Global Information Assurance Certification
v1.9

Nick Richmond

Proposed Network Security Architecture for GIAC Enterprises

17 Jul, 2003

INDEX

Abstract

This document attempts to provide a network security solution to a fictional company, GIAC Enterprises. The solution to GIAC Enterprises has been broken down into four key sections.

Firstly the business needs of GIAC Enterprises have been gathered and analysed to produce a set of requirements that can ultimately be fulfilled through sound security design principles.

Once formal requirements have been gathered, the task at hand moves towards designing a solution to meet the businesses requirements. This solution will comprise of detailed technical apects which will be implemented on the systems concerned.

Finally, after out solution has been implemented, it needs to be tested or audited. By auditing our solution we can say with a high degree of confidence that it has performed as it was intended and as such is ready to move to a final production level stage.

After this has been completed an audit of another network design was performed, with the intention of compromising an internal system. Although the equipment that is based on the design is not present, an acceptable strategy for attacking it can be done based on the design alone.

Introduction

GIAC Enterprises is an online E-Business company who deals with the sale of bulk fortune cookies over the Internet. The clients of GIAC Enterprises are small to medium sized companies who purchase bulk fortunes over the Internet. GIAC Enterprises also has a partnership with another company, Partner Co. that provides GIAC Enterprises with the fortune cookie content.

Fortune cookies over the last ten years have experienced a strong incline in demand primarily by the Asian market, but increasingly so in the Western markets as well. Revenues are expected to top $20m this year, and $25m has been foreseen for next year. With fortune cookies becoming an increasingly lucrative commodity, competition for market share in the industry is becoming just as difficult. As such GIAC Enterprises has a strong need to protect its business from other companies and/or individuals who may gain advantage from accessing company data or disrupting services that are critical to the functioning of the GIAC Enterprises business.

With GIAC Enterprises current IT infrastructure it is clear that the business has a large exposure to both external and internal threats. As such GIAC Enterprises needs their network redesigned to meet their new security requirements.

Security Architecture

Business Requirements

GIAC Enterprises has five distinct group of differing access requirements: staff who run the business, customers who purchase the product, suppliers who provide the fortune sayings, partners whom which the sayings are shared with and mobile employees who work remotely.

Staff

All staff will require basic Internet access: Web and Email. For internal access, accounting department will need access to the database servers.
All staff should be able to dial up from home and access all resources that they would usually be able to do so on the LAN.
There should also be a facility to use non standard applications like streaming media should the need arise.

Systems Administrators

Relevant IT staff should have access to all systems for the purpose of administration. Access should only be as sufficient as needed and should be tightly controlled.

Customers

Customers tend to be small to medium businesses and as such need a simplistic way of ordering fortune cookies over the Internet. Customers should be able to securely purchase and arrange for delivery over the web based ordering system. Corporate purchases in excess of $5k should have extra consideration for security.

Suppliers

For business reliability and stability reasons, GIAC Enterprises has decided to order it's fortune cookie sayings from several supplier companies. All suppliers need to be able to securely transfer their cookie sayings to our systems such that we can process the sayings into the database. Their access should be tightly restricted to uploading cookie sayings.

Partners

GIAC Enterprises has several other fortune cookie companies for which they are partners of. The partnership allows other companies within the partnership, to retrieve the repository of fortune cookie sayings for which they later translate and sell themselves. GIAC Enterprises does not need access to the translated fortune cookie sayings.

Mobile Employees

Some employees will work from home and some will occasionally be at customer sites. Both groups need to be able to access appropriate IT resources over a dial up solution.

Design Goals

Once the security infrastructure is in place, IT employees at GIAC Enterprises will be resuming management of the network. As such it is desirable to keep complexity and maintenance levels to a minimum, where possible in order to keep ongoing costs such as maintenance and staff training, to a minimum.

Technical Requirements

Business requirements state the functionality that is needed from the design. As such these need to be analysed and translated into technical specifications in preparation for implementation. When considering technical requirements for access there are two key items that need to be identified for each separate requirement:

- who requires access and
- what do they require access to.

Although these are perhaps over simplifications they allow us to break down the task and define the two technical aspects for implementation:

- Users' environment. Critical to determine what methods of access are feasible.
- Data sensitivity. Perhaps the most important aspect as the more sensitive the data the stronger the authentication, and encryption if required, should be.

Staff

General staff will sit on the internal network and will generally be assigned a dynamic IP address from their local DHCP server. In situations where some staff will require access to machines within a DMZ, their IP address will have to be changed to a static equivalent.
Services that general staff require access to have a low sensitivity and therefore a high degree of security is not necessary. However, when ever Internet access is concerned, there must be sufficient security measures in place to insure that access to the Internet is as controlled as possible to reduce any chances of a security incident.
All staff will at least need access to the following services to meet basic web/Internet access:

- HTTP
- HTTPS
- FTP
- Telnet
- SSH

The top three protocols especially may sometimes be listening on a non-standard port in which case, the additional ports will have to be added to both the web proxies and external firewall.
Additional protocols, should the need arise will be reviewed on a case by case basis but should be minimal as only basic internet connectivity is require for general staff.
Should the need for more complex protocols arise, then there is a facility to use a socks proxy. The proxy services DMZ is ideally designed for just this, expansion..
Other services that staff will need access to such as:

- Email
- Internal DNS
- File Servers
- Printers
- Internal Web Servers
- NT Domain Servers

are on the internal network and as such are not internally protected by the security infrastructure.

One exception to regular staff are the accounting and HR departments who will need access to the database servers in the Database DMZ. This can be easily accomplished using:

- SQL*Net

The database servers, as stated by the business are especially critical to GIAC Enterprises. As such it is important that all access to the database servers is done as securely as possible. It therefore seems reasonable to require all staff needing access to the database to use the session authentication to ensure stronger authentication.

System Administrators

Systems administrators will all have fixed or static IP addresses and sit on their own segregated subnet. Having a static IP address allows source restrictions on any firewalls which they may need to pass though. Segregating the workstations from the rest of the internal network further protects the machines from any potential attacks. This is especially important so that the workstations aren't used as a platform for further attacks, especially ones into the DMZs for which we are trying to protect.
Protocols required will primarily be:

- SSH: Secure remote access method.
- FW1-auth: Provides additional authentication.

SSH will be also used to access all servers from the management server itself. As such it is especially critical that all authentications to the management server should be as strong as possible. Using Checkpoints Firewall-1 authentication/encryption combination with the two factor authentication provided by the ACE server should provide an especially strong and secure method of access.

Customers

There are two main types of customers:

- Regular: who purchase smaller quantities totalling less than $5000.
- High Valued: who tend to purchase large amounts of cookie sayings with a total value of greater than $5000

Both types of customers will be redirected to the secure web servers where the purchasing side of the operation takes place. The public web server will be used to provide static content and non-purchasing related info. This allows seperation of resources and allows both servers to be locked down to a greater extent.

Regular customers will be presented with options to select type of cookie sayings, quantities and input their credit card details for purchase. Once the card is validated the user proceeds to download their purchase.

High valued customers will login to their account using a username and an RSA SecurID token. Using the SecurID token provides strong authentication in the form of a two-factor authentication scheme. Two-factor authentication is especially strong because it not only requires the user to possess something, a SecurID card but also that the user knows something, a PIN number.

Suppliers

All suppliers will reside on the Internet, behind their own security infrastructure. They will be responsible for transferring their cookie sayings in bulk to the server within the GIAC Enterprises network. The Internet is inherently insecure and as such using it for a transport medium requires an especially secure communications channel.
A VPN is the ideal choice of method here as it provides the three crucial elements for a secure transport mechanism: confidentiality, integrity and authenticity. It is also is an especially scalable option as any protocols can be tunnelled over the VPN, should extra functionality be required sometime in the future.
The transport application would typically involve:

- FTP: File transport protocol itself.
- IPSec: Provides secure communication channel.

FTP provides sufficiently for both bulk file transfers and remote storage options such as filename and directory structure while IPSec provides the secure communications channel. For extra security precautions, the FTP server would run under a chroot'ed environment.

Partners

Partners fall into a similar category as the suppliers as both will use VPNs to connect to GIAC Enterprises Network. However unlike the suppliers, partners need read only access to the entire repository of cookie sayings. There is also a greater level of trust with partnership companies as it is in both parties interest to succeed. As such it is feasible to allow partnership companies, read-only access to the database. This can be accomplished using the following protocols:

- IPSec: Create a secure communications channel
- SQL*Net: Used to connect to SQL*Net proxy which then connects to cookie sayings database.

Using SQL*Net provides a simple yet efficient method for partner companies to access the repository of cookie sayings. However this does transfer some of the security work to concentrating on locking down the database more.

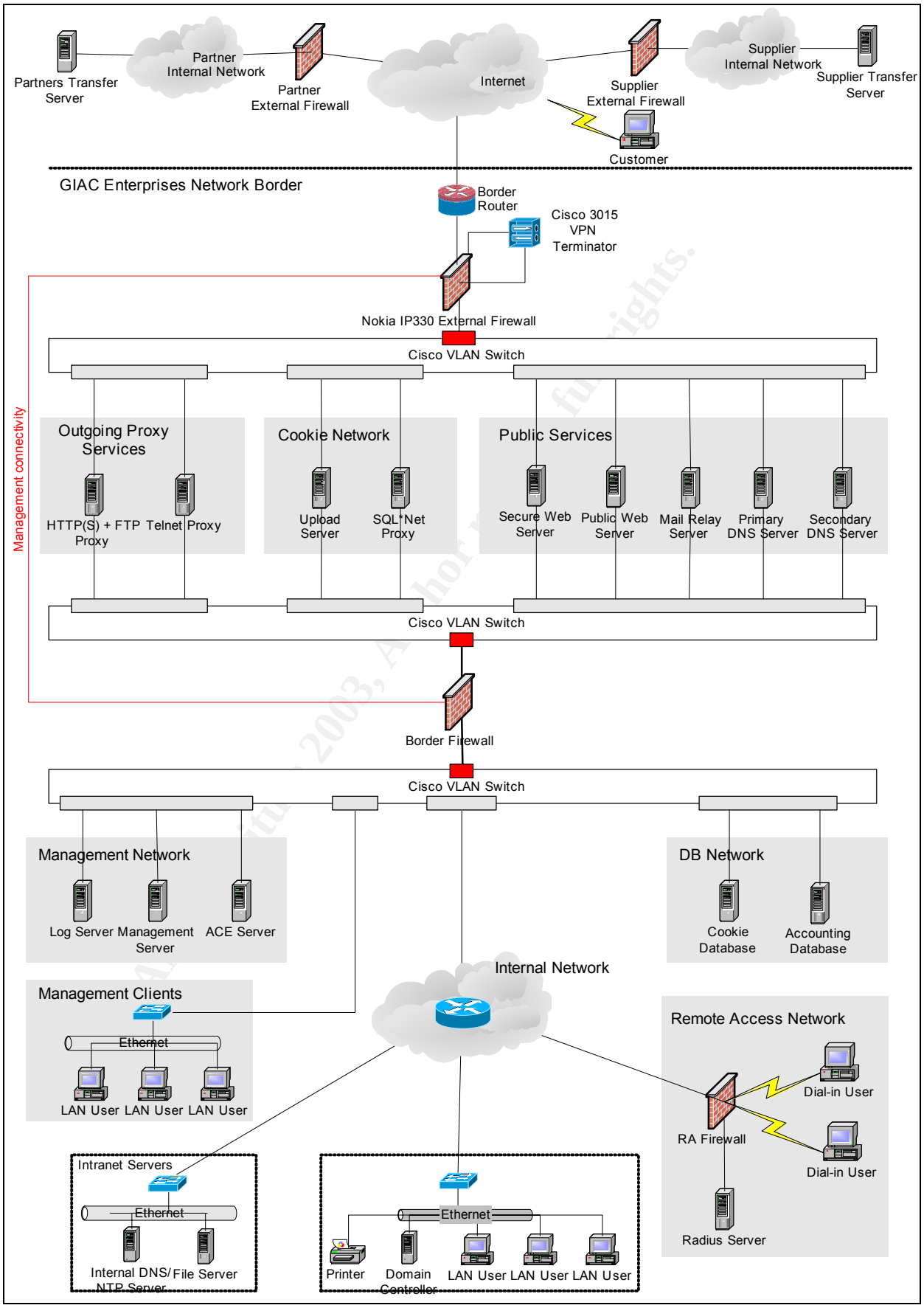
Mobile Employees

Mobile Employees are somewhat similar to clients on the Internet: the network which they connect over cannot be trusted. It is therefore critical to ensure that a secure channel can be created when connecting. Checkpoint supplies a product called SecuRemote which is ideal for this type of purpose. It allows the user to authenticate to the firewall which subsequently, upon success will create a point to point VPN between the user and the firewall.
Although this ensures confidentiality, authenticity and integrity, it is still critical to limit access for anyone connecting and to ensure that each person is only permitted access to the relevant resources. It is important to remember that remote access firewalls offer a way into the internal network and as such it is especially important to ensure that security is as tight as possible.
Employees will require access to a large number of services to ensure they can transparently work remotely. Services the will require access to are:

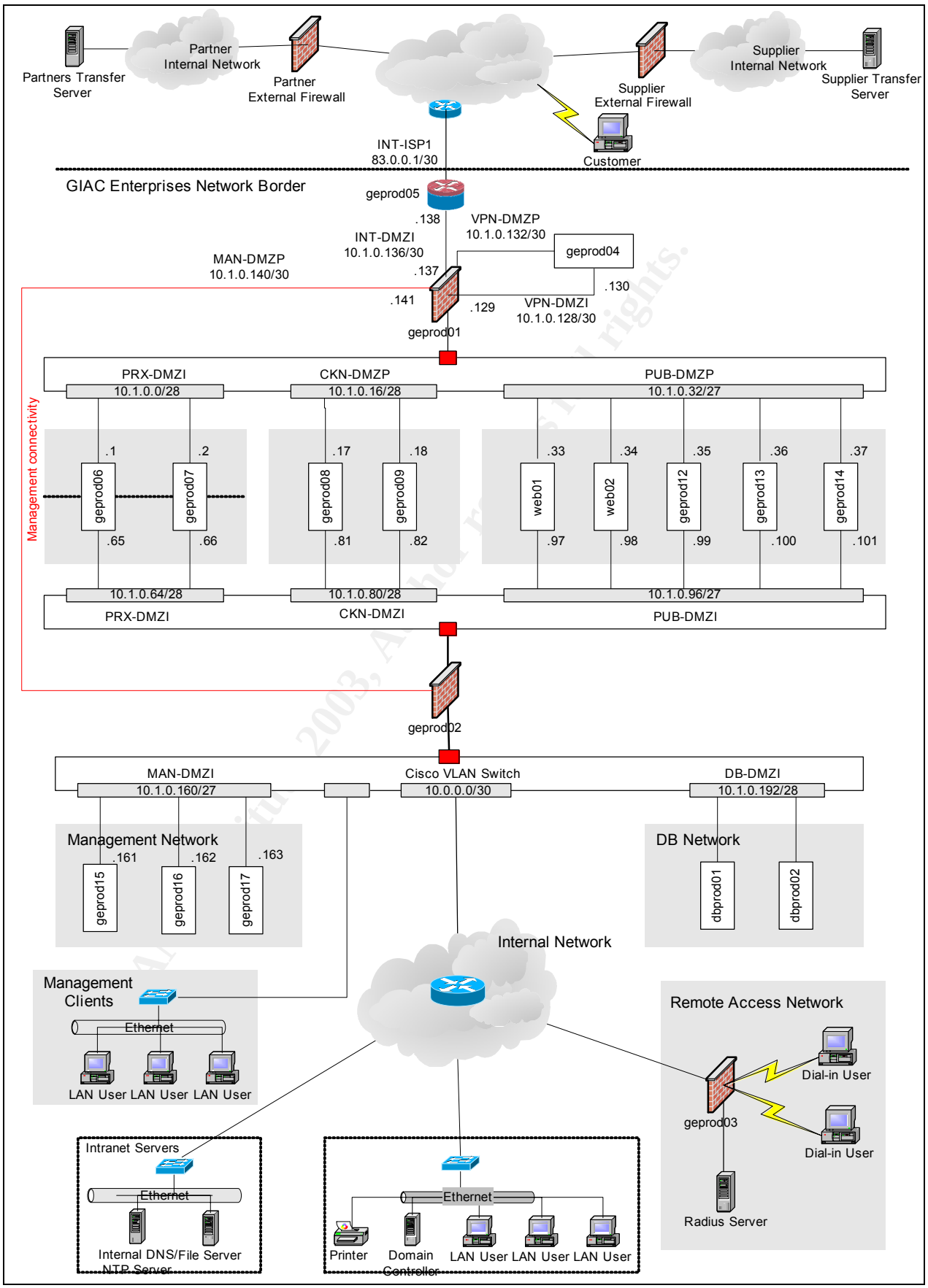
- Web
- Email
- DNS
- NetBIOS
- FTP
- Telnet
- SSH

Network Design

Logical Layout



Physical Layout



Network Overview

General Design Goals

When implementing a secure network there some axioms that should guide the design to its final stage. When these axioms are applied it generally leads to a significantly more secure design and aids in the principle of 'Defence in Depth'.

Identifying Sensitive Resources

In any network there are a multitude of servers and services offered. Securing all of these not only significantly adds to the complexity, which in itself can reduce security visibility, but is also unnecessary, not to mention prohibitively expensive. As such resources that are deemed important to an organisation or which have security repercussions need to be identified so that they can be secured.

Traffic Flow and Classification

One of the general design goals is to keep the more sensitive data closer to the internal network. Attackers will generally originate from the external side of the network thus to get access to the data on the internal side requires that they pass through more layers of security. This makes it more difficult for an attacker, to not only sniff more sensitive data but also to attack the channels by which the sensitive data travels over.

Resource Separation

Resources fall into two categories, services and data. One of the most important aspects of security is never to rely on any one component. As such it is important to physically separate different services so that if any one service is compromised, then it will not adversely affect other services. The same rule applies to data. If the data is of similar type to other data, but is differing in sensitivity then both data streams should physically separated from each other to help prevent one compromising the other.

Design Reasoning

Checkpoint NG on Nokia IP330

Checkpoint is renowned for ease of use and Nokia was chosen for its low maintenance. As stated in the business design objectives, one of the design intentions was to "keep ongoing costs such as maintenance and staff training, to a minimum." By using Checkpoint, it keeps the training to a minimum as the Checkpoint GUI is an intuitive product whilst providing a secure, commercially supported firewall. The Nokia appliance is a hardware device which comes packaged with a pre-hardened OS (Operating System). This eliminates the need to create and maintain a custom build of the OS. For any OS updates this can be performed easily and quickly via a central management system.

One of the most critical features of the Nokia appliance to this design is its ability to support VLANs which have been used extensively in the design. Support for VLANs is embedded in the kernel and as such can't be supplied by an application.
The combination of these two products results in a low total cost of ownership while meeting all our security requirements.

Single Vendor Reasoning

There is a trade off for going with a single product, it generally means, however unlikely if correctly configured, that if one firewall is compromised, or subverted the other firewalls can be compromised or subverted in the same manner. Using two different types of firewalls helps prevent against this but does result in higher maintenance and costs. As GIAC Enterprises have stated that they want to keep maintenance low, it has been decided to go with a single vendor solution.

Dual Firewalls

Although many designs for a similar network may chose to use only a single firewall, it was decided that the network was of sufficient size and required the added security of using two firewalls. Having an extra firewall allows us to better segregate networks of differing security levels and better flexibility to implement new networks.

Cisco 2950 VLAN Switches

VLAN switching has had a history of several security problems, but which were mostly related to trunking. In our design trunking is not used which alone mitigates most of the security risks.
VLAN technology itself has matured since then and is now increasingly becoming an acceptable device for use in secured environments. With the onset of appliance/hardware firewalls such as the suite from Nokia and Cisco's PIX's, network interfaces can be somewhat limited. By supporting VLAN switching, the lack of available interfaces is no longer an issue as it is only restricted by the number of ports on the VLAN switch.
Finally, VLAN switching provides significant more security over standard switches by preventing servers on the same subnet from talking to each other directly. If any server wishes to communicate with another server on the same subnet, it must pass through the primary port on theVLAN switch, thereby passing through the firewall rule set as well. This gives significant more control over traffic flow and is especially important when trying to reduce any potential further damage that may result after a server has been compromised. If a regular switch or hub was used for the subnet, then an intruder would have unrestricted network access to all the other servers on the same subnet. Clearly this is a bad idea.

Cisco 3620 External Router

The border routers goal is to not only route packets between the service providers and GIAC's network but also to do basic filtering of both incoming

and outgoing traffic. This basic level of filtering will provide the first line of defence for the network. It will not have an extensive security policy as that will be performed by the external firewall, but it will drop packets that are not needed such as some ICMP types, source routed packets and other packets that do not meet any ingress or egress rules. Having an extensive security policy on the router as well as the firewall is somewhat better from a security standpoint but unnecessarily complicates the network, especially when troubleshooting. As such there has to be a trade off between a marginally more secure network or a more manageable one.

Remote Access Firewall

Remote access is an especially important entry point to any network. Once authenticated to the Remote Access service, the user generally has a very high level of visibility of the internal network. As such it is especially important to ensure that this entry point is as secured as much as possible.
A VPN over the Internet is an option but if numbers of remote staff is sufficient it is not only more cost effective to have dedicated dial in but also more secure. Publishing any service on the Internet should be considered a large risk, due to the ease of access and network visibility that the Internet provides. Combining this with the generally high level of access that is granted for remote employees, using this as an access method should be strongly discouraged.

IDS

Network IDS tend to be noisy and do require a significant amount of work to implement and maintain successfully. Seeing as GIAC Enterprises are concerned about costs, this is an unnecessary addition to the network. Host based IDS's are much cheaper, less noisy and potentially more useful that a network based IDS. Products like Tripwire provide a method of ensuring file system integrity by comparing files against a known secure baseline. Should a compromise occur, then the administrator knows exactly what files have been changed, which is critical in determining what the intruder did and how they did it.

Cisco 3015 VPN

If we used checkpoints SecuRemote on the external firewall instead of a dedicated VPN the firewall now has a services listening on a public interface. This is especially bad for security as an attacker now has a much greater opportunity to compromise the firewall through the SecuRemote service. Having a separate VPN segregates this so that should the VPN be compromised, it will be limited to the services that are available through the VPN.

IP Addressing

The IP addressing has been structured such that all public services are allocated a publicly routable IP address which are all then passed through a

NAT (Network Address Translation)/PAT (Port Address Translation) table which translates them to private IP addresses. That is, all Internet reachable servers will hide behind a NAT'ed IP address. There is one exception to this which is the VPN. This will have a publicly assigned IP address which will not pass through the NAT table. The reason for this is that IPSec, the protocol which provides the VPN transport, will not function when the connection is NAT'ed. This is due to the Authentication Header (AH) in the IPSec protocol relying on the source address for part of it's authentication.
The actual public subnet that will be used will be 223.0.0.0/26. This allows for 64 IP addresses but which must be further split into smaller subnets, resulting in much less that 64 usable IP addresses. Although the subnet is actually reserved, it will be assumed that this network has been assigned and allocated to GIAC Enterprises.
One other public subnet that will be used will be 83.0.0.0/30 and 83.0.0.4/30. These will be used for the router to connect to upstream providers.

Split DNS

DNS is such an integral part of any network these days so it helps to separate DNS resources where possible. On solution to this is to use a system called Split DNS where by two main sets of DNS servers are maintained, one for public DNS queries which sits in the public services DMZ and one for internal queries which sits on the internal network. This prevents any queries on the public DNS server to reveal any information about the addressing on the internal network. Any internal queries about external IP addresses can be done by the internal DNS server forwarding the request to the public DNS server.

Mail Relay

Sendmail, the most commonly used e-mail server implementation, has a history of security problems so it is not unlikely that future implementation will occasionally have security problems as well. This makes it especially important to attempt to secure the mail server as much as possible. One of the ways to do this is by implementing a cut down version of sendmail whose only function is to store and forward email to an internal email server. This allows the internal mail server to be fully functional while the mail relay simply forwards mail to and from the internal mail server.

SQL*Net Proxy

Cyberguard provides a hardened server with many proxying abilities. The protocol that is of interest here is SQL*Net. Allows partners access to the database while giving GIAC Enterprises extensive logging on what requests can be made. Although the cookie sayings database is at the core of GIAC Enterprises business, it has been agreed that partner companies are to have access to the database. Combining the SQL*Net proxy with access rules on the database itself, should provide a secure enough solution for both GIAC Enterprises and their partners.

Upload Server

This would ideally be an FTP server running in an application or chroot jail. Suppliers could upload their cookie saying to this server which would later be retrieved by the database server for processing.

ACE Server

This server provides strong two-factor authentication which is needed for high value transactions, remote access and authentication for administrative management. The strength of this authentication scheme is two-fold: the user must posess a physical object, a SecurID card which provides a one-time pad and they must also know something, the PIN number to the SecurID card. This prevents any replay style attacks as each passcode can only be used once and getting the token card itself is difficult as it requires an attacker to be in physical contact with the user.

Security Policy and Tutorial

Different security devices have differing policies due to differing requirements. The external routers are only to act as a preliminary filtering device while the firewalls have a much more thorough policy. The third type of device, the VPN has a different purpose altogether, to secure incoming connections by encrypting a tunnel.
The reason for the routers not having extensive security policies is primarily for manageability reasons but also for functionality reasons. Having extensive policies on both the external routers and the firewalls can come with an increased overhead, not only in implementation of security policies but also with problem troubleshooting. Firewalls are also much better at handling the flow of traffic and the protocols associated with that traffic flow. This is partly due to the fact that most routers do not perform stateful inspection of traffic where as firewalls, at least modern ones are optimised to do this and more.

