Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst (GCFW)

Assignment Practical v2.0

Miles Parkin

14th November 2003

Contents

1 Abstract

This document has been written to answer the four assignments set as the GIAC Certified Firewall Analyst assignment, and thus the paper is split into four main sections.

The first section details the design methodology for GIAC Enterprises new e-business solution for the sale of fortune cookie sayings. The second section looks at the firewall and boarder router policies for the new solution, along with a tutorial on the implementation of the firewall policy. The third section details the process to verify the firewall policy, looking at the firewalls from every angle.

Finally, the fourth section looks at how an attack against another design is structured and what the possible outcome could be. This section is designed to highlight areas of possible weakness within any design, and thus increase awareness in these areas. To guard against a thief, you need to know how a thief works.

2 Assignment 1 – Security Architecture

2.1 Introduction

GIAC Enterprises is an established company who has been trading in fortune cookie saying for a number of years. Recently the company has moved into the e-business market and is now solely trades online. With ever increasing sales and the advent of a number of partners who translate and resell fortune cookie sayings, it was decided to completely redesign the way the company e-business infrastructure operates, whilst integrating it fully into the main IT infrastructure.

During the initial phases of the design, an audit of all business processes was carried out. When the results of this audit were analysed, it showed that there were six groups whose requirements dictate the final design specification. These six groups are:

- Customers - Companies of Individuals who purchase Fortune Cookie Sayings in bulk.
- Suppliers - Companies that supply GIAC Enterprises with Fortune Cookie Sales.
- Partners - Companies that translate and resell fortune cookie sayings
- GIAC Enterprises employees located within the internal network.
- GIAC Enterprises employees who require remote access to the internal services.
- The general public.

These six groups require different access levels, and all interact with GIAC Enterprises infrastructure in a different manner. With these requirements in mind, the design of the whole solution will implement the concept of "Defence in Depth", the multiple layers of security ensuring that each group can only perform the operations they are meant to.

2.2 Business Requirements

The six groups identified within the initial design audit all have different business requirements, and need to access GIAC Enterprises infrastructure with different levels of security and availability.

It was decided to break the design of the new e-business solution, and look at it from the requirements of each of the six groups. Looking further into the requirements of these six groups, it was discovered that they could be split into three distinct super sets. These are:

- Customers and the general public – Web access for browsing and online purchases for customers and prospective customers of GIAC Enterprises.

- Suppliers and partners – Secure data flow between selected companies and GIAC Enterprises.
- Internal and Mobile GIAC Enterprise employees requiring access to GIAC Enterprises internal services.

These three groups as can be seen cover all the requirements of the original six groups but simplify the design into three distinct blocks, whilst ensuring that the needs of each are fully met.

2.2.1 Customers and the General Public

Both GIAC Enterprises existing and prospective customers require the same level of accessibility to their e-business infrastructure, but once connected have very separate requirements.

The general public, that is prospective customers, requires a view of what GIAC Enterprises has to offer. This includes details of the types of fortune cookie sayings that are available and a free selection of each type. Details of how to become a customer and the limitations the GIAC Enterprises impose on its customers are also available.

GIAC Enterprises customers require access to the e-business site to purchase fortune cookie sayings in bulk. All customers have their own account that records the number and type of fortune cookie sayings that they have purchased, and details of payment methods that the customer has agreed to use.

Main access to the web site is via HTTP. Both existing and prospective customers see the same information when initially connecting to the site, with an option to login to the site for all existing customers. Once logged in, customers then connect to their personal secure GIAC Enterprises web site and the communication channel changes to HTTPS. From this point, all ordering, payment and delivery of the fortune cookie sayings is then encrypted.

2.2.2 Suppliers and Partners

After looking at great detail at the requirements of both GIAC Enterprises suppliers and partners it was recognised that both groups were very similar in their relationship with GIAC Enterprises. Both groups deal with large amounts of fortune cookie sayings using a similar order and delivery model, both work on an account basis with payment within a set time period, and both transfer data at set times.

With the requirements of both groups to take into consideration, along with the nature of their relationships with GIAC Enterprises, it was decided that the e-business web site would not suit the business needs.

After looking into all possibilities, GIAC Enterprises decided on implementing Business to Business (B2B) links to all their suppliers and partners, using the

Electronic Data Interchange (EDI) format for data exchange. This communication link would allow both GIAC Enterprises and its partners the ability to securely order fortune cookie sayings using an agreed format, and also allow GIAC Enterprises and their suppliers to deliver the fortune cookie sayings.

2.2.3 Internal and Mobile GIAC Enterprises Employees

After looking at the requirements of both the internal and mobile employees of GIAC Enterprises, it was recognised that their only difference was where they were physically working.

Mobile and teleworkers will be working from a computer with remote access. Historically this was via dialup, but the cost of long distance phone calls in the past has made this option more and more undesirable. Further to this, the spread of cheap Internet access has motivated GIAC Enterprises to switch to a remote VPN client to provide access, thus extending the internal network out to the mobile user's computers. Once connected, mobile users have the same access as their office based colleagues to both internal services and the Internet.

To increase security within GIAC Enterprises internal network, it is to be split into a number of zones, with different levels of security for each zone. GIAC Enterprises internal services are required for all users and include several specific systems providing resources for all parts of the business.

2.3 Design Overview

The three groups detailed above translate into three distinct areas within the GIAC Enterprises solution. These three areas are the web site, the B2B connection and the internal network with the remote VPN connection.

Operationally, these three areas divide into the e-business infrastructure and the internal infrastructure. Although these two parts of GIAC Enterprises infrastructure overlap, it is important to look at them as two separates with common features.

One common device crossing all boundaries is the GIAC Enterprises monitoring suite based around the BigBrother monitoring tool.

2.3.1 E-Business Operational Process

Central to the operation of the GIAC Enterprises e-business solution design is a SQL database that holds all the fortune cookie sayings along with customer, supplier and partner data.

GIAC Enterprises order fortune cookie sayings from their suppliers, over the B2B connection, and move them into the central database. From this

database, the fortune cookie sayings are available to both GIAC Enterprises customers and partners.

Partners order fortune cookie sayings, which are sent to them via the B2B connection, and removed from the central database. All the rest of the fortune cookie sayings are uploaded to the e-business SQL database for purchase by GIAC Enterprises customers via the web interface. In addition to uploading all available fortune cookie sayings to the e-business database, the central database is updated on a 30-minute basis with transactions from the e-business database and the data held modified accordingly.

Diagram 2-1 graphically represents the links used for these processes.

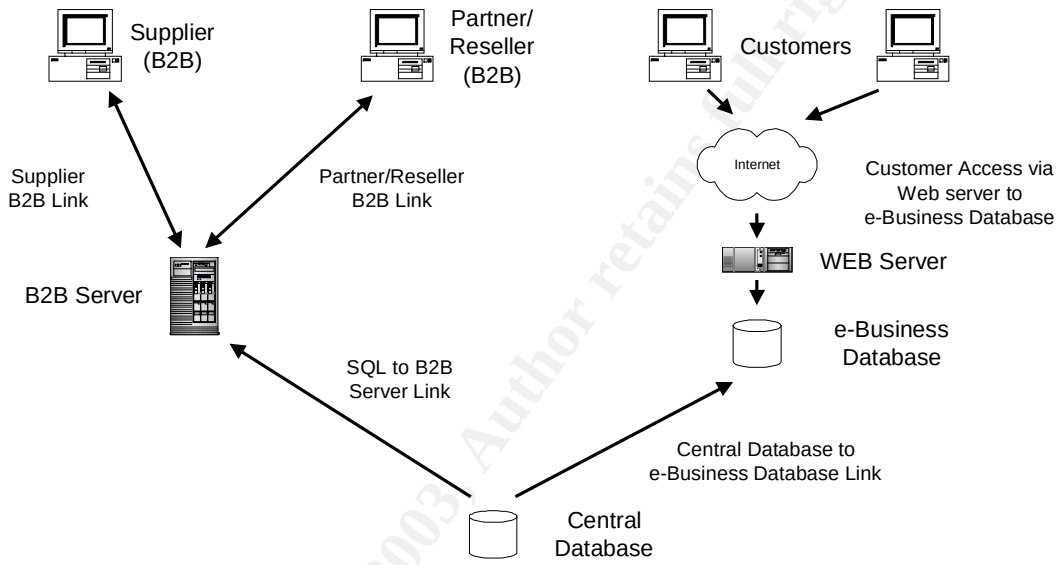


Diagram 2-1 GIAC Enterprises e-business Operational Process Links

2.3.2 GIAC Enterprises Internal Operational Process

Within the internal infrastructure, there are two main networks, the server network and the user's network. In addition to this there are two other networks both having a specific use, these being the admin network and the IDS management network.

When looking at the operational processes for the internal Infrastructure, it is apparent that the only certain servers within the environment require access to the front-end networks. These are the internal SQL servers, housing the central database, the main mail system, the monitoring server, the firewall management server, and the IDS management server. In addition to this, all users have been granted simple web access via a caching proxy server, and certain users require administration access to all devices. Email access for GIAC Enterprises utilises an SMTP gateway between the internal mail system and the Internet. All other systems that are within GIAC Enterprises internal infrastructure only require communication on the server network.

Diagram 2-2 graphically represents the links used for these processes.

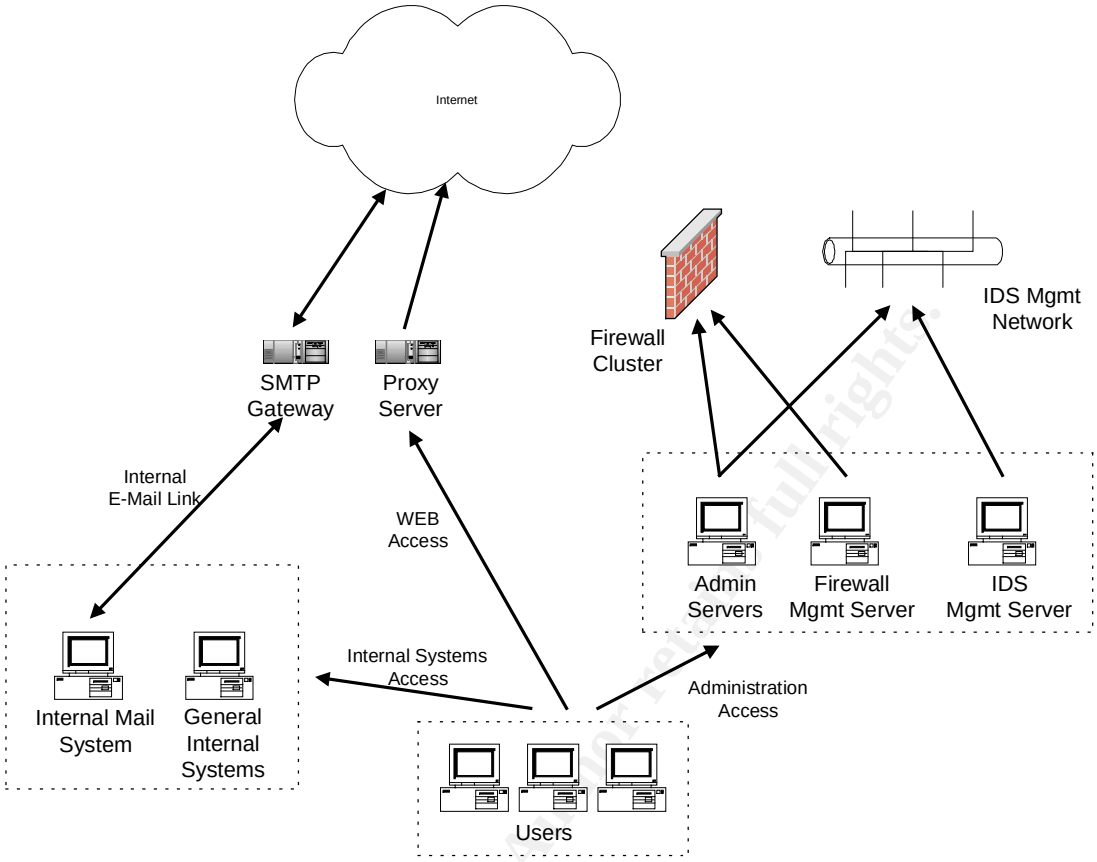


Diagram 2-2 GIAC Enterprises Internal Operational Process Links

2.3.3 Operational Security

Central to any design is the issue of security. That is ensuring that, in the first instance, only suitable traffic can flow between devices, secondly that all possible effects of intrusion are reduced, and thirdly that any intrusions are monitored.

The first layer of security in this instance is a fully redundant firewall cluster which is configured to only allow required traffic flow, and which segregates secure networks, both from each other and also from internal networks and the Internet. Additionally, a secure boarder router is implemented as a second level of defence to increase protection from the Internet, reducing the possible risk associated with configuration errors on the firewall. A secure router has also been implemented within the internal infrastructure to provide an extra level of security between the internal networks. The VPN termination is on the firewall cluster with rules limiting connections from trusted parties.

Secondly, but in no way of less importance, all servers within GIAC Enterprises infrastructure are built to stringent security standards, with only required processes and services available, as well as restricted user access. All operating systems are implemented with the highest level of patching, and

are patched on a regular basis after each new patch has been tested. As well as regular patching, all systems run anti-virus software as appropriate, and data flow between the Internet and GIAC Enterprises infrastructure is virus checked at the boarder, with both the SMTP gateway and proxy servers running anti-virus software for this purpose. All virus signatures are updated on a regular basis to reduce the risk of viruses causing damage to GIAC Enterprises.

Finally, an Intrusion Detection System (IDS) is implemented, looking for any rouge traffic on each monitored network. The IDS management system sends alerts when an Intrusion is recorded. This alert must be acted on by the administrator in charge dependant on the risk associated with that alert.

2.3.4 Web Site

The web site has been designed to reduce the risk of failure and consists of a pair of load-balanced web servers communicating directly with a SQL cluster. This combination ensures availability of the web site of 99.9% uptime or greater.

Each customer's records and preferences are loaded dynamically from the e-business SQL server by the application software running behind the web server software, along with information about what fortune cookie sayings are available. Customers select fortune cookie sayings from a menu and add them to their basket. Once all required fortune cookie sayings have been selected, payment is made by debit/credit card. Once the payment has been authorised, the fortune cookie sayings that have been selected are released.

Credit/Debit card payments are dealt with by a third party payment system which GIAC Enterprises uses.

2.3.5 B2B Connectivity

The B2B link consists of one B2B server on a secured network within the GIAC Enterprises e-business solution, and one on each supplier's site. Communication between B2B servers is bi-directional using FTP, and the communication link is encrypted using a VPN tunnel.

The B2B server within the e-business solution is in communication with the central SQL database, which due to the type of traffic flow across the B2B link, only connects on a three hourly basis to collect orders and deliver fortune cookie sayings. Data held on the B2B server is in EDI format with data translation being performed in the central SQL database.

2.3.6 GIAC Enterprises Employees Access

GIAC Enterprises employees may be split into two groups for the purposes of network design, general users and administrators. Both types of user may be internal or mobile and thus both require distinct access from the Internet and

inside the GIAC Enterprises network. All users require access to the Internet and server network.

GIAC Enterprises administrators have the added responsibility of looking after all servers and services within whole infrastructure and have higher levels of access than general users. The administrators' client machines reside on fixed IP addresses that have access to all areas as required.

2.4 Detail Design

The design as a whole builds up into a secure but flexible network, which ensures that all GIAC Enterprises employees can do their job without hindrance, and that all external connections to suppliers, partners, customers and the general public are secure.

In looking at the design of the solution, it was decided to break it down into the three main areas and look at each in detail. Each area looks into how traffic flows between devices. Where a device is used in more than one area, it is looked at in relation to the part of the solution being discussed.

2.4.1 Web Site Design

GIAC Enterprises web site consists of a pair of load-balanced web servers running as an active-active pair, connecting through to a SQL database running on a cluster. Customers accessing the web site get directed to the web server with the least load by the load-balancer, and from then on all connections from that customer go to that web server.

The application software on the web servers connects to the SQL database for uploading the customer data and available fortune cookie sayings. The web servers update the SQL database, either on modification of customer data or when fortune cookie sayings are sold. Communications to the SQL database utilise MS-SQL-SERVER communication on TCP port 1433.

The SQL database is built as a SQL cluster running in active passive mode. The cluster is built using two cluster members, with a shared storage device connected to the primary member of the cluster. Only manual fail-over or node failure will cause the secondary node to become primary. In this event, the shared storage moves with the active node of the cluster to ensure data integrity within the cluster.

Communication between the central SQL database and the e-business SQL database is uni-directional, with the central SQL database initiating the connection at very regular intervals to ensure that both databases are synchronised. As sales are made on the web site, the central SQL database updates itself with the sale details. Likewise, when GIAC Enterprises receives more Fortune Cookie Sayings, new data is uploaded to the e-business SQL database to be available for customers to purchase. The central SQL database checks the integrity of the data on the e-business SQL database to

ensure that the data has not been corrupted in any way. If corruption does occur, synchronisation is stopped, and an alert is sent to the monitoring system.

Payment for fortune cookie sayings is dealt with through Secpay, (www.secpay.com), an online credit and debit card authorisation service. When the customer enters their credit/debit card information within the web page, the web server connects to Secpay over an HTTPS link. Secpay returns an authorisation code to the application server, which then completes the transaction with the customer.

Diagram 2-3 shows the required traffic flows for all web transactions.

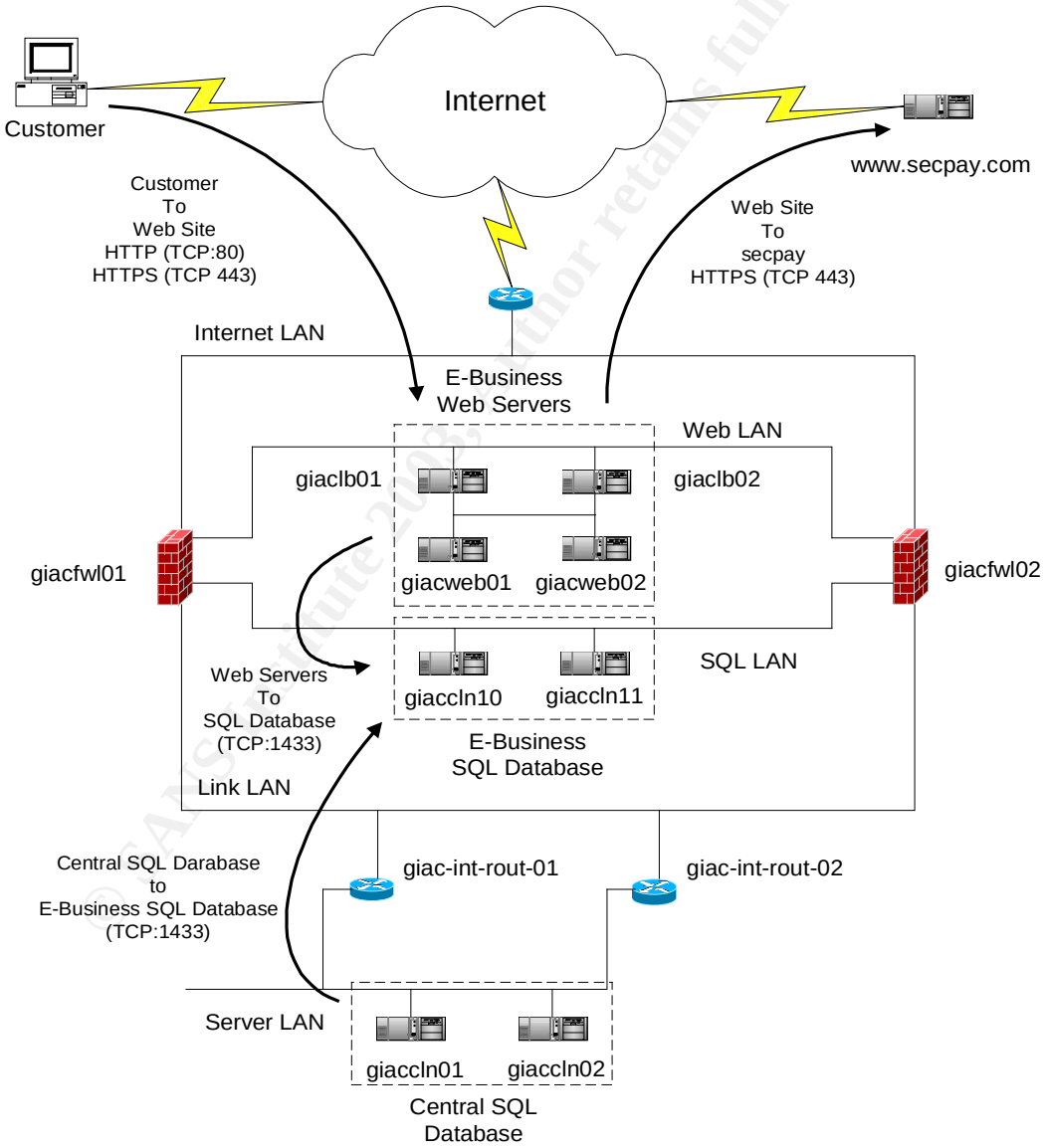


Diagram 2-3 Web Site Traffic Flow

2.4.2 B2B Connection

The B2B connection utilises FTP as the medium for data transfer between GIAC Enterprises and its suppliers and partners. Due to the commercial sensitivity of the data being transferred, it was decided to implement site to site VPN's between GIAC Enterprises and all its suppliers and partners to reduce the risk of data being stolen in transit. For this link, 3DES encryption was considered sufficient, as the time taken to break the encryption far exceeds the value of the data.

