Global Information Assurance Certification Paper

SANS GCFW Practical Assignment

Firewalls, perimeter protection and VPN's
Version 1.7

Monterey, CA February 2002

By
Mark J. Ballister

Security Architecture

Requirements

Define a network security architecture for GIAC Enterprises, an e-business which deals in the online sale of fortune cookie sayings. Your architecture must consider access requirements (and restrictions) for:

- Customers (Companies or individuals that purchase bulk online fortunes)
- Suppliers (Companies that supply GIAC Enterprises with their fortune cookie sayings)
- Partners (International companies that translate and resell fortunes)
- GIAC Enterprises employees located on GIAC Enterprise's internal network
- GIAC Enterprises mobile sales force and teleworkers

You must explicitly define how the business operations of GIAC Enterprises will take place. How will each of the groups listed above connect to or communicate with GIAC Enterprises? How will GIAC Enterprises employees access the outside world? What services, protocols, or applications will be used?

Defining access requirements and the reasoning for those requirements is critical to this assignment. If you have not thought through how this access will take place, you will not be able to adequately define your security policy and ACLs/rulesets later in the paper.

In designing your architecture, you must include the following components:

Filtering Router(s)
Firewall(s)
VPN(s)

Your architecture may also include the following optional components if they are appropriate to your design:

Internal firewalls (Are internal firewalls appropriate for additional layered protection; to segment internal networks…?) Additional secure remote access (Is additional remote access – other than the VPN – required by administrators, salespeople, telecommuters…?). Intrusion detection systems

Security Strategy

Early on in the design process GIAC Enterprise determined the need for security strategies to help implementing our network design. These strategies may seem like a common sense approach, but without this foundation, securing the network can be an erogenous task.

1) Least privilege is the principle of granting the access that is need to perform the task at hand. This is not only used for users, but for anything that is assigned privileges, to include; programs, systems and even administrators.
2) GIAC Enterprise will follow the 'Defense in Depth' approach. Realizing there is no "Silver Bullet", GIAC Enterprise will incorporate many layers of protection from the gateway router to a password policy.
3) Design must be implemented with future expansion in mind. Although cost is a consideration, price should not be the deciding factor in implementing the network design. Growth should be a importance since the cost of upgrading current equipment is much greater then planning for growth in the designs infancy.
4) As the old saying goes, "the chain is only as strong as its weakest link." Through penetration testing and monitoring, GIAC will have to determine it's weakest link and strive to improve.
5) Default deny stance will be applied to all areas. This simply stated, only what you allow and deny everything else.
6) Implement a disaster recovery, BCP plan.
7) Training and security awareness to have universal participation.
8) Construct and enforce a security policy.
9) Keep up with the latest and greatest vulnerabilities/exploits by protect against the SANS top 20. With new vulnerabilities/exploits being exposed regularly the network must be constantly monitored.
10) The needs of the business must be taken into consideration during implementation. GIAC Enterprise will take the most secure avenue unless there is a business need to take a less secure route. These decisions be will handled on a case by case basis, with the final decision made by upper management in writing.

Although the list above is numbered, it is not in order of importance. One could argue for or against why one is more important then the next. The fact is, a breakdown in one area listed, has the potential for an unfavorable result. For example, your network could have the perfect (although unlikely perfect, but for sake of argument) design, but fail to address a natural disaster (BCP). The end result would be similar to becoming victim to a DoS attack.

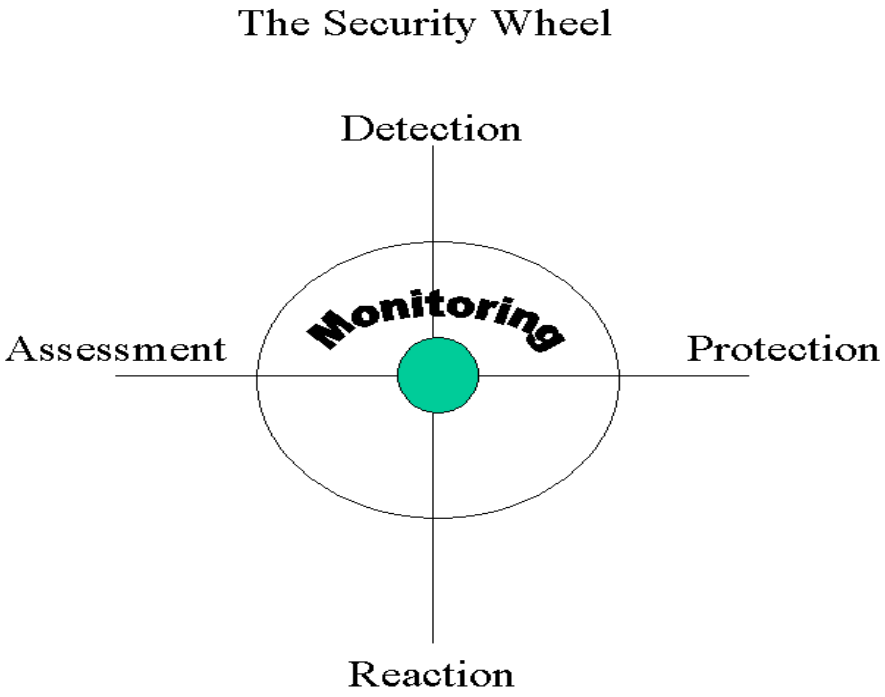


Figure 1.1

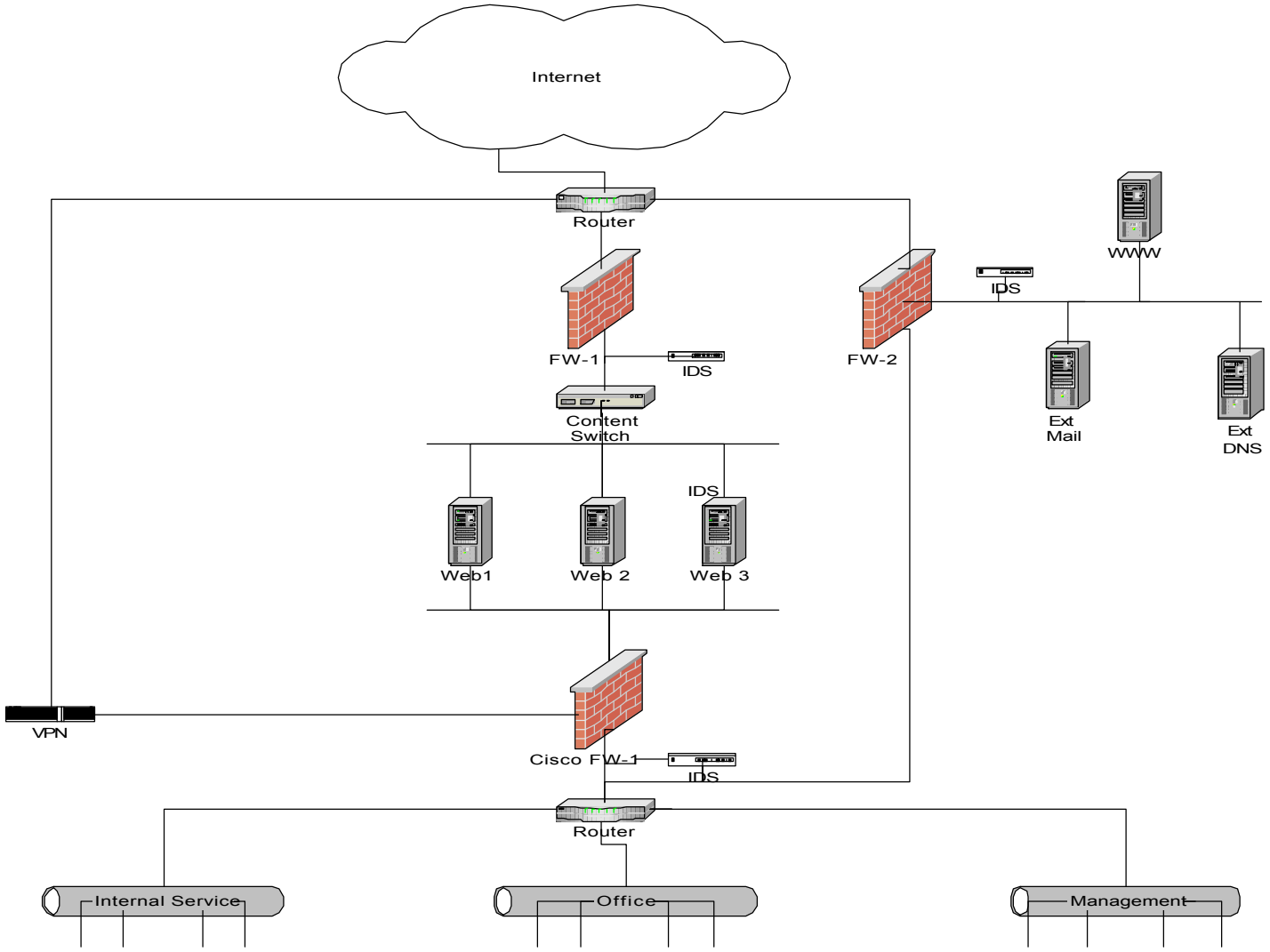
Assessment - Test at least once a year
Protection - Secure
Detection - Monitor
Reaction - Improve

Policies

Like our security strategy, Network Perimeter Security Policies were written early in the design process. The reason is without a solid foundation and policy, how will the organization know when the desired security results have been achieved. Policies have to be reviewed on a regular basis and keep up with the latest needs of the organization and hazards to the network. Any changes to the policy will require management approval prior to the change being implemented. GIAC Enterprise will take the stance of, “deny all, unless explicitly required”. The Network Security policy will address high level issues such as the following:

- Defining Roles
- Permissions
- Rules of Conduct
- Responsibilities

Network Design



Network Components

Border Router

GIAC Enterprise will deploy a Cisco 3661-AC running IOS 12 for their internet gateway. The border router will be configured to allow inbound web traffic to our web farm via policy based routing. The exterior router will be leveraged to also provide our first layer of perimeter security as a screening router. The two areas are attack detection and attack prevention.

Attack detection in the form of detailed logging will be used as early warning and intelligence gathering. All logging from routers will be sent to a centralized sys log server for storage and examination. Good logging will not only help in detecting and defending probes and scans, they can be used to detect configuration error, understanding past attacks and service disruptions. Attack prevention will consist of static packet filtering by using extended access lists. GIAC Enterprise will use a combination of ingress filtering for inbound and egress filtering for outbound traffic to be allowed or denied. This will enable GIAC Enterprise to mitigate some will known attacks such as:

1) IP Address Spoofing for both inbound and outbound traffic.
2) TCP SYN Attack.
3) Land Attack.
4) Smurf Attack.
5) ICMP Message Types and Traceroute
6) DDoS Attack.

Firewall

GIAC Enterprise decided to utilize Check Point Firewall-1, version 4.1, service pack 5, as the core security element. The checkpoint software will reside on two “hardened” Sun Microsystems Neta105 servers. These servers will be running Sun Solaris 2.7 with the most recent patches. Firewall-1 was chosen for Check Point’s stateful and application proxy design. This gives you the best of both worlds, the speed of a stateful inspection and the increased security of a proxy. Since these firewall’s are placed closest to the internet gateway, it will be handling the second largest amount of traffic (second only to the border router). Two firewalls were chosen at the border for both load balancing and network segregation. All web traffic will be routed to one firewall, while all corporate traffic will be behind the other. The two firewall-1 design can also be further leveraged in load balancing by loading StoneBeat and configuring active-to-active for fail-over redundancy. The third will be a Cisco Pix firewall placed in front of the corporate network and behind the web farm. The Pix firewall was chosen to further leverage our defense in depth strategy, by implementing multiple technologies in the network. This firewall will also received the VPN traffic coming into the corporate network.

Similar to our border router the firewall provides both attack detection and attack prevention. Attack prevention is accomplished by logging and programmed alerts (in the form of paging or email). Firewall-1 also has a IDS (Intrusion Detection System) "like" feature known as MAD (Malicious Activity Detection). This feature detects abnormal traffic patterns and can (if configured to do so) alert when detected. Attack prevention is a combination of access control lists and security policies. These will allow GIAC Enterprise to defend against various DoS, DDoS and SYN flood attacks, as well as known vulnerabilities from unnecessary services and unused ports not specifically denied.

VPN

Even though the Check point Firewall-1 does provide an all in one firewall and Virtual Private Network (VPN) solution, GIAC Enterprises decided on a separate hardware solution. The hardware chosen is Cisco 3030 VPN concentrator. This particular device will fit our current need and can be upgraded to the 3060 for future requirements. Some of the key features for deciding on Cisco's 3030 VPN:

- Split tunneling.
- 50 Mbps maximum performance (100 Mbps with upgrade).
- Up to 1500 simultaneous sessions (5000 simultaneous sessions with upgrade).
- Multiple operating systems for VPN client.
- Redundant configuration available.

For a tunneling mechanism, IPsec was chosen for its versatility and flexibility. IPsec is a suite of protocols wrapped into one, including Authentication Header (AH port 50) and Encapsulation Security Payload (ESP port 51), and the use of cryptographic key management including Internet Security Association and Key Management Protocol (ISAKMP port UDP/500) and the Internet Key Exchange protocol (IKE). Because GIAC Enterprise will be using private non-routable IP addresses, AH will not be activated.

Switch – web farm load balancing

To insure performance, transaction integrity and continuos availability, the Cisco CSS 11000 content series switch with Web Network Services software will be employed in front of the web farm. To protect e-business transactions, SSL (Secure Socket Layer) will be used on all connections. Securing the transaction comes with a price, SSL imposes significant processing overhead on a server. Cisco has address this issue by using a front-end SSL accelerator device for load balancing. The switch cache and reuse SSL sessions, effectively offloading the excessive overhead from web server by negotiating the SSL handshake. This is accomplished by one of the following solutions:

1) Authenticated transactions based on HTTP connections.
2) Transactions encrypted end to end with SSL connections.