Border Router Policy

The purpose of the border router is to act as a preliminary filter for network traffic that could be deemed malicious or useless as far as GIAC Enterprises network is concerned. It should not have a comprehensive policy as that is not the routers primary function. It would also unnecessarily increase overhead in maintaining the network, whilst providing only a marginal increase in security.

Router Lockdown

Before ACLs can be written, the router itself needs to be locked down so that unnecessary services and options are disabled.[1]

Source routing is where an attacker can specify the list of routes a packet should take. This can be dangerous because it allows the attacker to spoof their real address but are also able route all packets via their own host,

[1] http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/

regardless of spoofed address used. Clearly this is a bad idea to accept any traffic matching this type.

```
geprod01(config)# no ip source-route
```

Many Cisco routers also come packaged with a service called CDP (Cisco Discovery Protocol) which is enabled by default. Not only is this function not required, but it has been vulnerable to DoS attacks.

```
geprod01(config)# no cdp run
```

Targeting broadcast addresses are often used in DoS attacks by using the broadcast address as traffic amplifiers.

```
geprod01(config)# no ip directed-broadcast
```

Proxy-arp'ing is where internal addresses can be arp'ed for on external interfaces. There is no need for any external sources to know about the internal subnet so this is best left disabled

```
geprod01(config) # no ip proxy-arp
```

The router itself can offer a variety of services but when these services are offered, it opens up the router to attacks. Only service that is needed is one for management.

```
geprod01(config)# no service tcp-small-servers
geprod01(config)# no service udp-small-servers
geprod01(config)# no service finger
geprod01(config)# no ip http-server
geprod01(config)# no ip bootp-server
geprod01(config)#
```

Cisco ACL Types

Standard

This provides a very basic method for controlling traffic flow. It can only target addressing information specified in the IP header of any packet and as such can not specifying anything more detailed such as the service as that is contained in the TCP/UDP header. The benefit of this is that it is especially efficient which allows for a much higher throughput even if at the expense of a much finer grained access control. As such, standard ACLs generally do not provide enough flexibility to be useful for any effective filtering.

Extended

Extended ACLs build on standard ACLs by providing filtering rules based on addressing as well as other properties such as service, protocol types and protocol options. This provides a much more thorough and more useful method for filtering traffic. Filtering on addresses alone is generally insufficient.

Reflexive

Extended ALCs also offer a useful feature called 'reflexive' access lists. Reflexive rules utilise a state table for TCP connections which means that it can perform stateful inspection of any TCP connections. This can provide a much better form of access control that is less prone to allowing non-legitimate traffic though. However there is a problem with reflexive access lists and that is that they can be prone to DoS(Denial of Service) attacks. As with any stateful inspection engine, the device must keep the connection in its state table for a certain period of time. Keep in the state table to too short a period and the connection will be dropped prematurely. Keep it in the table for too long then it can be open to DoS attacks as each connection consumes resources and when the device is flooded with connections it can exhaust the resource pool of the router. As such reflexive rules should be used with caution.
Reflexive rules will not be used in this design as state of all connections will be maintained by the stateful firewall and the only device that hangs off the router is the firewall anyway. This limits the need to impose reflexive rules.

ACL Policy

Router filtering policies can generally be broken down into two sections: ingress and egress. Ingress filters aim to stop inbound traffic whilst egress filters attempt to filter outgoing traffic. The reason for the dividing the rules into two sections are due to the way that an ACL router works. Generally routers are not stateful and therefore they do not keep track of whether a packet is a part of an existing session. As such rules need to be written to determine whether any packet is allowed to enter or leave the network on an individual basis. This is opposed to writing a rule on a stateful device which keeps track of which packets may or may not belong to an existing session.

Ingress Filter

Most important rule for the router is to firstly lock down the interfaces. This will prevent any unwanted traffic from being targeted at the router itself.

```
geprod01(config)# access-list 101 deny ip any 83.0.0.0 0.0.0.3 log
router-ext link
```

Second most important rule is to stop any IP spoofing attempts for our public subnet.

```
geprod01(config)# access-list 101 deny ip 223.0.0.0 0.0.0.63 log
```

Private addresses should never appear on the internet as they are strictly for internal use. As such there could be no feasible reason for accepting these networks. Once again these addresses could be used in IP spoofing attempts.

```
geprod01(config)# access-list 101 deny ip 10.0.0.0 0.255.255.255 any
log
```

```
geprod01(config)# access-list 101 deny ip 172.16.0.0 0.15.255.255 any
log
geprod01(config)# access-list 101 deny ip 192.168.0.0 0.0.255.255 any
log
```

Multicast traffic is not used at GIAC Enterprises and there is no foreseeable need for using it either

```
geprod01(config)# access-list 101 deny ip 224.0.0.0 31.255.255.255
any log
```

Broadcast addess for all networks. Targeting broadcast addresses has no legitimate application use for non-local segments. Broadcast addresses can be used in eliciting network information and also used as traffic amplifiers which themselves can be used in DDoS attacks.

```
geprod01(config)# access-list 101 deny ip 255.255.255.255 0.0.0.0 any
log
```

IANA reserved networks should not appear on the Internet, unless recently converted to a public address. Although these addresses don't really pose any particular threat, there have been recent worms which spoof these addresses. Seeing as these addresses are not needed then it can further protect against traffic like this.

Note: Some sequential networks have been omitted for clarities sake and are therefore implied.

```
geprod01(config)# access-list 101 deny ip 0.0.0.0 0.255.255.255 any
log
geprod01(config)# access-list 101 deny ip 1.0.0.0 0.255.255.255 any
log
geprod01(config)# access-list 101 deny ip 2.0.0.0 0.255.255.255 any
log
geprod01(config)# access-list 101 deny ip 5.0.0.0 0.255.255.255 any
log
geprod01(config)# access-list 101 deny ip 7.0.0.0 0.255.255.255 any
log
geprod01(config)# access-list 101 deny ip 23.0.0.0 0.255.255.255 any
log
geprod01(config)# access-list 101 deny ip 27.0.0.0 0.255.255.255 any
log
geprod01(config)# access-list 101 deny ip 31.0.0.0 0.255.255.255 any
log
geprod01(config)# access-list 101 deny ip 36.0.0.0 0.255.255.255 any
log
geprod01(config)# access-list 101 deny ip 37.0.0.0 0.255.255.255 any
log
geprod01(config)# access-list 101 deny ip 39.0.0.0 0.255.255.255 any
log
geprod01(config)# access-list 101 deny ip 41.0.0.0 0.255.255.255 any
log
geprod01(config)# access-list 101 deny ip 42.0.0.0 0.255.255.255 any
log
geprod01(config)# access-list 101 deny ip 58.0.0.0 0.255.255.255 any
log
geprod01(config)# access-list 101 deny ip 59.0.0.0 0.255.255.255 any
log
```

```
geprod01(config)# access-list 101 deny ip 70.0.0.0 0.255.255.255 any
log
geprod01(config)# access-list 101 deny ip 71.0.0.0 0.255.255.255 any
log
.
.
.
geprod01(config)# access-list 101 deny ip 79.0.0.0 0.255.255.255 any
log
geprod01(config)# access-list 101 deny ip 82.0.0.0 0.255.255.255 any
log
.
.
.
geprod01(config)# access-list 101 deny ip 126.0.0.0 0.255.255.255 any
log
geprod01(config)# access-list 101 deny ip 173.0.0.0 0.255.255.255 any
log
.
.
.
geprod01(config)# access-list 101 deny ip 187.0.0.0 0.255.255.255 any
log
geprod01(config)# access-list 101 deny ip 189.0.0.0 0.255.255.255 any
log
geprod01(config)# access-list 101 deny ip 190.0.0.0 0.255.255.255 any
log
geprod01(config)# access-list 101 deny ip 197.0.0.0 0.255.255.255 any
log
geprod01(config)# access-list 101 deny ip 240.0.0.0 0.255.255.255 any
log
.
.
.
geprod01(config)# access-list 101 deny ip 255.0.0.0 0.255.255.255 any
log
```

ICMP is a particularly dangerous protocol to let through our network border primarily because of the amount of functions it can perform. It is used in many illegitimate activities, such as DDoS, covert communication channels, network surveying and information elicitation. However there is one important usage of ICMP for legitimate traffic. That is to allow packets which are larger than what out network can accept. By informing the client that their packets are too large, and that our network is unable to fragment them on their behalf, the client can reduce their packet size thereby allowing an end to end connection to take place. This ICMP type is usually referred to as “ICMP Fragmentation Needed and Don't Fragment was Set” [RFC792]

```
geprod01(config)# access-list 101 allow icmp 223.0.0.0 0.0.0.63 any 3
4 log
geprod01(config)# access-list 101 deny icmp any any log
```

Port 0 is reserved under the IANA so it can’t have any practical use.

```
geprod01(config)# access-list 101 deny ip any any eq 0 log
```

To help prevent any access to any management services all attempts to any port which may be used for this will be dropped.

```
geprod01(config)# access-list 101 deny tcp any any eq 20 log !ftp
geprod01(config)# access-list 101 deny tcp any any eq 21 log !ftp
geprod01(config)# access-list 101 deny tcp any any eq 22 log !ssh
geprod01(config)# access-list 101 deny tcp any any eq 23 log !telnet
geprod01(config)# access-list 101 deny udp any any eq 69 log !tftp
geprod01(config)# access-list 101 deny udp any any eq 111 log
!portmapper
geprod01(config)# access-list 101 deny tcp any any eq 111 log
!portmapper
geprod01(config)# access-list 101 deny udp any any eq 161 log !snmp
geprod01(config)# access-list 101 deny tcp any any eq 512 log !exec
geprod01(config)# access-list 101 deny tcp any any eq 513 log !login
geprod01(config)# access-list 101 deny tcp any any eq 514 log !shell
```

Syslog can contain a lot of information about internal networks as it is the main protocol used in logging information over a network. As such it is a good idea to include an explicit rule to drop this traffic to prevent any leakage.

```
geprod01(config)# access-list 101 deny udp any any eq 514 log !syslog
(leak prevention)
```

Now that the ingress ACL had been created, it needs to be attached to an interface.

```
geprod01(config) # interface ethernet0/0
geprod01(config-if) # ip access-group 101 in
```

Egress Filter

Need to enable management access but only from the management server geprod16.

```
geprod01(config) # access-list 151 permit tcp 10.1.0.162 0.0.0.0
10.1.0.138 0.0.0.0 eq 22 log
geprod01(config) # access-list 151 deny ip any 10.1.0.138 0.0.0.0 log
```

Need an exception for the ICMP Fragmentation needed to allow traffic to flow seamlessly over networks with differing MTUs.

```
geprod01(config)# access-list 151 allow icmp any any 3 4 log
```

Also need an ICMP Host unreachable and Net Unreachable to be allowed through so that our outgoing proxies can tell if a host is not available.

```
geprod01(config) # access-list 151 allow icmp any 223.0.0.2 0.0.0.1 3
log
```

Drop all traffic which doesn't have a valid source address. This useful not only to prevent private addresses from potentially leaking out but also because if the source address isn't publicly routable, it wont go anywhere useful.

```
geprod01(config)# access-list 151 allow ip any 223.0.0.0 0.0.0.63 log
geprod01(config)# access-list 151 deny ip any any log
```

Router Management

We need to enable management and logging for the device. Management of the device will be restricted to the management server geprod16 (10.1.0.162). *Note: admins is a usergroup that defines the users who can authenticate to the router.*

```
access-list 11 permit 10.1.0.162 0.0.0.0
line vty 0
access-class 11 in
login authentication admins
```

All logs will be sent to the logging server geprod15 (10.1.0.161)

```
logging 10.1.0.161
```

Synchronising the time with other servers is important so that logs can be more easily correlated when other events. This task is performed by using NTP(Network Time Protocol) to ensure that the clock of the routers is the same as that of the external NTP servers, geprod13 and geprod14.

```
ntp server 10.1.0.36
ntp server 10.1.0.37
```

Using SSH for management purposes has significant gains over the traditional telnet as it provides an encrypted communications channel.
ip ssh

VPN Policy

The VPN device employed here will be for the suppliers and partners of GIAC Enterprises. One of the most critical aspects of configuring a VPN is to ensure that both parties can perform secure transactions with GIAC Enterprises. Seeing as the VPN runs over the Internet, it is especially important to ensure that the integrity and security are as robust as possible from would be attackers. It is also equally as important to ensure that both parties can't compromise the security of GIAC Enterprises network, either intentionally or unintentionally. By configuring the VPN correctly, both risks will be significantly reduced.

Tunnelling Policy

Split Tunnelling

Split tunnelling is where by a remote user can can access both their local network and the VPNs network at the same time. This is achieved by the VPN assigning the client a list of networks for which the client should use the VPN to tunnel for with the rest of the address space being access via regular channels.
The problem with split tunnelling is that it potentially allows network access to the clients workstation or server whilst the VPN is connected. This allows for a small window of opportunity where by an attacker can also utilise the VPN

tunnel to launch further attacks into the hosts network. However if split tunnelling is disable is prevents this from occurring by effectively isolating the client from it's own network and forcing it to dedicate all network communication via the tunnel.