Communication between the B2B server and the central SQL database is proprietary to the EDI software, and uses TCP 9245. The EDI software runs in client server mode, with the server software running on the B2B server, and the client running on the central SQL database server, where it interacts with the SQL database. The EDI client polls the EDI server on a regular basis to collect any new data from suppliers or orders from partners, and also to place data for partners and orders for suppliers.

Diagram 2-4 shows the required traffic flows for the B2B links.

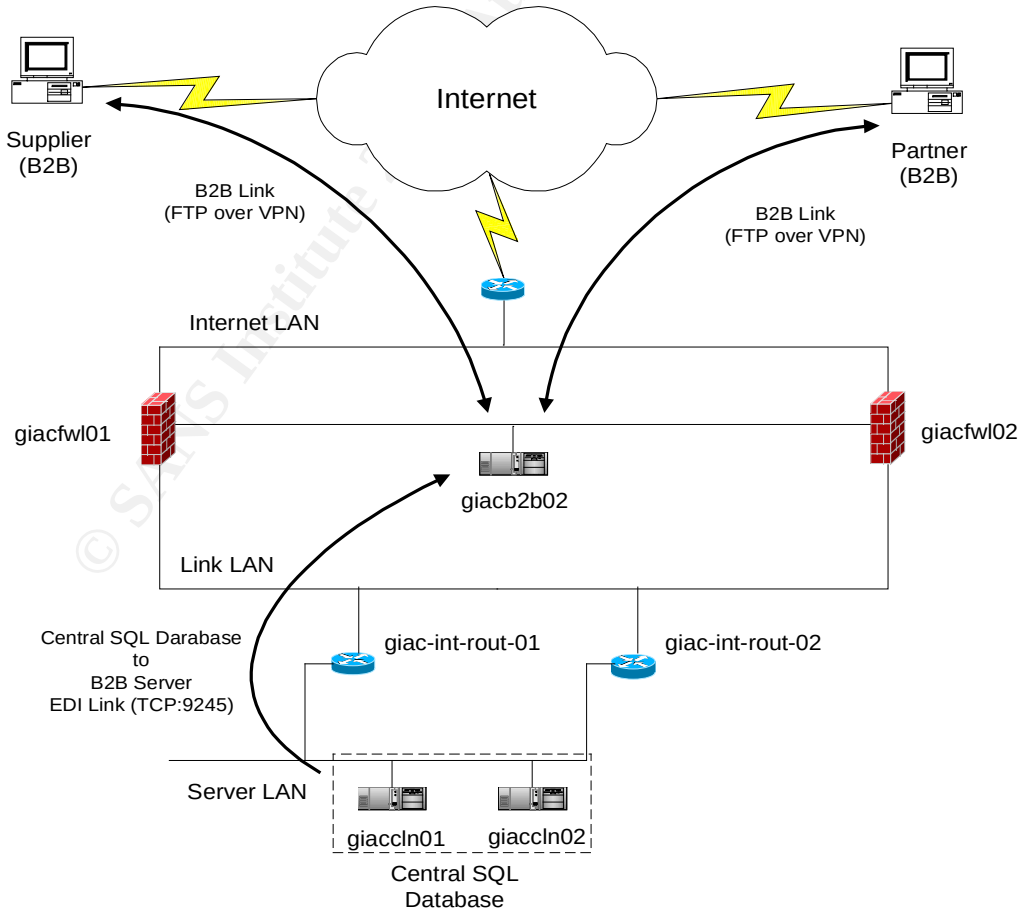


Diagram 2-4 B2B Communications Links

2.4.3 Internal Network

AS already discussed, there are two types of user within GIAC Enterprises, general users and administrators. The internal networks are split into four zones with a router providing the security between them. The four zones, or networks, are the server network, the user network, the admin network and the Intrusion Detection System management network.

In looking at user access to these networks, there is no difference if a user comes in from the Internet using the VPN client, or if the user is sitting at their desk.

All users have full access to the server network so that they can perform their day to day tasks without restriction. Unfortunately this policy is dictated by the use of a Microsoft Active Directory infrastructure, as this requires most TCP ports to be open. In addition to this, all users have web access to the Internet via the proxy server on the access network.

Administration users additionally have access to the admin network with both ssh and MS Terminal Services, the access being restricted to certain IP addresses that are fixed to their workstations. From the admin network, the administrators can access all areas of the solution being authenticated on the firewall for direct access to all secure networks.

VPN access is available to GIAC Enterprises mobile sales staff, management and administrators for out of hour's access. Of these three groups, there is a distinct split in that the administration staff require access to the admin network as well as the server network and the proxy server for web browsing. This split is defined by two vpn user groups, the first being general users, and the second being the administration users. All user VPN access into GIAC Enterprises network is controlled by SecurID authentication, with the firewalls communicating directly with the internal SecurID servers.

2.4.4 IP Addressing

IP addressing for the site has been implemented using non-routable (RFC 1918) addresses on the inside and routable addresses as provided by GIAC Enterprises Internet Service Provider on the outside.

Internally, with the network being split into several distinct sections, a number 10.44.X.Y address ranges have been utilised, with several different subnet masks used as appropriate. Table 1 lists the address ranges in use.

Network Name	IP Address/Mask	Notes
Internet	80.169.251.0/28	Between router and Firewall
Sync	10.0.0.0/30	Synchronisation LAN
Access	10.44.248.0/24	Internet Access LAN
B2B	10.44.253.0/29	B2B Server LAN
Web	10.44.254.0/25	Public Web LAN
SQL	10.44.254.128/25	Front-end SQL LAN
Link	10.44.60.0/24	Link LAN between front-end and back-end NW's
Server	10.44.50.0/24	Server LAN
User	10.44.0.0/23	User (DHCP) LAN
Admin	10.44.20.0/24	Admin LAN
IDS	10.44.21.0/24	IDS Mgmt LAN

Table 1 GIAC Enterprises IP Addressing Schema

Full details of IP addresses used and applicable to this design may be found in Appendix A.

2.5 Hardware and Software Specification

When moving forward with this project, GIAC Enterprises made the decision to standardise on hardware and software for as many systems as possible. This has resulted in most servers being built round a common hardware specification with some variables. Each server type is described below, in some detail, although not to too great a depth as this would be outside the scope of this document.

2.5.1 Firewalls and Firewall Management Server

Part of the design process was to look at what firewalls were best to be employed in the solution. After much consideration, CheckPoint Firewall-1 was chosen as it is very versatile and it was felt that it suited the solution, although its logging capabilities let it down. Also as a couple of the administration staff at GIAC Enterprises had CheckPoint experience, even though on a previous version, it was thought that a short course to upgrade their knowledge would be more beneficial that them having to learn a completely new firewall system.

A CheckPoint reseller was contacted, and the decision was taken to use CheckPoint SecurePlatform NG with AI, as the throughput of the firewall is only limited by the Intel server chosen to host the application. To provide redundancy at the firewall level, CheckPoint ClusterXL was enabled within the SecurePlatform software in load sharing multicast mode.

ClusterXL is the CheckPoint high availability and load sharing software that has been developed to provide a high level of resilience within a group of firewalls. Three modes are possible, but the mode chosen allows for maximum usage of the firewall hardware, whilst ensuring full redundancy. ClusterXL monitors all the firewall daemons as well as its network connectivity, and ensures seamless fail-over in the event of failure of any part of the firewall.

For management of the firewalls, a single server was implemented running CheckPoint SmartCenter on a Windows 2000 server, running win2k professional SP3. The server is built, fully patched as recommended by CheckPoint, and the CheckPoint SmartCenter software loaded. After the software was proved to run without any problems, the windows 2000 operating system was then hardened.

HP Prolient DL380's were chosen as a hardware platform for both the Firewall management and Firewall modules, although a different specification was employed for the two different environments.

The Firewall management server is built with dual 2.8GHz processors, 1Gb memory, and four 36G disks arranged as two mirrored disks of 36G. The primary disk is split into two, with 9G of disk being reserved for the Windows 2000 operating system, and the remainder being used for applications. The remaining pair of disks are configured as a single 36G device and is used for CheckPoint logging.

Both of the Firewall modules are built with a single 2.8GHz processor, dual four port, 10/100MHz cards, 1Gb memory and a single 36G hard disk. The apparent lack of redundancy on these devices is due to the fact that it is easier to rebuild a firewall module from scratch, and have two modules for HA, than it is to build a fully redundant single device.

2.5.2 Routers and Switches

GIAC Enterprises have a long running relationship with Cisco routers and switches, and for that reason it was decided to utilise them in this design.

Initially the design included dual Internet connections with a Cisco router installed for each link, but it was decided to only have a single Internet connection and therefore a single Cisco 2612 router as the boarder device, running IOS 12.2.

Within the design, Cisco switches have been installed, with the internal routers being installed as blades on a single Cisco 4006 switch. All networks off the firewalls are built on Cisco 2912 switches, with the Web and SQL LAN's being built using two switches each for redundancy.

2.5.3 Web Servers

The front-end web servers are each designed to be able to take the full load that the e-business site is expected to have. For this to be possible, they are identical in build, running IIS 5.0 on Windows 2000 professional, service pack 4.

HP Prolient DL380's were chosen for the web server applications to run on. These servers are built using dual 2.8GHz processors, 1G memory, and dual 36G hard disks as a mirrored pair. The disks are split into two areas, one of 9G for the Windows operating system, and the rest being used for the IIS and application software.

2.5.4 SQL Servers

Both SQL databases are built as SQL clusters running in active passive mode. Each cluster is built using two Windows 2000 servers, with a shared storage device, which is connected to both nodes in the cluster, but is only mounted on the primary node. Only manual fail-over or node failure will cause the secondary node to become primary. In this event, the shared storage moves with the active node of the cluster to ensure data integrity within the cluster. The SQL servers run on Windows 2000 professional, service pack 4.

HP Prolient DL380's were chosen for the SQL servers. Each SQL cluster consists of two servers, with single 2.8GHz processors, 1G memory and dual 36G hard disks for the operating system and application software as per the web servers. In addition, a further five 36G hard disks are implemented as a raid 5 device for data storage.

2.5.5 B2B Server

The EDI software chosen for the Business to Business link run by GIAC Enterprises dictates that the operating must be either Linux or Solaris, but there is no specification for disk, processor, etc. In common with the other servers in the solution, it was decided to utilise the HP Prolient DL380 for this application, running Suse Linux 7.3, which is one of the supported combinations.

The server was built with a single 2.8GHz processor, 1G of memory and two 36G hard disk configured as a mirrored pair. Susie Linux was installed to as directed by the EDI software installation notes, and locked down after the EDI software was installed.

2.5.6 Mail Relay Server

The mail relay server on the access network has been implemented to try to split the internal mail system from the outside world. As the internal mail system utilises Microsoft Outlook, and considering the need for anti virus software at some point of the e-mail path, the mail relay server was built using Suse Linux 7.3, with Trend Micro InterScan VirusWall version 3.8 and

Sendmail 8.12.10. Between them, these two programs reduce the risk of viruses and remove the possibility of using the e-mail gateway as an open relay. In addition, sendmail rewrites all header information within outgoing e-mails to remove any internal server names and addresses.

The server was built with a single 2.8GHz processor, 1G of memory and two 36G hard disk configured as a mirrored pair. Susie Linux was installed in a basic configuration and locked down after the mail relay software was installed.

2.5.7 Proxy Server

Like the mail relay server, the proxy server is built on Suse Linux 7.3 and is running InterScan VirusWall to ensure that all downloads are clean. In addition, the proxy server is running Squid Proxy version 2.5, providing caching.

2.5.8 User LAN

The User LAN hosts both users and printers, and has full access to the Server LAN. Normal users reside in the bottom half of the address space from 10.44.0.0 to 10.44.0.255. Administrators have machines in the lower part of the second half of the address space from 10.44.1.0 to 10.44.1.127, and printers in the upper half from 10.44.1.128 to 10.44.1.255. In addition the Administrators have ssh and MS-terminal access to all servers on the Admin LAN.

2.5.9 Server LAN

The server LAN contains all internal servers that are used for the smooth running of GIAC Enterprises including the internal database, the BigBrother monitoring server and the internal e-mail system. All servers on this network are built to the same level as all the servers within the front-end network.

2.5.10 Admin LAN

The Admin LAN is used for all administration of the front-end networks and associated architecture. This network holds a number of Microsoft and Linux administration servers that may be connected to from the User LAN by the administrators. Also on this network are the firewall and IDS management servers and the SecureID servers. Administrators when logged on to the administration servers can access any other part of the infrastructure, once authenticated.

2.5.11 IDS LAN

The IDS LAN provides management for the IDS network sensors, which are the only devices on this network. Access to this LAN is only possible from the administration servers on the Admin LAN, and from the IDS management server itself.

2.5.12 Hardening Windows 2000 Professional

When looking into hardening the Windows 2000 servers, the first port of call was the NSA, where several documents dealing with the securing of Windows 2000[1] were found. With this guide, along with regular updates from Microsoft, and the experience of the administration team, an internal security policy was created, which is now followed for all Windows 2000 server builds.

2.5.13 Hardening Suse Linux 7.3

The process for hardening the Suse Linux servers has been generated from a couple of sources, coupled with the experience of the server administrators. When looking into the process of securing Linux, the server administrators first investigated the Suse Security web page[2], which is SUSE's security team home page. In addition to this, they found an online book entitled "Securing and Optimising Linux"[3], which although is written with RedHat Linux in mind was found to be an excellent resource. As with windows 2000, an internal security policy was created, which is now followed for all Linux server builds.

2.5.14 Complete design

Diagram 2-5 shows the design as a whole.

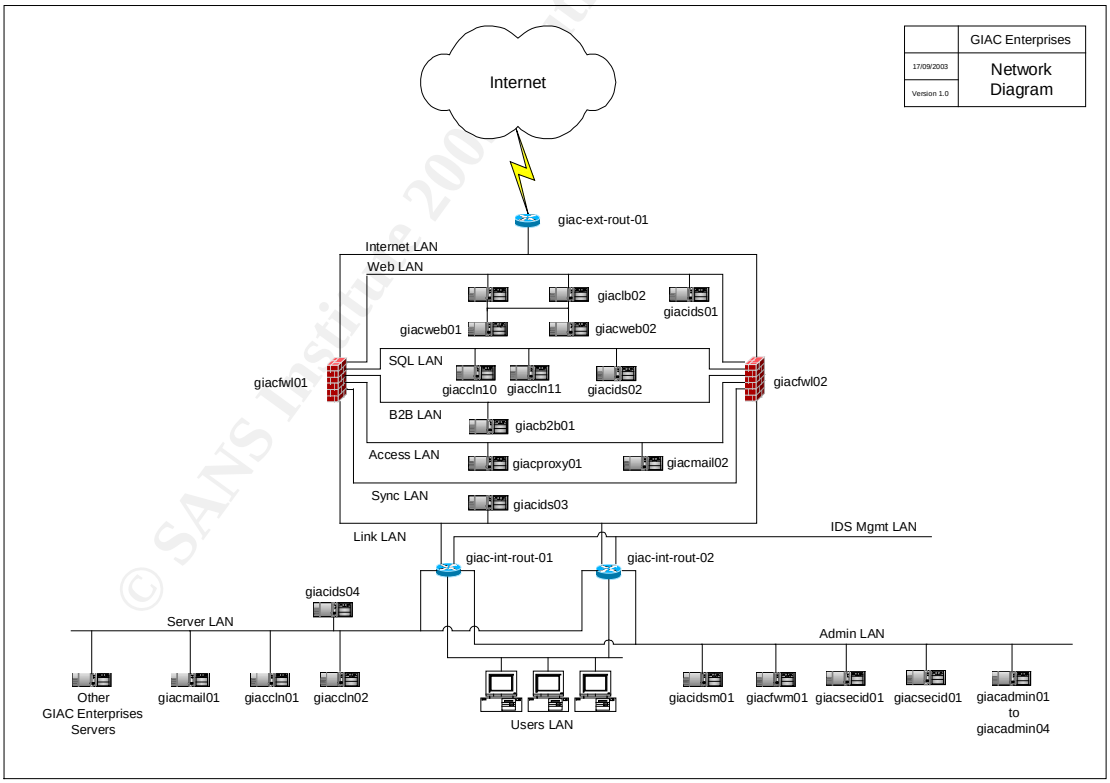


Diagram 2-5 Complete Network Diagram

3 Assignment 2 – Security Policy and Tutorial

3.1 Introduction

Following the design of the security architecture described in the previous section, it was felt fit to fully document the security policy for the main components utilised. This section fully details the policies for the boarder router and primary firewall. As the VPN connections terminate on the firewall, the VPN policy has been included as part of the firewall policy.

In addition to these policies, a tutorial has been added to describe how to build the firewall policy, detailing how each type of device is constructed and what pitfalls there are to the novice. In addition, reasons for removing Firewall-1 default settings have been included, along with a discussion on what services are required for management of the firewall software, and valid connections into the firewalls.

3.2 Boarder Router Policy

The boarder router is implemented as the first line of defence in this design, and therefore has to provide a good level of security for the rest of the network. The policy here defines access for customer, partners, suppliers and the general public. It also defines access for GIAC Enterprises employees, both for employees coming in over a VPN to the GIAC main systems within the back-office, and also for employee's web browsing and sending e-mails.

The boarder router is built on Cisco IOS 12.2, and employs static routing for all traffic. Management of the router is from the Admin LAN, without network address translation, and a static route exists for that connection. In addition, the router sends logging information back to a central logging server on the Admin LAN. The policy that is employed on this router is described in the following three sections.

3.2.1 Router Configuration

The first five lines of the policy disable finger, echo, discard, chargen, daytime, http and bootp servers on the router. These services, if running, would give an attacker information about the router that we do not wish that person to have.