3) Hybrid transactions that combine both of the above types of connections.

This device can be further leveraged with built security software named FlowWall. As the name suggests FlowWall provides filtering of content requests. This is done by comparing traffic with signatures of known DoS attacks and malicious connections. While not fool proof it adds one more layer of security without hindering performance.

Web Servers

Realizing the main source of revenue and the related security risks involved in e-commerce, GIAC Enterprise will take every effort to secure their web farm. GIAC will use four Sun Netra T1AC200 Servers with Sun Solaris 2.7. The Sun boxes will be hardened to only allow necessary applications and services. Apache web server 2.0 software, using the http (TCP port 80) and https (TCP port 443) protocols. To reduce some confusion the https protocol may cause (i.e. https://www.giacfortune.com), customers will enter only non-sensitive data on the http site. Then they will be redirected to the https for sensitive information input. To enable the 128-bit SSL, VeriSign Global Serve ID will be obtained.

IDS

In an effort to ensure the network is continually monitored for potential security violations, a combination of network (NIDS) and host (HIDS) based intrusion detection systems (IDS) will be deployed. In most cases it is not a case of if your network will be compromised, it is a question of when. To make sure GIAC Enterprise can identify intrusions NIDS will be placed in the following locations:

- Internet access point
- Behind the firewall in the service network
- Behind the VPN
- In front of the switch to web farm
- On the internal network

HIDS agents will be placed on the following servers:

- The firewall
- The mail server
- The DNS server
- Servers in the web farm

Access

Customer Access Method

Customers will need to access our web sites and securely purchase fortune cookie sayings. Theoretically, anyone can access the web site from anywhere in the world.

As mentioned above to protect customer information, all transactions will be conducted via SSL. GIAC Enterprise clientele will be uniquely identified by user ID and password. GIAC will email the user their username and temporary password to the email address the user provides on the new user set up page. The user will then authenticate using their username and temporary password. After authenticated the user will be prompted to change their password to meet the password security policy. Once the order is placed the information is passed to a backend database for accounting and request completion.

Partners Access Method

Once the sayings are gathered, they will need to be distributed to partners for reselling. Initially, to mitigate the risk of exposing critical data by allowing partners in our network. GIAC Enterprise was going to have partners access the web site to place orders. This was considered a greater risk then by limiting network access using a VPN. Partners will authenticate with two party authentication using SecureID provided by GIAC. By all partners having a unique login name we are able to restrict their access by ACL's (Access Control Lists) on both the internal router (since the packets will be decrypted when passing the inside router) and the VPN gateway.

Suppliers Access Method

Suppliers will be a small group of authors and companies that will require limited access to the GIAC network. One solution is to require the suppliers to attain a VPN Gateway, but this was quickly determined unreasonable. The decision was to provide access via host to gateway VPN. Similar to the access method of GIAC's partners, suppliers will have to authentic with a SecureID that we provide and access will be restricted by ACL's. Once logged on the network, they will be able to launch an application (backend database) to submit their ideas.

GIAC Employee Access Method

All internal users will have a limited access to the Internet, internal DNS, and mail server. Internet access will be monitored and controlled by Services Strategies Inc., Internet Access Management. Filters will be configured to block certain web pages, as well as keyword matching for topics inappropriate in a professional environment, to include but not limited to: pornography, hate sites and hacker site. All web surfing will be backed by an acceptable use policy. All user access will be based on the principle of least privilege.

As specific needs arise, GIAC employees will be allowed to remotely access the network using remote access VPN. Users will be required to use a company provided asset with a pre-configured router for additional security. ACL's will be maintained to restrict what access the remote user has on a case by case basis.

Subnets

Service Network

The service network will use legal IP addresses and house our publicly available servers, including our web server, external DNS server and external mail server. The service network will be the only segment accepting stateful in-bound traffic from the internet. As mentioned earlier all servers will be OS hardened according to best practice. By utilizing the Cisco CSS 11000 switch we can provide high-speed web content delivery. This also gives us the ability to expand via an eight full-duplex fast Ethernet ports. GIAC Enterprise decision for separating the

Internal Network

The internal network will use private address and house internal servers (internal mail and DNS), workstations, printers, databases and the fortune cookie sayings application. The corporate network will be divided into three subnets; Internal Services, Office, and Management.

IP Addressing

Legal Address

To meet our current and future needs, GIAC Enterprise will obtain one Class C Block of IP addresses. The net block is 206.123.224.0/24, with this block we have the expandability of up to 254 different hosts.

Private Address

For GIAC Enterprise's private address we refer to RFC 1918 for internal IP schema. To make certain GIAC has sufficient address space for future expansion, the private address will be a class B. Our net block will be 172.16.0.0/12 and then subnetting into multiple class B networks for separation.

Security Policy

Requirements

Based on the security architecture that you defined in Assignment 1, provide a security policy for the following three components:

Border Router(s)
Primary Firewall(s)

VPN(s)

You may optionally include policy for other devices (i.e., - internal firewalls).

By "policy" we mean the specific set of ACLs, ruleset, or IPSec policy for that device – not corporate or organizational policy (though note that organizational policy may dictate the specific ACLs or ruleset in effect).

For each component, be sure to consider the access requirements for customers, suppliers, partners, remote users, and internal users that you defined in Assignment 1. The policies you define must accurately reflect those business needs as well as appropriate security considerations.

You must include the complete policy (meaning explicit ACLs, Ruleset, IPSec policy, etc.) in your paper. It is not enough to simply state "I would include ingress and egress filtering…" The policies may be included in an Appendix if doing so will help the "flow" of the paper (clearly state if this is the case).

For each rule in all policies, you must include the general purpose of the rule and why it is important.

You must also include a discussion of the order of the rules, and why order is (or is not) important.

For one of the three security policies defined above, you must incorporate a tutorial on how to implement the policy. Clearly separate and label your tutorial. Use screen shots, network traffic traces, firewall log information, and/or URLs to find further information to clarify your instructions. Be certain to include a general explanation of the syntax or format of the ACL, filter, or rule for your device, as well as a general explanation of how to apply a given ACL, filter, or rule.

Network Security

Network security can be broken down into four basic layers:

- Physical Integrity - Physical/Electronic Access.
- Core static configurations - Administrative access and software updates.
- Dynamic Configuration – Routing and management protocols.
- Network Traffic – Access to the network.

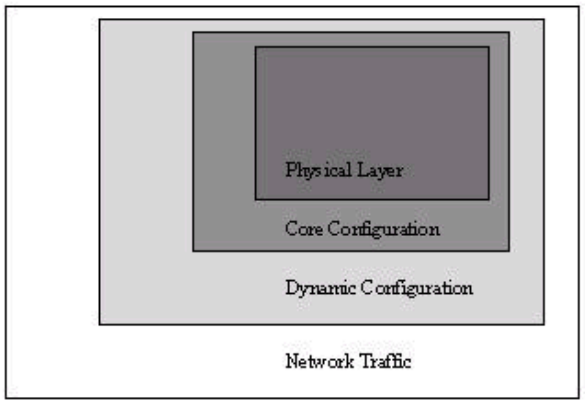


Figure 2.1

Figure 2.1 is a graphical representation of how the outer layer is codependent on the layer it is inside. For an example, if an attacker gains physical access to the router or firewall, no matter how well the boxes are configured it can be compromised.

Configuration

Router

A router's primary function is to route packets. Nonetheless, it is a major player in an organization over all security. Because the primary purpose of a router is routing and not a acting as a firewall, to leverage the device for security it should be used to block (static filtering) not manage connections (stateful filtering). As mentioned earlier when configuring GIAC Enterprise will only permit services and protocols that are needed and deny everything else.

With the above in mind GIAC will turn off all unneeded servers on the router. This is done for a few other reasons besides the obvious risk of an attacker. By having only the services that are required, the router will have more memory and processor slots available for services that are required. The full router configuration is listed in Appendix C.

First we are going to set the password protection schema to use type 5 or MD5. This will protect the password from being viewed in plain text from stray eyes passing by.

```
Border1(config)# service password-encryption
Border1(config)# enable secret mark$~34%rt
Border1(config)# no enable password
```

To avoid DNS spoofing we define the domain name and server for DNS lookups by the router.

```
Border1(config)# domain-name giacenterprise.com
Border1(config)# ip name-server 206.123.224.100
```

Login banners are important especially to law enforcement is involved to prosecute a trespasser. Wording is key, if you do not specifically state unauthorized access is prohibited it will be very difficult to take legal action.

```
Border1(config)# banner exec <control c>
Border Router for GIAC Enterprise <control c>
Border1(config)# banner login <control c>
All GIAC Enterprise Communications, Information Systems and related equipment are
for the interchange, transmission, processing, and storage of GIAC Enterprise
information exclusively. Unauthorized access or configuration to this device will be
subject to prosecution or other criminal punishment. <control c>
```

There is a lot of controversy whether or not the company name should be on the banner page. Some say it should not because it will announce the owner of the device (i.e. GIAC Enterprise). Others say by specifically stating the company name, if the system was compromised it may be easier to prosecute. I choose to have the company name since the IP address is public knowledge.

Shutting down unneeded services globally on the router:

CDP (Cisco Discovery Protocol) is a protocol specific to Cisco used for identification purposes.

```
Border1(config)# no cdp run
```

Small services that have been abused in the past include; echo, chargen and discard and daytime.

```
Border1(config)# no service tcp-small-servers
Border1(config)# no service udp-small-servers
```

Bootp and finger services if enabled can provide an attacker user login information and a copy of the ISO from the router.

```
Border1(config)# no service finger
Border1(config)# no ip bootp server
```

Http and snmp are remote administration services to manage the router. With the recent snmp vulnerability it is far to risky to leave enabled.

```
Border1(config)# no ip http server
Border1(config)# no snmp-server enable traps
Border1(config)# no snmp-system-shutdown
Border1(config)# no snmp-server trap-auth
Border1(config)# no snmp
```

Source routing is used for routing individual packets to a specific destination. The router is also setup to forward a classless IP to the best possible route. Although these can be a useful tools, there are far too many exploits.

```
Border1(config)# no ip source-route
Border1(config)# no ip classless
```

Configuration auto-loading has a feature that allows you to load startup configurations from the network or local memory. Once again if it is not on a fully trusted network, this feature should be disabled.

```
Border1(config)# no boot network
Border1(config)# no service config
```

Other services to be disabled.

```
Border1(config)# no ip subnet-zero
Border1(config)# no ip unreachable
Border1(config)# no service pad
Border1(config)# no identd
Border1(config)# no logging console
```

Shutting down unneeded services at interface on the router:

The Cisco 3600 GIAC is using is equipped with four interfaces but only three are being utilized. It is a good practice to disable all unused interfaces.

```
Border1(config)# interface eth0/3
Border1(config-if)# shutdown
```

Other services to be disabled on all interfaces.

```
Border1(config-if)# no ip redirects
Border1(config-if)# no ip proxy-arp
Border1(config-if)# no cdp enable
Border1(config-if)# ntp disable
Border1(config-if)# no ip directed-broadcast
```

Logging:

Logging will be turned on for help in detecting and defending probes and scans. It can also be used to detect configuration error, understanding past attacks and service disruptions.

```
Border1(config)# logging buffered 10000
Border1(config)# logging trap debugging
Border1(config)# logging 172.16.224.161
Border1(config)# service timestamp debug datetime localtime show timezone
msec
```

ACL

Access Control Lists (ACL) are used for packet filtering on the Cisco router. This is accomplished by two types of access lists, standard and extended. Standard ACL's has the limitations of only allowing source IP address filtering. For standard ACL's the list numbers are between 1-99. Extended ACL's can be applied much more granular. With extended ACL's you are able to permit or deny based on protocol, source or destination IP address, source or destination TCP/UDP ports or ICMP or IGMP message types. The list numbering for extended ACL's are 100-199.

Ingress and Egress Filtering

To further protect the GIAC Enterprise network, we will apply ingress and egress filtering on the border router. Egress filtering in a nutshell is being a good Internet neighbor, by not allowing any packets to be sent out that is not legally assigned to us. Not only is this being a good neighbor, without egress filtering a lawsuit can be brought against GIAC if the site was involved in a DDoS attack against another site. Ingress filtering conversely is protecting your network against IP packets with an untrusted source address. This can mitigate such concerns as: DDoS, vulnerable services and spoofed addresses.

```
Border1# config terminal
Border1(config)# !Outside interface
Border1(config)# Interface Ethernet0/0
Border1(config-if)# ip address 206.123.224.5 255.255.255.252
Border1(config-if)# ip access-group 130 in

Border1# config terminal
Border1(config)# !Inside interface
Border1(config)# Interface Ethernet0/1
Border1(config-if)# ip address 206.123.224.18 255.255.255.240
Border1(config-if)# ip access-group 131 in

Border1# config terminal
Border1(config)# !Inside interface
```

```
Border1(config)# Interface Ethernet0/2
Border1(config-if)# ip address 206.123.224.34 255.255.255.240
Border1(config-if)# ip access-group 141 in

Border1# config terminal
Border1(config)# !Inside interface
Border1(config)# Interface Ethernet0/3
Border1(config-if)# ip address 206.123.224.66 255.255.255.240
Border1(config-if)# ip access-group 151 in

Border1(config)# no access-list 130
Border1(config)# !For incoming to Corporate Network from Outside
Border1(config)# !Prevent anti-spoofing ref: RFC 1918, RFC 2827, RFC 3013
Border1(config)# !and IANA Reserved
```

GIAC Enterprise will explicitly deny all inbound traffic that uses private address space.

```
Border1(config)# access-list 130 !IANA Private Address Space
Border1(config)# access-list 130 deny ip 10.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 172.16.0.0 0.15.255.255 any log
Border1(config)# access-list 130 deny ip 192.168.0.0 0.0.255.255 any log

Border1(config)# access-list 130 !GIAC Enterprise Routable Address Space
Border1(config)# access-list 130 deny ip 206.123.224.0 0.0.0.31 any log
```

