GCFW Practical

V1.5d

SANS Darling Harbour
February 2001

Darren Bilby
April 2000

Table of Contents

1 Security Architecture

1.1 Assumptions

- With a 200 Million per year expected income the GIAC Enterprises can afford finance two permanent security implementati on professionals for managing the network security systems and one security analyst for auditing of the internal network.
- Although included IDS is not a major part of this assignment. In an environment such as GIAC full host and network based IDS should b e implemented, however, full details on this is outside the scope of this assignment.

1.2 Overview

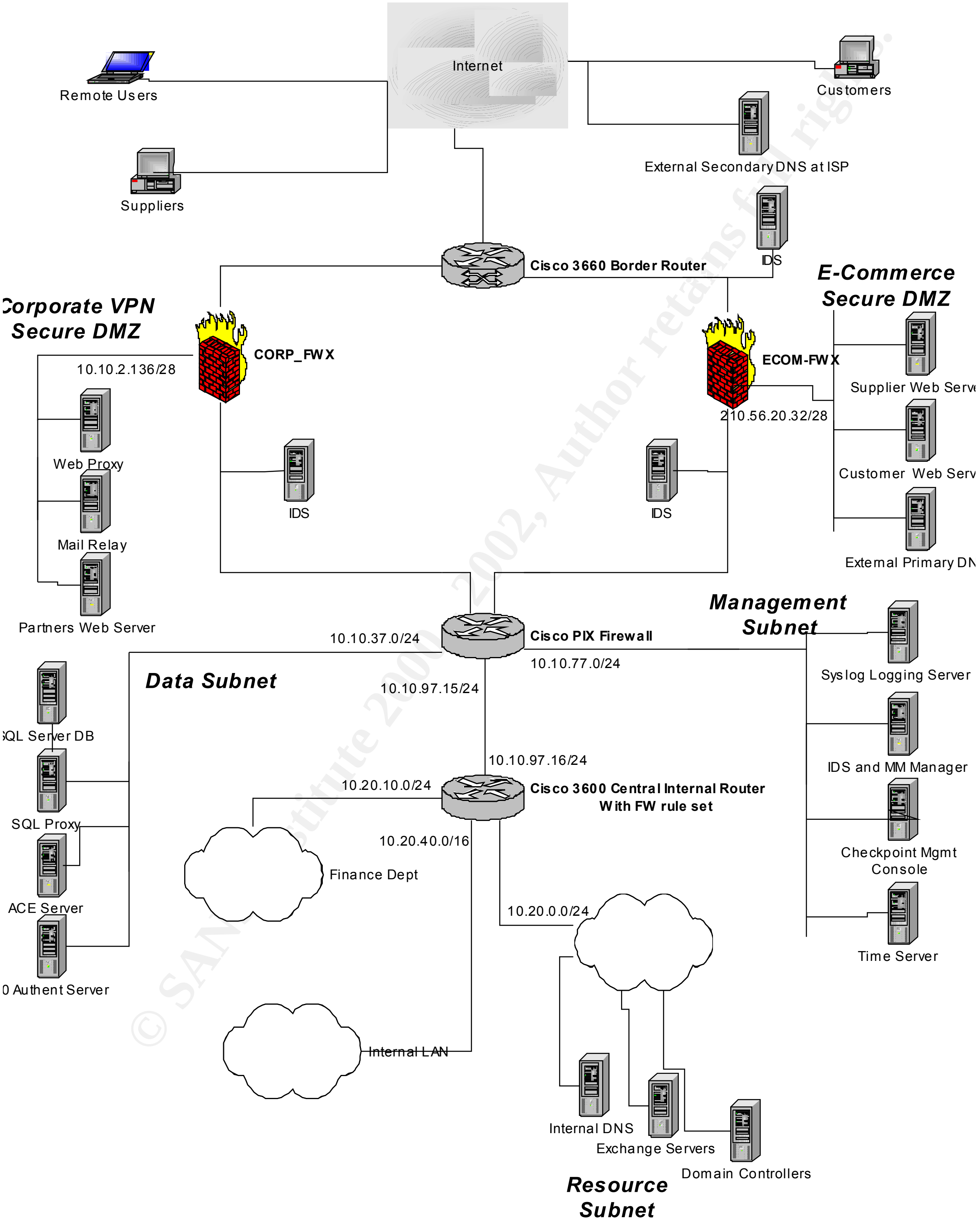
GIAC Enterprises has chosen to adopt a Microsoft, Checkpoint, and Cisco architecture. Adopting this architecture means ignoring the major security, cost and spe ed benefits of free operating systems such as linux and the various BSD environments, as well as the commercial Unix versions. It is believed in this case, however, that these losses are counterbalanced by the advantages of wide industry support, and avail ability of employees for the management of these servers in the current IT security staff shortages.

A dual firewall architecture has been developed utilising Checkpoint VPN -1 and FW-1. A Cisco Pix Firewall sits as a secondary level of defence and acts as a filter for important subnets.

Underlying architecture principles:

1. A layered approach must be used in securing each system; a single vulnerability should never allow compromise of the internal network.
2. All unauthenticated connections coming from the I nternet must go via an intermediary in a secured subnet.
3. All servers must be time synched to ensure log integrity.
4. Logs must be stored securely in real -time in a centralized remote store.
5. Any access to the internal network from a party external to the co mpany must be made using two-factor authentication including a physical token or other device.
6. Where possible internal company traffic should be kept physically separate from public traffic.

1.3 Network Diagram



1.4 Border Environment

1.4.1 BRD_ROUTEX

The border router is a Cisco 3660 running IOS 12.1. This router implements basic anti - spoofing rules including ingress and egress filters and logs to a central syslog server.

It is connected via serial interface on a T3 ~45Mbps connection to GIAC's Internet Service Provider.

1.4.2 DNS2

This is the secondary name server that is hosted by GIAC's ISP. The server runs BIND 8.2.3 release version.

1.5 E-Commerce Environment

1.5.1 ECOM_FWX – Checkpoint FW1 4.1 Service Pack 3

ECOM_FWX runs on a NT 4.0 box and manag es access to and from the E -Commerce secured subnet. It protects the primary external DNS server and both the supplier and customer web servers. All connections directly to the firewall are disabled unless made from the management subnet. This server logs via user-defined logging to a syslog server via the SL4NT service.

1.5.2 SUPP_WEB1 - Supplier Web Server

The supplier web server runs on a fully hot fix patched, hardened NT4.0 SP6a server running IIS4. A custom ASP application handles the management of uploa ding and downloading of cookie files, billing and all supplier relations. The web server runs off an SQL server backend stored in the data subnet.

1.5.3 CUST_WEB1- Customer Web Server

The supplier web server is a fully hot fix patched, hardened NT4.0 SP6a serve r running IIS4. A custom ASP application handles customer queries, purchases and billing. The web server runs off an SQL server backend stored in the data subnet.

1.5.4 DNS1 - External Primary DNS server

The primary DNS server runs BIND 8.2.3 release version. V ersion checks have been disabled via the version command in named.conf.

1.6 VPN and Corporate Environment

1.6.1 CORP_FWX - Checkpoint VPN1 4.1 Service Pack 3

The CORP_FWX server manages access to and from GIAC Enterprises for internal users and trusted third parties. The server has three NICs an external, internal, and one for the secured corporate DMZ.

This server controls all access to the corporate secure DMZ including the proxy server and smtp server. CORP_FWX also controls VPN access to the internal LAN and V PN access for partners to PART_WEB1. All VPN users are authenticated via RSA SecureID token through the radius server in the Data Subnet.

1.6.2 WPROXY – Microsoft Proxy Server 2.0

WPROXY handles web-browsing connections from the internal LAN to the Internet. Rules on CORP_FWX disable all but ports 80 and 443 leaving for the Internet. This server logs via an ODBC connection to the secure logging server in the management subnet.

1.6.3 MMARSH1 - Mail Relay, Virus and Content Management Server

MMARSH1 runs a Marshal Softw are, MailMarshal secure SMTP virus and content management server. It implements reverse DNS to ensure valid remote hosts and is managed via a management console kept in the management subnet.

1.6.4 PART_WEB1- Partners Web Server

The partner web server is a full y hot fix patched, hardened NT4.0 SP6a server running IIS4. A custom ASP application handles customer queries, purchases and billing. This server has been placed in the Corporate DMZ as access to this server is via VPN only. Partners use SecureID343 tokens with SecuRemote to connect to this server via the Internet. The web server runs off an SQL server backend stored in the data subnet.