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

Timestamp all normal and debug log entries.

```
service timestamps debug datetime msec show-timezones
service timestamps log datetime msec show-timezones
```

Store all passwords for the router in encrypted text.

```
service password-encryption
```

Set the router hostname.

```
hostname giac-ext-rout-01
```

Set the enable password.

```
enable secret 5 **************************
```

Discard all packets with source routing header options.

```
no ip source-route
```

Allow use of the zero subnet and remove class-based limitations of IOS.

```
ip subnet-zero
ip classless
```

Set the timezone to GMT.

```
clock timezone GMT 0
```

Configure Ethernet 0 and stop IP redirects, broadcasts, and disable proxy ARP's and CDP.

```
interface Ethernet0
 ip address 80.169.251.1 255.255.255.240
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 no cdp enable
```

Configure Serial 0 on a 2M frame-relay connection with access lists on incoming and outgoing traffic. Stop IP redirects, broadcasts, and disable proxy ARP's.

```
interface Serial0
 bandwidth 1984
 ip address 195.110.67.18 255.255.255.252
 ip access-group 100 in
 ip access-group 110 out
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 encapsulation frame-relay
 frame-relay map ip 195.110.67.17 16 IETF
 frame-relay interface-dlci 16
 frame-relay lmi-type ansi
```

Configure Serial 1 and BRI0 as shutdown.

```
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
interface BRI0
 no ip address
 no ip directed-broadcast
 shutdown
```

Configure routing for all connections. Default out via Serial 0 and static routes for all connections via Ethernet 0

```
ip route 0.0.0.0 0.0.0.0 195.110.67.17
ip route 10.44.20.0 255.255.255.0 80.169.251.14
ip route 10.44.50.0 255.255.255.0 80.169.251.14
ip route 80.169.251.4 255.255.255.255 80.169.251.14
ip route 80.169.251.5 255.255.255.255 80.169.251.14
ip route 80.169.251.6 255.255.255.255 80.169.251.14
```

Configure logging on the router and forward all logs to the BigBrother server using syslog facility local4.

```
logging source-interface Ethernet0
logging buffered 8192 debugging
logging trap debugging
logging facility local4
logging 10.44.50.10
```

3.2.2 Access Lists

Access list 10 is used for snmp queries and telnet access to vty 04.

```
access-list 10 permit 10.44.20.0 0.0.0.255
```

Access list 100 filters incoming traffic on Serial 0.

Stop access from spoofed addresses. These are private IP addresses, Multicast addresses, loopback addresses and the public address of GIAC Enterprises. All except the private address ranges are logged.

```
access-list 100 deny ip 10.0.0.0 0.255.255.255 any
access-list 100 deny ip 172.16.0.0 0.15.255.255 any
access-list 100 deny ip 192.168.0.0 0.0.255.255 any
access-list 100 deny ip 224.0.0.0 31.255.255.255 any log
access-list 100 deny ip 127.0.0.0 0.255.255.255 any log
access-list 100 deny ip 80.169.251.0 0.0.0.15 any log
```

Allow incoming http and https connections to the web site.

```
access-list 100 permit tcp any gt 1023 host 80.169.251.5 eq www
access-list 100 permit tcp any gt 1023 host 80.169.251.5 eq 443
```

Allow established https connections back from www.secpay.com.

```
access-list 100 permit tcp host 80.172.29.92 eq 443 host 80.169.251.4 gt 1023 established
```

Allow established incoming and new incoming e-mail connections to the mailrelay server.

```
access-list 100 permit tcp any eq smtp host 80.169.251.6 gt 1023 established
access-list 100 permit tcp any gt 1023 host 80.169.251.6 eq smtp
```

Allow incoming established connections for ftp, http and https for the proxy server.

```
access-list 100 permit tcp any eq ftp host 80.169.251.14 gt 1023 established
access-list 100 permit tcp any eq ftp-data host 80.169.251.14 gt 1023
access-list 100 permit tcp any gt 1023 host 80.169.251.14 gt 1023 established
access-list 100 permit tcp any eq www host 80.169.251.14 gt 1023 established
access-list 100 permit tcp any eq 443 host 80.169.251.14 gt 1023 established
```

Allow ESP and IKE connections to the firewall cluster for both new and established traffic.

```
access-list 100 permit udp any eq 500 host 80.169.251.14 eq 500
access-list 100 permit esp any host 80.169.251.14
```

Allow Client to Site VPN topology download.

```
access-list 100 permit tcp any gt 1023 host 80.169.251.14 eq 264
```

Allow established DNS connections for proxy and mailrelay servers.

```
access-list 100 permit tcp any eq domain host 80.169.251.14 gt 1023 established
access-list 100 permit tcp any eq domain host 80.169.251.6 gt 1023 established
access-list 100 permit udp any eq domain host 80.169.251.14 gt 1023
access-list 100 permit udp any eq domain host 80.169.251.6 gt 1023
```

Drop and log any other traffic.

```
access-list 100 deny   ip any any log
```

Access list 110 filters outgoing traffic on Serial 0.

Allow established http and https connections from the web server.

```
access-list 110 permit tcp host 80.169.251.5 eq www any gt 1023 established
access-list 110 permit tcp host 80.169.251.5 eq 443 any gt 1023 established
```

Allow https connections to www.secpay.com.

```
access-list 110 permit tcp host 80.169.251.4 gt 1023 host 80.172.29.92 eq 443
```

Allow outgoing e-mail and established incoming e-mail connections.

```
access-list 110 permit tcp host 80.169.251.6 gt 1023 any eq smtp
access-list 110 permit tcp host 80.169.251.6 eq smtp any gt 1023 established
```

Allow the proxy server ftp, http and https access to the Internet.

```
access-list 110 permit tcp host 80.169.251.14 gt 1023 any eq ftp
access-list 110 permit tcp host 80.169.251.14 gt 1023 any eq ftp-data established
access-list 110 permit tcp host 80.169.251.14 gt 1023 any gt 1023
access-list 110 permit tcp host 80.169.251.14 gt 1023 any eq www
access-list 110 permit tcp host 80.169.251.14 gt 1023 any eq 443
```

Allow ESP and IKE connections from the firewall cluster for both new and established traffic.

```
access-list 110 permit udp host 80.169.251.14 eq 500 any eq 500
access-list 110 permit esp host 80.169.251.14 any
```

Allow established connections for Client to Site VPN topology download.

```
access-list 110 permit tcp host 80.169.251.14 eq 264 any gt 1023 established
```

Allow DNS connections for proxy and mailrelay servers.

```
access-list 110 permit tcp host 80.169.251.14 gt 1023 any eq domain
access-list 110 permit tcp host 80.169.251.6 gt 1023 any eq domain
access-list 110 permit udp host 80.169.251.14 gt 1023 any eq domain
access-list 110 permit udp host 80.169.251.6 gt 1023 any eq domain
```

Drop and log any other traffic.

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

3.2.3 Connections to the Router

Snmp connections. Access-list 10 has read-only connections to retrieve location, contact and chassis-id information. Snmp traps are enabled and sent to the BigBrother server for monitoring purposes.

```
snmp-server community ******** RO 10
snmp-server location Boarder Router
snmp-server contact admin@giac.org
snmp-server chasis-id 102345678
snmp-server enable traps snmp
snmp-server host 10.44.50.10 traps ********
```

Put up a login banner to warn of unauthorised login and the consequences of such.

```
banner login ^C

                THIS DEVICE IS PART OF A
                   PRIVATE NETWORK

        ************************************************
        * Unauthorised access or use of this equipment  *
        * is prohibited and constitutes an offence under*
        * the Computer Misuse Act 1990.                 *
        * This system is being monitored and logs will  *
        * be used as evidence in court.                 *
        * If you are not authorised to use this system, *
        * Terminate this session now!                   *
        ************************************************


^C
```

Configuration for both Console and telnet access. Both connections have a 15 minute timeout on idle sessions. Telnet access is only allowed from the Admin LAN.

```
line con 0
 password 7 ******************
 exec-timeout 15 0
 transport input none
line aux 0
line vty 0 4
 access-class 10 in
 password 7 **************
 exec-timeout 15 0
 transport input telnet
```

The end of the router policy.

```
end
```

3.2.4 Router Policy Order

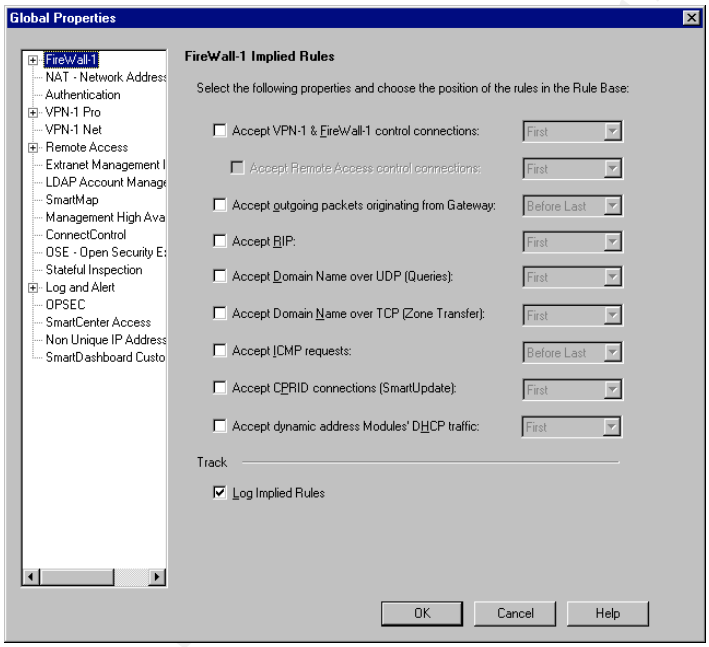
The access-lists within the router policy are read from the top down, which means the rules that get most hits are among the first in the policy. Within access-list 100, the first five rules are there to stop any spoofed traffic that is using RFC1918 private addresses, the loopback address, or multicast addresses, with the sixth rule ensuring that nobody spoofs the public IP address range of GIAC Enterprises. Apart from the order here, the rest of the router policy affects the manner in which the router operates, and is not affected by policy order, but is rather laid out for ease of understanding.

3.3 Firewall Policy

The firewall is the second line of defence from the Internet, and also ensures that there is security between the internal networks. The policy implemented at this level is far more complex than the policy on the boarder router, as it deals with internal as well as external traffic. The firewall policy also deals with the termination of the VPN traffic from both partners and resellers, as well as from GIAC Enterprises mobile workforce.

The order within the firewall rulebase is important as it is read using a top down approach, with the first rule to match being the one used. With this in mind, the most important rules are placed first, that is connections to the firewalls themselves, followed the rules which handle most traffic, and finally the low import connections such as administrator access and server monitoring. This order reduces the loading on the firewall module, and ensures that traffic throughput is as high as necessary.

To increase security within the firewall implementation, the Global Properties are modified to remove all Implied Rules as shown below. The reasons for this are dealt with in section 3.4.1.



As discussed above, the rulebase may be split into three separate parts. The firewall management, the external and internal connections that allow GIAC Enterprises to function, and finally system monitoring and management traffic.

3.3.1 Firewall Management Rules.

The first part of the rulebase details all connections to and from the firewalls. This part of the rulebase is of primary importance as it deals with the security of GIAC Enterprises Primary Firewalls.

The first two rules, as show below, provide communication between the firewall management station on the Admin LAN and the firewalls themselves, with the second rule controlling logging access.

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	FW-Management giacgw	giacgw FW-Management	Any Traffic	FW1-Mgmt	accept	None	Polic	*	Firewall management control.
2	giacgw	FW-Management	Any Traffic	TCP FW1_log	accept	None	Polic	*	FW1 Logging.

Rule 3 and 4 allow the VPN traffic to connect to the firewalls.

3	giacgw	* Any	Any Traffic	UDP IKE ESP	accept	None	Polic	*	Allow VPN traffic out of Firewalls
4	* Any	giacgw	Any Traffic	UDP IKE ESP TCP FW1_topo	accept	None	Polic	*	VPN Traffic to Firewalls and SecureClient topology Download.

Rules 5 and 6 cover authentication to the firewall, with rule 5 allowing client Authentication connection, and rule 6 the connection back to the SecurID servers for authentication of the users.

5	Admin-LAN	giacgw	Any Traffic	TCP FW1_clntauth_tel	accept	None	Polic	*	Client Authentication connection for authenticating Administrator Access.
6	giacgw	GIAC-SecurID-Servers	Any Traffic	securid	accept	None	Polic	*	SecurID authentication connection

Rules 7 and 8 provide access for monitoring of the firewalls using BigBrother.

7	giacbb01	giacgw	Any Traffic	ICMP echo-request	accept	None	Polic	*	BigBrother ping test
8	giacgw	giacbb01	Any Traffic	TCP bigbrother	accept	None	Polic	*	BigBrother stats

Rule 9 allows authenticated administrator access to the firewalls from the Admin LAN.

9	Admin_Iseg@Admin-I	giacgw	Any Traffic	TCP https TCP SSH	Client Auth	Log	Polic	*	Firewall management connection for Firewall obsequio system.

The final rule of this section, is the Firewall stealth rule, which is designed to hide the firewall from all unwanted traffic.

10	* Any	giacgw	Any Traffic	* Any	drop	Log	Polic	*	Firewall stealth rule

3.3.2 External and Internal Connections

The next part of the rulebase deals with the External and internal traffic for GIAC Enterprises network. These rules are ordered by expected traffic rather than by function.

Rules 11, 12 and 13 deal exclusively with traffic to and from the GIAC Enterprises web site. Rule 11 allows http and https connections from outside the network, rule 12 allows the web servers to communicate with the SQL cluster, and rule 13 provides the connection to www.secpay.com for secure payment.

11	GIAC-LANs	www	Any Traffic	TCP http TCP https	accept	None	Polic	*	Web access to GIAC Enterprises web site.
12	GIAC-Web-Servers	giacsqlcl10	Any Traffic	TCP MS-SQL-Server	accept	None	Polic	*	Web to SQL querry connection
13	GIAC-Web-Servers	www.secpay.com	Any Traffic	TCP https	accept	None	Polic	*	Secure payment link

Rules 14 to 16 allow GIAC Enterprises users Internet access and access to the web site for internal queries, running statistics, and a number of other tasks. All access to both the Internet and the web site are via the proxy server.

14	Users-LAN	giacproxy01	Any Traffic	tcp-1080	accept	None	Policy	Ai	Proxy access for Internal users.
15	giacproxy01	giacvip01	Any Traffic	http https	accept	None	Policy	Ai	Access to GIAC Enterprises web site for Internal users.
16	giacproxy01	GIAC-LANs	Any Traffic	ftp http https dns	accept	None	Policy	Ai	External web traffic from proxy server.

Following this are rules for e-mail access both to and from the Internet, with all access being forced through the mail-relay server.

17	GIAC-LANs	mailgateway	Any Traffic	smtp	accept	None	Policy	Ai	Mail connection into GIAC Enterprises.
18	giacmail02	GIAC-LANs	Any Traffic	smtp dns	accept	None	Policy	Ai	Mail connection out of GIAC Enterprises.
19	giacmail01 giacmail02	giacmail02 giacmail01	Any Traffic	smtp	accept	None	Policy	Ai	Mail connection between internal mail system and mail relay.

Rule number 20, allows the internal SQL server access for updates to the e-business SQL server.

20	giacsqlcl01	giacsqlcl10	Any Traffic	MS-SQL-Server	accept	None	Polic		Update traffic from inetnal SQL server to e-business SQL server.

And rule 21 allows the internal SQL server access to the B2B server on TCP port 9245.

21	giacsqlcl01	giacb2b01	Any Traffic	EDI-Trans	accept	None	Polic		Internal SQL to B2B server communication

The next two rules, numbers 22 and 23 provide ftp access over the VPN between GIAC Enterprise and their partners and suppliers.

22	Partners Suppliers	giacb2b01	Suppliers-Partnel	ftp	accept	None	Polic		B2B link from Supliers and Partners to GIAC Enterprises.
23	giacb2b01	Partners Suppliers	Suppliers-Partnel	ftp	accept	None	Polic		B2B link to Supliers and Partners from GIAC Enterprises.

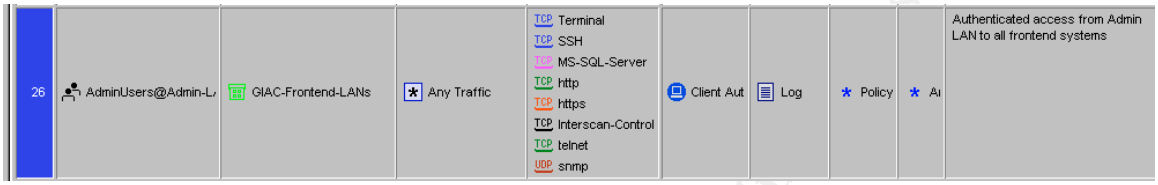
The final rule within this part of the rulebase are for GIAC Employees to access the back-office so that they can continue their job whilst off site. Two different rules exist, one for the normal users, and the other for the administration users, giving them additional access to the Admin LAN.

24	MobileUsers@Any	GIAC-Remote-User-Acce	Remote-Access	Any	accept	Log	Policy	Ai	Remote VPN Access for mobile workers
25	AdminUsers@Any	GIAC-Remote-Admin-Acc	Remote-Access	Any	accept	Log	Policy	Ai	Remote VPN Access for administrators

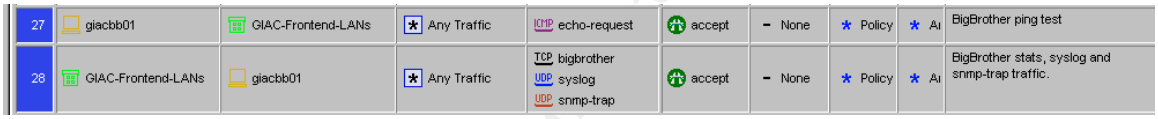
3.3.3 System Monitoring and Management

This part of the rulebase details the requirements for monitoring and managing all servers within the front-end network. As well as the B2B, SQL and Web servers, this includes the Proxy server, mail relay server and boarder router.

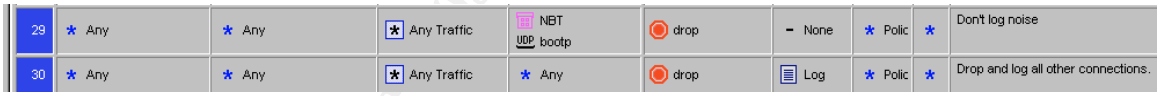
The first rule in this section allows authenticated access from the Admin LAN to all the networks that these devices are on, with a limited number of protocols that may be used for connection.



Rules 27 and 28 provide access for monitoring of all these devices using BigBrother, along with syslog and snmp-trap connections from all Linux and Cisco devices.



Finally rules 29 and 30 are the cleanup rules. Rule 29 filters out white noise, whilst rule 30 drops and logs all other traffic.



3.3.4 Network Address Translation

Network address translation for the firewall policy is dealt with by a separate part of the rulebase, and is shown below. The method of network translation used in this firewall policy is that of manual, rather than automatic, network address translation as it is by far more flexible and reduces issues that can arise from automatic address translation being incorrectly mixed with manual address translation.

Rule 1 ensures that no address translation is done for internal network communication. Rule 2 provides translation for incoming traffic to the web site. Rules 3 and 4 are address translation rules for e-mail. Rule 5 hides the web servers behind a single address for connection to www.secpay.com. Rule 6 hides all outgoing web traffic from the proxy server.

The order for these rules is paramount as if they are in the wrong order, the wrong address translation is likely to happen.

NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON	COMMENT
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
1	GIAC-LANs	GIAC-LANs	Any	Original	Original	Original	Policy Targets	Don't NAT internal traffic
2	Any	www	Any	Original	giacvip01	Original	Policy Targets	NAT for public address for web site.
3	Any	mailgateway	Any	Original	giacmail02	Original	Policy Targets	NAT for public address for mailgateway.
4	giacmail02	Any	Any	mailgateway	Original	Original	Policy Targets	Translate source IP for all outgoing e-mail
5	GIAC-Web-Serve	www.secpay.cc	Any	web-hide	Original	Original	Policy Targets	Hide web servers behind single address.
6	giacproxy01	Any	Any	giacgw	Original	Original	Policy Targets	Hide proxy server behind firewall.