Although the last line will in the ACL will be, “ip deny any any” we decided to specifically deny all address space reserved by IANA. Listing all reserved addresses will be reviewed to insure the router is processing optimally.

```
Border1(config)# !IANA Reserved Address Space
Border1(config)# access-list 130 deny ip host 0.0.0.0 any log
Border1(config)# access-list 130 deny ip 0.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 1.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 2.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 5.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 7.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 23.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 27.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 31.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 36.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 37.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 39.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 41.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 42.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 58.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 59.0.0.0 0.255.255.255 any log
```

```
Border1(config)# access-list 130 deny ip 60.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 69.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 70.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 71.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 72.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 73.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 74.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 75.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 76.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 77.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 78.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 79.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 82.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 83.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 84.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 85.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 86.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 87.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 88.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 89.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 90.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 91.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 82.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 93.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 94.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 95.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 96.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 97.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 98.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 99.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 100.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 101.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 102.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 103.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 104.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 105.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 106.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 107.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 108.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 109.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 110.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 111.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 112.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 113.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 114.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 115.0.0.0 0.255.255.255 any log
```

```
Border1(config)# access-list 130 deny ip 116.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 117.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 118.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 119.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 120.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 121.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 122.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 123.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 124.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 125.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 126.0.0.0 0.255.255.255 any log
Border1(config)# access-list 130 deny ip 169.254.0.0 0.0.255.255 any log
Border1(config)# access-list 130 deny ip 192.0.2.0 0.0.0.255 any log
Border1(config)# access-list 130 deny ip 197.0.0.0 0.0.255.255 any log

Border1(config)# !Exploit Protection

Border1(config)# !Telnet from Internet
Border1(config)# access-list 130 deny tcp any any range ftp telnet log

Border1(config)# !ICMP Message and Traceroute
Border1(config)# access-list 130 deny icmp any any echo log
Border1(config)# access-list 130 deny icmp any any redirect log
Border1(config)# access-list 130 deny icmp any any mask-request log
Border1(config)# access-list 130 deny icmp any any time-exceeded
Border1(config)# access-list 130 deny udp any any range 33400 34400 log

Border1(config)# !TCP SYN Attack
Border1(config)# access-list 130 permit tcp any 206.123.224.0 0.255.255.255 establish
```

A Land attack is a possible DoS, where an IP packet is sent to the router with the same IP address and port for the source and destination address.

```
Border1(config)# !Land Attack
Border1(config)# access-list 130 deny ip host 206.123.224.5 host 206.123.224.5 log
```

A Smurf Attack is leveraging a router that is configured to forward broadcast requests. This is done by spoofing the victims address and flooding ICMP Echo packets to a subnet's broadcast address. By allowing the request to be forwarded the victim will be inundated with request. By blocking the broadcast addresses traffic you can prevent your router from being used in an attack.

```
Border1(config)# !Smurf Attack
Border1(config)# access-list 130 deny ip any host 206.123.224.255 log
Border1(config)# access-list 130 deny ip any host 206.123.224.0 log
```

```
Border1(config)# !Buffer Overflow
Border1(config)# access-list 130 deny tcp any any 111 log
Border1(config)# access-list 130 deny tcp any any 551 log

Border1(config)# !Multicast Addresses
Border1(config)# access-list 130 deny ip 224.0.0.0 31.255.255.255 any log

Border1(config)# !SNMP Traffic
Border1(config)# access-list 130 deny udp any any range snmp snmptrap log

Border1(config)# !DHCP Auto Config
Border1(config)# access-list 130 deny ip 169.254.0.0 0.0.255.255 any log
Border1(config)# access-list 130 deny ip 192.0.2.0 0.0.0.255 any log

Border1(config)# !Loopback Address
Border1(config)# access-list 130 deny ip 127.0.0.0 0.255.255.255 any log

Border1(config)# !Allowing web traffic to web servers on port 80 and 443.
Border1(config)# access-list 130 permit tcp any 206.123.224.114 0.0.0.0 eq http
Border1(config)# access-list 130 permit tcp any 206.123.224.114 0.0.0.0 eq 443

Border1(config)# !Netbios
Border1(config)# access-list 130 deny tcp any any range 135 139 log
Border1(config)# access-list 130 deny tcp any any eq 445 log
Border1(config)# access-list 130 deny udp any any eq 135 log
Border1(config)# access-list 130 deny udp any any range 137 138 log
Border1(config)# access-list 130 deny udp any any eq 445 log

Border1(config)# !Other known Trojan
Border1(config)# access-list 130 deny udp any eq 34555 log
Border1(config)# access-list 130 deny udp any eq 27573 log
Border1(config)# access-list 130 deny udp any eq 27444 log
Border1(config)# access-list 130 deny udp any eq 27374 log

End the ACL by denying all packets not explicitly prohibited.
Border1(config)# access-list 130 deny any any log
```

All traffic leaving the corporate network will have to contain a valid IP address assigned to GIAC. All other traffic will be denied.

```
Border1(config)# no access-list 131
Border1(config)# !For outgoing from Corporate network to Outside for Border1(config)#
!Anti Spoofing - Egress
Border1(config)# access-list 131 permit ip 206.123.224.0 0.0.0.31 any
Border1(config)# access-list 131 deny ip any any
```

Allow ports 50, 51 and 500 for VPN traffic to the VPN concentrator.

```
Border1(config)# no access-list 141
Border1(config)# access-list 141 permit 50 any host 206.123.224.35 log
Border1(config)# access-list 141 permit 51 any host 206.123.224.35 log
Border1(config)# access-list 141 permit 500 any host 206.123.224.35 log
Border1(config)# access-list 141 deny ip any any log

Border1(config)# no access-list 151
Border1(config)# access-list 151 permit tcp host 206.123.224.99 eq http
Border1(config)# access-list 151 permit tcp host 206.123.224.99 eq 443
Border1(config)# access-list 151 permit tcp host 206.123.224.100 eq 53
Border1(config)# access-list 151 permit tcp host 206.123.224.101 eq 25
Border1(config)# access-list 151 deny any any log
```

Firewall

The purpose of GIAC Enterprise firewalls, is to defend the network against exploits and malicious code. After the majority of the "noise" is removed by the router, the firewalls controls the access to the separate subnets. We will filter out some of the same traffic as the border router such as anti-spoofing. GIAC Enterprise firewall security policy was written to complement the network security policy. This will be accomplished by referencing SANS Institutes, "The Most Critical Internet Security Vulnerabilities List."

- The operating system the firewall resides on, will be hardened to remove all unnecessary services and applications.
- Anti-spoofing will be configured on the firewall.
- Protecting against Buffer Overflow.
- Detailed logging.
- All traffic from the Service Network will be denied, except for SMTP TCP 25 and DNS TCP 53.
- Web Farm will be access through IP 206.123.224.114.

Rule	Source	Destination	Service	Action	Track	Comment
1	MGT	Firewalls Routers	Ssh Icmp-all	Accept	Long	Admin rule only allow from MGT network all others drop
2	X MGT	Firewalls	Any	Drop	Alert	Admin rule only allow from MGT network all others drop
3	X Internal	Any	Echo-request	Drop	Long	ICMP request drop
4	Internal	Any	Echo-reply Dest-unreach Time-exceded	Drop	Long	ICMP echo-reply, dest-unreachable and time exceeded drop

5	Any	Any	Netbios Tftp Snmp	Drop		Drop vulnerability ports
6	Any	Web server	http https	Accept	Long	Web traffic
7	Any	WWW	http	Accept	Long	WWW traffic
8	IN mail	Ext mail	Smtp	Accept	Long	IN mail sent to Ext mail server
9	Ext Mail	IN mail	Smtp	Accept	Long	External Mail sent to IN mail
10	Any	Broadcast	Any	Drop		Drop all broadcast address
11	Any	VPN	IPSEC	Accept	Long	VPN in
12	VPN	Any	IPSEC	Accept	Long	VPN out
13	Any	Internal DNS	Udp 53	Accept	Short	DNS in rule
14	Internal DNS	ISP DNS	Udp 53	Accept	Short	DNS out rule
15	Routers	MGT	Syslog	Accept	Long	Logging
16	Internal	Web	http https	Accept	Long	Allow internal users to surf the web
17	Any	Any	Any	Deny	Long	The clean up rule drop all

Rule 1: Allow only the management network to access and maintain routers and firewalls. All other IP address will be dropped. The firewall and router administrators will use secure shell (SSH) to access devices.

Rule 2: Sometimes called the stealth rule, this rule prevents users from access the firewall from outside the management network. If an attempt is made to connect directly an alert will alert the firewall administrator.

Rules 3-4: Limiting the ICMP from the internal network.

Rule 5: Dropping traffic on know vulnerable ports. Since there are known exploits for these ports and GIAC does not have a business need for the ports. All traffic distend to these ports will be dropped.

Rules 6-9: Allow application traffic to the service network but only on specified ports.

Rule 10: Drop all broadcast address from internal or external coming into the firewall.

Rules 11-12: Allows authorized VPN traffic in and out of the network.

Rules 13-14: Allows DNS queries in and out of the network.

Rule 15: Allows routers logs to the syslog server for centralized logging. Since the traffic needs to pass through the firewall, a rule needs to specifically allow logs to get sent to the syslog server.

Rule 16: All GIAC Enterprise employees will have Internet access. All web traffic will be filtered by Services Strategies Inc., Internet Access Management. Therefore, all users will be allowed to access the Internet.

Rule 17: Drops all other traffic not explicitly accepted. This rule must be the last entry in the rule set since all traffic reaching this rule will be dropped. Although the rule is placed last in order when configuring the firewall this rule was created first then configured backwards. The "clean-up" rule goes along with deny all unless explicitly allowed.

Just like the router ACL's the order of the rules on the firewall is very important. Since FW-1 works by examining each packet in chronological order, having the same rules but in different order can drastically change the way the rule set functions. Therefore when the packet is examined by the firewall as soon as it matches a rule, the firewall stops inspecting and applies the rule.

A quick example of how ordering can be a major factor. If your "clean up" rule (any any any deny) is your first rule, no packets will pass through the firewall. The reason being, all traffic will match this rule and be dropped without even reaching the other rules. This is why the more specific rules are first and the more general rules (like the "clean up" rule) last.

VPN

As mentioned earlier IPsec will be used for tunneling mechanism. IPsec is a collection mechanisms that provides a set of security services. These services are enabled through Authentication Header (AH port 50) and Encapsulation Security Payload (ESP port 51), and the use of cryptographic key management including Internet Security Association and Key Management Protocol (ISAKMP port UDP/500) and the Internet Key Exchange protocol (IKE).

The primary use of the VPN will be for conductivity for remote users to the corporate network. The remote users are required to sign an acceptable use policy and must use an approved GIAC Enterprise device. The device will be loaded with the approved VPN Client, personal firewall and anti-virus software. Also, split tunneling will not be enabled due to the potential outside treat using the VPN tunnel. Internet access will be granted through the corporate Internet gateway.

Authentication Header

The IPsec Authentication Header (AH) protocol is used to provide data integrity and

data origin authentication on a per packet basis. This implies that the data is authentic and that it will arrive at the destination without modifications. Although there is benefit in implementing AH, since we are using non-routable IP addresses we will not be able to use it.

Encapsulating Security Payload

The IPsec Encapsulating Security Payload (ESP) is responsible for authentication, data confidentiality through encryption and protecting the IP packets from replay. All three of the ESP's features are optional, but generally speaking either authentication or encryption are employed. Otherwise there would be no value added from the protocol. Given that GIAC Enterprise will use all three features of ESP, will provide data integrity via a one-way-hash.

Internet Key Exchange

Although the IPsec AH and ESP protocols determine how the data security are to be applied to each IP packet, it does not tell how the security associations are negotiated. This can be done manually or by Internet Key Exchange (IKE). IPsec uses the Internet Key Exchange (IKE) to exchange secure encryption keys over the Internet. This is a three-phase negotiation:

1) Initiator (VPN client) sends multiple Security Associations (SA) proposals to the responder (VPN gateway). The responder picks one proposal and sends it back to the initiator (this includes what type of encryption that will be used).
2) The two exchange their key exchange parameters and random use-once values (nonces).
3) The exchange information is authenticated.

VPN Configuration

An access list will need to be created to define the network traffic that will be encrypted and tunneled.

```
VPN1(config)#

access-list 151 permit ip 192.168.200.0 0.0.255.255
```

The ISAKMP policy defines what kind of authentication will be used.

```
VPN1(config)#crypto isakmp policy 20
VPN1(config-isakmp)#authentication pre-share
VPN1(config)#crypto isakmp key KEY address 192.168.1.2

VPN1(config)#crypto ipsec transform-set AH_MD5 ah-md5-hmac
VPN1(cfg-crypto-trans)#mode tunnel
```

Create crypto mapping and IPSec policy.

```
VPN1(config)#crypto map partner 20 ipsec-isakmp
VPN1(config-crypto-map)#set peer 192.168.10.2
VPN1(config-crypto-map)#set transform-set AH_MD5
VPN1(config-crypto-map)#match address 151

VPN1(config)#

interface s1/0
VPN1(config-if)#ip address 192.168.10.1 255.255.0.0
VPN1(config-if)#crypto map partner
```

Testing ACLs

To make sure the routers are filtering as intended, a small section of the rules will be tested. Before this occurs GIAC will need to turn on some additional logging to capture the output of our test. The three policies we will be testing are:

1) Test to see if the network can be used as a Smurf Amplifier.
2) Test the ingress anti-spoofing rule.
3) Test accessing Netbios port access.

Smurf Amplifier

Test
Insure the router is not forwarding broadcast requests.

