Global Information Assurance Certification Paper

DEFENCE IN DEPTH: PREVENTING THE COOKIE FROM CRUMBLING

Being an analysis and description of perimeter defences provided for GIAC Enterprises networks.

PRACTICAL ASSIGNMENT VERSION 2.0

SUBMITTED FOR

GIAC CERTIFIED FIREWALL ANALYST

BY JONATHON BERRY

ON 21 JULY 2003

PART ONE
SECURITY ARCHITECTURE

Definition of the business

GIAC Enterprises (GIAC Ent) is a successful e-business that sells fortune cookie sayings online. The product sold is a small piece paper with a fortune printed on it. Customers may select from a variety of sizes, themes and languages. Whilst selection and ordering is online the delivery takes place in the physical world. GIAC Ent is not yet satisfied with the legal controls surrounding the sales of fortune sayings in electronic form to customers. GIAC Ent receives the sayings from partner companies that upload data files containing the sayings. GIAC Ent recognizes the efficiencies and cost savings gained by conducting business online and seeks to conduct the majority of its business as e-business.

GIAC Ent may be described as an aggregator, printer, distributor and retailer of fortune cookie sayings with an online front-end. Organizationally, GIAC Ent is comprised of:

- Management and HR group. The CEO and managers who run the business as well as address HR matters.
- Operations group. This group conducts quality control on sayings, prepares and ships orders and coordinates translations.
- Technical group. Deploys and maintains all electronic services for GIAC Ent, such as the internal network, web servers, databases and telecommunications
- Security group. Addresses physical and electronic security. Maintains and monitors IT system security services in conjunction with Technical group
- Finance group. Looks after all financial transactions, such as salaries, payments to suppliers and receipt of payments from customers.
- Sales group. The sales force that seeks customers and new markets. This group may also place orders on behalf of customers.

Identifying the Business Relationships

The consideration of appropriate network architecture for GIAC Ent is a reflection of the company's business activity, its customer relationships and staff activities. The company has five business relationships and a workforce that is comprised of static and mobile elements. All of these groups impact directly upon how the network is to be structured. Understanding the relationships and their requirements will lead to an appropriate configuration. Correct identification of services required will allow the network to be designed such that only required services are accessible and that the minimum of privileges are granted.

Nature of the Business Relationships

Described below are the business entities and nature of their relationship with GIAC Ent. It is possible that entities may be a member of one or more groups.

For example an employee, when at home, may be considered a member of the general public in terms of web browsing.

Customers. This group can be divided into two distinct parties; customers with whom GIAC Ent has an established relationship or new customers. These customers are either individuals or companies that purchase fortunes in bulk, online. These entities need a means to select what they want to buy, purchase the goods in a secure way and communicate with GIAC Ent. The established customers have established an account with GIAC Ent which gives them preferential treatment.

Suppliers. Suppliers are contracted by GIAC Ent to provide sayings in a particular theme. The suppliers are creative individuals who invent the sayings and record them in a data file the upload them to GIAC Ent. After a quality control check, the supplier is paid by GIAC Ent. Suppliers gain contracts through an on-line bidding process.

Partners. The business partners that GIAC Ent has are those entities that translate sayings into other languages and on-sell sayings in regional markets. GIAC Ent transfers the data files of sayings in bulk for translation and receipts the translated versions back as a data file. For regional sales, business partners require a means to submit orders online in a secure manner.

Employees. This group is broken into three components.

- Office workers. The individuals who work on the premises of GIAC Ent. These individuals, subject to their functional responsibilities, need access to GIAC Ent networks in order to carry out their duties. This group will contain individuals who have the highest privileges on networks, such as administrators and security engineers.
- Mobile sales force. This group is distributed world wide and from time to time needs the following services; file transfers, email access, place orders and check status. This group will need secure access and authentication.
- Teleworkers. Individuals who do their work off site, generally either at home or from a telecommuting hub. These individuals may belong to any of GIAC Ent organizational groups. This group needs to be able to access the network in a secure manner and will need to be authenticated. This group will need to transfer files and access email.

General Public. This group is essentially everyone else who does not fall into one of the above categories. This group only needs access to information about goods and services available from GIAC Ent. They may then make a decision about entering into one of the relationships described above.

Security Ethos

GIAC Ent is a business organization that recognizes that information system security is vital to its business operations. It considers its reputation and financial well-being have some dependency upon the security of its systems and business processes. Accordingly, GIAC Enterprises has detailed 8 approaches to security:

- All staff are responsible for security.
- At all times and in all cases at least two forms of security are to be provided.
- Defence-in-depth is to be employed in all aspects of security.
- Services and resources are to be compartmentalized and allow only access to those entities that require it.
- The principle of least privilege is to be applied.
- Where possible, devices are to operate in a "deny all except that which is approved" mode.
- Remote management of devices is not preferred.
- Redundancy is to be provided.

Physical security. Network security is to complement physical security and vice-a-versa. The more sensitive network hosts are to be placed within the inner most offices of GIAC Enterprises. To implement this GIAC Ent has a robust physical security architecture. Access to the GIAC Ent buildings is by swipe card. Access to the GIAC Ent offices is by wireless proximity card, supplemented by PIN after hours. Throughout GIAC Ent offices staff are required to wear photo identification. Visitors are escorted and given a visitor badge to wear. Entry into server rooms is limited and requires a swipe card and PIN.

Personnel security. All staff has passed through background checks to ensure they meet certain character standards. Staff sign an annual contract that details, *inter alia*, behaviour that is acceptable and unacceptable on the network. For example, staff are not to install unauthorized software on their computers, whether by download or from physical media. Staff is also required to attend an annual computer security course that keeps them aware of secure computer use, such as reporting (and not opening) unsolicited email with attachments.

Connections Needs and Provisioning Matrix

In order to meet the needs of the business relationships a communications method had to be selected. A matrix was constructed for this purpose, which described a generic communication method that would satisfy the relationship and identified those communications that may contain sensitive or privileged information. The matrix also describes the level of trust inherent in the relationship. The matrix is shown below.

Entity	Level of trust	Connections[1]	Sensitive[2] data?	Solution and/or protocol
New Customers	Low	Email Web browsing Online sales	N N Y	smtp http https
General public	None	Email Browsing	N N	smtp http
Implementation. No further implementation required by GIAC. These are normal services to be offered, the client will of course need the appropriate applications; browser, email.				
Established Customers	Medium	Email Browsing Online sales	Y N Y	VPN, encrypted smtp http VPN, https
Suppliers	High	Email Browsing	Y N	VPN, encrypted smtp http
Partners	Medium	Email File transfer Browsing	N Y N	smtp VPN, file encryption http
Mobile sales	High	Email File transfer Browse	Y Y N	VPN, encrypted smtp VPN, file encryption http
Teleworkers	High	File transfer Email Browse	Y Y N	VPN, file encryption VPN, encrypted smtp http
Implementation. The entity must have a fixed IP address and can then be included in to a VPN solution. If needs be a PKI system for file/email encryption can be used. All other services need no further clarification. Where mobile sales force is not able to use a fixed IP, file encryption is to be used for sensitive material.				
Office workers	High	Email Web browsing File transfer	Y N Y	VPN, encrypted smtp http https, file encryption
Implementation. These are the terminus of previous mentioned implementations and so will have available all means used by other entities.				

Risk Analysis

Having determined relationships and their communications requirements, a thorough risk analysis was carried out by GIAC Ent and reviewed by a third party. The Risk Analysis highlighted the desirability of separating services to well known entities from the less well-known or untrusted entities. The Risk Analysis

[1] These are connections initiated by the entity as part of it's business with GIAC Ent, or in the case of employees connections initiated in order to carry out GIAC Ent business.

[2] Sensitive data refers to that data that GIAC Ent requires to be kept confidential. If there is an element of sensitive data in any exchange then it is marked "Yes", so that provision may be made. However, there will also be data that may not be considered sensitive.

also emphasized a need for defence-in-depth to mitigate against single points of failure that could lead to the compromise of the network at large.

Upon identifying the nature of the relationship and it's associated risk, a matrix can be created detailing services required. Consideration is also given to the trust GIAC Ent has in the entity and whether or not the data exchanged is sensitive. These aspects will influence the technical implementation of the services provided. Connections described on the table overleaf are in terms of the GIAC Ent network.

How communications are to be provided: Product Suites
GIAC Ent seeks to standardize platforms and applications to ease maintenance concerns. Standardization of platforms will also allow for a more rigorous and effective hardening processes. Hardening will take place with the intent of leaving minimum services required for the device to operate effectively in its role. The routers, firewalls and VPN will be explained in greater detail later on.

Routers. CISCO 1760. See Part 2 for configuration details.

Outer Firewall and VPN. Check Point Firewall/VPN 1, NG to Feature Pack 1. See Part 2 for configuration details.

Switches. CISCO Catalyst 2950. Allow for intelligent routing and security filtering.

Inner firewalls. CISCO PIX 535. See Part 2 for configuration details.

IDS. ISS Real Secure. This product will be used as the Intrusion Detection suite. Intrusion detection will be run as a network service. IDS will be looking for breaches of the firewall rule set and for signatures of known attacks, where applicable to the network. This particular product interfaces well with the Checkpoint firewall using the OPSEC program.

AntiVirus. All computers (servers and clients) will have an anti virus suite running on them. The only exception will be the firewall. Antivirus suites will be acquired in accordance with the Operating System they are to be run on.

Content Checker. The content checker suite will be SurfControl. This will be checking files (arriving through FTP or as attachments) as well as scanning for (and blocking) malicious or inappropriate email.

Web server and http server. Debian GNU Linux 3.0, Apache 2.0.47

http outbound proxy. All Debian GNU Linux 3.0, Squid 2.4.6-2.
Email and smtp proxy. Debian GNU Linux 3.0, Exim 3.35-1.

FTP Server. Debian GNU Linux 3.0, FTPD 0.17-13.

DNS Server. Debian GNU Linux 3.0, BIND ver 9.2.1.2.

Concept for the Architecture

As detailed in the "Security Ethos", GIAC Ent prefers to adopt a "denial all except that which is approved" approach to services. However, there is already a degree of trust in established relationships. Therefore, services will be split into two domains; Untrusted and Trusted. The two domains will be on a separate private IP ranges and accessed through different Internet Service Providers, ISPs. The Service Level Agreements (SLAs) entered into will oblige the ISPs to prevent the routing of any RFC 1918 addresses across their network. The ISP are to have a plan in place with upstream providers to defend against various forms of Denial of Service (DoS) attacks, particularly packet flooding. The GIAC Internal LAN will also be on a different subnet and use RFC 1918 addressing.

The Untrusted domain will be readily accessible from the Internet and offer services required by parties to communicate with GIAC Ent and conduct their business. This is effectively the Demilitarized Zone, DMZ. The Trusted domain is also accessible from the Internet but is not publicized and will require additional processes to establish connectivity. The term "Trusted" does not imply that parties connecting through this domain will have unfettered access to services. The Trusted domain will not have a URL and hence no need for DNS. Connections will be directly to an IP address. This domain is for parties known to GIAC and will require authentication in order to be accessed.

Connections from the Trusted and Untrusted zones into the Internal LAN, in general, will not be permitted. However, clients on the Internal LAN may establish communications with hosts therein to update data, improve services etc. Furthermore, the Internal LAN will use the Untrusted DMZ for proxy services. Direct connection between the two DMZ will not be permitted.

GIAC Ent wishes to standardize it's technologies to facilitate better management. It also prefers its staff to become masters in one technology rather than jacks of all. However, in the interests of defence-in-depth, different technologies will be employed to reduce the probability of a vulnerabilities being exploitable throughout the network. Furthermore, GIAC Ent intention to purchase "best-of-breed" technologies may increase the variety of Operating Systems and applications. All hosts and clients are to be hardened and unnecessary services removed. Furthermore, computers are to have all unnecessary devices removed, such as floppy disk drives. User permissions are to be kept as low as practicable for effective working.

The Network Architecture

The most sensitive part of the GIAC Ent network is its Internal LAN and the servers where critical business is stored. This is where the backend processing

is conducted, where orders are fulfilled, the intellectual property is kept and financial transactions authorized. In general, network architecture will consist of three layers to defend this LAN. Sandwiched between each security layer will be services, as shown below. This "defence-in-depth" approach will employ variety at each layer so an exploit may not be repeated if one layer fails. Services required for the conduct of business will be proxied and pushed out as far as possible from the LAN and defended as much as practicable. Defence begins at the outermost perimeter with Internet Protocol (IP) address and port filtering, where practicable. The second layer will conduct more rigourous defence using firewalls and IDS sensors. Firewalls will provide NAT for private IP addresses. Sitting behind this are the services and proxy services which is the publicly accessible part of GIAC Ent, the DMZ. Proxy services are being used to prevent direct connectivity between the Internet and the Internal LAN. There will also be anti-virus and content checking performed in this layer/DMZ. Immediately behind this is another firewall and IDS before connection to the GIAC Ent LAN. In summary, the architecture will follow:

Layer One: Routing; IP address and port filtering
Layer Two: Firewall, IDS, VPN terminations. Address translation.
Layer Three: Switched network with services and proxy services. Switches will be configured to deny unnecessary connections. This layer includes Anti-virus applications and content filters. Uses private addressing.
Layer Four: Firewall with address translation and IDS.
Layer Five: The GIAC Ent LAN. This is the place where the Trusted and Untrusted networks converge. A switched network with anti-virus applications and content filters. Desktop clients may use personal firewalls.

This structure has been selected as it can be configured to allow connections into needed services but away from the sensitive networks. It also allows for GIAC Ent staff to maintain services from within the network whilst denying connectivity from the Internet. Applying this structure to our Trusted and Untrusted networks is described below.

Trusted

Layer One. This router is a CISCO 1760 and has the firewall feature set installed. The router has been configured to accept connections from known IP addresses only. Once an entity has been verified by GIAC Ent their IP address will be entered into the router ACL. Traffic passing through this router is exclusively VPN traffic. This allows for the dropping of all other traffic attempting to pass through the router. However, for management purposes the router will respond to ICMP Type 8 (ping) traffic. The router is on-site and can only be reconfigured using a direct console connection. The router will be configured to drop any IP packets conforming to RFC 1918.

Layer Two. The security provided here starts with the firewall. This is a Checkpoint Next Generation Firewall/VPN 1 firewall. This firewall is running on a hardened MS Windows 2000 Professional OS. The firewall has a single interface (eth01) to the router. The VPN connections will terminate at the firewall. This will allow for effective IDS deployment behind the firewall. All other inbound connections are dropped. The firewall has one internal interface connecting directly to a switch. NAT will be performed on the firewall translating through to a RFC 1918 subnet. IDS an IDS sensor is placed directly behind the firewall and monitors all traffic passing through the firewall.

Layer Three. Services are provided here. The services are designed to meet specific business needs and adopt a minimalist approach. The hosts are connected to the firewall via a switch.
http server: There is an http server which is similar the web server but provides a less glamorous interface. The http server provides a minimal interface for partners and customers to place orders and browse product ranges.
FTP. The FTP server is not a true proxy FTP server, but more a location where files may be accessed by clients. GIAC staff will only place files available for sale, or to be retrieved on this server. All other files are kept on the Internal LAN FTP server. Once connected clients may up/download files in accordance with privileges granted to them.
LDAP server. Provides authentication services for the VPN.

Layer Four. This is a CISCO PIX firewall. The firewall has been hardened IAW. The firewall has two interfaces; eth0 to the switch in the Trusted DMZ and eth1 to switch in the Internal LAN. The firewall prevents connections from the Trusted DMZ and allows certain connections out from the Internal LAN. The firewall also performs NAT. An IDS sensor is placed immediately behind the firewall that monitors all traffic passing through the firewall.

Layer Five[3]*.* The internal network is a switched network using structured cabling. All clients and servers will be hardened in accordance with their purpose. The network will be organized using Windows 2000 Active Directory. All devices will be running an AntiVirus client. For critical servers an integrity checker will be used.

Untrusted

Layer 1. This router is a CISCO 1760 and has the firewall feature set installed. The router has been configured to drop connections from RFC 1918 IP addresses. However, for management purposes the router will respond to ICMP Type 8 (ping) traffic. The router is on site and may only be reconfigured using a direct console connection.