1.7 Secondary Firewall

A Cisco PIX 525 Firewall running version 5.3(1) has been implemented to manage access between the secu red DMZs, the data subnet, management subnet and the rest of the internal LAN. The PIX 525 has been chosen due to its high throughput and ease of management. The reason another Checkpoint solution has not been adopted is that it is assumed that two firewal l manufacturers are unlikely to have the same vulnerability at the same time. Therefore running different branded firewalls at different protection levels within the organization adds some additional assurance of security. The actual configuration of this device will not be included as part of this assignment.

1.8 Management Environment

The management environment is where all management of perimeter servers is done. Management consoles, configuration, backups and logging are all managed from this subnet. This subnet is locked down extremely tightly with full mac address authentication required on the managed switch it runs off, as well as tight physical controls around the location of the machines in this environment.

1.8.1 LOGSRV1 – NTP, Syslog and SQL Logging Server

This server runs an SQL server for centralized logging from each of the IIS servers. This server also runs a Syslog server, which gathers logs from each of the routers and the Checkpoint firewalls. All logs are securely hashed and synchronized via an NT P service, which is run on this box and updates itself via the Internet.

1.8.2 NPRWLMG - IDS and MM Manager

This box runs the console for both Symantec Netprowler and ITA IDS. It also provides the console for the MailMarshal mail content server.

1.8.3 FW_MNGX – Checkpoint and PIX Management Console

This box is used for managing both the Checkpoint firewalls and the Cisco Pix firewall.

1.9 Intrusion Detection System

Three network NetProwler IDS boxes have been detailed in the main architecture diagram. Each of these boxes runs off an ethertap device, and has no IP bound on the listening interface. A secondary NIC is installed in each IDS agent that runs on a separate network and connects back to the management subnet and the NetProwler management console. These connections have not been shown in the architecture diagram to maintain simplicity.

1.10 Data Environment

The data environment has been created as a separate subnet to allow control of the flow of data around the organization. Most access to the data environment should b e made from other servers and not directly by users, the separate subnet architecture allows enforcement of this.

1.10.1 SQLPROX1 - SQL Proxy

This server acts a protective proxy for the SQL database; all database connections to the main SQL server must pass via this proxy. This proxy filters all potentially malicious SQL statements such as xp_cmdshell or statements that do not meet strict syntax requirements. This aids in preventing application level database attacks.

1.10.2 DBSERV1 - SQL Database

This box runs NT4.0SP6a with hotfixes with MSSQL 2000 server. The SQL server has been locked down as per the recommendations of http://www.sqlsecurity.com/ .

1.10.3 AUTHACEX

This RSA ACE server handles the SecureID authentication of VPN use rs.

1.11 Internal LAN

1.11.1 INT_ROUTEY Cisco 3620 with IOS Firewall

This is a 3620 router with the Cisco IOS Firewall package installed. The firewall package has been added to this router to enable effective filtering between the finance and resource domains and the rest of the internal LAN. This router will run IOS 12.1.

Due to time and resource restraints the configuration of this router is considered outside the scope of this assignment.

1.11.2 Resource Subnet

The resource subnet has been created to allow access contr ols to be applied to all internal servers. With this set-up it will be possible to lock down important file servers and exchange servers to ensure only valid traffic passes between the networks. The resource subnet will contain primarily NT4.0 SP6a servers , which will include domain controllers, Exchange servers, file and print servers, as well as the internal DNS server.

1.11.3 Finance Subnet

As with most organizations, the financial data at GIAC is considered highly confidential. It has therefore been placed wi thin its own subnet to allow effective filtering and protection. The finance subnet will be mainly NT4.0 workstations with a few selected NT4.0 servers.

1.11.4 The Rest

Although further routers and subnets may be set -up to manage the internal LAN, very few ACLs or security measures will be utilised on these and they are therefore considered out of scope for this assignment.

2 Security Policy

2.1 BRD_ROUTEX

The border router chosen is a Cisco 3660 series running IOS 12.1.

The router configuration aims to achieve the following:

- Disable the spoofing of internal addresses from external
- Disable spoofed traffic from leaving the network
- Disable spoofing of non -routable addresses
- Disable all unnecessary services
- Reduce the risk of DoS attacks
- Log to a central server

Note that there are no ACLs implemented to actually block services at the border router. GIAC have decided that it is important that all UDP and TCP traffic be passed and logged at the firewalls. In the future ACLs may be implemented to block common scans on por ts such as 137 or 139, however, at the initial set -up it is desired that the IDS system and Firewalls are given full information on all invalid traffic.

Initial set-up

```
Hostname Brd_RouteX
service password encryption
enable secret ph33r54n5
banner #
******************************************
Warning! Authorized Users Only! All access and attempted
access to this device is recorded. Unauthorized access will
be investigated and prosecuted accordingly.
******************************************
#
```

Set-up logging to remote server

```
logging 10.10.77.5
```

Disable unneeded services

```
no service tcp -small-servers
no service udp -small-servers
no service finger
no ip bootp server
no ip http server
no ip proxy arp

no cdp running                    #disable Cisco discovery protocol
```

```
     no cdp enable
```

Initialise access groups and set as ingress or egress

```
     ip access-group 130 in
     ip access-group 140 out
```

Set ingress filters

```
     access-list 130 deny ip 10.0.0.0 0.255.255.255 any log
     access-list 130 deny ip 192.168.0.0 0.0.255.255 any log
     access-list 130 deny ip 172.16.0.0 0.15.255.255 any log
     access-list 130 deny ip 127.0.0.0 0.255.255.255 any log
     access-list 130 deny ip 210.56.20.0 0.0.0.255 any log #anti spoof
     access-list 130 permit any
```

Set egress filter

```
     access-list 140 permit ip 210.56.20.0 0.0.0 .255 any  #anti spoof
     access-list 140 deny ip any any log
```

Disable potential "bad" traffic

```
     no ip directed-broadcast  #prevent directed broadcasts
     no ip source route              #prevent source routing
     no ip unreachables        #prevent distribution of ICMP errors
     no snmp                   #disable snmp management
```

Set up Serial interface for local management

```
     line con 0
      transport input none
     line aux 0
     line vty 0 4
      password 54n531337
      login
```

2.2 CORP_FWX

2.2.1 Hardware

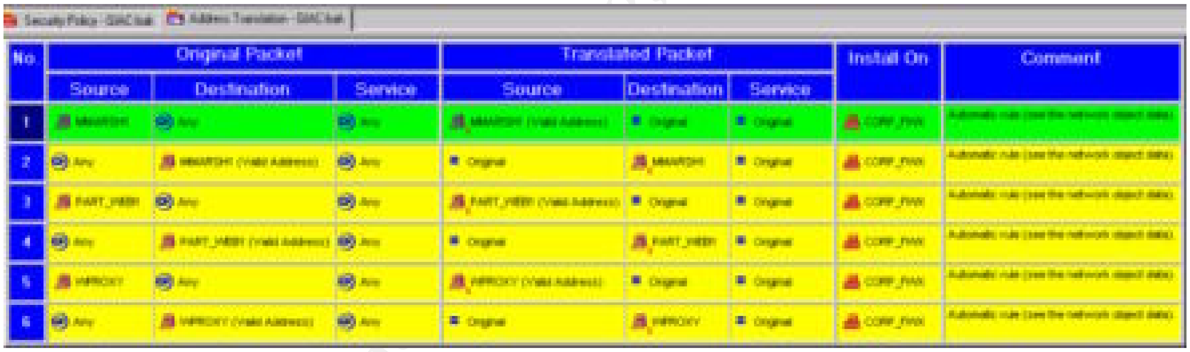
This machine will run as high spec dual processor server. It will contain t hree high-end 10/100 Ethernet NICs.

2.2.2 Base Configuration

ECOM_FWX will run on a base operating system of NT4.0. Despite the speed and stability benefits of a Windows 2000 platform, it is still considered too early to trust this configuration in a production environment. The server will be hardened according to the specifications in "Armoring NT for a Firewall" by Lance Spitzner and with the additional recommendations from Phoneboy (http://www.phoneboy.com/ faq/0073.html).

