Global Information Assurance Certification Paper

SANS GIAC Certified Firewall Analyst Practical Assignment

GWFC Version 1.7

Authored by:
Bernard Russell Beland

Date submitted: May 21, 2002

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

The Art of War; by Sun Tzu, edited by James Clavell, Delacorte Press

Table of Contents

Introduction

This document represents the practical assignment given by Global Information Assurance Certification (GIAC) to demonstrate my understanding of the technologies presented by the SANS Institute course "track-2: Firewalls, Perimeter Protection, and VPN's". The intent of submitting this document is earning the GIAC certification of GCFW. Briefly, it is a four-part assignment that involves designing the security architecture for a fictitious company named GIAC Enterprises. Included with the design are definitions of the security policy, an implementation tutorial, and methods for testing and auditing the design. The final part involves finding weaknesses in the architecture of a previously submitted assignment. The complete description of the assignment can be found on the www.GIAC.org web page as the GCFW practical assignment version 1.7.

Part 1 – Define the Security Architecture

Description of GIAC Enterprises and Philosophy

GIAC Enterprises is a wholesale business for fortune cookie sayings. Its business is conducted entirely online as an e-business. Since they sell no physical product, information transfer is their sole competency and thus their bread and butter. With that background the company has developed certain philosophies for survival. The first being: "if the system is down the company is doing no business". An online business that is 'offline' is even worse off than merely doing no business at all. Customers will swiftly lose faith in an e-tailer that cannot keep its system available at all times. Secondly, they must be able to protect the integrity of the data. Corrupted data is useless to customers and would likely cause them to seek other supply sources.

Armed with these basic tenets GIAC Enterprises is prepared to invest whatever is required to keep their systems online and secure. Realizing of course that certain reasonable limits exist for this expectation, it is recognized that diminishing returns on investment can occur for expenditures on the security architecture. No 100% foolproof system could exist using this business model.

Overview of Business Operations and Environment

The operational model for GIAC Enterprises has groups for actors. The first group is employees that connect to the network on the premises via the corporate intranet. Whereas employees are presumed a trusted entity that will act responsibly, there are still several policies that should be enacted. Some of these include limiting

internal access only to required resources, installing virus-scanning tools, and filtering outbound access. These policies and their reasoning will be described at length in Part-2 of this assignment. In addition to internal access, there will be employees who need to get into the network from either their homes or from any remote location with access to the public Internet. They are called telecommuters or mobile employees.

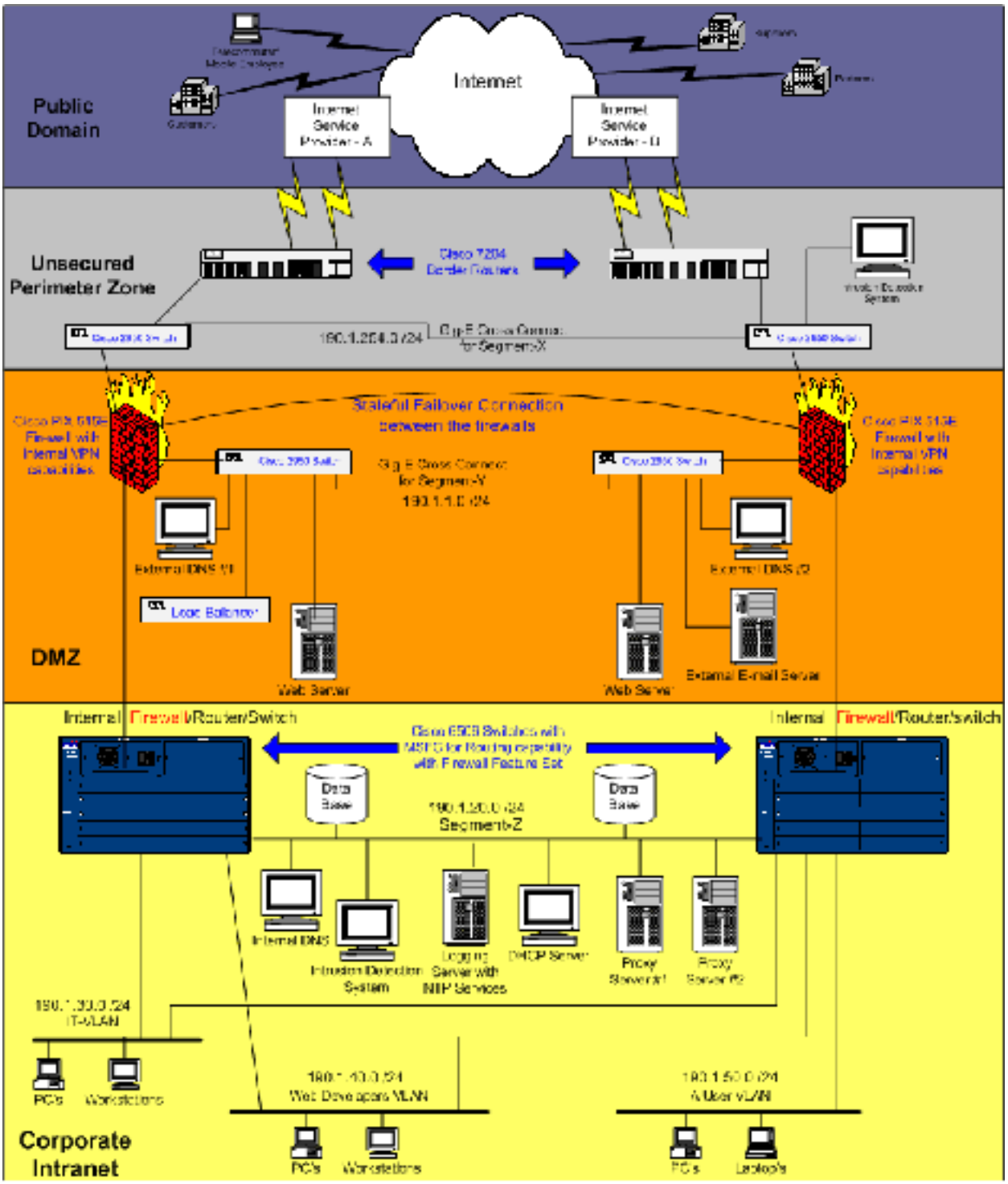
The next group that requires access is the customers. They are the companies or individuals who buy our fortune cookie sayings online via our web site. Their access must be secure, timely, and made available at all times. This is mission critical. Suppliers are the next group that we need to consider. These are companies or individuals that supply us with the fortune cookie sayings for bulk resale. It is assumed that GIAC Enterprises has established a business relationship with its suppliers and that we have a trusted working association with them. This means that we work cooperatively with them in establishing network connectivity for our mutual benefit. However, both companies realize the prudence of restricting access to an 'as need' basis and of securing and filtering content. Policies to establish these restrictions will be detailed in Part-2 of this assignment.