Security Associations

A security association is an agreement between two parties with regards to as how they will securely communicate[2]. In any SA there are basically three components: security protocol, encryption and hashing. All three components should be carefully selected to ensure that the weaker types have been removed.

- Security Protocol: Encapsulating Security Payload(ESP) combined with Authentication Header(AH) provides the strongest form of security protocol. However because AH is involved it will not be able to pass through any NAT devices. The design was done with this in mind from the start to ensure that the strongest security was available.
- Encryption: Triple DES(3DES) is a high standard for encryption that will remain secure for near future at worst. This has recently replace DES, which is readily brute forcible, as the defacto standard in encryption.
- Hashing: MD5 is one of the strongest hashing functions, and one of the most commonly used. This provides integrity in the form of a one way hashing function.

Tunneling Protocol

The tunnelling protocol is the protocol used to create an end-to-end tunnel by which the two endpoints can communicate. There are several options for this but by far the most secure one is IPSec due to the number of layers and the strength of the individual layers themselves.

VPN Users

There are two distinct groups that will be using the VPN, suppliers and partners. These groups will also form the logical groups that the users will first authenticate to. This group that is authenticated against will also determine most of the properties associated with the VPN tunnel.

Global Properties

User Authentication

After having authenticated to the users respective group, the user will then be prompted to authenticate themselves. The credentials of this authentication will be checked against the ACE server geprod17. This provides and especially secure means of authentication on top of what is already provided by IPSec.

[2] Nortcut, S.Zeltser, L., Winters, S., Frederick, K., Ritchey, R., "Inside Network Perimeter Security", January 2003

Partner Group

Address Pools

Once connected to the VPN the VPN concentrator will dynamically allocate an address to the client. In the partners case it will be:

- 192.168.1.1 – 192.168.1.250.

Tunneled Address List

This is the list of addresses for which the VPN will route connections for:

- 192.168.1.254

Supplier Group

Address Pools

Clients in the suppliers group will be allocated an address in the range of:

- 192.168.0.1 – 192.168.0.250

Tunneled Address List

Addresses for which suppliers connections will be routed are:

- 192.168.0.254

Firewall Policy

As with any firewall, a policies first priority is security and then efficiency. The first few rules should be concerned with locking down the firewall as far as traffic goes followed by the general rules in the order of most used to least used.

All rules should log the action that was taken on that particular rule, such as accept, reject or drop. One exception to this can be rules which are specifically written so that their action is not logged. This can be commonly used to filter out unwanted events which are extremely common such as netbios and bootp.

Actions for all rules should always be either accept or drop and not reject or any other action that elicits a response from the firewall. Firewalls should exist transparently and rejecting connections not only makes the firewall visible but can an attacker can elicit certain information about the firewall from the traffic sent from it.

Finally, the most essential rule of any policy is to deny everything other than that which is specifically permitted. The reasoning for this is that the firewall should let through as little as possible, thereby limiting any opportunity for a compromise or for an attacker to learn anything about the network behind the firewall.

Once the traffic requirements have been defined, IP addresses can be allocated for the NAT'ing of these connections. By using NAT(Network Address Translation) the real IP address and the IP addressing structure of the internal network can be hidden.

External Firewall Policy

NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON
1	geprod01	geprod01	* /	icmp-frag-failed icmp-frag-needed	accept	Log	geprod01
2	geprod16	geprod01	* /	ssh https	accept	Log	geprod01
3	Management-Clients	geprod01	* /	CP_rtm CPMI	accept	Log	geprod01
4	* Any	geprod01	* /	* Any	drop	SnmpTrap	geprod01
5	geprod01 geprod04-pri geprod05-pri	geprod15	* /	syslog snmp-trap	accept	Log	geprod01
6	geprod01 geprod04-pri geprod05-pri	DNS-NTP-Servers	* /	ntp	accept	Log	geprod01
7	geprod01 geprod04-pri	geprod17	* /	securid	accept	Log	geprod01
8	geprod01	* Any	* /	* Any	drop	SnmpTrap	geprod01
9	geprod16	geprod04-pri geprod05-pri	* /	ssh https	accept	Log	geprod01
10	* Any	Web-Servers-NAT	* /	http https	accept	Log	geprod01
11	* Any	geprod12-nat	* /	smtp	accept	Log	geprod01
12	geprod12	internal-10-net	* /	smtp	accept	Log	geprod01
13	* Any	DNS-NTP-Servers-NAT	* /	domain-udp	accept	Log	geprod01
14	DNS-NTP-Servers	internal-10-net	* /	domain-tcp domain-udp	accept	Log	geprod01
15	GE-Partners GE-Suppliers	geprod04-pub	* /	AH IKE ESP	accept	Account	geprod01
16	GE-Suppliers-VPN-Pool	geprod08-nat	* /	ftp	accept	Account	geprod01
17	GE-Partners-VPN-Pool	geprod09-nat	* /	sqlnet2	accept	Account	geprod01
18	Internet-Proxies	internal-10-net	* /	ssh telnet ftp https http	accept	Log	geprod01
19	* Any	* Any	* /	* Any	drop	Log	geprod01

Rule Base Explanation

Rule 1

1	geprod01	geprod01	* /	ICMP icmp-frag-failed ICMP icmp-frag-needed	accept	Log	geprod01

ICMP Fragment Needed messages are needed to ensure that a host sending large packets through a network which can only handle smaller packets, is notified that it needs to reduce its packet size. If this was not permitted then in some situations larger packets would simply be dropped.

Rule 2

2	geprod16	geprod01	* /	TCP ssh TCP https	accept	Log	geprod01

Allow management of the firewall and IPSO by the secured management server.

Rule 3

3	Management-Clients	geprod01	* /	TCP CP_rtm TCP CPMI	accept	Log	geprod01

This allows for GUI management of the firewall from the management clients subnet. Having this rule separate from Rule 2 allows a separation of privilege levels. Admins who have access to the GUI don't necessarily need access to the OS.

Rule 4

4	* Any	geprod01	* /	* Any	drop	SnmpTrap	geprod01

This is the first firewall lock down rule. It will drop any traffic thatis targeted at the firewall. It will also send an alert notifying of this event because there should be no servers attempting to connect to the firewall. As such this could be a notification to a security issue.

Rules 5,6

5	geprod01 geprod04-pri geprod05-pri	geprod15	* /	UDP syslog UDP snmp-trap	accept	Log	geprod01
6	geprod01 geprod04-pri geprod05-pri	DNS-NTP-Servers	* /	ntp	accept	Log	geprod01

Allows servers in the DMZ to log to the logging server and synchronise their time with the NTP servers.

When the firewall or other server encounters an event that is critical enough to notify an operator, the firewall typically will send an SNMP trap, containing the event to another server. When the server receives the trap it can notify the administrator by what ever means possible, such as SMS, paging, or a simple email.

Rule 7

7	geprod01 geprod04-pri	geprod17	* /	securid	accept	Log	geprod01

This allows servers to utilise the ACE server for authentication. Typically this will be not only for internal use, such as SSH to the firewall, but also to authenticate the VPN users.

Rule 8

8	geprod01	* Any	* /	* Any	drop	SnmpTrap	geprod01

All rules that concern the traffic flow of the firewall have been done so it is now appropriate to add the final lockdown rule. This will prevent the firewall from sending out any traffic which may occur under some circumstances.

Rule 9

9	geprod16	geprod04-pri geprod05-pri	* /	TCP ssh TCP https	accept	Log	geprod01

Management rule for the VPN and external router.

Rules 10,11

10	* Any	Web-Servers-NAT	* /	TCP http TCP https	accept	Log	geprod01
11	* Any	geprod12-nat	* /	TCP smtp	accept	Log	geprod01

Allow the web servers and mail server to be accessible to the Internet.

Rule 12

12	geprod12	internal-10-net	* /	TCP smtp	accept	Log	geprod01

This allows the email server to deliver outgoing email to other email servers.

Rule 13,14

13	* Any	DNS-NTP-Servers-NAT	* /	UDP domain-udp	accept	Log	geprod01
14	DNS-NTP-Servers	internal-10-net	* /	TCP domain-tcp UDP domain-udp	accept	Log	geprod01

The DNS servers are permitted to accept DNS requests from anyone as long as they're UDP requests. TCP domain requests are generally zone transfers, that is a request for a copy of all records. This could be used against GIAC Enterprises for further information into the structure of the network. However it may be appropriate at times for the local name server to do zone transfers from other name servers.

Rule 15

15	GE-Partners GE-Suppliers	geprod04-pub	* /	AH UDP IKE ESP	accept	Account	geprod01

Partners and suppliers, with their respective restricted IP addresses will be able to initiate an IPSec session to GIAC Enterprises VPN.

Rules 16,17

16	GE-Suppliers-VPN-Pool	geprod08-nat	* /	TCP ftp	accept	Account	geprod01
17	GE-Partners-VPN-Pool	geprod09-nat	* /	sqlnet2	accept	Account	geprod01

This governs what the partners and suppliers can do once they have successfully connected to the VPN. As stated in the initial solution, supplier would be using FTP to upload new cookie sayings whilst partners were able to access the database via the SQL*Net proxy.

Rule 18

18	Internet-Proxies	internal-10-net	* /	TCP ssh TCP telnet TCP ftp TCP https TCP http	accept	Log	geprod01

Staff will use proxies to browse the web so this rule will govern what ports they are allowed access to. Most likely this will need to be expanded as needs arise to connect to web servers and the likes on non-standard ports.

Rule 19

19	* Any	* Any	* /	* Any	drop	Log	geprod01

The final rule in any firewall policy. Reason for this is that only what is specifically permitted should be allowed thought. That way there is tight control over the flow of traffic in and out of the network.

Verify the Firewall Policy

Verifying a firewall policy is about testing whether our firewall policy protects the resources that it's supposed to. This verification is independent of the applications that may be behind the firewall and the security of those applications.

Audit Plan

To successfully audit a firewall there needs to be a two part process to ensure that all results are as they seem. An audit of the physical security of the firewall and any applications sitting behind the firewall is outside the scope of this section.
By only analysing one portion of the data from, for example, the network scanners result, some critical data may be lost resulting in an invalid analysis. As such we need to perform:

- Firewall verification by means of generating appropriate network traffic and
- Traffic analysis and validation to ensure that the audit's preliminary results are what they seem to be.

Firewall Verification

The verification of the firewall policy can be broken down into two stages[3], verifying that the firewall itself is secure and then verifying that only valid traffic is allowed to the secured resources. The scanners that will be used will provide the preliminary results which can later be concluded with the data analysis.

Traffic Analysis and Validation

For both auditing stages network data needs to be collected by a network sniffer operating behind (or infront depending upon where the scanning is initiated from) the firewall.
The firewall itself will also produce logs of what it believes it has either allowed or dropped. By correlating the network sniffer data and the firewall log data, a conclusive decision can be made as to whether the firewall policy has been validated.

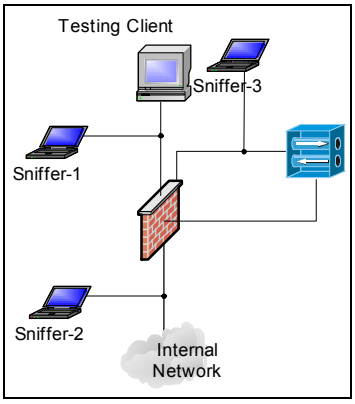
Testing Locations

The firewall audit will be initiated from three main network segments, with a different focus on different areas, depending up the primary function of that subnet

Internet

Logical Location Diagram

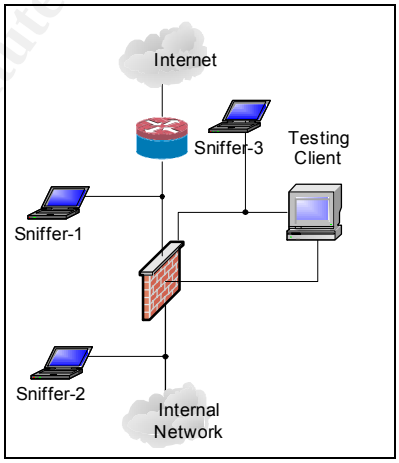
[3] Spitzner, L. "Auditing You Firewall Setup", http://www.spitzner.net/audit.html



The most crucial part of the audit will take place from the Internet facing side. The goals of the scanning here are to ensure that:

- The private network is not visible externally
- Only valid addresses can connect to the VPN
- The firewall is not listening on any accessible ports
  Note: Firewall does not have any publicly routable IP addresses attached to any of its interfaces, only addresses which it will perform NATing for. As such the private addresses used should not be routable and therefore would not generally be reachable over the Internet.
- The firewall itself will not transmit any traffic
- All publicly accessible servers are only accessible via the intended ports
- IP spoofing fails and is logged accordingly
- Fragmented packets are handled properly and not just passed through

VPN DMZ

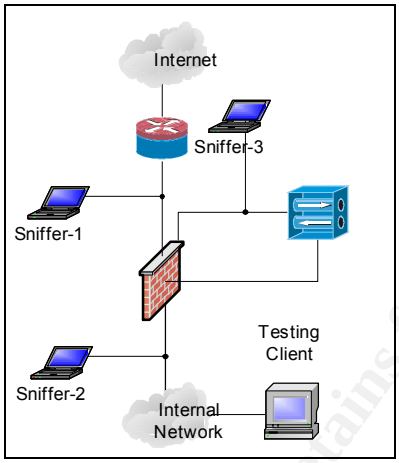


Direct access to the DMZ is not feasible as it would entail replacing the hardware VPN device with that of another device capable of performing the network scans. As such the scan will be conducted from one of the partners sites where by a connection into GIAC Enterprises will be created with a VPN/IPSec tunnel. This should provide an adequate solution.
Once connected to the VPN DMZ the scanning can take place. The main goals of scanning from this particular DMZ are to test that:

- Firewall itself is not listening on any publicly accessible ports.