Rule

```
Border1(config)# access-list 130 deny ip any host 206.123.224.255 log
Border1(config)# access-list 130 deny ip any host 206.123.224.0 log
```

Command

```
Nmap –n –sP –Pl –o amp.log '206.123.224.1,24,25,63,64,127,128,191,192,255'
```

Results (Router log)

```
May 10 14:24:23 EST: %SEC-6-IPACCESSLOGP: list 130 denied icmp 206.123.224.1
(4613) (Serial1 *PPP*) -> 206.123.224.19(723), 1 packets

May 10 14:24:29 EST: %SEC-6-IPACCESSLOGP: list 130 denied icmp
206.123.224.24 (2709) (Serial1 *PPP*) -> 206.123.224.19(723), 1 packets

May 10 14:24:36 EST: %SEC-6-IPACCESSLOGP: list 130 denied icmp
206.123.224.25 (3178) (Serial1 *PPP*) -> 206.123.224.19(723), 1 packets
```

Anti-Spoofing

Test
Try to connect through the router using a spoofed IP address.

Rule
Border1(config)# access-list 130 deny ip 206.123.224.0 0.0.0.31 any log

Command
Nmap –sS 206.123.224.19 -D 206.123.224.5

Results (Router log)
May 10 14:24:23 EST: %SEC-6-IPACCESSLOGP: list 130 denied tcp 206.123.224.19 (2781) (Serial1 *PPP*) -> 206.123.224.19(723), 1 packets

May 10 14:24:29 EST: %SEC-6-IPACCESSLOGP: list 130 denied tcp 206.123.224.19 (5910) (Serial1 *PPP*) -> 206.123.224.19(723), 1 packets

May 10 14:24:36 EST: %SEC-6-IPACCESSLOGP: list 130 denied tcp 206.123.224.19 (3398) (Serial1 *PPP*) -> 206.123.224.19(723), 1 packets

Netbios

Test
Try to connect through the router via Netbios port.

Rule
Border1(config)# access-list 130 deny tcp any any range 135 139 log
Border1(config)# access-list 130 deny udp any any eq 135 log
Border1(config)# access-list 130 deny udp any any range 137 138 log

Command
Nmap –p135-139 –P0 206.123.224.5

Results (Router logs)
*May 10 04:16:35 EST: %SEC-6-IPACCESSLOGP: list Ingress denied tcp 207.207.207.207 (1253) -> 206.123.224.5(137), 1 packet
*May 10 04:16:41 EST: %SEC-6-IPACCESSLOGP: list Ingress denied tcp 207.207.207.207 (1267) -> 206.123.224.5(137), 1 packet
*May 10 04:16:47 EST: %SEC-6-IPACCESSLOGP: list Ingress denied tcp 207.207.207.207 (1289) -> 206.123.224.5(138), 1 packet
*May 10 04:16:53 EST: %SEC-6-IPACCESSLOGP: list Ingress denied tcp 207.207.207.207 (1213) -> 206.123.224.5(138), 1 packet

Router Tutorial

To configure a new router, you will need to connect the router to a terminal to get to a command prompt. Once this is set you should see the following:

Router>

At this prompt you are in exec mode, this is were you are able to issue commands from the command line. From this prompt you have very limited privileges. From here you can enter the privileged mode by typing enable at the prompt.

Router> enable
Router #

Since the router is not configured there will not be a password protecting this mode. At this point you should password protect the privileged mode.

To begin configuring the router you must go into the "sub" mode of the privileged mode named Global Configuration mode. The Global Configuration mode is were all router configurations are done. To enter into this sub mode type the following:

Router # config
Router (config) #

As long as you pay attention to the router prompts, you will know what mode you are in. In the Global Configuration mode you will be able to issue a host name, set a password, etc. or configure a specific interface on the router.

Router (config) # hostname Border1
Border1 (config) # Interface Ethernet0/0
Border1 (config-if) # ip address w.x.y.z a.b.c.d
Border1 (config-if) # no shutdown
Border1 (config-if) # <ctrl-c>
Border1 (config) #
Border1 (config) # <ctrl-c>
Border1 #

Firewall Audit

Requirements

You have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises. You are required to audit the Primary Firewall

described in Assignments 1 and 2. Your assignment is to:

1. Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.

2. Implement the assessment. Validate that the Primary Firewall is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.

3. Conduct a perimeter analysis. Based on your assessment (and referring to data from your assessment), analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.

Note: DO NOT simply submit the output of nmap or a similar tool here. It is fine to use any assessment tool you choose, but annotate the output.

Introduction

The network design after implementation, will need to be tested to make sure the configuration will work as expected. This will be done from both the inside and outside of the network. Although the audit process is primarily for the primary firewall, other devices will be indirectly tested, including; routers, secondary firewalls, public servers, mail servers and DNS servers.

This also afforded an opportunity to put the GIAC Enterprise staff to the test. Only management will be aware of the audit. This will allow GIAC's security department to witness how incidents are handled and if proper procedures are followed. Upper management will need to be informed for the simple reason some of the test have a risk of a Denial of Service (DoS). If this occurs all key personal (determined before the test) will be informed, so firewall and other devices can be restarted.

Project Plan

The project plan will consist of 3 primary parts

1) Port scan – Scan the firewall for TCP, UDP, and ICMP protocols from the internal network as well as outside the network. This is done to insure no unnecessary ports are open or unnecessary information is leaked (via ICMP reply).
2) Testing the rule base – The rule base will be tested to insure the rules are performing as intended. This will include packets that should be accepted as well as packets that should not. To accomplish this we will need to have a laptop on the other side of the firewall sniffing packets.

3) Checking for known vulnerabilities and patches - Researching known vulnerabilities and attempting to exploit them on the firewall. This could be patch level specific or services running on the appliance (such as tftp).

One week prior to the audit, management will be briefed on the full scope of the audit. This briefing will include such topics as; exposing security holes, accessing confidential information and the possibility of denial of service (DoS). Also during this meeting we will require them to sign the consent to perform the audit.

Time and Cost

Time will be broken down by onsite and offsite with a per hour rate of $250.

- 8 hours offsite – Port scanning, penetration testing and fingerprinting.
- 12 hours onsite – Information gathering, internal scans and analyzing results.
- Total estimated cost $5000.
- This cost does not take into consideration problems that may occur as a result of the testing.

As mentioned above the audit will be preformed from both internally and externally. For the offsite testing we will break down the testing times into peak and non-peak time. The peak time will be when the GIAC staff is physically onsite (traditionally 8-5 on weekdays). While non-peak will be defined as the remaining time.

Tools

Network Mapper (NMAP) is a utility that can be used for network security auditing. It was designed to scan networks, and will help determine what ports are listening. Although the same could be accomplished by the netstat command run at the O/S level, it does not ensure the utility is a “clean” copy. In addition, NMAP examines IP packets to determine what hosts are available on the network, what operating system (and O/S version) running, what type of packet filters/firewalls are in use, and more.

Nessus is a security scanner that allows the user to remotely determine what possible vulnerabilities are associated with the specific port. Although this seems a bit over kill running two scanners against the network each tool has their advantages and disadvantages. One of the big advantages of Nessus is it’s very paranoid. What I mean by this is it does not trust version numbers or ports. If the network is listening on port 21 for http and 80 for ftp, Nessus will know and scan appropriately.

Tcpdump allows us to sniff network packets and make some statistical analysis from the “dumps”. The tcpdump utility will be running behind the firewall sniffing for traffic produced by NMAP. This will help determine if the security policy is letting undesired traffic into the network.

Execution of Audit

NOTE: The below scans were preformed on a HP-UX workstation in a test lab.

Services

To determine what services are running on the firewall, the NMAP utility returns all services running. If services are running that should not be they will be identified and disabled. This will be preformed on both the external and internal interface in the same mannor.

TCP scan
Nmap –sS –v –P0 –O –p 1-65535 –oN fw1_tcp.out 206.123.224.19

For the TCP scan we will not attempt a full connect to a specific port (-sS instead of –sT for a full connection). The advantages to a "half open" connection is a more stealthy approach to the scan. By only sending the SYN packet and determining if the port is listening by receiving a SYN/ACK, there is less of a chance of being noticed. The scan will be run in verbose (-v) mode to get as much information as possible. The next option (-PO) turns off the automatic pinging of the network prior to scanning. Next we will attempt TCP/IP fingerprinting (-O) as well as other tests such as uptime guessing and TCP sequence predictability. The scan will hit all available ports (-p 1-65535) and log the results (-oN fw1_tcp.out).

UDP scan
Nmap –sU –v –PO –O –p 1-65535 –oN fw1_udp.out 206.123.224.19

The UDP scan (-sU) will check all listening ports (-p 1-65535) to determine which are open and log results (-oN fw1_udp.out).

TCP SCAN

nmap (V. 2.54BETA22) scan initiated Mon Aug 12 09:38:18 2002 as: nmap –sS -v - P0 -O -p 1-65535 -oN test.out w.x.y.z
Interesting ports on firewall.com (w.x.y.z):
(The 65507 ports scanned but not shown below are in state: closed)

Port	State	Service
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
37/tcp	open	time
111/tcp	open	sunrpc
883/tcp	open	unknown
888/tcp	open	accessbuilder
890/tcp	open	unknown
892/tcp	open	unknown
894/tcp	open	unknown
892/tcp	open	unknown

894/tcp open unknown
2121/tcp open unknown
4045/tcp open lockd
6000/tcp open X11
6111/tcp open spc
7161/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49157/tcp open unknown
49169/tcp open unknown
49174/tcp open unknown

Remote operating system guess: HP9000 Model 804 K450 running HP/UX 11.00
Uptime 45.882 days (since Thu Jun 27 13:26:38 2002)
TCP Sequence Prediction: Class=random positive increments Difficulty=5679 (Worthy challenge)
IPID Sequence Generation: Incremental

Nmap run completed at Mon Aug 12 10:36:27 2002 -- 1 IP address (1 host up) scanned in 3489 seconds

UDP SCAN

nmap (V. 2.54BETA22) scan initiated Mon Aug 12 10:46:10 2002 as: nmap -sU -v -P0 -O -p 1-65535 -oN test.out w.x.y.z
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port Interesting ports on firewall.com (w.x.y.z):
(The 65509 ports scanned but not shown below are in state: closed)

Port	State	Service
13/udp	open	daytime
37/udp	open	time
67/udp	open	bootps
111/udp	open	sunrpc
882/udp	open	unknown
889/udp	open	unknown
891/udp	open	unknown
893/udp	open	unknown
895/udp	open	unknown
898/udp	open	unknown
1023/udp	open	unknown
2049/udp	open	nfs
2121/udp	open	unknown
4045/udp	open	lockd
49158/udp	open	unknown
49160/udp	open	unknown
49161/udp	open	unknown
49162/udp	open	unknown
49163/udp	open	unknown
49164/udp	open	unknown

Remote OS guesses: MacOS 8.1 running on a PowerPC G3 (iMac), HP-UX B11.00 U 9000 /839, Solaris 2.4 w/most Sun patches (jumbo cluster patch, security patches, etc)

Nmap run completed at Mon Aug 12 10:46:42 2002 -- 1 IP address (1 host up) sca

nned in 32 seconds

Nessus scan

```
timestamps|||scan_start|Tue Aug 13 05:30:34 2002|
timestamps||w.x.y.z|host_start|Tue Aug 13 05:30:34 2002|
results|a.b.c.d|w.x.y.z|daytime (13/tcp)
results|a.b.c.d|w.x.y.z|ftp (21/tcp)
results|a.b.c.d|w.x.y.z|ssh (22/tcp)
results|a.b.c.d|w.x.y.z|telnet (23/tcp)
.
.
.
results|a.b.c.d|w.x.y.z|smtp (25/tcp)|10260|Security Warning|You are runnin
g a version of Sendmail which is older\nthan version 8.9.0.\n\nThere's a flaw in
 this version which allows people to send\nmail anonymously through this server
(their IP won't be shown\nto the recipient), through a buffer overflow in the HE
LO\ncommand.\n\n*** Nessus reports this vulnerability using only\n*** informatio
n that was gathered. Use caution\n*** when testing without safe checks enabled.\
n\nSolution : upgrade to sendmail 8.9.0 or newer\nRisk factor : Low\nCVE : CAN-1
999-0098\n
results|a.b.c.d|w.x.y.z|unknown (882/udp)|10544|Security Hole|\nThe remote
statd service may be vulnerable\nto a format string attack.\n\nThis means that a
n attacker may execute arbitrary\ncode thanks to a bug in this daemon.\n\n*** Ne
ssus reports this vulnerability using only\n*** information that was gathered. U
se caution\n*** when testing without safe checks enabled.\n\nSolution : upgrade
to the latest version of rpc.statd\nRisk factor : High\nCVE : CVE-2000-0666\n
timestamps||w.x.y.z|host_end|Tue Aug 13 05:46:40 2002|
timestamps|||scan_end|Tue Aug 13 05:46:40 2002|
```