Address translations with regard to the VPN connections is dealt with in the next section.

3.3.5 Supplier and Partner VPN Connections

All VPN connections are terminated on GIAC Enterprises primary firewalls, and have rules within the firewall policy. The actual configuration of the site to site VPN connections is managed by the VPN Manager, which details information on end-points, IKE and IPsec properties, encryption domains and traffic routing characteristics. This collection of information is called the community properties.

Configuration is for the VPN between both the Suppliers and Partners and GIAC Enterprises is detailed below.

IKE (Phase 1) Characteristics:

Key exchange encryption:	DES
Data Integrity:	MD5
Diffie-Hellman group:	Group 2 (1024 bit)
Renegotiate SA every:	1440 Minutes

IPsec (Phase 2) Characteristics:

IPsec data encryption:	3DES
Data Integrity:	SHA1
Renegotiate SA every:	3600 Seconds

NAT within VPN community is Disabled.

These characteristics have been chosen to provide the optimum key exchange and encryption within between GIAC Enterprises and its suppliers and partners. For key exchange, DES (56-bit key) encryption and MD5 (128-bit hash) hashing have been used to provide a secure and effective transport for IPsec key exchange, whilst minimising load on the firewalls. For actual data encryption and integrity checking, although AES is available, 3DES (156-bit key) and SHA1 (160-bit hash) have been chosen, as although they require greater processing than DES and MD5, they provide better protection from

attempted attacks and data errors, and are supported by all GIAC Enterprises suppliers and partners.

Authentication for initial key exchange is performed using certificates that are managed by a third party certificate agency.

3.3.6 Remote User Access VPN Connections

Like the supplier and partner VPN connections, the VPN Manager manages the configuration of the remote user access over VPN, but unlike the supplier and partner VPN connections, the IKE and IPsec properties are managed within each remote user's profile.

Two distinct groups of remote user have been configured, one for normal users, and one for administrators. These two groups have different access rights as described within the rulebase.

Client Characteristics:

Data encryption:	AES-128
Data Integrity:	SHA1
Diffie-Hellman group:	Group 2 (1024 bit)

These characteristics are enabled for all remote users and provide a high level of security for uploading and downloading data from the user's remote machine. Each user is running CheckPoint SecureClient, with different desktop policies on for each group.

The desktop policy for the two groups is described in two separate sections, firstly inbound connections to the remote machine, and secondly outbound connections.

Inbound connections as shown below, allows encrypted traffic from different parts of GIAC Enterprises network for each user type. Normal users can receive traffic from the server LAN and the proxy server, but administrators can also receive traffic from the admin LAN.

Rules 1 and 4 detail what to do with other traffic; that is drop all NBT traffic and drop and log any other traffic.

Inbound Rules

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	COMMENT
1	* Any	All Users@Any	NBT	Block	None	Block NetBIOS traffic
2	GIAC-Remote-User-Access	MobileUsers@Any	* Any	Encrypt	Log	Decrypt rule for normal users
3	GIAC-Remote-Admin-Access	AdminUsers@Any	* Any	Encrypt	Log	Decrypt rule for administrators
4	* Any	All Users@Any	* Any	Block	Log	Cleanup Rule

The desktop policy for both mobile users and administrators allows unrestricted access to all servers on the Server LAN and access to the proxy

server on port 1080. In addition to this, administrators have ssh and MS-terminal access to all servers on the Admin LAN. All access to the Internet is blocked by rules 5 and 9. When the remote user is not connected to GIAC Enterprises network via the VPN connection, normal Internet connections are possible using rule 10.

Outbound Rules

NO.	DESKTOP	DESTINATION	SERVICE	ACTION	TRACK	COMMENT
5	All Users@Any	* Any	NBT	Block	None	Block NetBIOS Traffic
6	MobileUsers@Any AdminUsers@Any	Server-LAN	* Any	Encrypt	Log	Allow Access to Server Lan
7	MobileUsers@Any AdminUsers@Any	giacproxy01	TCP tcp-1080	Encrypt	None	Web Browsing via GIAC Proxy Server
8	AdminUsers@Any	Admin-LAN	TCP SSH TCP Terminal	Encrypt	Log	Admin Access Only
9	AdminUsers@Any MobileUsers@Any	* Any	* Any	Block	Log	Block Internet Traffic while Encrypting
10	All Users@Any	* Any	* Any	Accept	Log	Allow Internet Traffic while not Encrypting

3.4 Firewall Policy Implementation Tutorial

This tutorial covers many of the issues that somebody configuring a CheckPoint Firewall will encounter. The objects described are those used in the firewall policy described above, and the actions taken to modify default properties are those that are in use on a daily basis and have been proved to work, rather than theoretical best practice.

Details on how the firewalls work, and software installation guides are available on the CDROM that is supplied with the CheckPoint software, and for that reason, I will not cover this material again.

3.4.1 Creation of Firewall-1 Rulebase Objects

When building a security policy using Firewall-1 from scratch, it is important to create the Firewall-1 rulebase objects with names that are meaningful in their own right. An object's name should tell the person viewing the rulebase what it is, and what it is used for. Multiples of the same kind of object should have a number postfixed to their name. Also it is important that the correct type of object is used, and that groups are used to group together objects that are similar, or are used together for specific operations.

In creating a Firewall-1 rulebase, it is important that you create the firewall object(s) and firewall cluster, a firewall management station, server objects for all internal servers that connect across the firewall, network objects for internal networks, and finally if required, third party VPN devices and associated networks and server objects.

The Firewalls utilised within this design, are configured in a cluster using CheckPoint ClusterXL. The object for this cluster is shown in the following diagram.

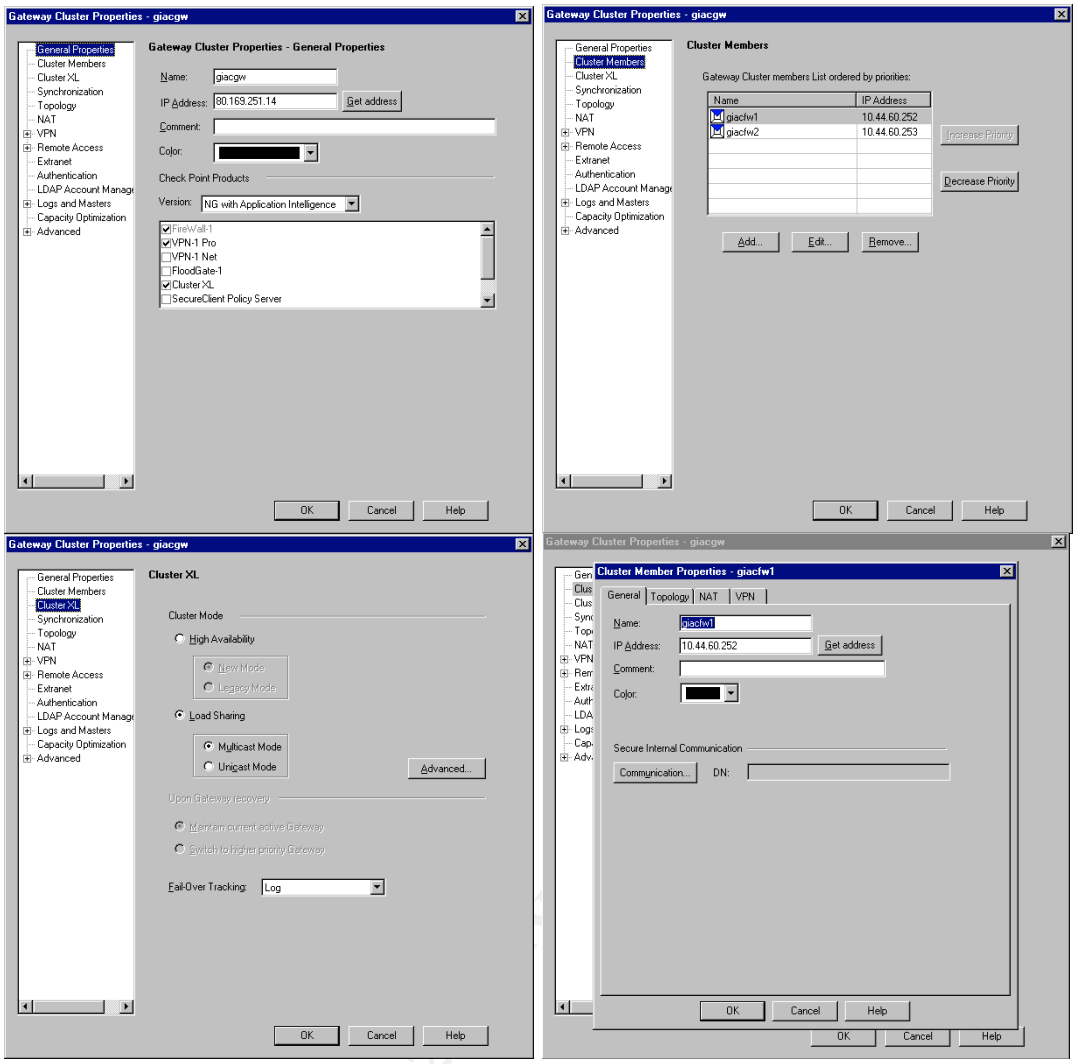


Diagram 3-1 Part Configuration of Gateway Cluster Object

As can be seen in Diagram 3-1, the configuration of the gateway cluster, amongst other things, has the configuration of the cluster members within one of its options. Under NG AI, this is the only place that the cluster members may be found, and therefore, they are never considered as two individual objects. The configuration of other parts of this object, such as VPN, Logs and Masters, etc, are configured as described in the Firewall-1 getting started guide.

3.4.2 Firewall Management and Global Settings

The first step when configuring a firewall is that of ensuring the communication channels used between the management server and the firewalls is open, but only for the required traffic. By default, the firewall policy has certain connections open for management, authentication, OPSEC communication, VPN communication, etc… Although this apparently reduces the need for adding these services, it actually leaves the firewall open to being identified. With this in mind, we shall look at the required services for the management of any number of firewalls.

The services that are required for management are:

CPD	(TCP 18191)
CPD_amon	(TCP 18192)
FW1	(TCP 256)
FW1_ica_push	(TCP 18210)
FW1_ica_pull	(TCP 18211)
FW1_ica_services	(TCP 18264)

In our design, these have been grouped together as “FW1-Mgmt”. These services allow the firewall module and management station to communicate, with the management station being able to obtain statistics from the firewall module. In addition to this, one further connection is made back to the logging server, which in this case is the management station as:

FW1_log	(TCP 257)

This service ensures that all logging that is generated on the firewall module is sent to the log server.

These services are built up as the first two rules of our firewall policy.

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	FW-Management giacgw	giacgw FW-Management	Any Traffic	FW1-Mgmt	accept	None	Polic	*	Firewall management control.
2	giacgw	FW-Management	Any Traffic	FW1_log	accept	None	Polic	*	FW1 Logging.

It is common to terminate VPN traffic on the firewall module, as this reduces the requirement for a second device to perform this task. The two phases of connection are configured within the firewall policy, and may be tailored to suit the requirements of the VPN connection required.

If a site to site VPN is required, it is advisable to reduce the visibility of the VPN tunnel by defining the endpoints for the tunnel within the rule allowing VPN access to the firewall module. When using VPN tunnelling with authentication and encryption, there are only two services that are required:

IKE	(udp 500)
ESP	(ip protocol 50)

The IKE handles the key exchange, and the ESP is used to deliver the encrypted data.

If the VPN required is a client to firewall VPN, it is not possible to define the VPN endpoints, as they may come from anywhere in the world, and so the firewall is shown as being a VPN endpoint to anyone who is looking. Unfortunately it is impossible to do anything about this, so the best action that can be taken is to ensure the highest level of authentication possible is used for the remote client VPN’s so that a hacker will not be able to obtain access. The VPN rules that are used within this design come under this category.

Also for client to firewall connections there is the requirement for the client to upload topology information for the networks that they are connecting to. For this to happen, a single service needs to be opened:

FW1_topo (TCP 264)

Unfortunately, this port is only used by Firewall-1 and so it opens up the firewall for identification.

3	giacgw	Any	Any Traffic	IKE ESP	accept	None	Polic		Allow VPN traffic out of Firewalls
4	Any	giacgw	Any Traffic	IKE ESP FW1_topo	accept	None	Polic		VPN Traffic to Firewalls and SecureClient topology Download.

Further to these services, there are certain services that are required to allow authentication, such as client authentication, on the firewall. The most common authentication used, as it is one of the most versatile, is client authentication, where the user attaches to the firewall module, authenticates, and then is allowed to use certain services as per the firewall rulebase. There are two services that may be used for authenticating:

FW1_clntauth_telnet (TCP 259)
FW1_clntauth_http (TCP 900)

In general use, it is often easiest to only allow FW1_clntauth_telnet as there are no issues of the request being sent via a proxy server, and allowing multiple users access from a single authentication session.

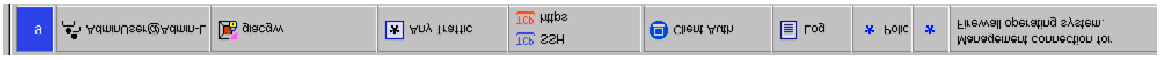
Connection that are authenticated, require some form of authentication method, weather it be username and password, or a more advanced method such as SecureID. To configure SecureID, you are required to generate the file on the SecureID server, and put it on the firewall module. This then allows the firewall to connect to the SecureID server listed in that file for authentication purposes. In addition to this file being in the correct place, a rule allowing SecureID traffic to the SecureID servers is required.

5	Admin-LAN	giacgw	Any Traffic	FW1_clntauth_tel	accept	None	Polic		Client Authentication connection for authenticating Administrator Access.
6	giacgw	GIAC-SecurID-Servers	Any Traffic	securid	accept	None	Polic		SecurID authentication connection

Monitoring of the firewall modules is performed using the BigBrother software suite. A BigBrother client has been installed on the firewall, and a rule is required for this to access the BigBrother server. The BigBrother server also must be able to ping the firewall module to ensure that it is up.

7	giacbb01	giacgw	Any Traffic	echo-request	accept	None	Polic		BigBrother ping test
8	giacgw	giacbb01	Any Traffic	bigbrother	accept	None	Polic		BigBrother stats

Network management of the firewall modules should be authenticated, and limited to specific sources. The rule for this connection should be logged and reside just above the firewall stealth rule.



The final rule that is directly related to the firewall cluster is the Firewall stealth rule. This rule is designed to hide the firewall from all unwanted traffic by dropping it and logging all unwanted traffic.

3.4.3 Non Management Rules

The configuration of the main part of the rulebase, I will not cover in detail, as it is mostly self-explanatory. All rules are set-up so that particular traffic may transfer from server A to server B over service C. On the whole, logging is not used for this traffic as it is allowed and firewall logs would provide no benefit in the event of an investigation. What I will cover however, is the configuration of the two types of VPN rules that are in the rulebase.

Fireall-1 NG introduced the concept of “simplified mode” for VPN configuration, rather than the traditional mode. In this mode, the VPN characteristics are configured under the VPN Manager tab. The rules using these properties are shown below, and apart from the VPN information, they are identical to a “normal” rule.

22	Partners Suppliers	giacb2b01	Suppliers-Partnei	ftp	accept	None	Policy	B2B link from Suppliers and Partners to GIAC Enterprises.
23	giacb2b01	Partners Suppliers	Suppliers-Partnei	ftp	accept	None	Policy	B2B link to Suppliers and Partners from GIAC Enterprises.
24	MobileUsers@Any	GIAC-Remote-User-Acce	Remote-Access	Any	accept	Log	Policy	Remote VPN Access for mobile workers
25	AdminUsers@Any	GIAC-Remote-Admin-Acc	Remote-Access	Any	accept	Log	Policy	Remote VPN Access for administrators

Two types of VPN configuration are used within this rulebase, and it is important that you use the correct one. For the B2B link, a star VPN topology has been utilised, as all of the suppliers and partners require access to GIAC Enterprises B2B server, but do not require access between each other. The configuration of this is shown in the following diagrams.

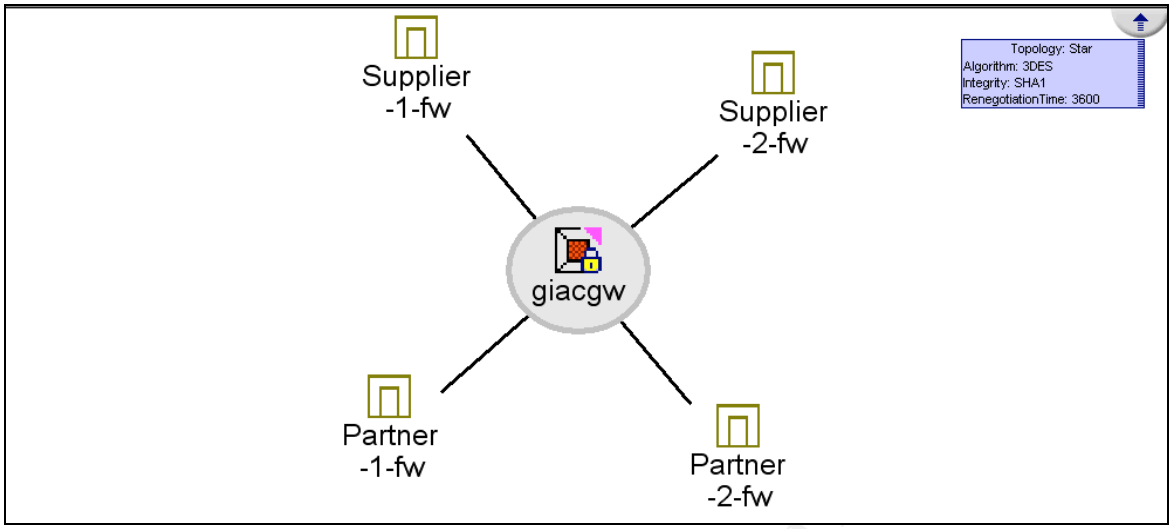


Diagram 3-2 VPN Star Topology

Diagram 3-3 shows two of the screens used to implement the VPN Star Topology. Two other screens are important, but are not shown, as their use is fairly straightforward. These are the "Central Gateways" and "Satellite Gateways" screens, which define what the VPN endpoints are. This information is shown in Diagram 3-2.

The VPN endpoints are defined as "Interoperable Devices", as they are outside of our control. They are devices that are VPN terminators, and may be any hardware, software combination. Their only requirement is that they can perform their task.

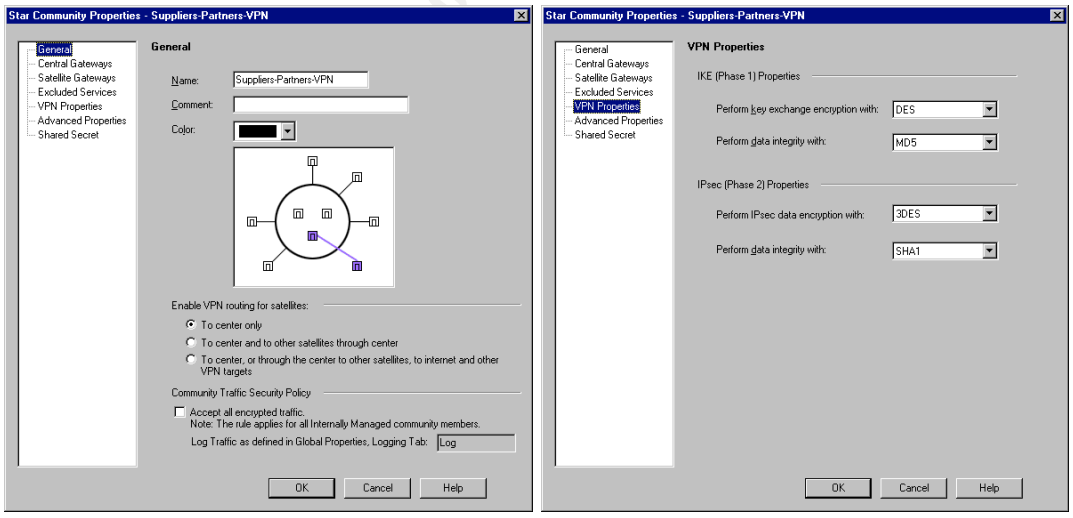


Diagram 3-3 VPN Star Topology Configuration

The second type of VPN configuration used, is the Remote Access Community configuration, which is used for all client to firewall communications. The following Diagrams show the configuration details for this.

