISS BlackICE personal firewall. This will shield the GIAC internal network from unauthorised access.

The office administrator will process and compile all the incoming fortunes from suppliers. This is achieved by connecting to Lotus Notes database server, which stored the fortunes database. IT staff will archive the database into media (DAT tape) daily.

1.2.2 Customer and business partner

Customer could purchase online cookies through connecting to GIAC web server that will accept order. The connection is encrypted in 128 bits SSL(Secure Shell Layered) mode.

As for the business partner, GIAC has 2 international partner i.e. Allianz Star Ltd and Predictor Ltd. They could access to GIAC to download fortunes and resale. The connection is done through establishing VPN tunnel into the internal database server.

Both of these connections require authorised users to authenticate through user name and password. For any access problem encountered, the customer could contact the GIAC employees via phone or email (cust-service@giac.com.my).

1.2.3 Supplierss

GIAC employs international freelance writers to come up with the fortunes saying. In the past, these writers submit their work by mail or fax. Some of their work are lost and could not be accountable for, GIAC decide to improve and adopt standardized electronic format for their submission. This measure will help in reducing processing cycle especially time required by GIAC staff. To initiate the task, the writers are requires to connect to the GIAC server via SSH (Secure Shell). This is where they deposit their work.

This paper is going to describes about the:-

a) company's network architectures.
b) configuration of defense perimeters ie border router, firewalls and VPN devices.
c) firewall policy and the audit output.
d) weaknesses in the network design and the recommendation to overcome it.

1.3 Policy and Procedure

Currently, 3 types of policies exist in GIAC IT department i.e.:-

a) General policies (covers stuffs like physical access control and disaster recovery procedure)
b) Operating System (OS) System Administration Manual (covers OS functions, job scope of system administrator, list of vendors' contact)
c) OS and Application Security Manual (encompass steps to follow in maintaining the application and OS security)

These guidelines will serve as the minimum standard in daily IT work.

1.3.1 Quality Assurance

To ensure GIAC IT staffs are competent in carrying their work, they are sent for professional training and certification twice a year. Staff attended the courses are required to brief others on their subjects, so as to ensure that knowledge replication are practiced.

1.4 Network Architecture

GIAC's IT department missions are to provide cost effective and scalable solutions to complement its business operations. It has also defined one of its priorities to ensure high standard of IT security.

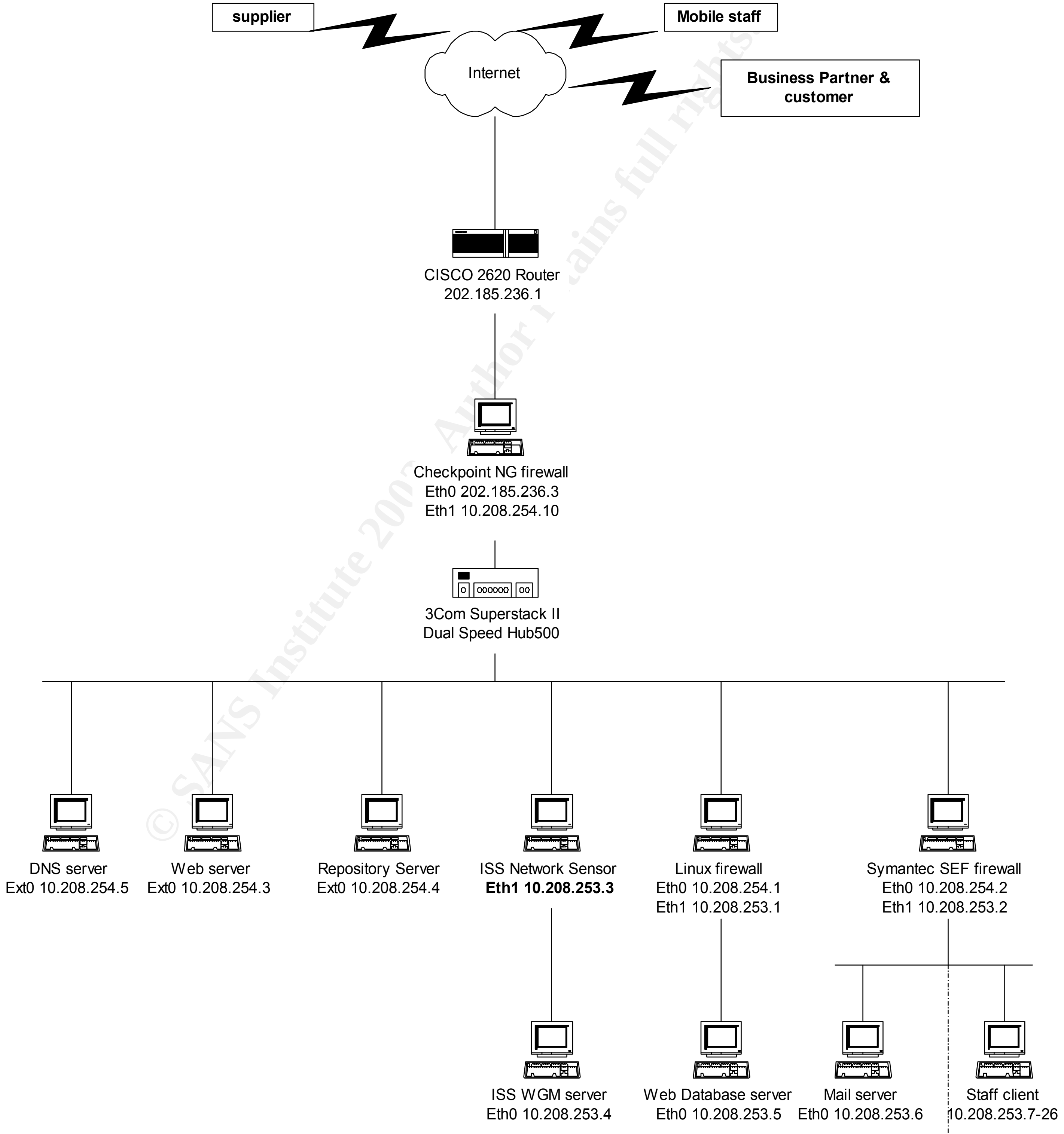
To understand GIAC network architecture, we first look at the company:-

1 Network diagram

2 IP address assignment
3 Security devices
4 Services and ports required for the servers to operate

(Please refer to the below GIAC network diagram)

GIAC Network Diagram



1.4.1 Network Diagram

From the above network diagram, GIAC network is running on 1 Megabytes (1 Mb) leased lines as to connect to internet. Its security strategy is adopting “defense in depth” approach i.e. using multiple layers of protection in a network. In other word, defense-in-depth assumes that any individual security precaution might fail, and has another line of defense ready **[1]**.

The first layer of protection came about at its border router. GIAC bought a CISCO 2620 router for this purpose. The device is chosen to provide performance and scalability. Some of the notable 2620’s features include:-

- VPN access with Firewall and Encryption options
- Quality of Services (QoS)
- Traffic monitoring
- Wide range of routing protocols

CISCO 2620 Traffic flow
Other than allowing HTTP, HTTPS, SMTP, SSH and DNS traffic passed into the network, the following are the required port and service:-

1) telnet (TCP - Port 23)
It is used configure the border router from internal network. The router only allowed authorised access of logging into the router.

The next level of network is protected by distributed firewalls. The first perimeter of defense is provided by Checkpoint VPN-1 NG firewall. Known for its stateful inspection technology to control traffic, this firewall runs on Windows 2000 Server. Its task is to screen all traffic coming from the border router and direct it to internal network.

Checkpoint NG is chosen because of its stateful inspection architecture, which intercepts, analyzes and takes action on all communications before they enter the operating system of the gateway machine. By performing the task, it ensures full security and integrity of the network. Theoretically, it proves to be safer than a packet filtering firewall.

Checkpoint NG VPN-1 traffic flow
Refer to Section 1.4.4. In addition, Checkpoint internal processes requires the following ports to be opened in the machine **[2]**:-

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.

In addition, the following protocol and service are required for VPN connection:-

Destination	Service	Port
VPN Gateway	ESP	IP Protocol 50
VPN Gateway	IKE	UDP Port 500

Deep down internal network, it is protected by Linux firewall (IP Table) and Axent Symantec Enterprise Firewall (Axent SEF). Linux firewall functions as the gateway into database server. While Axent SEF is the proxy providing email and web browsing activities for GIAC employees. The rationale of having separate firewall is to ensure critical servers like database server can be closely monitored when they are isolated behind an internal firewall. Any malicious activity would be much easier to detect, since the firewall has a limited amount of traffic passing through it.

Linux and Axent SEF traffic flow
Refer to Section 1.4.4

GIAC adopt a multiple-vendor solution approach so as to perform risk management. This is because different skills and efforts are required to penetrate the security architecture of multiple solutions. The disadvantage of this approach is it incurred higher operational cost as there is a need to employ different expertise in managing the firewalls.

From the network segment 1 (Public Zone), we noted that there are 4 Windows 2000 Servers ie:-

a) DNS server	(TCP/UDP – Port 53)
b) web server	(TCP – Port 80 / 443)
c) repository server	(TCP – Port 1352)

GIAC's DNS is running on Windows 2000 DNS. This server will provide name resolution services from all external queries for giac.com.my. While web server is powered by Netscape Navigator engine (version 3.6) and Lotus Notes application (v5.07) will act as the repository server where supplier could store their cookies.

The web's database server is located in Network segment 2 (Private Zone). This database is sit on Lotus Notes server (v5.07). The rationale of placing Checkpoint NG firewall between the web server and database server is to prevent direct attack into the database and also corruption of information if it was placed together with the web server.

Lastly, in Network Segment 3 (Private Zone 2), we could see the email server (Exchange server NT4 SP6a) lying behind Axent SEF firewall. Port used in SMTP / POP is TCP – Port 25 / 110. This firewall server acts as the gateway where employees could receive and sent email (inbound and outbound) from the email server. Port 80 and 443 also opened for web surfing.

Additional security includes installation of Realsecure Server Sensor (Service Release 3.6) in web, repository and database servers. The rationale is to block suspicious traffic and intercept packet before it reaches the operating system. The monitoring is performed in inbound and outbound manner.

GIAC also install an ISS Realsecure Network Sensor (NS) version 7.0 in its network. ISS Realsecure NS is an automated, real-time intrusion detection and response system that analyses activity across the network. It consists of 2 components:-

i) Sensors – software that looks for attacks and generates responses.

ii) Workgroup Manager (WGM) – act as the GUI interface and manages sensors' operations.

The NS is running on stealth mode i.e. no IP address attached to the detection interface or no layer 3 presence in the network. The signature pattern is updated in the ISS WGM through Axent SEF connection into ISS website.

ISS Realsecure traffic flows

Realsecure Network Sensor (TCP – Port 901)
This is the communication port between the workgroup manager (console) and the network sensor. As the 2 components lied in the same segment, it would shown up as a rule in the Checkpoint NG.

Realsecure Server Sensor (TCP – Port 902)
This is the communication port used between the workgroup manager (console) and the network sensor. As the 2 components lied in the same segment, it would shown up as a rule in the Checkpoint NG.

Realsecure Event Collector (TCP – Port 903)
All sensors communicate with Event Collector with this port. As the 2 components lied in the same segment, it would shown up as a rule in the Checkpoint NG.

Realsecure ISS Daemon (TCP – Port 2998)
The ISS Daemon listens at this port. It manages the starting and stopping of ISS services.

GIAC also installs Norton Anti-Virus (NAV) version 7.03 (corporate edition) to prevent the proliferation of viruses and worms (eg Klez or Slammer worm). The virus patterns are updated directly from the Norton websites.

1.4.2 Hardening of Devices

The hardening of GIAC's Windows 2000 servers are based on National Security Agency (NSA) Security guides (downloadable from http://nsa1.www.conxion.com/win2k/download.htm). Realizing the fact that new vulnerabilities are discovered each day, it is appropriate to subscribe to relevant mailing lists (eg, SANS Newsbites, ISS X-force and CERT) to keep abreast of the development in IT security.

Patching of servers are performed with care with the following steps:-

a) Seek advise from related hardware and software vendors on its feasibility to apply patches.
b) Test the patches in its development environment.
c) If everything goes smoothly, applies it in Production environment with change management form filled up.

In addition, disaster recovery plans for all the devices are documented. Database and configuration for respective system are archived and stored in secured off-site. There will be two mock run (simulation test) to test on the functionable of archived information.

1.4.3. IP address assignment

GIAC uses the IP block of 202.185.236.1 – 202.185.236.14 with the subnet mask of 255.255.255.240. The internal network runs on 10.208.253.x and 10.208.254.x with subnet mask of 255.255.255.0.

Routers and Firewall	Interface	Interface Name	Internal IP address	External IP address
Cisco Border Router	External	Ext		202.185.236.1
Checkpoint NG firewall	External	Eth0		202.185.236.3
	Internal	Eth1	10.208.254.10	
Linux Firewall	External	Eth0		10.208.254.1
	Internal	Eth1	10.208.253.1	
Axent SEF	External	Eth0		10.208.254.2
	Internal	Eth1	10.208.253.2	
Intrusion Detection system	**Interface**	**Interface Name**	**Internal IP address**	**External IP address**

ISS Network Sensor	External	(Running on stealth mode – no IP defined)		
	Internal	Eth1	10.208.253.3	
ISS Database server	External	Eth0		10.208.253.4
Network Segment 1	**Interface**	**Interface Name**	**Internal IP address**	**External IP address**
Web server	External	Ext0		10.208.254.3
Repository server	External	Ext0		10.208.254.4
Internal DNS	External	Ext0		10.208.254.5
Network Segment 2	**Interface**	**Interface Name**	**Internal IP address**	**External IP address**
Web Database server	External	Eth0		10.208.253.5
Network Segment 3	**Interface**	**Interface Name**	**Internal IP address**	**External IP address**
Exchange Email server	External	Eth0		10.208.253.6
Staff client	Range from 10.208.253.7-10.208.253.26			

1.4.4 Services and ports required

From the business requirement, we derived the following services and ports are needed for the flow of network traffic:-

Application / Services	Where to effect	Protocol (Direction)	Ports	Purpose
Web services	Checkpoint NG	TCP (inbound)	443	Customer connection into web services (SSL)
POP	Checkpoint NG & Axent SEF	TCP (inbound)	110	Marketing staff connection to check email and submit report
Email	Checkpoint NG & Axent SEF	TCP (inbound and outbound)	25	Head office staff to receive and send out email
SSH	Checkpoint NG	TCP (inbound)	22	Supplier to submit their work
DNS	Checkpoint NG	UDP (inbound and outbound)	53	DNS services
DNS	Checkpoint NG	TCP (inbound and outbound)	53	DNS Zone Transfer to ISP
Web browsing	Checkpoint NG & Axent SEF	TCP (outbound)	80 and 443	Staff to do internet browsing
Lotus Notes	Checkpoint NG & Linux firewall	TCP - inbound	1352	Uploading and retrieving database

NAV	Linux firewall Checkpoint NG Axent SEF	TCP- outbound	80 (restrict access to Virus Update server)	i) Virus pattern update ii) ISS signature update

Assignment 2 Security Policy and Tutorial

2.1 Border router

There are 3 primary security measures in protecting GIAC network ie:-
a) Border router
b) Firewall
c) VPN

The first component in GIAC's security perimeter is the CISCO 2620 Router. This router is part of 2600 series, which provides flexible LAN and WAN configurations, multiple security options and a range of high performance processors. Its notable features make it the ideal branch-office router for today's and tomorrow's customer requirements **[3]**.

Running on CISCO IOS version 12.2, its main function is to act as filtering router which filtered out unauthorised IP access and permit allowed traffic to pass to primary firewall (Checkpoint NG) for analysis. Other functions include:-

- Control ICMP traffic
- Block source routing and non valid IP addressing
- Implement ingress filtering – to deny spoofed IP from private IP ranges and inbound packets with a source IP of internal network.
- Implement egress filtering – preventing sending bad traffic into internet world.