A simple way to determine how well the firewall is hidden from the outside, we can execute a ping to the external IP of the firewall. Or use nmap specifying the ports.

```
E:\>ping 206.123.224.19
Pinging 206.123.224.19 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 206.123.224.19:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

nmap –sP <port number> 206.123.224.0/24

Penetration Testing

Penetration testing will be in three distinct stages, Discovery, Enumeration and Exploitation.

Stage I - Discovery
The first stage will be devoted to information gathering and discovery. The GIAC audit team will attempt to gather all available information concerning the GIAC Enterprise network environment. This will include: querying various whois servers, examining DNS records (both authoritative and non-authoritative), and utilizing standard network utilities.

Once the information is gathered, the public information will be consolidated and an attempt will be made to map the network. This will include devices such as routers or firewalls, and the routes to other targets.

Stage II - Enumeration
The second stage will be the network penetration test and vulnerability assessment. The systems targeted will be the ones identified in stage I to specify host configuration and settings. This will include versions and their vulnerability. Once this is determined, the potential vulnerabilities will be researched.

Stage III – Exploitation
The third stage uses the vulnerabilities found and researched in stage II, and attempt to exploit known weaknesses. The goal of this stage is to gain user level access to an internal system.

FTP and DNS

The next scan is very similar to the one above, the difference is now the port will be specified. In many cases ports 20 and 53 can circumvent access lists.

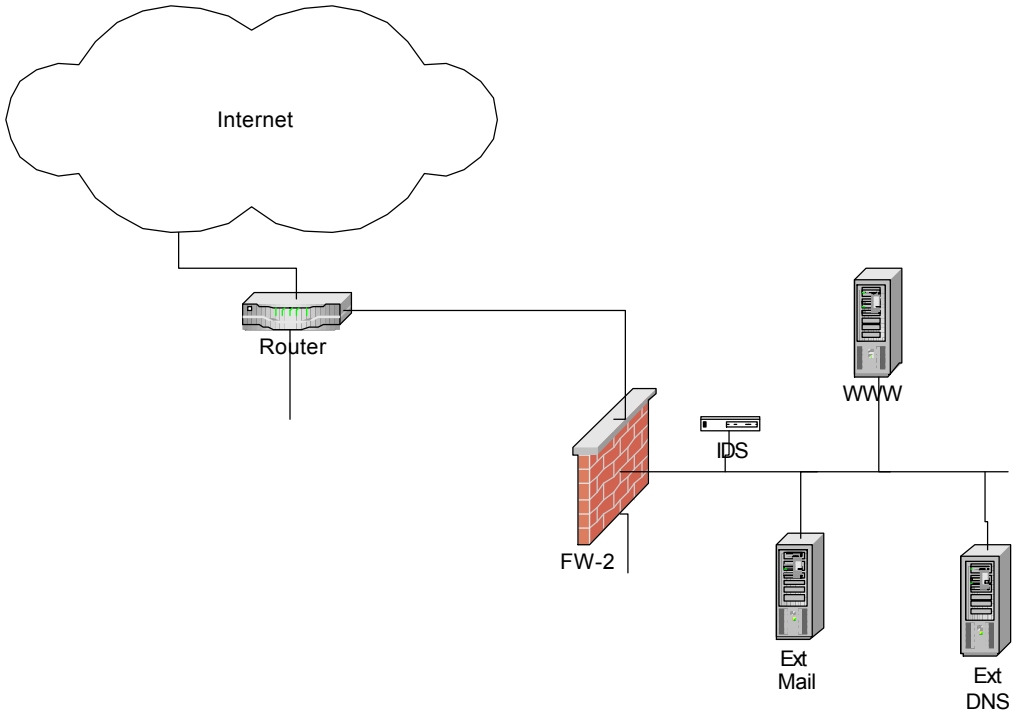
```
nmap –v –sU  –g53 –P0 –O –p 1-65535 –o fw1_1.out target
nmap –v –sS  –g53 –P0 –O –p 1-65535 –o fw1_1.out target
nmap –v –sS  –g20 –P0 –O –p 1-65535 –o fw1_1.out target
```

(Repeated on all interfaces of the firewall.)

Access from unauthorized subnet

Attempt to access the firewall from somewhere other then the management network. The results were the connection was not established.

Access to External Service Network and WWW

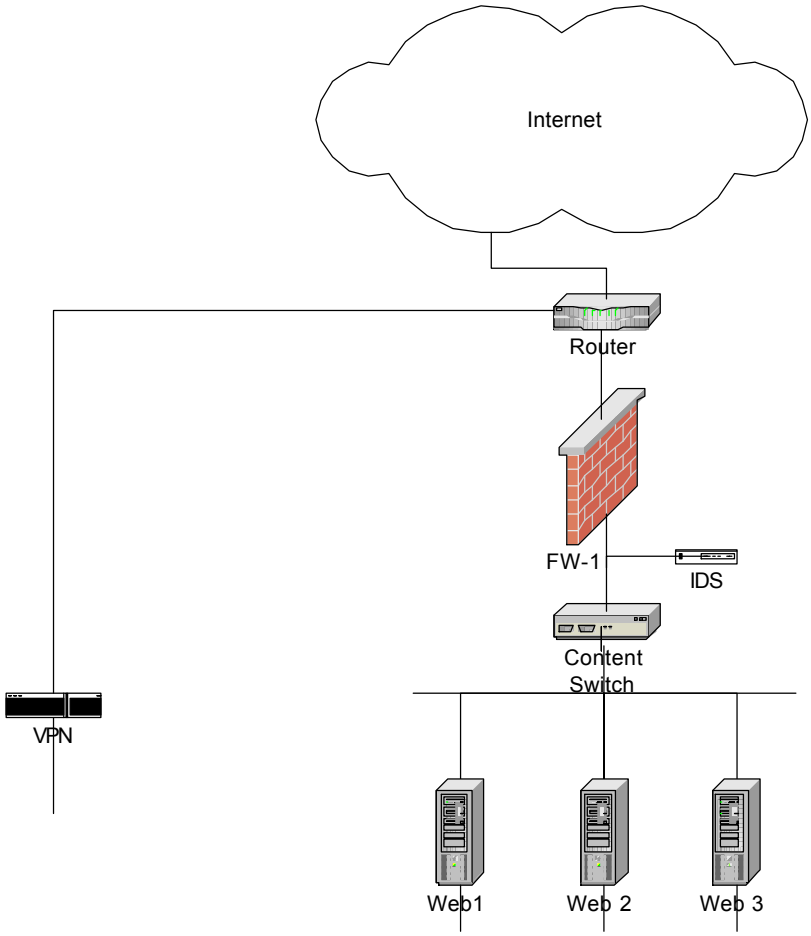


DNS – Attempt to lookup a valid IP address through the external DNS server. Then attempt to lookup a valid IP address to a DNS server on the Internet.

WWW – Access the web page from an external connection and negotiated through the site.

Mail – Mail can be tested by sending a email to a valid Internet address and sending email from a valid Internet address to GIAC Enterprise.

Web Servers and VPN



Web servers – Access the web servers from an external connection and complete a transaction.

VPN – To examine VPN there will need to be a sniffer running between the border router and the VPN concentrator. The reason for this is to ensure the traffic is being encrypted crossing the Internet.

Syslog – All logs should be stored on the syslog server.

IDS – The IDS systems should be working overtime during the audit. All logs will be checked to make certain they are working properly.

Backups – A random check and restore will be performed on backup tapes, from both onsite storage and offsite storage.

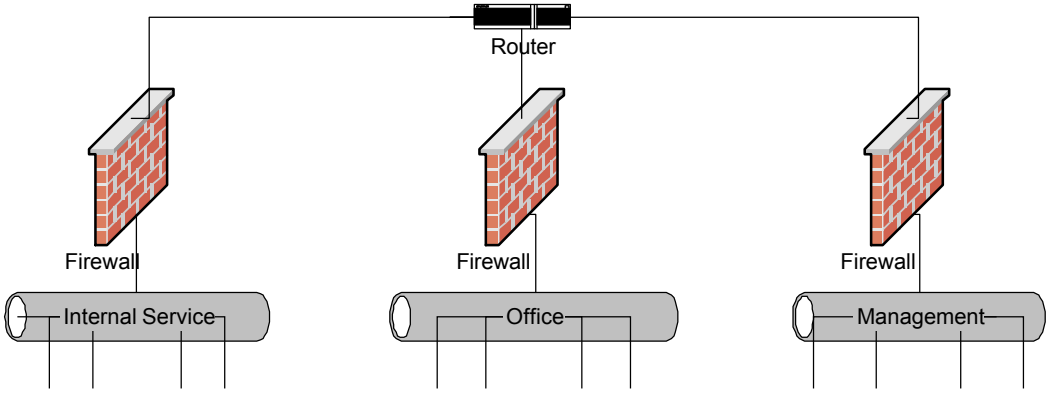
Audit Conclusion

The audit demonstrates the architecture is functional, while maintaining a high level of network security. The firewall's ACL's performed as expected, by not allowing spoofed address and unauthorized services to be forwarded. When spoofed address and

unauthorized services were attempted all actions were logged and denied. One area that will need to be looked at further is the attempt to diversify with two different firewalls (FW-1 and Pix). By having both the internal and external firewalls being packet filtering firewalls, GIAC is not fully leveraged having two different solutions. One area that will be further reviewed is to replace the internal Pix with a proxy firewall. The main reason this was not implemented in the original design was lack of expertise in the area of proxy configuration.

The security audit will help GIAC Enterprise not only assess the configuration of the network, it will measure the effectiveness of the internal staff. There is no guarantee of absolute security in a network architecture, one can only mitigate the potential risk. GIAC Enterprise feels confident that this has been accomplished with their layered approach.

Future consideration would be to place separate firewalls on each of the internal networks. This would not only that the strain off the internal router it would allow an additional security layer to critical networks. This was not in the initial network design due to staffing and cost issues.



Another future consideration would be to have an independent company perform a penetration test and vulnerability assessment against the network. By having a working knowledge of the network one could overlook possible exploits. The recommendation is to have an independent company perform a penetration test and vulnerability assessment annually and GIAC staff perform them quarterly.

Design Under Fire

Requirements

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

will be attacking your architecture!

Select a network design from any GCFW practical posted in the previous 6 months and paste the graphic into your submission. Be certain to list the URL of the practical you are using.

Research and design the following three types of attacks against the architecture:

1) An attack against the firewall itself.
   - Research and describe a vulnerability that has been found for the type of firewall chosen for the design.
   - Design an attack based on the vulnerability.
   - Explain the results of running that attack against the firewall.

2) A denial of service attack.
   - Subject the design to an attack from 50 compromised cable modem/DSL systems.
   - Describe the countermeasures that can be put into place to mitigate the attack that you chose.

3) An attack plan to compromise an internal system through the perimeter system.
- Select a target and explain your reasons for choosing that target.
- Describe the process to compromise the target.

Your attack information should be detailed – include the specifics of how the attack would be carried out. Do not simply say "I would exploit the vulnerability described in Vendor Security Bulletin XXX". What commands would you use to carry out the attack? Are exploit tools or scripts available on the Internet? What additional steps would you need to take prior to conducting the attack (reconnaissance, determining internal network layout, determining valid account name…)? Would any of your methods be noticed (log files, IDS…)? What "stealth" techniques could you employ to avoid detection? What countermeasures would help prevent your attack from succeeding?

If it is possible to carry out the attack on a test system, include screen shots, log files, etc. as appropriate to illustrate your methods.

In designing your attacks, keep the following in mind:

- The attack should be realistic. The purpose of this exercise is for the student to clearly demonstrate that they understand that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.

- The attack should be reasonable. The firewall does not necessarily have to be impenetrable (perfectly configured with all of the up-to-the-minute patches

installed). However, you should not assume that it is an unpatched, out-of-the-box firewall installed on an unpatched out-of-the-box OS. (Remember, you designed GIAC Enterprises' firewall; would you install a system like that?)

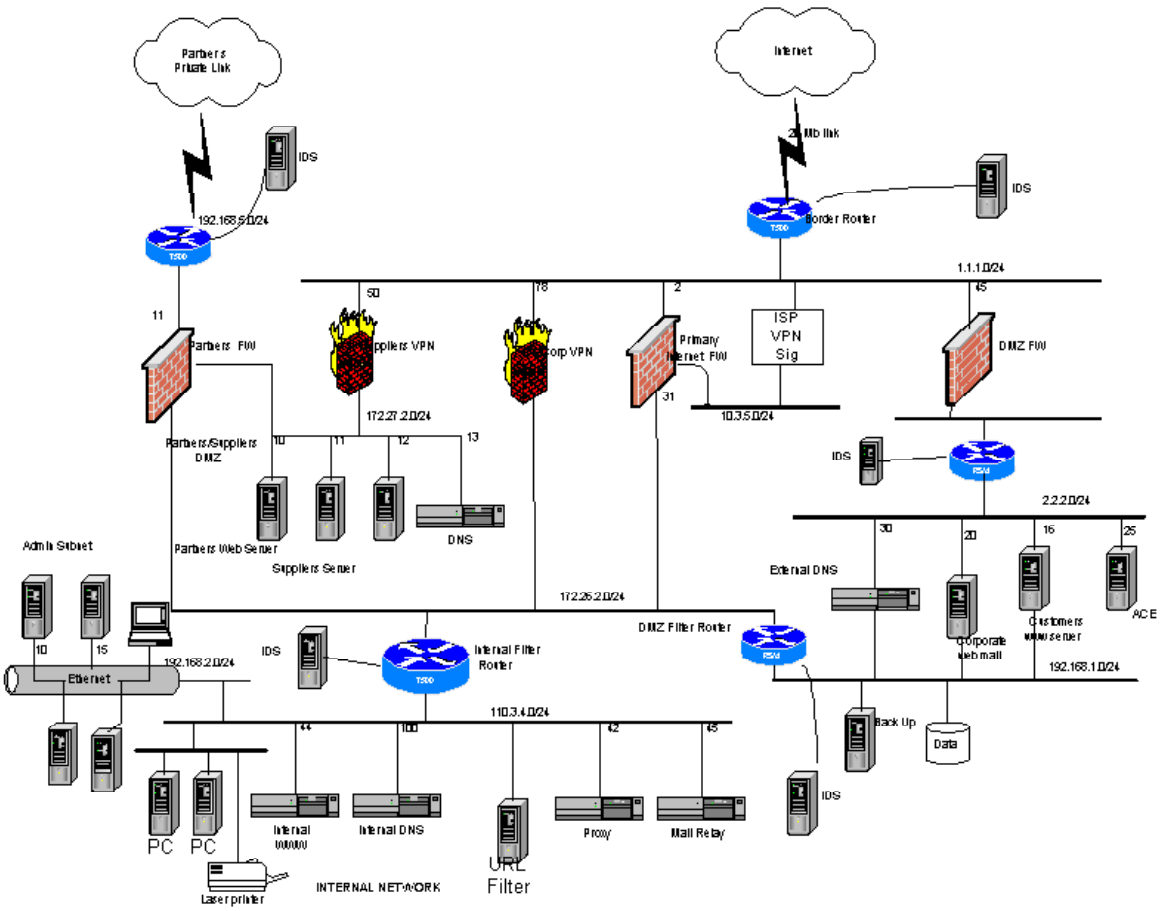
- You must supply documentation (e.g., a URL to the security bulletin, bugtraq archive, or exploit code used) for any vulnerability you use in your attack.

The attack does not necessarily have to succeed. If, given the perimeter and network configuration you have described above, the attack would fail, you can describe this result as well.

Attack

There are a few assumptions we are going to take liberty using. This includes information gathering consisting of whois searches, port scanning O/S fingerprinting and social engineering. These beginning steps are very important and cannot be overlooked, but since we have the network design, the research will start after information is gathered.

I have chosen Jim Phan's (247) network design located at http://www.giac.org/practical/Jim_Phan_GCFW.zip. I decide on Mr. Phan's network design (Figure 4) due to the implementation of Check Point Firewall-1. Since GIAC Enterprise's primary firewall is also Firewall-1 it will be a good exercise to expose possible flaws in GIAC's network.



Firewall Exploits

CAN-2001-1102 - Firewall-1 Policy-name Temporary File Creation Vulnerability

Check Point FireWall-1 3.0b through 4.1 for Solaris allows local users to overwrite arbitrary files via a symlink attack on temporary policy files that end in a .cpp extension, which are set world-writable.

The attack on this vulnerability has to be done locally. It is possible to change the permissions of root-owned files and increase privileges beyond the ones originally granted. The problem is in the creation of predictable /tmp files. Upon editing firewall rules and committing them, a file is created in /tmp using the name of the policy as a filename, and .cpp as an extension (http://online.securityfocus.com/bid/3300).

There are two ways I see to exploit this vulnerability:

1) Gain low level access, by piggy-backing on another vulnerability, then attempt to "bump up" your access.
2) The other way is to combine social engineering and physical access.

I will attempt to attack is the firewall with a known vulnerability, detailed on the Checkpoint web site (www.checkpoint.com/techsupport/alerts/pasvftp.html). This particular vulnerability exploits passive mode ftp through Firewall-1, with the possibility of gaining root access on the device. This attack is performed by triggering an internal host to generate a TCP packet that, when inspected by the firewall, will change the firewall's internal state and enable an attacker to establish a TCP connection to a filtered port through the firewall.

Firewall-1 screens packets sent from the FTP server to the client, looking for the string 227 at the beginning of each packet. When Firewall-1 has a match, it will pull out the destination IP address and destination port. Once this information is verified with source address of the packet, a TCP connection is allowed through the firewall.

To exploit this and deceive Firewall-1 into opening up a TCP connection, you must have the server send the 227 string in the first four bytes. This can be done by using the error handler of the FTP daemon, along with limiting MMS of the TCP connection. This is easy to do by setting the MTU of our interface to a small value we can work with, before we establish a control connection to the victim FTP server. In this case, the returning packets from the server will be smaller, allowing us to control how data is split into packets. Thus, we can make the 227 message returned by the error handler appear at the beginning of a packet.

Some ways to reduce the risk of this threat is:

- Disable passive mode ftp.
- Use a dedicated ftp server.

Compromise an Internal System

The attack to compromise an internal system is a combination of social engineering, Trojan crafting and human nature. There will be three phases to the attack:

1) Information gathering of user emails.
2) Craft a Trojan.
3) Send the email to the users.

Finding user id's is not as difficult as it may seem. There are a number of ways this can be accomplished.

- Business cards of employee's that work for GIAC
- Check web page for company.

- View the source on the web page for the email address off the web administrator (don't laugh I've seen it).
- Check chat rooms and bulletin boards for postings by GIAC employees.
- Call the company and ask the person for their email.

The last one is not sexy but very effective. After receiving a few email address you may be able to notice a pattern of email naming. An example of this is as follows:

Name	Email	Email Naming
John Johnson	jjohnson@giac.com	First initial last name
John Johnson	jjohnso@giac.com	First initial and first 6 letters of last name

By figuring out the naming convention we may be able to guess a few more email names, based on common last names. This can be done by simply by sending emails to ajones, bjones, cjones, etc. This can be vary easily scripted using Perl to loop a few hundred names.

Once this is accomplished we will move into phase 2.

Phase 2 is crafting a Trojan to email to our unsuspecting list of users we gathered in the first phase. Since users have access to the internet via port 80 we could wrap a small piece of code in a picture and attach it in our email via a tool such as Saranwrap). The code would be similar to that of the software gotomypc.com uses (the download is only 1.4 MB for gotomypc.com). How it works is once the software is installed, a service waits for a connection request. This request comes in the form of an ping via port 80. Once the request is received a connection is established and we have access through the firewall on port 80. The final phase is to send out the emails.

Some ways to deter an attack like this:
1) Educate the work force – By educating the users on social engineering and general security awareness you can greatly decrease the chances of this happening. Another reason to educate users is to increase your security staff without increasing your head count.
2) Anti-Virus Software – Anti-Virus software must be up to date for the most recent signatures and enabled. There should be Anti-Virus checking on the mail server as well as personal Anti-Virus on the individual workstations.
3) Limit Internet access to users – If there is not a business need for users to have Internet access, don't open it up.

Although the attack may not have made it past the mail gateway (due to the Anti-Virus) an alternative solution would be to host a web site similar to gotomypc. This would allow us to send a link instead of an attachment.

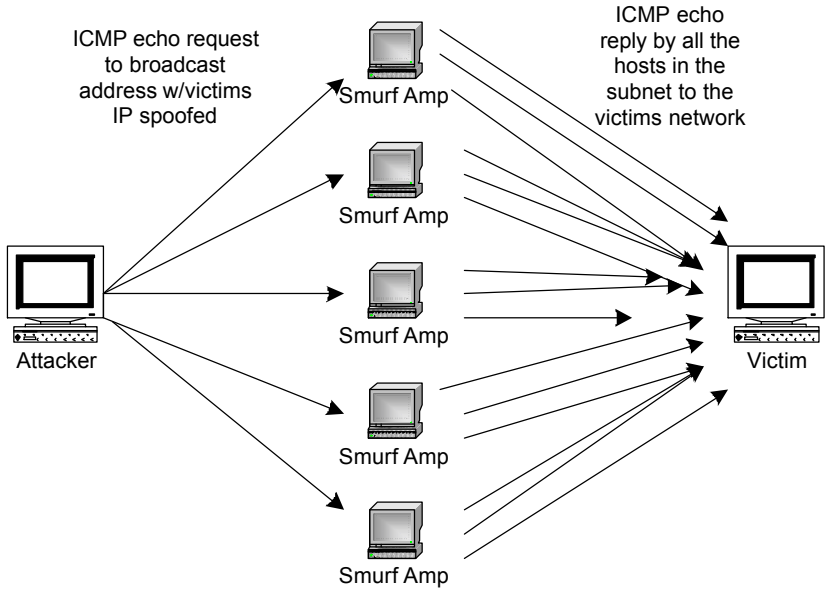
DoS on Network

A Denial of Service attack (DoS) is an attack through which a person can render a

system unusable or significantly slow down the system for legitimate users by overloading the resources so no one else can access it (Eric Cole, Hackers Beware, New Riders Publishing 2002, Pg. 193). DoS attacks are extremely hard to defend against since you have no control over the determination of the attacker. Even if you increase the bandwidth of your network, the attacker can just send more packets.

Seeing as our goal is to deny service to Mr. Phan's network design, the DDoS of choice is a Smurf attack. In early 2000, five major Internet sites were denied service by flooding the sites with multiple packets.

A Smurf can be broken down into two basic parts, forged packets and the use of a broadcast address. The attacker sends ICMP echo request to the broadcast address of an IP subnet. When the request is sent, it is done so with the victims IP address spoofed as the source. If the routers are not setup to deny echo requests and allows ICMP echo replies out (known as Smurf Amplifiers), every host on the broadcast will respond with ICMP replies to the victims machine. With all the unwanted traffic hitting the victims network, there is a potential to make the network unusable. As stated above, if at first the traffic does not cause the desired results, simply add more Smurf Amplifiers.



Finding Smurf Amplifiers

With all the publicity on security and possible legal implications of companies not taking due diligence, you would figure better care would be taken to configure them correctly. There are a few ways to find networks to leverage for Smurf Amplifiers.

First the manual way of finding a Smurf Amplifier, with the use of NMAP complements of Fydor.

Nmap –n –sP –PI –o amp.log '1.1*.1,24,25,63,64,127,128,191,192,255'

This command essentially performs a scan with ICMP echo requests conducted before the scan begins. This command will also send the results to the file amp.log for analyzing the results. Although this is relatively easy to do by dumping the command into a script and hitting multiple networks, there is an easier way.

There is a web site, www.pulltheplug.com, designed to open the eyes of companies that can be used as Smurf Amplifier. The down side is, this web site makes it all too easy to pick a network(s) to leverage in an attack (See Appendix E for example www.pulltheplug.com/broadcasts.html). The site even breaks it down by how many responses come back with each broadcast. Per the web site there were 125,102 networks misconfigured in late 2000.

Launching the Attack

You have the addresses you want to use as Smurf Amplifiers now it is time to launch the attack. First we identify our target, in this case it would be 1.1.1.1. Second we need to make a file (or if NMAP was used with the –o option we can use that file) with the subnet's of Smurf Amplifiers.

The actual attack command would be:

Smurf 1.1.1.1 smurf.amp 0 1 512

It is vary difficult to prevent this type of an attack and can potentially DoS the systems being leveraged as the amplifier. One way to insure your system cannot be used as an amplifier is with proper router configuration.