Lastly are our partners. They are international companies that translate and resell our fortune cookie sayings. Like our customers and suppliers, they will transact business with us over the Internet. And like our suppliers, it is presupposed that we have signed some sort of business contract with them before we establish network connectivity. Some additional things to be aware of with international companies are export restrictions and encryption standards. Both our government and foreign governments have restrictions regarding encryption. In some countries, the voice and data networks are government controlled. This can present several non-technical and frustrating problems for network engineers! Again, these issues will be addressed in subsequent sections.

GIAC Enterprises Network Diagram

The network diagram shown below (Figure-1) is a logical depiction of GIAC Enterprise's security infrastructure. Each zone and component of the drawing is described in detail in the sections that ensue. In order to avoid overly cluttering the diagram some information, such as device IP addressing, was left off the drawing but will be discussed at length in the following sections as well.

Figure-1



Definition of the Public Domain and its Components

This area of the diagram represents the public network that is freely available to everyone. It is out of GIAC Enterprises control and indeed any other corporation's control as well. It is considered to be totally insecure. The fact that I placed partner and supplier companies in this domain is not meant to imply that their networks are insecure, but rather that information exchanged between our companies must traverse this unprotected zone.

Internet

The Internet is the world's largest publicly accessible communications network. It is a globally connected collection of hardware and software that enables voice and data networking. Components of the Internet may be owned by public utilities, domestic and foreign governments, the military and private companies. It is in the public domain and has few regulations regarding its access or content. Information transmitted through the Internet can traverse through several entities before reaching its destination. Anyone connected to the Internet between you and your destination can observe and even alter your data transmission! These reasons are why it is considered to be extremely insecure.

Given its convenience and usefulness though, it has become a necessary way of life for transacting business. Thus it becomes necessary to augment its utility with your own security measures when using it.

ISP

An Internet Service Provider (ISP) is a company provides connectivity to the Internet. Generally ISP's have direct access to the Internet backbone and can provide you with a variety of bandwidth options. ISP's can, however, be daisy chained through other ISP's thereby putting the end customer farther away from the backbone. This can produce more latency as well enable more potential points of failure.

Telecommuters and Mobile Employees

External employees will connect to the GIAC corporate network across the Internet using the TCP/IP suite of protocols. The tools they will use will provided to them on GIAC supplied laptop computers. The laptops will be pre-loaded with VPN client software that is configured for secure and encrypted communication with the

corporate VPN services located on the DMZ Firewalls. In addition to having physical possession of the laptop with the configured VPN client, each user will need to authenticate their identity using an issued signon and password combination. A signon and password policy is defined later in this report (see Appendix A: Signon and Password Policy).

Each laptop will also come loaded with corporate licensed and configured personal firewall software and virus scanning software. This helps protect the mobile laptops from computer viruses and Trojan horse software. Since the laptops will be Internet connected they will be susceptible to these attacks. This in turn helps protect the corporate intranet when those mobile users do connect back inside the DMZ. When remote users do connect into the office a script will be run to update the laptop with the latest virus protection files.

An informative comparison on personal firewalls can be found at: http://www.pcmag.com\firewalls. I recommend an integrated suite package such as those made by Norton or McAfee for ease of corporate management and integrated virus protection.

Before receiving a laptop, each employee will have to complete training on safe usage practices. Some items covered would include physically safeguarding the laptop, use of BIOS and system passwords, use of screen saver with password lockout, the opening of e-mail from unknown sources, the running or saving of executable attachments, and safe Internet usage. Employees will also receive training on how to avoid social engineering attacks i.e. not giving out information, access, or passwords to other people. Internal employees will get similar training as documented in an upcoming section.

One final note for mobile users, they will have the same access (or restriction thereof) to resources that they would have if they were physically in the office. That is, access to some resources, services and parts of the intranet are on an "as-need" basis. What these restrictions are and how they are implemented are defined in the sections: "Definition of the Corporate Intranet and its Components" and Part-2 of the assignment, respectively.