Firstly, administrator needs to write the configuration in a simple text editor (eg Microsoft Notepad) and apply to the router once testing has been completed. This is essential so as not to disrupt the normal operation. The loading and backup the router's configuration can be performed via hyper-text terminal (from a laptop or desktop).

Following is the command to apply and backup a config in the router:-
Copy running-config tftp : Apply configuration
Copy tftp running-config : Backup of running config.

Secondly, one must know to enter into privileged mode. This mode allows viewing of router's main status. It can be achieved by typing **enable** at the command prompt. The privileged mode is differentiated from the non-privileged mode by "#" sign at the command prompt.

For eg, router > : non-privileged mode
router # : privileged more

Some of the commands an administrator needs to familiar with in the respect to router configuration includes:-

Purpose	Command
Change hostname	i) hostname <*intended hostname*>
Assign message banner	i) banner login / <*banner message*> /
Assign password to console access	i) line console 0 ii) login iii) password "consolepassword"
Enable password protect in privileged mode	Enable secret "secretpassword"
Lockdown password in MD5 hash	Service password encryption
Set timeout limit at console	i) line console 0 ii) exec-timeout *minutes*
Turn off Cisco Discovery Protocol and prevent display it is a CISCO router	i) no cdp enable
To block services that might be used to gain information about the network and prevent the router from sending unknown subnets of directly connected networks from using the default route	i) no ip classless
Disable service	No service *servicename*
Switch interface configuration	Interface *interfacename*
Prevent direct broadcast (eg smurf attack)	No ip directed-broadcast
Prevent router to return ICMP error messages	No ip unreachables
Blocking packets to be redirected	No ip redirects
Disallow source routing	No ip source-route

2.1.1 Access Control List (ACL)

There are 2 types of ACLs ie. standard ACL and extended ACL. Standard ACL only dropped or passed traffic based on source IP. The syntax for standard ACL's are as follow:-

Access-list <*list number 1-99*> <*permit/deny*> <*source address*> <*subnet mask*> <*log*>

As the name suggested, extended ACL examined packets in more detailed manner. Details like source port, destination IP and port, protocol and protocol options. The syntax for extended access list follows:-
Access-list <*list number 1-99*> <*permit/deny*> <*protocol*> <*source address*> <*subnet mask*> <*source port*> <*destination address*> <*subnet mask*> <*destination port*> <*log*> <*options*>

2.1.2 Configuration on border router

The security administrator has programmed the following configuration in router. First, he created access list named **access-list 88** for *inbound traffic* and **access-list 99** for *outbound traffic*.

<u>Inbound traffic</u>

Ingress filtering – stop non-valid IP addresses from entering the network

```
Access-list 88      deny  ip     0.0.0.0   0.255.255.255  any  log
Access-list 88      deny  ip     10.0.0.0   0.255.255.255  any  log
Access-list 88      deny  ip     127.0.0.0   0.255.255.255  any  log
Access-list 88      deny  ip     172.16.0.0  0.15.255.255  any  log
Access-list 88      deny  ip     192.168.0.0  0.0.255.255  any  log
```

Block Login services and review unauthorized attempt to access and control the router

```
Access-list 88      deny  tcp    any  any  range  ftp  telnet  log
Access-list 88      deny  tcp    any  any  range  exec  lpd  log
```

Block Netbios and log any activities

```
Access-list 88      deny  tcp    any  any  135  log
Access-list 88      deny  udp    any  any  135  log
Access-list 88      deny  udp    any  range  137  138  log
Access-list 88      deny  tcp    any  any  eq  139  log
Access-list 88      deny  tcp    any  any  eq  445  log
Access-list 88      deny  udp    any  any  eq  445  log
```

Allow SMTP services only to the email server

```
Access-list 88      permit      tcp    any  202.185.236.13  0.0.0.0  eq  25
```

Allow DNS traffic to DNS server

```
Access-list 88      permit      tcp    any  202.185.236.11  0.0.0.0  eq  53
Access-list 88      permit      udp    any  202.185.236.11  0.0.0.0  eq  53
```

Allow HTTP / HTTPS traffic only to the web server

```
Access-list 88      permit      tcp    any  202.185.236.7  0.0.0.0  eq  80
```

```
Access-list 88      permit      tcp    any  202.185.236.7  0.0.0.0  eq  443
```

Allow VPN traffic to the repository server

```
Access-list 88      permit      udp    any   eq  500  host  202.185.236.14   eq  500
log
Access-list 88      permit      50   any   host   202.185.236.14   log
Access-list 88      permit      51   any   host   202.185.236.14   log
```

Outbound traffic

Allow IP address from GIAC network leaving outbound

```
Access-list 99      permit      202.185.236.0   240.255.255.255   any
```

Allow outbound established web server replies

```
Access-list 99      permit      tcp    202.185.236.7   0.0.0.0   any   gt   1023   est
```

Allow outbound replies from the mail server

```
Access-list 99      permit      tcp    202.185.236.13   0.0.0.0   gt 1023   est
```

Allow outbound replies from the DNS server

```
Access-list 99      permit      tcp    202.185.236.11   0.0.0.0   any   gt   1023   est
Access-list 99      permit      udp    202.185.236.11   0.0.0.0   any  eq  53
```

Apply egress filtering – only valid IP address leaving GIAC network

```
Access-list 99      deny   ip   10.0.0.0   0.255.255.255   any   log
Access-list 99      deny   ip   127.0.0.0   0.255.255.255   any   log
Access-list 99      deny   ip   172.16.0.0   0.15.255.255   any   log
Access-list 99      deny   ip   192.168.0.0   0.0.255.255   any   log
```

Allow VPN traffic from the repository server

```
Access-list 88      permit      udp    202.185.236.14   eq  500  host   any   eq  500
log
Access-list 88      permit      50   202.185.236.14   host   any   log
Access-list 88      permit      51   202.185.236.14   host   any   log
```

2.2 Checkpoint VPN-1 / Firewall-1 Policy and Configuration Tutorial

GIAC has chosen Checkpoint VPN-1 Next Generation (NG) as the primary gateway firewall. There are reasons why GIAC chosen an integrated VPN/firewall solution instead of purchasing a separate VPN box and firewall.

As for business decision, it is more comfortable to purchase Checkpoint VPN-1 as it is market leader and it commands 41% of world market share **[4]**. In term of security aspect, the integrated solution is able to offer single management over VPN and firewall. Furthermore, users did not have to worry on the placement of VPN box (behind or in front of firewall) in standalone VPN box. The unified logging between firewall and VPN could leverage and reduce network administration work.

The current version of Checkpoint GIAC in on is Features Pack (FP) 2. Even though FP3 was issued on August 2002, there is not much effect with GIAC on the rectified issue. As such, GIAC prefer to maintain at current version.

As for operating system (OS), the firewall runs on a hardened Windows 2000 Server SP2. The server contained 2 interfaces, one connected to Network segment 1 and another to Network segment 2. Checkpoint NG processed and analysed traffic based on “top-down” approach i.e. any packet that did not match the rule-sets will be dropped.

Before we begin the tutorial, we need to identify the relevant Checkpoint reference web-sites. Some of the good resources available are:-

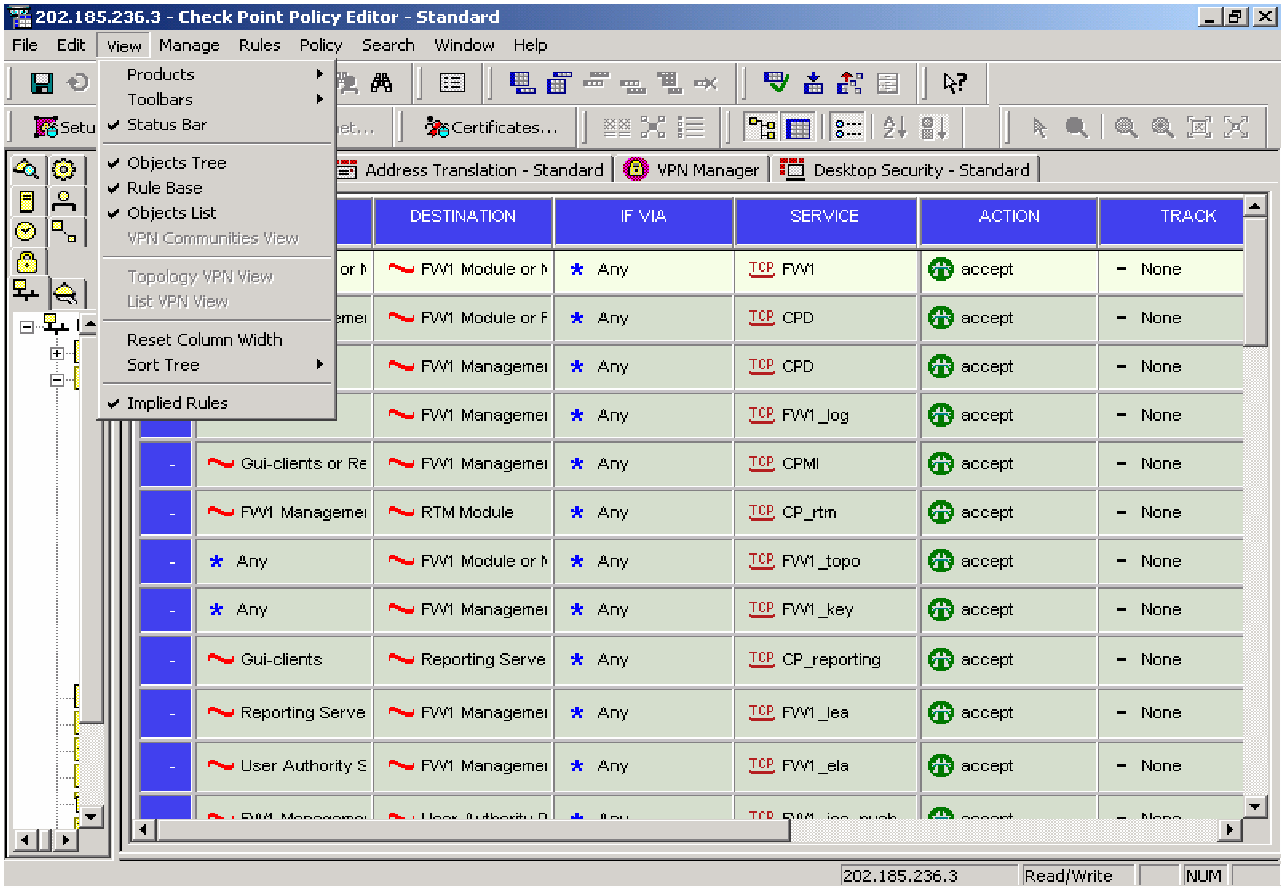
a) https://usercenter.checkpoint.com.
b) http://www.phoneboy.com/fw1/
c) http://www.securityfocus.com

These references are good for troubleshooting and exchange views on Checkpoint’s issues. It helps to zero in information and save time.

2.2.1 Steps to perform before Rule set Configuration

a) Anti-spoofing

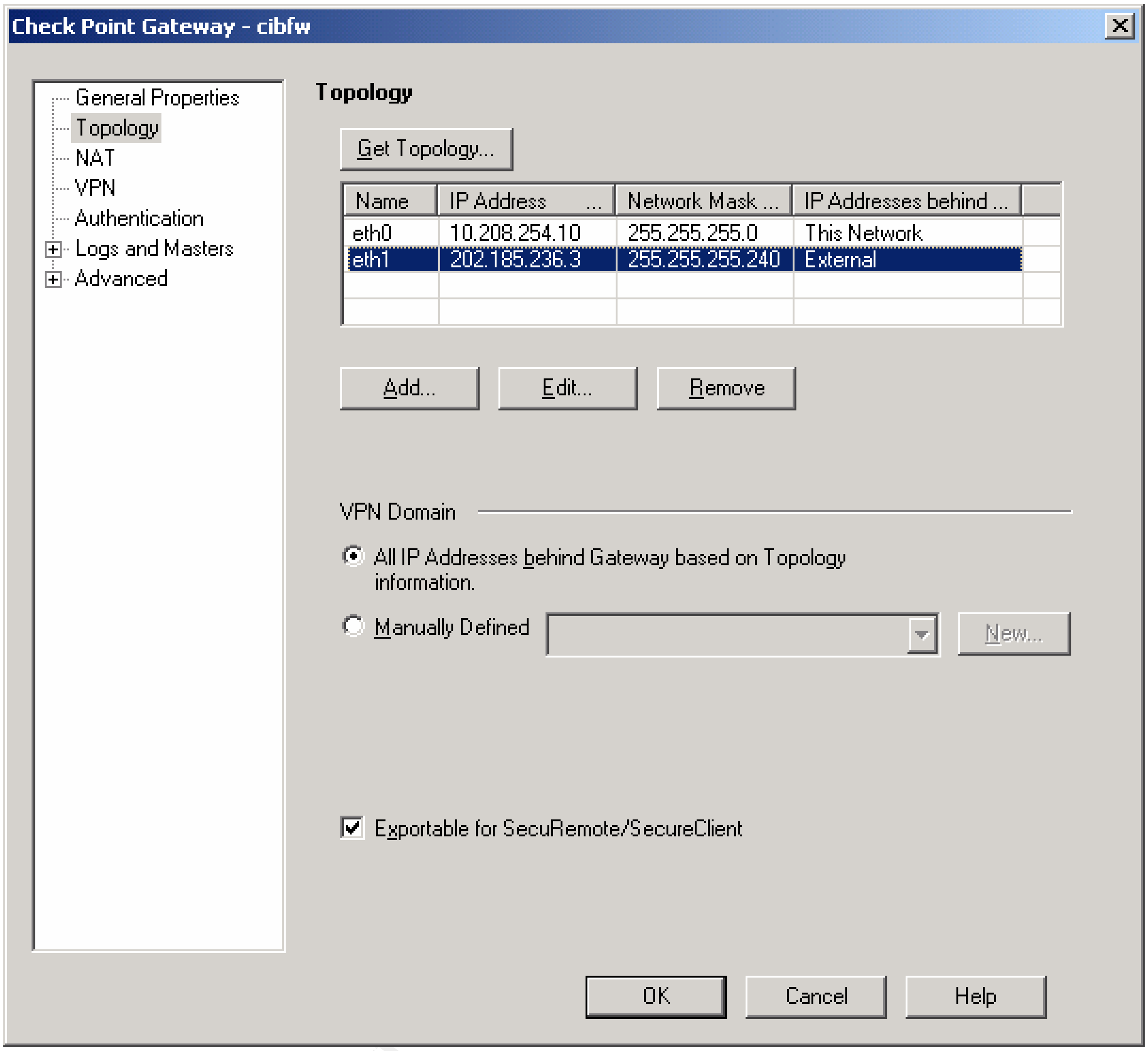
Before going to the rule base setting, we need to turn off unnecessary configuration. First, we need to disable all the implied rules in Checkpoint NG, which has been turned on by default. This could be achieved by going to “**View pull down menu** – **Implied Rules**” and unchecked all the “implied rules” section in the pop up menu, except the “**Accept outgoing packets originating from gateway**”. This is because the said functionality is required for Network Address Translation (NAT) to work properly. The snapshot of the Implied rules pop up menu can be found as follows:-



		DESTINATION	IF VIA	SERVICE	ACTION	TRACK
	or N	FW1 Module or N	Any	TCP FW1	accept	None
	emei	FW1 Module or F	Any	TCP CPD	accept	None
		FW1 Managemei	Any	TCP CPD	accept	None
		FW1 Managemei	Any	TCP FW1_log	accept	None
-	Gui-clients or Re	FW1 Managemei	Any	TCP CPMI	accept	None
-	FW1 Managemei	RTM Module	Any	TCP CP_rtm	accept	None
-	Any	FW1 Module or N	Any	TCP FW1_topo	accept	None
-	Any	FW1 Managemei	Any	TCP FW1_key	accept	None
-	Gui-clients	Reporting Serve	Any	TCP CP_reporting	accept	None
-	Reporting Serve	FW1 Managemei	Any	TCP FW1_lea	accept	None
-	User Authority S	FW1 Managemei	Any	TCP FW1_ela	accept	None
	FW1 Manageme	User Authority D	Any	TCP FW1_ica_push	accept	None

Secondly, we could utilize Checkpoint's Anti-spoofing capabilities to limit IP spoofing attempts. IP spoofing involves imitating the IP address of a "trusted" host in order to gain access to protected information resources. To initiate anti-spoofing features, one must clearly define the network sitting behind each interface on the firewall. The firewall will then detect and examine the IP address of the incoming packets to validate whether these are coming from authorized network, and not spoofed IPs. There are 3 options for tracking ie. *No* (No action taken), *Log* (Turn On logging) and *Alert* (send alerts to administrator once spoofing detected)

To initiate the task, we select the option **Manage – Network Objects – highlight firewall object – select Edit (GIAC firewall object is term as cibfw)**. We derived at the firewall properties. Further, selecting the **Topology tab – Get Interfaces option** will discern all the firewall interfaces. The snapshot is as follows:-



Topology

Name	IP Address	Network Mask	IP Addresses behind
eth0	10.208.254.10	255.255.255.0	This Network
eth1	202.185.236.3	255.255.255.240	External

VPN Domain

● All IP Addresses behind Gateway based on Topology information.