```
Border1(config)# !Smurf Attack
Border1(config)# access-list 130 deny ip any host 206.123.224.255 log
Border1(config)# access-list 130 deny ip any host 206.123.224.0 log
```

The victims network may have all the right configurations and more then enough bandwidth for their particular network. But as long as there are networks that allow IP broadcast traffic in and out of their networks this problem will continue to exist. When this attack occurs the administrator should contact the administrator who's network is being leveraged and educate them on proper configuration. To stop this attack once in progress, the victim would need to contact their ISP to filter the attack "up stream."

Appendix A - GIAC Enterprise Security Policy

A.1 Anti-Virus And Worm Incidents

Although virus and worm incidents are very different, the procedures for handling them are very similar. The principal difference is in the initial isolation of the system and the time criticality.

Viruses are not self-replicating, so virus incidents are not as time-critical as worm or hacker incidents. Time is a critical factor when dealing with a worm attack because worms are self-replicating and can spread to hundreds of machines in a matter of minutes. If you are not sure of the type of the attack, then proceed as if the attack was worm-related.

A.1.1 Isolate the System

Isolate infected system(s) from the remaining GIAC Enterprise network as soon as possible. If a worm is suspected, then a decision must be made whether to disconnect GIAC Enterprise from the outside world. Network isolation is one method to stop the spread of a worm, but the isolation can also hinder the clean-up effort since GIAC Enterprise will be disconnected from sites that may have patches. The GIAC Enterprise Security Officer must authorize the isolation of the GIAC Enterprise network from the outside world. **Log all actions.**

Do not power off or reboot systems that may be infected. Some viruses will destroy disk data if the system is power-cycled or rebooted. Similarly, rebooting a system could destroy needed information or evidence.

A.1.2 Notify The Appropriate People

Notify the GIAC Enterprise Security Administrator as soon as possible. If unable to reach him/her within 10 minutes, contact the backup person. The GIAC Enterprise Security Administrator will then be responsible for notifying other appropriate personnel. ***NOTE - Below, different times are given for suspected worm attack and for a suspected virus attack.

- The GIAC Enterprise Security Administrator will notify the GIAC Enterprise Security Officer as soon as possible. If unable to reach him within one hour (10 minutes for a worm attack), his backup person will be contacted.
- The GIAC Enterprise Security Administrator or Security Officer will notify the GIAC Enterprise ISO within two hours (one hour for a worm attack). The GIAC Enterprise ISO will escalate to higher level management if necessary.
- The control room or GIAC Enterprise Security Administrator should notify all involved local system administrators within four hours (two hours for a worm attack).

A.1.3 Identify the Problem

Try to identify and isolate the suspected virus or worm-related files and processes. Before removing any files or killing any processes, take a snapshot of the system and save it securely.

A sample list of tasks to make a snapshot of a UNIX system follows:

1) Save a copy of all system log files. The log files are usually located in /usr/adm.
2) Save a copy of the root history file, */.history*.
3) Save copies of the */etc/utmp* and */etc/wtmp* files. These files are sometimes found in

the */usr/adm* directory.

A.1.4 Contain the Virus or Worm

All suspicious processes should now be halted and removed from the system. Make a full dump of the system and store in a safe place. The tapes or disks should be carefully labeled so they will not be used by unsuspecting people in the future. Then remove all suspected infected files or worm code. In the case of a worm attack, it may be necessary to keep the system(s) isolated from the outside world until all GIAC Enterprise systems have been inoculated and/or the other Internet sites have been cleaned up and inoculated. **Log all actions.**

A.1.5 Inoculate the System(s)

Implement fixes and/or patches to inoculate the system(s) against further attack. Prior to implementing any fixes, it may be necessary to assess the level of damage to the system. If the virus or worm code has been analyzed, then the assessing the damage is not very difficult.

However, if the offending code has not been analyzed, then it may be necessary to restore the system from backup tapes. Once the system is brought back into a safe mode, then any patches or fixes should be implemented and tested. If possible, the virus or worm may be used to infect an isolated system that has been inoculated to ensure the system(s) are no longer vulnerable.

Log all actions.

A.1.6 Return to a Normal Operating Mode

Prior to bringing the systems back into full operation mode, you should notify the same group of people who were notified in stage one. The users should also be notified that the systems are returning to a fully operational state. It may be wise to ask all users to change their passwords.

Before restoring connectivity to the outside world, verify that all affected parties have successfully eradicated the problem and inoculated their systems. **Log all actions.**

A.1.7 Follow-up Analysis

Perform follow-up analysis. This involves identifying, if possible, the method by which the problem was introduced and any mistakes made in isolating and eradicating it.

A.2 Password Assessment

A.2.1 Assessment GIAC Enterprise systems users have the ability to change their own passwords. As a result, there is a large potential for having weak passwords protecting GIAC Enterprise computers and resources. Members of the GIAC Enterprise system administration staff are responsible for ensuring that all passwords are of sufficient quality to protect proprietary information from disclosure or modification. When dealing with password assessment, members of the GIAC Enterprise system administration staff should use the following guidelines:

* When possible, ensure the computer system enforces good passwords using tools such as passfilt.dll for Windows NT and passwd+ for UNIX.
* The only tools authorized for password assessment are: l0phtcrack for NT and crack for Unix systems.
* Before performing password assessment, the lead system administrator shall inform the GIAC Enterprise computer security officer.
* System administrators shall work in teams of two while performing password

assessment.
* Notify account owners immediately by telephone, and ask the owner to change the password. If possible, ensure the password has been updated. If the account owner cannot be reached, lock out the account. Schedule the account owner for the next available GIAC Enterprise mandatory computer security awareness class and inform him/her of the requirement to attend.
* Store cracked password files in a locked container. After all accounts have been fixed or deactivated, all files, paper and electronic shall be shredded in a manner to preclude reconstruction.

A.2.2 Guidance for Password Selection

* Do not use any personal names, places, birthdays, nouns, verbs, etc.
* Do not use anything that can be traced back to you. (e.g. auto license number, bank account number, anniversary date, amateur radio license, etc.)
* Do not use anything that has to do with your profession. (e.g. job title, degree, etc.)
* Do not use the same password for all computers. It is preferred that you have a different password for each host login prompt. Never use your local password outside the GIAC Enterprise domain.
* Do use 8 places in your password.
* Do use characters with numbers and punctuation. Intersperse capitals with lower case to increase the number of possibilities. Example: ~aIH4b/,
* Do change your passwords regularly, at least four times a year. And do not use a previous password as the new one.

A.3 Backups

A.2.1 Philosophy GIAC Enterprise systems used as servers will be backed up nightly. Users are responsible for backups of files maintained on local hard drives and mobile computers. Members of the GIAC Enterprise support staff should use the following guidelines:

* Members of the GIAC Enterprise system administration staff are responsible for managing backups for all Windows NT servers and the firewall.

(For Windows NT systems) Staff authorized to perform backups shall be added to the Backup Operator group.

* Backup Operators shall perform full backups at 4:00 AM on Mondays and Fridays. Differential backups shall be performed at 8:00 PM Monday through Friday.
* A legible, unique label shall be placed on all tapes and/or CDs or disks.
* Create a log in which you record which tapes/disks are used and for which servers. Note any errors or pertinent events every day. Logs should contain information about successful backups, unsuccessful backups, tapes that were left in place accidentally and overwritten, when and where tapes were sent off site, the success or failure of restore tests, and bad tapes encountered which may affect your ability to obtain files from a previous backup.

If possible, maintain two logs. First, the backup software should capture a list of all files and directories encountered and saved to tape or CD. These electronic logs should be kept as long as a tape/CD is kept. Unfortunately electronic storage media can go bad on the shelf. It will be important later on to know that a file was

successfully copied onto the backup medium. Without a log, a missing file may be confused with a media error.
The second log is manual and records activity. Assign a primary and backup staff member whose job responsibility is to rotate tapes and note any problems or exceptions. Write an entry for successful backups, the date and which tape was utilized. Unfortunately the task of changing tapes and maintaining valid backups can become repetitive and boring. Writing a log every day encourages accountability and accuracy. Such logs also encourage backup personnel to follow procedures and note any difficulties. Keep the written log with the computer or tape unit that performs the backup.
* Monthly and yearly tapes shall be stored off site. GIAC Enterprise has contracted with Iron Mountain for tape pick up and storage. Always check the ID of the pickup operator and only release tapes to: [Individuals to be named at a later date], employees of Iron Mountain. Ensure they sign the activity log for receipt of tapes.
* A fireproof safe shall be used for onsite storage.

A.4 Incident Handling (Hacker/Cracker)

Attacker incidents include any active session or commands executed by an unauthorized person. Examples include an active rlogin or telnet session, an active ftp session, or a successful dial-back attempt. In the case of active hacker/cracker activity, a decision must be made whether to allow the activity to continue while you gather evidence, or to get the hacker/cracker off the system and lock the person out. Since an attacker can do damage and be off the system in a matter of minutes, time is critical when responding to active attacks. This decision must be made by the GIAC Enterprise Information Security Officer or someone he/she designates (i.e., the GIAC Enterprise Security Officer). The decision will be based on the availability of qualified personnel to monitor and observe the hacker/cracker and the level of risk involved.

A.4.1 Notify Appropriate People

Notify the GIAC Enterprise Security Officer as soon as possible. If unable to reach him/her within 5 minutes, contact the backup person. The GIAC Enterprise Security Officer will then be responsible for notifying other appropriate personnel.
The GIAC Enterprise Security Administrator will notify the GIAC Enterprise Security Officer as soon as possible. If unable to reach him within ten minutes, the backup person should be contacted. The GIAC Enterprise Security Officer can make the decision to allow the attacker to continue or to lock the attacker out of the system. Based on the decision, follow the procedures in 2.1 or 2.2 below.
The GIAC Enterprise Security Administrator or Security Officer will notify the GIAC Enterprise Information Security Officer (ISO) within 30 minutes. The GIAC Enterprise ISO will escalate to higher-level management if necessary.

A.4.2 Removal of Hacker/Cracker From the System

A.4.2.1 Snap-shot the System

Make copies of all audit trail information such as system log files, the root history files, and the utmp and wtmp files, and store them in a safe place. Capture process status information in a file and then store the file in a safe place. Move suspicious files to a safe place or archive them and remove them from the system. Also, get a listing of all active network connections. **Log all actions.**

A.4.2.2 Lock Out the Attacker

Kill all active processes for the hacker/cracker and remove any files or programs that he/she may have left on the system. Change passwords for any accounts that were accessed by the hacker/cracker. At this stage, the hacker/cracker should be locked out of the system. **Log all actions.**

A.4.2.3 Restore the System

Restore the system to a normal state. Restore any data or files that the hacker/cracker may have modified. Install patches or fixes to close any security vulnerabilities that the hacker/cracker may have exploited. Inform the appropriate people. All actions taken to restore the system to a normal state should be documented in the log book for this incident.

A.4.2.4 Notify Other Agencies

To be a good Internet citizen, inform outside organizations of the intrusion. Confidential reporting may be made to intrusion@sans.org by the GIAC Enterprise ISO or someone he/she designates. **Log all actions**.

A.4.2.5 Follow-up

After the investigation, a short report describing the incident and actions that were taken should be written by the GIAC Enterprise Security Officer or Security Administrator and distributed to the appropriate people.

A.4.3 Monitoring of Hacker/Cracker Activity

There are no set procedures for monitoring the activity of an attacker. Each incident will be dealt with on a case by case basis. The GIAC Enterprise ISO or the person authorizing the monitoring activity should provide direction to those doing the monitoring. Once the decision has been made to cease monitoring the attacker's activities and have the attacker removed from the system(s), the steps outlined in section A.4.2 above should be followed.

A.4.4 Evidence of Past Incidents

When an incident is discovered after the fact, there is not always a lot of evidence available to identify who the attacker was or how they gained access to the system. If you discover that someone successfully broke into a GIAC Enterprise system, notify the GIAC Enterprise Security Officer within one working day. The GIAC Enterprise Security Officer will be responsible for notifying the appropriate people and investigating the incident.

A.5 Proprietary Information

Due to the nature of GIAC Enterprise Systems Division, there is a large potential for having proprietary information stored on/in GIAC Enterprise computers and resources. Examples of information that would be considered proprietary include vendor source code, benchmark programs, benchmark results, scientific codes, and data sets. Since members of the GIAC Enterprise support staff will have full access to the GIAC Enterprise systems and resources, they may also have access to proprietary information. Members of the GIAC Enterprise support staff are responsible for ensuring that all proprietary information is protected from disclosure or modification. When dealing with proprietary information, members of the GIAC Enterprise support staff should use the following guidelines:

* Ensure appropriate measures are in place for protecting proprietary information.

* Do not attempt to access proprietary information for which you have not been given authorization.
* Do not make copies of proprietary information unless specifically permitted by the owner of the information.
* Do not disclose to third parties the types of proprietary information you can access.

Appendix B – IP Schema

OUTSIDE

	IP	Subnet	Subnet Mask
ISP	206.123.224.6	206.123.224.0/30	255.255.255.252
Router Out ISP	206.123.224.5	206.123.224.0/30	255.255.255.252
Router to FW-1	206.123.224.18	206.123.224.16/28	255.255.255.240
FW-1 to Router	206.123.224.19	206.123.224.16/28	255.255.255.240
Router to VPN	206.123.224.34	206.123.224.32/28	255.255.255.240
VPN to Router	206.123.224.35	206.123.224.32/28	255.255.255.240
VPN to FW-3	206.123.224.50	206.123.224.48/28	255.255.255.240
FW-3 to VPN	206.123.224.51	206.123.224.48/28	255.255.255.240
Router to FW-2	206.123.224.66	206.123.224.64/28	255.255.255.240
FW-2 to Router	206.123.224.67	206.123.224.64/28	255.255.255.240
FW-1 to Switch	206.123.224.82	206.123.224.80/28	255.255.255.240
Switch to FW-1	206.123.224.83	206.123.224.80/28	255.255.255.240
FW-1 to Service	206.123.224.98	206.123.224.96/28	255.255.255.240
WWW	206.123.244.99	206.123.224.96/28	255.255.255.240
DNS	206.123.224.100	206.123.224.96/28	255.255.255.240
Ext Mail	206.123.224.101	206.123.224.96/28	255.255.255.240
IDS	206.123.224.102	206.123.224.96/28	255.255.255.240
Switch to FW-3	206.123.224.114	206.123.224.112/28	255.255.255.240
FW-3 to Switch	206.123.224.115	206.123.224.112/28	255.255.255.240
Web1 to Switch	206.123.224.116	206.123.224.112/28	255.255.255.240
Web2 to Switch	206.123.224.117	206.123.224.112/28	255.255.255.240
Web3 to Switch	206.123.224.118	206.123.224.112/28	255.255.255.240
Web1 to FW-3	206.123.224.130	206.123.224.128/28	255.255.255.240
Web2 to FW-3	206.123.224.131	206.123.224.128/28	255.255.255.240
Web3 to FW-3	206.123.224.132	206.123.224.128/28	255.255.255.240

INSIDE

	IP	Subnet	Subnet Mask
FW-2 to In Router	172.16.1.1	172.16.1.0/30	255.255.255.240
In Router to FW-2	172.16.1.2	172.16.1.0/30	255.255.255.240
FW-3 to In Router	172.16.2.1	172.16.2.0/30	255.255.255.240
In Router to FW-3	172.16.2.2	172.16.2.0/30	255.255.255.240
In Router to Corp	172.16.224.1	172.16.224.0/24	255.255.255.0
Office LAN	224.40 - 224.80	172.16.224.0/24	255.255.255.0
M & S LAN	224.81 - 224.120	172.16.224.0/24	255.255.255.0
R & D LAN	224.121 - 224.160	172.16.224.0/24	255.255.255.0
Mgt LAN	224.161 - 224.200	172.16.224.0/24	255.255.255.0
Service LAN	224.201 - 224.240	172.16.224.0/24	255.255.255.0

Appendix C – Router Configuration