Customers

Being an online company, our customers will access our services via the World Wide Web. Our customers need only have a browser that supports a minimum of 128-bit SSLv3 encryption and a credit card. Both Microsoft's Internet Explorer and Netscape's Navigator browser have had built in support for this level of security for a couple of years now. Once credit card information has been verified through an

online billing system, the customer will be issued a certificate that will enable them to download a file containing the purchased amount of fortune cookie sayings.

Suppliers

Once a business relationship has been established, our IT department can work with the engineers of our suppliers company to establish a secure tunnel. Tunneling to our firewall can easily be setup with the VPN technology built into our Cisco firewalls. Information on our firewalls and VPN infrastructure is discussed in a subsequent section. An alternative to using a VPN solution would be to use leased lines or frame relay circuits. However this requires expensive equipment, recurring monthly line charges, and usually requires six to eight weeks to setup time. For more information on the cost savings advantages, see an online report prepared for Cisco Systems by Gartner Consulting. The URL link is:
http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/news/vgano_ai.pdf

Partners

Our corporate partners will enjoy the same arrangement for connectivity as our suppliers. That is; a secure VPN tunnel between our firewall and their terminating network equipment. It should be noted, however, that this secure tunnel is not our only line of security. While we will have business contracts with our partners and suppliers and at least some level of trust with them, caution must still be observed because they will have privileged access to our network via the secured tunnel! Our network could be jeopardized if their security became compromised; they had a corporate spy, or even an unhappy engineer. These are situations that aren't exactly unheard of. Therefore we will rely on firewall/router rules and application level security for extra layers of security.

By definition, our partners will by located in foreign countries. Many countries own, operate, control, monitor, or regulate the communication lines in their country and have strict laws about encryption. Moreover, the U.S. has export laws regarding encryption technology. These should be investigated as part of establishing the business relationship. "For more information on international encryption regulations see: http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm " [1] and also
http://www.cisco.com/wwl/export/crypto/

Definition of the Unsecured Perimeter Zone and its Components

This zone is called unsecured because it sits outside of the firewall. Its components reside safely on corporate premises and enjoy some level of trust with the directly connected ISP. Yet they remain the most visible targets to the outside world and so are directly in the line of fire.

Border Routers

The two border routers that connect directly to our ISP's will be Cisco model 7204's. As of this writing, the current Cisco preferred GPD release of the IOS is version 12.0. We will fully load the routers processor memory to 256mb DRAM and the flash memory to 128mb. More memory for the processor always improves throughput and makes you that much less susceptible to DOS attacks. Flash memory is handy to have for making backups of the current and previous version of the IOS and of the running configuration.

(NOTE: for those reasons it is recommended that all the mission critical network equipment be maxed out on memory. I will not keep retyping those reasons but the amount of memory on all subsequent equipment will be the maximum amount.)

Border routers provide an important first line of defense in our layered security approach. By using packet filtering at the perimeter, the border routers can prevent IP spoofing, some denial of service attacks, and intercept some other types of attacks before they reach the firewall. This saves firewall processing, internal bandwidth, and provides another hurdle an attacker must clear.

The Cisco 7204 is my choice for a variety of reasons. First, it has impressive processor speed of 400,000 packets per second. Next, it has a huge variety of interface support that gives us flexibility for migration. And lastly it is a scalable solution that supports future growth and easy termination of new or acquired offices. Redundancy of design is another key element here. Having two routers greatly minimizes the chance of customer downtime, due to hardware failure, denial of service attacks, or sabotage.

In addition to having two border routers, each router is connected to a different ISP via different physical paths leading into the building. This helps reduce outages caused by the ISP or by accidental line cuts. Each router is equipped with redundant power supply modules and each module will be plugged into a different electrical circuit.

(NOTE: all circuits that feed networking gear will be connected to an uninterruptible power source backup.)

The initial design calls for two T1 lines to terminate into each router. Each T1 line has a speed of 1.54Mb times 4 gives an effective throughput of slightly over 6Mb. This amount of bandwidth should meet the business requirements. Of course, the line utilization should be monitored. If this proves to be a bottleneck then more T1 lines can be added to the border routers or even an upgrade to T3's.

For more information on the Cisco 7204, the following links provide a staggering amount of content:

http://www.cisco.com/univercd/cc/td/doc/product/core/7204/index.htm
http://www.cisco.com/univercd/cc/td/doc/pcat/7200.htm

Picture-1

Switches and Segment-X

The switches in this zone will be Cisco Catalyst switches model 2950G-24 (EI). The Cisco IOS software version they run will be Release 12.1(6)EA2c. They provide 24 ethernet ports of 10/100 MB speed and Gigabit uplink ports. The two switches will be linked together by the Gigabit ports and will redundantly define a single segment that for reference is named Segment-X. The IP network number will be discussed in Part-2 of this paper. For further backup, each border router will connect to a different switch.

Picture-2

Reference the following link for more information on the Cisco Catalyst 2950 series switches: http://www.cisco.com/warp/public/cc/pd/si/casi/ca2950/index.shtml

Intrusion Detection System

The selection for an intrusion detection system (IDS) in the perimeter zone is the Cisco Secure IDS 4210 Sensor. It is a network appliance that has a 566MHz Celeron processor with 256MB ram.

Placing an IDS in front of the firewall aids in detecting attacks before the firewall drops the packets and provides us with a more complete log. The IDS can detect, log and alert us to known attack patterns. Alerts can take the form of a message to

a network monitor or a page to an on-call technician. This information allows us to take technical and/or legal action.