○ Manually Defined

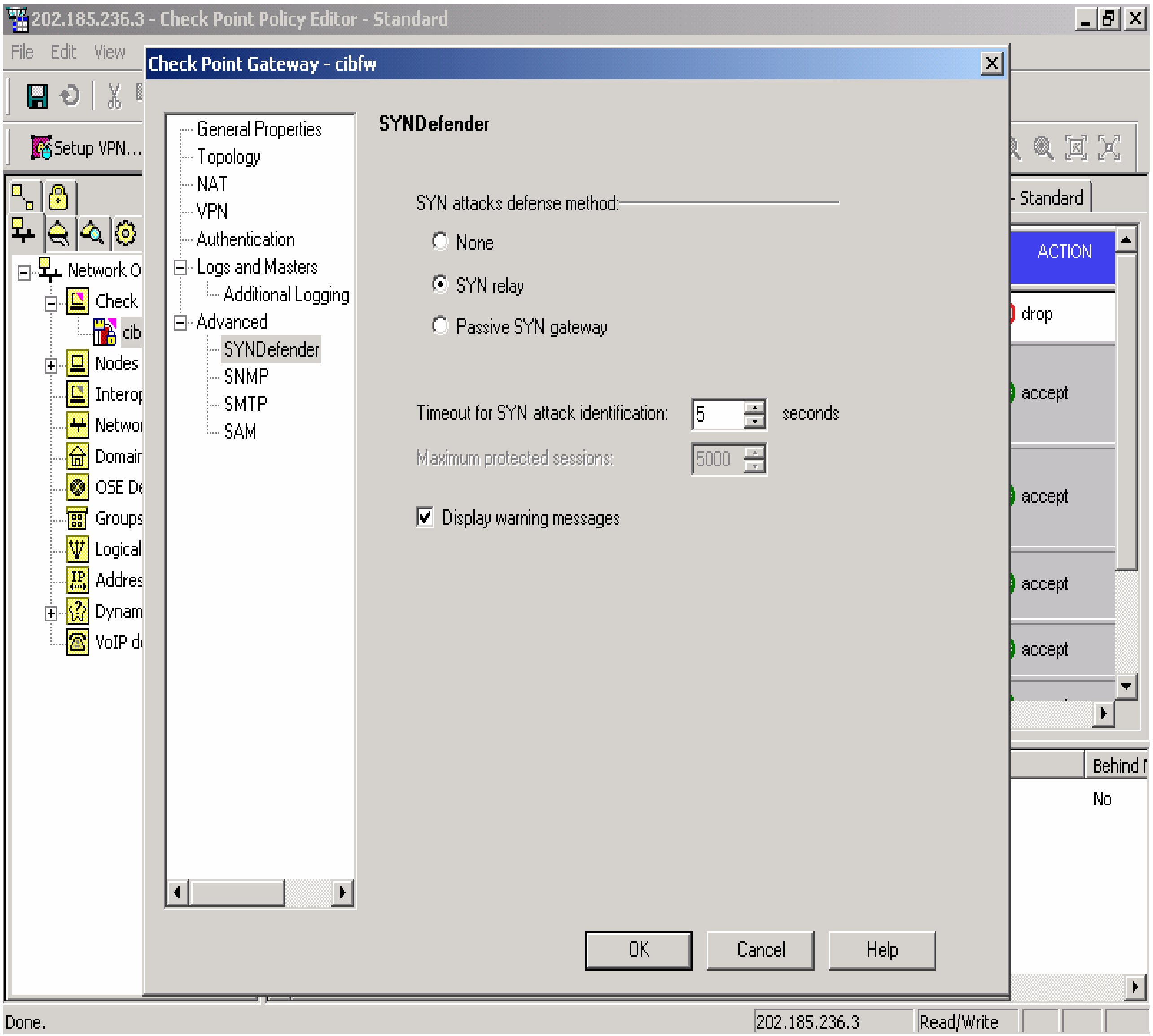
☑ Exportable for SecuRemote/SecureClient

b) SYN-defender

In addition, SYN-defender option is available as to defend the protected hosts from Syn-flood attack. The configuration of SYN-Defender requires us to go to **the firewall object** and **selecting the Advanced option**. Then, we should able to see 3 SYN attacks defense method ie:-

i) None
ii) SYN relay – counter attack by sending SYN once 3 way handshake is completed.
iii) Passive SYN gateway

GIAC chooses on SYN relay option and set the timeout to 5 seconds (default 10 seconds). The rationale of reducing the timeout time is to reduce the overhead cost / loading to firewall's connection table.



SYNDefender

SYN attacks defense method:

○ None
● SYN relay
○ Passive SYN gateway

Timeout for SYN attack identification: 5 seconds

Maximum protected sessions: 5000

☑ Display warning messages

c) Command Line

On top of these options, a firewall administrator needs to familiar with Checkpoint NG command lines (which can be execute from command prompt) ie.:-

Purpose	Command
Determine Checkpoint's available commands.	Fw /?
Load Checkpoint firewall's module and start the following 4 processes:- • VPN-1 / Firewall-1 daemon (fwd) • The Management server (fwm) • VPN-1 / Firewall-1 SNMP daemon	Fwstart

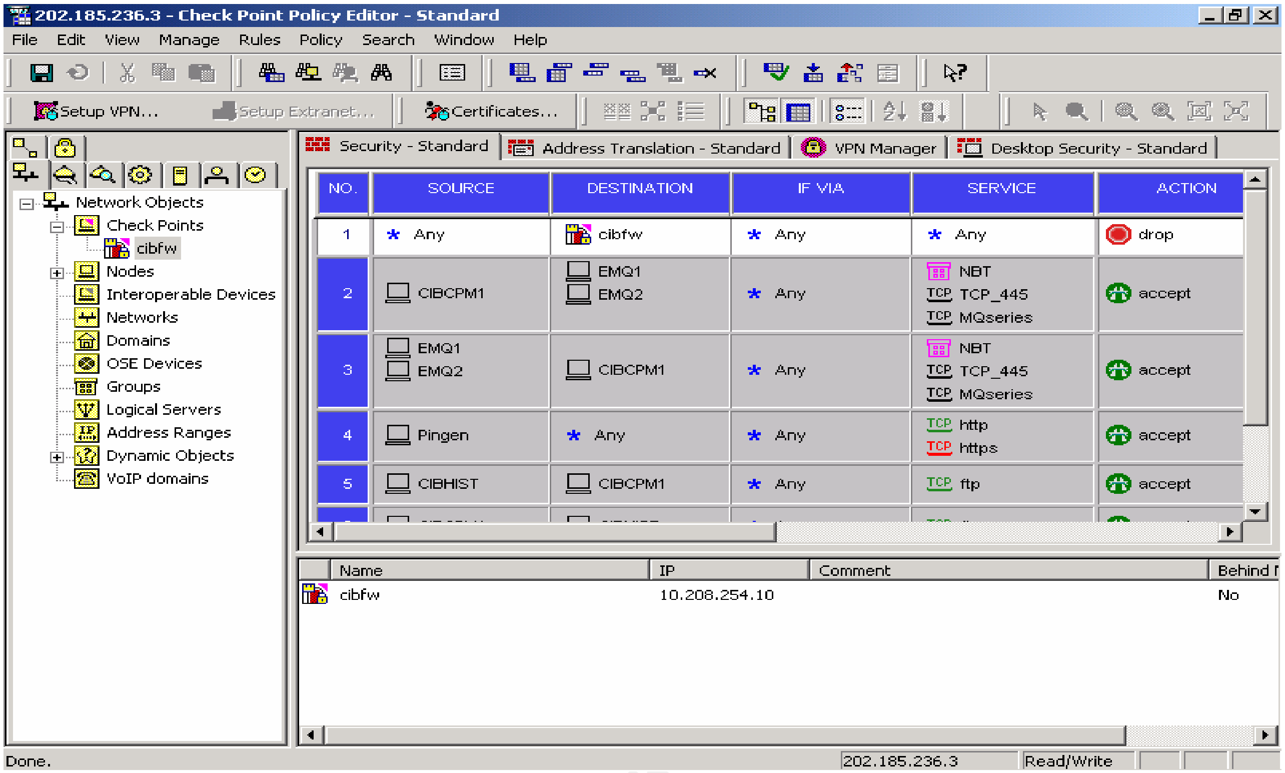
(snmpd) • The authentication daemon	
Unload the Checkpoint's module and kill the Checkpoint firewall's processes:- • VPN-1 / Firewall-1 daemon (fwd) • The Management server (fwm) • VPN-1 / Firewall-1 SNMP daemon (snmpd) • The authentication daemon	Fwstop
Display Checkpoint's version	Fw ver
Compiles and installs a security policy to the target's VPN / Firewall Modules.	Fw load
Send signal to a daemon	Fw kill
Monitor VPN-1 traffic	Fw monitor
Control kernel	Fw ctl <arg>
Display logs	Fw log
Create a new log file	Fw logswitch
Fetch last policy	Fw fetch *target*

d) Backup Firewall's Configuration

Next, a copy of the Checkpoint NG's configuration files is to be archived into media (eg diskette) for safekeeping / disaster recovery purpose. The configuration files are normally contained in the path ***Windows NT/Checkpoint/conf***. They need to be archived so as to shorten the recovery time if there is firewall failure.

2.2.2 Checkpoint's Policy Editor (PE) – "Security Dashboard" [5]

Checkpoint's PE has made more visual and clear view of the inter-relationship between various objects. One could also drag and drop items between panes. Generally, there is 2 types of windows available in PE i.e. **Workstation properties** window and **Global Properties** window. Below is an example snapshot of PE:-



NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION
1	Any	cibfw	Any	Any	drop
2	CIBCPM1	EMQ1 EMQ2	Any	NBT TCP_445 MQseries	accept
3	EMQ1 EMQ2	CIBCPM1	Any	NBT TCP_445 MQseries	accept
4	Pingen	Any	Any	http https	accept
5	CIBHIST	CIBCPM1	Any	ftp	accept

Name	IP	Comment	Behind I
cibfw	10.208.254.10		No

To summarize, here is some of the tasks that could performed under Checkpoint's PE:-

a) New Host creation

To create a new host, select **network object - workstation tab – New – Host**. Fill in the appropriate information. Same goes to new group creation (select **the workstation tab – new – group**).

b) New Group creation

Group creation eases the work of duplicating same rules for times. Eg, workstation A and B needs to access internet. We can put workstation A and B into a Group named C. Then, we could set up a rules allowing Group C into internet, instead of two rules into internet. This help to cut down the workload of firewall.

c) Create new rule base

The provided GUI interface has made the creation of new rule base easier. To create a rule, go to Rules – Add Rule – Top. To modify a rule, simply right click on the rule in the relevant column changes are needed.

d) Logging

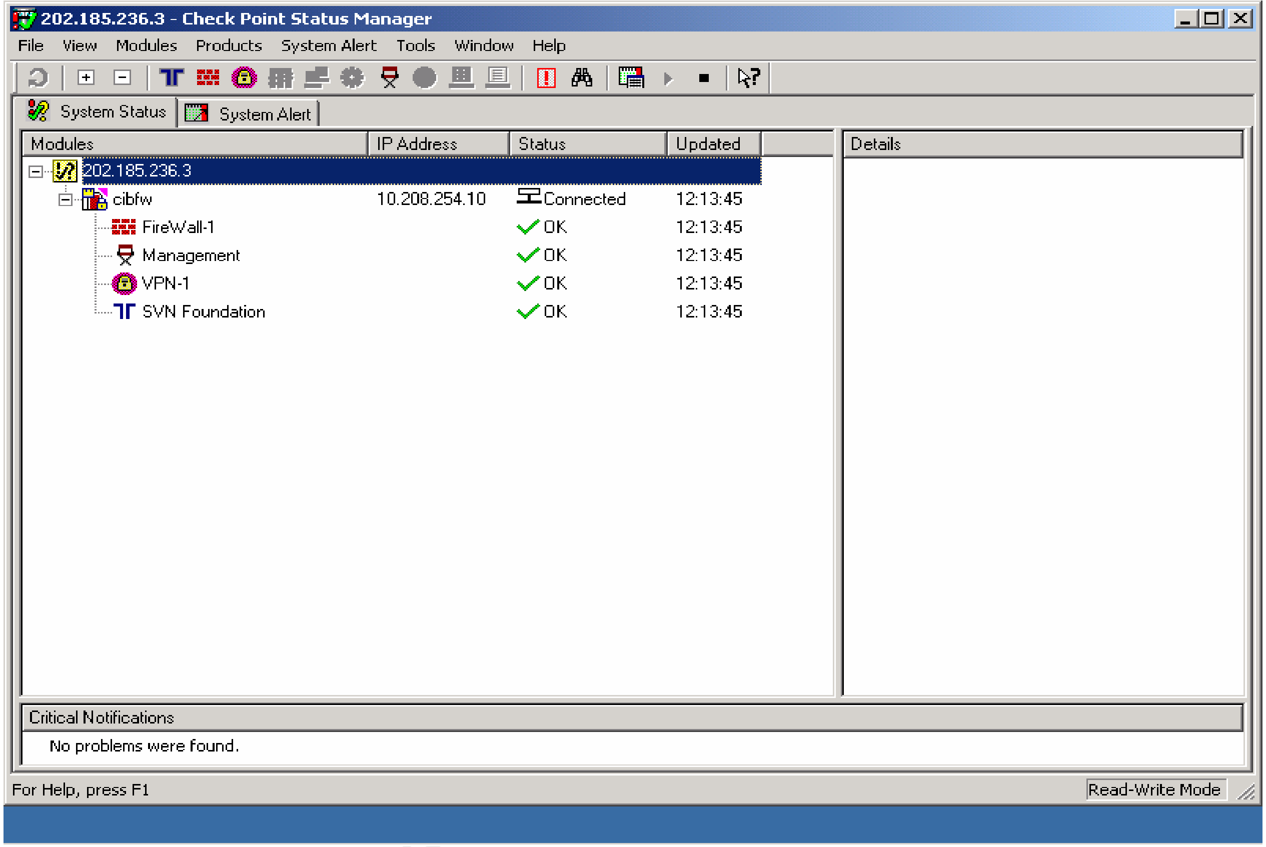
Security log is an important component of security policy **[6]**. We enabled the logging to gather data. Logs in Checkpoint are written in a binary format and could be exported in ASCII format. Logging is available in 3 modes i.e.:-

i) Log - Display the traffic logs
ii) Active - Display all the active connection currently open through firewall
iii) Audit - Tracked information include administrator's activities pertaining to

account login, account logout and rule base changes in the firewall.

e) System Status

Checkpoint has GUI interface to show the system status. To initiate the task, **select Window pull down menu – System Status.** This window presents a high-level view of operation and statistics for all firewall objects.



Modules	IP Address	Status	Updated
202.185.236.3			
cibfw	10.208.254.10	Connected	12:13:45
FireWall-1		✓ OK	12:13:45
Management		✓ OK	12:13:45
VPN-1		✓ OK	12:13:45
SVN Foundation		✓ OK	12:13:45

Critical Notifications

No problems were found.