```
!Outside interface
Interface Ethernet0/0
ip address 206.123.224.5 255.255.255.252
ip access-group 130 in
!
!       Private addresses
access-list 130 deny ip 10.0.0.0 0.255.255.255 any log
access-list 130 deny ip 172.16.0.0 0.15.255.255 any log
access-list 130 deny ip 192.168.0.0 0.0.255.255 any log
!
!       IANA Reserved Address Space
access-list 130 deny ip host 0.0.0.0 any log
access-list 130 deny ip 0.0.0.0 0.255.255.255 any log
access-list 130 deny ip 1.0.0.0 0.255.255.255 any log
access-list 130 deny ip 2.0.0.0 0.255.255.255 any log
access-list 130 deny ip 5.0.0.0 0.255.255.255 any log
access-list 130 deny ip 7.0.0.0 0.255.255.255 any log
access-list 130 deny ip 23.0.0.0 0.255.255.255 any log
access-list 130 deny ip 27.0.0.0 0.255.255.255 any log
access-list 130 deny ip 31.0.0.0 0.255.255.255 any log
access-list 130 deny ip 36.0.0.0 0.255.255.255 any log
access-list 130 deny ip 37.0.0.0 0.255.255.255 any log
access-list 130 deny ip 39.0.0.0 0.255.255.255 any log
access-list 130 deny ip 41.0.0.0 0.255.255.255 any log
access-list 130 deny ip 42.0.0.0 0.255.255.255 any log
access-list 130 deny ip 58.0.0.0 0.255.255.255 any log
access-list 130 deny ip 59.0.0.0 0.255.255.255 any log
access-list 130 deny ip 60.0.0.0 0.255.255.255 any log
access-list 130 deny ip 69.0.0.0 0.255.255.255 any log
access-list 130 deny ip 70.0.0.0 0.255.255.255 any log
access-list 130 deny ip 71.0.0.0 0.255.255.255 any log
access-list 130 deny ip 72.0.0.0 0.255.255.255 any log
access-list 130 deny ip 73.0.0.0 0.255.255.255 any log
access-list 130 deny ip 74.0.0.0 0.255.255.255 any log
access-list 130 deny ip 75.0.0.0 0.255.255.255 any log
access-list 130 deny ip 76.0.0.0 0.255.255.255 any log
access-list 130 deny ip 77.0.0.0 0.255.255.255 any log
access-list 130 deny ip 78.0.0.0 0.255.255.255 any log
access-list 130 deny ip 79.0.0.0 0.255.255.255 any log
access-list 130 deny ip 82.0.0.0 0.255.255.255 any log
access-list 130 deny ip 83.0.0.0 0.255.255.255 any log
```