Freeware does exist that can fulfill this function, but you still need to purchase a suitable hardware platform and operating system to run it on. Furthermore, the company founders are leery of freeware that may fade from existence or run out of support. Besides, with the amount of Cisco gear we are purchasing, we should be getting a sizable discount from our sales representative.

Picture-3

For complete product information reference:

http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/prodlit/ids41_ds.htm

Definition of the DMZ and its Components

The demilitarized zone (DMZ) as it is called, is a buffer zone between the unsecured networks outside of the organization and our internal protected network. Devices in this zone are on premises and physically secured. These devices also reside behind our firewalls to help secure them from hostilities coming from through the Internet. However, these devices run services that are meant to be publicly accessible. This exposure will always produce some degree of vulnerability. This makes it prudent to equip the DMZ with only the minimum amount of devices and services as is necessary to fulfill the business requirements.

Firewalls and the Failover Connection

A firewall is a collection of hardware, software, or both working in concert to enforce an access control policy. It serves as a single point of access between your local network and an outside foreign network (usually the Internet). The access control policy dictates what types of information are allowed to flow between the two networks. Its main purpose is to protect your private network and information stored upon it from intruders.

The strategy it uses to implement this policy is to deny all traffic not specifically permitted by using dynamic packet filtering. Dynamic packet filtering checks the header information of each packet and can filter traffic based on the source address, destination address, and port number it contains. Filtering based on source/destination address allows you to prevent traffic between particular networks

and hosts. Port number filtering lets you control traffic based on an IP-protocol service: (e.g. SNMP, Telnet, etc…). In addition to filtering on packet header information, dynamic packet filtering can create state tables. State table traffic-control enables the firewall to ensure that all inbound packets from the Internet are in response to an outbound request.

The make and model for our firewalls will the Cisco PIX 515E firewall. It runs on and Intel Celeron 433-MHz processor and will have 64MB of SDRAM. This configuration will support clear text throughput of 188 Mbps and 168-bit 3DES IPSec VPN throughput of 63 Mbps. The operating system will be Cisco IOS version 6.2(1). This is a secure embedded O/S with no UNIX or Windows O/S security holes. For redundancy these firewalls support Stateful failover and will be cabled to support that functionality. According to the specifications, this is well suited to support a small to medium sized business, of which our company is classified. As the diagram depicts each firewall will have three active ethernet ports.

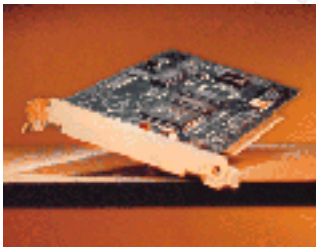
Picture-4

This information and more can be found on the Cisco web site at the following links:

http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/index.shtml
http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/p515e_ds.htm
http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/tech/nat_wp.htm

Our firewalls will also serve as the termination point for our VPN services. In order to offload this work from the firewall's main processor, the PIX firewall will be equipped with the Cisco VPN Accelerator Card. This hardware add-on has its own processor, random access memory, and software specifically optimized to handle the intensive IPSec encryption/decryption requirements. This increases the performance of both the firewall and VPN services.

Picture-5



For more specifications visit:
http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/vac_ds.htm

Switches and Segment-Y

The switches here will be Cisco Catalyst switches model 2950G-24 (EI). The Cisco IOS software version they run will be Release 12.1(6)EA2c. They are identical to the switches located in Unsecured Perimeter Zone and have the same specs and links to information on the web. They differ in that they will be defining a different segment located in the DMZ. The IP address and policies concerning Segment-Y are explained in Part-2 of this paper.

External DNS Servers

Domain name services (DNS) provide a convenient way for customers to access Internet resources by mapping the resource name to the cumbersome IP address. "DNS is defined in RFC-1033."[2] This allows the customer to enter that easy name into their web browser instead of having to know the desired IP address. For example, they could enter "Cisco. COM" versus an IP address of 171.69.2.132.

For DNS we will employ a split approach using both an internal and external DNS server. The external DNS server will only list entries for those devices and services on our network that we want the public to be able to access. Conversely the internal DNS will have a host table containing entries for devices on the corporate intranet. These internal resources are only available to people connected to the internal network.

"To implement of DNS, we will utilize Berkley Internet Name Domain (BIND). The latest release is BIND Version-9.2.0. A release candidate (vesion-9.2.1rc2) is available that patches several bugs and should be applied."
http://www.isc.org/products/BIND/

Again, since we are an e-commerce business, it behooves us to build redundancy into our design for all mission critical systems. This is why there are two external DNS servers each connected to a different switch. A policy defining who can access these servers and do zone transfers is written in Part-2 of this paper.

Load Balancer

As the name suggests, the function of a load balancer is to evenly distribute the traffic. In this case, it will balance the incoming web requests between our web servers. Generally speaking, load balancers are not security devices unless you wish to argue that they would slow down a denial of service attack. Nor are they a mission critical device. This is why we don't have need for redundancy for this

service. Yet they are useful devices for an e-commerce business that wants to maximize its efficiency and availability.

Picture-6

This load balancer, Equalizer by Coyote Point Systems Inc., should fit our needs. It is a low cost solution that can easily cover our expected bandwidth and number of servers.