2.2.3 Network Address Translation (NAT)

There are 4 different types of variation on how a NAT can be deployed i.e.:-

a) Port Forwarding or redirection

b) Hide NAT (many to one)

c) Static NAT (one to one)

d) NAT address Pool

Of which, GIAC is using static NAT in its network. Static NAT maps one internal private IP address to a legal IP address. The NAT tables are as such:-

Private IP	Legal IP
10.208.254.1	202.185.236.2
10.208.254.2	202.185.236.13
10.208.254.3	202.185.236.7
10.208.254.4	202.185.236.14
10.208.254.5	202.185.236.15

Configuration of static NAT requires the following steps:-

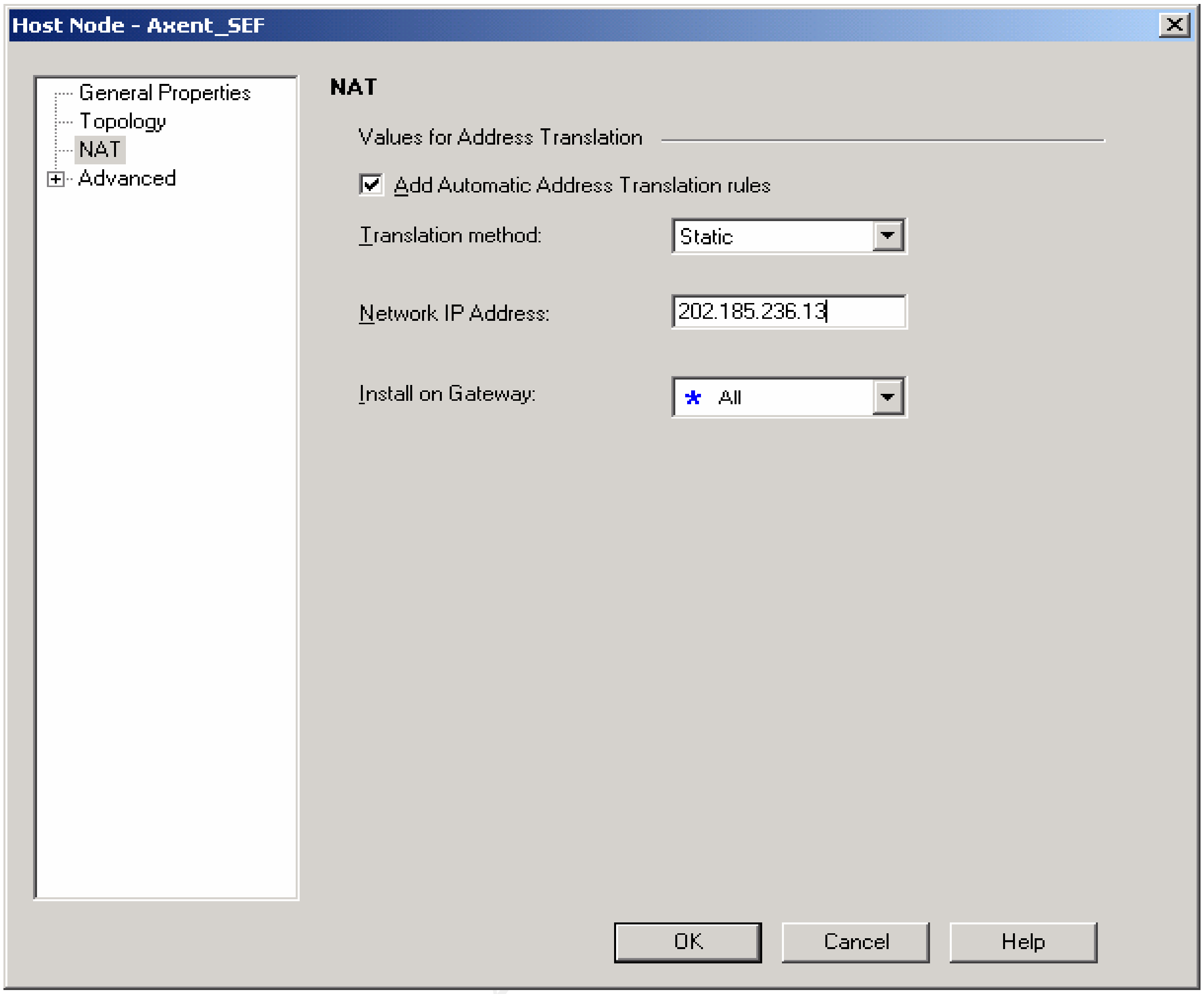
a) Create a workstation object and fill the private IP in the General tab

b) Switch to NAT tab. Check on "Add to Automatic Address Translation rules"

c) Change the translation method to "Static" and network valid address into the legal IP.

d) Install on "* All"

Example, insert NAT for Axent SEF like below:-



NAT

Values for Address Translation

☑ Add Automatic Address Translation rules

Translation method: Static

Network IP Address: 202.185.236.13

Install on Gateway: * All

2.2.4 VPN Tutorial

(Note : This tutorial I am running on demo mode, as such there might be some functions that did not appear as it wished)

Checkpoint Virtual Private Network (VPN) module protects the communication on the Internet and enables an enterprise to build its own VPN using private and public network segments. Checkpoint offers IKE encryption schemes, noting that FWZ encryption scheme is no longer supported in FP2 **[7]**.

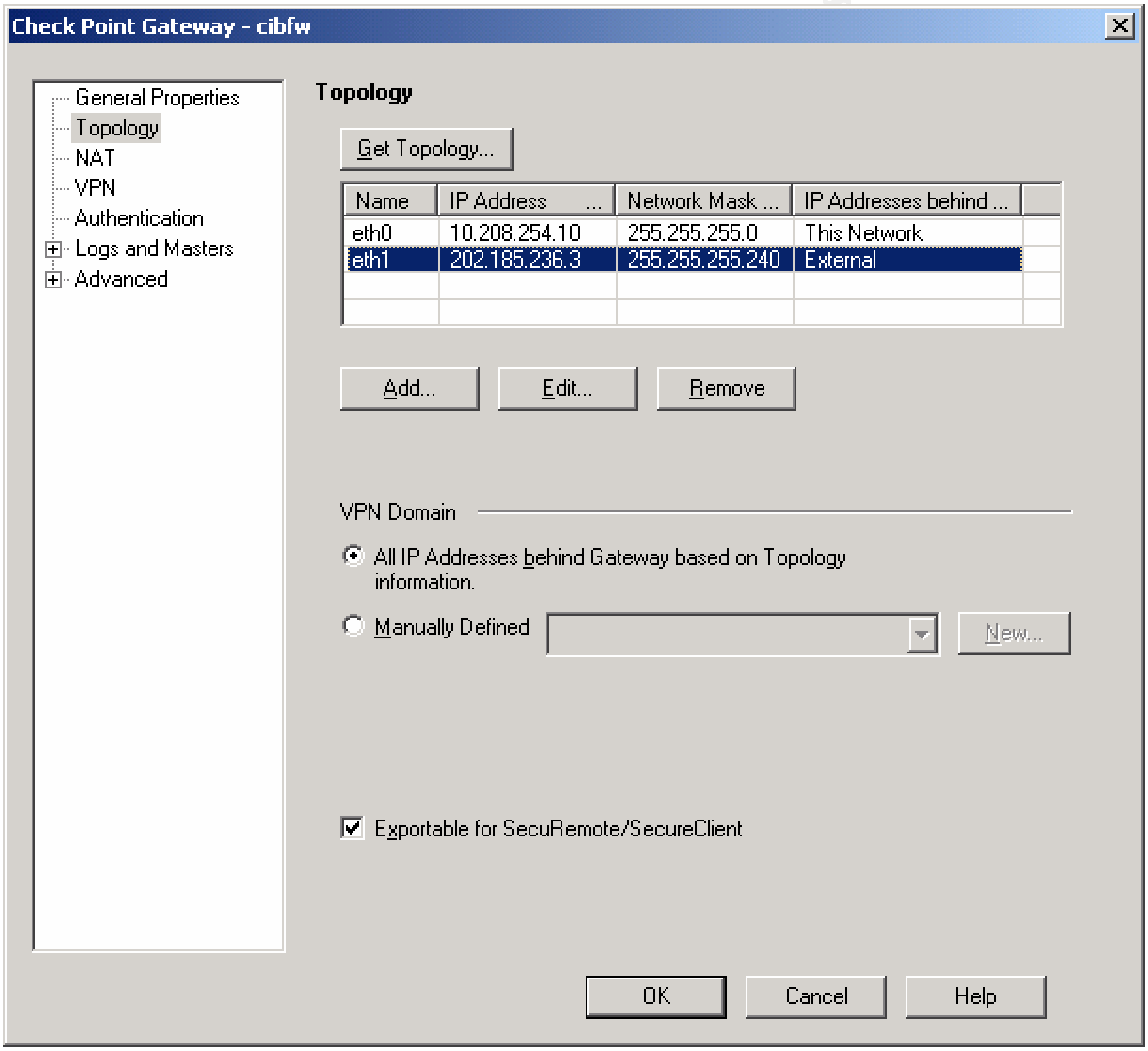
Encryption scheme	Authentication algorithm	Encryption algorithm
IKE	HMAC-MD5 HMAC-SHA-1	DES, 3DES, CAST, AES

In GIAC scenario, it will set up VPN connection with each of its partner companies using IKE (formerly known as ISAKMP / OAKLEY) encryption scheme. IKE is a standard for negotiating Security Associations (SAs) between 2 hosts that will be using IPSec. IKE offers improved authentication (HMAC) and Perfect forward Secrecy (PFS).

Following are the steps need to be taken in VPN set up:-

a) *Establish VPN encryption domain for GIAC network*.

To initiate the task, go to **Manage – Network Objects -** highlight **cibfw – edit –** select **topology** tab **–** check on **"All IP Addresses behind gateway based on topology information" & Exportable for SecuRemote/SecureClient**.



Name	IP Address	Network Mask ...	IP Addresses behind ...
eth0	10.208.254.10	255.255.255.0	This Network
eth1	202.185.236.3	255.255.255.240	External

VPN Domain

● All IP Addresses behind Gateway based on Topology information.

○ Manually Defined

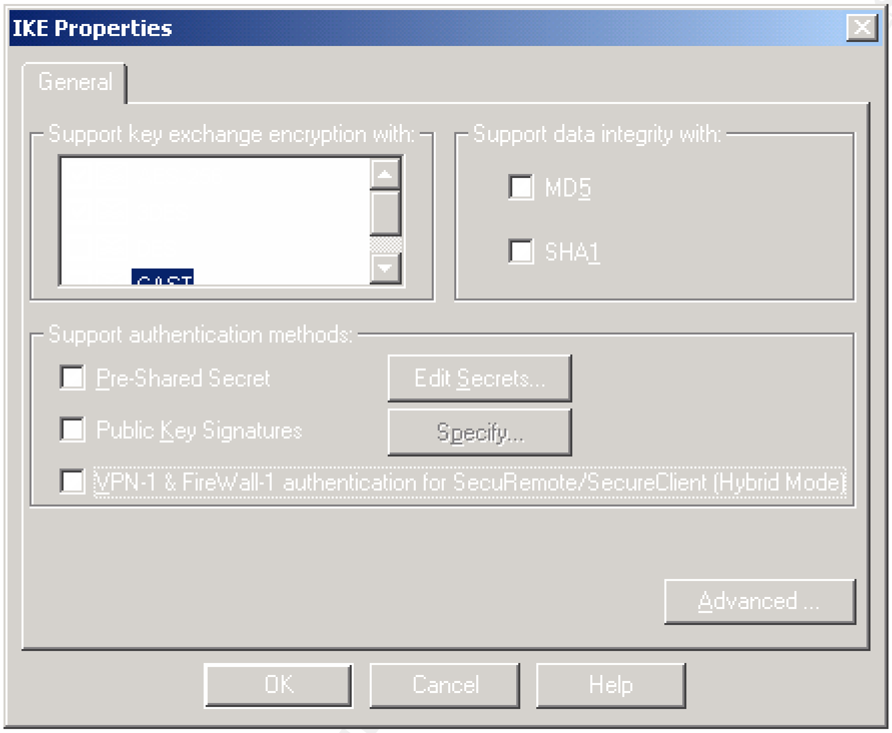
☑ Exportable for SecuRemote/SecureClient

b) *Define encryption scheme*

i) Go to VPN tab – check on the box to use IKE encryption – press Edit.

ii) In the **"support key exchange encryption with"** box, unchecked DES and CAST. The reason being we only accept 3DES and AES.

iii) In the **"support authentication methods"**, enable the Pre-shared secret and VPN-1 & Firewall-1 authentication to SecuRemote/SecureClient (Hybrid mode)



Support key exchange encryption with: CAST

Support data integrity with:

□ MD5

□ SHA1

Support authentication methods:

□ Pre-Shared Secret

□ Public Key Signatures

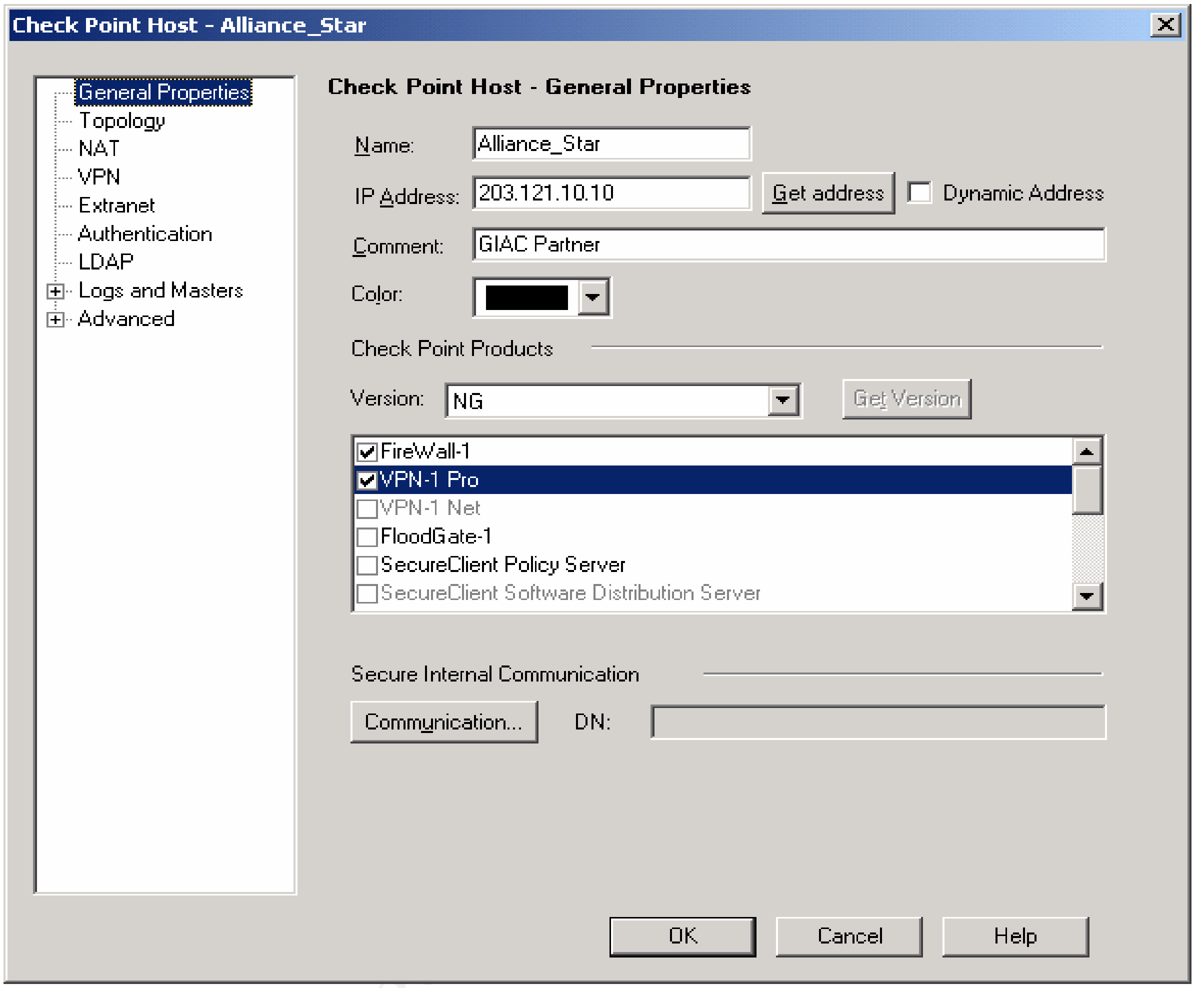
□ VPN-1 & FireWall-1 authentication for SecuRemote/SecureClient (Hybrid Mode)

c) *Establish Partner VPNs equipment*
We checked with our partner and noted that they are using these equipments:-