2.2.3 NAT

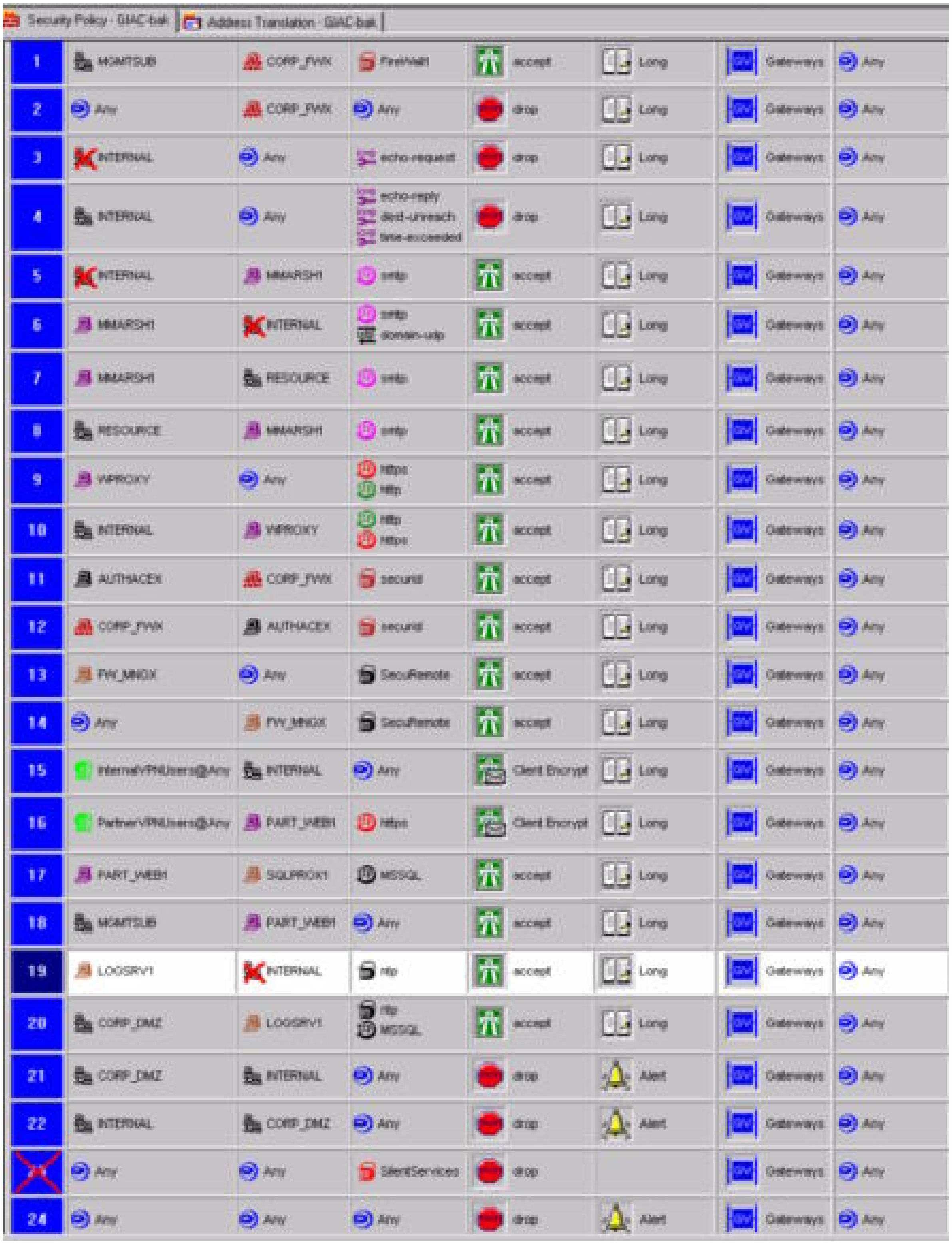
Network Address Translation has been enabled on this firewall to add an additional layer of protection to the secured corporate DMZ. The three servers have been given static NAT address as detailed by the following screenshot.



No	Original Packet			Translated Packet			Install On	Comment
	Source	Destination	Service	Source	Destination	Service		
1	MMARSH1	Any	Any	MMARSH1 (Valid Address)	Original	Original	CORP_FWX	Automatic rule (see the network object data)
2	Any	MMARSH1 (Valid Address)	Any	Original	MMARSH1	Original	CORP_FWX	Automatic rule (see the network object data)
3	PART_WEB1	Any	Any	PART_WEB1 (Valid Address)	Original	Original	CORP_FWX	Automatic rule (see the network object data)
4	Any	PART_WEB1 (Valid Address)	Any	Original	PART_WEB1	Original	CORP_FWX	Automatic rule (see the network object data)
5	WPROXY1	Any	Any	WPROXY1 (Valid Address)	Original	Original	CORP_FWX	Automatic rule (see the network object data)
6	Any	WPROXY1 (Valid Address)	Any	Original	WPROXY1	Original	CORP_FWX	Automatic rule (see the network object data)

2.2.4 Rulebase

The following is the rulebase implemented for CORP_FWX:



Security Policy - GIAC-bak | Address Translation - GIAC-bak

1	MGMTSUB	CORP_FWX	FireWall1	accept	Long	Gateways	Any
2	Any	CORP_FWX	Any	drop	Long	Gateways	Any
3	✗ INTERNAL	Any	echo-request	drop	Long	Gateways	Any
4	INTERNAL	Any	echo-reply dest-unreach time-exceeded	drop	Long	Gateways	Any
5	✗ INTERNAL	MMARSH1	smtp	accept	Long	Gateways	Any
6	MMARSH1	✗ INTERNAL	smtp domain-udp	accept	Long	Gateways	Any
7	MMARSH1	RESOURCE	smtp	accept	Long	Gateways	Any
8	RESOURCE	MMARSH1	smtp	accept	Long	Gateways	Any
9	WPROXY	Any	https http	accept	Long	Gateways	Any
10	INTERNAL	WPROXY	http https	accept	Long	Gateways	Any
11	AUTHACEX	CORP_FWX	securid	accept	Long	Gateways	Any
12	CORP_FWX	AUTHACEX	securid	accept	Long	Gateways	Any
13	FW_MNGX	Any	SecuRemote	accept	Long	Gateways	Any
14	Any	FW_MNGX	SecuRemote	accept	Long	Gateways	Any
15	InternalVPNUsers@Any	INTERNAL	Any	Client Encrypt	Long	Gateways	Any
16	PartnerVPNUsers@Any	PART_WEB1	https	Client Encrypt	Long	Gateways	Any
17	PART_WEB1	SQLPROX1	MSSQL	accept	Long	Gateways	Any
18	MGMTSUB	PART_WEB1	Any	accept	Long	Gateways	Any
19	LOGSRV1	✗ INTERNAL	ntp	accept	Long	Gateways	Any
20	CORP_DMZ	LOGSRV1	ntp MSSQL	accept	Long	Gateways	Any
21	CORP_DMZ	INTERNAL	Any	drop	Alert	Gateways	Any
22	INTERNAL	CORP_DMZ	Any	drop	Alert	Gateways	Any
~~23~~	Any	Any	SilentServices	drop		Gateways	Any
24	Any	Any	Any	drop	Alert	Gateways	Any

2.2.5 Rulebase Breakdown

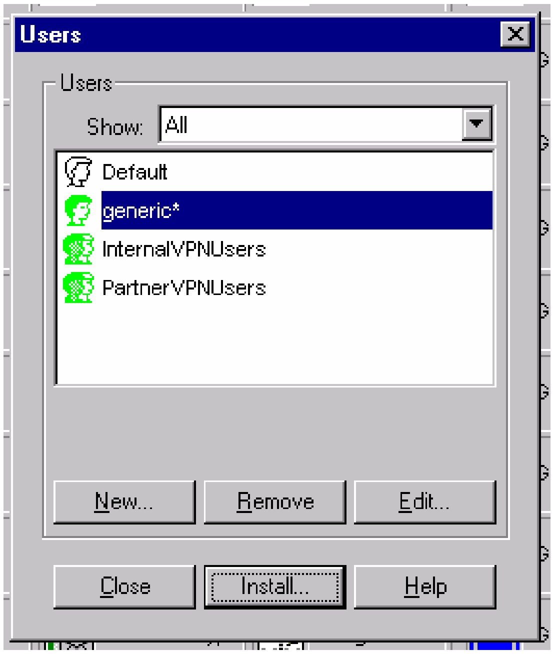
Rule	Description
1	Allow management of the Firewall from the management subnet. The Firewall -1 service group is a built in group that specifies all services required t o manage a Firewall-1 configuration.
2	Stealth Firewall rule to disable all connections directly to the firewall. This is placed after rule 1 to ensure management is possible.
3	Stealth the company by explicitly block all incoming icmp requests
4	Reduce information leakage by blocking all outgoing destination unreachable, time exceeded and echo reply icmp messages.
5	Allow any servers that are not part of the internal network to access the MailMarshal smtp server. This is for the receiving of mail fr om external parties.
6	Allow the Mail Marshal server to send mail to external hosts, and also allow it to do dns lookups to find those hosts.
7	Allow the Mail Marshal server to forward external mail to the internal exchange servers.
8	Allow the excha nge servers in the resource subnet to communicate with Mail Marshal and
9	Allow web traffic to the Internet from the proxy server
10	Allow browser connections from the internal network to the proxy server
11-16	VPN rules – see section below
17	Allow access to the SQL proxy from the partners web server
18	Allow management of the partners web server from the management subnet
19	Allow the NTP server to update itself via the Internet
20	Allow the servers in the corporate DMZ to time synchronize with th e NTP server
21	Protect the internal network from the corporate DMZ
22	Protect the corporate DMZ from the internal network
23	Drop noisy services without logging to reduce noise in firewall logs. Note: this has been disabled as a rule in the initial sta ges of deployment to ensure we have a full picture of all traffic hitting the firewall
24	Final drop everything clean up rule