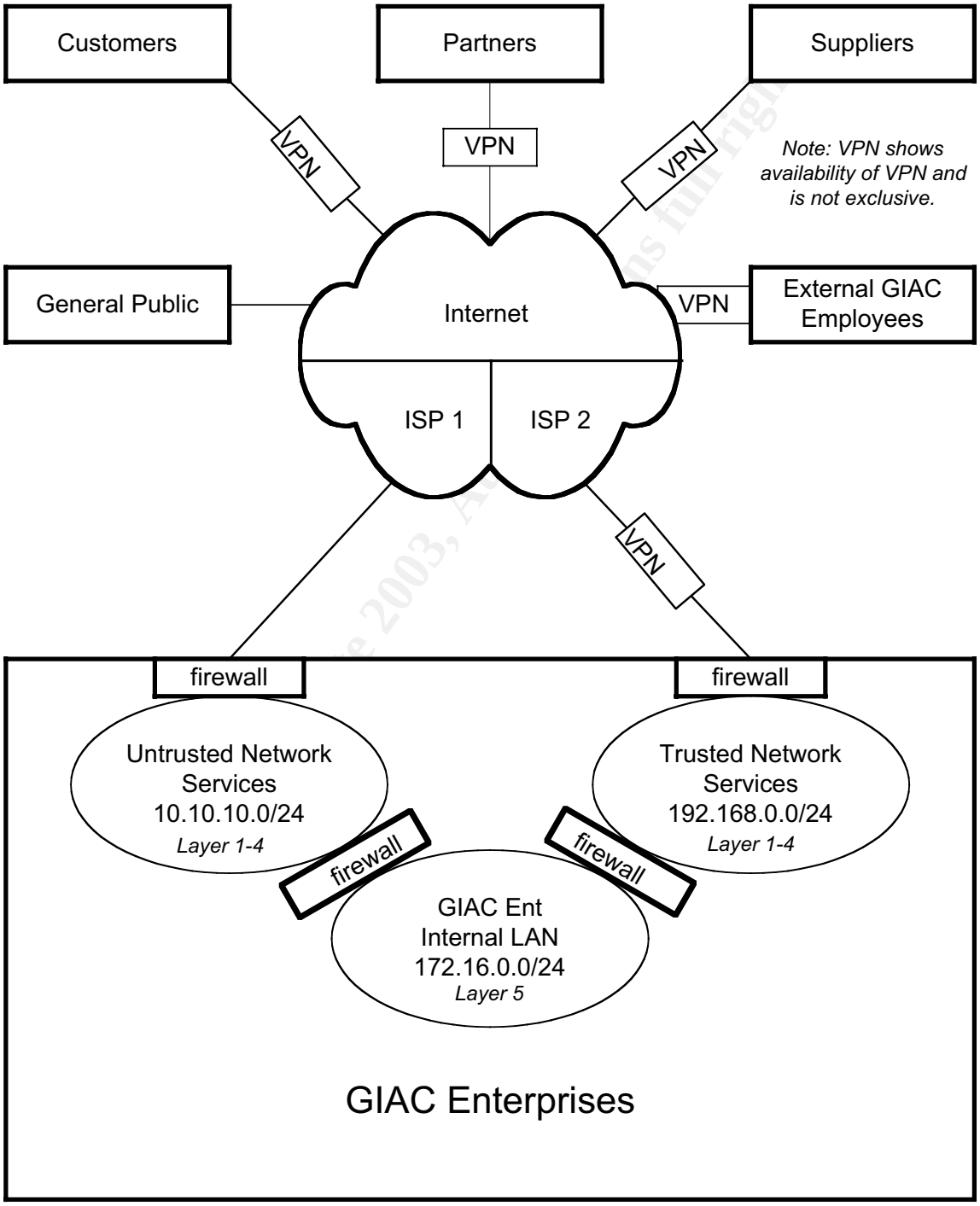
[3] The Internal LAN will only be described once. Layer five for the Untrusted DMZ is also the Internal LAN.

Layer Two. The BPS provided here start with the firewall. This is a Checkpoint Next Generation Firewall/VPN 1 firewall. This firewall is running on a hardened MS Windows 2000 Professional OS. The firewall has a single interface (eth0) to the router and one internal interface connecting directly to a switch (eth1). This will allow for effective IDS deployment behind the firewall. The firewall will accept connections for the services offered in the DMZ and all other inbound connections are dropped. NAT will be performed on the firewall translating through to a RFC 1918 subnet (DMZ). An IDS sensor is placed directly behind the firewall and monitors all traffic passing through the firewall.

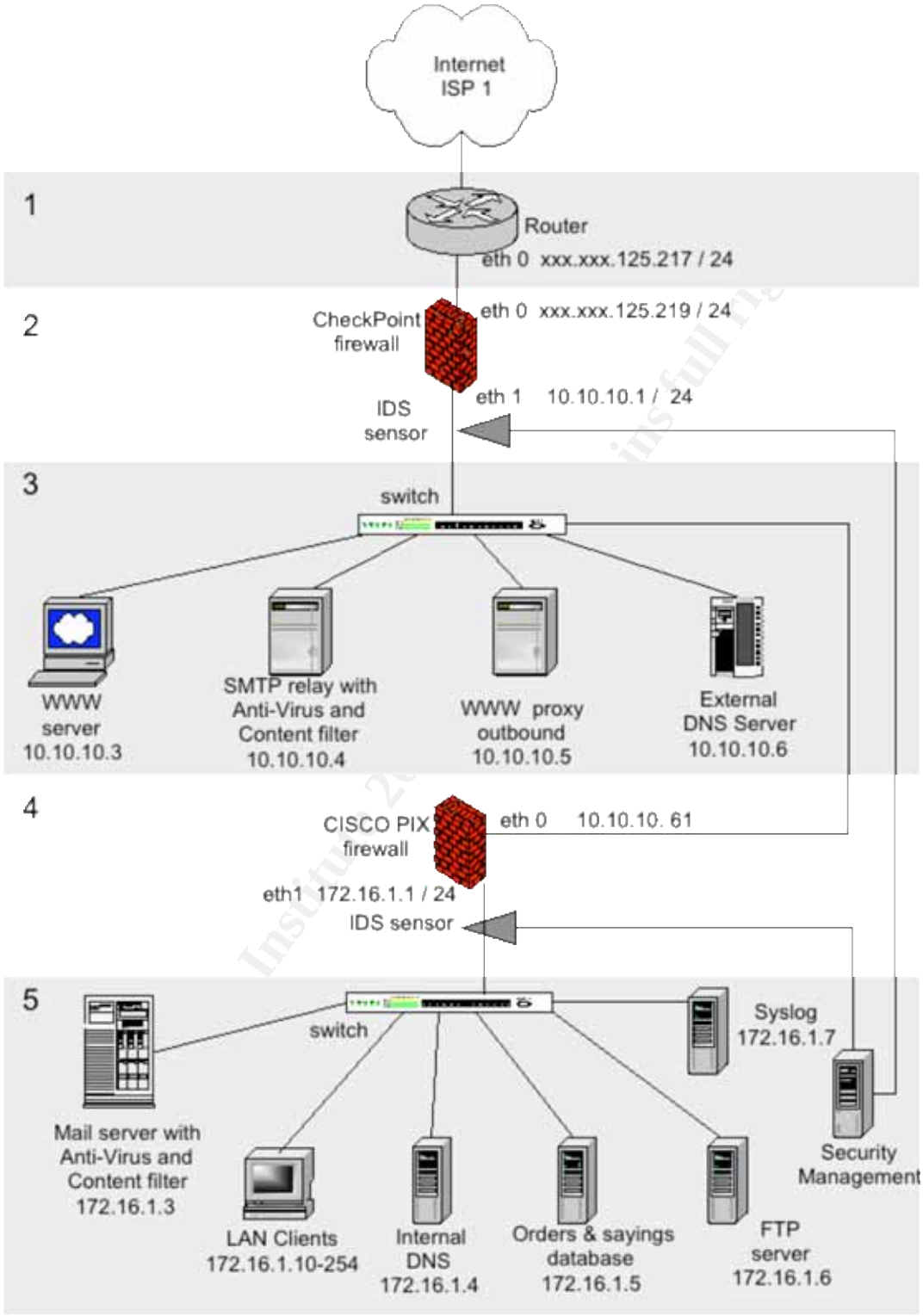
Layer Three. This is the DMZ and here public services and proxy for internal clients are provided. The servers are connected to the firewall via a switch. The switch will not accept connections from one server to another. Connections may not be initiated from the DMZ into the Internal LAN. The services are provided on separate servers so failure or compromise of a service/server does not affect others. Antivirus and content checking will be carried out on certain servers.
Web server: Hosts the GIAC.com address.
SMTP proxy. Handles inward outward and inward smtp traffic.
WWW proxy outbound. Provides http and https proxy for Internal LAN clients.
External DNS. Provides name resolution for the GIAC.com site. Also acts as proxy for the Internal DNS server.

Layer Four. This is a CISCO PIX firewall. The firewall has been hardened IAW. The firewall has two interfaces; eth0 to the switch in the Untrusted DMZ and eth1 to switch in the Internal LAN. The firewall prevents connections from the Untrusted DMZ and allows connections out from the Internal LAN for Web services and maintenance of services in the DMZ. This firewall also performs NAT. An IDS sensor is placed immediately behind the firewall that monitors all traffic passing through the firewall.

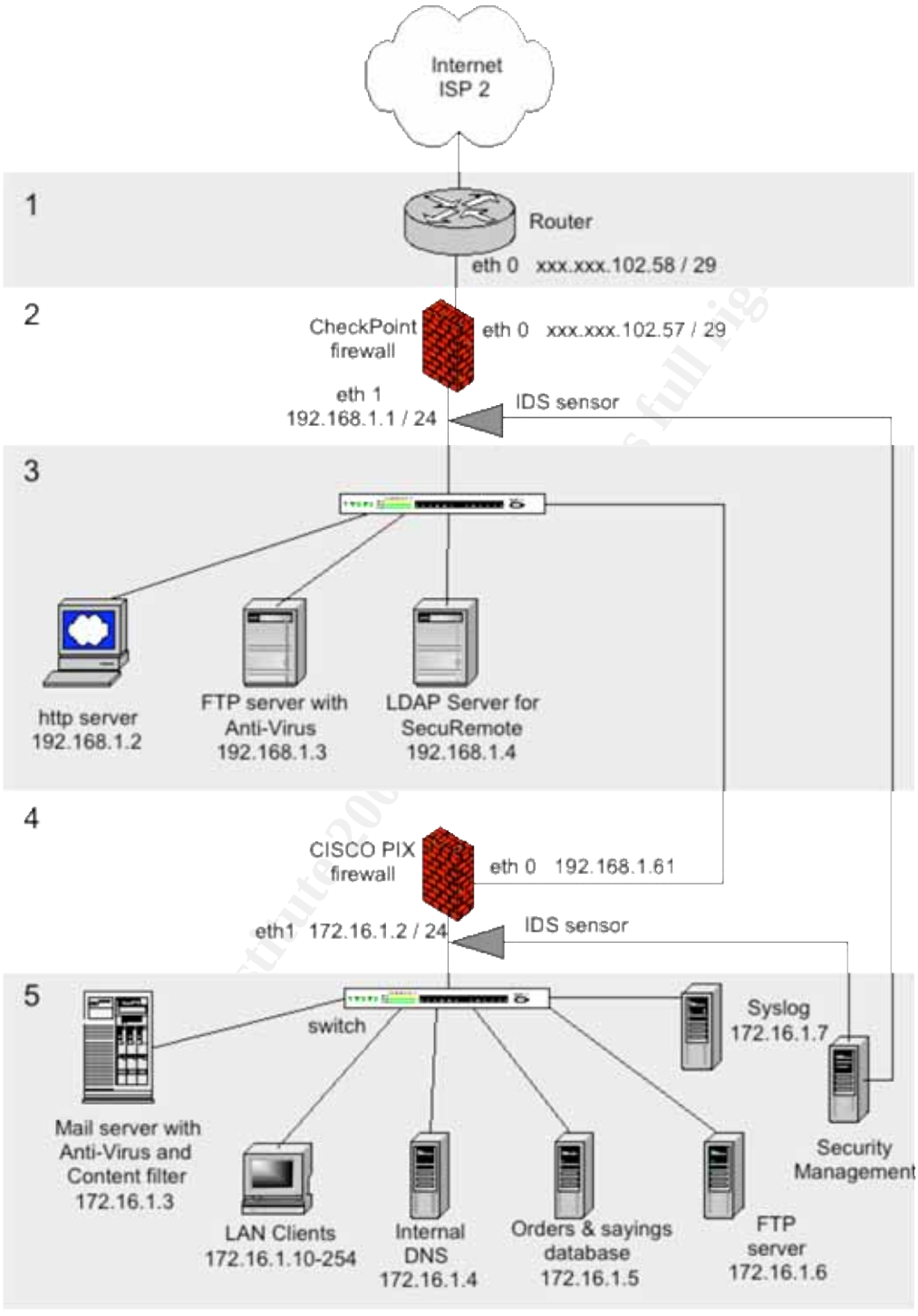
GIAC Enterprises
Conceptual Network Architecture Model



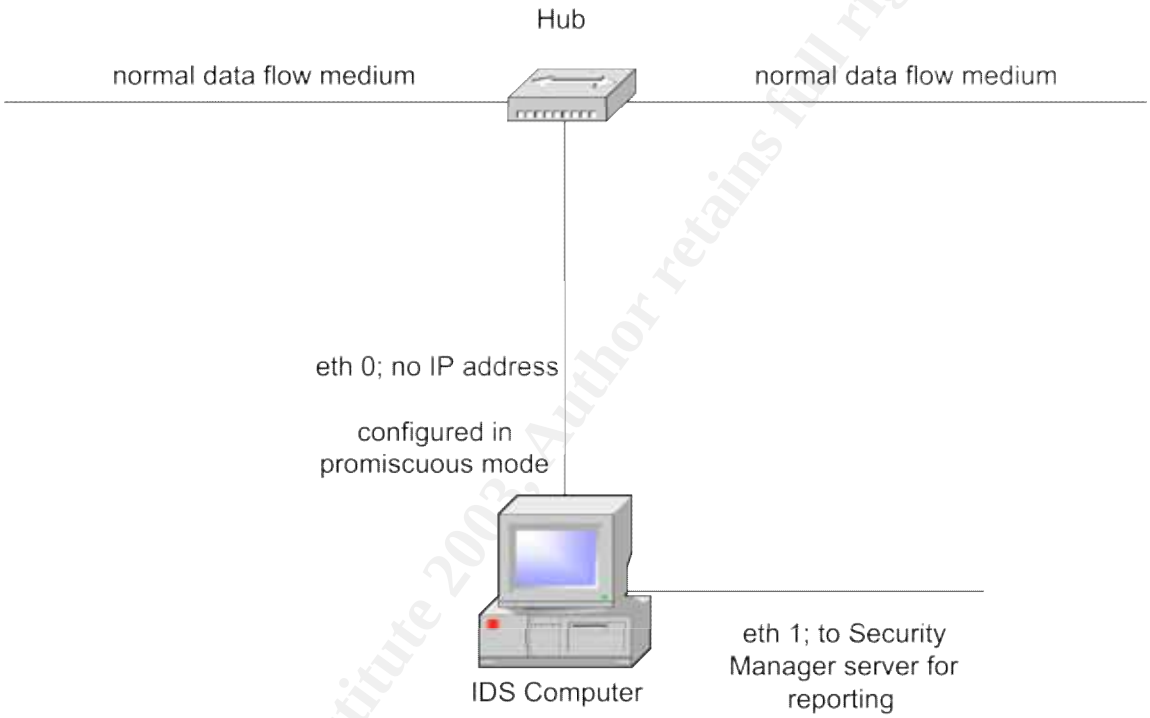
Untrusted (Public) Network Architecture



Trusted (Private) Network Architecture



IDS Sensor Design



PART TWO
SECURITY POLICY AND TUTORIAL

Generic Policies for Untrusted Network

The table below shows the IP allocation for the Untrusted network.

Legal Address	*Role*	**DMZ address (NAT)**
xxx.xxx.125.216	Network address	
xxx.xxx.125.217	router	
xxx.xxx.125.218	router	
xxx.xxx.125.219	firewall	10.10.10.1
xxx.xxx.125.220	Web server	10.10.10.3
xxx.xxx.125.221	Email server	10.10.10.4
xxx.xxx.125.222	DNS server	10.10.10.6
xxx.xxx.125.223	broadcast	

Router. This router will be configured to allow connections through to the firewall conforming to those services offered in the DMZ.

Firewall. The rule set is to achieve two aims;

- facilitate desired connections through specific use of protocols and judicious positioning of rules,
- drop all other connections

Specific Policies and Configurations for the Untrusted Network

Untrusted Network Router

This router is a Cisco 1760 router with IOS 12. Other than usual routing tasks we also want this router to filter out unwanted traffic and prevent information leakage. These purposes will add "defence-in-depth" to our network. The router will be configured to accept any form of remote management; all configurations must be done via the console. This layers physical defences around the router and minimizes the chance of unauthorized connections and modifications to the ACLs.

The ACL will be constructed to conduct blocking of traffic early in the processing of the ACL (i.e. at the top) for the types of traffic for which we expect to see the greatest quantity or pose the greatest danger. Thereafter the rules can be more granular.

Generic Preamble

Establish generic settings for the router, including disabling unwanted / un-needed services.

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname UNTRUGIAC
enable secret 5 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
enable password yyyyyyyy
ip subnet-zero
no ip source-route
no ip bootp server
call rsvp-sync
```

Define the nature and IP address of the outer interface.