- Customers and partners can only access the servers they're supposed to.
- The firewall itself will not transmit any traffic
- Private network is not accessable.

Internal Network



This will be limited to a single server as opposed to extensively testing all servers in the network. Although testing all servers would be more comprehensible it is generally infeasible due to time and cost constraints. The server that will be used in the testing (scanning applications will be installed on it) is the primary DNS server, geprod13.
The main goals of the internal scanning is to ensure that:

- The external network or the Internet is only reachable by specific ports thereby preventing direct Internet access.
- Other subnets are not reachable (same subnet will not be reachable due to private VLAN but VLAN testing is outside the scope of this audit).

Cost and Time Estimates

Task	Time
Gathering information required to perform audit	5hrs
External IP addressing information via whois	1hr
DNS records	1hr
GIAC supplied information	1hr
Firewall scanning and data collection (Testing from three separate locations, includes swapping hardware in and out)	3 x 6hrs
Analysis of data	8hrs

Report generation	12hrs

Total Time: 46hs @ $160/hr = $7360

Risk Analysis

Service Outage

The most important and biggest risk is that of an outage. Not only can network scanning place a high load on security devices, it can also cause some to malfunction, resulting in an outage. As such it is critical to ensure that technical staff is prepared to restore the device to its original state, should this occur.
To reduce the risk of devices being overloaded or flooded, network scanning can be performed at a reduced rate. To further reduce this risk, the scanning should be done during the period of least activity which is typically around midnight to 6am.

Information Leakage

Some devices such as switches have problems when their internal information store or state table becomes full. This can cause the devices to malfunction or drop some of their security functions in favour of functionality. Should this happen it is possible that some packets may leak from the network.
The best mitigation for this is an effective policy on the external router. Although the risk and impact of this is fairly low, it should still be considered a potential security exposure, due to the potential contents of the packets.

Customer Data Corruption

During the audit it is possible that customer data may be affected. This would most likely take the form of incomplete, partial transactions that have been terminated prematurely due to the auditing activity.
Data corruption detection strategies should already be in place as data corruption can lead to serious problems if gone undetected. Although many secure protocols offer data integrity as a part of their transport features, end to end integrity is the best solution. For batched information transfers, encrypting and signing with products like PGP provide an excellent assurance. For streaming and more complicated data flows transport protocols like SSL and IPSec are also good solutions.

Loss of Logging Information

Due to the amount of network data generated and the resulting logging data associated with that network data, it is possible that some logging devices will stop logging when their memory or buffers become full. The impact of this is that of a security exposure. Should logging be stopped then it will be more difficult to determine whether there has been any other malicious activity that may have occurred during that time.

All devices that perform logging should have the logging area as empty as possible before the audit. During the audit, logging areas should be passively monitored to ensure that they are operating below capacity.

Audit Scheduling

Scheduling an audit when the network is not in use would be the best time for least disruption to any services. This would be appropriate when temporarily replacing the VPN with the scanner host. However it would not be appropriate to conduct all of the audit under these conditions as it would not adequately reflect how the network regularly operated. Taking into consideration the low risk profile of an audit as such, it would seem reasonable to conduct other sections of the audit in the late afternoon. This avoids peak hour where service availability is most important but also allows the audit to be performed under normal circumstances.

Technical Approach

The audit itself will consist of using two primary tools for network discovery nmap[4] and hping2[5]. Because the applications themselves are not being tested for any vulnerabilities or weaknesses, these tools should be sufficient to generate the required network traffic.
Nmap will be used for network scanning where by an attempt is made to connect to a multiple addresses on multiple ports behind the firewall. If the firewall is configured correctly then no connections should be allowed through which are not intended to be so.
hping2 is a useful tool used to create custom packets. One of the useful features of hping2 for auditing is that it can set the TTL(Time To Live) field on packets which it creates. This is of particular interest when a packet with a TTL field value of 1 reaches the firewall because it should elicit an ICMP Time to Live Exceeded in Transit[6] from the firewall itself. However if the firewall is configured correctly with a secure lockdown rule, then this response should be dropped before it leaves the firewall. This also applies to servers that sit behind the firewall. They too should not be allowed to transmit any ICMP messages with the exception of two as stated in the firewall policy.
Before these tools are run, sniffers will be set up by putting the port, connected to the sniffer, into promiscuous mode, thereby catching all packets that traverse the switch.

Technical Procedure

Check firewall for any open ports. Because the firewall doesn't have any public addresses on any of its interfaces

---

[4] http://www.insecure.org/nmap/
[5] http://www.hping.org/
[6] [RFC792] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, USC/Information Sciences Institute, September 1981.

nmap

nmap will be the primary tool used for scanning the networks as it has excellent capabilities. The scans that will be used will use some of the options described below.

Option	Description	Reason
-sS	SYN stealth port scan (half-open scan). SYN packet is sent and a reply is waited for. No further packets sent.	Detect if port is open and if connection is logged. Because connection is only half open some devices may not log it.
-sU	UDP port scan.	Detect UDP services listening. May produce many false positives.
-sR	RPC portscan. Detects all RPC services listening if it finds the portmapper.	If NMap can find a portmapper than it can scan for RPC services.
-sA	ACK scan. ACK packet is sent expecting a RST in respose.	If RST is received then port is allowed, if nothing is received then port is blocked. Need to check if connection is logged too.
-p <port range>	Determines which ports to scan.	Usually use 1-65535 for a comprehensive scan attempt.
-v	Verbose reporting	Produces more informative output
-P0	Don't ping hosts to see if they're up	Many firewalls will block ICMP echo attempts so not performing this to test for availability is usually a good idea
-n	Don't do DNS resolution	Not interested in DNS lookups as there are fast.

hping2

This tool can be used to craft custom packets that will be used to attempt to get the firewall to send back ICMP messages in response. The options that will be used to create these packets are as such:

Option	Description	Reason
-c <count>	Number of packets to send	Can send multiple packets in case some are lost or dropped.
-2	UDP mode	Will send out UDP packets instead of the default TCP.
-t <ttl>	TTL value to set.	This is the critical option which needs to be carefully set such that the TTL is 1 when it reaches the firewall
-f	Fragment packets	Some firewalls have problems handling fragments.
-x	Fragment more	Fragments packets as much as possible to assist in evasion.
-p	Destination port	Need to set port otherwise packet will get dropped as 0 is an invalid port.
-S	Set SYN flag in TCP packet	Sets SYN flag to initiate a connection. If this is not set stateful firewalls will drop the connection.
-a	Spoof source address	Test if spoofed addresses will be allowed through. Allows the attacker to masquerade as a legitimate host.

Internet

Internal Addresses
Using ports 1-2048 should suffice for this scan as we are already scanning 256 hosts and only ports below 2048 are used for regular services. Using the full port range of 65535 ports would be excessive and would consume a significant amount of resources, both time wise and server wise. As such port scans need to be restricted to meet these needs.
Note: Internal/private addresses will be non-routable over the public network so this scan in reality would only be possible if the scanner was placed close to the network border.

Command: `nmap -sT -sU -sR -v -P0 -p 1-1024 -n 10.1.0.0/24`
Result: All ports filtered.
Sniffers: Nothing
Firewall Logs: All dropped.
Summary: Expected result.

Command: nmap -sA -v –P0 –p 1-1024 –n 10.1.0.0/24
Result: All ports filtered
Sniffers: Nothing
Firewall Logs:

```
14:23:41 drop   10.1.0.137 >eth-s2p1c0 product: VPN-1 & FireWall-1;
src: 10.1.0.1; s_port: 46931; dst: 10.1.0.4; service: ingres-net;
proto: tcp; th_flags: 10;message_info: TCP packet out of state;
```

Summary: Firewall dropped packets as expected, out of state. Reason being is that stateful firewalls expect a SYN before an ACK.

VPN
UDP port 500 is commonly used for IKE, a core protocol associated with IPSec. Only partners and suppliers should be able to connect to this port.

Command: nmap –sT -sU –sR –sA –v –P0 –p 500 223.0.0.1
Result: All ports filtered
Sniffers: Nothing
Firewall Logs: All dropped.

Summary: Should only be able to connect to VPN with correct IP addessess so the firewall succeeded in doing this. Access restrictions to the VPN from the Internet can be confirmed.

Firewall Initiated Traffic

Connections to the web servers should be allowed from all public IP addresses which makes it a good target to test for firewall initiated traffic.

Command: hping –c 1 –t 2 –f –x –p 80 –S 223.0.0.7

Result:

```
winblows:~# hping2 -c 1 -t 2 -p 80 -f -x -S 223.0.0.7
HPING 223.0.0.7 (eth0 223.0.0.7): S set, 40 headers + 0 data bytes
TTL 0 during transit from ip=10.1.0.137 name=UNKNOWN

--- 223.0.0.7 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Sniffer:

```
15:04:54.524493 10.1.0.138.2593 > 223.0.0.7.www: S
1039720052:1039720052(0) win 512 [ttl 1]
15:04:54.529245 10.1.0.137 > 10.1.0.138: icmp: time exceeded in-
transit [tos 0xe0]
```

Firewall Log:

```
 14:53:20 accept 10.1.0.137 >eth-s1p1c0 product: VPN-1 & FireWall-1;
src: 10.1.0.138; s_port: 2688; dst: 223.0.0.7; service: http; proto:
tcp; xlatedst: 10.1.0.34; NAT_rulenum: 9; NAT_addtnl_rulenum: 0;
rule: 19;
```

Summary: It seems that Checkpoint firewall has failed not only to stop the traffic, as the rules suggest, but also to log the traffic that was sent.
SECURITY NOTE: This is an 0-day vulnerability which is currently being co-ordinated with Checkpoint and should be treated as such. See summary for security implications.

IP Address Spoofing

This will attempt to connect to the VPN device using a spoofed address of the management server

Command: hping2 –c 1 –t 2 –f –x –S –p 22 –a 10.1.0.162 223.0.0.1
Result: All ports filtered
Sniffers: Nothing
Firewall Logs:

```
15:06:31 drop   10.1.0.137 >eth-s1p1c0 product: VPN-1 & FireWall-1;
src: 10.1.0.162; s_port: 2747; dst: 223.0.0.1; service: ssh; proto:
tcp; message_info: Local interface address spoofing;
```

Summary: Firewall correctly identified this as a spoofing attempt and dropped it.

Public Servers

Ensure that public servers are only accessible via the intended ports.

Command: nmap –sT -sU –sR –sA –v –P0 –p 1-1024 223.0.0.0/26

Result: Select ports open
Sniffers: Confirmed
Firewall Logs: All valid ports were accepted and others dropped
Summary: Only valid ports were open on all public servers.

VPN DMZ

Firewall
Test for firewall listening on accessible ports

Command: nmap –sT -sU –sR –sA –v –P0 –p 1-65535 10.1.0.129
Result: All ports filtered
Sniffers: Nothing
Firewall Logs: All dropped.
Summary: Firewall dropped everything as expected.

Other Servers
Partners and suppliers should not be able to connect to internal addresses.

Command: nmap –sT –sU –v –P0 –p 1-1024 10.1.0.0/24
Result: All ports filtered
Sniffers: Nothing
Firewall Logs: All dropped.
Summary: Partners cannot connect to any internal private addresses so firewall policy succeeds.

Firewall Initiated Traffic
Connections to the file transfer server should be allowed from all public IP addresses which make it a good target to test for firewall initiated traffic.

Command: hping2 –c 1 –t 3 –f –x –S –p 21 192.168.1.254
Result: ICMP TTL Exceeded received
Sniffers: Confirmed
Firewall Logs: ICMP transmission not logged.
Summary: As above

Internal Network

Internet Connectivity
The target address is a reserved address, but publicly routable and as such should get blocked by the external router. Using a real, non-reserved address would not be ethical because if the test did succeed, it would entail someone else's server on the Internet getting scanned.

Command: nmap –sT –sU –v –P0 –p 1-1024 71.0.0.1
Result: All ports filtered
Sniffers: Detected packets with ports 21, 22, 23, 80, 443.
Firewall Logs: All dropped except ports as above.
Summary: Because it would be unethical to scan a real server on the internet, the outgoing packets had to be dropped by the external router.

However, the fact that the packets reach here is confirmation of our rules only letting out the required packets.

Other Subnets
Other subnets should not be reachable. Servers in the same subnet will not be reachable either as the private VLAN configuration prevents servers communicating directly.

Command: nmap –sT –sU –v –P0 1-1024 10.1.0.0/24
Result: All ports filtered
Sniffers: Nothing
Firewall Logs: All dropped.
Summary: Firewall dropped all packets as expected.

Audit Evaluation

General Comments

The audit was extremely successful. All access restrictions imposed by the policy were confirmed with the audit. Although every possible port from every possible server wasn't scanned, due to impracticality, the more critical resources were scanned to a sufficient degree. It could therefore be said with a high degree of confidence that the firewall policy and design goals stated, are being inforced.

Checkpoint NG Audit Failure

This portion of the audit was a failure, but not due to design or policy decisions. The failure lies in the Checkpoint NG product itself. When the firewall receives a packet, that has a TTL value of 1 and would normally match an accept rule, the firewall returns an ICMP Time to Live Exceeded and without any accompanying log entries. An ICMP message of this type is normally a valid response[7] to receiving a packet with a TTL value of 1. However, a firewalls primary function is to control all traffic entering and exiting the server which it sits on. As such if it has been stated in policies that it should be dropped, then the firewall should promptly do so with an accompanying log entry. A firewall which has problems performing these tasks can pose as a significant security exposure.

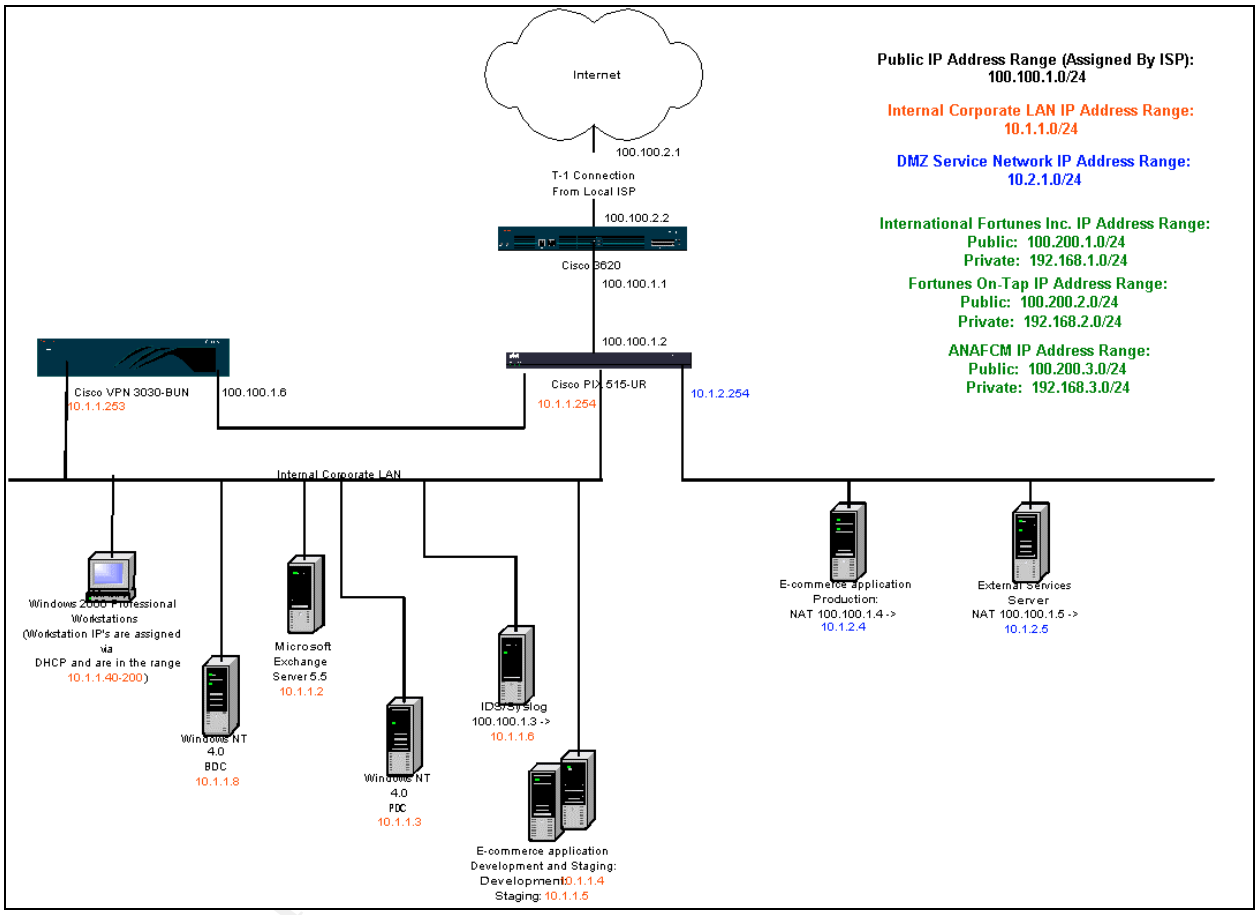
[7] [RFC792] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, USC/Information Sciences Institute, September 1981.

Design Under Fire

The design that has been selected is that of Matt Progue:

GCFW #351 - http://www.giac.org/practical/Matt_Pogue_GCFW.doc

Network Diagram



Attacking the Firewall

Matt has decided to use a Cisco PIX v6.1 as his primary external firewall. Unfortunately for Matt, there are several vulnerabilities[8] associated with the 6.1 release of PIX. The vulnerabilities are as such:

- http://www.securityfocus.com/bid/2347
- http://www.securityfocus.com/bid/6110

The first of the vulnerabilities is a vulnerability in the SSH protocol. Unfortunately this would be extremely difficult to exploit to our advantage as shell code for IOS is not something commonly available nor easy to write.

[8] http://www.cisco.com/warp/public/707/advisory.html#advisories

The second of the vulnerabilities is one of a DoS condition which more readily attacked. This will be out attempt at compromising the firewall even if it is only a DoS attack.

Conditions Required

As the vulnerability states[9]:

> Cisco PIX Firewalls are reported to be prone to a denial of service condition.
>
> The vulnerable condition occurs when telnet/SSH access has been enabled on the firewall for hosts on the internal network. If TCP SYN packets are sent repeatedly to the subnet address, this may cause a denial of service condition.

Matt has also restricted SSH access to the internal network as it is:

```
ssh 10.1.1.0 255.255.255.0 inside
```

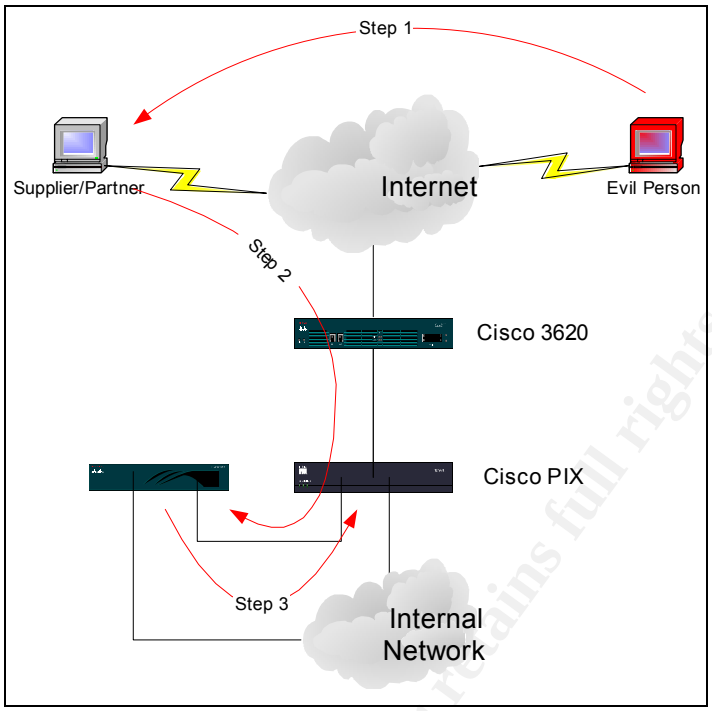
This means that the attack will have to be originated from the internal network.

Getting Inside Access

One of the less guarded communication channels can, ironically, be the VPN. When a partner or supplier connect to Matt Pogue's network, they now have a communications channel to the internal network. Any secure network would not allow connections into the internal network without stringent traffic filtering. Unfortunately for us, connecting directly to the VPN would not be feasible as brute forcing is not an option when dealing with high levels of encryption such as what IPSec offers.
There is a much simpler way and that is going via the back door, which in this case is a supplier or partner who already has access to the VPN tunnel. If the clients machine can be compromised, it can now be used as a launching point for attacks into the internal network.

[9] http://www.securityfocus.com/bid/6110/discussion/

Attack Diagram



Attack Details

Step1:

Evil Person is intent on attacking Matt Pogue's network as such decides to look for ways in. Upon hearing that Partner Company P has partnered with GIAC Enterprises, Evil Person looks up Partner Company P's network block via whois which is then scanned for unsecured hosts. After such a host is found, due to partner company P's poor security, Evil Person installs a rootkit[10] (dependant on clients OS). Once the client's system has been compromised Evil Person can now hide all actions from the user.

Step 2

Evil person now sets up a netcat session to listen for an incoming connection that would be a successful exploit returning a shell:

```
victim# nc -p 45295 -l
```

When Evil Person detects that the user has created a VPN session a snort exploit[11] is sent to not only disable any IDS systems, but the get a login shell. This is one of the reasons why IDS systems can be so dangerous to deploy. They can pose more of a threat than they do reducing threats.

```
victim# p7snort119.sh <VPN tunnel IP>
```

This is a particularly crafty attack as it means that the IP addressing scheme for the remote network doesn't need to be known, just the tunnel endpoint

[10] http://www.antiserver.it/Backdoor-Rootkit/
[11] http://www.securityfocus.com/data/vulnerabilities/exploits/p7snort191.sh

(see script for details). By specifying the VPN tunnel address on the exploit, and upon success, a connection will be opened back to us with a shell.

Step 3

Now that there is a root shell on an internal system, we need to scan for the firewall. Running a stealth SYN scan with OS detection on the local subnet would be a good place to start. Using port 22 is a good choice because the firewall will most likely utilise SSH.

```
nmap -sS -v -p 22 -O -P0 -n 10.1.1.0/24
```

This should net us something like:

```
Initiating SYN Stealth Scan against 10.1.1.254 at 11:07
Adding open port 22/tcp
The SYN Stealth Scan took 0 seconds to scan 1 ports.
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
For OSScan assuming that port 22 is open and port 43276 is closed and
neither are firewalled
Interesting ports on 10.1.1.254:
Port       State       Service
22/tcp     open        ssh
Remote operating system guess: Cisco PIX 515 or 525 running 6.1(4) -
6.2(1)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=3596290 (Good luck!)
IPID Sequence Generation: All zeros
```

Now that the firewall has been discovered, it should be trivial to start our exploit against the PIX firewall:

```
ids-server# hping2 -n -P0 -S -p 22 -v -T Insane -c 10000 10.1.1.254
```

Denial of Service Attack

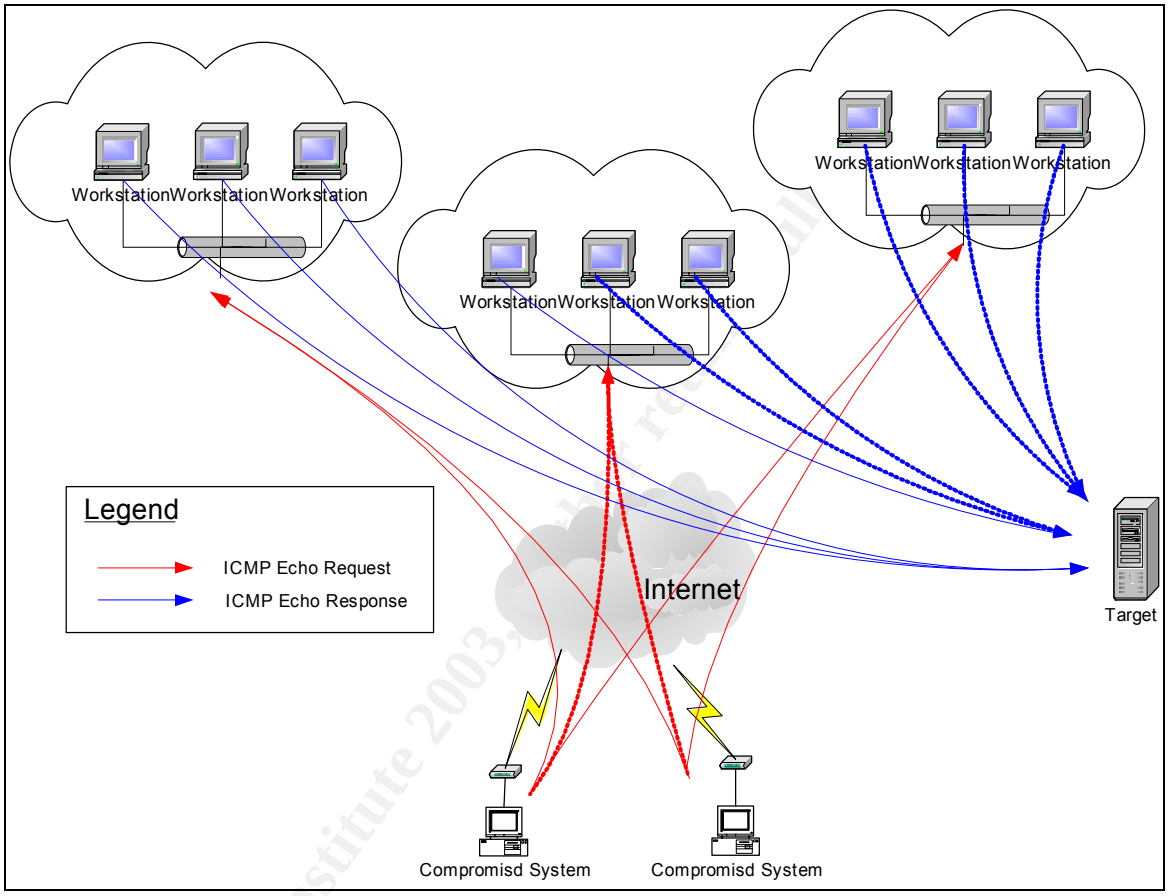
Rather than use the regular script-kiddie style attacks that tools like tfn2k[12] provide there are more efficient methods of generating excessive amounts of traffic. One of these particularly potent methods is by using broadcast amplifiers. A broadcast amplifier is where ICMP Echo Requests, in particular, are sent to the broadcast address of any subnet (all bits in the host portion of a subnet are set to 1). For subnets that are poorly protected and incorrectly configured, this can lead to all hosts on that same subnet responding with an ICMP Echo Reply. The larger the subnet, the more hosts that may respond. One website in particular, netscan.org[13], performs regular scanning for this type of configuration. The list as it currently stands holds almost 14,000 subnets for which this condition holds true.

For a successful DoS ICMP Echo Requests are sent to these broadcast addresses but the source address of these packets is spoofed to be that of the intended target. This allows the responses, that is the ICMP Echo Response packets, to travel back to the target rather than the real host,

[12] http://staff.washington.edu/dittrich/misc/tfn.analysis
[13] http://netscan.org

thereby creating excessive traffic for the target. In this case using any of the public IP addresses registered to the network would suffice as the smallest pipe/link in the network is the one to the upstream provider. Using 50 compromised broadband connections could easily flood a moderately size link.

Network Diagram

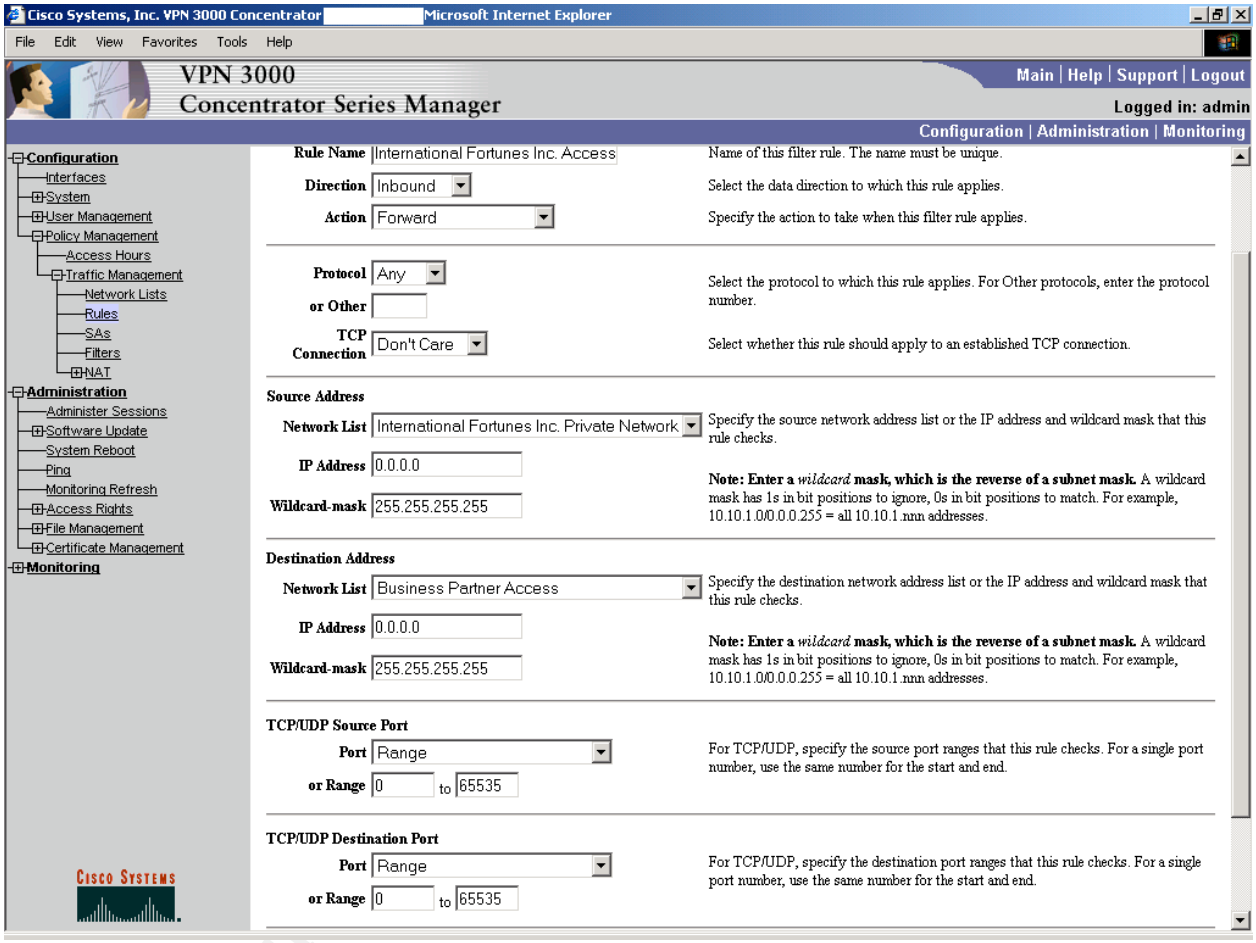


Countermeasures

This can be difficult to prevent against as it requires upstream providers to participate in the solution. For more severe bandwidth style DoS's it may even require a two tier participation in the solution. Either way, there is little that can be done on the clients end of the connection.
Upstream providers or service providers are ultimately the ones who control traffic flow in and out of the network. Most providers will have multiple streams or links from which they connect with to other providers. By analysing which links are causing the saturation, ACLs can be applied to those links that drop the offending traffic. This way, the traffic wont be able to flood the downstream links, preventing the DoS from occurring any more.

Attack Plan

As shown in the initial attack against the firewall, the internal system can be compromised via the VPN connections.
Not only that but there is a configuration error in Matt Pogues VPN setup where by any VPN client can connect to any server on the network, with the exception of a few by which the firewall protects.
The error in the configuration is as such:



Under the *Destination Address* field he has listed the subnet mask to be 255.255.255.255. Cisco use an inverted subnet masking system so this mask therefore translates to a regular subnet mask of 0.0.0.0. Clearly this is a bad policy as the VPN concentrator will now accept any address that is sent over the VPN tunnel. This will now allow us to connect directly to any server that sits off the same subnet as the VPN. It will even allow address spoofing over the VPN tunnel as the same error has been applied to the source address restrictions.
Probing for other servers would also go undetected as the IDS system has already been successfully exploited.
To E-Commerce servers don't look particularly interesting but spoofing any connections to them should be trivial considering that the managers would be on the same LAN. This could be done with arp cache poisoning of the management servers so that their traffic could be redirected to one of the compromised servers thereby preventing them from interfering with out TCP

connections. On top of this the E-Commerce servers are directly accessible via
As such this network could be considered as fully exploited.

Appendix

External Firewall NAT Table

NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE	
1	* Any	web01-nat	* Any	= Original	web01	= Original	geprod01
2	* Any	web02-nat	* Any	= Original	web02	= Original	geprod01
3	* Any	geprod13-nat	* Any	= Original	geprod13	= Original	geprod01
4	geprod13	* Any	* Any	geprod13-nat	= Original	= Original	geprod01
5	* Any	geprod14-nat	* Any	= Original	geprod14	= Original	geprod01
6	geprod14	* Any	* Any	geprod14-nat	= Original	= Original	geprod01
7	* Any	geprod12-nat	* Any	= Original	geprod12	= Original	geprod01
8	geprod12	* Any	* Any	geprod12-nat	= Original	= Original	geprod01
9	geprod06	* Any	* Any	geprod06-nat	= Original	= Original	geprod01
10	geprod07	* Any	* Any	geprod07-nat	= Original	= Original	geprod01
11	GE-Suppliers-VP	geprod08-nat	* Any	= Original	geprod08	= Original	geprod01
12	GE-Partners-VPN	geprod09-nat	* Any	= Original	geprod09-nat	= Original	geprod01

Checkpoint NG on Nokia IPSO Tutorial

Recently Checkpoint have partnered with Nokia to develop a solution that puts Checkpoints Firewall-1/VPN-1 product onto the Nokia appliance. This combines the leading commercial firewall product with a low maintenance server for which sit on.

Initial IPSO Install

Once the IPSO image has been downloaded to a networked workstation, the appliance can FTP the image and install it.

```
################### IPSO Full Installation ####################
You will need to supply the following information:
```

```
        Client IP address/netmask, FTP server IP address and
filename,
        system serial number, and other license information.
This process will DESTROY any extant files and data on your disk.
##################################################################
Continue? (y/n) [n] y
```

Enter ‘y’ to continue with the installation.

```
Motherboard serial number is 12345678.

The chassis serial number can be found on a
sticker on the back of the unit with the letters
S/N in front of the serial number.
Please enter the serial number:
```

Enter the appliances serial number.

```
Please answer the following licensing questions.

Will this node be using IGRP ? [y] n

Will this node be using BGP ? [y] n
```

Enter the following information that will be used to connect a web based client to the Nokia appliance for remote configuration. Note: the addressing stated here can be changed later.

```
1. Install from anonymous FTP server.
2. Install from FTP server with user and password.
Choose an installation method (1-2):  1
Enter IP address of this client (0.0.0.0/24): 10.0.0.1/24
Enter IP address of FTP server (0.0.0.0): 10.0.0.2
Enter IP address of the default gateway (0.0.0.0):
Subnet of client and the gateway does not match.
Enter IP address of this client (10.0.0.1/24):
Enter IP address of FTP server (10.0.0.2):
Enter IP address of the default gateway (0.0.0.0): 10.0.0.2
```

Enter ‘1’

```
Choose an interface from the following list:
1) eth-s1p1
2) eth-s2p1
3) eth-s3p1
4) eth-s4p1
5) eth-s5p1


Enter a number [1-5]:
```

Select speed/duplex settings

```
Would you like to use 100 Mb speed for eth-s1p1? [n] y
Half or full duplex? [h/f] [h] f
```

Enter location of IPSO images

```
Enter path to ipso image  on FTP server [/]:  /nokia/IPSO-images/
Enter ipso image filename on FTP server [ipso.tgz]:

1. Retrieve all valid packages, with no further prompting.
2. Retrieve packages one-by-one, prompting for each.
3. Retrieve no packages.
Enter choice [1-3] [1]:  1

Client IP address = 10.0.0.1/24
Server IP address = 10.0.0.2
Default gateway IP address = 10.0.0.2
Network Interface = eth-s1p1, speed = 100M, full-duplex
Server download path = [/nokia/IPSO-images//]
Package install type = all
Mirror set creation = no

Are these values correct? [y] y
Checking what packages are available on 10.0.0.2.
Hash mark printing on (1048576 bytes/hash mark).
Interactive mode off.
#
The following packages are available:



Building filesystems...
done.
Making initial links...done.
Downloading compressed tarfile(s) from 10.0.0.2.
Hash mark printing on (1048576 bytes/hash mark).
Interactive mode off.
100%  36968 KB    00:00 ETA
(remote-files) Checking validity of image...(no system signature file
found, con
tinuing)...done.
No packages found in /nokia/IPSO-images/, continuing.
Installing image...done.
Image version tag:  IPSO-3.7-BUILD023-06.05.2003-193500-1206.
Checking if bootmgr upgrade is needed...
No need to upgrade bootmgr.
Do you want to upgrade bootmgr anyway? [n]
Installation completed.
```

Installation has now completed. Hit enter to reboot and configure the server.