For more product information see:
http://www.coyotepoint.com/equalizer.shtml
http://www.coyotepoint.com/

For an industry write up on this product, reference this article:
http://www.pcmag.com/article/0,2997,s=1470&a=3566,00.asp

Web Servers

Our selection for web servers will be IBM RS6000 Model B50. They are rack mountable units at a modest cost of around $4,000. They run on 375MHz PowerPC 604e processors with 1MB L2-cache and 256MB SDRAM. The provided operating system is AIX version 4.3.3. AIX is a Unix clone and, in my opinion, is far more stable an operating than any of the ones provided by Microsoft. There are two web servers and each will be connected to a separate switch. Another precaution taken here is that the database servers are kept separate form the web servers, thus even if the web servers get compromised the database is still secured on the intranet. Additional guidelines (the following checklist is taken from book reference number 6) for the application server:

"• Remove all unnecessary server software that's not specifically for operational purposes. This may include:

- Language compilers
- Perl libraries
- Administrative utilities
- Factory –supplied log-ins and passwords.

• On any open port not specifically configured for incoming requests, firewalls should disallow:

- FTP
- TFTP
- Telnet
- Requests

• Don't operate software such as FTP, TFTP, Telnet or e-mail systems on any special-purpose server or Web server hardware. Rather, dedicate a separate system for those uses that you can adequately control.

• Whenever remote operations (such as telnet and xterm) are needed, make sure the Secured Socket Handler (SSH) and Secure Copy (SCP) are used.

• Make sure your Web server software is protected against hostile browsers; apply patches to the software as rapidly as possible when you discover and correct new vulnerabilities.

• As much as possible, set up your servers to provide unique functions and capitalize on the distributed nature of the network." [6]

Picture-7

For more detailed information on this model of RS6000 and of the AIX operation system, reference the following links:

http://commerce.www.ibm.com/content/home/shop_ShopIBM/en_US/eServer/pSeries/entry/B50_7046B50B.html
http://commerce.www.ibm.com/content/home/shop_ShopIBM/en_US/eServer/pSeries/entry/B50.html
http://www-1.ibm.com/servers/aix/products/aixos/

External E-mail Server

The external e-mail server is a store-and-forward gateway device for electronic mail that enters or exist our corporate network via the Internet. The E-mail server is not part of the security architecture but rather a resource like the web servers that must be protected. E-mail is now a necessary part of business with its own special security challenges. E-mail utilizes specific TCP/IP ports that are well known to hackers, as well as being an effective method for spreading viruses.

Microsoft Exchange 2000 with service pack 2 will be the server software running on a Microsoft Windows 2000 server. MS Exchange 2000 has a number of built in security features including virus scanning and disabling of executable attachments. Further security for this resource is provided in Part 2 of this paper. For more information on the Microsoft Exchange 2000 server and some of its security features access the following web sites:

http://www.microsoft.com/exchange/techinfo/default.asp
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/mailexch/default.asp

Definition of the Corporate Intranet and its Components

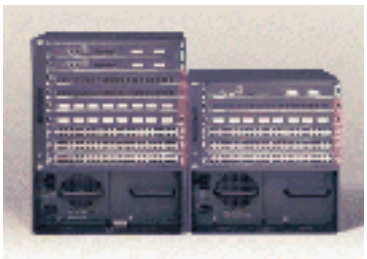
The corporate intranet is the most secured and trusted zone in the design. It is the network physically under our control and the most protected from access by threats from outside the company. The intranet is what all the employees connect to in order to work and it also houses all of the hardware, software, and information vital to running the company. This does not mean it is 100% secure or free from evil forces. On the contrary, we will enact several measures internally to minimize risk to corporate assets and information.

Switches with Route Processors

Cisco Catalyst 6506 switches will power our internal network with supervisor-2 engines equipped with the multilayer switch feature card (MSFC) 2. The MSFC card allows us to perform layer-3 control, routing, on this device. Since the devices are on the border of the DMZ and the intranet, they serve as an internal firewall. This is possible by using either ACL's on the interfaces or by load the Cisco firewall feature set onto the operating system.

The operating system software will be Cisco IOS 12.0(7)XE enterprise edition. The MSFC will run Cisco IOS version 12.0.3.XE enterprise edition and will be loaded with its own 512MB ECC DRAM. The supervisor engine runs on a 250MHz RM7000 RISC processor. The Catalyst 6506 has redundant power supplies and supports very high port density.

Picture-8



Picture-9

Picture-8 is the supervisor engine module that fits into the top slot of the Catalyst 6506 switch (on the right in picture-9). For complete information on these products reference the following web links:

http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/index.shtml
http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/supcc_ov.htm

Segment-Z

The Catalyst switches redundantly define this ethernet segment. It represents a backend segment that contains network equipment and services necessary to run the business. We will discuss the IP addressing scheme and particular security policies of this segment in Part-2. Suffice to say for now that some backend resources are only reachable through granted and privileged access.

Internal DNS

The internal DNS server provides name to IP address mapping to corporate users for services located in the intranet. Like the external DNS servers, we will run the DNS service using BIND version 9.2.0 with the current release patches. Zone transfers between the internal and external DNS servers will be prevented. This helps prevent crackers from mapping out our internal network, in the case where our external DNS serves have been compromised.

Logging Server with NTP Services

The logging server provides a centralized repository for housing log files. The log files capture information regarding access, changes, failures, and intrusion into network devices and services. The logging can come from routers, switches, firewalls, proxy servers, web servers and intrusion detection devices. The logging server will run on a Unix based system with a sizable hard drive. It will be the responsibility of some IT staff to monitor the logs and periodically back them up to tape or CD. Backups of the logs prevent the log files from getting too large and save them for future reference. The reason for monitoring the logs is to alert the staff to changes and possible problems or attacks.