```
interface ethernet1/0
description Internet interface
ip address xxx.xxx.125.218 255.255.255.248
ip access-group 101 in
no ip unreachables
no ip mroute-cache
full-duplex
no cdp enable
```

Define the nature and IP address of the inner interface.

```
interface ethernet0/0
ip address xxx.xxx.125.217 255.255.255.248
ip access-group 102 in
no ip unreachables
no ip mroute-cache
full-duplex
no cdp enable
```

Allows ACL's to be classless and defines the upstream IP at the ISP.

```
ip classless
ip route 0.0.0.0 0.0.0.0 xxx.xxx.125.214
```

Prevent unwanted/undesirable connections to the router. This router is to be managed by direct console connection.

```
no ip http server
no telnet
no tftp
```

Access List 101. This ACL applies to traffic coming from the Internet and presents the greatest threat at this position of our network. The rules here will be more stringent, whilst maintaining connectivity. Drop all RFC 1918 (private) IP addresses and the IP address of our network. Denies what is probably/definitely IP spoofing for inward traffic.

```
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 deny ip xxx.xxx.125.217 0.0.0.255 any
```

For engineering and "good netizenship" we will allow certain types of icmp traffic.

```
access-list 101 permit icmp any any echo-reply
access-list 101 permit icmp any any time-exceeded
access-list 101 permit icmp any any host-unreachable
access-list 101 permit icmp any any port-unreachable
access-list 101 deny icmp any any
```

Deny all NETBIOS traffic, as these services are not available or wanted.

```
access-list 101 deny tcp any any range 135 139
access-list 101 deny udp any any range 135 139
access-list 101 deny tcp any any eq 445
access-list 101 deny udp any any eq 445
```

Deny the loopback and broadcast address of a subnet.

```
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 deny ip 0.0.0.255 0.255.255.255 any
```

Permit all other traffic.

```
access-list 101 permit ip any any
```

Access List 102. This ACL applies to traffic that has left the outside face of the firewall and is traveling to the Internet. Our greatest concern here is to ensure delivery of service and preventing information leakage.

Accept only that traffic which has come from the firewall outside IP address.