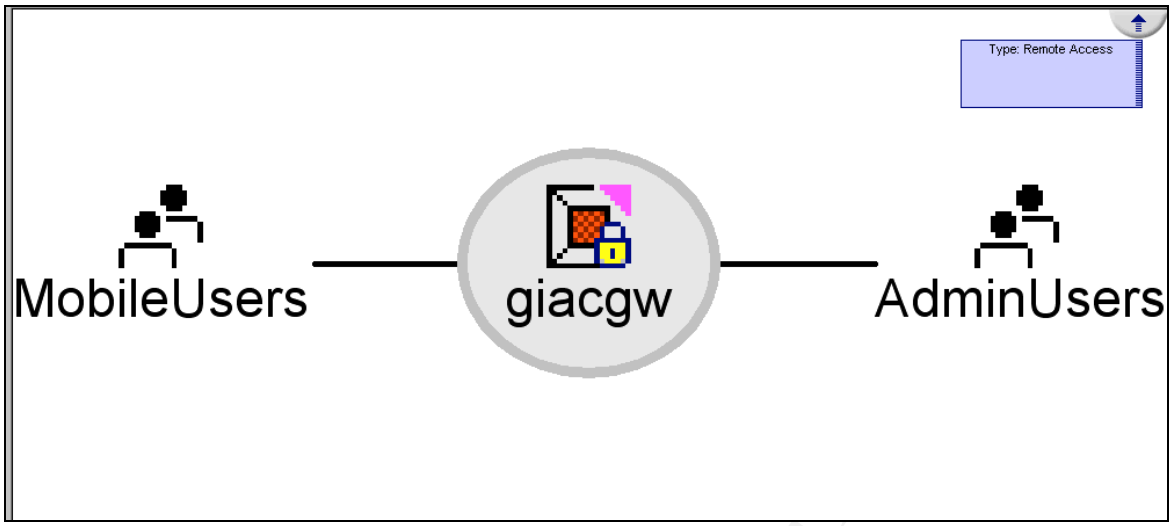


Diagram 3-4 Remote Access VPN

AS shown in diagrams 3-4 and 3-5, it is apparent that no actual VPN characteristics are configured within this part of the rulebase. This data is configured on a per user basis, although it is advisable to force these properties on all users from the “Global Properties”, under the Remote Access tag. The configuration of this is shown in Diagram 3-6.

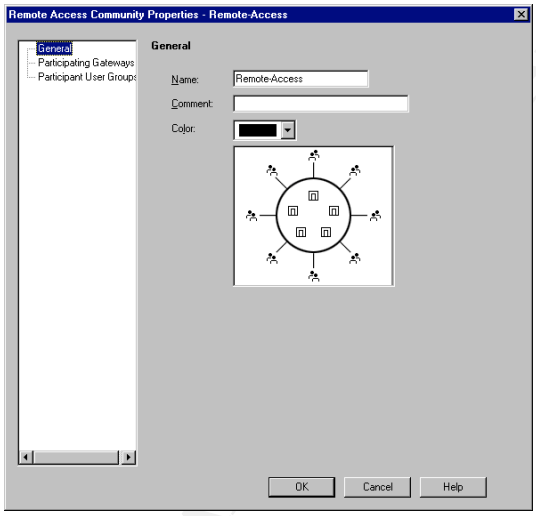


Diagram 3-5 Remote Access VPN Configuration.

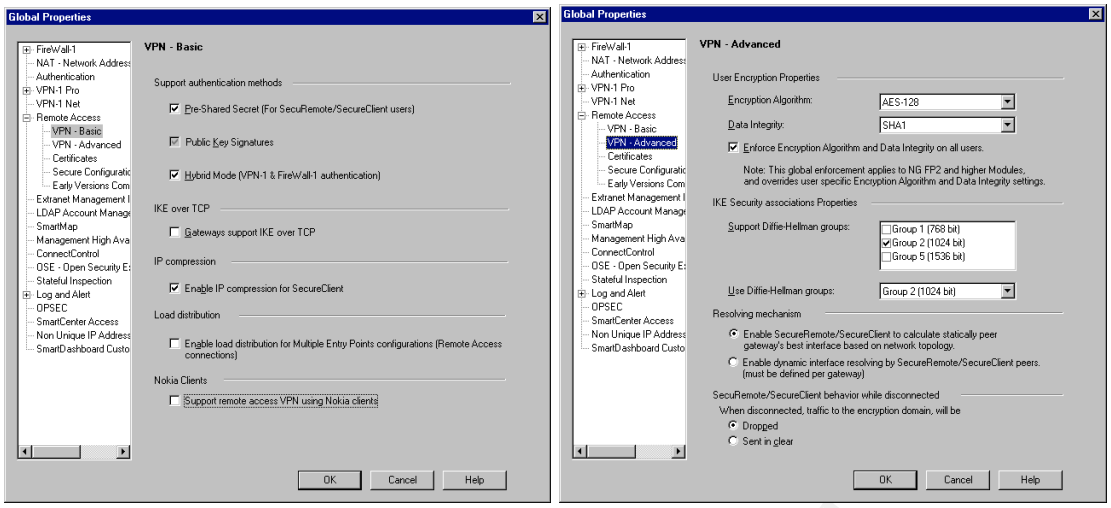


Diagram 3-6 Remote Access VPN Configuration within Global Policy

3.4.4 Server Management and Cleanup Rules

The last few rules on the rulebase deal with management of the devices on the network, along with the cleanup rule at the end of the rulebase. Up to this point, all connections, except for the remote user VPN connections, have been server to server connections.

In this last part of the rulebase, the rules for server monitoring and management exist. These rules define access for the BigBrother monitoring system, but more importantly, deal with administrator access to all front-end servers. As these servers are highly vulnerable, only administration staff with the correct knowledge are allowed access, and then only after logging onto a server on the admin LAN. All connections for this access are authenticated, with full logging being employed, and are limited to a selection of services as shown below.

26	AdminUsers@Admin-L	GIAC-Frontend-LANs	Any Traffic	TCP Terminal TCP SSH TCP MS-SQL-Server TCP http TCP https TCP Interscan-Control TCP telnet UDP snmp	Client Aut	Log	Policy	A	Authenticated access from Admin LAN to all frontend systems

The final two rules in the rulebase are used to drop all the unwanted traffic, but to keep the logs clean, NBT services and bootp are dropped but not logged. Any other services that could be considered noise would be added to this rule. Drop is used as it ignores, but logs the unwanted traffic. Anybody trying to connect, who is dropped, will have to wait for TCP timeout before trying a new connection.

29	Any	Any	Any Traffic	NBT UDP bootp	drop	None	Polic		Don't log noise
30	Any	Any	Any Traffic	Any	drop	Log	Polic		Drop and log all other connections.

3.4.5 SmartDefense

"SmartDefense provides a unified security framework for various components that identify and prevent cyber attacks. In addition to the security enforcement policy, defined in the rule base, SmartDefense unobtrusively analyses activity across your network, tracking potentially threatening events and optionally sending notification."

This statement from the initial screen of the SmartDefense tab within the firewall policy probably best describes it. SmartDefense itself is split into two parts, Network Security and Application Intelligence (AI). Both of these sections may be mainly left as default, unless there is a good reason to modify a setting. The only setting that should be investigated is SYNDefender, or "SYN Attack configuration", as described in the next section.

3.4.6 SYNDefender or "SYN Attack Configuration"

Within NG with AI, SYNDefender has been changed and is a more flexible tool than it used to be. It is considered good practice to employ SYNDefender in the new SYN Attack protection mode where the firewall module runs as a passive syn gateway, unless it detects an attack. In this case it switches to syn relay defence mode and handles all SYN connections. The only problem with this mode of operation is that when the firewall module changes to an active syn gateway, it does so for all connections, thus increasing the load on the firewall module.

3.4.7 Logging and Log Switching

Logging is always a question of taste. Some people like to log all traffic through the firewall with a few exceptions, others feel that only certain traffic needs to be logged. Over time I have found that one of the biggest overheads that a firewall module faces is producing logs for what could be called normal traffic, sometimes causing the firewall module to stop working due to high logging levels. What is required, are logs that are meaningful and will capture unusual and abnormal traffic patterns.

In the design detailed above, logging is performed for all management connections to servers on the front-end networks as well as the firewalls, remote access by mobile workers, and all dropped traffic. All other traffic through the firewall is either logged by an intermediate server, as in the case of the proxy server and mail-relay server, or is logged by the server it is connecting to. Therefore, it is possible to obtain full details of what is passing through the firewall module without overloading it.

When looking through the log files, it is helpful if they are not too large. To aid this, regular log switching must be undertaken. In versions of CheckPoint Firewall-1previous to NG, logs had to be switched, either using a scheduled command, or manually.

Within NG, this has been changed so you can configure log switching from within the management/logging object. Diagram 3-7 shows this as configured for the Firewall management host shown in this design.

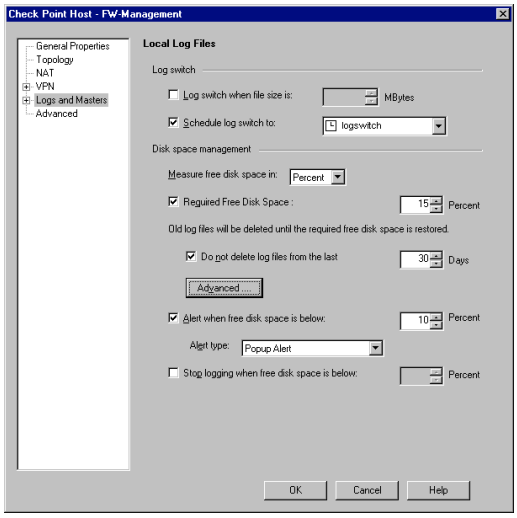


Diagram 3-7 Cofiguration of Log Switching

4 Assignment 3 – Verify the Firewall Policy

4.1 Introduction

The firewall policy described in section 3.3 has been implemented, and now the management of GIAC Enterprises require that it is fully verified. They require assurance that traffic is flowing as required, and also that unwanted traffic is not getting through the firewall and connecting to the front-end servers.

As with all e-commerce web sites, there are peaks and troughs during the day, with the quietest period being between 1 am and 6 am, and the quietest day being Sunday.

Unfortunately, I have not been able to build the firewalls surrounding this design, so the discussion will be theoretical, with expected results rather than practical results.

4.2 Management Buy-In

As with all tasks regarding the security of GIAC Enterprises existence, it is important that Management is involved from the very beginning. With this in mind, and to ensure management approval from the beginning, we must first look at what is at stake, i.e. the data that GIAC Enterprises is founded on, and that which it relies on.

A meeting was called with senior management to discuss the issues of firewall validation and security in general. One of the issues with validating the firewall is the fact that the site should be taken down for the duration to ensure that no spurious data is allowed to interfere with the validation. Following this discussion, it was decided that the system could be taken down between 1and 6am Sunday Morning, as this is the quietest period within GIAC Enterprises week. During this time, the web site would be displaying a banner to advise that the system is down.

In addition to the system down message, a message warning about the downtime is to be posted on the website for a week in advance of the validation work.

It was felt that two people would be required for the validation process, firstly to ensure two sets of eyes are overseeing the work, as well as the two sets checking all the data collected to ensure that the validation process provides no issues to the e-business site as a whole.

Management were made aware that the validation work is only for looking at the firewall security policy and will not be looking at any vulnerabilities that may be present in the servers and applications that form the e-business site.

4.3 Verification Methodology

The verification of the firewall policy, should not only look at traffic flowing from the outside inwards, but needs to look at possible traffic flow between different network segments. Performing a series of scans between all network segments, although taking a large amount of time, will provide us with a complete picture of the ports that are open as well as those that are filtered.

To perform basic scanning nmap[4] will be used as it is a very versatile tool, capable of scanning large numbers of hosts in a short time frame.

One the scanning has been performed, the results should show what access is available between networks, and therefore validate the security policy.

To further increase the usefulness of the scans, it was agreed with GIAC Enterprises management to shutdown the web site for a period, so that scanners could be implemented with the addresses of the actual hosts in the network. For each scan from a single point, e.g. from the B2B LAN, the server, e.g. the B2B server, is shutdown, and a scanner is put in place that has the same IP address as the server it replaces. This method of replacing the servers in the network with scanners, although interrupting business, allows the greatest level of validation of the firewall policy.

Scans on the source network of the device are designed to probe the firewall for access, and therefore all results not related to the firewall for these scans have been ignored.

4.4 Scanning the Networks

To get the best results, multiple scans will be run against each network, using different hosts to perform the scan, one being a host that is allowed some access and one that is denied all access. In the event of no hosts on a subnet having access, then only one host will be used for the scan.

To fully test each possible connection, three scans will be employed. These are an icmp scan, a TCP Syn scan, and a UDP scan.

The three scans are similar in design, but use three different switches as described below.

icmp echo-request Scan:	-sP
TCP Syn Scan:	-sS
UDP Scan:	-sU

The nmap command line for icmp scans is:

```
nmap –sP LowIPAddress-HighIPAddress
```

or

```
nmap –sP NetworkIP/Netmask
```

For UDP and TCP scans, an extra switch is required to ensure an echo-request is not sent during the scan, and another switch is added to ensure all ports are scanned. These two scans are:

-P0	Don't ping the host before scanning,
-p 1-65535	Scan all ports between 1 and 65535.

The nmap command line for TCP and UDP scans look like:

```
nmap –sS –p 1-65535 –P0 LowIPAddress-HighIPAddress
nmap –sU –p 1-65535 –P0 LowIPAddress-HighIPAddress
```

or

```
nmap –sS –p 1-65535 –P0 NetworkIP/Netmask
nmap –sU –p 1-65535 –P0 NetworkIP/Netmask
```

Where

LowIPAddress:	First IP Address to be scanned
HighIPAddress:	Last IP Address to be scanned

and

NetworkIP:	Network IP Address
Netmask:	Network Netmask.

For example, the three scans directed at the Web LAN would look as follows:

```
nmap -sP 10.44.254.0/25
nmap -sS -p 1-65535 -P0 10.44.254.0/25
nmap -sU -p 1-65535 -P0 10.44.254.0/25
```

These scans would be performed from hosts on all other networks within GIAC Enterprises front-end networks to see what services are available.

In practice, the scans are run from each network against all others, which although increases the scanning time, ensures the validity of the results by scanning through the firewall, on an open port, onto the actual host.

In addition to scanning the internal networks, an extra host has been configured on the Internet with web, ftp and mail services running for scanning from the internal networks. This device has an IP address of 80.200.10.51.

Scans performed in the manner described above can have one of three results.

- Open: traffic is allowed through the firewall to connect to a service that is running.

- Closed: traffic is allowed through firewall, but there is no service running to connect to.

- Filtered: traffic is dropped by the firewall module with no icmp error messages or TCP resets being sent back to the originating server.

These three possible results will show us what the firewall is allowing and blocking, but will also let us glimpse at what services are running on the hosts scanned.

In addition, sniffers running tcpdump have been placed within the network for the duration of the scan, recording and double-checking what the scanner really is seeing. Sample outputs from these sniffers have been included below the results of the nmap scan to uphold the data gathered. Where a Network IDS sensor has been implemented, a sniffer is used to replace that device for the duration of the audit. I have shown part of the tcpdump output from the sniffers for two scans, one being between the Users LAN and the Access LAN, and the other between the Admin LAN and the Access LAN post authentication.

4.4.1 Scanning from the Users LAN

The first set of scans performed is from the Users LAN, scanning all networks behind the firewall, as well as a host outside of the firewall. Due to the nature of this network, only one source was used.

The only expected result is TCP port 1080 for access to the proxy server.

The table below details these scans, their origin, and the response.

Source	Scan	Result
Users LAN	Nmap –sP 10.44.60.0/24	0 hosts up
10.44.0.1	Nmap –sP 10.44.248.0/24	0 hosts up
	Nmap –sP 10.44.253.0/29	0 hosts up
	Nmap –sP 10.44.254.0/24	0 hosts up
	Nmap –sP 80.169.251.0/28	0 hosts up
	Nmap –sP 80.200.10.51	0 hosts up
	Nmap –sS –P0 –p 1-65535 10.44.60.0/24	All filtered.
	Nmap –sS –P0 –p 1-65535 10.44.248.0/24	Port 1080 open to 10.44.248.100, rest filtered
	Nmap –sS –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sS –P0 –p 1-65535 80.200.10.51	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.60.0/24	All filtered.
	Nmap –sU –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.253.0/29	All filtered

	Nmap –sU –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sU –P0 –p 1-65535 80.200.10.51	All filtered

The nmap scan between the Users LAN and the Access LAN gives us the following tcpdump data. Using the tcpdump from the sniffer on the Link LAN, the only port open was TCP 1080 on the proxy server, all others showed up as TCP timeouts as shown in the sample below.

```
: : .  l . . . .  . . . . : S
   :  win
: : .  l . . . .  . . . . : S
   :  win
: : .  l . . . .  . . . . : S
   :  win
: : .  l . . . .  . . . . : S
   :  win
: : .  l . . . .  . . . . : S
   :  win
: : .  l . . . .  . . . . : S
: : . :  l . . .  win . . . . : S
   :  win
: : .  l . . . .  . . . . : S
   :  ack  win  mss
DF
: : .  l . . . .  . . . . : S
   :  win
: : .  l . . . .  . . . . : S
   :  win
: : .  l . . . .  . . . . : S
   :  win
```

Looking at the tcpdump output from the sniffer on the Access LAN, the following was seen, with no other connections showing up.

```
: : .  l . . . .  . . . . : S
   :  win
: : .  l . . . .  . . . . : S
   :  ack  win  mss
DF
```

The results, tabulated above, and verified by the tcpdump outputs, verify access to the proxy server on TCP port 1080, with all other ports being filtered by the firewall.

4.4.2 Scanning from the Admin LAN

Two sets of scans were performed from the Admin LAN, the first set with no authentication on the firewall, and the second set as an authenticated user. The only expected results are when the connections are authenticated, and within the results gathered, both open and closed ports are recorded. This is due to the hosts having limited services available. This second has partial tcpdump data to backup the information recorded within nmap.

The table below details these scans, their origin, and the response.

Source	Scan	Result
Admin LAN	Nmap –sP 10.44.60.0/24	0 hosts up
10.44.20.1	Nmap –sP 10.44.248.0/24	0 hosts up
	Nmap –sP 10.44.253.0/29	0 hosts up
	Nmap –sP 10.44.254.0/24	0 hosts up
	Nmap –sP 80.169.251.0/28	0 hosts up
	Nmap –sP 80.200.10.51	0 hosts up
	Nmap –sS –P0 –p 1-65535 10.44.60.0/24	Port 259 open to 10.44.60.252, 253 & 254. All rest filtered.
	Nmap –sS –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sS –P0 –p 1-65535 80.200.10.51	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sU –P0 –p 1-65535 80.200.10.51	All filtered
10.44.20.1	Nmap –sP 10.44.60.0/24	0 hosts up
Authenticated	Nmap –sP 10.44.248.0/24	0 hosts up
	Nmap –sP 10.44.253.0/29	0 hosts up
	Nmap –sP 10.44.254.0/24	0 hosts up
	Nmap –sP 80.169.251.0/28	0 hosts up
	Nmap –sP 80.200.10.51	0 hosts up
	Nmap –sS –P0 –p 1-65535 10.44.60.0/24	Ports 22, 259 and 443 open to 10.44.60.252, 253 & 254. All rest filtered.
	Nmap –sS –P0 –p 1-65535 10.44.248.0/24	Ports 22 & 1812 open, ports 23, 3389, 1433, 80 & 443 closed on 10.44.248.10 & .20. All rest filtered.
	Nmap –sS –P0 –p 1-65535 10.44.253.0/29	Port 22 open, ports 23, 1812, 3389, 1433, 80 & 443 closed on 10.44.253.1. All rest filtered.