```
access-list 130 deny ip 84.0.0.0 0.255.255.255 any log
access-list 130 deny ip 85.0.0.0 0.255.255.255 any log
access-list 130 deny ip 86.0.0.0 0.255.255.255 any log
access-list 130 deny ip 87.0.0.0 0.255.255.255 any log
access-list 130 deny ip 88.0.0.0 0.255.255.255 any log
access-list 130 deny ip 89.0.0.0 0.255.255.255 any log
access-list 130 deny ip 90.0.0.0 0.255.255.255 any log
access-list 130 deny ip 91.0.0.0 0.255.255.255 any log
access-list 130 deny ip 82.0.0.0 0.255.255.255 any log
access-list 130 deny ip 93.0.0.0 0.255.255.255 any log
access-list 130 deny ip 94.0.0.0 0.255.255.255 any log
access-list 130 deny ip 95.0.0.0 0.255.255.255 any log
access-list 130 deny ip 96.0.0.0 0.255.255.255 any log
access-list 130 deny ip 97.0.0.0 0.255.255.255 any log
access-list 130 deny ip 98.0.0.0 0.255.255.255 any log
access-list 130 deny ip 99.0.0.0 0.255.255.255 any log
access-list 130 deny ip 100.0.0.0 0.255.255.255 any log
access-list 130 deny ip 101.0.0.0 0.255.255.255 any log
access-list 130 deny ip 102.0.0.0 0.255.255.255 any log
access-list 130 deny ip 103.0.0.0 0.255.255.255 any log
access-list 130 deny ip 104.0.0.0 0.255.255.255 any log
access-list 130 deny ip 105.0.0.0 0.255.255.255 any log
access-list 130 deny ip 106.0.0.0 0.255.255.255 any log
access-list 130 deny ip 107.0.0.0 0.255.255.255 any log
access-list 130 deny ip 108.0.0.0 0.255.255.255 any log
access-list 130 deny ip 109.0.0.0 0.255.255.255 any log
access-list 130 deny ip 110.0.0.0 0.255.255.255 any log
access-list 130 deny ip 111.0.0.0 0.255.255.255 any log
access-list 130 deny ip 112.0.0.0 0.255.255.255 any log
access-list 130 deny ip 113.0.0.0 0.255.255.255 any log
access-list 130 deny ip 114.0.0.0 0.255.255.255 any log
access-list 130 deny ip 115.0.0.0 0.255.255.255 any log
access-list 130 deny ip 116.0.0.0 0.255.255.255 any log
access-list 130 deny ip 117.0.0.0 0.255.255.255 any log
access-list 130 deny ip 118.0.0.0 0.255.255.255 any log
access-list 130 deny ip 119.0.0.0 0.255.255.255 any log
access-list 130 deny ip 120.0.0.0 0.255.255.255 any log
access-list 130 deny ip 121.0.0.0 0.255.255.255 any log
access-list 130 deny ip 122.0.0.0 0.255.255.255 any log
access-list 130 deny ip 123.0.0.0 0.255.255.255 any log
access-list 130 deny ip 124.0.0.0 0.255.255.255 any log
access-list 130 deny ip 125.0.0.0 0.255.255.255 any log
access-list 130 deny ip 126.0.0.0 0.255.255.255 any log
access-list 130 deny ip 169.254.0.0 0.0.255.255 any log
access-list 130 deny ip 192.0.2.0 0.0.0.255 any log
access-list 130 deny ip 197.0.0.0 0.0.255.255 any log
```

```
access-list 130 deny ip 206.123.224.0 0.0.0.31 any log
!
!       Telnet from Internet
access-list 130 deny tcp any any range ftp telnet log
!
!       ICMP Message and Traceroute
access-list 130 deny icmp any any echo log
access-list 130 deny icmp any any redirect log
access-list 130 deny icmp any any mask-request log
access-list 130 deny icmp any any time-exceeded
access-list 130 deny udp any any range 33400 34400 log
!
!       TCP SYN Attack
access-list 130 permit tcp any 206.123.224.0 0.255.255.255 establish
!
!       Land Attack
access-list 130 deny ip host 206.123.224.5 host 206.123.224.5 log
!
!       Smurf Attack
access-list 130 deny ip any host 206.123.224.255 log
access-list 130 deny ip any host 206.123.224.0 log
!
!       Buffer Overflow
access-list 130 deny tcp any any 111 log
access-list 130 deny tcp any any 551 log
!
!       Multicast Addresses
access-list 130 deny ip 224.0.0.0 31.255.255.255 any log
!
!       SNMP Traffic
access-list 130 deny udp any any range snmp snmptrap log
!
!       DHCP Auto Config
access-list 130 deny ip 169.254.0.0 0.0.255.255 any log
access-list 130 deny ip 192.0.2.0 0.0.0.255 any log
!
!       Loopback Address
access-list 130 deny ip 127.0.0.0 0.255.255.255 any log
!
!       Allowing web traffic to web servers on port 80 and 443
access-list 130 permit tcp any 206.123.224.114 0.0.0.0 eq http
access-list 130 permit tcp any 206.123.224.114 0.0.0.0 eq 443
!
!       Netbios
access-list 130 deny tcp any any range 135 139 log
access-list 130 deny tcp any any eq 445 log
```

```
access-list 130 deny udp any any eq 135 log
access-list 130 deny udp any any range 137 138 log
access-list 130 deny udp any any eq 445 log
!
!       Other known Trojan
access-list 130 deny udp any eq 34555 log
access-list 130 deny udp any eq 27573 log
access-list 130 deny udp any eq 27444 log
access-list 130 deny udp any eq 27374 log
!
!       Log Everything Else
access-list 130 deny any any log
!
!
Interface Ethernet0/1
ip address 206.123.224.18 255.255.255.240
ip access-group 131 in
!
!       Anti-Spoofing
access-list 131 permit ip 206.123.224.0 0.0.0.31 any
access-list 131 deny ip any any
!
!
Interface Ethernet0/2
ip address 206.123.224.34 255.255.255.240
ip access-group 141 in
!
!       Allow VPN Traffic
access-list 141 permit 50 any host 206.123.224.35 log
access-list 141 permit 51 any host 206.123.224.35 log
access-list 141 permit 500 any host 206.123.224.35 log
access-list 141 deny ip any any log
!
!
Interface Ethernet0/3
ip address 206.123.224.66 255.255.255.240
ip access-group 151 in
!
!       Allow traffic to DNS Mail and Web Traffic
access-list 151 permit tcp host 206.123.224.99 eq http
access-list 151 permit tcp host 206.123.224.99 eq 443
access-list 151 permit udp host 206.123.224.100 eq 53
access-list 151 permit tcp host 206.123.224.101 eq 25
access-list 151 deny any any log
!
!
```

```
!       Prevent CDP
no cdp run
!
!       Disable Small Services
no service tcp-small-servers
no service udp-small-servers
!
!       Disable Bootp and Finger
!
no service finger
no ip bootp server
!
!       Disable HTTP and SNMP
!
no ip http server
no snmp-server enable traps
no snmp-system-shutdown
no snmp-server trap-auth
no snmp
!
!       Disable Source Routing Classless IP
!
no ip source-route
no ip classless
!
!       Disable Configuration auto-loading
!
no boot network
no service config
!
!       Misc services to be disabled
!
no ip redirects
no ip proxy-arp
no cdp enable
ntp disable
no ip directed-broadcast
no ip subnet-zero
no ip unreachable
no service pad
no identd
no logging console
!
!       Shutting down unneeded services at interface on the router
!
interface eth0/4
```

```
shutdown
!
!         Logging to Syslog
logging buffered 10000
logging trap debugging
logging 172.16.224.161
service timestamp debug datetime localtime show timezone msec
```

Appendix D

Network	#Dups	#Incidents	Registered	at	Home AS
12.17.161.0/24	13	0	11/29/2000	19:05	not-analyzed
129.78.64.0/24	37	0	8/13/1998	8:54	AS7570
148.233.6.159/32	1	0	10/20/2000	0:53	not-analyzed
155.64.107.0/24	11	0	2/20/1999	9:58	AS1239
159.14.24.0/24	20	0	2/20/1999	9:39	AS2914
164.106.163.0/24	14	0	2/20/1999	10:11	AS7066
168.180.213.0/24	10	0	2/18/1999	10:47	AS210
192.220.134.0/24	19	0	2/20/1999	9:38	AS685
194.170.103.255/32	1	0	10/27/2000	2:00	not-analyzed
198.253.187.0/24	16	0	2/20/1999	9:34	AS22
199.98.24.0/24	13	0	2/18/1999	11:09	AS6199
203.85.34.0/24	10	0	2/18/1999	13:43	AS4058
204.158.83.0/24	27	0	2/20/1999	10:09	AS3354
204.193.121.0/24	19	0	2/20/1999	8:54	AS701
205.163.203.0/24	3	0	10/6/2000	6:37	not-analyzed
206.210.247.0/24	6	0	2/20/1999	8:56	AS5673
207.236.217.0/24	7	0	2/20/1999	9:42	AS577
208.196.38.0/24	9	0	2/20/1999	10:23	AS7046
209.38.124.255/32	2	0	11/1/2000	22:08	not-analyzed
209.38.126.0/24	7	0	11/5/2000	16:45	not-analyzed
209.38.126.0/32	7	0	11/1/2000	22:08	not-analyzed
209.38.126.255/32	7	0	11/1/2000	22:08	not-analyzed
209.39.53.255/32	9	0	10/13/2000	8:45	not-analyzed
209.39.150.0/24	7	0	10/7/2000	17:20	not-analyzed
209.39.150.255/32	4	0	11/1/2000	22:17	not-analyzed
209.44.28.255/32	9	0	10/13/2000	8:27	not-analyzed
209.44.64.255/32	4	0	10/13/2000	8:25	not-analyzed
209.44.67.255/32	4	0	11/1/2000	22:39	not-analyzed
209.44.68.252/30	6	0	10/5/2000	5:06	not-analyzed
209.44.68.255/32	6	0	11/1/2000	22:39	not-analyzed
209.46.65.0/24	10	0	9/4/2000	7:31	not-analyzed
209.46.65.255/32	8	0	10/13/2000	8:15	not-analyzed
209.47.47.0/24	9	0	6/22/1998	18:58	AS816
209.47.49.0/24	3	0	8/28/2000	20:42	not-analyzed
209.47.49.255/32	4	0	10/13/2000	8:06	not-analyzed
209.47.51.255/32	6	0	10/13/2000	8:04	not-analyzed
209.47.55.0/32	13	0	11/1/2000	22:51	not-analyzed
209.47.58.0/24	11	0	9/11/2000	0:09	not-analyzed
209.48.218.255/32	13	0	10/13/2000	8:00	not-analyzed
209.49.5.0/32	4	0	10/13/2000	7:57	not-analyzed
209.49.5.255/32	4	0	10/13/2000	7:57	not-analyzed
209.49.136.0/24	10	0	10/27/2000	16:56	not-analyzed
209.49.136.0/32	11	0	11/1/2000	23:03	not-analyzed
209.241.162.0/24	27	0	2/20/1999	8:51	AS701
210.111.77.255/32	10	0	10/13/2000	4:40	not-analyzed

210.111.78.0/32	10	0	10/13/2000	4:40	not-analyzed
210.111.78.255/32	10	0	10/13/2000	4:40	not-analyzed
212.1.130.0/24	38	0	2/20/1999	9:41	AS9105

References

Address Allocation for Private Internets, http://www.rfc-editor.org/

Stallion Technologies, "What is Internet-based Virtual Private Networking?" (25/2/01) http://www.stallion.com/html/solutions/vpn-overview.html

Lee Chae, Article, "Virtual Private Networks" (10/01/98) http://www.networkmagazine.com/article/NMG20000727S0029/2

Jeff Tyson, Technical Paper, "How Virtual Private Networks Work" (2001) http://www.howstuffworks.com/vpn.htm

Andrew Brandt and Alexandra Krasne, Article, "How It Works: Encryption" (14/02/00) http://www.pcworld.com/hereshow/article/0,aid,15230,00.asp

Robert Moskowitz, Article – "What is a Virtual Private Network?" 23/02/01 http://www.networkcomputing.com/905/905colmoskowitz.html

Ruixi Yaun and W. Timothy Strayer, Virtual Private Networks, Technologies and Solutions (2001)

Harold F. Tipton and Micki Krause, Information Security Management, (2000)

Spitzner, Lance. "Building Your Firewall Rulebase". 26 January 2000. http://www.enteract.com/~lspitz/rules.html

Networking Working Group, A Framework for IP Based Virtual Private Network, (2000)

Cisco Secure PIX 515 Firewall, http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pix51_ds.htm

Eric Cole, Hackers Beware, New Riders Publishing 2002

Cisco Systems. http://www.cisco.com

Spitzner, Lance. "Understanding The FW-1 State Table". 29 November 2000 http://www.enteract.com/~lspitz/fwtable.html

SANS Institute. Track 2 – Firewalls, Perimeter Protection, and Virtual Private Networks

SANS Defense In-Depth module 1, SANS Institute

Stevens, W. Richard. TCP/IP Illustrated, Volume 1 The Protocols

Nessus Vulnerability Scanner, http://www.nessus.org

Cisco IOS Security Configuration Guide, Release 12.1, http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/index.htm

Common Vulnerabilities and Exposures, http://www.cve.mitre.org, The MITRE Corporation

SANS/FBI Top 20 List, http://www.sans.org/top20.htm

Phan, Jim "SANS GIAC Level 2: GCFW – Firewalls, Perimeter Protection, and VPNs Practical Assignment". http://www.sans.org/y2k/practical/Jim_Phan_GCFW.doc

Firewalking, Cambridge Technology Partners, http://www.packetfactory.net/Projects/Firewalk/firewalk-final.html