Name	IP address	VPN Product Type	Encryption setting
Allianz Star Ltd	203.121.10.10	Checkpoint NG VPN-1	3DES
Predictor Ltd	200.50.30.30	Cisco Pix Firewall	3DES

d) *Create Workstation for Partner's VPNs*

Then, we have to create new workstation object for Alliance Star Ltd and Predictor Ltd. Alliance Star workstation will be created as follows:-



Check Point Host - Alliance_Star

Check Point Host - General Properties

Name: Alliance_Star

IP Address: 203.121.10.10 Get address □ Dynamic Address

Comment: GIAC Partner

Color: ■

Check Point Products

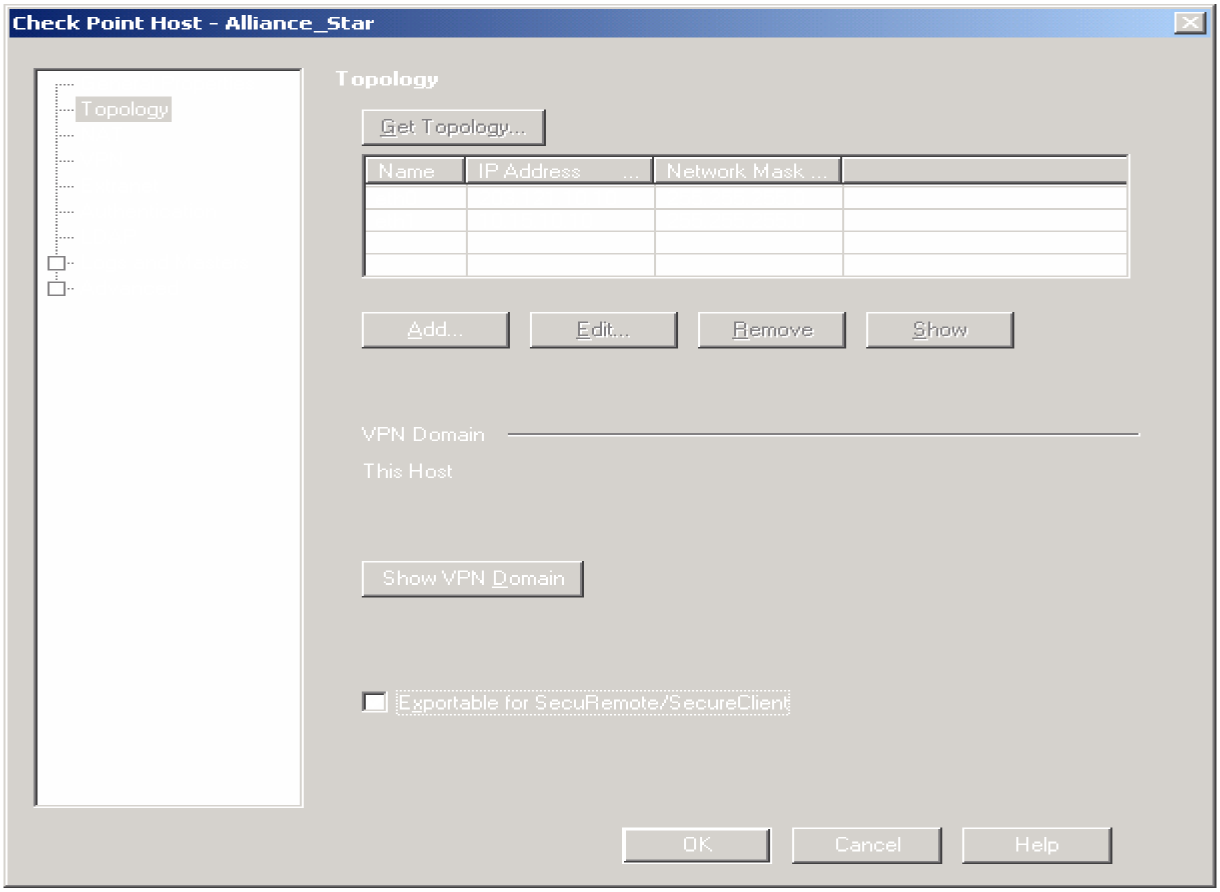
Version: NG Get Version

☑ FireWall-1
☑ VPN-1 Pro
□ VPN-1 Net
□ FloodGate-1
□ SecureClient Policy Server
□ SecureClient Software Distribution Server

Secure Internal Communication

Communication... DN:

Then, defines the interfaces available on the Partner’s gateway. This step is to ensure communication is enable from GIAC network into Alliance Star’s network. (From the workstation properties, select the topology tab – edit – add in interfaces name, IP address and subnet mask)



Check Point Host - Alliance_Star

Topology

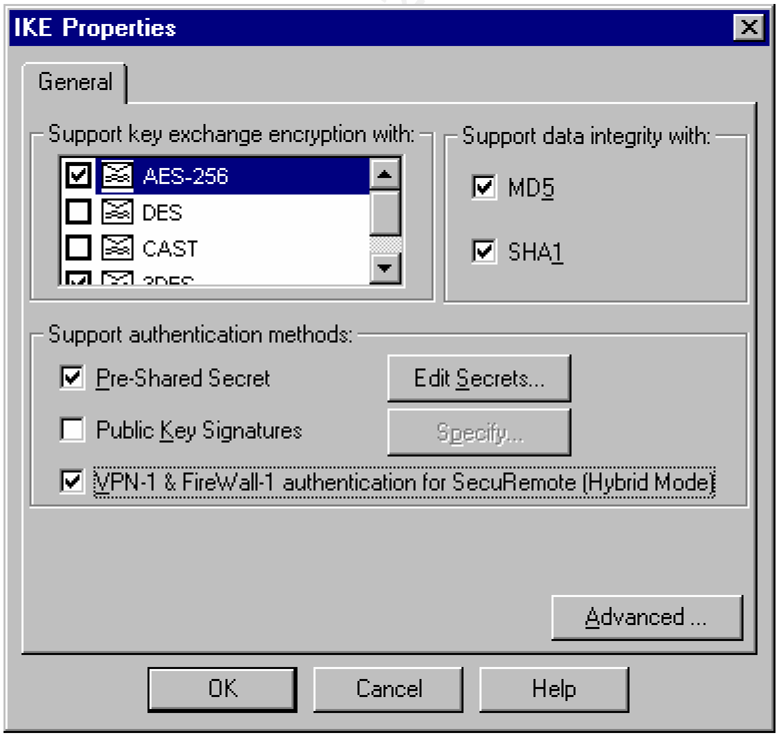
Name	IP Address ...	Network Mask ...	

VPN Domain

This Host

□ Exportable for SecuRemote/SecureClient

Then, select on the VPN tab and check on the IKE encryption tab. Select AES-256 & 3DES encryption and check the "Pre-shared Secret".



IKE Properties

General

Support key exchange encryption with:

☑ AES-256
□ DES
□ CAST
☑ 3DES

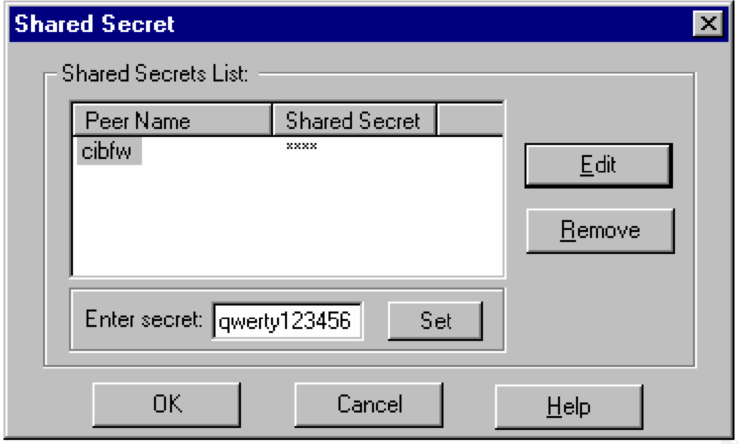
Support data integrity with:

☑ MD5
☑ SHA1

Support authentication methods:

☑ Pre-Shared Secret
□ Public Key Signatures
☑ VPN-1 & FireWall-1 authentication for SecuRemote (Hybrid Mode)

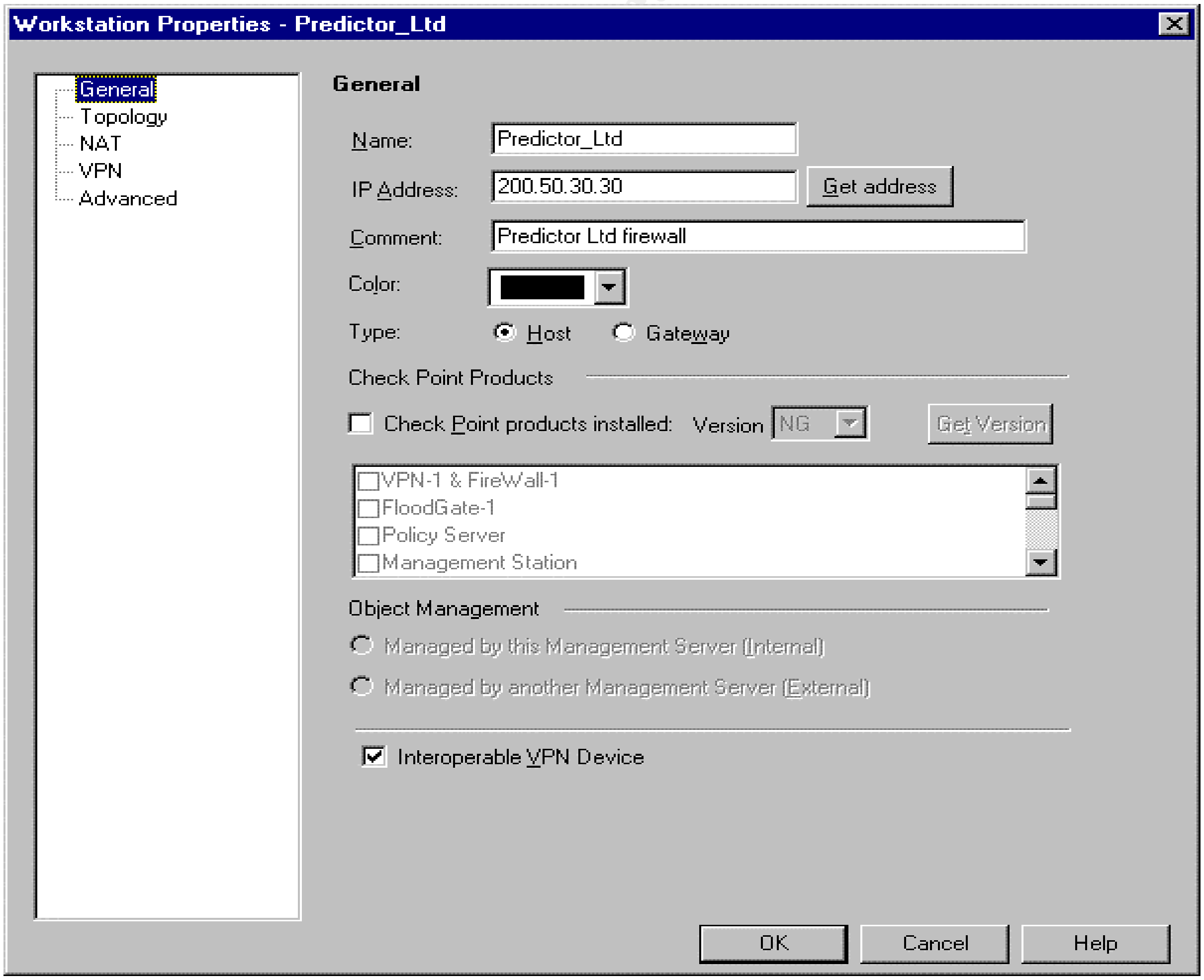
Press on the “Edit Secret” button - highlight the cibfw – press edit and enter the shared secret of **qwerty123456**



Peer Name	Shared Secret
cibfw	****

Enter secret: qwerty123456

Subsequently, we will create the Predictor Ltd’s workstation. As Predictor is using CISCO PIX, the “interoperable VPN device” has to be checked.



Name: Predictor_Ltd

IP Address: 200.50.30.30

Comment: Predictor Ltd firewall

Color: ■

Type: ● Host ○ Gateway

□ Check Point products installed: Version NG

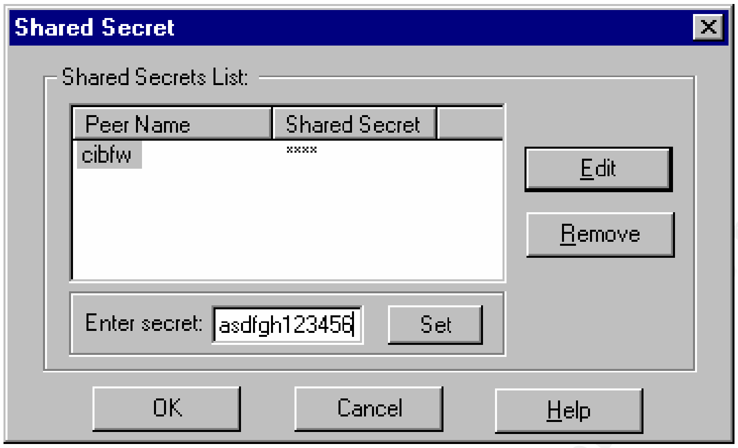
○ Managed by this Management Server (Internal)

○ Managed by another Management Server (External)

☑ Interoperable VPN Device

We add in interfaces for Predictor Ltd's to define the VPN domain. One thing to note is that the topology tab is not available as the partner is not using Checkpoint's product.

Select the VPN tab and check on the IKE encryption tab. Select 3DES encryption and "Pre-Shared Secret". Press the Edit secret button - highlight the GIAC – press edit - enter the shared secret **asdfgh123456.**

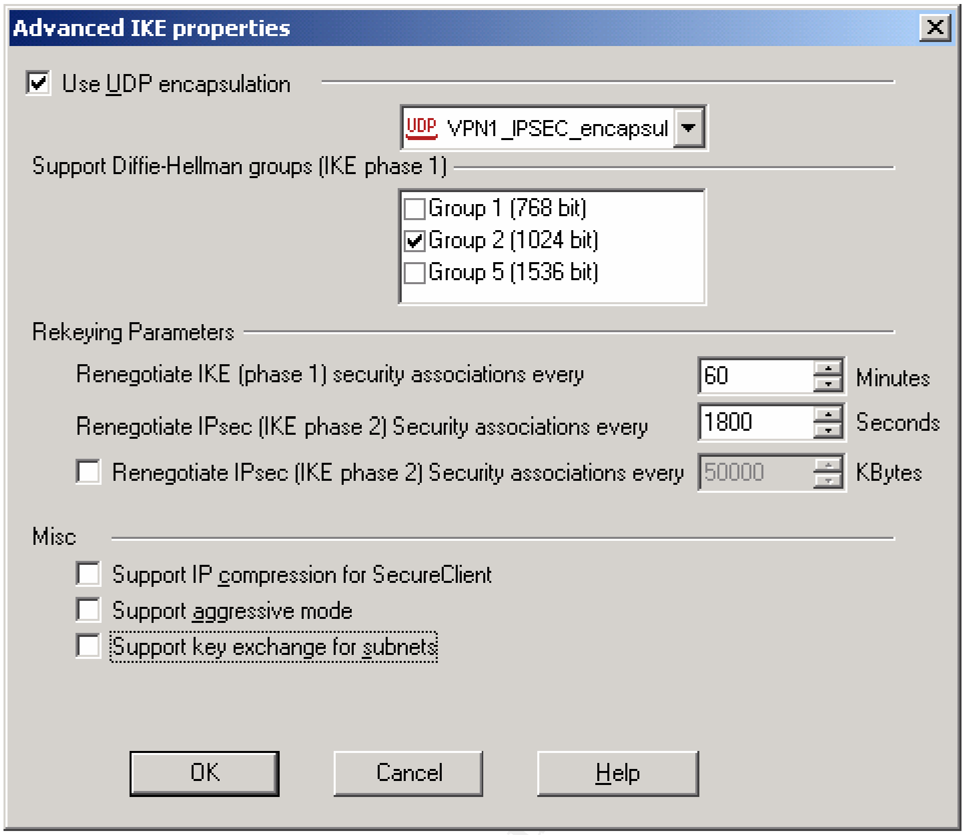

Shared Secret

Shared Secrets List:

Peer Name	Shared Secret
cibfw	****

Enter secret: asdfgh123456

The last thing to perform is to reduce the default renegotiation interval for IKE and IPSEC to 60 minutes and 1800 seconds respectively. This can be done by going to **Manage** – **network object** – select the appropriate **VPN object** – **edit** – select **VPN tab** – **edit IKE properties** – press the **Advanced** button. This setting should apply to the other 2 partner to maintain consistency.