	Nmap –sS –P0 –p 1-65535 10.44.254.0/24	Ports 3389, 80 & 443 open, ports 22, 23, 1433& 1812 closed on 10.44.254.10, 20. Ports 80 & 443 open, ports 3389, 1433, 22, 23 & 1812 closed on 10.44.254.100. Port 22 open, ports 3389, 1433, 80, 442, 1812 & 23 closed on 10.44.254.120 & 121. Ports 3389 & 1433 open, ports 22, 80, 443, 1812 & 23 closed on 10.44.254.129, 130, 131 & 132. Rest filtered.
	Nmap –sS –P0 –p 1-65535 80.169.251.0/28	Port 23 open, ports 3389, 22, 1433, 80, 443 & 1812 closed on 80.169.251.1. Rest filtered.
	Nmap –sS –P0 –p 1-65535 80.200.10.51	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.248.0/24	Port 161 closed on 10.44.248.10 & 20, rest filtered.
	Nmap –sU –P0 –p 1-65535 10.44.253.0/29	Port 161 closed on 10.44.253.1, rest filtered.
	Nmap –sU –P0 –p 1-65535 10.44.254.0/24	Port 161 closed on 10.44.254.10, 20, 100, 120, 121, 129, 130, 131 & 132, rest filtered.
	Nmap –sU –P0 –p 1-65535 80.169.251.0/28	Port 161 open on 80.169.251.1, rest filtered.
	Nmap –sU –P0 –p 1-65535 80.200.10.51	All filtered

When running the scan against all networks, with no authentication, the only response is from the firewall itself showing TCP port 259 being open for client authentication.

With the connection authenticated, TCP ports 22, 259 and 443 are open on the firewall, allowing authentication, as well as management traffic for managing the firewall module's operating system.

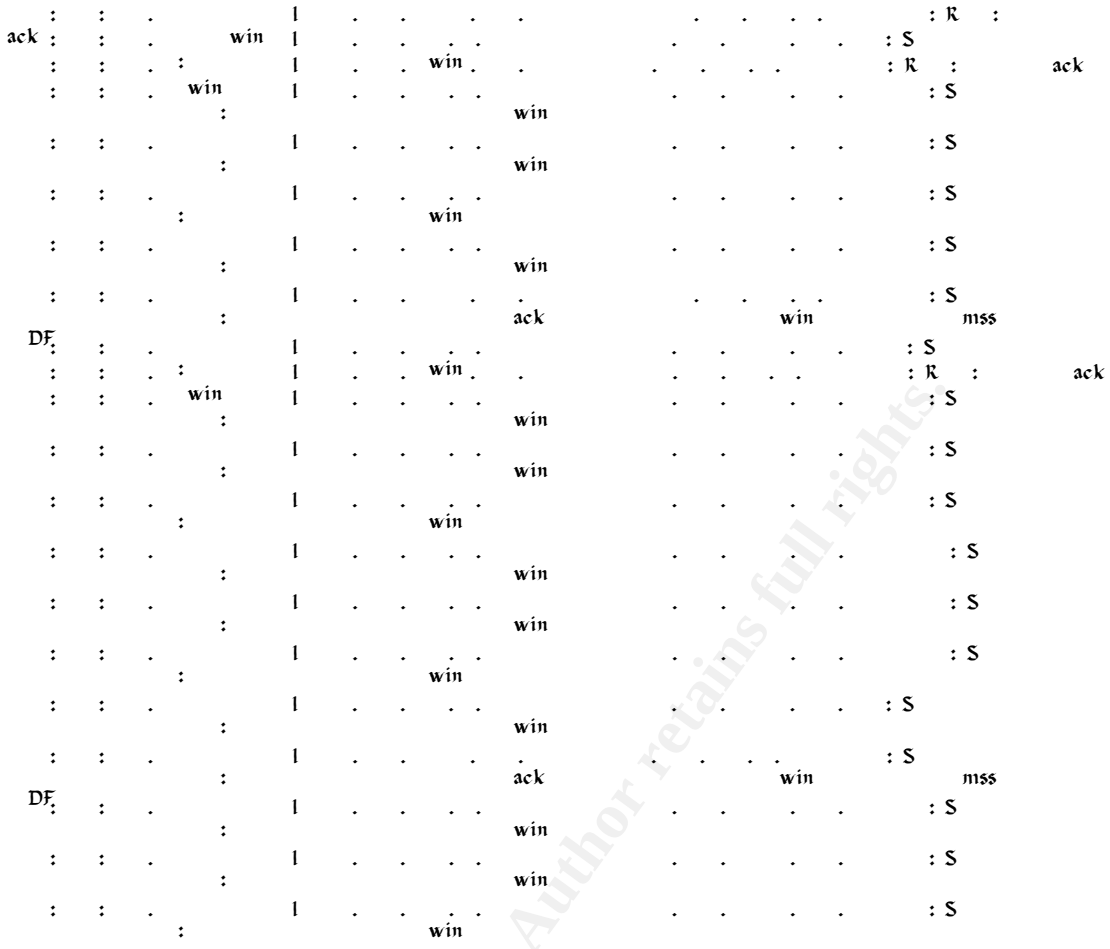
On the proxy and mail relay servers, the only ports that are open are TCP 22 and 1812, with TCP ports 23, 3389, 1433, 80 & 443 and UDP port 161 showing closed. These ports are allowed through the firewall, but the services they are for are not running on these servers. Likewise, for connections to the Web LAN, SQL LAN, B2B LAN, and the Boarder router, the expected services were shown as open, with services not running on the devices on those networks showing as closed. All other ports were dropped by the firewall and showed up as filtered.

The nmap scan between the Users LAN and the Access LAN gives us the following tcpdump data. Using the tcpdump from the sniffer on the Link LAN, the only ports open were TCP 22 and 1812, with TCP ports 23, 3389, 1433, 80 & 443 showing closed on the proxy server, all others showed up as TCP timeouts as shown in the sample below.

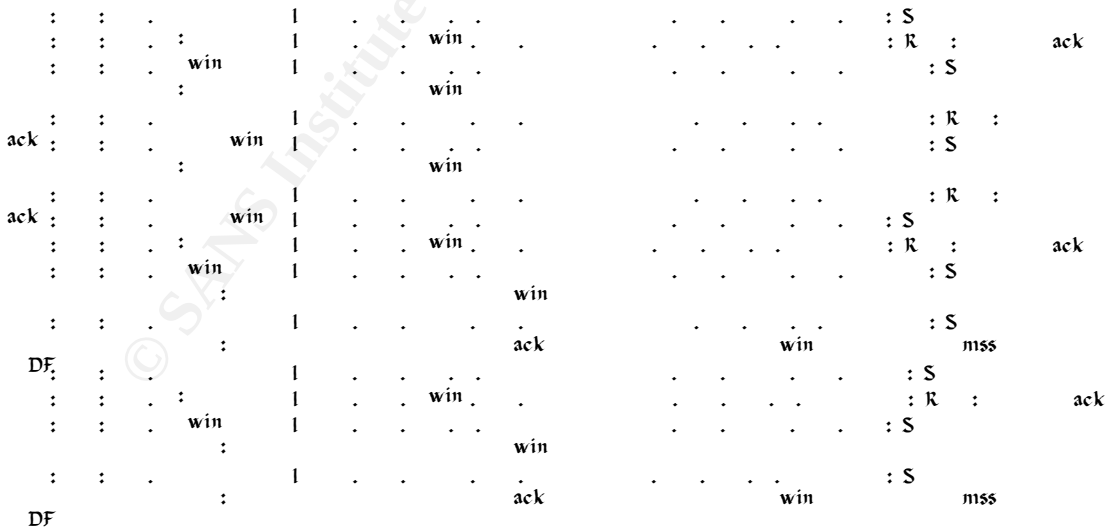
```
 : : .        l  . . . .        . . . . . : S
        :                win
 : : .        l  . . . .        . . . . . : S
        :                win
 : : .        l  . . . .        . . . . . : S
     :              win
 : : .        l  . . . .        . . . . . : S
 : : . :      l  . . win .      . . . . . : R  :    ack
 : : .  win   l  . . . .        . . . . .  : S
        :                win
 : : .        l  . . . .        . . . . .  : S
        :                win
 : : .        l  . . . .        . . . . .  : S
     :              win
 : : .        l  . . . .        . . . . . : S
        :                win
 : : .        l  . . . .        . . . . . : S
        :                win
 : : .        l  . . . .        . . . . . : S
     :              win
 : : .        l  . . . .        . . . . . : S
     :              win
 : : .        l  . . . .        . . . . . : R  :
ack : : .  win  l  . . . .      . . . . . : S
        :                win
 : : .        l  . . . .        . . . . . : S
        :                win
 : : .        l  . . . .        . . . . . : S
     :              win
 : : .        l  . . . .        . . . . . : S
        :                win
 : : .        l  . . . .        . . . . . : S
        :                win
 : : .        l  . . . .        . . . . . : S
     :              win
```

Time GAP

```
 : : .        l  . . . .        . . . . . : S
     :              win
```



Looking at the tcpdump output from the sniffer on the Access LAN, the following was seen, with no other connections showing up.



These results are as expected, and show that not only is the firewall doing its job, but also only services required are running on the devices scanned, and all unrequired services have been shutdown.

4.4.3 Scanning from the Server LAN

Three scans are run from the Server LAN, one from an IP address that has no access, and two from servers IP addresses that have limited access. These scans should show any holes in the firewall from the Server LAN to the front-end networks, which is important as all users have access to the machines on the Server LAN.

The table below details these scans, their origin, and the response.

Source	Scan	Result
Server LAN	Nmap –sP 10.44.60.0/24	0 hosts up
10.44.50.1	Nmap –sP 10.44.248.0/24	0 hosts up
	Nmap –sP 10.44.253.0/29	0 hosts up
	Nmap –sP 10.44.254.0/24	0 hosts up
	Nmap –sP 80.169.251.0/28	0 hosts up
	Nmap –sP 80.200.10.51	0 hosts up
	Nmap –sS –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sS –P0 –p 1-65535 80.200.10.51	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sU –P0 –p 1-65535 80.200.10.51	All filtered
10.44.50.10 (giacbb01)	Nmap –sP 10.44.248.0/24	5 Hosts up: 10.44.248.10 10.44.248.20 10.44.248.252 10.44.248.253 10.44.248.254
	Nmap –sP 10.44.253.0/29	4 Hosts up: 10.44.253.1 10.44.253.4 10.44.253.5 10.44.254.6

	Nmap –sP 10.44.254.0/24	18 hosts up: 10.44.254.10 10.44.254.20 10.44.254.120 10.44.254.121 10.44.254.129 10.44.254.130 10.44.254.131 10.44.254.132 10.44.254.124 10.44.254.125 10.44.254.126 10.44.254.129 10.44.254.130 10.44.254.131 10.44.254.132 10.44.254.252 10.44.254.253 10.44.254.254
	Nmap –sP 80.169.251.0/28	4 hosts up 80.169.251.1 80.169.251.12 80.169.251.13 80.169.251.14
	Nmap –sP 80.200.10.51	0 hosts up
	Nmap –sS –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sS –P0 –p 1-65535 80.200.10.51	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sU –P0 –p 1-65535 80.200.10.51	All filtered
10.44.50.120	Nmap –sP 10.44.60.0/24	0 hosts up
(giacmail01)	Nmap –sP 10.44.248.0/24	0 hosts up
	Nmap –sP 10.44.253.0/29	0 hosts up
	Nmap –sP 10.44.254.0/24	0 hosts up
	Nmap –sP 80.169.251.0/28	0 hosts up
	Nmap –sP 80.200.10.51	0 hosts up
	Nmap –sS –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.248.0/24	Port 25 open to 10.44.248.10, rest filtered
	Nmap –sS –P0 –p 1-65535 10.44.253.0/29	All filtered

	Nmap –sS –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sS –P0 –p 1-65535 80.200.10.51	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sU –P0 –p 1-65535 80.200.10.51	All filtered
10.44.50.130	Nmap –sP 10.44.60.0/24	0 hosts up
(giacsqlcl01)	Nmap –sP 10.44.248.0/24	0 hosts up
	Nmap –sP 10.44.253.0/29	0 hosts up
	Nmap –sP 10.44.254.0/24	0 hosts up
	Nmap –sP 80.169.251.0/28	0 hosts up
	Nmap –sP 80.200.10.51	0 hosts up
	Nmap –sS –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.253.0/29	Port 9245 open to 10.44.253.1, rest filtered.
	Nmap –sS –P0 –p 1-65535 10.44.254.0/24	Port 1433 open to 10.44.254.129, rest filtered.
	Nmap –sS –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sS –P0 –p 1-65535 80.200.10.51	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sU –P0 –p 1-65535 80.200.10.51	All filtered

As expected there is limited access from the Server LAN to any other networks that are screened by the firewall. The internal mail server can connect to the mail relay server to forward outgoing e-mails, and the internal SQL server cluster can connect to the front-end SQL server cluster via SQL and the B2B server on TCP port 9245. In addition to this, the BigBrother server can ping all the servers on the front-end networks as expected, but is unable to connect to any other device using either TCP or UDP ports.

4.4.4 Scanning from the Link LAN

Scans from the Link LAN, to all other networks should show no access, as this network is designed to link the main firewalls to the back-end networks via the internal routers. The only device attached to this network is the Network IDS sensor which looks at all traffic flowing across this network.

The table below details these scans, their origin, and the response.

Source	Scan	Result
Link LAN	Nmap –sP 10.44.60.0/24	0 hosts up
10.44.60.1	Nmap –sP 10.44.248.0/24	0 hosts up
	Nmap –sP 10.44.253.0/29	0 hosts up
	Nmap –sP 10.44.254.0/24	0 hosts up
	Nmap –sP 80.169.251.0/28	0 hosts up
	Nmap –sP 80.200.10.51	0 hosts up
	Nmap –sS –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.253.0/29	All filtered.
	Nmap –sS –P0 –p 1-65535 10.44.254.0/24	All filtered.
	Nmap –sS –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sS –P0 –p 1-65535 80.200.10.51	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sU –P0 –p 1-65535 80.200.10.51	All filtered

As expected, the Link LAN has no connectivity onto any device on any front-end network. This shows that this network is only capable of acting as an interconnection network between the main firewalls and the internal routers.

4.4.5 Scanning from the Access LAN

Scans from the Access LAN is run from three IP addresses, as this shows full verification of the firewall policy for connections from this network. These IP addresses have been chosen, as two should have limited access, and the third has no access whatsoever.

The table below details these scans, their origin, and the response.

Source	Scan	Result
Access LAN	Nmap –sP 10.44.0.0/23	0 hosts up
10.44.248.1	Nmap –sP 10.44.20.0/24	0 hosts up
	Nmap –sP 10.44.21.0/24	0 hosts up
	Nmap –sP 10.44.50.0/24	0 Hosts up
	Nmap –sP 10.44.60.0/24	0 Hosts up

	Nmap –sP 10.44.248.0/24	0 Hosts up
	Nmap –sP 10.44.253.0/29	0 Hosts up
	Nmap –sP 10.44.254.0/24	0 Hosts up
	Nmap –sP 80.169.251.0/28	0 hosts up
	Nmap –sP 80.200.10.51	0 hosts up
	Nmap –sS –P0 –p 1-65535 10.44.0.0/23	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.20.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.21.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.50.0/24	Port 1984 open to 10.44.50.10, rest filtered.
	Nmap –sS –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sS –P0 –p 1-65535 80.200.10.51	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.0.0/23	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.20.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.21.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.50.0/24	Port 162 & 514 open to 10.44.50.10, rest filtered.
	Nmap –sU –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sU –P0 –p 1-65535 80.200.10.51	All filtered
10.44.248.10	Nmap –sP 10.44.0.0/23	0 hosts up
(giacmail02)	Nmap –sP 10.44.20.0/24	0 hosts up
	Nmap –sP 10.44.21.0/24	0 hosts up
	Nmap –sP 10.44.50.0/24	0 Hosts up
	Nmap –sP 10.44.60.0/24	0 Hosts up
	Nmap –sP 10.44.248.0/24	0 Hosts up
	Nmap –sP 10.44.253.0/29	0 Hosts up
	Nmap –sP 10.44.254.0/24	0 Hosts up
	Nmap –sP 80.169.251.0/28	0 hosts up
	Nmap –sP 80.200.10.51	0 hosts up
	Nmap –sS –P0 –p 1-65535 10.44.0.0/23	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.20.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.21.0/24	All filtered

	Nmap –sS –P0 –p 1-65535 10.44.50.0/24	Port 25 open to 10.44.50.120 & 1984 open to 10.44.50.10, rest filtered.
	Nmap –sS –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sS –P0 –p 1-65535 80.200.10.51	Port 25 open to 80.200.10.51, rest filtered.
	Nmap –sU –P0 –p 1-65535 10.44.0.0/23	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.20.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.21.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.50.0/29	Port 162 & 514 open to 10.44.50.10, rest filtered.
	Nmap –sU –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sU –P0 –p 1-65535 80.200.10.51	Port 53 closed, rest filtered.
10.44.248.20	Nmap –sP 10.44.0.0/23	0 hosts up
(giacproxy01)	Nmap –sP 10.44.20.0/24	0 hosts up
	Nmap –sP 10.44.21.0/24	0 hosts up
	Nmap –sP 10.44.50.0/24	0 Hosts up
	Nmap –sP 10.44.60.0/24	0 Hosts up
	Nmap –sP 10.44.248.0/24	0 Hosts up
	Nmap –sP 10.44.253.0/29	0 Hosts up
	Nmap –sP 10.44.254.0/24	0 Hosts up
	Nmap –sP 80.169.251.0/28	0 hosts up
	Nmap –sP 80.200.10.51	0 hosts up
	Nmap –sS –P0 –p 1-65535 10.44.0.0/23	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.20.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.21.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.50.0/24	Port 1984 open to 10.44.50.10, rest filtered.
	Nmap –sS –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.253.0/29	All filtered

	Nmap –sS –P0 –p 1-65535 10.44.254.0/24	Port 80 & 443 open to 10.44.254.100, rest filtered.
	Nmap –sS –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sS –P0 –p 1-65535 80.200.10.51	Port 21, 80 & 443 open to 80.200.10.51, rest filtered.
	Nmap –sU –P0 –p 1-65535 10.44.0.0/23	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.20.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.21.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.50.0/29	Port 162 & 514 open to 10.44.50.10, rest filtered.
	Nmap –sU –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sU –P0 –p 1-65535 80.200.10.51	Port 53 closed, rest filtered.

These results show that all devices on this network can connect to the BigBrother server on TCP port 1984 and UDP ports 162 and 514. The ideal would be that only servers which require access should to BigBrother should get it.

In addition to this, the mail relay server is only able to access the internal mail system on TCP port 25 and any external device on both TCP port 25 and UDP port 53.

Also the proxy server can connect to the GIAC Enterprises web site using TCP Ports 80 and 443, and can connect to any device on the Internet using TCP ports 21, 80 and 443 and UDP port 53.

These results are as expected, but start to show that there are servers within the front-end networks that have more access to the BigBrother server than is required.

4.4.6 Scanning from the B2B LAN

Scans from the B2B LAN should show access to the BigBrother server only, as the B2B server has limited access capabilities.

The table below details these scans, their origin, and the response.