2.2.6 VPN

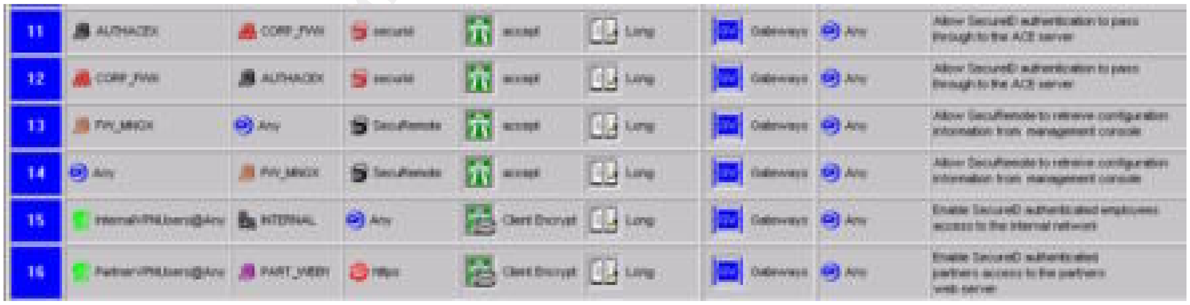
To implement VPN the Checkpoint VPN capabilities will be used. Securemote will be used in conjunction with SecureID toke ns to authenticate users. IKE will be used with DES encryption and MD5 and SHA1 hashing supported.

The guidelines in http://www.phoneboy.com/docs/securemote -securid.pdf will be used for setting up the SecureID authentication.

- The users have been first configured as per below:

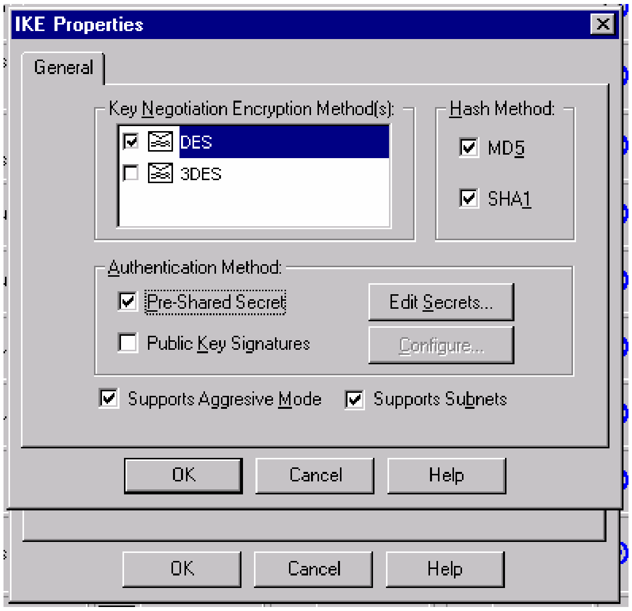


- The following rules have been implemented in the firewall to allow SecureID authentication pass through and SecureRemote configuration information.
  - Rules 11&12 allow authentication communications with the ACE server.
  - Rules 13&14 allow the retrieval of SecureRemote configuration information by the remote clients.
  - Rule 15 allows authenticated employees that are enabled for VPN to access the internal network.
  - Rule 16 allows SecureID authenticated partners to access the partners website.



11	AUTHACEX	CORP_FWX	securid	accept	Long	Gateways	Any	Allow SecureID authentication to pass through to the ACE server
12	CORP_FWX	AUTHACEX	securid	accept	Long	Gateways	Any	Allow SecureID authentication to pass through to the ACE server
13	FW_MNGX	Any	SecuRemote	accept	Long	Gateways	Any	Allow SecuRemote to retrieve configuration information from management console
14	Any	FW_MNGX	SecuRemote	accept	Long	Gateways	Any	Allow SecuRemote to retrieve configuration information from management console
15	InternalVPNUsers@Any	INTERNAL	Any	Client Encrypt	Long	Gateways	Any	Enable SecureID authenticated employees access to the internal network
16	PartnerVPNUsers@Any	PART_WEB	https	Client Encrypt	Long	Gateways	Any	Enable SecureID authenticated partners access to the partners web server

The Firewall object has been configured for IKE, using DES (SecureID does not support 3DES). Both SHA1 and MD5 will be supported as hash algorithms, and both aggressive mode, and subnets are supported by the SecuRemote client.



Key Negotiation Encryption Method(s):
☑ DES
□ 3DES

Hash Method:
☑ MD5
☑ SHA1

Authentication Method:
☑ Pre-Shared Secret — Edit Secrets...
□ Public Key Signatures — Configure...

☑ Supports Aggresive Mode
☑ Supports Subnets

Configuration of the actual SecuRemote client is considered outside the scope of this assignment, however the fore mentioned document on the PhoneBoy site could give guidance for this.

Although exact numbers of VPN clients has not been specified it is expected that the ECOM_FWX will handle the load. If VPN requirements increase in the future the use of a hardware encryption card may become a possibility.

2.3 ECOM_FWX

2.3.1 Hardware

This machine will run as high spec dual processor server. It will contain three high end 10/100 Ethernet NICs.