Advanced IKE properties

☑ Use UDP encapsulation

UDP VPN1_IPSEC_encapsul

Support Diffie-Hellman groups (IKE phase 1)

□ Group 1 (768 bit)
☑ Group 2 (1024 bit)
□ Group 5 (1536 bit)

Rekeying Parameters

Renegotiate IKE (phase 1) security associations every 60 Minutes

Renegotiate IPsec (IKE phase 2) Security associations every 1800 Seconds

□ Renegotiate IPsec (IKE phase 2) Security associations every 50000 KBytes

Misc

□ Support IP compression for SecureClient
□ Support aggressive mode
□ Support key exchange for subnets

2.2.5 Checkpoint NG's rules settings

Finally, we defined the access requirements as below in the rule setting:-

No.	Source	Destination	Service	Action	Track	Installation	Time	Comment
1	Any	Checkpoint Firewall	any	Reject	Log	cibfw	Any	Prevent anyone from getting on the gateway
2	Any	DNS	UDP – port 53	Allow	Log	cibfw	Any	Allow DNS servers to communicate via UDP
3	DNS	Any	UDP - port 53	Allow	Log	cibfw	Any	Allow DNS replies on UDP only
4	ISP DNS	DNS	TCP – port 53	Allow	Log	cibfw	Any	Zone transfer
5	DNS	ISP DNS	TCP – port 53	Allow	Log	cibfw	Any	Zone transfer
6	Any	Axent SEF	TCP – port 25	Allow	Log	cibfw	Any	Allow incoming email
7	Axent SEF	Any	TCP – port 25	Allow	Log	cibfw	Any	Allow outgoing email
8	Any	Web server	TCP – port 443	Allow	Log	cibfw	Any	Allow incoming web traffic.
9	Axent SEF	Any	TCP – port 80 & 443	Allow	Log	cibfw	Any	i) Allow GIAC staff web surfing ii) To enable ISS event signature update
10	Supplier IPs	Repository server	TCP – port 22 & 1352	Allow	Log	cibfw	Any	Allow access and deposit of cookies
11	Any	Axent SEF	TCP – Port 110	Allow	Log	cibfw	Any	Allow remote access for email retrieval.
12	Supplier IPs	Checkpoint Firewall	IKE	Encrypt	Log	cibfw	Any	VPN logging
13	Checkpoint Firewall	Supplier IPs	IKE	Encrypt	Log	cibfw	Any	VPN logging
14	Supplier Ips	Checkpoint Firewall	Any	Allow	Log	cibfw	Any	VPN logging

15	Checkpoint Firewall	Supplier IPs	Any	Allow	Log	cibfw	Any	VPN logging
16	Any	Any	Any	Drop	Log	cibfw	Any	Implicit drop – deny and log all other communication.

Assignment 3 Verify the Firewall Policy

One of the key factors to ensure GIAC network's security is of high standard, we need to continuously audit the network resources and implement improvement to it. As described by Mark Hofman **[8]**, audits are an essential part of keeping the environment secure. A good audit will help strengthen the security solution by verifying that what should be implemented is, documentation reflects the environment accurately, and highlights areas of improvement.

Our audit objective, in this case, is to ensure the GIAC network maintains "CIA" framework i.e. confidentiality, integrity and availability. This framework defines:-

a) *Confidentiality* as information is only available to those who authorized to access it.

b) *Integrity* as systems is producing reliable information to user.

c) *Availability* as systems services is available to users with little disruption and high level of continuity.

All these factors assist in preventing major problem to occur and minimize business damage.

3.1 Audit planning

To start an audit, we detailed the audit steps into a written plan. The written plan is discussed and presented in Management meeting. Once the mandate is obtained, we could plan the groundwork which include:-

a) Scheduling resources (eg human and monetary budget)

b) Preparing an audit program to follow throughout the audit.

c) Having a dialogue with IT management to find out their concerns, if any.

As there is budget concern, we only ***focused on auditing the primary firewall***, Checkpoint NG. Our ***audit objective*** is to ***verify the firewall policy***. The budget will be based on labour cost of $100 per hour and it works out to be as follows:-

Task	Hours required	Total Cost ($)
Documentation		
Review network and firewall documentation	3	300
Physical access control		
Review the physical security of firewall	2	200
Logical access control		
Check the security level of firewall's operating system (OS)	2	200
Check the patches and configuration for the firewall.	2	200
Conduct penetration and vulnerability test on the firewall	5	500
Ensure firewall rules are working correctly	8	800
Business Continuity Plan		

Review disaster recovery document and past report	2	200
SUB-TOTAL		**2,400**
Add : 20% allowance for unexpected event		**480**
GRAND TOTAL		**2,880**

3.2 Risk Management

Audit Time and Firewall Backup

To minimize disruption to business operation, the actual audit should take place at the non-peak hour i.e. during the weekend (Saturday and Sunday). The best time suggested is from 12am –6am.

Vulnerabilities test is also carried out against firewall. This can be harmful and might crash the firewall system. Hence, we need to backup the firewall configuration and rule sets into another spare machine. In any event if the firewall failed to function within the tolerance windows (1 hours after the audit), we should revert to the spare machine.

Inform users on the exercise

Users (internal staff, supplier and business partner) are informed of the audit exercise. Performance degradations are expected during the period of time. To mitigate the risk of real attack, we should pre-determine the IP addresses to be used in the audit exercise. An extra staff would be placed to monitor the firewall logs.

It is also important to ensure that adequate of disk qoutas are available on all the devices involved. System and network administrators are present to react to necessary situation arised such as reboot of server if it hang.

Inform Vendors and ISP on the exercise

To manage and contain external uncertainties, all of the software and hardware vendors are informed of the exercise. They are asked to standby and react should there be an emergency. Upstream ISP provider is told as to segregate and deal with non-audit related attack.

3.3 Audit Program

a) Documentation review

- Review the network diagram and placement of firewall.
- Review Checkpoint Firewall manual.
- Review Operating System (Windows 2000) System and Security Manual.
- Determine whether administrator operates within the guidelines.

b) Physical Access Control

- To ensure unauthorized personnel cannot physically gain access to the firewall.

- Review staff entry into the network room.

c) Logical Access Control

- Review software and hardware version of firewall. Determine whether the latest patches are applied.
- Verify the firewall rule base.
- Conduct vulnerabilities test against the firewall.
- Determine whether there is any alternative to overcome these vulnerabilities and minimized its risk.
- Log file are archived and kept.
- Determine changes to the firewall configurations are authorized and tested prior to implementation.

d) Business Continuity

- Review business continuity plan. Determine its thoroughness and its coverage.
- Determine whether past report's failure are rectified.

3.4 Tools used in Audit

We would use the following tools in performing testing against the firewall:-

Scanning Tool	Function
NmapWin v1.3.1	Port scan and OS fingerprinting
Sam Spade v1.14	TCP DNS Zone
Hping2	To perform fragmentation testing

Nmap ("Network Mapper") is an open source utility for network exploration or security auditing. Nmap is chosen because its ability to scan large networks, determine what hosts are available on the network, what services (ports) they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics **[9].** NmapWin v1.3.1 is Nmap Windows edition and available from http://www.insecure.org/nmap.

Sam Spade for Windows (v1.14) is a freeware network query tool that we could use it to perform a DNS zone transfer and a dig. The zone transfer request would inform us all the information a DNS server it has about *a domain*. A dig is an advanced DNS query tool which probe a DNS server for all the information it has about *a host*. Sam Spade could be obtained from http://www.samspade.org/ssw/download.html.

Hping2 is a tool developed and maintained by antirez@invece.org (downloadable from http://www.hping.org/hping2.0.0-rc2.tar.gz). It is used to carry out fragmentation testing. A fragmentation test would able to reassure us that any disallowed packet still not able to pass through the firewall in when the packet is fragmented.

3.5 Audit Result

We carried out test on the firewall and the servers protected by the firewall to verify the rule base and policy.

3.5.1 Documentation Review

We reviewed all the relevant manuals related to firewall and its OS. They are found to be in order and updated. We interviewed the firewall administrator and noted that his practice is in line with the documentation. The firewall administrator had continuously improved himself by:-

a) attending Checkpoint certification course and security seminar in town.
b) subscribing to security mailing list / joining security forum.

3.5.2 Physical Access Control

We evaluated the Checkpoint firewall's physical location. We noted that the firewall and relevant security equipment are located at GIAC IT data center. All the racks contain the security equipment is locked. We also checked all the cable connections and noted that they are not easily accessible for tapping.

Besides that, authorised staff is given magnetic swipe card to enter Data center. There is also closed circuit camera surveillance system to monitor human movement (in and out) from data center. All these records / measures are reviewed by Data center administrator periodically.

3.5.3 Logical Access Control

Security Patches

One of the important steps in auditing firewall is to determine latest patches are applied. There are 2 things we need to check i.e. the operating system and firewall version.

First, we checked the firewall using the "**fw ver**" command line and noted that the firewall is using Features Pack 2. From the System information in Windows 2000, we noted that the OS is running Windows 2000 Server SP 2.

We entered into http://www.checkpoint.com and login into our account with Checkpoint. The latest patches we noted is Features Pack 3. We read *the "What's New in Checkpoint Enterprise Suite NG FP3"* dated August 2002 and noted that no critical issue raised is relevant to us. They further explained installation of patches would be performed if there is any vulnerability pertaining to the FP2 surfaced.

It is also crucial to determine whether Windows 2000 server SP3 is the supported version for Checkpoint NG FP2. We checked the "*Checkpoint Enterprise Suite Next Generation Features Pack(FP) 2 Release Notes"* dated June 2002. We noted that the supported platform for FP2 is Windows 2000 SP1 and SP2. Hence, we feel that it is suffice to have SP2 installed at the time being.

Change Management

In the same time, we reviewed the change management forms, which detailed the changes took place in the firewall rules base. We noted that there is proper testing prior to actual implementation in production environment.

Security audit against Checkpoint NG firewall

Reconnaissance Activity

First, we have to identify the target host. There is 2 general we could adopt ie:-

1) via www.apnic.net (Asia Pacific Network Information Centre) Whois search, we noted that GIAC's IP address range (202.185.236.1 – 202.185.236.14) is registered under GIAC.

2) Alternatively, we could use *nslookup* command to guess GIAC registered IP address range via GIAC domain name:

```
$ nslookup giac.com.my

Server: localhost
Address: 127.0.0.1

Non-authoritative answer:
Name:giac.com.my
Address:       202.185.236.7

> set type=mx
> giac.com.my

Server:localhost
Address: 127.0.0.1

Non-authoritative answer:
giac.com.my perference = 10, mail exchanger = mail.giac.com.my

Authoritative answers can be found from:
giac.com.my              name server = ns1.giac.com.my
mail.giac.com.my         internet address = 202.185.236.13
ns.giac.com.my           internet address = 202.185.236.11
```

It is then noted that GIAC could be occupying 202.185.236.x – 202.185.236.y. Subsequently, we could use the NMAP scanners to check on the IP range and ports opened.

NMAP scanner

Before we proceed, it is essential to understand the types of scanning provided by using Nmap scanner **(Nmap Help File – NmapWin Folder – Option Folders – Scan folder Page)** i.e.:-

1) TCP connect scanning

It identifies all the ports that are listening on the target machine. This scan is very "noisy" in that it generates volume of logs at the target system.

2) TCP SYN (half open) scanning

This type of scanning is "quiet" and begins with sending out SYN packet to a particular port of the target machine. A RST reply will indicate that the port is not listening and a SYN-ACK that it is listening.

3) TCP FIN (stealth) scanning

Known as stealth scan and often used in OS fingerprinting. An RST reply tend to relate the system as NT system.

4) TCP Ping scan

This approach is useful in probing a network whereby ICMP echo packets are not allowed. However, it is extreme noisy and could flag alarm if noted. To initiate the scan, an ACK packet is sent out to random ports on the target machine. If the machine respond with an ACK packet then the port is open or else it would reply RST if it is closed.

5) UDP Scans

To determine whether the target UDP port is listening, we could choose this option. If the UDP port is listening, the test should received no reply. Or else, we should receive an ICMP port unreachable message.

NMAP Audit Result

We placed an laptop outside the primary firewall and performed the NMAP scanning. The target is the Checkpoint firewall (202.185.236.3). The following is the result we obtained:-

Type / Purpose of Scan	Command Issued	Result
TCP Connect Scan	*nmap -sT -vv –P0 -p 1-65535 –T 3 202.185.236.3*	Host (202.185.236.3) appear to be up... good
TCP SYN Scan	*nmap -sS –vv –P0 -p 1-65535 –T 3 202.185.236.3*	1600 ports are scanned but are not shown below are in the state of filtered:- Port State Service 53 Closed Domain
TCP FIN Scan	*nmap -sF –vv -PT -p 1-65535 –T 3 202.185.236.3*	Host seems down. If it is up, but blocking our ping probe, try –PO

TCP ACK Scan	*Nmap –sA –vv –PT –p 1-65535 –T 3*	Host seems down. If it is up, but blocking our ping probe, try –PO
Identify the version of OS	*nmap –sS –P0 -v -O 202.185.236.3*	Too many fingerprint for me to give an accurate OS guess.

Key:-

-P0	:	scan even if host is not reachable via ICMP echo request (i.e. ping)
-sT	:	perform a **TCP connect** scan
-sS	:	perform a **SYN stealth** scan
-sF	:	perform a **FIN stealth** Scan
-sA	:	perform a **ACK** scan
-p 1-65535	:	scan all possible 65k ports
-O	:	guess the target host operating system

Additional test 1 : Ping Test on the firewall

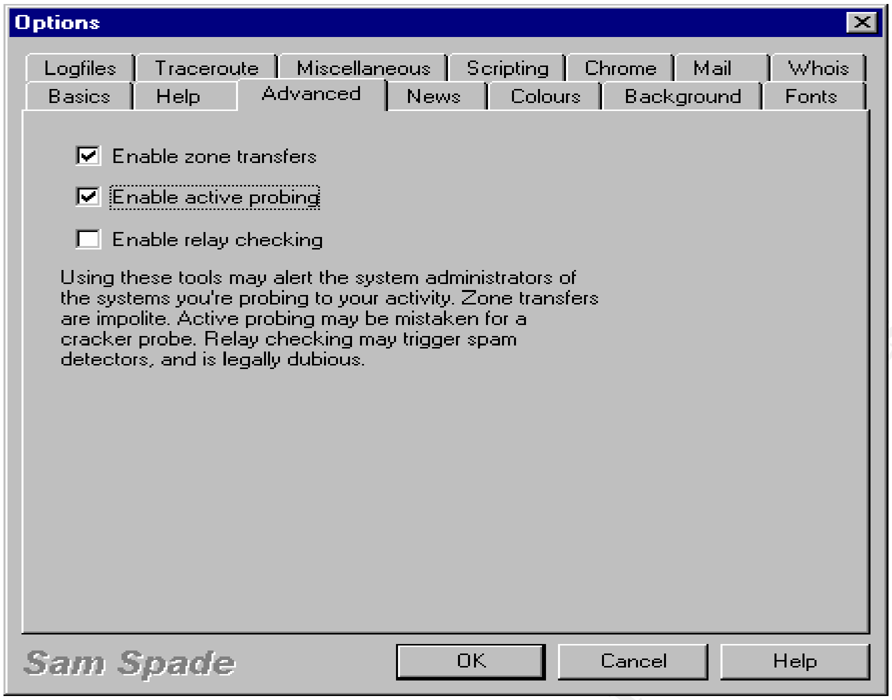
We tried to ping the firewall from internet but noted reply with the message *"Request timed out".* From the firewall log, it showed that the firewall rule base (Rule 1) has dropped the packet.