The logging server will also serve as the Network Time Protocol (NTP) server. It will draw time from the naval observatory atomic clock, and will serve as the source from which all other devices on our network will time synchronize. Besides being a cool feature, time synchronization helps us when monitoring logged events from different devices.

DHCP Server

A dynamic host control protocol (DHCP) server is a device for assigning IP addresses to host computers during the process of connecting to the intranet. It is extremely useful for managing your corporate IP address. In addition to avoiding the pain of manually assigning IP addresses to host pc's, it can also provide hosts with default router information and sometimes dynamic DNS mapping. Whereas all network equipment and servers will have statically assigned IP address, it does help prevent users from accidentally assigning duplicate IP addresses and filling the logs with clutter. This makes it worth mentioning within the security architecture diagram. One last important aspect is that the DHCP server will only serve IP addresses to host on the corporate intranet. DHCP is not enabled for segments in the DMZ or in the perimeter zone.

Proxy Servers

The proxy server serves many functions. First, it serves as a gateway for all traffic between the intranet and the Internet. This makes for a single route of traffic and thus tighter control. Second, it serves as a caching device for serving up web pages. This not only helps speed up response time but also saves bandwidth usage on our Internet lines. Next, it compliments our firewall by being able to scan the payload of packets instead of just the IP header as the firewall does. And lastly, it serves as a convenient platform to install content filtering software.

Our PIX firewalls will be configured to accept intranet web destined traffic only from the proxy servers. This will force an additional bit of work in that all employees' web browsers must have the correct settings for proxy configuration.

We will use Microsoft's ISA server for our proxy server, running on a Microsoft Windows 2000 platform with the latest service pack. The content filtering software we will purchase from Surf Control. See the following web links for more information on the Microsoft products, the content filtering software, and an interesting article on proxy server comparison:

http://www.microsoft.com/isaserver/
http://www.microsoft.com/windows2000/server/
http://www.surfcontrol.com
http://serverwatch.internet.com/proxyservers.html

Intrusion Detection System

The intranet will also sport an intrusion detection system. It will be the same network appliance, Cisco Secure IDS 4210 Sensor, as exists in the Perimeter Zone. It is important to have an IDS on the inside of the firewall too, so that we can monitor and log the traffic that is actually making it through the outer defenses.

IT-VLAN

It is important to distinguish the differences between a few of our internal virtual local area networks. The IT-VLAN is a segregated logical segment where network engineers with special privileges will connect. These are the people who will need to periodically access all of the infrastructure and security architecture. Restricting access to those resources as originating from only a certain VLAN helps protect those resources in a layered approach. The policy for this enforcement is articulated in Part-2 of this paper.

Web Developers VLAN

Another group that requires specialized access are the web developers who often need to update or upgrade our web services. Again, access control lists on the routers will enable users on their segment admission to those resources.

A Standard User VLAN

This VLAN is meant to depict a typical ethernet segment. The employees that connect to these segments can have a wide range of functions (accounting, sales, marketing) but generally will not need to work specifically with the networking gear. They will of course be need to pass through this equipment and utilize their services, but they should never have need to directly connect to those components. Thus our security policies will need to reflect this generic case.

Part 2 – Security Policies and Tutorial

IP Addressing Scheme

For purposes of this assignment the Class-B network 190.1.0.0 will be used as the GIAC corporate owned network. To the best of my research this network is unassigned not currently in use. I checked the American Registry for Internet Numbers (ARIN) and the Internet Assigned Numbers Authority (IANA) to verify this. If this network is or becomes assigned, please note that it is used in this paper only for illustrative and learning purposes, and the company depicted here is fictional.

Furthermore, using public addressing for our entire enterprise negates the need to use Network Address Translation (NAT). NAT is primarily employed by entities that use private addressing on their intranet and need to connect to the Internet. Since private addresses are not routable over the Internet, NAT hides and translates all of their internal addresses into public addresses. This still requires them to purchase at least on public address for the translation. Many people consider this to be a security feature as well since it hides the actual IP addresses and is therefore security through obscurity. As part of a layered security approach it provides one more obstacle (albeit and easy one) for an attacker to overcome. I will not argue the point. However, private addressing can present major headaches when extranets are needed with other companies or when mergers and acquisitions occur. Since it is assumed in this assignment that we have been assigned our own Class-B network, NAT won't be employed.

With the Class-B network 190.1.0.0, we will use a subnet mask of 255.255.255.0 to break it into 254 networks each with 254 hosts. This should be more than enough networks and hosts for a company this size. It also allows for future expansion. To further use or network more economically, we plan to subnet wide area network (WAN) links into two host networks. All our routers allow for this variable length subnet masking (VLSM). Here is a table of the segments and some hosts from the diagram and their IP network numbers. Individual interface addresses will appear in the device configuration.