```
Reset system or hit <Enter> to reboot.
Starting
1   Bootmgr
2   IPSO

Default: 1

Starting bootmgr
Loading boot manager..
Boot manager loaded.
Entering autoboot mode.
Type any character to enter command mode.
```

```
Booting /dev/wd0f:/image/IPSO-3.7-BUILD023-06.05.2003-193500-
1206/kernel
.
.
.
```

When the box comes back up, enter the hostname for the system. In this case it will be geprod01

```
Please choose the host name for this system.  This name will be used
in messages and usually corresponds with one of the network hostnames
for the system.  Note that only letters, numbers, dashes, and dots
(.) are permitted in a hostname.

Hostname? geprod01
```

Set admin/root password

```
Please enter password for user admin:
Please re-enter password for confirmation:
```

Use the web based Voyager option for easier configuration.

```
You can configure your system in two ways:

    1) configure an interface and use our Web-based Voyager via a
remote
       browser
    2) VT100-based Lynx browser

Please enter a choice [ 1-2, q ]: 1
```

Select an interface from the following for configuration:

```
    1) eth-s1p1
    2) eth-s2p1
    3) eth-s3p1
    4) eth-s4p1
    5) eth-s5p1
    6) quit this menu

Enter choice [1-6]: 1
```

Set the IP address and mask length of the interface that will be used for web base configuration.

```
Enter the IP address to be used for eth-s1p1: 10.1.0.137

Enter the masklength: 30
```

Enter ‘n’ to skip entering a default route at this stage.

```
Do you wish to set the default route [ y ] ? n
```

```
This interface is configured as 10 mbs by default.
Do you wish to configure this interface for 100 mbs [ n ] ? y

This interface is configured as half duplex by default.
Do you wish to configure this interface as full duplex [ n ] ? y

You have entered the following parameters for the eth-s1p1 interface:

                IP address: 10.1.0.137
                masklength: 30
                      Speed: 100M
                     Duplex: full

Is this information correct [ y ] ?
```

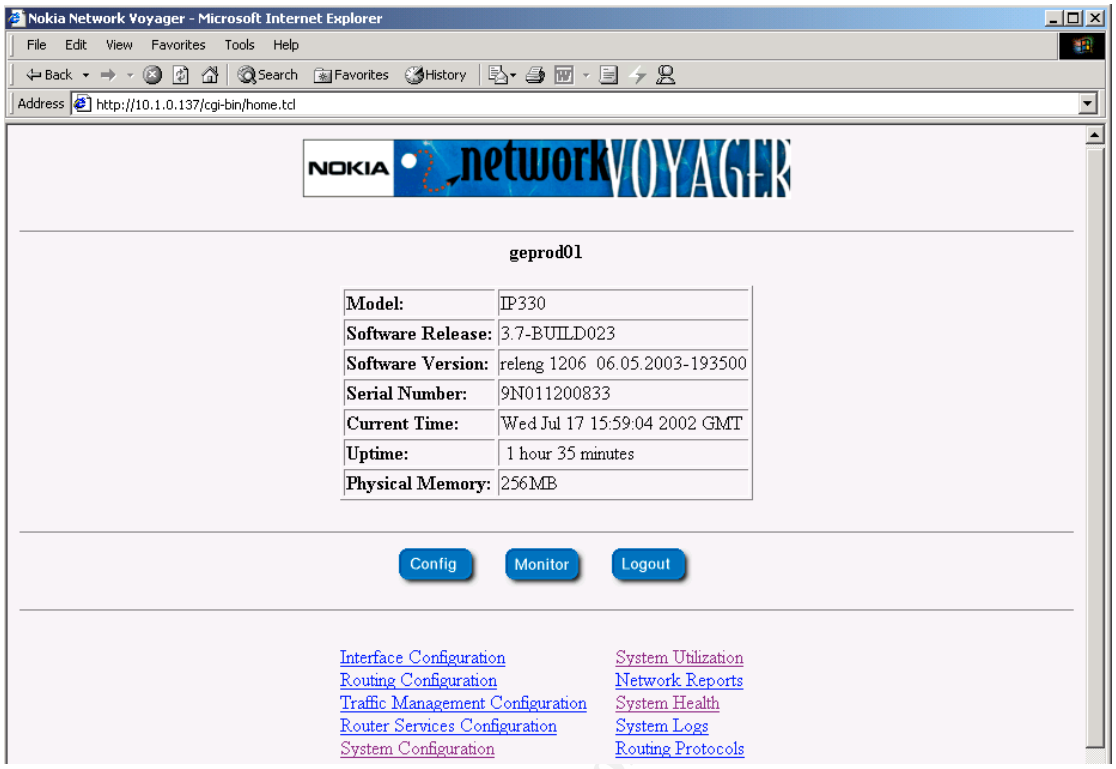
Enter ‘n; to skip VLAN configuration at this stage

```
Do you want to configure Vlan for this interface[ n ] ? n

You may now configure your interfaces with the Web-based Voyager by
typing in the IP address "10.1.0.137" at a remote browser.
```

The server has now been setup such that it is ready for more extensive configuration and package installation via the web based configuration tool Voyager.

Voyager

Voyager Splash Screen



Interfaces

[Interface Configuration -> Interfaces]

To add interfaces, simply click on the link for the interface that needs to be configured and enter in IP address and mask length values. Repeat this for all interfaces.

Install Packages

[System Configuration -> Manage Installed Packages -> FTP and Install Packages]

Enter ftp user details so that the Checkpoint packages can be download. Once all packages have been retrieved, select CP_FP3_IPSO.tgz. This will automatically install all packages needed for Checkpoint FW-1/VPN-1 NG

Configuring Checkpoint

After installing the Checkpoint packages via Voyager, go to the command line and type: ‘cpconfig’

Select 1 if we’re building a self managed firewall.

```
Please select Management type:
------------------------------

(1) Enterprise Primary Management.
```

```
(2) Enterprise Secondary Management.

Enter your selection  (1-2/a-abort) [1]: 1
IP forwarding disabled
Hardening OS Security: IP forwarding will be disabled during boot.
Generating default filter
Default Filter installed
Hardening OS Security: Default Filter will be applied during boot.
This program will guide you through several steps where you
will define your Check Point products configuration.
At any later time, you can reconfigure these parameters by
running cpconfig



Configuring Licenses...
=======================
Host             Expiration  Signature
Features

Note: The recommended way of managing licenses is using SmartUpdate.
cpconfig can be used to manage local licenses only on this machine.

Do you want to add licenses (y/n) [y] ? n
```

Configure the NG administrators

```
Configuring Administrators...
=============================
No Check Point Administrators are currently
defined for this Management Station.

Do you want to add administrators (y/n) [y] ? y
Administrator name: admin
Password:
Verify Password:
Permissions for all Management Clients (Read/[W]rite All, [R]ead Only
All, [C]ustomized) w
        Permission to Manage Administrators ([Y]es, [N]o) y

Administrator admin was added successfully and has
Read/Write Permission for all Management Clients

Add another one (y/n) [n] ?
```

Enter IP address of the GUI

```
Configuring Management Clients...
=================================
Management clients are trusted hosts from which
Administrators are allowed to log on to this Management Station
using Windows/X-Motif GUI.

No Management clients defined

Do you want to add a Management client (y/n) [y] ?
Please enter the list hosts that will be Management clients.
```

```
Enter hostname or IP address, one per line, terminating with CTRL-D
or your EOF
character.
10.1.0.142
^D
Is this correct (y/n) [y] ?
```

Enter random key strokes for entropy

```
Configuring Random Pool...
==========================
You are now asked to perform a short random keystroke session.
The random data collected in this session will be used in
various cryptographic operations.

Please enter random text containing at least six different
characters. You will see the '*' symbol after keystrokes that
are too fast or too similar to preceding keystrokes. These
keystrokes will be ignored.

Please keep typing until you hear the beep and the bar is full.
```

```
Configuring Certificate Authority...
====================================
The system uses an Internal Certificate Authority
to provide Secured Internal Communication (SIC) certificates
for the components in your system.

Note that your components will not be able to communicate
with each other until the Certificate Authority is initialized
and they have their SIC certificate.

Press 'Enter' to initialize the Certificate Authority...
 Internal Certificate Authority created successfully
 Certificate was created successfully
Certificate Authority initialization ended successfully
Check Point product Trial Priod will expire in 15 days.
During this period you are able to use the complete Check Point Product
Suite.
Please obtain a permanent license from Check Point User Center at:
http://www.checkpoint.com/usercenter
```

Enter ‘n’

```
The FQDN (Fully Qualified Domain Name) of this Management Server
is required for proper operation of the Internal Certificate
Authority.

Would you like to define it now (y/n) [y] ? n
```

Enter ‘n’

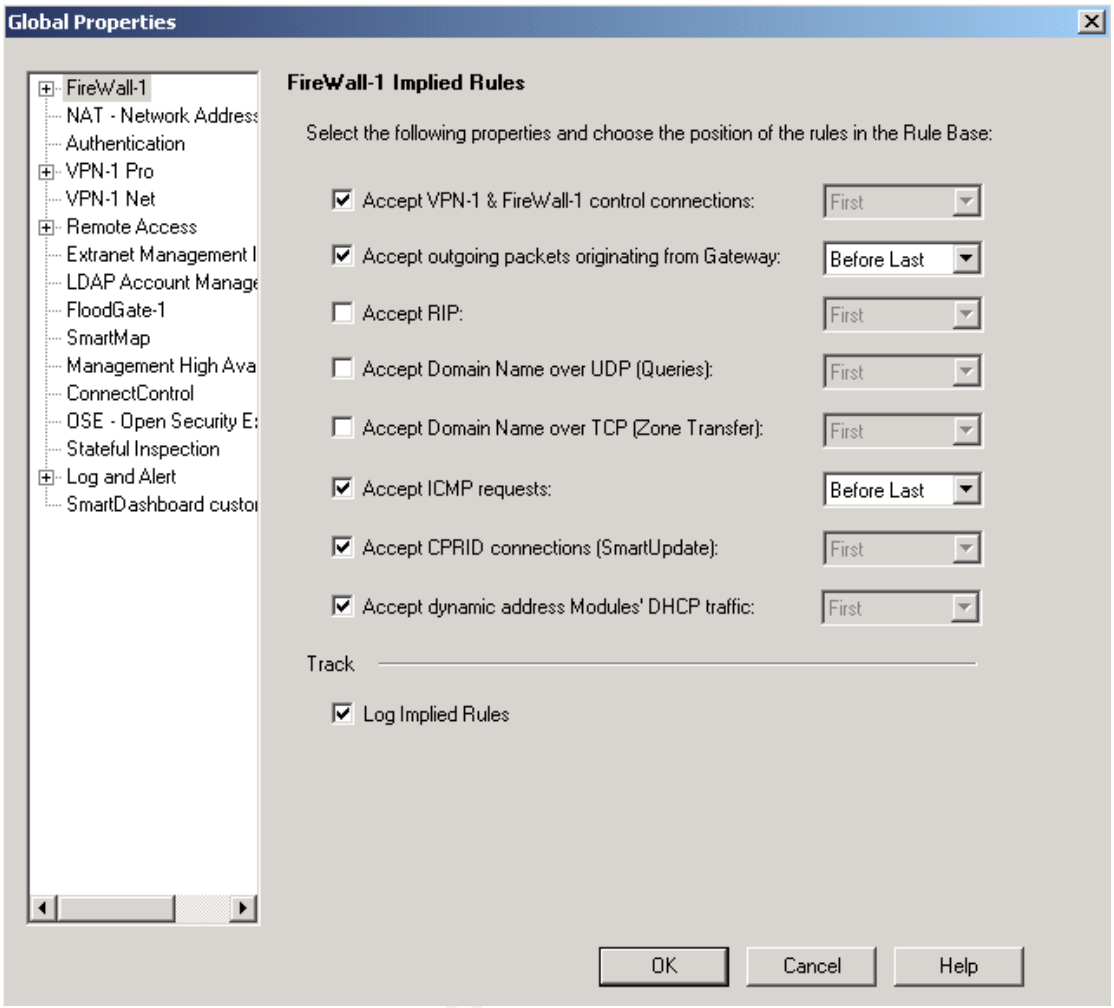
```
Configuring Certificate's Fingerprint...
========================================
The following text is the fingerprint of this Management machine:
KAY EYED NOV HUT SNUG ROOT QUO HELD BAIL AGO EMIT DIME

Do you want to save it to a file? (y/n) [y] ? n

generating GUI-clients INSPECT code
initial_management:
Compiled OK.

Hardening OS Security: Initial policy will be applied
until the first policy is installed


In order to complete the installation
you must reboot the machine.
Do you want to reboot? (y/n) [y] ?y
```

Configuring FW-1/VPN-1

The firewall services should now be up and running so connect to the server with the Checkpoint SMART Dashboard utility.

Upon successfully connecting the firewall must first have it’s default policies removed as they are insecure.

Goto *Policy* and select *Global Properties*



As can be seen there are several options checked by default. These options can cause exposures as they may be forgotten about when writing then rule base. All traffic go to and leaving the firewall should be explicitly defined in the policy and not via implied rules such as these.
The firewall is now ready for policies to be created.