210.56.20.104 EXT

210.56.20.33 DMZ

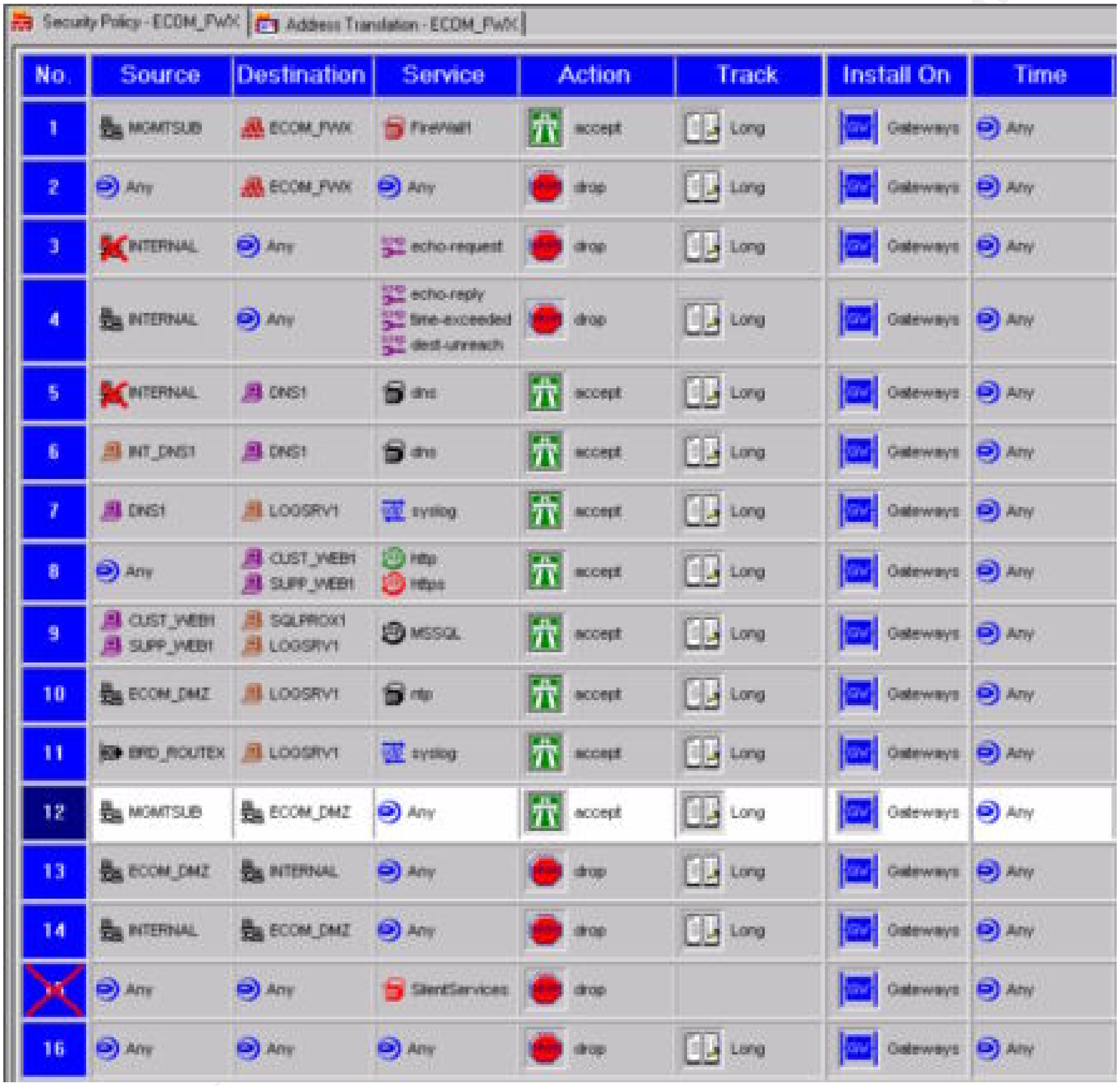
10.10.8.115 INT

2.3.2 Base Configuration

ECOM_FWX will run on a base operating system of NT4.0. As with CORP_FWX, despite the speed and stability benefits of a Windows 2000 platform, it is still considered too early to trust this configuration in a production environment. The server will be hardened according to the specifications in "Armoring NT for a Firewall" by Lance Spitzner and with the additi onal recommendations from Phoneboy (http://www.phoneboy.com/faq/0073.html).

2.3.3 Rulebase

Note that while the both the ECOM_FWX and CORP_FWX will be managed from the same console with the same policy. The rule base for the two firewalls have been split for clarity in the diagrams included in this assignment.



No.	Source	Destination	Service	Action	Track	Install On	Time
1	MGMTSUB	ECOM_FWX	FireWall1	accept	Long	Gateways	Any
2	Any	ECOM_FWX	Any	drop	Long	Gateways	Any
3	✗ INTERNAL	Any	echo-request	drop	Long	Gateways	Any
4	INTERNAL	Any	echo-reply time-exceeded dest-unreach	drop	Long	Gateways	Any
5	✗ INTERNAL	DNS1	dns	accept	Long	Gateways	Any
6	INT_DNS1	DNS1	dns	accept	Long	Gateways	Any
7	DNS1	LOGSRV1	syslog	accept	Long	Gateways	Any
8	Any	CUST_WEB1 SUPP_WEB1	http https	accept	Long	Gateways	Any
9	CUST_WEB1 SUPP_WEB1	SQLPROX1 LOGSRV1	MSSQL	accept	Long	Gateways	Any
10	ECOM_DMZ	LOGSRV1	ntp	accept	Long	Gateways	Any
11	BRD_ROUTEX	LOGSRV1	syslog	accept	Long	Gateways	Any
12	MGMTSUB	ECOM_DMZ	Any	accept	Long	Gateways	Any
13	ECOM_DMZ	INTERNAL	Any	drop	Long	Gateways	Any
14	INTERNAL	ECOM_DMZ	Any	drop	Long	Gateways	Any
✗ 15	Any	Any	SilentServices	drop		Gateways	Any
16	Any	Any	Any	drop	Long	Gateways	Any

2.3.4 Rulebase Breakdown

Rule	Description
1	Allow management of the Firewall from the management subnet. The Firewall -1 service group is a built in gr oup that specifies all services required to manage a Firewall -1 configuration.
2	Stealth Firewall rule to disable all connections directly to the firewall. This is placed after rule 1 to ensure management is possible.
3	Stealth the company by explicit ly block all incoming icmp requests
4	Reduce information leakage by blocking all outgoing destination unreachable, time exceeded and echo reply icmp messages.
5	Enable external parties to make DNS queries on our primary DNS server
6	Enable name lookups and domain transfers from the internal DNS server to the external DNS server
7	Enable DNS1 to Syslog to the logging server stored in the management subnet
8	Enable internal and external people to access the http and https web sites on the customer and supplier websites.
9	Enable the customer and supplier web sites to retrieve data via the SQL proxy in the data subnet, and also enable ODBC logging to the SQL logging server in the management subnet
10	Enable all servers in the E -Commerce DMZ to access th e NTP server
11	Enable the border router to syslog to the logging server
12	Enable the machines in the management subnet to manage the machines in the E - Commerce DMZ
17	Allow access to the SQL proxy from the partners web server
18	Allow management of t he partners web server from the management subnet
19	Protect the internal network from the E -Commerce DMZ
20	Protect the E-Commerce DMZ from the internal network
21	Drop noisy services without logging to reduce noise in firewall logs. Note: this has bee n disabled as a rule in the initial stages of deployment to ensure we have a full picture of all traffic hitting the firewall
22	Final clean up – drop everything rule

3 Security Audit

3.1 Plan

The plan for auditing the perimeter is to test the network using f reely available tools, testing each of the implemented access control rules independently moving through each of the network devices.

The assessment will be done over three nights, starting as customer traffic declines at around 7pm through to 5am in the morning. Installation of the hubs and ethertap devices will mean brief network outages, and performance will be degraded during some of the scans. It is therefore recommended that valued customers that often make transactions during these times are forewarned of the potential issues.

Due to the complexity of the architecture, and multiple paths through firewalls a comprehensive audit will require a lot of effort. I expect the resource of at least two fully qualified security professionals will be required for the three ten hour evening shifts at a cost of US$150 per hour each (assuming the use of external consultants).

The following will also be required to perform the assessment:

- Full network diagrams including IP addresses and OS patch information.
- Access passwords for viewing of the configuration files of each network device.
- Three laptops running a recent distribution of linux with the specified tools installed.
- 3 basic hubs and two ethertap devices.

3.1.1 Scope

This audit will cover the following devices:

- BRD_ROUTEX
- ECOM_FWX
- CORP_FWX
- INT_FWX

3.1.2 Tools

- Nmap – testing port controls.
- Netcat – for checking banners.
- Nessus – testing for common vulnerabilities.
- Tcpdump – assessing the traffic passing through a device.
- Ethereal – assessing the traffic graphically.
- Hping2 – testing firewall rules under custom generated packets.
- Perl - for automating scripted scans.
- Cisco Pix and Checkpoint Management Consoles – for viewing generated log entries.

3.2 Tests

For each device there is a set of things that needs to be tested. T he pseudo tests and the way to implement these tests are detailed below. Note that each command set starts with a baseline test to ensure there is connectivity; the first test should always succeed.

3.2.1 Ingress Spoof Filtering

This test ensures that spoofed I P addresses are filtered correctly coming from the unprotected network into the protected network by utilizing ethereal on the internal side of the device to listen for traffic, and using Nmap to scan from the external side. Note: due to the spoofed sources, Nmap will detect that all ports are filtered on every network device.

Commands used:

```
nmap –sS –P0 –v –T Insane –p <internalhost1 allowed port>  -S
<validexternalhost>  -i eth0 <internalhost1>
nmap –sS –P0 –v –T Insane –p <internalhost1 allowed port>  -S
<internalhost1>  -i eth0 <internalhost1>
nmap –sS –P0 –v –T Insane –p <internalhost1 allowed port>  -S
<internalhost2>  -i eth0 <internalhost1>
nmap –sS –P0 –v –T Insane –p <internalhost1 allowed port>  -S <127.0.0.1>
-i eth0 <internalhost1>
nmap –sS –P0 –v –T Insane –p <internalhost1 allowed port>  -S
<192.168.0.1>  -i eth0 <internalhost1>
nmap –sS –P0 –v –T Insane –p <internalhost1 allowed port>  -S <172.16.0.1>
-i eth0 <internalhost1>
nmap –sS –P0 –v –T Insane –p <internalhost1 allowed port>  -S <10.1.1.1>  -
i eth0 <internalhost1>
```

Once these commands have been run, the output of Ethereal should be checked to ensure only the valid traffic passed through the filtering device. The devices logs should then be checked to ensure correct logging of each event has taken place.

3.2.2 Egress Spoof Filtering

This test ensures that spoofed IP addresses are filtered correctly coming from the protected network going towards the unprotected network. The anti -spoofing rule usually involves disallowing all traffic except that in the s ubnet mask of the participating interface. A list of 20 external addresses (including standard non -routable addresses) should be used as the spoofed source for this test. By using ethereal on the external side of the device to listen for traffic, and Nmap from the internal side we can test whether this rule is successful in it's filtering.