Additional test 2 : DNS Server Test

To determine whether a zone transfer could be performed from our DNS server, we utilised Sam Spade utility. From the firewall rule base, we noted that our DNS server is allowed to have zone transfers from our ISP, which maintains our secondary DNS server. The rulebase on DNS zone transfer could be found at:-

4	ISP DNS	DNS	TCP – port 53	Allow	Log	cibfw	Any	Zone transfer
5	DNS	ISP DNS	TCP – port 53	Allow	Log	cibfw	Any	Zone transfer

The following screen shot shows how to enable zone transfers. We used a laptop and dial up into internet and try on the Zone transfer test. Then, we come across the following options at Sam Spade set up:-



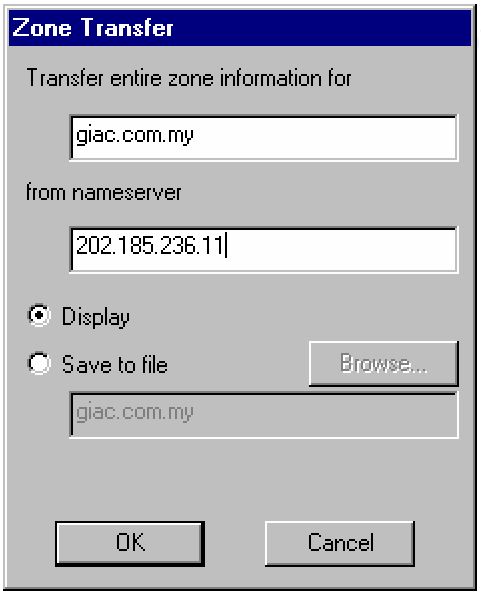
☑ Enable zone transfers

☑ Enable active probing

☐ Enable relay checking

Using these tools may alert the system administrators of the systems you're probing to your activity. Zone transfers are impolite. Active probing may be mistaken for a cracker probe. Relay checking may trigger spam detectors, and is legally dubious.

Eventually, we will attempt the zone transfer test. The following screen shot details which domain and name server to attempt a zone transfer from and display if it was successful.



Transfer entire zone information for: giac.com.my

from nameserver: 202.185.236.11

● Display

○ Save to file: giac.com.my

Results

The zone transfer is unsuccessful. We further tested using nslookup on whether information could be gather about our network and noted the same result.

```
C:\>nslookup
Default Server:  ns1.giac.com
Address:  202.185.236.11

> ls -d giac.com.my
[ns1.giac.com]

*** Can't list domain giac.com: Query refused
```

Additional Test 3 : Further Verification on Firewall Rule Base
We would like to ensure Rule 17 ie the implicit drop rule is working. To do so, we pick rule 10 for verification purpose.

10	Supplier IPs	Repository server	TCP – port 22	Allow	Log	cibfw	Any	Allow access and deposit of cookies

We dial-up into internet and try to connect the repository server using SecureCRT 3.0 software (download from http://www.vandyke.com/download/securecrt/index.html). We are unable to logged onto the repository server. The dropped packet is logged in the Checkpoint firewall.

Additional Test 4 : Fragmentation test
We used Hping2 to test on the firewall block rules (say port 500) by issuing the following command:-
Hping2 –V –I eth0 --data 40 --count 3 --syn –p 500 202.185.236.3
Hping2 –V --frag eth0 --data 40 --count 3 --syn –p 500 202.185.236.3

The result shown no replies, which indicate fragmented packet is not allowed through the firewall.

3.5.4 Business Continuity

We reviewed GIAC's business continuity plan and noted that the recovery plan is well documented. After every disaster recovery exercise, there are post-mortem meeting held. The Business Continuity coordinator would document and highlight the problem encountered. The outstanding issue are rectified in the next exercise.

3.6 Evaluating the results

This is our summary on the gateway firewall functionality. We rated GIAC security policy as "Satisfactory". Our findings noted that the following plus points in the security measures:

1. Firewall Rules

We verified all the firewall rules and noted that they functioning correctly.

2. Logging

Term as important element in auditing and forensic, we noted that Checkpoint firewall logging is properly configured. All the scanning performed are logged and reviewed by firewall administrator periodically.

To complement firewall, the IDS alerting and logging mechanism also managed to capture the scanning activities.

3. Anti Spoofing features and NAT

This feature of the firewall able to identify unauthorised incoming IP packets to an interface (ie IPs that do not belong to that segment) and dropped the packets. NAT provides extra protection by masquerading its internal network and prevent external world (Internet) to know its internal network.

4 Stateful inspection technology

With this technology, it uses patented INSPECT engine which enforces security policy on the gateway on which it resides **[10]**. This engine looks at all communication layers and able to fend off scanning like ACK scan. Unlike a static firewall, it is able to identify and reset the said connection.

On top of this, it is also able to secure the connectionless protocol like UDP used in DNS services without exposing the internal network. This is achieved by having state information maintained for each session that passed through the gateway.

However, there is still possible improvement could be done ie:-

1 Reverse Proxying

By having a reverse proxy server in front of the Internet Web Server, it would introduce additional layer of security. The malicious attempts would first have to compromise the reverse proxy before hitting the real target. In the same time, it also serves to intercept a SYN flood and successfully mitigate its affects.

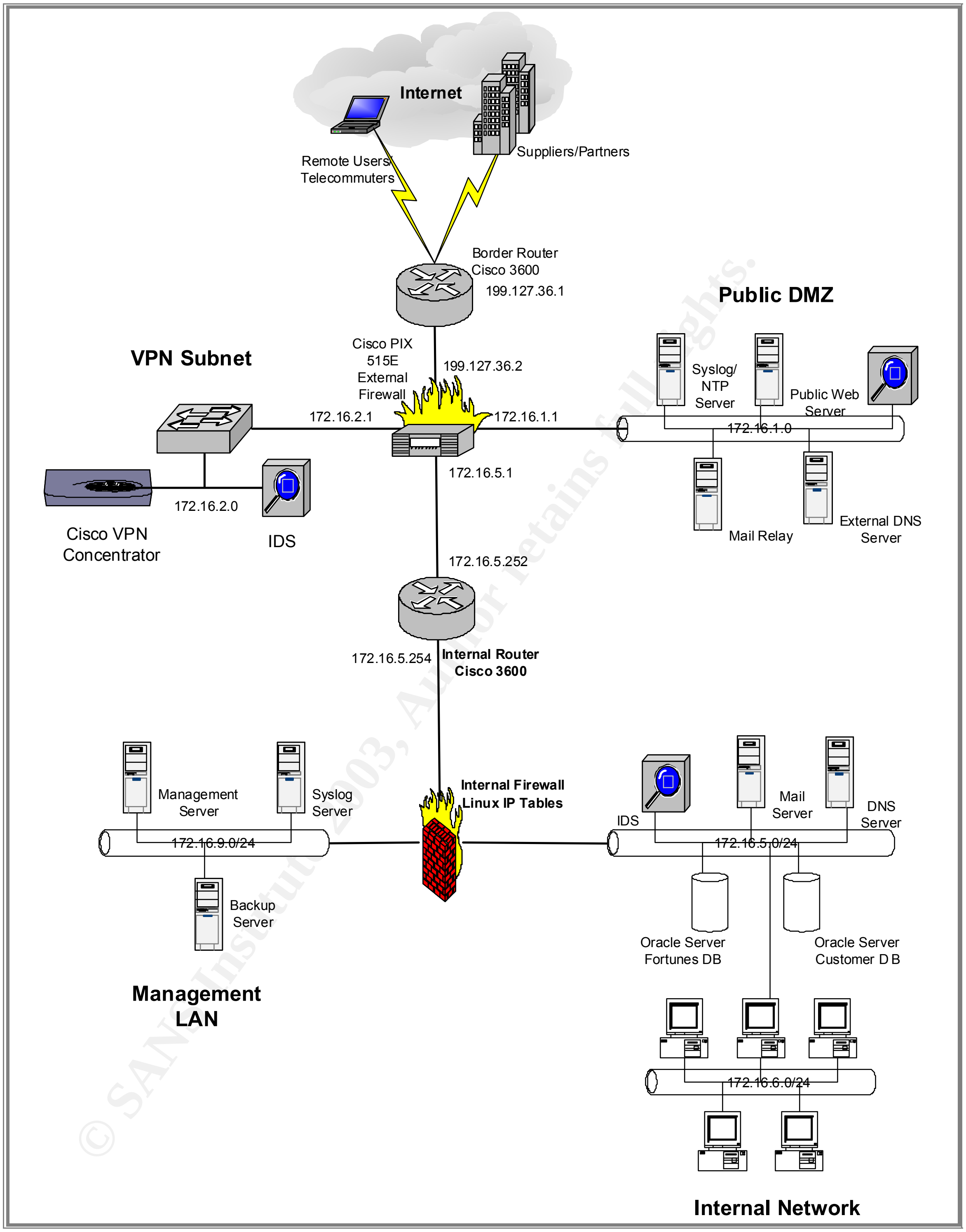
2 Firewall redundancy

If the budget permit, we would like to recommend buying another unit of Checkpoint firewall and implement load balancing and high availability mechanism to optimize overall performance.

Assignment 4 Design Under Fire

4.1 Network Diagram

We have selected Janice Robinson assignment for exploiting her design. The following are the network diagram we extracted from http://www.giac.org/practical/Janice_Robinson-Wells.doc


Internet
Remote Users/
Telecommuters
Suppliers/Partners
Border Router
Cisco 3600
199.127.36.1
Public DMZ
VPN Subnet
Cisco PIX
515E
External
Firewall
199.127.36.2
172.16.2.1
172.16.1.1
Syslog/
NTP
Server
Public Web
Server
172.16.1.0
172.16.5.1
172.16.2.0
Cisco VPN
Concentrator
IDS
Mail Relay
External DNS
Server
172.16.5.252
172.16.5.254
Internal Router
Cisco 3600
Management
Server
Syslog
Server
Internal Firewall
Linux IP Tables
IDS
Mail
Server
DNS
Server
172.16.9.0/24
172.16.5.0/24
Backup
Server
Oracle Server
Fortunes DB
Oracle Server
Customer D B
Management
LAN
172.16.6.0/24
Internal Network

The relevant point of this diagram:-

- The router is Cisco 3620 modular access router running IOS 12.2.
- The external firewall is Cisco PIX 515 running firmware version 6.2.
- IDS is running on Snort Version 1.8.7 on Linux 7.3 server.
- External DNS is running BIND Version 9.2.1 on a Linux 7.3 server.
- External Web server is using Apache Version 2.0.42 on Sun Solaris version 8.
- External Mail server is adopting Sendmail Version 8.12.6 on hardened Linux 7.3 server

4.2 Attack Plan

4.2.1 *Information Gathering*

In this section, there are 3 aspect to our attack ie:-

a) Direct attack on the firewall
b) Distributed Denial of Service (DDOS) Attack on the design.
c) Compromise an internal machine through perimeter

Before we perform an attack on Janice's GIAC network architecture, we need to perform information gathering on her network IP range. Hence, we could use *nslookup* command to gather information about the web server external IP address. Then we could assume about the scope of their IP range. Having the possible IP range will assist us in running Nmap scan to gain OS fingerprint on the network.

4.2.2 *Determine the firewall vulnerabilities*

Subsequently, we could use the following resources to gather vulnerabilities in CISCO firewall.

a) http://online.securityfocus.com/cgi-bin/sfonline/vulns.pl
b) http://icat.nist.gov/icat.cfm
c) http://www.cert.org

4.3 Direct attack against firewall

Janice has deployed Cisco PIX 515 running firmware version 6.2 as the external firewall. Using the firewall model and firmware version, we performed our vulnerability search at :-

i) http://www.kb.cert.org/vuls
ii) http://cve.mitre.org/

Our research suggests that this version of CISCO firewall is potentially exposed to password encryption exploit at http://cve.mitre.org. It could summarise as below:-

Name	CAN-2002-0954 (under review)

Description	The encryption algorithms for enable and passwd commands on Cisco PIX Firewall can be executed quickly due to a limited number of rounds, which make it easier for an attacker to decrypt the passwords using brute force techniques.
Reference	• BUGTRAQ:20020712 The answer to the PIX encryption issue • URL:http://marc.theaimsgroup.com/?l=bugtraq&m=102651159507659&w=2 • VULNWATCH:20020621 [VulnWatch] Weak Cisco Pix Password Encryption Algorithm • URL:http://archives.neohapsis.com/archives/vulnwatch/2002-q2/0121.html

For further detail, we made references to http://archives.neohapsis.com/archives/vulnwatch/2002-q2/0121.html, we noted the following explanation:-

1. Summary

The encryption algorithm used by Cisco PIX Firewall software to encrypt
passwords for "enable" and "passwd" commands is very fast...too fast.
An off-line password guessing attack could be really effective against
this kind of passwords.

2. Systems Affected

Cisco PIX Firewalls (all models and all versions)

3. Details

Cisco PIX passwords are limited to a length of 16 Bytes, so in theory there are 255^16 possible passwords, but in real life there are about 80^16 useful password combinations, take a look at your keyboard to verify, even if strong passwords are used.

Cisco's password encryption is based on base64 encoded MD5 hashes. Routers IOS uses 1000 MD5 Update rounds to make password brute forcing attacks harder, but the PIX firewall uses only one MD5 update and then the digest is base64 encoded.

For base64 encoding Cisco uses the _crypt_to64() Function of the FreeBSD libcrypt library.

Here's the code to compute PIX password hashes:

==

```
MD5Context ctx1;
unsigned char final[MD5_SIZE+1];
unsigned char cleartext [16+1];
unsigned char cisco_encoded [16+1];
memset(cisco_encoded,0,sizeof(cisco_encoded));
memset(cleartext,0,sizeof(cleartext));
strcpy((char*) cleartext,"test");
MD5Init2(&ctx1);
MD5Update2(&ctx1,(unsigned char*) cleartext,16);
MD5Final2(final,&ctx1);
char* p = (char*) cisco_encoded;
_crypt_to64(p,*(unsigned long*) (final+0),4); p += 4;
_crypt_to64(p,*(unsigned long*) (final+4),4); p += 4;
_crypt_to64(p,*(unsigned long*) (final+8),4); p += 4;
_crypt_to64(p,*(unsigned long*) (final+12),4); p += 4;
============================================================
```

Due to some weaknesses in the MD5 hash algorithm (den Boer and Bosselaers found a so called pseudo-collision), there may be more effective attacks in the future.