Source	Scan	Result
B2B LAN	Nmap –sP 10.44.0.0/23	0 hosts up
10.44.253.1	Nmap –sP 10.44.20.0/24	0 hosts up
	Nmap –sP 10.44.21.0/24	0 hosts up
	Nmap –sP 10.44.50.0/24	0 Hosts up
	Nmap –sP 10.44.60.0/24	0 Hosts up
	Nmap –sP 10.44.248.0/24	0 Hosts up
	Nmap –sP 10.44.253.0/29	0 Hosts up
	Nmap –sP 10.44.254.0/24	0 Hosts up
	Nmap –sP 80.169.251.0/28	0 hosts up
	Nmap –sP 80.200.10.51	0 hosts up
	Nmap –sS –P0 –p 1-65535 10.44.0.0/23	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.20.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.21.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.50.0/24	Port 1984 open to 10.44.50.10, rest filtered.
	Nmap –sS –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sS –P0 –p 1-65535 80.200.10.51	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.0.0/23	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.20.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.21.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.50.0/24	Port 162 & 514 open to 10.44.50.10, rest filtered.
	Nmap –sU –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sU –P0 –p 1-65535 80.200.10.51	All filtered

This scan shows that the only access from the B2B server is to the BigBrother server on TCP port 1984 and UDP ports 162 and 514 as expected. In this case, UDP 162 – snmp-trap probably is not required.

4.4.7 Scanning from the WEB LAN

Servers on the Web LAN have limited access, as required by the application. The expected access from servers on the Web LAN is to the e-business database cluster, to the internal BigBrother server, and externally to the payment server.

The table below details these scans, their origin, and the response.

Source	Scan	Result
WEB LAN	Nmap –sP 10.44.0.0/23	0 hosts up
10.44.254.1	Nmap –sP 10.44.20.0/24	0 hosts up
	Nmap –sP 10.44.21.0/24	0 hosts up
	Nmap –sP 10.44.50.0/24	0 Hosts up
	Nmap –sP 10.44.60.0/24	0 Hosts up
	Nmap –sP 10.44.248.0/24	0 Hosts up
	Nmap –sP 10.44.253.0/29	0 Hosts up
	Nmap –sP 10.44.254.0/25	0 Hosts up
	Nmap –sP 10.44.254.128/25	0 Hosts up
	Nmap –sP 80.169.251.0/28	0 hosts up
	Nmap –sP 80.200.10.51	0 hosts up
	Nmap –sP 213.52.208.67	0 hosts up
	Nmap –sS –P0 –p 1-65535 10.44.0.0/23	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.20.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.21.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.50.0/24	Port 1984 open to 10.44.50.10, rest filtered.
	Nmap –sS –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.254.0/25	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.254.128/25	All filtered
	Nmap –sS –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sS –P0 –p 1-65535 80.200.10.51	All filtered
	Nmap –sS –P0 –p 1-65535 213.52.208.67	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.0.0/23	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.20.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.21.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.50.0/24	Port 162 & 514 open to 10.44.50.10, rest filtered.
	Nmap –sU –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.254.0/25	All filtered

	Nmap –sU –P0 –p 1-65535 10.44.254.128/25	All filtered
	Nmap –sU –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sU –P0 –p 1-65535 80.200.10.51	All filtered
	Nmap –sU –P0 –p 1-65535 213.52.208.67	All filtered
10.44.254.10	Nmap –sP 10.44.0.0/23	0 hosts up
(giacweb01)	Nmap –sP 10.44.20.0/24	0 hosts up
	Nmap –sP 10.44.21.0/24	0 hosts up
	Nmap –sP 10.44.50.0/24	0 Hosts up
	Nmap –sP 10.44.60.0/24	0 Hosts up
	Nmap –sP 10.44.248.0/24	0 Hosts up
	Nmap –sP 10.44.253.0/29	0 Hosts up
	Nmap –sP 10.44.254.0/25	0 Hosts up
	Nmap –sP 10.44.254.128/25	0 Hosts up
	Nmap –sP 80.169.251.0/28	0 hosts up
	Nmap –sP 80.200.10.51	0 hosts up
	Nmap –sP 213.52.208.67	0 hosts up
	Nmap –sS –P0 –p 1-65535 10.44.0.0/23	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.20.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.21.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.50.0/24	Port 1984 open to 10.44.50.10, rest filtered.
	Nmap –sS –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.254.0/25	All filtered.
	Nmap –sS –P0 –p 1-65535 10.44.254.128/25	Port 1433 open to 10.44.254.129, All rest filtered.
	Nmap –sS –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sS –P0 –p 1-65535 80.200.10.51	All filtered
	Nmap –sS –P0 –p 1-65535 213.52.208.67	Port 443 open to 213.52.208.67, All rest filtered.
	Nmap –sU –P0 –p 1-65535 10.44.0.0/23	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.20.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.21.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.50.0/24	Port 162 & 514 open to 10.44.50.10. All rest filtered.
	Nmap –sU –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.254.0/25	All filtered
	Nmap –sU –P0 –p 1-65535	All filtered

	10.44.254.128/25	
	Nmap –sU –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sU –P0 –p 1-65535 80.200.10.51	All filtered
	Nmap –sU –P0 –p 1-65535 213.52.208.67	All filtered

As expected, this set of scans shows the limited access from the WEB LAN to all other GIAC Enterprises networks, with access being only to the e-business database cluster on TCP 1433, and the internal BigBrother server on TCP port 1984 and UDP ports 162 and 514. The only other connection that is possible from the web servers is on TCP port 443 to the web payment agency.

These connections are relevant for the application to work, but multiple possible connections to the BigBrother server could be used in an attack.

4.4.8 Scanning from the SQL LAN

The SQL servers require no access to any other part of GIAC Enterprises except for connections to BigBrother for monitoring of the operating system and the application.

The table below details these scans, their origin, and the response.

Source	Scan	Result
SQL LAN	Nmap –sP 10.44.0.0/23	0 hosts up
10.44.254.129	Nmap –sP 10.44.20.0/24	0 hosts up
(giacsqlcl10)	Nmap –sP 10.44.21.0/24	0 hosts up
	Nmap –sP 10.44.50.0/24	0 Hosts up
	Nmap –sP 10.44.60.0/24	0 Hosts up
	Nmap –sP 10.44.248.0/24	0 Hosts up
	Nmap –sP 10.44.253.0/29	0 Hosts up
	Nmap –sP 10.44.254.0/25	0 Hosts up
	Nmap –sP 10.44.254.128/25	0 Hosts up
	Nmap –sP 80.169.251.0/28	0 hosts up
	Nmap –sP 80.200.10.51	0 hosts up
	Nmap –sS –P0 –p 1-65535 10.44.0.0/23	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.20.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.21.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.50.0/24	Port 1984 open to 10.44.50.10, rest filtered.
	Nmap –sS –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.254.0/25	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.254.128/25	All filtered
	Nmap –sS –P0 –p 1-65535 80.169.251.0/28	All filtered

	Nmap –sS –P0 –p 1-65535 80.200.10.51	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.0.0/23	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.20.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.21.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.50.0/24	Port 162 & 514 open to 10.44.50.10, rest filtered.
	Nmap –sU –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.254.0/25	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.254.128/25	All filtered
	Nmap –sU –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sU –P0 –p 1-65535 80.200.10.51	All filtered
10.44.254.139	Nmap –sP 10.44.0.0/23	0 hosts up
	Nmap –sP 10.44.20.0/24	0 hosts up
	Nmap –sP 10.44.21.0/24	0 hosts up
	Nmap –sP 10.44.50.0/24	0 Hosts up
	Nmap –sP 10.44.60.0/24	0 Hosts up
	Nmap –sP 10.44.248.0/24	0 Hosts up
	Nmap –sP 10.44.253.0/29	0 Hosts up
	Nmap –sP 10.44.254.0/25	0 Hosts up
	Nmap –sP 10.44.254.128/25	0 Hosts up
	Nmap –sP 80.169.251.0/28	0 hosts up
	Nmap –sP 80.200.10.51	0 hosts up
	Nmap –sS –P0 –p 1-65535 10.44.0.0/23	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.20.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.21.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.50.0/24	Port 1984 open to 10.44.50.10, rest filtered.
	Nmap –sS –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.254.0/25	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.254.128/25	All filtered
	Nmap –sS –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sS –P0 –p 1-65535 80.200.10.51	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.0.0/23	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.20.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.21.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.50.0/24	Port 162 & 514 open to 10.44.50.10, rest

		filtered.
	Nmap –sU –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.254.0/25	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.254.128/25	All filtered
	Nmap –sU –P0 –p 1-65535 80.169.251.0/28	All filtered
	Nmap –sU –P0 –p 1-65535 80.200.10.51	All filtered

Again the only access that has been discovered from the SQL LAN is to the BigBrother server on TCP port 1984 and UDP ports 162 and 514.

Here, as with the Web LAN, too many possible connections to the BigBrother server could be used in attacking the system. Also, as shown by the second scan, a server could be placed onto this network having identical access as the servers that compromise the SQL cluster to the BigBrother server.

4.4.9 Scanning from the Public LAN

The boarded router is the only device on this network that requires limited access to internal networks for logging and monitoring traffic only. The boarder router sends all syslog traffic and snmp-traps back to the BigBrother server. No other device on this network should be able to access the internal networks.

The table below details these scans, their origin, and the response.

Source	Scan	Result
Internet LAN	Nmap –sP 10.44.0.0/23	0 hosts up
80.169.251.1	Nmap –sP 10.44.20.0/24	0 hosts up
(giac-ext-rout-01)	Nmap –sP 10.44.21.0/24	0 hosts up
	Nmap –sP 10.44.50.0/24	0 Hosts up
	Nmap –sP 10.44.60.0/24	0 Hosts up
	Nmap –sP 10.44.248.0/24	0 Hosts up
	Nmap –sP 10.44.253.0/29	0 Hosts up
	Nmap –sP 10.44.254.0/24	0 Hosts up
	Nmap –sP 80.169.251.0/28	0 Hosts up
	Nmap –sS –P0 –p 1-65535 10.44.0.0/23	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.20.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.21.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.50.0/24	Port 1984 open to 10.44.50.10, rest filtered.
	Nmap –sS –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.253.0/29	All filtered

	Nmap –sS –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 80.169.251.0/28	Port 264 open on 80.169.251.12, 13 & 14. All others filtered
	Nmap –sU –P0 –p 1-65535 10.44.0.0/23	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.20.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.21.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.50.0/24	Port 162 & 514 open to 10.44.50.10, rest filtered.
	Nmap –sU –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 80.169.251.0/28	Port 500 open on 80.169.251.12, 13 & 14. All others filtered
80.169.251.3	Nmap –sP 10.44.0.0/23	0 hosts up
	Nmap –sP 10.44.20.0/24	0 hosts up
	Nmap –sP 10.44.21.0/24	0 hosts up
	Nmap –sP 10.44.50.0/24	0 Hosts up
	Nmap –sP 10.44.60.0/24	0 Hosts up
	Nmap –sP 10.44.248.0/24	0 Hosts up
	Nmap –sP 10.44.253.0/29	0 Hosts up
	Nmap –sP 10.44.254.0/24	0 Hosts up
	Nmap –sP 80.169.251.0/28	0 Hosts up
	Nmap –sS –P0 –p 1-65535 10.44.0.0/23	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.20.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.21.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.50.0/24	Port 1984 open to 10.44.50.10, rest filtered.
	Nmap –sS –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sS –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sS –P0 –p 1-65535 80.169.251.0/28	Port 264 open on 80.169.251.12, 13 & 14. All others filtered
	Nmap –sU –P0 –p 1-65535 10.44.0.0/23	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.20.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.21.0/24	All filtered

	Nmap –sU –P0 –p 1-65535 10.44.50.0/24	Port 162 & 514 open to 10.44.50.10, rest filtered.
	Nmap –sU –P0 –p 1-65535 10.44.60.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.248.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.253.0/29	All filtered
	Nmap –sU –P0 –p 1-65535 10.44.254.0/24	All filtered
	Nmap –sU –P0 –p 1-65535 80.169.251.0/28	Port 500 open on 80.169.251.12, 13 & 14. All others filtered

As expected the only connections that are possible from the Internet router to GIAC Enterprises networks are to the BigBrother server on TCP port 1984 and UDP ports 162 and 514, as well as access to the firewall modules on TCP port 264 and UDP port 500. The second scan recorded shows that any device on the Public LAN can gain access to both the main firewalls and the BigBrother server.

The boarder router does not require all this connectivity to either the Firewall, or the BigBrother server. Access should be limited to UDP ports 162 and 514 only.

4.4.10 Scanning from the Internet

The final set of scans performed to verify the firewall policy is run from the temporary host on the Internet at 80.200.10.51. For these scans to be useful in verifying the firewall policy, the access lists on the boarder router were disabled.

The table below details these scans, their origin, and the response.

Source	Scan	Result
The Internet	Nmap –sP 80.169.251.0/28	0 hosts up
80.200.10.51	Nmap –sS –P0 –p 1-65535 80.169.251.0/28	Port 25 open on 80.169.251.6. Ports 80 & 443 open on 80.169.251.5. Port 264 open on 80.169.251.12, 13 & 14. All others filtered
	Nmap –sU –P0 –p 1-65535 80.169.251.0/28	Port 500 open on 80.169.251.12, 13 & 14. All others filtered

As expected, there is quite a bit that is visible from the Internet. Mail may be sent to the mail relay server on TCP port 25, both TCP ports 80 and 443 are open to the web site address, and TCP 264 and UDP port 500 are open on the Internet firewalls.

4.5 Scan Results Summary

All the scans were picked up by the firewall as such, with the default settings within the SmartDefense module logging the scans, and the firewall stealth rule and cleanup rule logging all dropped connections.

After analysing the results as shown above, it was agreed that the firewall configuration was as stated in the firewall policy, but a couple of points were noted with regard to server security.

As all servers can reach the BigBrother server on the Server LAN, it requires continued monitoring and patch updates as they are released. Although this is the normal policy for servers within GIAC Enterprises networks, the BigBrother server has been singled out as being a possible vulnerable access point to the internal networks if one of the servers within the front-end networks gets compromised.

In actual fact, the BigBrother server is assessable from all possible IP addresses on all the front-end networks, including the Public LAN between the boarder router and the main firewalls, opening it up for attack from any device that could be slotted into one of these network segments. Looking at this, shows that access to the BigBrother server should be as limited as possible, with servers only having the access that they require, rather than all devices on all networks having all possible access. This would reduce the possibility of attack leveraging on this weakness. As ever, the weakness is still the server and the software that it is running, even though BigBrother may be configured with some security settings to reduce the possibility of spoof data being sent.

It was also noted that although access from the Admin LAN to all front-end networks and the firewall is limited to authenticated sessions only, the logs of these connections should be monitored on a daily basis to ensure that they are not being abused.

5 Assignment 4 – Design Under Fire

5.1 Introduction

The final part of the assignment involves taking a previously submitted design and then putting it through a full attack. The design that I have selected is by Susan Delaney, and may be found at: http://www.giac.org/practical/GCFW/Susan_Delaney_GCFW.pdf.

Diagram 5-1 shows this design as a whole.

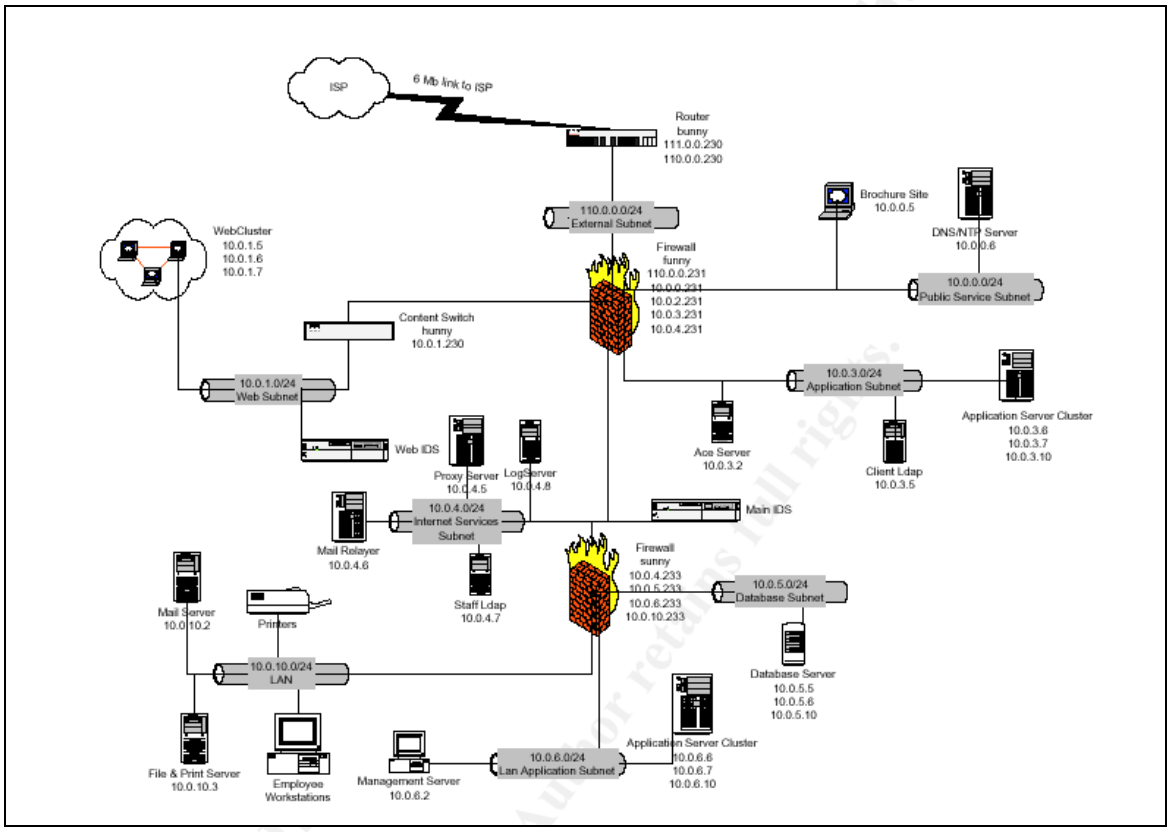


Diagram 5-1 Susan Delaney's Network Design

5.2 A Voyage of Discovery

Before starting the attack, it is important to obtain as much data about the site as possible. The initial point of contact for any site, is its DNA records, and a good starting point, is to look at the WHOIS information for GIAC.IE, this gives us the following data:

```
Organization:
   GIAC Enterprises
   xxxxxxxxxx
   xxxxxxxxxxx
   xxxxxxxxxx
   Ireland
   Phone: xxx-xxx-xxx
```

```
   Fax..: xxx-xxx-xxx
   Email: hostmaster@giac.ie

Registrar Name....: Register.com
Registrar Whois...: whois.register.com
Registrar Homepage: http://www.register.com

Domain Name: GIAC.IE

   Created on..............: Tue, Jul 03, 2001
   Expires on..............: Sat, Jul 03, 2004
   Record last updated on..: Tue, Sep 02, 2003

Administrative Contact:
   GIAC Enterprises
   xxxxxxxxxx
   xxxxxxxxxxx
   xxxxxxxxxx
   Ireland
   Phone: xxx-xxx-xxx
   Fax..: xxx-xxx-xxx
   Email: hostmaster@giac.ie

Technical Contact:
   GIAC Enterprises
   xxxxxxxxxx
   xxxxxxxxxxx
   xxxxxxxxxx
   Ireland
   Phone: xxx-xxx-xxx
   Fax..: xxx-xxx-xxx
   Email: hostmaster@giac.ie

Zone Contact:
   GIAC Enterprises
   xxxxxxxxxx
   xxxxxxxxxxx
   xxxxxxxxxx
   Ireland
   Phone: xxx-xxx-xxx
   Fax..: xxx-xxx-xxx
   Email: hostmaster@giac.ie

Domain servers in listed order:

NS1.GIAC.IE                                          110.0.0.6
NS.NET.IE                                            111.2.2.5
```


Although the administrator at GIAC Enterprises has done much to hide his/her identity we have some details. An address, a telephone number, a fax number and e-mail address. We also have details of GIAC Enterprise's domain servers.