Commands used:

```
nmap –sS –P0 –v –T Insane –p <externalhost1 allowed port>  -S
<validinternalhost>  -i eth0 <externalhost1>
nmap –sS –P0 –v –T Insane –p <externalhost1 allowe d port> -S
<externalhost1>  -i eth0 <externalhost1>
nmap –sS –P0 –v –T Insane –p <externalhost1 allowed port>  -S
<externalhost2>  -i eth0 <externalhost1>
```

Once these commands have been run, the output of Ethereal should be checked to ensure only the valid tr affic passed through the filtering device. The devices logs should then be checked to ensure correct logging of each event has taken place.

3.2.3 Device Service Availability

This test will test the services available directly on the device. Nmap will be used to scan the device for TCP and UDP services. The laptop used for scanning will be placed in the same network segment as the device to be scanned. In the case where the device has multiple interfaces and is therefore in multiple network segments, we will attac h to each segment and scan.

Commands used:

```
nmap –sS –P0 –p 1-65535 –T Insane <targetdevice>
nmap –sU –P0 –p 1-65535 –T Insane <targetdevice>
```

The output of Nmap will show the services that are available, this should be checked against the device configura tion to ensure all necessary services are responding and all unnecessary services are disabled. Log files on the device should also be reviewed to ensure that correct logging is taking place on the blocked or dropped packets.

3.2.4 Service Availability

This test will ensure that the device is effectively blocking all but allowed services through to the network devices it is protecting. Again, Nmap will be used to scan for open services. Note that –P0 is used again as icmp echo is disable on a number of these de vices to reduce information leakage. The laptop used for scanning will be placed in the same network segment as the external interface of the filtering device. Where there are multiple external network segments the scan will be performed from each of them.

Commands used:

```
nmap –sS –P0 –p 1-65535 –T Insane <targethost>
nmap –sU –P0 –p 1-65535 –T Insane <targethost>
```

The output of Nmap will show the services that are available; this should be checked against the rules on the filtering device to ensure all nec essary services are responding and that all unnecessary services are disabled. Log files on the filtering device should be reviewed to ensure that correct logging is taking place on the blocked or dropped packets.

3.2.5 Fragmentation

Hping2 will be used to tes t how the device handles fragmented packets. A valid service, which is normally blocked by the filtering device, will be targeted. An Ethereal listener will be set on the internal side of the filtering device, and hping2 will be run from the external side.

Commands used:

```
hping2 –V -I eth0 --data 40 --count 3 --syn –p <valid filtered target
service> <target>
hping2 –V --frag -I eth0 --data 40 --count 3 --syn –p <valid filtered
target service> <target>
```

If the filtering rule is set correctly, the first comma nd should be denied, nothing will return, and Ethereal will not see any traffic. However, if the filtering device does not handle the fragmentation correctly, the second command should produce traffic that is visible by Ethereal on the internal device.

3.2.6 ICMP management

Hping2 will be used again, but this time to test for handling of ICMP. A loop will be run to send using each of the valid icmp protocol and code pairs. A listener will be placed on the internal side of the filtering device, and hping2 will b e run from the external side targeting a machine on the internal.

Commands used:

```
hping2 -V --icmp --count 3 --icmp-proto <proto> --icmpcode <code> -I eth0
<target>
```

The results picked up with Ethereal will show the icmp packets that made it through the filtering device. Log files on the filtering device should also be reviewed to ensure that correct logging is taking place on the blocked or dropped packets.

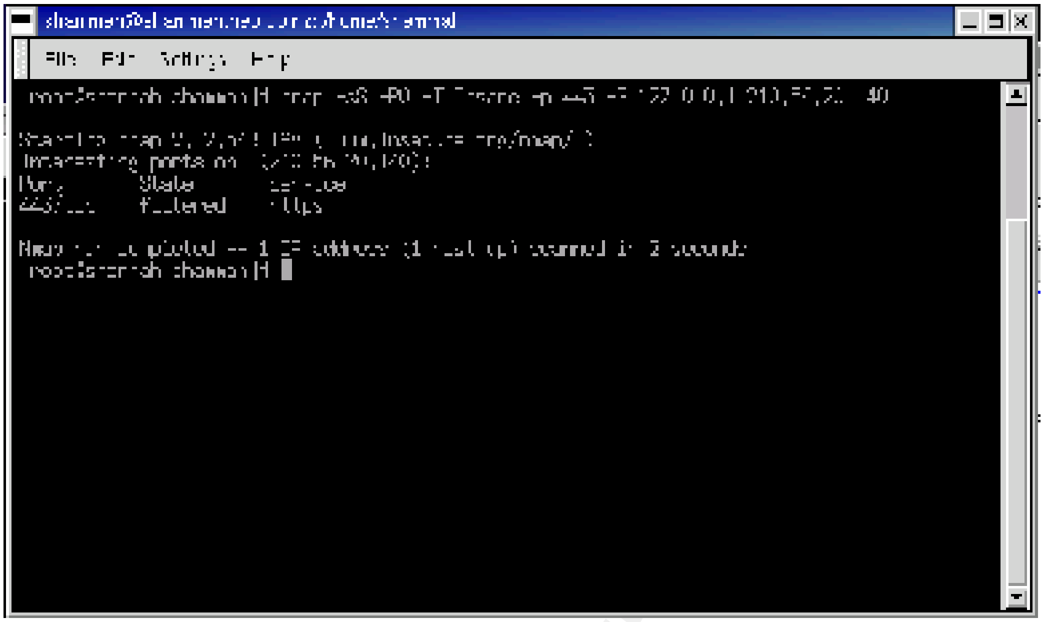
3.2.7 Common Vulnerabilities

As part of the Audit, Nessus will be used to scan for common vulnerabilities on both the filtering device, and the services that they protect. As the previous tests have determined the exact services that are running on each host, this information can be fed into Nessus to speed up its discovery process.

3.3 Implementation of Audit on ECOM_FWX

As discussed in the plan, a review of each of the filtering devices is a three -day job for two people. Therefore completing that audit as part of this assignment will not be possible. However, a full audit of the ECOM_FWX firewall will be con ducted. The results from the audit including screenshots is shown below. Note that screenshots and details of each part of the audit filled over 30 pages and therefore only a sample is included here.

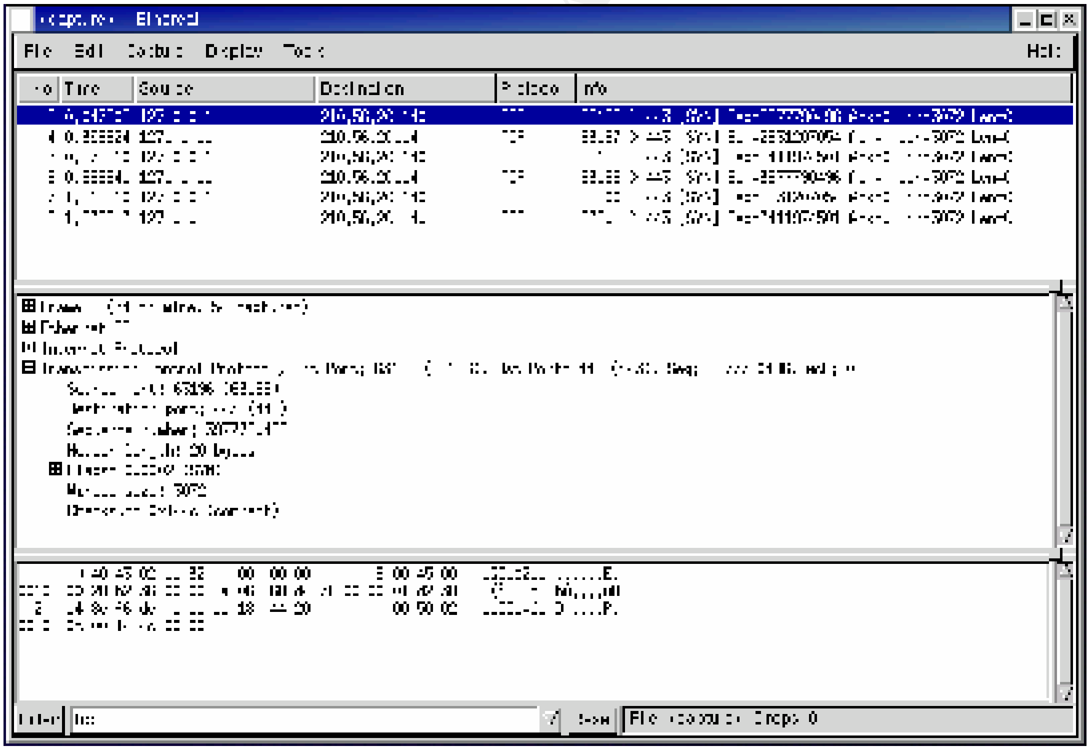
3.3.1 Ingress filtering



```
[illegible] nmap -sS -P0 -T Insane -p 443 -S 127.0.0.1 210.56.20.[illegible]

Starting nmap [illegible]
Interesting ports on [illegible] (210.56.20.[illegible]):
Port       State       Service
443/tcp    filtered    https

Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds
[illegible]
```



File Edit Capture Display Tools Help
No. Time Source Destination Protocol Info

Ingress filtering was tested from an external Internet host with:

```
nmap -sS -P0 -v -T Insane -p 80 -S 127.0.0.1 -i eth0 210.56.20.38
```

As you can see from the screenshots, even though the service is valid and should be open it is shown as filtered proving the activation of the spoof filteri ng on the ECOM_FWX for the localhost 127.0.0.1. The same results were found for each of the other non -routable addresses and the internal network addresses.