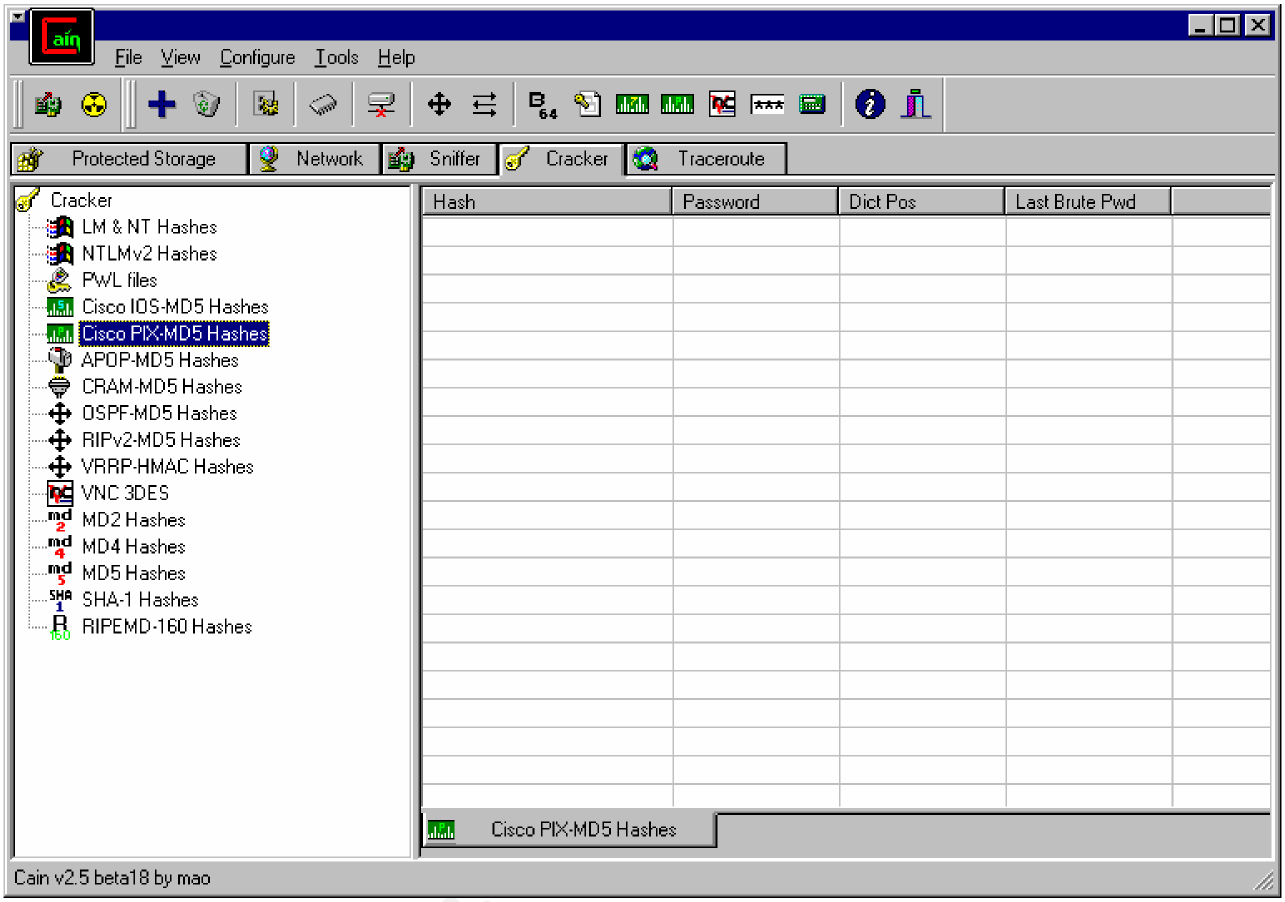
4. Impact

PIX Firewalls are security devices principally used for perimeter security. Once gained access to the Firewall by mean of a valid enable password an intruder could modify its configuration as wanted. In this situation all networks and resources protected by the Firewall could be affected.

Another important impact is due to the ability of recent version of PIX Firewalls softwares (new feature in version 6.2) to sniff traffic. The "capture" command could be used by an intruder to perform a sniffing of remote traffic based on pre-configured ACLs.

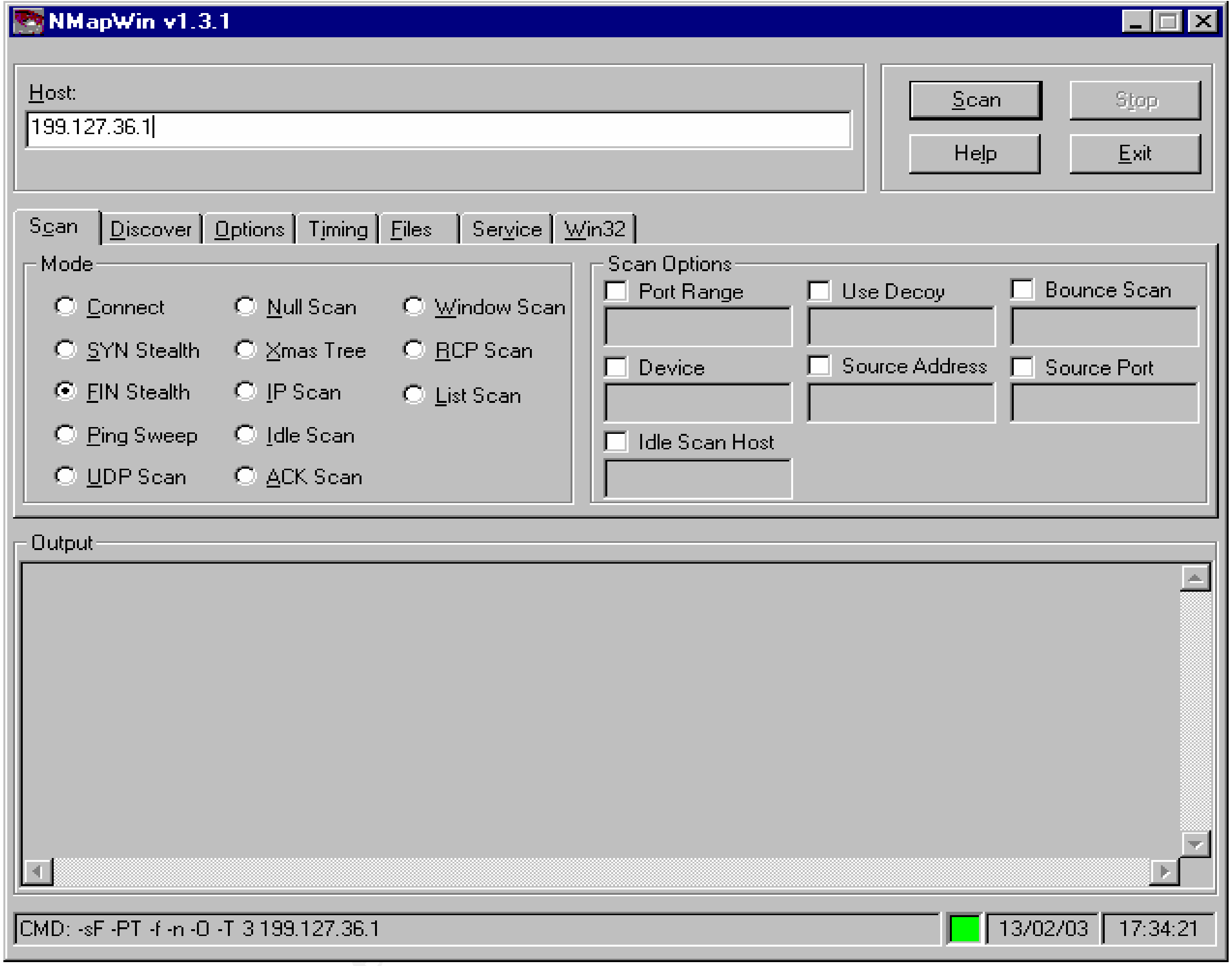
4.3.1 Attack Execution

To perform a brute force attack on the firewall password, we could use Cain & Abel version 2.5 (available from http://www.oxid.it). A snapshot of Cain and Abel:-



But the first step, we need to know whether we could log into the firewall console (be it telnet or SSH). To determine this point, we used Nmap scanner to determine whether the 2 ports are opened.

A snapshot of NmapWin could be seen as follows:-



Host: 199.127.36.1

● FIN Stealth

CMD: -sF -PT -f -n -O -T 3 199.127.36.1

13/02/03 17:34:21

4.3.2 Result

The scanning revealed no port opened. The scanning could be dropped by the firewall (external ACL - rule 9). Alternatively, we should exploit it from internal network.

4.3.3 Countermeasure

- Recommend to use stronger passwords with the full length of 16 bytes.
- To maintain firewall rulebase, to drop any services other than the authorised traffic.
- To use other independent authencation method like TACAACS or RADIUS for password encryption.

4.4 Denial of Service Attack (50 compromised cable mode systems)

The resources we had at hand are 50 compromised cable / DSL modem attached machines on the Internet. From these machines we will use to launch the attack Janice's GIAC web server (Public DMZ). The first step we would embark on is to determine the IP GIAC web server is sitting on and its operating system type (via OS fingerprinting). This could be achieved by using Nmap scanner.

We will then use Tribe Flood Network 2000 (TFN2K) to generate DDOS attack. TFN2K is an advanced tool that instructs multiple computers to flood a target computer with SYN packets, UDP packets, or a SMURF attack.

How TFN2K operate is that it consists of a master and client(s). The master will send commands to multiple agents and instruct them to attack a list of IP addresses. The source IP addresses of the flooded packets can be spoofed or randomized to mask the sending source.

TFN2K could be obtained at:-

i) http://1337.tsx.org/
ii) http://packetstorm.decepticons.org/distributed/tfn2k.tgz

4.4.1 DDOS Attack Execution

We will execute a SYN flood against the external web server at Janice's GIAC network. The command to execute TFN2K is as follows:-

```
# tfn –c5 –f tfn_daemons –I web_IP –p 80
Protocol : random
Source IP : random
Client input : tfn_daemons
TCP port : 80
Target(s) : web IP
Command : commence syn flood, port: 80
Sending out packets
```

The command explained by instructing the TFN daemons **(-f command)** in the list "tfn_daemons" to attack Janice's web server on port 80. This is achieved by having TCP SYN Flood attack launched **(-c5 command)**.

4.4.2 Result

As a result of the attack, Janice's GIAC web server's CPU utilisation would hit maximum and knock down web services. They may need to reboot the host to recover the web service.

4.4.3 Countermeasures

- Consider implement intrusion detection system (eg Snort IDS if budget is concerned, or else Dragon / Realsecure IDS) in the network to detect and counter the TCP Syn Flood.

- Configure border router to perform egress filtering ie preventing bogus traffic from exiting your network. This will prevent others using GIAC network as springboard to launch DDOS.

- Configure border router to filter any reserved IP and private IP from entering the network.

- Disallow unnecessary ICMP, TCP, and UDP traffic entering the network. Preferably only ICMP type 3 (destination unreachable) packets should be allowed. If ICMP cannot be blocked, disallow unsolicited (or all) ICMP_ECHOREPLY packets.

- Be a good neighbour by periodically check and scan GIAC servers for not implanted with TFN2K agents.

4.5 Compromise A Machine through the Perimeter

In normal circumstances, a firewall administrator would define universal access to and from web server (Public DMZ). This might be a chance for us to exploit the web services. From her assignment, she mentioned that she used Apache version 2.0.42 (released on 24/09/02) running on Sun Solaris version 8.

First, we visited http://www.apacheweek.com. We search for security issue related to its current version (v2.0.42) in Issue 311 dated 04/10/2002 and noted 3 security issues:-

- Fix the security vulnerability regarding a cross-site scripting vulnerability in the default error page when using wildcard DNS. CAN-2002-0840
- Fix the exposure of CGI source when a POST request is sent to a location where both DAV and CGI are enabled. CAN-2002-1156
- Fix the security vulnerability regarding some possible overflows in ab.c which could be exploited by a malicious server. CAN-2002-0843

In this case, we concentrate working on CAN-2002-1156 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1156). The explanation of CAN-2002-1156 can be found as follows:-

Name	CAN-2002-1156 (under review)
Description	Apache 2.0.42 allows remote attackers to view the source code of a CGI script via a POST request to a directory with both WebDAV and CGI enabled.

CERT Vulnerability Notes VU#910713 further illustrates this incident impact by saying that remote attackers can obtain the source code of CGI scripts located on affected servers.

Subsequently, we need to understand on POST method and WebDav.

- A POST request is sending data to a script of some kind on the web server. It is usually used with online forms of some type. Originally defined as a request to add this information to the URL to request more information. This method is used extensively in CGI-based systems where the POST data is used as input to a program that will be called by the CGI based systems **[11].**

- WebDav is an extension of HTTP/1.1 protocol. It exists to allow users to create, edit and share documents over the Internet or Intranets using the HTTP protocol. Additional details of WebDav can be found at RFC 2518 **[12].**

4.5.1 Attack Execution

The first step we might need to use tool like Netcat program (available from http://www.atstake.com/research/tools/network_utilities) to confirm the version of Apache and HTTP protocol it is running.

Next, we need to determine whether the WebDav and CGI are running on the Apache server. One of the tricks we tried is to view the httpd.conf file (normally found in /usr/HTTPServer/) to determine which directory WebDav service is enabled. This can be viewed in the following lines:-

```
#add other directives as needed such as Order allow,deny
<IfDefineDAV>
DAVOn
</IfDefine>
</Directory>
```

To ascertain whether which is the CGI enable directory, we presumed that the common one will be available in the directory /cgi-bin where cgi script is normally stored. As such, add in /cgi-bin into httpd.conf and restart the HTTPD service.

However, all these required access into the server. To do so, we need to have root ID privilege and made necessary changes. This can be achieved through social engineering / having sniffer in the network to capture the root password.

4.5.2 Result

With the setting amended, simply run the POST command in command prompt after issuing telnet command (telnet *web server IP* 80). This should be done against the directory containing the CGI and WebDav. From here, we should be able to view the source code of CGI script.

4.5.3 Countermeasure

- Subscribe to security mailing list (eg CERT) and learn about the latest exploit on the running version. Upgrade the Apache server into version 2.0.43
- Having network Intrusion system (in this case, SNORT) in the network assist in detecting and droppring any HTTP_POST traffic if properly configured.
- One could also disable the usage of POST command in the httpd.conf file.

References

[1] Dr. Janice S. Alberts, Defensive Information Warfare, August 1996. http://www.ndu.edu/ndu/inss/books/diw/ch15.html

[2] *Common Ports used by Checkpoint Next Generation (NG),* Solution ID :sk9408. https://support.checkpoint.com/public/idsearch.jsp?id=sk9408&QueryText=%28 %22common%22+AND+%22port%22+AND+%22used%22%29&

[3] http://www.cisco.com/univercd/cc/td/doc/2600.htm#ov

[4] Checkpoint Software "Check Point Software Gains Nearly Ten Percent Additional Market Share in the Worldwide Firewall Market." <http://www.checkpoint.com/press/2000/idc112800.html> (30 May 2001).

[5] Checkpoint NG *Getting Started Guide June 2001* Page 20

[6] John T. Ryan, Security Logs and Checkpoint Firewall-1**,** June 4, 2001. http://rr.sans.org

[7] *Cannot use "undefined" as an authentication method for the user definition*, Solution ID : sk12276. https://support.checkpoint.com/public/idsearch.jsp?id=sk12276&QueryText=%28 %22sk12276%22%29&

[8] Mark Hofman, SANS GCFW Practical Assignment (v1.6a) (August 2001)

[9] http://www.insecure.org/nmap

[10] http://www.sofaware.com/html/tech_stateful.shtm

[11] Jeffrey McKay, “Apache HTTP Server Chunked Encoding”, GCIH dated 20/09/2002. Page 16

[12] http://andrew2.andrew.cmu.edu/rfc/rfc2518.html

Websites references

http://www.samspade.org/ssw/download.html

http://www.hping.org/hping2.0.0-rc2.tar.gz

http://www.checkpoint.com

http://www.vandyke.com/download/securecrt/index.html

http://www.giac.org/practical/Janice_Robinson-Wells.doc

http://online.securityfocus.com/cgi-bin/sfonline/vulns.pl

http://icat.nist.gov/icat.cfm

http://www.cert.org

http://www.kb.cert.org/vuls

http://cve.mitre.org/

http://archives.neohapsis.com/archives/vulnwatch/2002-q2/0121.html

http://www.oxid.it

http://1337.tsx.org/

http://packetstorm.decepticons.org/distributed/tfn2k.tgz

http://www.apacheweek.com

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1156

http://www.atstake.com/research/tools/network_utilities