```
access-list 102 permit xxx.xxx.125.217 0.0.0.255
```

Deny all other traffic

```
access-list 102 deny ip any any
```

UNTRUSTED FIREWALL RULESET

Note that this firewall is the firewall between the Internet and the GIAC Untrusted zone (DMZ). This firewall does not directly affect the communications of clients on the Internal LAN to services in the GIAC Untrusted zone because the switch handles these. This firewall will affect the subsequent communications from the proxy services.

This rule set has the functions of allowing connections from the Internet to the Web site, proxy email server and DNS. It is also to let out DNS, email, web page requests (http proxy) and anti-virus updates. Subsequently rules should be configured to facilitate these business purposes. This will be implemented by giving DNS traffic a priority. Secondly, inbound traffic to the web server and then email services. The rule set should also defend the network and prevent information leakage and direct connections into the Internal LAN. These rules can be placed further down in the rule set.

The object name of this firewall is “trans”.

Rule 1

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1	* Any	DNS_ServerExternal	UDP domain-udp	accept	None	Gateways	* Any

This rule is placed first for business reasons. It facilitates any external client requests for DNS resolution of the GIAC domain. It is a prelude to most inbound connections and it is desirable to have it concluded early in the rule set. Http, https and smtp will use this service, so this rule should appear before rules handling those services. This traffic is not being logged as it would generate too much of an analysis burden.

Rule 2

2	DNS_ServerInternal	* Any	TCP domain-tcp UDP domain-udp	accept	None	Gateways	* Any

This rule is created to allow the GIAC DNS server to access DNS servers on the Internet for the purpose of creating name resolution for internal clients. As a prelude to other services, it is kept near the top. This traffic is not being logged as it would generate too much of an analysis burden.

Rule 3

3	* Any	WebServerExternal	TCP http TCP https	accept	None	Gateways	* Any

Provides access for any entity (on the Internet) to the GIAC web server. It is positioned higher in the order as this rule will relate to a significant amount of traffic that the firewall will handle and it is prudent to hand this off early. This traffic is not being logged as it would generate too much of an analysis burden.

Rule 4

This rule allows for the inward delivery of smtp traffic to the smtp relay server inside the DMZ. This traffic is being logged because GIAC Ent wants to keep track of email behaviour, particularly the additional rules created that drop certain attachments.

Rule 5

This rule allows for the outward delivery of email to the upstream ISP. It also allows the AV application to retrieve updates to its signature database. This traffic is logged to monitor activity.

Rule 6

This rule lets the http proxy used by internal clients access the Internet to retrieve requested data. This traffic is low priority as far as the business is concerned, so it is positioned further down the rule set. This is not logged, as it would generate a large quantity of data.

Rule 7

This rule has been created to facilitate network engineering. It allows hosts and the depth firewall within the Untrusted DMZ to “ping” the firewall so that connectivity can be verified. This traffic is being logged so that unauthorized use can be identified. After a period of network stability this rule could be disabled and then turned on as required.

Rule 8

This rule has been created to alert the Network Administrator(s) that a suspicious and undesirable connection is being sought. The rule prevents any entity from

establishing a direct connection, from the Internet, into the Internal LAN and the firewall that protects it. All the services that GIAC Enterprises wishes to make available are in the DMZ, so there is no need for connections from the Internet to these areas. Through address translation the IP address of the Internal LAN should not be known, so an attempt to make a direct connection raises concerns about that network and we want to separate that event from Rule 10 noise. This rule is positioned further down the rule set; as it is unlikely there will be a match.

Rule 9

This rule denies (rejects) outward connections from the Untrusted DMZ that has not already been approved by earlier rules and so has to be positioned after authorized connections. It also prevents connections from the depth firewall and Internal LAN directly out to the Internet. The rule uses reject as opposed to drop, so that hosts/clients do not persist in their attempts and have more meaningful log entries. The rule also helps in the identification of hosts that may have been compromised (by Trojan for example) and are attempting outward connections.

Rule 10

Our final “catch all” rule that drops all connection requests except those that are accepted by earlier rules. Acts as an insurance policy to prevent “unforeseen” and probably undesirable connections. Logged so such events may be investigated.

Tutorial for establishing the rule set on the Untrusted Network firewall.

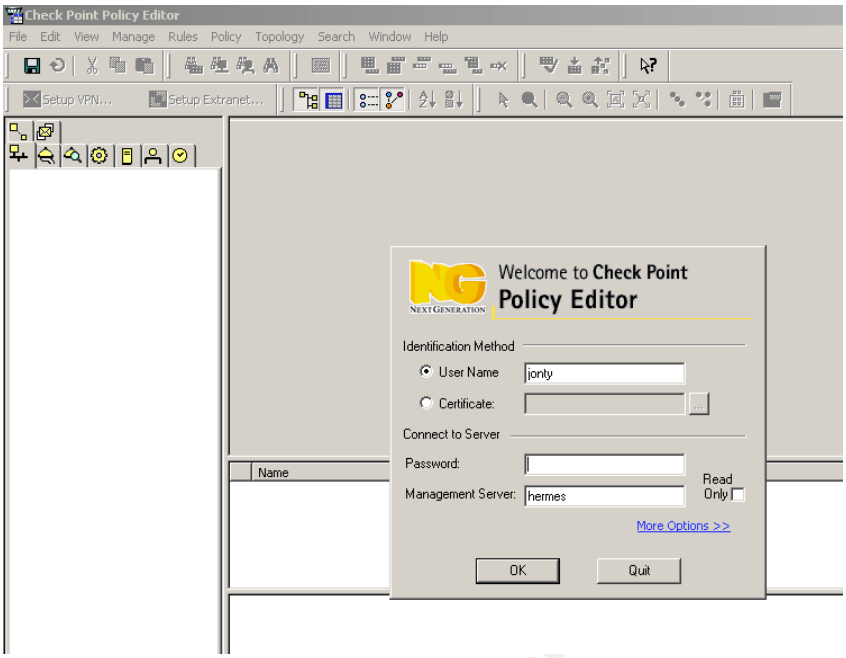
With your network topology in hand and defined services you are armed and ready to build the firewall rule set. However, there are some steps that should have been completed prior to this point.

Obviously, the firewall should have been procured / built. The box should have the correct number of network interface cards (NIC) and/or IP addresses to perform the Address translation and service isolation we intend to perform. The box in this tutorial has two interfaces. Furthermore the box should have been configured to prevent unauthorized use. Consideration should be given to a Basic Input Output System (BIOS) and boot password. Ensure, however, that these will not interfere with operation should the system need to be rebooted when unattended. Furthermore, consideration should be given to removing devices that allow unauthorized connectivity, such as floppy drives, USB ports etc. The BIOS should also be configured such that the box boots from the hard drive first, not other media. Once hardware/BIOS issues have been dealt with we can begin to install software. In this case we are dealing with a Check Point NG-1 FP1 installed on a hardened MS Win 2000 Professional box. This computer should ideally be disconnected from any other device, to prevent infection, when installing the firewall software. However, this will prevent using some of the acquire/search for functionality in the firewall.

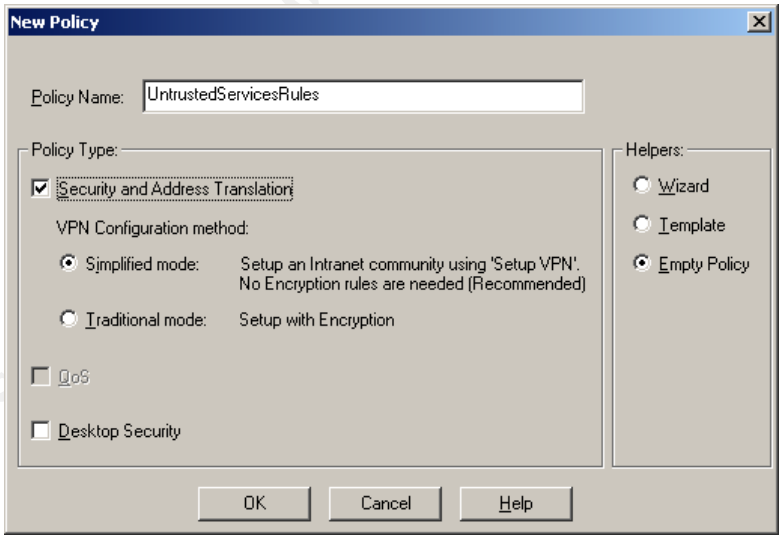
This tutorial will assume you have carried out all the preliminary activities (hardening and installation) to get the box in a state where the firewall application can be used and a rule set can be entered.

Beware; Check Point licensing can be tricky. Ensure that you have the license entered correctly and use the Validation Code to verify that you have entered the correct details. An easier path is to download the license file and dump it to the hard drive *before* installing the firewall. When prompted point the installation at the file.

All of the policy work is done in the "Policy Editor". This is started from *Start → Programs → CheckPoint Management Clients → Policy Editor NG*. Then you will be presented with the screen as below. Enter your details, as per the installation.

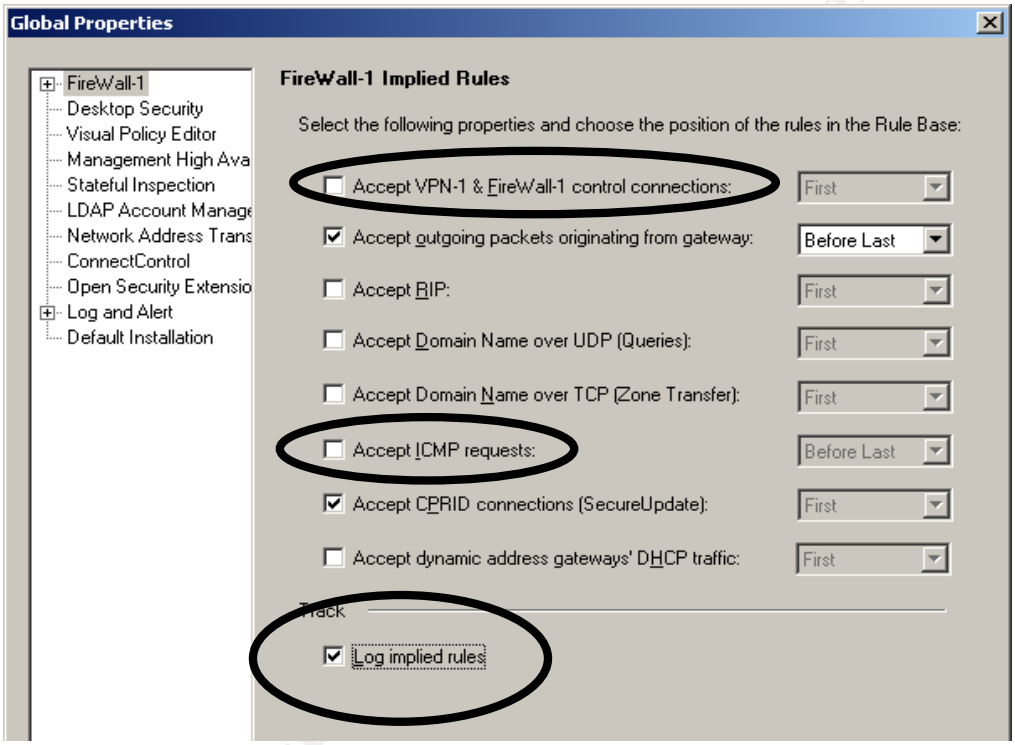


Now you have successfully logged on there are some things to be done to set the stage. It is prudent to give the policy you are about to install a name. This facilitates management and can help you keep track of what you are looking at if you manage multiple firewalls. This is done by *File → New* and completing the details in the window shown below. The options selected will depend upon what you are doing but this tutorial uses the settings shown below.

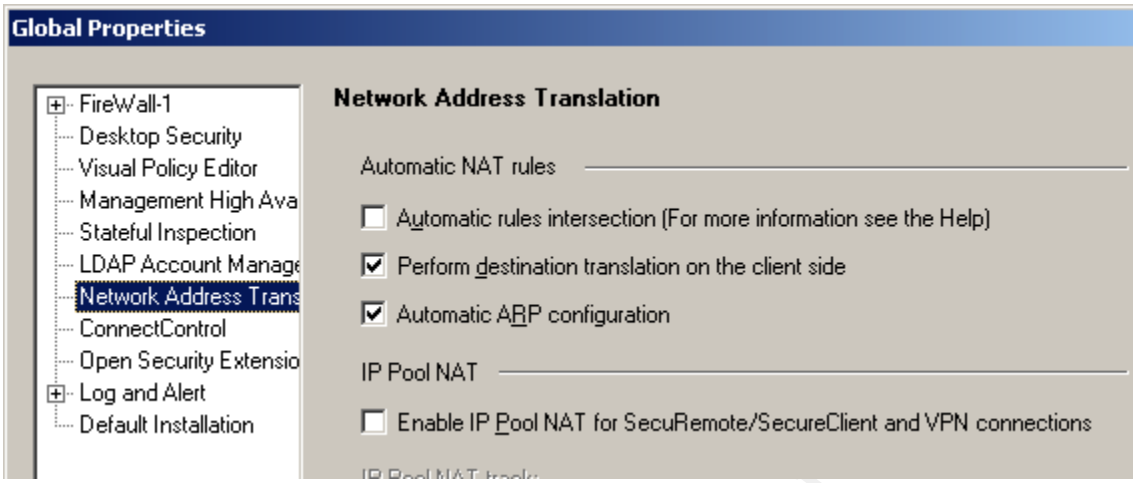


At this point it is useful to configure the "Global Properties". There are various generic configurations that can be set here, but of most use to us at this point is the Implied Rules and the Network Address Translation (NAT) settings. The Global Properties are accessed from the *Policy → Global Properties* drop down menu.

Implied Rules. These should be configured in accordance with your policies. I prefer to turn as much off as possible so that I may configure rules myself in the Policy Editor. This gives you better control over firewall behaviour and makes log analysis easier as activity can be matched to a specific rule. This is especially important for the ICMP requests and Firewall Control Connections. Accepting Control Connections is only useful for certain services, so make sure this is not required before disabling it. The logging of Implied Rules is useful, so that you may see exactly what these rules are doing.



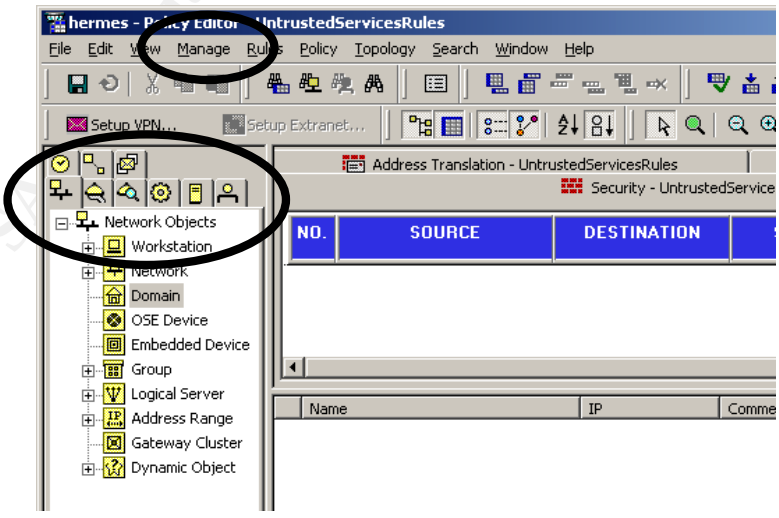
If you are performing NAT at the firewall then it is important to configure it correctly here. This will save you much heart ache later on when you can't work out why it is not working! The global NAT rules are accessed via the tab on the left. Check Point FW-1 NG has introduced some new features that take some of the tricky aspects of routing and handles them automatically. Unless you are comfortable with these aspects it is prudent to use the automatic settings.



You are now presented with the almost "blank sheet" upon which we will write our policy. There are three major steps to get the firewall into an operational state. They are; defining objects[4], defining services and then adding rules.

Define Objects

Check Point refers to devices on the network (or interacting with it) as "Network Objects". There are default objects but it pay's to enter your own so that you may name and configure them in a more tailored or specific manner. I prefer to add network "service" objects first, as individual items, and then group them into a "Group". The first object to be created is the firewall itself, which allows a tidier set-up for the Network Address Translation (NAT) later on. Defining objects may be done in two ways; using the *Manage → Network Objects . . .* or use the tabs to the left by right mouse clicking on the *Network Objects* types; *Workstation, Network, Domain* etc.

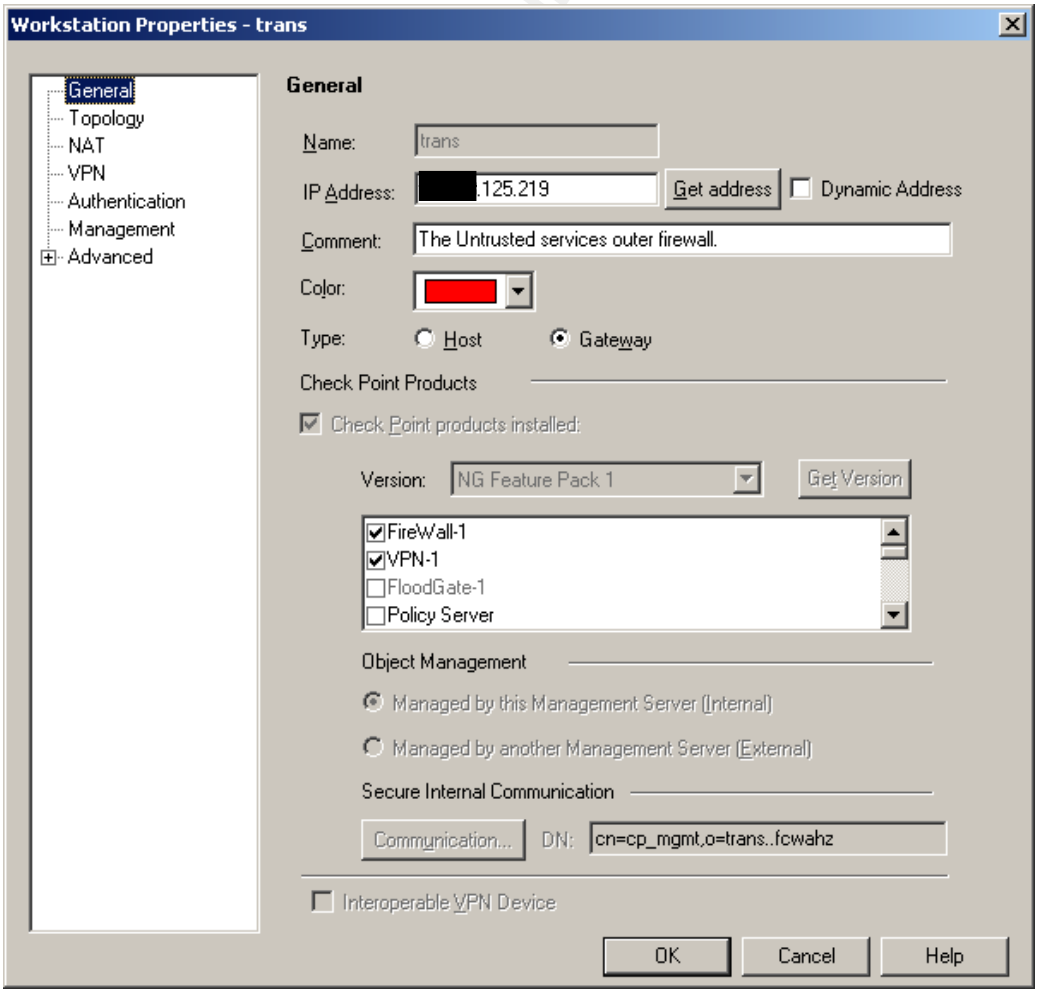


[4] You may do services or objects first depending on taste. However, I prefer to do objects first because it helps me clarify the "players" in the network that will use services.

We will use the tabs to the left as they provide a better schematic view of the network. For the purposes of this tutorial I will demonstrate one of each object being created. The process is generally the same for all; you just need to alter the specifics.

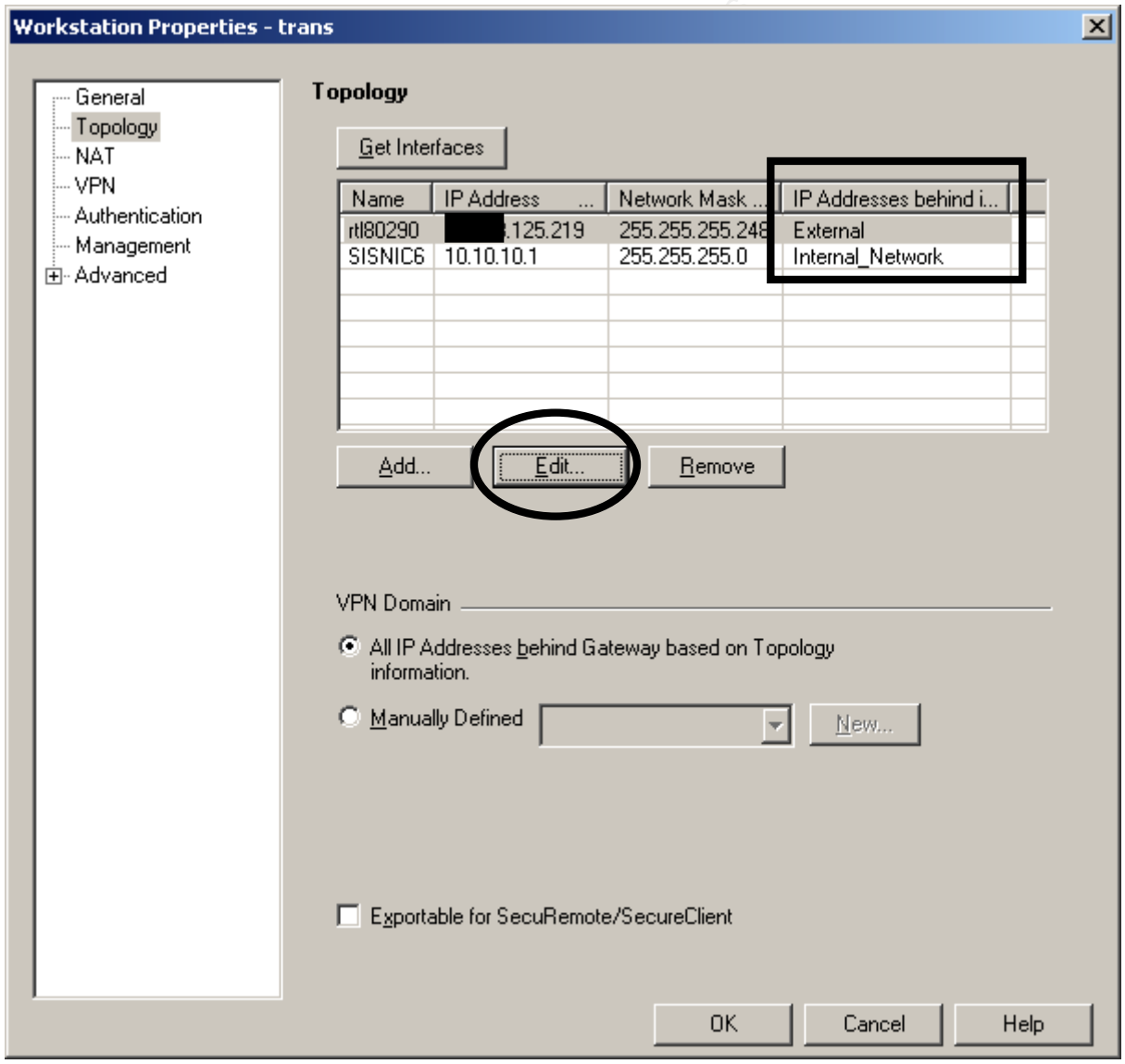
In the architecture we determined that we wish to use NAT for the services that we were providing to the public. The NAT would occur from a legal IP address on the outside face of the firewall to an illegal (private) IP address resident on a subnet. The methodology that I will use to perform NAT is to create "virtual" objects with the legal IP and then NAT them through to the actual object with the illegal IP address. With the selection of the correct settings, FW-1 will create the NAT automatically, which eliminates the need to get involved in arp and route issues. However, this means we create two objects for each service. The firewall object itself needs to be created once only.

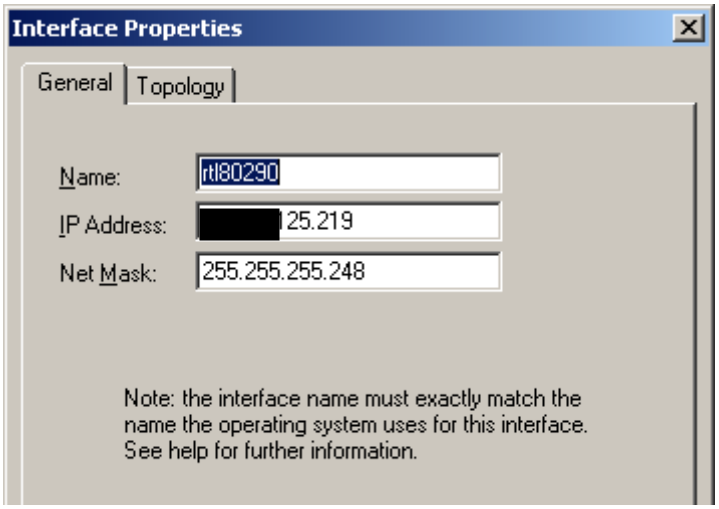
Defining the firewall network object.
This is created as a *New Workstation*. Enter in the details as per below ensuring that you select gateway for the Type. The IP address entered here is the one that the license pertains to, and is generally the IP address you have facing the Internet.



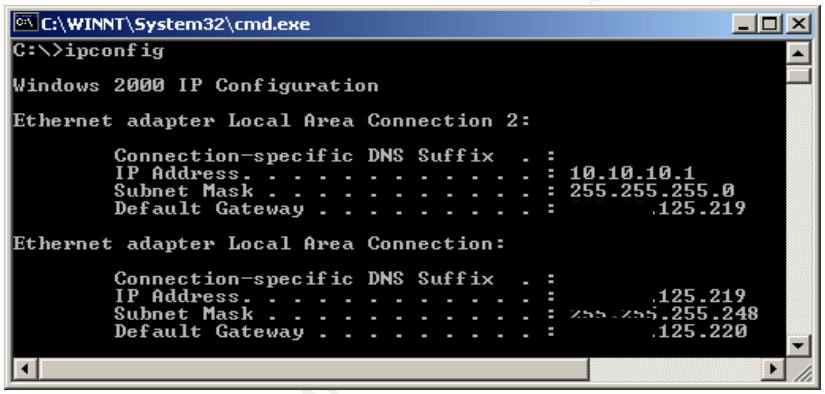
The more critical part of configuring the firewall is defining the topology, as this is where you "orientate" the firewall. It is also important for configuring the NAT correctly. Access this window by clicking on the *Topolgy Tab* to the left. You will be presented with a window that allows you to enter the details of each interface card present in the firewall.