3.3.2 Egress Filtering

As with the ingress filtering test Ethereal showed traffic in the default test but showed no traffic passing through in when a spoofed external address was given with the Nmap –S option.

An example of this test is a packet from the internal interface spoofed with the source address of the SUPPWEB1 server going to a web server at 209.150.158.10.

```
    nmap -sS -P0 -v -T Insane -p 80 -S 210.56.20.38  -i eth0 209.150.158.10
```

The spoofed address attempt was logged with the following log entry by ECOM_FWX:

```
    "20850"  "16Apr2001"  "10:26:17"  "El90xnd2"  "10.10.8.115"  "alert"
    "drop"  "http"  "10 .10.8.69"  "203.29.160.4"  "2"  "0"  "4452"  ""  ""
    ""  ""  ""  ""  ""  ""  ""  "firewall"  " h_len 24 ip_vers 4"
```

Note that it was dropped by rule 0, the rule that is stated for anti-spoofing violations.

3.3.3 Device Service Availability

Device service availability was tested using the following commands:

From the Internet:

```
    nmap -sS -P0 -p 1-65535 210.56.20.104
    nmap -sU -P0 -p 1-65535 210.56.20.104
```

From the internal network:

```
    nmap -sS -P0 -p 1-65535 10.10.8.115
    nmap -sU -P0 -p 1-65535 10.10.8.115
```

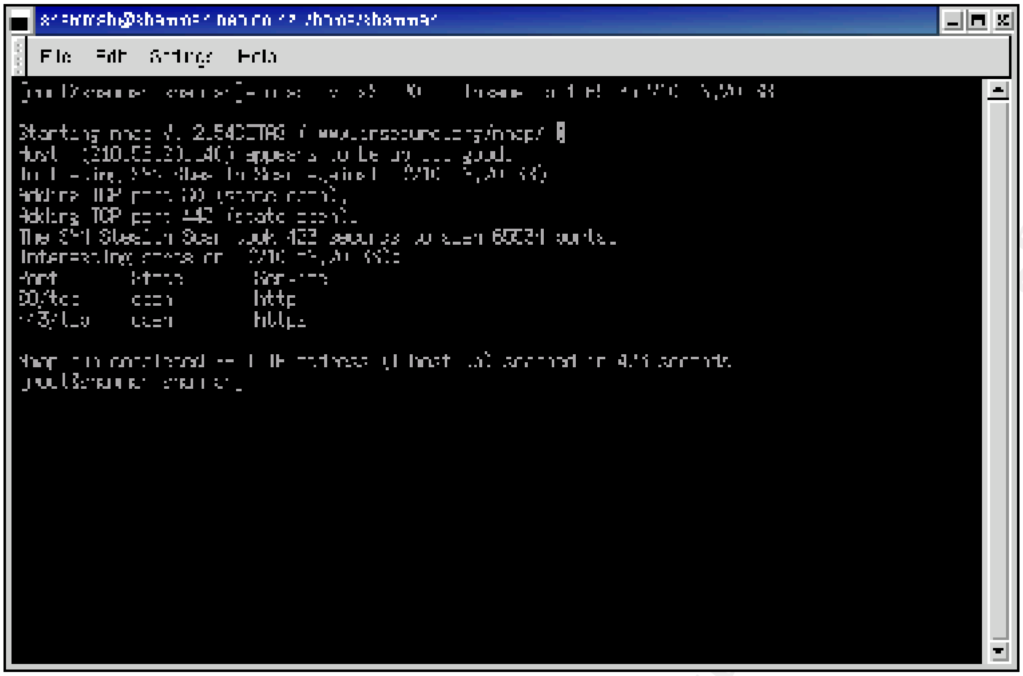
From the DMZ:

```
    nmap -sS -P0 -p 1-65535 210.56.20.32
    nmap -sU -P0 -p 1-65535 210.56.20.32
```

In each case all ports were shown as filtered.

3.3.4 Service Availability

For this test a scan was made from an Internet host on each device in the DMZ. The following are screenshots from the scan of the the SUPPWEB1 server. The results show that the only services open are those that are configured, ie http and https.



```
[illegible]

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Host (210.56.20.40) appears to be up ... good.
Initiating SYN Stealth Scan against (210.56.20.40)
Adding TCP port 80 (state open).
Adding TCP port 443 (state open).
The SYN Stealth Scan took 423 seconds to scan 65534 ports.
Interesting ports on (210.56.20.40):
Port        State       Service
80/tcp      open        http
443/tcp     open        https

Nmap run completed -- 1 IP address (1 host up) scanned in 4[illegible] seconds
[illegible]
```

Scans of each of the other services showed the same results; that ECOM_FWX was doing its job of filtering the packets correctly.

3.3.5 Fragmentation

The fragmentation tests will be conducted from an external Internet host aimed at the SUPPWEB1 web server which is running an sshd service which is filtered by ECOM_FWX.

```
hping2 -V -I eth0 --data 40 --count 3 --syn -p 22 210. 56.20.38
hping2 -V --frag -I eth0 --data 40 --count 3 --syn -p 22 210.56.20.38
```

As expected, the result of both tests showed ECOM_FWX denying the attempts to connect to port 22. The Ethereal listener placed in the DMZ did not detect the traffic. As hoped the fragmentation had no effect on the filter.

3.3.6 Common Vulnerabilities

Nessus was run from a remote host using its generic scan, DNS tests and web server tests.

Screenshots were not available for this section, however, no vulnerabilities were found on the web servers or DNS server. The only warning given was that the IP sequence number was reasonably easy to guess. Unfortunately this is a NT4.0 issue and cannot be easily resolved.

3.4 Review

Based on the findings of the audit I am reasonably happy with the a rchitecture chosen. It is reasonably hard to assess, however, as there are still a number of elements that would require auditing before a full objective view could be had.

Perhaps the most important process from here is the setting of policy on how each of the servers and network devices are updated on the release of new vulnerabilities. One of the concerns with the specified architecture is the continual release of vulnerabilities for NT4.0 and IIS4.0. Of course another major issue being the current BIND problems.

One of the other major things that has not been considered is fail over. A number of single points of failure exist within this architecture. Ideally, each of the firewalls should run in a load - balanced array and each router should be running i n a dual configuration with a virtual IP interface.

Another thing that has not been considered is backups. While these would be managed from the management subnet, the firewall rules we need to be reworked to incorporate the solution chosen.

4 Design Under Fire

4.1 Assignment

The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!

Select a network design from any previously posted GCFW practical (http://www.sans.org/giactc/gcfw.htm) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following thr ee attacks against the architecture:

- An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewal l.
- A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose.
- An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

Note: this is the second time this assignment has been used. Th e first time, a number of students came up with magical "hand -waving" attacks. You must supply documentation (preferably a URL) for any vulnerability you use in your attack, and the exploit code that you use to accomplish the attack. The purpose of this exercise is for the student to clearly demonstrate they understand that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.

4.2 Selection

The practical selected is that of Gavin Vallance, dated December 10 -15, 2000 URL (as of 15/04/01) http://www.sans.org/y2k/practical/gavin_vallance_GCFW.zip . This practical has been selected, as it seems to use a number of the same ideas that have been used in the develo pment of the architecture involved in the previous sections of this assignment. It is based on a primarily Microsoft environment, utilises Checkpoint FW -1 and makes a logical separation between corporate and customer traffic.

4.3 Attack on the Firewall

In the selected practical the actual Nokia 440 FW1 version and patch level is not specified. While there are numerous bypass or layer violation attacks available for the configuration detailed there are very few that directly target the firewall. This is especia lly the case when most traffic going directly to the firewall is blocked, as it is in this example. Issues such as the " Nokia IP440 Remote Denial of Service Vulnerability" (bugtraq ID 2054) and the numerous issues presented at the Blackhat Briefings 2000 http://www.phoneboy.com/docs/bh2000/ are largely mitigated by the anti-spoofing rule sets that have been enabled on the border routers. This reduces us primarily to indirect or parsing attacks, of which few exist for current Firewall1 implementations.