The next thing to do, is to see which, if any, of the domain servers is within the public IP address range for GIAC Enterprises. For this, we will lookup the IP address of the web server; www.giac.ie.

```
C:\>nslookup
Default Server:  ns1.pop.net
Address:  80.100.65.19
> server 110.0.0.6
Default Server:  ns1.giac.ie
Address:  110.0.0.6
> set type=a
> www.giac.ie
Server:  ns1.giac.ie
Address:  110.0.0.6
Name:  www.giac.ie
Address:  110.0.0.5
```

This shows that the primary name server and the web server are within the same address space. Now try for mail servers.

```
> set type=mx
> giac.ie
Server:  ns1.giac.ie
Address:  110.0.0.6
giac.ie   MX preference = 10, mail exchanger = mx.giac.ie
```

Now to find the IP address for this server.

```
> set type=a
> mx.giac.ie
Name:  mx.giac.ie
Address:  110.0.0.7
>
```

So far I have gained the following information

The mail gateway and the main web server are within the same range of public IP addresses as the primary DNS server.

We can map the IP addresses as:

www	110.0.0.5
ns1	110.0.0.6
mx	110.0.0.7

To discover what else is within the 110.0.0.0/24 network further tests need to be run.

Firstly, let's have a look at www.giac.ie. After much digging through the site, a link to another site, in this case https://buy.giac.ie.

Performing a lookup for this device shows the following information:

>
> buy.giac.ie
Name: buy.giac.ie
Address: 110.0.0.2
>

Now it is time to perform a couple of scans on the 110.0.0.0/24 network. The best scan to perform should be invisible to the firewall, assuming that there is one, and any Intrusion Detection System that has been implemented. To do this, a very slow scan must be run, and as there is no time limit, a full TCP and udp scan will be run against each IP address. The only chance of detection is if an eagle eyed network/firewall administrator spots the trace.

The scans run for this is are:

Nmap –sS –T Paranoid –P0 –p 1-65535 110.0.0.0/24

and

nmap –sU –T Paranoid –P0 –p 1-65535 110.0.0.0/24

The following results were obtained:

IP Address	Ports	Comment
110.0.0.2	TCP 443 open. All rest filtered.	https web server
110.0.0.3	All filtered	
110.0.0.4	All filtered	
110.0.0.5	TCP 80 open. All rest filtered.	http web server.
110.0.0.6	udp 53 open. All rest filtered.	External dns server
110.0.0.7	TCP 25 open. All rest filtered.	Mail relay server.
110.0.0.8	All filtered	
110.0.0.230	All filtered	
110.0.0.231	TCP ports 264 and 18231 and udp ports 500 and 18234 open. All rest filtered.	VPN Enabled firewall, TCP ports 264 and 18231 show that this is a CheckPoint firewall running CheckPoint NG and allowing SceureClinet Access.
110.0.0.232	All filtered	

With this mapping behind us, we can see where the weaknesses of the solution may lie.

I now know the following:

- There is a single CheckPoint Firewall filtering all traffic from the Internet. The firewall is also used for VPN termination, and remote users connect using SecureClient.

- There are two web servers, one being http, the other https, possibly on different servers.

- You can only perform udp, dns lookups from the Internet as TCP port 53 is blocked.

- There is a publicly assessable smtp server for e-mails entering the network.

These are the points to attack.

5.3 Going Beneath the Surface

Our next task is to enumerate each opening to see if it is a viable entry point, and if it is vulnerable to attack. Any possible attack will be discussed in the next section.

5.3.1 The Firewall

After a considerable time searching for vulnerabilities for Checkpoint, and only being able to obtain them for versions prior to CheckPoint NG, it was felt that more use would be gained by looking at each of the other entry points and attempting to launch an attack on them.

The manner in which the firewall has been configured leaves very little open from the outside world, but it does give us an idea of how the connections to the other accessible servers are handled.

Firewall-1 is a stateful inspection firewall that may be configured to allow access across certain ports to internal servers. One of the strong points of Firewall-1 is its ability to perform complex address and port translations, designed to hide the server that is being connected to.

One attack that may be possible, and would take down the firewall, is a denial of service attack designed to flood the firewall with logging traffic and logs, using badly formatted data to attach to open ports on the firewall. As the firewall accepts/drops and logs the traffic, bring more connections on line in the form of a distributed denial of service attack (DDoS) may cause the firewall to become overloaded and stop the site. This form of attack is of limited value, as it is only effective for the period of the attack, and has no real lasting effects.

5.3.2 The Web Servers

Of the two web servers available to outside access, the https site, buy.giac.ie, is rejected. The probability that the https site and the http site are on different servers is high, as it is unusual to use different IP addresses for different services on the same physical server. So in this case, the http site for www.giac.ie will be our main target.

The first operation is to see what this server is running in the way of operating system and web server. Once this information has been established, possible vulnerabilities are investigated.

Testing the web server by logging in on port 80 should give us some data.

Telnet 110.0.0.5 80

GET HEAD HTTP/1.1

Gives:

HTTP/1.1 400 Bad Request
Date: Wed, 05 Nov 2003 15:07:30 GMT
Server: Apache/1.3.12 (Unix)
Connection: close
Content-Type: text/html; charset=iso-8859-1

This tells us that the web server is running Apache 1.3.12 on UNIX, possibly Solaris 8 with which it is shipped as default.

This version of Apache is vulnerable to the CHUNK vulnerability described in CERT Advisry CA-2002-17[5]. This vulnerability may be exploited in two different ways, as a Denial of Service (DoS) attack or as a buffer overrun.

5.3.3 The Mail Server

Obtaining details from the mail server should give us more data about the internals of the network. First we connect to the mail server and see what it has to say.

Firstly, we send an e-mail to a user who is unlikely to exist by connecting to the mail server on port 25 and entering the following:

Telnet 110.0.0.7 25
220 chucky.giac.ie SMTP Ready.
EHLO me@me.me
250-chucky.giac.ie supports the following ESMTP extensions:
250 SIZE 0
HELO me@me.me

250 chucky.giac.ie Hello me@me.me.
MAIL FROM: meme@google.com
250 meme@google.com: Sender OK
RCPT TO: dumboy@giac.ie
250 dumboy@giac.ie: Recipient Ok
DATA
354 chucky.giac.ie: Send data now. Terminate with "."
Test
.
250 chucky.giac.ie: Mail Accepted
QUIT
221 chucky.giac.ie: closing connection. Goodbye!

Well, just doing this has told me that the name of the mail relay is "chucky". Just got to wait for the rest of the data after rejection.

Obviously the mail was rejected and the following was obtained from the headers.

Mailsweeper is being used as a mail-gateway for forwarding mail between the Internet and the Internal mail system. This will be running on a Windows NT or 2000 server.

A vulnerability for Mailsweeper has been uncovered as described by Securityfocus bugtraq id 7044[6]. This vulnerability allows MIME encoded attachments to bypass the Mailsweeper software, potentially opening a hole into the system.

5.3.4 The DNS Server

The final possible point of attack is the DNS server. Given that it serves the Internet for giac.ie, there is a possibility that it is used for internal DNS queries too, and if so, a DoS attack could be used with great effect. A good DoS attack is the OPT DoS attack as described in bugtraq id 6161[7].

First we need to find out what version of BIND is running. To do this, we use nslookup as follows:

nslookup
Default Server: ns1.pop.net
Address: 80.100.65.19
> server 110.0.0.6
Default Server: ns1.giac.ie
Address: 110.0.0.6

> set class=chaos
> set type=txt
> version.bind
Server: ns1.giac.ie
Address: 110.0.0.6

```
VERSION.BIND    text = "9.2.0-REL-NOESW"
>
```

Unfortunately, it seems that this is one of the few servers that has been built using a relatively new binary for the application it is running, and is therefore not vulnerable to this attack.

5.4 The Attacks

To circumnavigate the security enforced by both the boarder gateway and primary firewall two destinations for attacks have been identified. Firstly, an attack on the www.giac.ie web server is considered utilising the weakness identified in section 5.3.2, and secondly, an attack on the e-mail system is considered utilising the weakness identified in section 5.3.3

5.4.1 Web Site DoS Attack

For the DoS attack, a Perl program "apache-DoS.pl"[8] is run against the vulnerable system. This script is run with the host and port details as its only arguments as:

```
./apache-DoS.pl www.giac.ie 80
```

This script has been designed to run as a continuous loop, generating multiple chunked requests. The chunked requests are designed to make the child process that it has attached to die, so that another process is started in its place. The net result of this attack will be the increased use of resources on the web server, slowing down the server's response time. To further increase the effectiveness of this attack, two or more scripts may be run from the same client, providing two or three time the number of processes dying, and thus reducing the availability of the web server.

5.4.2 Web Site Buffer Overflow

To produce a buffer overflow, a more ingenious script must be obtained and utilised. GOBBLES security have written a script called "apache-nosejob.c"[9] which is designed to pass several variables to the web server under attack, and when the buffer overflow takes place to run any commands on a shell created by the overflow. Although only on BSD systems are described in the source code, information on what switches are required to run the attack on any other system is also included.

Once compiled, the script is run as:

```
./apache-nosejob –hwww.giac.ie:80 –b0x??????
                –d?? –z?? –r?? –c"netstat –an"
```

where

-h host[:port]
-b Base address used for brutefore
-d delta between s1 and addr to overwrite
-z number of times to repeat \\0 in the buffer
-r number of times to repeat retadd in the buffer
-c command to run on the shell created from the overflow

With the correct values for these variables a shell was opened and the output of the "netsatt –an" command was displayed. This gave me details of what connections are on the web server, including all connections to internal systems, and we find the following connections from 10.0.0.5 to 10.0.3.10 on TCP port 8993. This must be the link to some data feed.

From this, I can now look deeper into the local server and discover what communication protocols are used for the link to the application server, and what other connections the web server can make. Digging around further I find:

DNS server is on 10.0.0.6
NTP server is on 10.0.0.6
Syslog server is on 10.0.4.8

From this data, I am able to feed the syslog server with a large amount of spurious logs, possibly taking it down, but most likely hiding any commands I run against this system. Also the internal DNS and NTP servers are running on a single host, and by running DNS and NTP queries against this server I can obtain more information about the way GIAC Enterprises have designed their internal network.

Next I try for the /etc/passwd file using the

-c"cat /etc/passwd"

command.

It looks like the /etc/shadow file has not been created, and therefore I am able to download all the encrypted passwords for this server. All I have to do now is to crack the password for root, and I have full access on this system through my buffer overflow. If the root password is too problematic, I am sure that one of the user accounts on the server should be useable.

Once root access has been obtained using this access method, it is only a matter of a few seconds work to completely delete the operating system using the

rm –rf /

command rending the site useless to the general public.

5.4.3 Email MIME Attack

The success of this attack is dependent on the Mailsweeper software being at version 4.3.6 or earlier. The attack utilises the fact that vulnerable versions of Mailsweeper will allow MIME encoded messages through unchecked if there is no MIME version field. The discussion on the subject by Security Focus describes the vulnerability in the best manner as follows:

> "Clearswift MailSweeper does not properly process certain malformed MIME email message attachments. If the attachment does not contain a MIME-Version field, MailSweeper does not recognize the attachment as being an executable type. MailSweeper allows such attachments through, even if it is set to filter executable type file attachments from incoming email messages."

The first part of the attack is to find somebody within GIAC Enterprises who will open an attachment within an email.

Looking through the www.giac.ie web site, I found a page containing contact details for obtaining information from GIAC Enterprises. Amongst the contacts listed are two interesting ones:

Information	info@giac.ie
Sales	sales@giac.ie

These two email addresses will probably be routed to two different groups of non-technical staff within GIAC Enterprises.

Firstly I will send an email to the info@giac.ie address from one of my hotmail accounts, which has an executable attachment containing code to forward me data to another free e-mail account that I have obtained. The executable is designed to become an invisible service running on a MS Windows machine, which gathers username/passwords and any data relating to current customer information. The email that I send has the following text:

> Hi,
>
> I am interested in becoming a customer of GIAC enterprises, but am not able to look at all the data on you Brochure site. When I attempt to get to certain areas, I get an error message as shown in the attached image. Please could you let me know what I am doing wrong, as I am not able to work it out myself?
>
> Regards,
>
> Freddy.

Hopefully, this email will have the employee who reads it, open the attachment, at which point their machine starts to send me back data. Even if this "virus" is discovered, hopefully, I will have had enough data sent to me to

sell to a competitor if they are interested, or possibly to blackmail GIAC Enterprises with.

If the email does not get through, I will expect an error message from their e-mail system telling me that executable attachments are not allowed.

When the email has been sent, I check both mailboxes, and am pleased to see data coming through to my second one. Time to download it, ready to trawl through and find the really useful data that I am after.

In addition to this data gathering exercise, it could be possible, by crafting an executable that opens up an access link into the compromised machine by connecting to a "special" web server that I own, to gain full access into that workstation.

5.5 Conclusions

A silent scan run against GIAC Enterprises public address range has given me a wealth of data that I have been able to use to launch three good attacks against GIAC Enterprises, gaining access into their system using well publicised vulnerabilities.

Two vulnerable system were identified, one the www.giac.ie apache web server, and the external e-mail gateway running Mailsweeper.

The apache web server, although only having a single vulnerability, is actually vulnerable to two types of attack. Firstly a buffer overflow, which gives us plenty of data to digest, and secondly a DoS attack which can be used to take the www.giac.ie web site off air.

The Mailsweeper e-mail gateway has a single vulnerability that gives me access into the internal network by sending a cleverly crafted e-mail. As seen, this executable could be used to gain data from that machine, or could actually provide remote access directly into the heart of their operations.

Between them, these attacks, and the data gathered, could be used to discredit GIAC Enterprises to a greater or lesser degree. What is more important, is that I am able to get right into the heart of their network, leveraging off the security devices that have been implemented, and getting to a position where I can almost be in control of their internal systems.

6 Appendix A IP Address Details

6.1 Internal IP Addresses

The internal IP addresses for GIAC Enterprises shown below fall within the allocated list for private IP addresses listed in RFC 1918.

Name	IP Address	Comment
Users LAN	10.44.0.0/23	Users network
	10.44.0.0 – 255	Non Admin users DHCP range
	10.44.1.0 – 127	Admin users fixed IP addresses
	10.44.1.128 – 250	Printers
Giac-int-rout-01	10.44.1.252	Internal Router-01
Giac-int-rout-02	10.44.1.253	Internal Router-02
Giac-int-rout-hsrp	10.44.1.254	Internal Router HSRP
Admin LAN	10.44.20.0/24	Administration LAN
Giacadmin01	10.44.20.1	UNIX admin server
Giacadmin02	10.44.20.2	UNIX admin server
Giacadmin03	10.44.20.3	Windows admin server
Giacadmin04	10.44.20.4	Windows admin server
Giacsecid01	10.44.20.100	Primary SecurID server
Giacsecid02	10.44.20.110	Secondary SecurID server
Giacfwm01	10.44.20.200	Firewall Management server
Giacidsm01	10.44.20.210	IDS Management server
Giac-int-rout-01	10.44.20.252	Internal Router-01
Giac-int-rout-02	10.44.20.253	Internal Router-02
Giac-int-rout-hsrp	10.44.20.254	Internal Router HSRP
IDS Mgmt LAN	10.44.21.0/24	IDS Management LAN – IP addresses for NIDS not shown.
Giac-int-rout-01	10.44.21.252	Internal Router-01
Giac-int-rout-02	10.44.21.253	Internal Router-02
Giac-int-rout-hsrp	10.44.21.254	Internal Router HSRP
Server LAN	10.44.50.0/24	
Giacbb01	10.44.50.10	BigBrother monitoring server
Giacmail01	10.44.50.120	Internal Mail Server
Giacsqlcl01	10.44.50.130	Internal DB SQL cluster address
Giacmscl01	10.44.50.131	Internal DB MS cluster address
Giaccln01	10.44.50.132	Internal DB Cluster node 1
Giaccln02	10.44.50.133	Internal DB Cluster node 2
Giac-int-rout-01	10.44.50.252	Internal Router-01
Giac-int-rout-02	10.44.50.253	Internal Router-02
Giac-int-rout-hsrp	10.44.50.254	Internal Router HSRP
Link LAN	10.44.60.0/24	FW Router link LAN
Giac-int-rout-01	10.44.60.249	Internal Router-01

Giac-int-rout-02	10.44.60.250	Internal Router-02
Giac-int-rout-hsrp	10.44.60.251	Internal Router HSRP
Giacfwl01	10.44.60.252	Primary firewall module
Giacfwl02	10.44.60.253	Secondary firewall module
Giacgw	10.44.60.254	Firewall cluster address
Access LAN	10.44.248.0/24	
Giacmail02	10.44.248.10	
Giacproxy01	10.44.248.20	
Giacfwl01	10.44.248.252	Primary firewall module
Giacfwl02	10.44.248.253	Secondary firewall module
Giacgw	10.44.248.254	Firewall cluster address
B2B LAN	10.44.253.0/29	
Giacb2b01	10.44.253.1	
Giacfwl01	10.44.253.4	Primary firewall module
Giacfwl02	10.44.253.5	Secondary firewall module
Giacgw	10.44.253.6	Firewall cluster address
WEB LAN	10.44.254.0/25	
Giacweb01	10.44.254.10	
Giacweb02	10.44.254.20	
Giacvip01	10.44.254.100	
Giaclb01	10.44.254.120	
Giaclb02	10.44.254.121	
Giacfwl01	10.44.254.124	Primary firewall module
Giacfwl02	10.44.254.125	Secondary firewall module
Giacgw	10.44.254.126	Firewall cluster address
SQL LAN	10.44.254.128/25	
Giacsqlcl10	10.44.254.129	
Giacmscl10	10.44.254.130	
Giaccln10	10.44.254.131	
Giaccln11	10.44.254.132	
Giacfwl01	10.44.254.252	Primary firewall module
Giacfwl02	10.44.254.253	Secondary firewall module
Giacgw	10.44.254.254	Firewall cluster address

6.2 Public IP Addresses

The IP addresses listed here are directly used by GIAC Enterprises. I have not included the IP addresses belonging to GIAC Enterprises Suppliers or Partners as these addresses are outside of the scope of the design.

Name	IP Address	Comment
Public LAN	80.169.251.0/28	GIAC Enterprises public address range.
Giac-ext-rout-01	80.169.251.1	Boarder Router
	80.169.251.2	
	80.169.251.3	
Unnamed	80.169.251.4	NAT for web servers (Hide NAT)
Www	80.169.251.5	Web site VIP (Static NAT)
Mailgw	80.169.251.6	SMTP Server (Static NAT)
	80.169.251.7	
	80.169.251.8	
	80.169.251.9	
	80.169.251.10	
Giacfwl01	80.169.251.12	Primary firewall module
Giacfwl02	80.169.251.13	Secondary firewall module
Giacgw	80.169.251.14	Firewall cluster address
NW Bcast	80.169.251.15	Broadcast Address
www.secpay.com	213.52.208.67	Secpay for remote payment.

7 Appendix B References

[1] www.nsa.gov/snac/win2k/index.html

[2] www.suse.com/de/security

[3] www.faqs.org/docs/securing/

[4] www.insecure.org/nmap/index.html

[5] http://www.cert.org/advisories/CA-2002-17.html

[6] http://www.securityfocus.com/bid/7044/info/

[7] http://www.securityfocus.com/bid/6161/info/

[8] http://packetstormsecurity.nl/0206-exploits/apache-DoS.pl

[9] http://www.immunitysec.com/GOBBLES/exploits/apache-nosejob.c