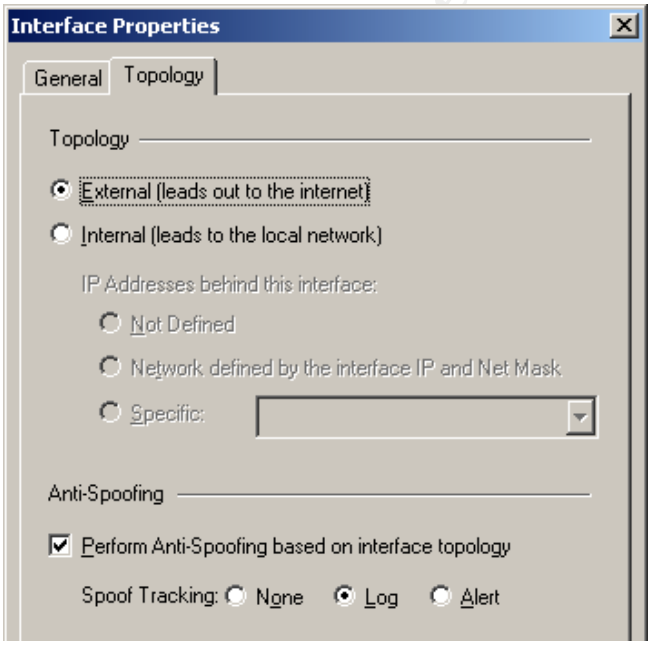
Enter interface details by clicking on the *Add* button or using the *Get Interfaces* button. The latter is the preferable option, as then all interfaces are named correctly. Using the *Get Interfaces* will produce results similar to those shown below as the firewall interrogates the Operating System about the interface cards. However, information shown in the square has yet to be entered. This must be done by clicking on the *Edit* button, which produces a similar window to the *Add* button, had we not used *Get Interfaces*.



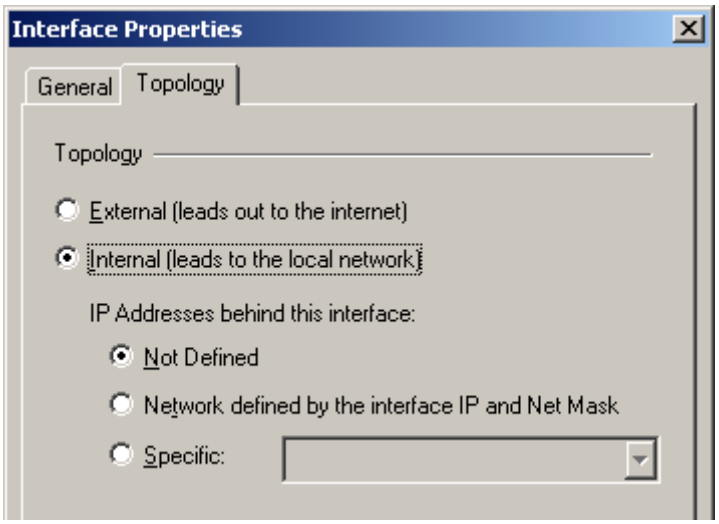


Following either button, you are presented with a screen as shown to the left. Enter details accordingly. Note the comment about the interface names, for Windows you can get this from the command prompt using the *ipconfig* command. See below.





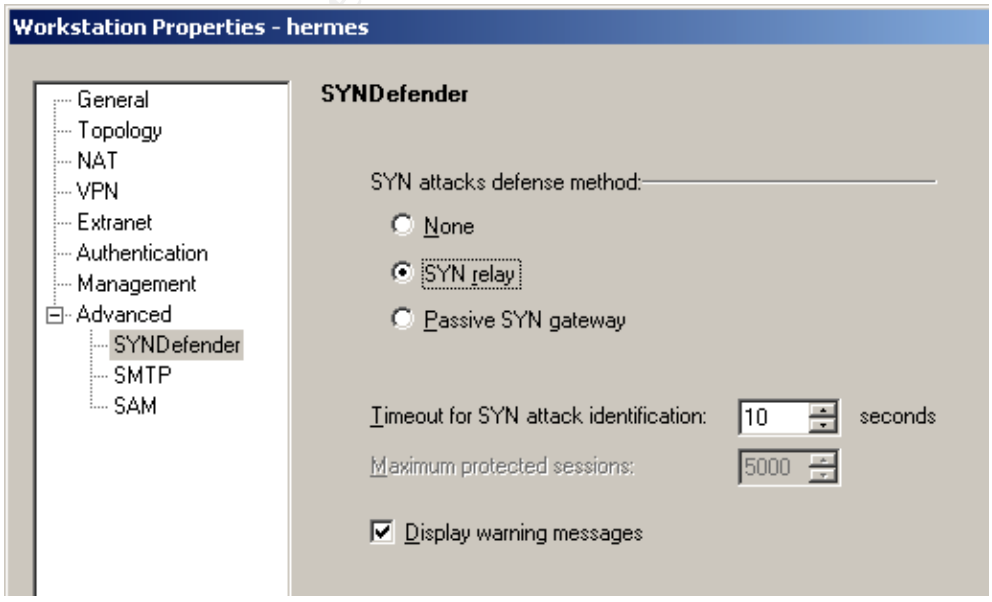
Click on the *Topology* tab to let the firewall know where this interface is positioned in the topology. In my case this interface is connected to the Internet. Also select the Anti-Spoofing and decide whether or not to log or receive alerts depending on your policy. I have logged as spoofing can create a lot of alerts that you may not want to have to react to. The *Topology* tab present the window shown below.



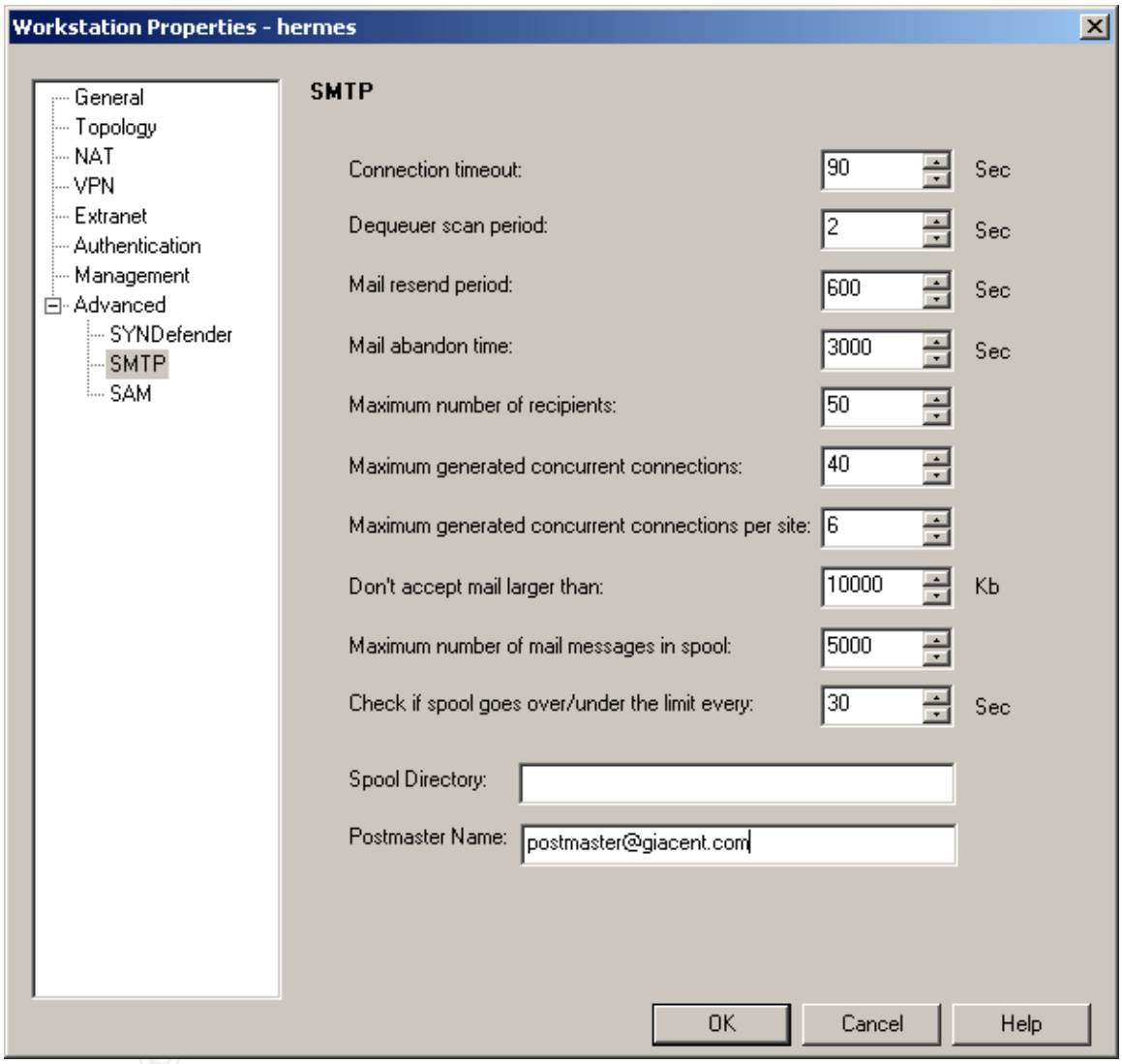
Now we have to configure the second interface on the firewall. This is set up in a similar way, however, when we define the topology on the interface, it is Internal. There are three options here, for the moment we will use Not Defined, but come change this later on. It is also quite acceptable to use the second option if you have correctly configured the inside interface card.

I will not display the configuration of the *Management* options available in the Workstation Properties window. These settings are very user dependant and also allow you to implement any procedures relating to how logs are to be handled. Needless to say, you should do some form of logging and give consideration to the maximum size and where logging is to be done. There are some settings that we should configure under the *Advanced* tab. These are explained below.

SYNDefender. The *SYNDefender* tab allows you to take measures that will protect the network from SYN attacks. Enabling the SYN Relay counters attacks by ensuring the three-way handshake is completed.



The last setting we want to affect relates to Simple Mail Transport Protocol (SMTP); this is accessed by clicking on the *SMTP* under the *Advanced* tab. Here you can define some rules about how email is to be handled. These will have a significant impact upon business activity so configure wisely. Of note is the setting that will allow you to reject email over a certain size. This will have a significant impact upon how GIAC Ent conducts business so this has been set to 10Mb.



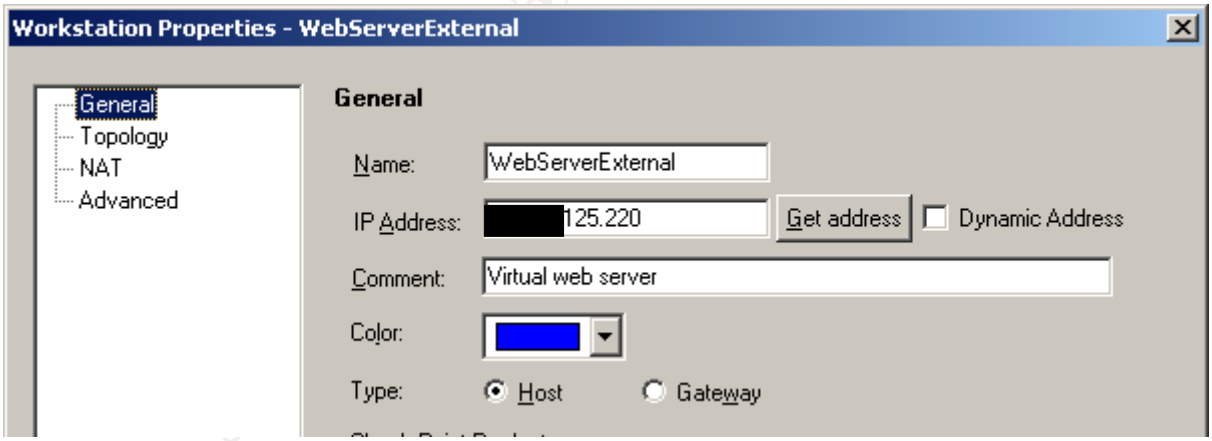
It is prudent at this point to mention that we will need to define further rules about how SMTP is to be handled. This will be done as part of defining our Services later in this tutorial.

We now turn to creating other Network objects that are present in the network and will be used in the rule set. The IP addresses to be used have been detailed earlier in the Policy statement. Recalling our earlier discussion on NAT, there are two types of objects we will be creating:

- Objects offering services to the public, as well as internal clients.
    - These objects require a virtual server to be created on the outside of the firewall, bearing the legal and public IP address with an equivalent real server in the DMZ bearing a illegal/private IP addresses.
    - NAT will be achieved using a **static NAT** methodology, where connections from the outside address are accepted and translated through with the response being allowed back out.
- Objects offering services to internal clients only; proxy services.
    - These objects will use the private IP addresses and use **hide NAT** to hide behind the firewalls address.

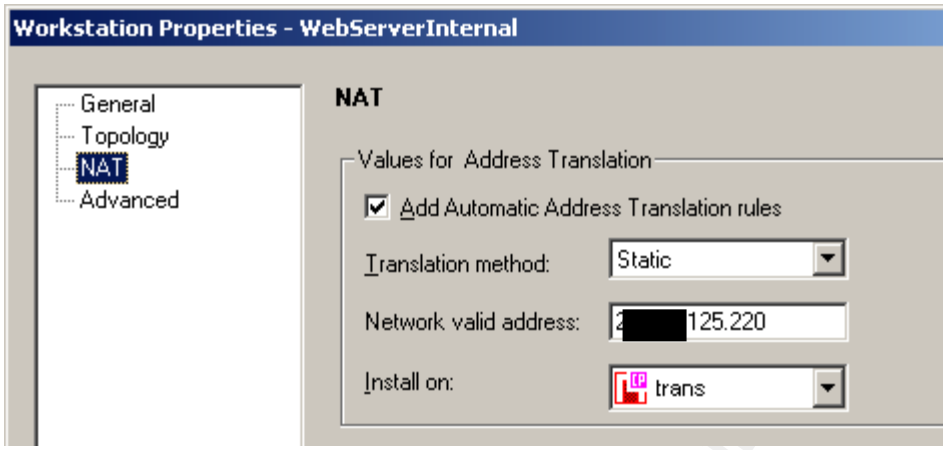
The first object to be added is our web server(s). This will be a new *Workstation*. Right click on the *Workstation* tab and select *New Workstation...*

We will create the virtual server first and then the actual/internal server after so we have an object to NAT to. Enter details as required, see graphic below. It is useful to make the name[5] and comments as specific as possible, particularly on a large network. I also try to use a consistent colouring scheme based on location in the network. This makes it easier to put devices into Groups later on. Using Groups facilitates management. We do not need to complete any of the tabs shown on the left for this object. However, ensure that the IP address is correct and that the object is annotated as a host.



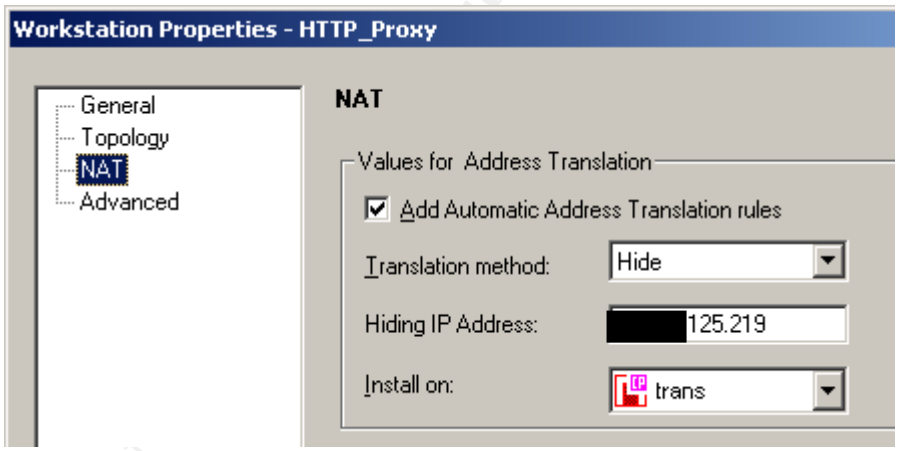
Next we create the actual/internal web server, using the same methodology and changing the details as necessary. However, for this object we want to add some NAT rules. Use the *Automatic Address Translation* rules and the firewall will generate the necessary instructions. The settings are shown below:

[5] Spaces are not allowed in the name.



The *Install on* drop down box relates to the policy object, in this case our local firewall. It avoids problems if you specify the box rather than the "all" option, even if it is a standalone. The other settings indicated in the left of the window are not necessary at this point. A similar process is observed to add other public objects on the network.

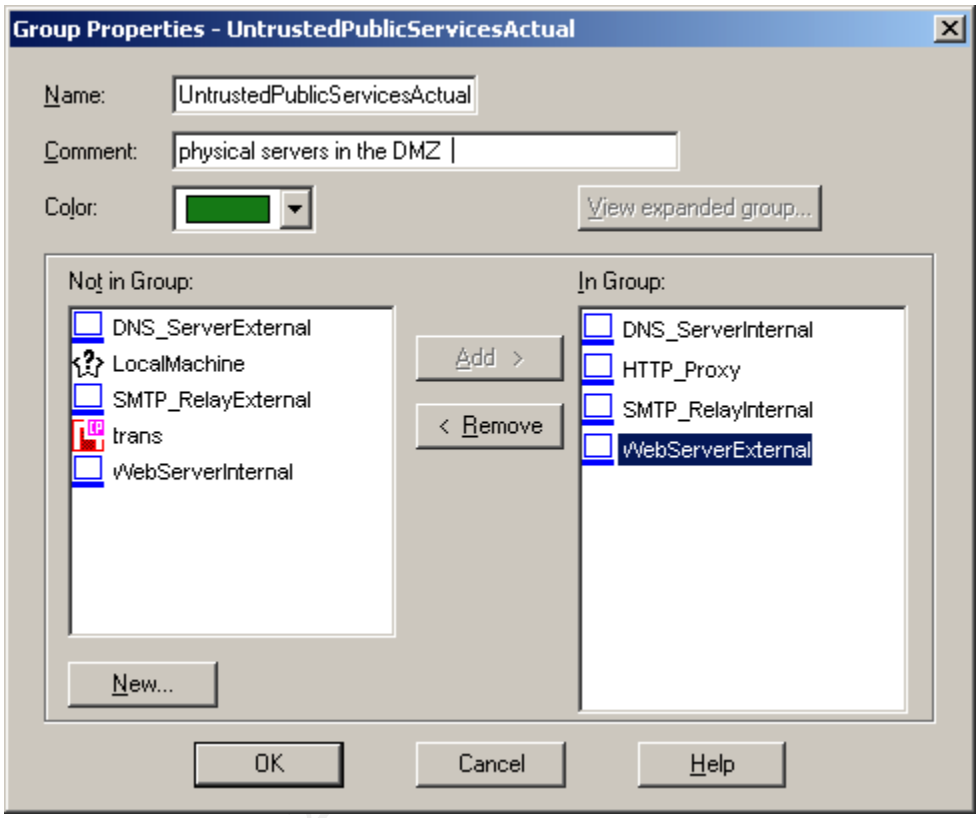
For the services that are doing proxy, we are using Hide as the NAT method:



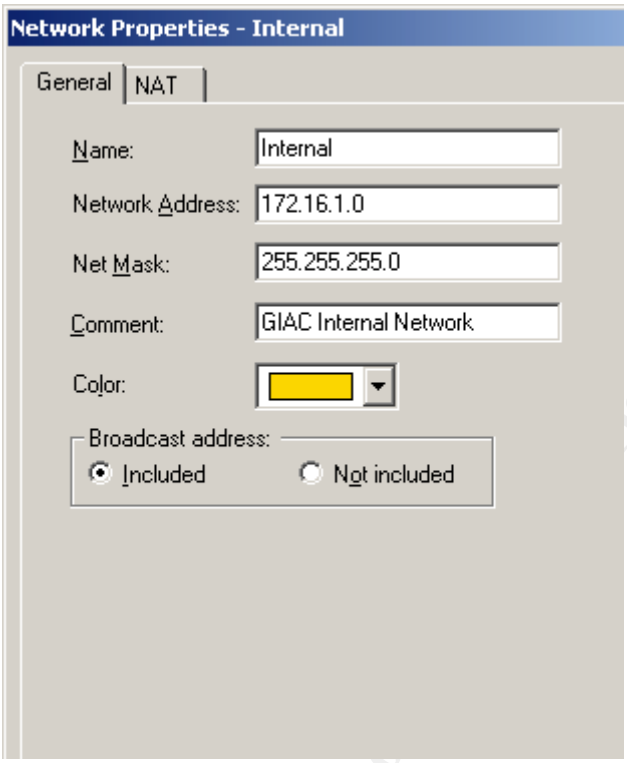
At this point you can check to see if the NAT rules have been created. Automatic rule generation should create two rules for static NAT (in and out bound) and one for hide (outbound). The actual NAT Rules were shown earlier in Part 2.

Once you have added all the devices present on the network, particularly those that have services that will traverse the firewall, you may group them. Grouping of devices keeps the rule set cleaner and is more efficient. However, care needs to be taken in the grouping used. I prefer to use groups for denying access but using specific objects when permitting access. A *Group* is created with a right mouse click on the Group icon and selecting *New → Simple Group*. You are then presented with a window that will allow you to define the *Group*. See the graphic

below. Once you have entered the general details pertaining to the *Group*, you may add the workstations/servers. This is done by selecting the desired items on the left and clicking on *Add* to move them to the right as part of the *Group*. See the graphic below.

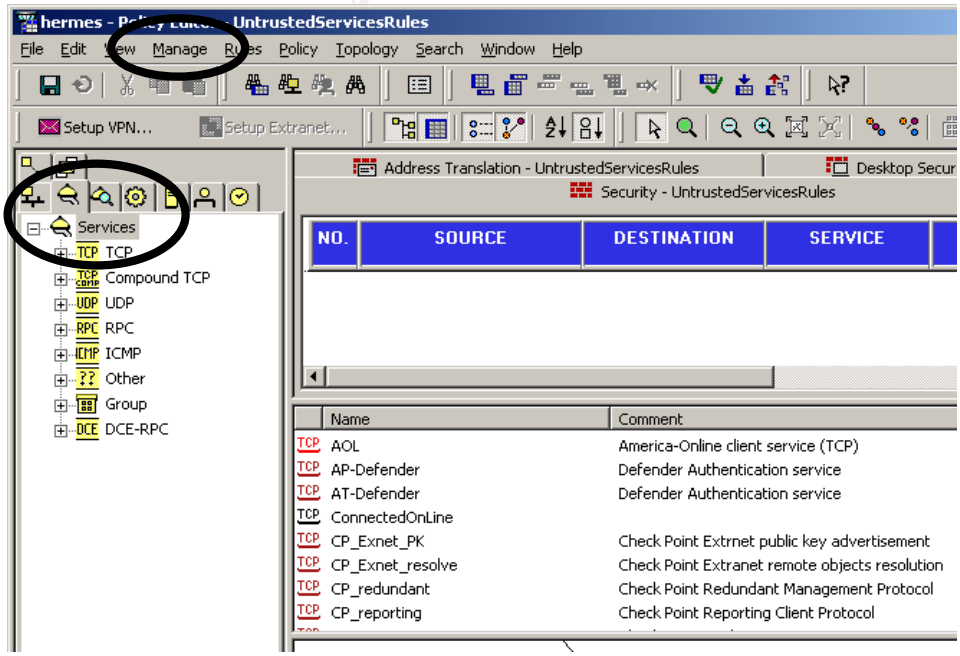


The final type of *Network Object* I will add for this rule set is a *Network*. In the topology I have designed, the internal network sits behind a firewall that separates it from the DMZ. The depth firewall is performing NAT, so no IP addresses should be leaking out from the internal network. To ensure this, I create a Network Object that covers the Internal Network and will include it in my rules et. A new *Network* is created using right mouse on the *Network* icon. You are presented with the window below, enter details as necessary. Whilst NAT will be performed on the Internal Network, it will not be by this firewall, so ignore the NAT tab.

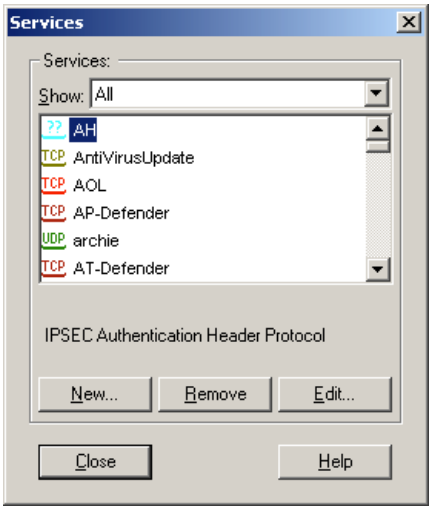


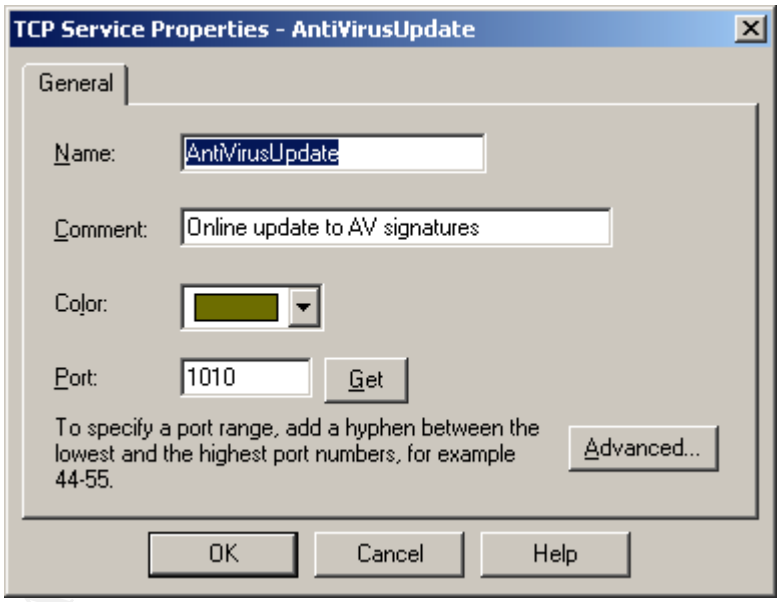
Define services

The CheckPoint Firewall comes with a large set of recognized services. If needs be you may enter in a proprietary service for your network. Services may be accessed in a similar way to network Objects, as shown below.



I have a requirement for a proprietary service on my network, the Antivirus Update. Selecting *Manage Services* produces the window shown on the left. Clicking on New brings up the window shown on the right. You will need to refer to the product vendor or documentation to understand what is required if you wish to add a service. Add the details[6] as appropriate from the vendor.

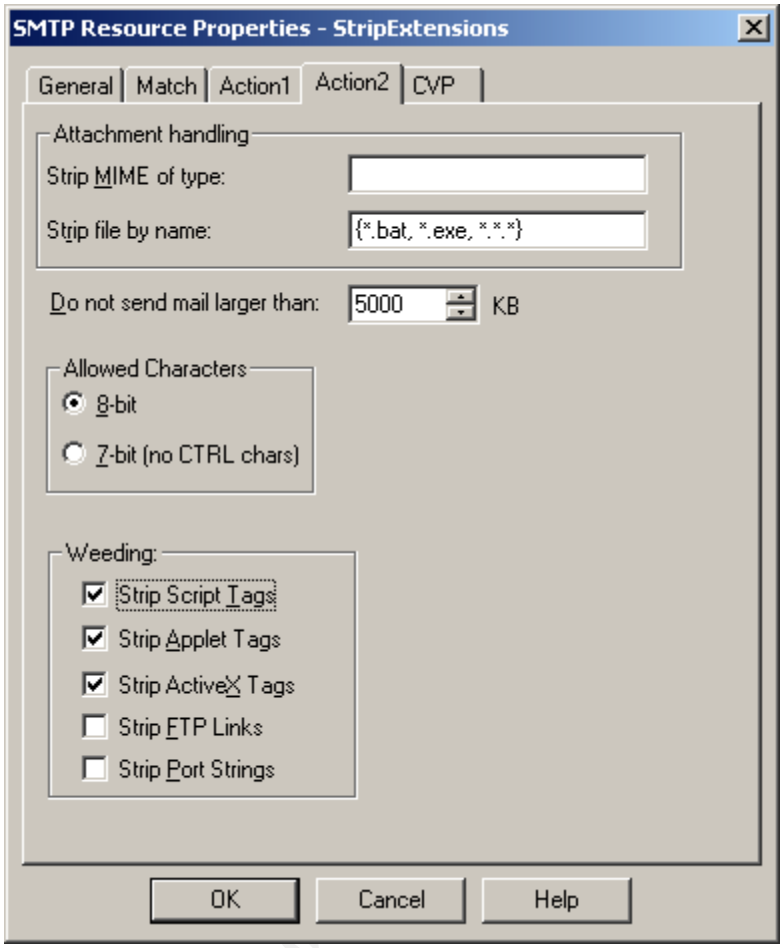




As mentioned earlier, we want to add additional rules regarding how email is handled. Email is a traditional vector for malware to arrive so we want to drop certain files from getting in via this method. A complete list of file extensions we may want to strip at the firewall is shown at the end of this tutorial. To get the firewall to strip extensions we manage the smtp resource. This is done by selecting *Manage → Resources*. Then add a new procedure using the *New* button.

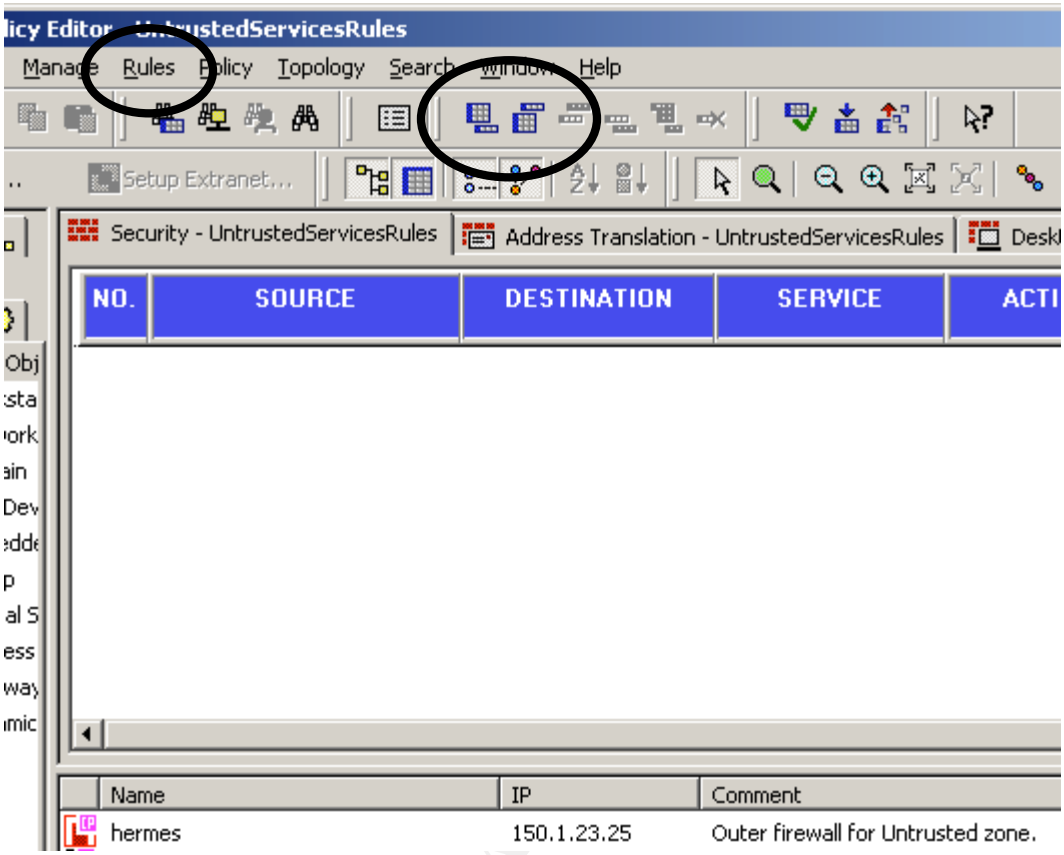
Name the procedure as you deem appropriate in the *General* tab. File extensions to be stripped are defined in the *Action2* tab. See below. Remember to use the { } brackets around the expression. The *.*.* is a catch all for files with "double-barreled" extensions, vis-à-vis the W32.Myparty@mm virus.

[6] The details shown here do not relate to any AntiVirus service *per se*, but serve as an example.



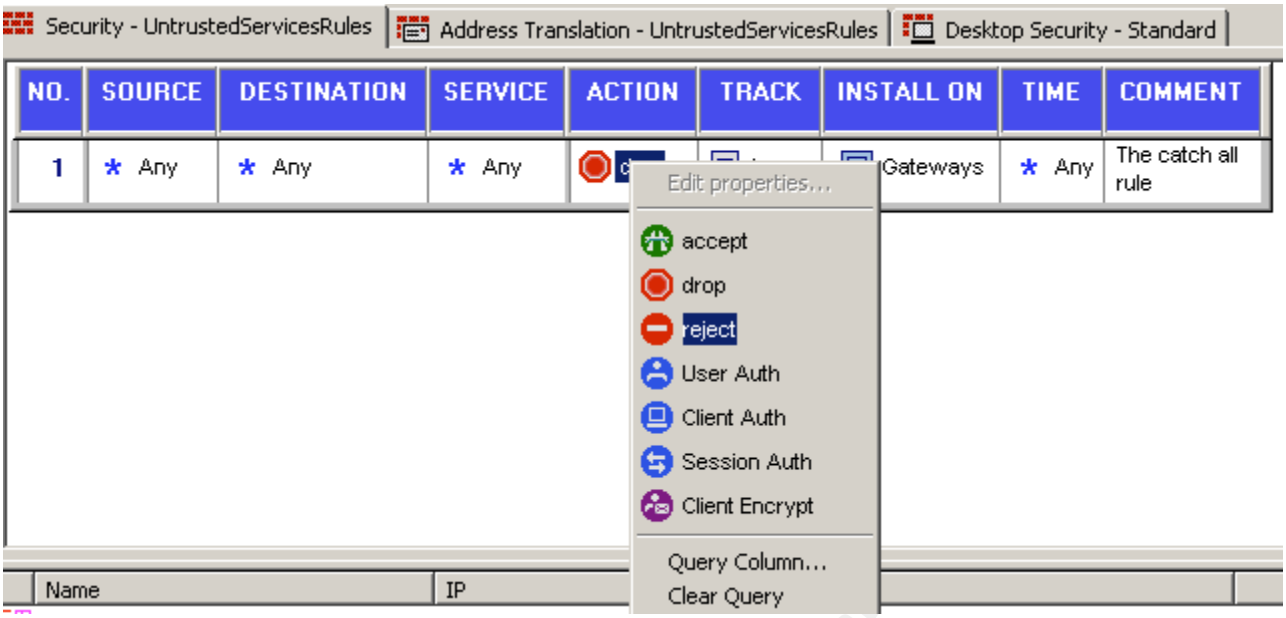
Add Rules

CheckPoint FW-1 NG comes out of the box with no rules viewable in the Policy Editor. The GUI is very easy to use and quite logical. The first rule we set should be the catch all rule which drops everything except that which we have approved. This is also the "default" rule that appears when one creates a new rule. To create a new rule use the *Rules* drop down or the "*Add Rule at the Top/Bottom*" buttons, see graphic below.



The rule that will appears is as below:

This is the basis rule from which we will create all other rules, adding rules above this one. However, this rule requires some minor adjustment to suit our purposes for the catch all rule. Changing any aspect of the rule can (generally) be done by a right mouse click on the item. See below:



We do this for the default rule so it finally appears as:

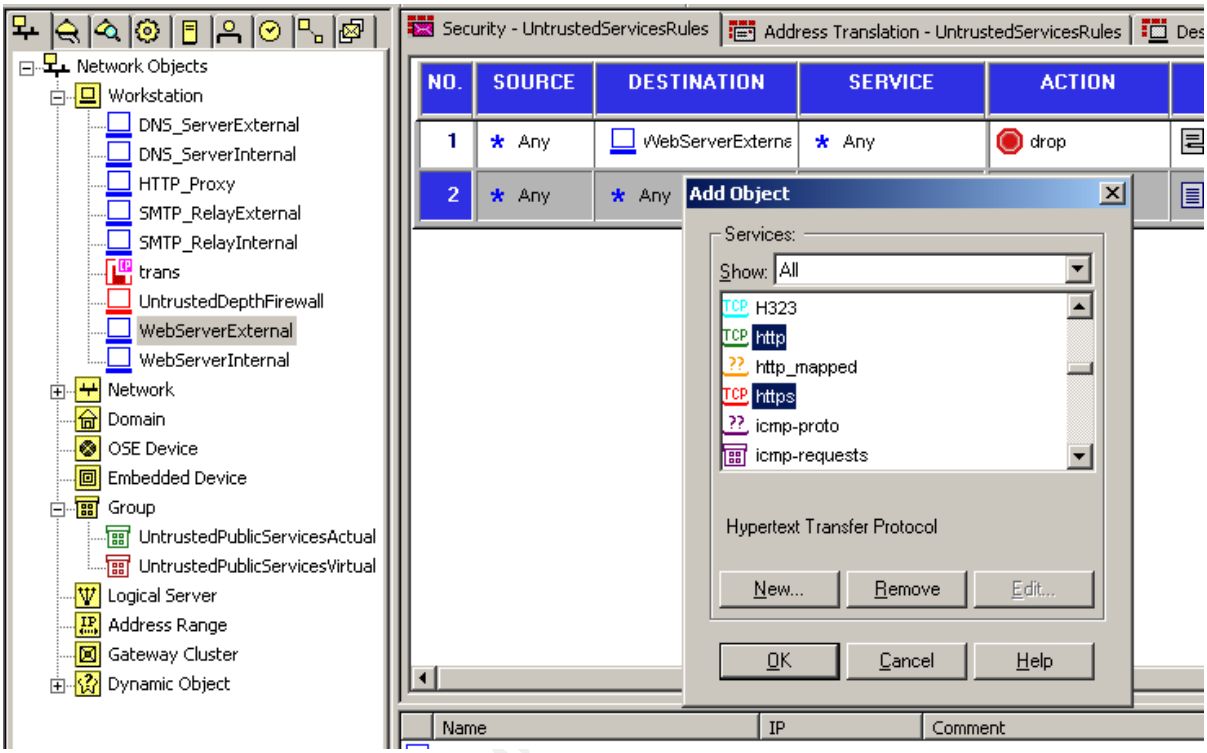
SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME
* Any	* Any	* Any	drop	Log	Gateways	* Any

Now that the catch all rule is set we can create the other rules appropriate for this firewall. It is useful to have a copy of your network diagram and services matrix nearby to ensure appropriate rules are being created. All other rules created must go above the catch all rule and their position relative to each other is important, but may be adjusted later. The second rule to be created will provide access to the GAIC web server. Rules may be added in one of three ways:

- from the *Rules → Add Rule* drop down menu or
- by using the icons in the tool bar or,
- with a right mouse click on the number area in the rule set itself.

Access to the GIAC web server is to be provided to the general public and has no restrictions placed on it in terms of this service. Therefore, for source we leave the setting as “All”. The destination is the external/virtual web server itself, which is added using right mouse and Add Object, and then scrolling to the Object created earlier as *WebServerExternal*. Next we need to define what services are allowed to connect to this object.

More than one service may be added, using right mouse *Add…* and by pressing the Ctrl key while selecting the multiple services. Our web server only offers http and https; so only those two services are selected. Click on OK to close the window.



Now we define an action that the firewall is to carry out in terms of the source, destination and service. We want everyone to be able to connect, so we accept these connections. The tracking is used to create a log entry relating to the transaction. This should be used intelligently, as logs can fill quickly. The other boxes are somewhat self-explanatory. Use the comments box to keep track of the purpose of the rule. Our final rule appears as:

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1	* Any	WebServerExterna	TCP http TCP https	accept	None	Gateways	* Any