One attack that does target the firewall directly and is not hampered by anti -spoofing or strict rule sets is the IP fragmentation DoS discovered by Lance Spitzner http://www.checkpoint.com/techsupport/alerts/ipfrag_dos.html . A program written by him named jolt2.c sends large data fragments which cause specific fragment logging capabilities of Firewall1 to increase CPU utilization beyond what is expected, causing a denial of service.

During this attack the following commands can be run to see the effect on connections, memory and CPU load.

```
fw ctl pstat
fw tab -t connections -s
ps auxw
vmstat
```

CPU load will be pushed to 100%, memor y usage will slightly increase but not to dangerous proportions, processing of other connections will slow and finally cease when CPU utilization hits 100%.

4.4 Denial of Service Attack

4.4.1 The Attack

A denial of service attack on the above architecture utilisin g 50 cable or DSL modems is really a non-event. The numbers really talk for themselves.

A full dedicated T3 runs at approximately 45Mbps, a full capability DSL modem runs at approximately 8Mbps. Factoring for actual send capability, operating system IP st ack send capability and network issues we can probably estimate a 3Mbps output from each DSL modem.

3,000,000 * 50 = 150,000,000bps or 150Mbps

Based on these simple numbers, 150Mbps going down a 45Mbps pipe just won't happen. You can choose your method, S yn flood, ICMP, UDP fragments or even full valid HTTP traffic, but the entire organisation is going to go offline. That said the following is the method I would most likely use if conducting a denial of service on the above organisation.

- To co-ordinate the attack a customised Trojan such as that used in Stacheldraht or Trinoo2k would be installed at each cable modem site, with master daemons installed at reliable compromised sites.
- A traceroute would be conducted from numerous locations around the world t o check the network configuration external to the GIAC Enterprises network. This would determine if multiple routes were being utilised that would require separate targeting, and also provide targets one or two hops from the GIAC border router.
- The ISP that provides bandwidth for GIAC would be investigated via a series of tracerouting exercises to determine vulnerable internal links.
- If the ISP is considered vulnerable, i.e. unable to handle 150Mbps of traffic terminating at one of their perimeter routers , the DoS agents would be configured

to attack this router. Most likely the one located one hop out from the GIAC border router.

- For a direct router attack a basic ICMP echo request would probably be used, utilising pseudo-randomised source IP addresses a nd differing buffer sizes. If the analysis proves fragmenting would be helpful, this would also be used to hinder defence. The aim is to create traffic that looks so much like legitimate traffic, that attempts to block it also blocks all legitimate traffic .
- The attack would be launched at a peak traffic time, most likely late on a Friday afternoon when the administrator is likely to be at the local bar.

The reason the ISP is attacked instead of the actual target, is that this way it leaves no trace in the targets logs (not that they would give valid IP addresses anyway), and also does not alert the destinations IDS system. The organisation would simply disappear off the Internet. The downside to this is that the ISP is more capable of dealing with a DoS a ttack, and will therefore respond more quickly. Once the ISP responds the attack can be changed to attack the smaller, and original target.

The same techniques as above could be used directed straight at the target, but in this situation it would be more beneficial to use a tool that will exploit issues with the remote operating system. If directing the attack at the firewall; the Nokia 440 boxes implemented in the described architecture run on IPSO, a FreeBSD type operating system. The fragmentation attac k noted above for attacking a FW -1 box directly would be useful in this case, but in case this has been patched, experience tells me these boxes are reasonably vulnerable to attacks by stream.c data stream. Information on this attack can be found at http://staff.washington.edu/dittrich/misc/ddos/ .

4.4.2 The Defense

I wish there was a simple form of defense from this type of attack. But faced with the bandwidth of this attack there is very little th at would be achieved by implementing all the anti - DoS tactics available. That said however, GIAC should protect itself against these form of attacks as best as possible. The following are recommendations for preventing DoS based on experience and a few papers as listed in the bibliography.

- Maintain close relationships with your upstream ISP and encourage them to implement the same anti DoS tools as you use. Under a heavy attack they are the only one that can null route an attacker and protect your systems.
- Use anti-spoofing defenses such as the Cisco router command " **ip verify unicast reverse-path".**
- Utilise ingress and egress filtering to protect against spoofed addresses and broadcast traffic.
- Use the Cisco "**rate-limit"** command to limit Syn and ICMP packet s to reasonable levels.
- Ensure at least service pack two is installed on the Nokia FW1 boxes to disable the fragmentation vulnerabilities.
- Ensure publicly accessible hosts have plenty of RAM and have
- Utilize any future operating system patches made avai lable by Nokia to reduce the impact of Syn flooding on the Nokia 440. An example of such a patch is that of the stealth kernel patch project for linux at http://freshmeat.net/projects/stealthpatch /.

- Implement a basic intrusion detection system behind the border router to ensure that a denial of service attack is detected as soon as it hits the network. You can only respond if you know about the issue.
- Implement additional strict, anti -DoS rule-sets on the firewalls and routers that can be enabled during attacks. This rule -set will most likely set aggressive timeouts and may even restrict traffic to only those subnets that are known regular users. This rule-set would not be used at all times due to performance and accessibility issues.
- Ensure strict anti DoS rule -sets have been tested and can easily be enabled. Note: a server that is under heavy DoS is *extremely* difficult to work on, even locally.

4.5 Internal System Compromise

4.5.1 Selection

The selected practical does not specify the actual system, version information or patch details for the servers located behind the firewalls, which makes it difficult to pick a system to exploit. My preference in this architecture however is the secondary DNS serve r located behind the External Web Firewall/VPN. While not specified it is assumed that this server will be running the BIND name server at revision 8.2.2 Px, due in large fact to the fact that newer versions were not available at the time the practical was published.

Although it is dependent on the configuration of the Internal Web Firewall running Raptor (the actual rule set was not been specified) the split DNS configuration should enable a jump through to the internal corporate network. If the external DNS server is vulnerable, root can be gained. With the necessary zone transfers allowed through the internal firewall, and the internal DNS server most likely running the same or possibly earlier version of BIND, the internal DNS server can also be comprom ised. UDP tunnelling over port 53 with port forwarders on the external DNS could then enable full internal access to the corporate network that would go undetected.

4.5.2 Execution

If the snort rule set was updated regularly it should detect the initial comprom ise, however, with current work on IDS evasion it should be possible to avoid detection. Sidestep by Robert Graham http://www.robertgraham.com/tmp/sidestep.html can be used as well as basic IP fragmentation which should completely blind the snort IDS system.

The initial query could be made using:

```
c:\sidestep 207.200.51.72 -evade -dns
```

Or alternatively using a standard dig piped through fragrouter:

```
dig txt chaos version.bind. @207.200.51.72
```

Assuming this query returns positive results the tsig.c exploit (http://www.hack.co.za/exploits/daemon/named/tsig.c) could be used to gain local access on the box. If root is not gained immediately (named has been modified to start in an unprivileged context) privilege escalation techniques should be used.

Once root access is gained, netcat over UDP 53 should be used to retrieve a toolkit, and then the same exploit should be used to get roo t on the internal BIND server. Once this has been achieved a customised BIND server should be compiled utilising tunnelling code such as that implemented in Loki, and installed on both the external and internal nameservers. This hacked daemon will automatically forward tunnelled traffic from the external box to the internal allowing full tunnel access via UDP 53 to the internal network. From here the entire Microsoft Windows based internal network could most likely be compromised using commonly available ex ploits.

5 Sources and References

SL4NT - Syslog http://www.netal.com/SL4NT.htm

Security Focus http://www.securityfocus.com

Packetstorm http://packetstorm.securify.com

PhoneBoy http://www.phoneboy.com/

DoS Analysis by Dave Dittrich http://staff.washington.edu/ dittrich/misc/ddos/

Fragrouter by DugSong http://www.anzen.com/research/nidsbench/fragrouter.html

SANS Covert Shells Information
http://www.sans.org/infosecFAQ/covertchannels/covert_shells.htm

Hack.co.za http://www.hack.co.za

Netcat http://www.l0pht.com/~weld/netcat/

SecureRemote with SecureID http://www.phoneboy.com/docs/securemote -securid.pdf

SQL Server Security http://www.sqlsecurity.com/

Armouring NT for Firewalls http://www.net-security.org/text/articles/spitzner/armoring_nt.shtml

Auditing your Firewall Set-up http://www.net-security.org/text/articles/spitzner/auditing.shtml

Cisco’s Web Site http://www.cisco.com

A whole lot of linux man pages including nmap, hping2, nessusd, fragrouter etc.