Segment/host name	IP network	Subnet Mask
Segment-X	190.1.254.0	255.255.255.0
Segment-Y	190.1.1.0	255.255.255.0
Segment-Z	190.1.20.0	255.255.255.0
IT-VLAN	190.1.30.0	255.255.255.0
Web Developers VLAN	190.1.40.0	255.255.255.0
Users VLAN	190.1.50.0	255.255.255.0
Logging/NTP Server	190.1.20.254	255.255.255.0
External E-mail Server	190.1.1.254	255.255.255.0

External DNS #1	190.1.1.253	255.255.255.0
External DNS #2	190.1.1.252	255.255.255.0
Internal DNS	190.1.20.253	255.255.255.0
Proxy #1	190.1.20.252	255.255.255.0
Proxy #2	190.1.20.251	255.255.255.0
Web Server #1	190.1.1.250	255.255.255.0
Web Server #2	190.1.1.249	255.255.255.0

Policies for the Border Routers

The policies and configuration for the border router shown here apply to both border routers. To save space I will list only one of them. Their policies are identical and their configurations are nearly identical. Only the IP addresses of the network interface cards and some entries for hot standby routing protocol (HSRP) will differ. This is also true for the firewalls and internal routers and so one example of each will be given.

NOTE: A general physical security policy for all of the networking gear (Segments X, Y, And Z) includes:

- All networking equipment is located in a secured room.
- Entry into the equipment room is card key access and a PIN number.
- Employees will be trained not to grant access to others people (no tailgating).
- Equipment in the secured room will be mounted into rack-mount cabinets that are key locked.
- Cables leading into cabinets are to be made as secure as possible.
- All electrical circuits are connected to an uninterruptible power source (UPS).
- All equipment capable of dual power supplies should be so equipped with each one connected to a different electrical circuit.

The following is a listing of the border routers configuration (rule set and ACL's). The policies **(bold and in parenthesis)** they enforce are listed after the commands**.** This listing a summary of the security related commands. A complete listing of the border routers configuration will be in the Tutorial section. Excerpts are taken from book references [1] and [5] and the Cisco web site.

Border Router Configuration Commands:

Service timestamps debug datetime localtime
Service timestamps log datetime localtime
(This turns on the service that will time stamp all log and debug activity in the log)

Service password-encryption
(This encrypts all router passwords)

No CDP
(Disallow Cisco discovery protocol)

No service tcp-small-servers
No service upd-small-servers
(Turn off access to these services)

No service finger
(Disallow finger protocol requests)

No SNMP server
(Disables both types of SNMP)

No IP unreachables
(Blocks all ICMP host unreachable messages)

No IP direct-broadcasts
(Discard all packets targeting the broadcast address, to defend against smurf attacks)

No IP source-route
No IP http server
No IP bootp server
(Discard any IP datagram containing any of these options)

AAA new-model
AAA authentication login it-staff tacacs+ enable
AAA authentication enable it-staff tacacs+ enable
(These commands authenticate the user logging in to this router via a tacacs+ server)

Enable password 7 24598wq300asd8324
(This sets an encrypted enable password for when tacacs+ is offline)

Interface FastEthernet0
Description Perimeter Zone segment-X

IP address 190.1.254.1 255.255.255.0
No mop enabled
No IP redirects
No IP proxy-arp
No CDP
(These commands define the ethernet interface connecting to segment-X, give it an address and disable some unwanted services)

Interface Serial0
Description T1 line to ISP
IP address 12.13.14.15 255.255.255.252 **(this fictitious address supplied by ISP)**
Bandwidth 1544
IP access-group 101 in
IP access-group 102 out
No IP redirects
No IP proxy-arp
No CDP
(These commands define the serial link to the ISP and disable some unwanted services. They also apply incoming and outgoing Access lists to the interface)

ACL Rules and Order: It is important to note a few rules about how the following Access Control Lists (ACL) function. Order of the rules in an ACL is very important for two reasons. The first reason being that they are executed in a top down line-by-line fashion. As each packet is examined, the first rule that applies to it (starting from the beginning of the list) is the only rule that will get applied. That is; as soon as a rule match occurs, that rule is applied and the rest are ignored. Therefore you must check for the specific cases and move to the general. Secondly, after some time goes by, you can tune your ACL by moving up rules that are used more often than others and save CPU time. Be careful when moving rules though, that you don't accidentally cause packets to get permitted or denied incorrectly. In addition, new rules are always added onto the end of the ACL. When you need to add a new rule or change the existing order, it's best to delete the old ACL and paste in the new one. You could also create a new ACL numbered list and then apply that to the interfaces you need. One last important note is that every ACL has an implied "Deny all" statement at the end of the list, even if you don't enter one. Therefore any traffic not specifically permitted in the list is automatically denied.

Much more information on Cisco ACL's can be found at:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_5_4/msfc/acc_list.htm

Access-list 101 deny IP 190.1.0.0 0.0.255.255 any log
(Deny all packets that are sourced with our IP address to prevent Spoofing, and log it)

Access-list 101 deny IP 10.0.0.0 0.255.255.255 any log
Access-list 101 deny IP 172.16.0.0 0.15.255.255 any log
Access-list 101 deny IP 192.168.0.0 0.0.255.255 any log
(Deny all private addressed packets as defined in RFC 1918)

Access-list 101 deny IP 127.0.0.0 0.255.255.255 any log
(Deny packets using the loop back address)

Access-list 101 deny IP 255.0.0.0 0.255.255.255 any log
(Deny packets using the broadcast address)

Access-list 101 deny IP 224.0.0.0 7.255.255.255 any log
(Deny packets with a multicast address)

Access-list 101 deny IP host 0.0.0.0 any log
(Deny any packets that don't have an IP address.)

Access-list 101 permit tcp any host 190.1.1.254 EQ SMTP log
(Allow only SMTP traffic to our external mail server.)