2	* Any	* Any	* Any	drop	Log	Gateways	* Any

Using similar methods other rules are built, as per your policy requirement. At this point the rule order is not critical, as CheckPoint FW-1 will let you drag rules from one place to another. However, before making the firewall operational the policy the rule order will need to be scrutinized.

LIST OF SUGGESTED FILE EXTENSIONS TO BE DROPPED

Before adding these to any firewall rule set, research should be conducted to ensure the extensions are not required for business purposes.

ade	adp	bas	bat	chm
cmd	com	cpl	crt	dll
exe	hta	hlp	inf	ins
isp	js	jse	lnk	mdb
mde	msc	msi	msp	Mst
pif	pps	reg	scr	sct
shb	shs	vb	vbe	vbs
wav	wsc	wsf	wsh	*.*.*

PART THREE
VERIFY THE FIREWALL POLICY

Plan the Validation

Overview. GIAC Ent primary firewall is the one defending the Untrusted DMZ. The purpose of validating the firewall policy is two fold:

1. Unwanted connections. Ensure the firewall is providing adequate defence by stopping unwanted connections.
2. Permitted connections. Ensure the firewall is allowing connections to services GIAC Ent wishes to make available.

An initial analysis will be conducted of GIAC Ent security policy to determine the context within which the firewall operates. Recognition will be made of the business purpose of the services in the DMZ that the firewall protects and the connectivity requirements verified. The initial analysis will also determine if the computer the firewall is operating on has been configured correctly. This will involve checking BIOS settings, OS hardening and firewall modules. Furthermore, research for vulnerabilities will be conducted and assurance sought that the firewall and its OS have been patched correctly.

Technical Approach. The two conditions described above will be tested:

1. Unwanted connections. Broken into two categories:
   a. Attempted connections to services not available; such as an attempt to ftp into the DMZ or a direct connection to the firewall.
   b. Attempted connections through open ports to something other than the offered service; such RAS through port 80.

2. Permitted connections will be verified using appropriate clients to ensure connectivity; i.e. using a web browser to connect to the web site

Considerations. Ideally all of this activity would have taken place in a laboratory environment earlier. The results of that audit would have been analysed and appropriate changes made to the firewall. Nevertheless there is benefit in conducting such an audit against an operational firewall to ensure it is behaving correctly "in the wild". Historical data will be used to determine when the least amount of traffic is passing through the firewall in any given 24 hour period. The audit will then be conducted just prior to this timeframe on a Friday. The desire is to minimize impact upon legitimate traffic and provide as much time as possible to return systems to full operation before the workforce returns.

Estimate of Costs and level of effort. A team will be formed of five staff to be assigned to the audit. They will be given a schedule as below:

- Five days to plan the audit. Consider the implications and possible network reactions. Conduct all research and gather necessary tools. The team must also ensure all concerned parties are informed.
- Two days conduct the audit. Run the audit as planned and collect all data.
- Five days to analyse results. Discuss the results and analyse output from various tools. If a critical flaw is found this can be passed to network administrators for immediate remedial action.

Salaries aside, a budget of $US 5000 will be assigned to this audit for the purchase of traffic generators, packet sniffers and scanning tools. A selection of free tools will also be used.

Risks. The conduct of the audit carries several risks:

- It is possible that this activity may cause irreparable damage to servers and/or the firewall. Before the audit is to be carried out, all services are to be backed up. For critical systems, such as the firewall itself, the web server and mail server, identical servers will be built that can be swapped in if needs be.
- Denial of Service. It is possible that during the audit people may have difficulty connecting to the services. GIAC Ent will publicise the audit a short time before the event, describing it as "maintenance" so that customers are not frustrated.
- Detection of Actual Attack. During the audit it is conceivable that an actual attack could be taking place. Those individuals who are monitoring the defensive devices; firewalls and IDS may ignore alerts as being a product of the audit and ignore them. To defend against this, all parties involved will have a clear understanding of the audit procedure and what can be expected. The IP addresses used by the audit team should be known and if appropriate ignored by certain security devices. During the audit itself

there will be communication between the auditors and those who monitor logs/alerts to ensure there is nothing additional occurring.

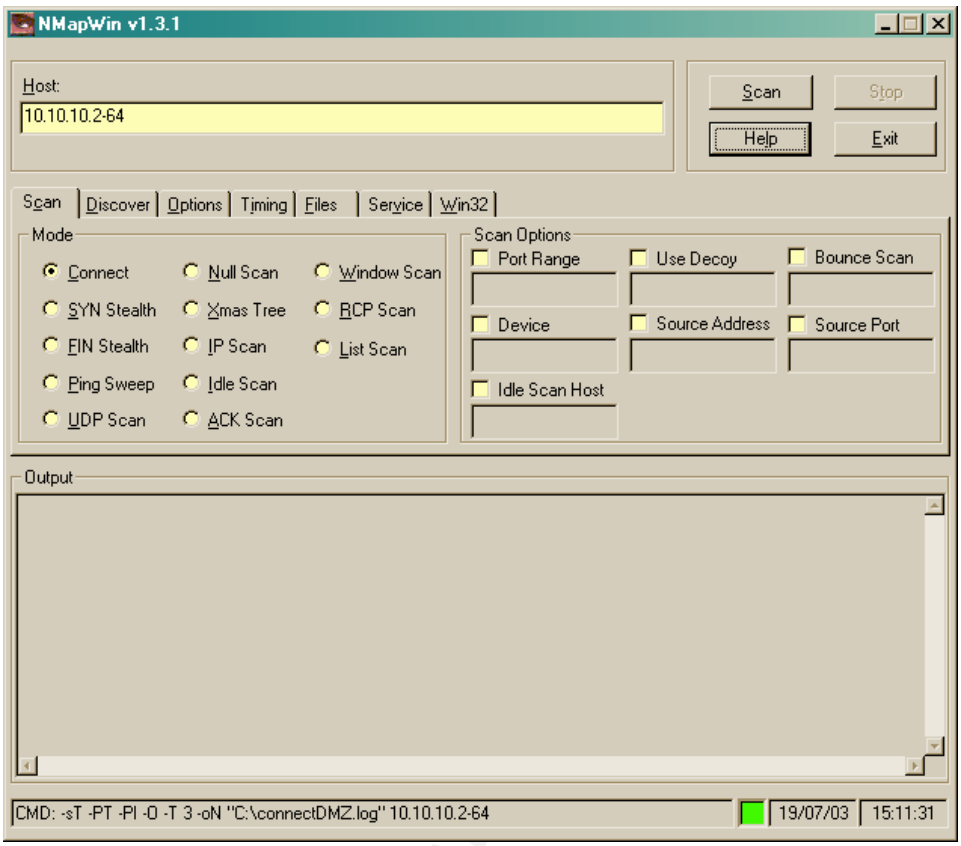
Conduct of the Validation

Technical Approach. The two conditions described above will be tested:

- Wanted connections will be verified using appropriate clients or a scanning tool to ensure connectivity; i.e. using a web browser to connect to the web site.
- Unwanted connections. These will be attempted using common applications and the nmap scanner. These tests are broken into two categories:
    a. Attempted connections to services not available; such as an attempt to ftp into the DMZ or a direct connection to the firewall.
    b. Attempted connections through open ports to something other than the offered service.

Verification of attempted connection will be via the appropriate application (if it returns a valid result) and by cross checking the firewall ruleset. For this purpose all the rules will be set to log all connections. Further assurance will be sought using traffic generators to send appropriate traffic to listening ports. Packet sniffers can be used to ensure correct traffic flow is being achieved.

Tools. Other than standard applications the Nmap scanning tool is used for this audit. In this case the version is NmapWin v1.3.1. Note that the output from Nmap in terms of the services it identifies are editable by the user and may not be accurate.



Verification of acceptable connections from the Internet:

Rule 1. Accept udp on port 53 to IP xxx.xxx.125.222 using nmap to send a udp datagram to that port:
Command:
-sU -P0 -p 53 -vv -T 3 -oN " port53.log" xxx.xxx.125.222
Result:
Interesting ports on (xxx.xxx.125.222):
Port State Service
53/udp open domain

Rule 3A. Accept http on tcp port 80 to IP xxx.xxx.125.220 using nmap to establish a connection (handshake) with a syn packet:
Command:
-sS -PT -PI -p 80 -T 3 -oN " port80tcp.log" xxx.xxx.125.220
Result:
Interesting ports on (xxx.xxx.125.220):
Port State Service
80/tcp open http

Rule 3B. Accept https on port 443 Accept https on tcp port 443 to IP xxx.xxx.125.220 using nmap to establish a connection (handshake) with a syn packet:
Command:
-sS -PT -PI -p 443 -T 3 -oN ” port443tcp.log” xxx.xxx.125.220
Result:
Interesting ports on (xxx.xxx.125.220):
Port State Service
443/tcp open https

Rule 4. Accept smtp on tcp port 25 to IP xxx.xxx.125.221 using nmap to send a SYN packet:
Command:
-sS -P0 -p 25 -vv -T 5 -oN ” port25.log” xxx.xxx.125.221
Result:
Interesting ports on (xxx.xxx.125.221):
Port State Service
25/tcp open smtp

Rule 8. Drop attempts to connect directly to Internal Network and the depth firewall using
Command:
sT -PT -PI -T 3 -oN “connectDMZ.log” 10.10.10.2-64
Result: This produced a mass of data, as nmap could not find a interface that would route packets through in order to make th connections. This is an expected result. An example is shown below.
WARNING: Could not determine what interface to route packets through to 10.10.10.2, changing ping scantype to ICMP ping only

Rule 10. Attempt connections on all other ports, across all hosts. Note by default nmap scans between ports 1-1024 but we need an extended range; ie. From 1 to 65535. Expected ports we can ignore in the results.
Command:
-sT -P0 -p 1-65535 -T 3 -oN "connectall.log" xxx.xxx.125.216-223
Result: These have been edited for brevity. However, the scan found two unexpected ports open:
Interesting ports on (xxx.xxx.125.219):
Port State Service
264/tcp open bgmp
265/tcp open maybeFW1

Verification of acceptable connections out from the DMZ.

These rules were tested in a similar method. For the sake of brevity the commands will not be repeated. The scans are conducted against the firewalls internal IP address; 10.10.10.1

Rule 2A. Allow through tcp port 53 from IP 10.10.10.6 by sending a SYN packet to establish a connection (handshake). This succeeded.

Rule 2A. Allow through UDP port 53 from IP 10.10.10.6 by sending a UDP packet. This succeeded

Rule 5A. Allow smtp on tcp port 25 from IP 10.10.10.4 using Nmap to send a SYN packet to establish a connection (handshake). This succeeded

Rule 5B. Allow AntiVirus update on tcp port 1010 from IP 10.10.10.4 using Nmap to send a SYN packet to establish a connection (handshake). This succeeded

Rule 6. Accept http on tcp port 80 from IP 10.10.10.5 using Nmap to establish a connection (handshake) with a SYN packet. This succeeded

Rule 7. Send a "ping" each server in the DMZ to the firewall and verify response, using ping 10.10.10.1 from command line. This succeeded, response were received.

Rule 9 and Rule 10. Reject connections from Untrusted services and the ctach all rule. This check will ensure all other connections initiated by hosts in the DMZ are rejected if not already explicitly approved. These rules can be checked with the same scan. The only difference being Rule 9 generates a reset packet to attempted connections from certain IP addresses. Note that by default, Nmap scans between ports 1-1024 but we need an extended range; i.e. from 1 to 65535. We can ignore expected/listening ports in the results. This will be done using the connect command and changing the scanners IP address to each one of the following three addresses; 10.10.10.2, 10.10.10.61 and 10.10.10.254. This scan produced large amounts of data, which is not included here. However, the following ports were found open.

Interesting ports on (10.10.10.1):

Port	State	Service
264/tcp	open	bgmp
265/tcp	open	maybeFW1

Evaluation of the Results

General. The firewall is responding as required for permitted connections. There were ports found open that should not have been. These ports are addressed below.

Results.
The Untrusted firewall had ports open on tcp ports 264 and 265 when viewed from outside and inside the firewall. These ports betray the existence of a Check Point firewall and could be useful information to a hacker and/or used to establish an unauthorized connection.

Improvements.
Close open ports on the firewall. Ports that were discovered open that are not necessary will be closed. This will be achieved in two locations to reinforce defence in depth:

- Deny those ports at the router by adding deny statements to the ACL.
- Insert a new rule in the firewall.

New Rule for the router.

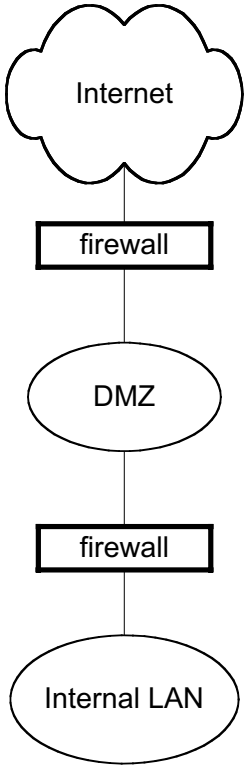
```
access-list 101 deny tcp any any range 264 265
```

New Rule for the firewall.
Create a rule in the firewall rule set to drop all attempted connections directly to the firewalls IP address. See below.

7	UntrustedDepthFirewa UntrustedPublicServic	trans	icmp-reques	accept	Log	Gateways
8	* Any	trans	* Any	drop	Log	Gateways

This rule is added as Rule 8. It must appear after the rule that allows “ping” requests. It is logged as attempts to connect to the firewall directly are a concern and should be investigated. Whilst the catch all rule would capture such events, this rule will allow separation from the general noise.

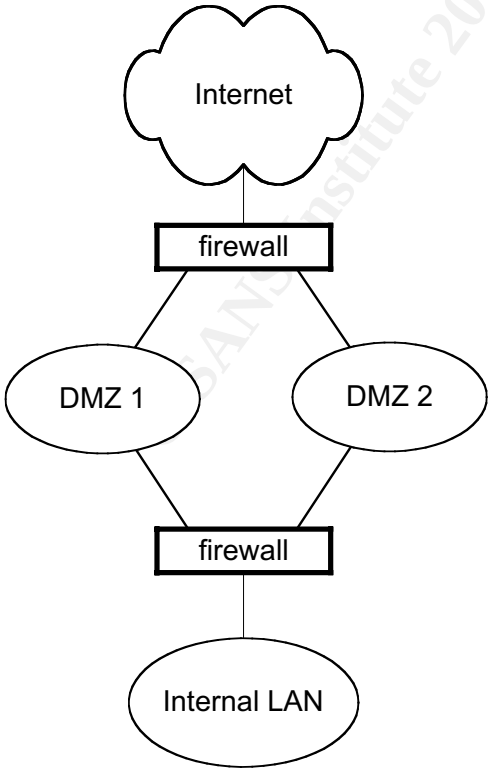
Alternate architectures.
From a security perspective it is more desirable to have the “public” face of GIAC Ent separate from the services made available to valued customers and partners. This has been achieved with the proposed architecture, however, it does create additional cost and additional maintenance. In the longer term one face of the network may become neglected over the other and security may suffer as a result. Some alternate architectures as presented below:



Alternate 1. A single firewall allowing all approved services into a single DMZ. This DMZ will offer services to the general public as well as VPN connections to partners. This is then separated from the Internal LAN by a second firewall. The firewalls will be different products on different Operating Systems.

Advantages. This configuration should reduce costs in terms of moving to a single ISP and less equipment is required. However, the external firewall will need to be capable of the tasks expected of it; VPN and the throughput of multiple services. Logging will be less distributed and therefore analysis may be easier.

Disadvantages. The external firewall is a single point of failure. In the event of a DOS attack or the router / firewall being compromised, then the whole network will suffer reduced or no services.



Alternate 2. Also uses a single firewall but separates the DMZ. Each DMZ will be on a separate subnet and off a separate NIC on the inside of the firewall. One DMZ will satisfy the public services and the other DMZ will handle VPN / private services.

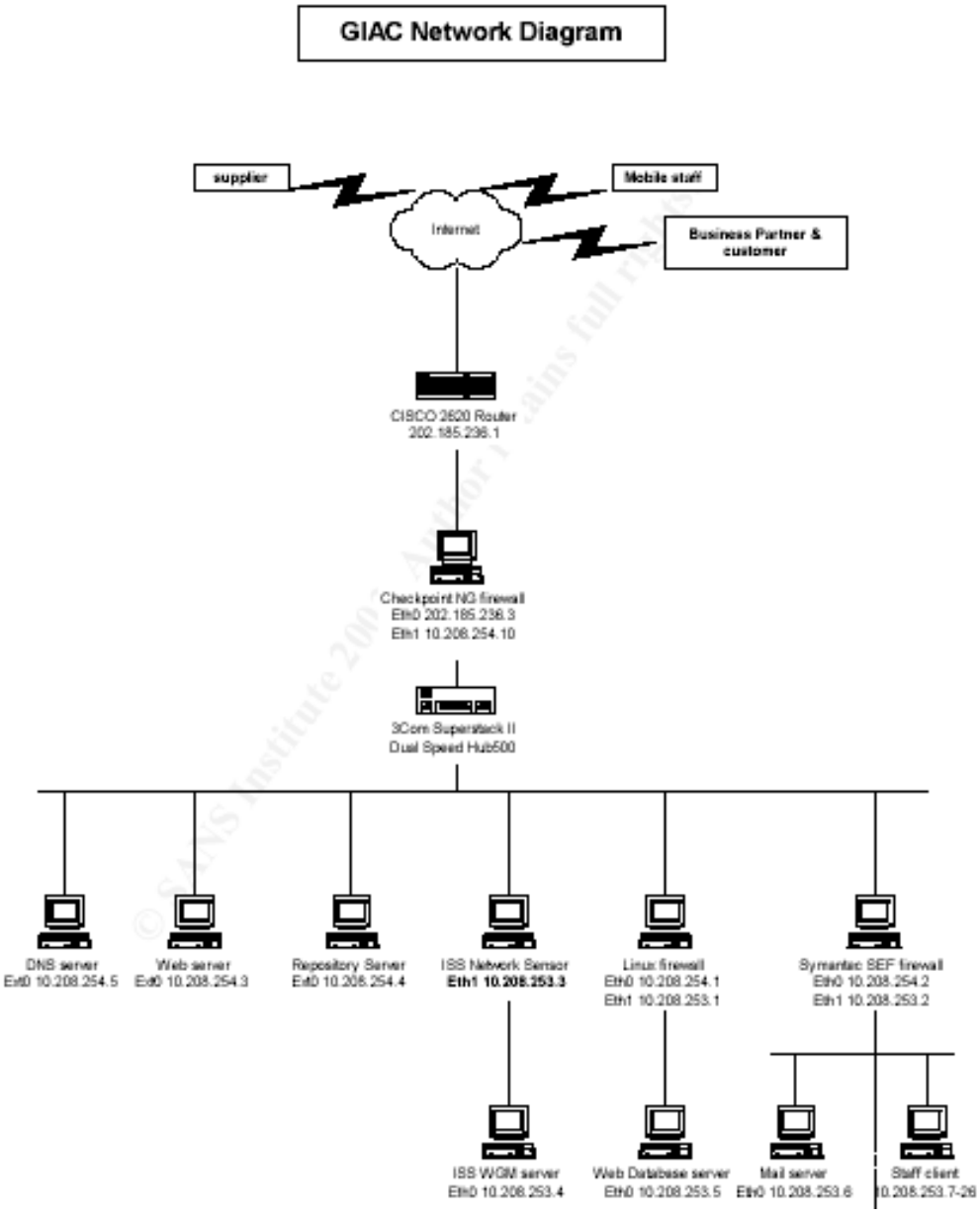
Advantages. Some cost savings again, but there will be increased costs associated with providing infrastructure for two DMZ. From a security perspective there is an improvement provided in the separation of services. The compromise of a system in one DMZ will not compromise all services, i.e. the second DMZ should remain unaffected as long as no trust relationship can be exploited.

Disadvantages. There is still a single point of failure with one external firewall.

PART FOUR
DESIGN UNDER FIRE

This evaluation is carried out against the network submitted by Chong Kah Sing. See http://www.giac.org/practical/GCFW/Chong_KahSing_GCFW.pdf

The network graphic is shown below:



Attack the Firewall

Overview. This network is using a Check Point FW-1 FP2 on a hardened Windows 2000 Server SP2, as per paragraph 2.2. The network diagram does not show a syslog server therefore it is assumed that the firewall is not logging remotely, but locally instead. If so then it is possible that the firewall may have udp port 514 open to accept connections from other logging systems. If so then the firewall is vulnerable to a malicious payload exploit.

Firewall Vulnerability. The vulnerability is documented at several locations:

http://www.aerasec.de/security/advisories/txt/checkpoint-fw1-ng-fp3-syslog-crash.txt

http://www.checkpoint.com/techsupport/alerts/syslog.html

http://www.secunia.com/advisories/8371/

Essentially, the syslog daemon can be crashed by sending malicious content to its listening port.

Attacking the vulnerability. The vulnerability is exploited through udp port 514. The attacker follows the following sequence:

- Send a valid syslog message. This verifies the existence of the firewall and that port 514 is open.
- Send a random payload
- Pause and wait for syslog daemon crash
- Attempt connection on 514 and if unavailable assume crash
- Run other probes/attacks against the firewall.

Results of the attack. The syslog daemon will crash and will not restart automatically. This has significant impact if there are any alerts set up to warn system administrators about malicious attempts to connect to/through the firewall. Whilst the rule set may still be enforced a remote attacker may be able to carry out probes and attacks without fear of logging and/or response. It is also possible, but not confirmed, that the remote attacker may be able to gain “root” permissions on the firewall itself. At that point, the whole DMZ could be exposed depending on how the new privilege is exploited. The attack may result in the following:

- Loss of logging of activity on the firewall.
- Possible compromise.
- Short term DOS if the firewall is service is restarted.
- Possible longer term DOS if the firewall is considered compromised and swapped out, depending on back-up readiness.

Countermeasures to mitigate the attack. Three actions can be taken to mitigate against this attack.

- Upgrading the firewall to FP3 HF 2 will mitigate the attack. This patch removes the vulnerability. See

http://www.checkpoint.com/techsupport/ng/fp3_hotfix.html#docs_hf1

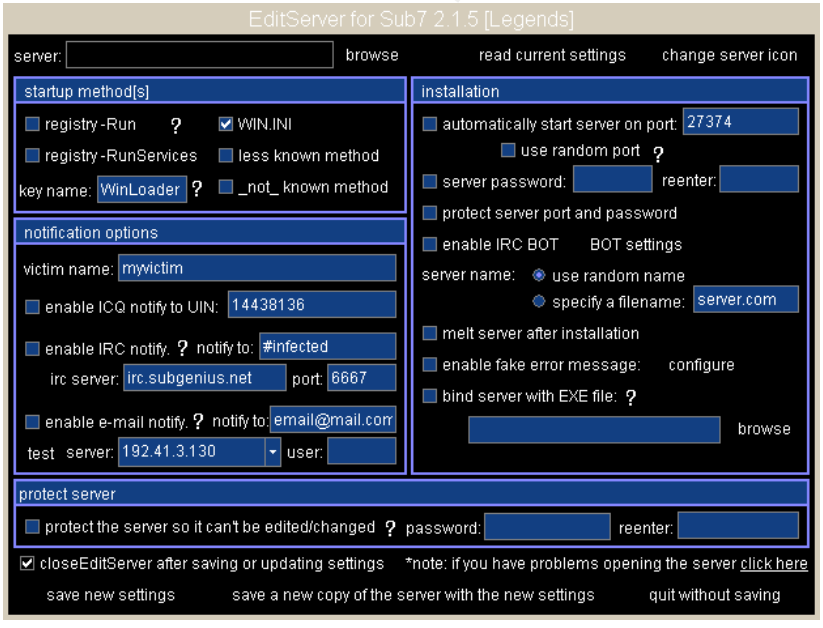
- Logging remotely, within the network should be implemented. If the firewall is logging to another device then the syslog will not be listening on this port.
- Deny connections to the port. Configure the router to deny connections to udp port 514 from the Internet. Add a rule in the firewall policy that drops/rejects such connections.

Distributed Denial of Service (DDOS) Attack

General. This DDOS attack will have three phases.

- Take control of the computers (victims) that are to be used to generate the DDOS attack using Sub Seven trojan.
- Upload selected DDOS tool (WinTrinoo) to the compromised systems.
- Launch attack.

Method to compromise 50 systems. Use spam email to distribute a Trojan, in this case Sub7. Sub7 has two components; the server and the client. The server program is run on the compromised system and listens for connections at a preconfigured port. See the screen dump to left for configuration options. The server can be password protected so that others may not use it. Distribution will be to email addresses on a selection of regional ISPs. The Trojan will be sent as an attachment, using various forms of social engineering to get the user to execute it. Once installed



the trojan can be instructed to listen for connections on preconfigured ports or make contact via IRC. Using the client to scan IP addresses owned by the ISP will yield specific IP addresses of the compromised systems.

Design of a Denial of Service attack. As systems are compromised or at any other time the DDOS tool may be uploaded and installed on the compromised system. Once 50 or more devices have been compromised the attack can be launched. Prior to the attack time, some research into the network would have been conducted. In this case the public IP addresses of the network have been determined using reverse address resolution of URL.

Assuming the intent of the DDOS attack is to cause harm to GIAC Ent business, the time selected to launch will be critical. The attack will be launched around 10am on a Monday. This is in anticipation of that being the time at which e-business is at its greatest volume. Hopefully there is also an increased chance of poor callout response as IT workers are late to work on a Monday morning! There is also a greater chance that the compromised systems are not being used by their owners who have gone to work and are not at home to notice a service degradation in Internet connectivity.

WinTrinoo launches a udp packet flood against random ports. The attack will be launched against the DNS server in the DMZ as this has three benefits from the attackers point of view;

- It floods the router, which may degrade its ability to handle legitimate traffic.
- It floods the firewall, which will consume processing resources/time and consume bandwidth.
- It may retard the DNS server itself and thus deny DNS service to legitimate users. This will have a flow on effect for web (http) and email (smtp) services that use DNS name resolution.

Countermeasures to mitigate the attack. This attack may be mitigated against at several levels:

- ISP.
- Router.
- Firewall
- Network Architecture
- Business Continuity Plan, BCP.

ISP. ISP should be encouraged to inform and/or educate consumers of broadband connections that they face increased risk and exposure to the undesirable aspects of the Internet. The ISP should recommend the use of firewalls and anti virus software on their client's systems. Furthermore, all ISPs should have means in place to identify DOS traffic and plans that may be enacted to defeat such attacks. This may involve dropping the traffic or denying all traffic from an IP address until such time as the DOS ceases. GIAC Ent may

wish to establish conditions in the SLA with its ISP which mandates such behaviour, including conforming to certain RFCs, such as RFC 2827 which details defence against DOS attacks that use address spoofing.

Router. The router ACL can be further configured to permit only that traffic which is expected for services offered by GIAC Ent. All other traffic may be dropped. This would reduce the chance of DOS traffic from getting to the firewall.

Firewall. The firewall rule set should be very specific. It should allow through only that traffic which is legitimately connecting to services offered in the DMZ. Consideration may be given to adding rules near the top of the rule set that drop the sort of traffic which is typical in a DOS attack, for example UDP ports above 1024.

Architecture. Som architectural improvements could be made to mitgate against DOS attacks. Load sharing across firewalls reduces resource consumption and better utilizes bandwidth. Consideration could also be given to splitting services offered across different subnets, this would remove sngle points of failure in terms of connectivity.

Business Continuity Plan. The organization should have a BCP implemented which will detail what is to be done in the event of a DOS attack. This may involve invoking a remote site with different IP addresses that takes over web traffic. Consideration could be given to outsourcing all web hosting to a third party as an interim solution. Such systems/responces would require modification to DNS records.

Attack Plan to Compromise the Internal System

Target and reason. The target of this attack is any one of the staff clients on the internal network. This network is selected as it is likely that internal network clients are the less well maintained and patched than servers and more vulnerable to exploitation. It is also likely that a variety of protocols and applications are being run on the clients that will generate significant amounts of logging. It is possible that the logs are not being monitored closely and so we may be able to establish connections without being discovered. Furthermore, users are sometimes less vigilant than IT professionals and may facilitate system compromise. Finally, compromise of a staff client will provide a useful launch pad for subsequent scanning and compromise of other hosts on the network. The path to the network will not be easy as it is defended by two firewalls.

Process to compromise the target. The email server being used is Microsoft Exchange, the actual client is not stated but it is fair to assume it too is a Microsoft product, either Outlook or Outlook Express. There is no mention of file extension dropping at the firewall so we can assume that all attachments are

being allowed in to the network. There is however, anti virus software being run at various locations that we must avoid.

There is an exploit that meets our requirements. A trojan can be delivered using a specially crafted email header that masquerades as a safe attachment. This methodology allows it to sneak past content filters and some anti virus products. This Trojan is known as **Backdoor.Sadhound**. Email addresses of internal clients will harvested from the web site and guessed from staff names that may be published on the web site. If this does not yield sufficient email addresses then bogus or false requests will be sent to customer services in the hope of getting a personal address in the reply. Once a number of email addresses have been gathered then emails will be sent with the Trojan attached.

The Trojan is executed once the user launches the attachment, which they believe is a picture. From the Symantec site, see reference page.

When Backdoor.Sadhound is executed, it does the following:

1. Copies itself to the %System% folder as MSWINS0CK.EXE. The file name contains a zero instead of the letter "O".

NOTE: %System% is a variable. The Trojan locates the System folder and copies itself to that location. By default, this is C:\Windows\System (Windows 95/98/Me), C:\Winnt\System32 (Windows NT/2000), or C:\Windows\System32 (Windows XP).

2. Adds the value:

```
Microsoft auto update %System%\MSWINS0CK.exe
```

to the registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

3. Queries IRC for commands to execute.

The Trojan software can also perform remote execution, deletion, or program uploading. However, the exploit may be further utilized if an Internet Relay Chat (IRC) channel can be established to the Trojan and commands sent.

Countermeasures.

Applications. This exploit does not work with Outlook. Removing all Outlook Express clients and replacing them with Outlook should protect the network.

Firewall. Two aspects to be addressed here:

- The firewall does not appear to be allowing (IRC) connections. Therefore, when the Trojan seeks to communicate by this means or an outside connection is sought to it is likely that the firewall will reject or drop the

connection. Such connections should be investigated if originating from inside the network and the source identified. This will allow remedial action to be taken, such as the removal of the Trojan. If IRC is a valid application on the network, consideration could be given to adding time constraints to rule set that permits such traffic.

- The firewall should be dropping all extensions that may be a malicious payload. What is permitted would have to be determined by business need.

Administration privileges. Employees should not have the ability to install software on their machines. This should prevent any malicious program/ attachment being run and becoming resident on a system.

Anti-virus and content filters. Anti virus applications are being used on the network and may detect this Trojan. Ensuring the signatures are kept up to date will increase assurance. Content filters should be modified to quarantine / delete any attachment with a double or triple extension.

User education. Constant user education will ensure users are aware of the threats and behave prudently.

REFERENCES

NSA Security recommendation Guides

http://www.nsa.gov/snac/index.html

DDOS Tools:

http://staff.washington.edu/dittrich/misc/ddos/

http://www.trojan.ch/index2.html

http://www.wickhill.com/products/webscreen/tools.asp

http://security.royans.net/info/posts/bugtraq_ddos3.shtml

http://www.sans.org/resources/idfaq/trinoo.php

Sub7 Trojan

http://www.subseven.ws/

http://520038635832-0001.bei.t-online.de/sub7getting-start1.htm

RFC's

ftp://ftp.rfc-editor.org/in-notes/rfc2827.txt Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

Sad Hound Exploit

http://www.theregister.co.uk/content/56/29137.html

http://techupdate.zdnet.co.uk/story/0,,t481-s2130783,00.html

http://www.sarc.com/avcenter/venc/data/backdoor.sadhound.html

http://vil.nai.com/vil/content/v_100011.htm