Access-list 101 permit TCP any any established log
(Permit TCP traffic that is part of an established TCP session)

Access-list 101 permit TCP any host 190.1.1.250 EQ WWW log
Access-list 101 permit TCP any host 190.1.1.249 EQ WWW log
(These permit HTTP traffic only to our web servers.)

Access-list 101 permit TCP any host 190.1.1.250 EQ 443 log
Access-list 101 permit TCP any host 190.1.1.249 EQ 443 log
(These permit SHTTP traffic only to our web servers.)

Access-list 101 permit TCP any host 190.1.1.250 EQ FTP log
Access-list 101 permit TCP any host 190.1.1.249 EQ FTP log
(These permit FTP traffic only to our web servers.)

Access-list 101 permit TCP any host 190.1.1.250 GT 1023 established log
Access-list 101 permit TCP any host 190.1.1.249 GT 1023 established log
(These allow established FTP traffic to ports 1024 and above on the web servers.)

Access-list 101 permit UDP any host 190.1.1.253 EQ DOMAIN log
Access-list 101 permit TCP any host 190.1.1.252 EQ DOMAIN log
Access-list 101 permit UDP any host 190.1.1.253 EQ DOMAIN log
Access-list 101 permit TCP any host 190.1.1.252 EQ DOMAIN log
(These allow DNS requests to our two external DNS servers.)

Access-list 101 deny IP any any log
(Deny any other traffic not specifically permitted above.)

Access-list 102 deny ICMP any any log
(Deny any outbound ICMP traffic)
Access-list 102 permit IP 190.1.0.0 0.0.255.255 any log
(Permit only traffic from our network)
Access-list 102 deny IP any any log
(Deny and log all other traffic not permitted above)

Logging trap debugging
Logging 190.1.20.254
(These statements enable logging and identify the IP address of the logging server.)

NTP Server 190.1.20.254
(This identifies the IP address of the NTP Server.)

Tacacs-server host 190.1.20.254 key zztop81
(This identifies the IP address of the Tacacs-server, it resides on the server as the logging server.)

Banner motd ^C

Unauthorized Access Here is Prohibited!! All activity is monitored
and Unauthorized Users will be Prosecuted!!!

Terminate your connection NOW!

^C
(This is a threatening banner message that is displayed whenever someone connects to this router.)

Access-list 5 deny 0.0.0.0 255.255.255.255
Access-list 7 permit 190.1.30.0 0.0.0.255

Line aux 0
Access-class 5 in
Transport input all
(This locks down the aux port on the router and blocks all traffic to it)

Line VTY 0 4
Access-class 7 in
Exec-timeout 15 0

Password 7 A34589jn2398UU4e3
(These statements secure the telnet ports to the router by permitting only the IT-VLAN subnet access and requiring a password that is shown encrypted.)

Policy for the PIX Firewall

Like the border routers, the two firewalls will have virtually the same policies and configurations except for some interface addresses. For space and redundancies sake I will list only one of them. The following is a partial listing of the Cisco PIX firewall commands as necessary for this assignment. The same ACL rules apply here as they do in the border router (top down flow, implied deny all at the end of the list). The specific configuration commands are listed, followed by a description **(bold and in parenthesis)** of the policy they enforce. A complete reference of PIX Firewall commands can be found at:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/cmdref/index.htm

Nameif ethernet0 outside security0
Nameif ethernet1 DMZ security50
Nameif ethernet2 intranet security100
(These statements map a name to each ethernet interface and give it a security designation in relationship to the others.)

Interface ethernet0 100full
Interface ethernet1 100full
Interface ethernet2 100full
(Set the speed and duplex mode of each interface to 100MBs full duplex)

Hostname GIAC-fw1
(Give the firewall a host name)

IP address outside 190.1.254.1 255.255.255.0
IP address DMZ 190.1.1.1 255.255.255.0
IP address intranet 190.1.20.1 255.255.255.0
(Assign an IP address to each interface)

Enable password 9823lkjasdf9823l encrypted
(This sets and encrypted password for command mode.)
Passwd po9d78jhs8dHHE793 encrypted
(This sets an encrypted telnet password.)
Fixup protocol FTP 21
Fixup protocol HTTP 80
Fixup protocol ILS 389

Fixup protocol RSH 514
Fixup protocol SMTP 25
Fixup protocol SQLNET 1521
Fixup protocol SIP 5060
Fixup protocol SKINNY 2000
Fixup protocol RTSP 554
(These commands enable the use of service protocols through the PIX firewall. These shown are default settings.)

Failover
Failover timeout 0:00:00
Failover poll 15
Failover IP address outside 190.1.254.3
Failover IP address DMZ 190.1.1.3
Failover IP address intranet 190.1.20.3
(These 'failover' commands active the failover mode using a serial cable connection to the other firewall. They also set timeout and polling intervals for failover as well as specify the HSRP address used by both firewalls.)

AAA-server IT-STAFF protocol tacacs+
AAA-server (intranet) host 190.1.20.254
AAA authentication telnet console IT-STAFF
AAA authentication SSH console IT-STAFF
(These 'AAA' statements set tacacs+ as the authentication protocol and give the IP address of the tacacs+ host. They also set access verification for certain services to the firewall console.)

Telnet 190.1.30.0 255.255.255.0
SSH 190.1.30.0 255.255.255.0
(These two commands set telnet and SSH access to the firewall as coming from the IT-VLAN segment.)

Floodguard enable
(Enables the Flood Defender to protect against flood attacks.)

NAT (intranet) 0 0.0.0.0
NAT (DMZ) 0 0.0.0.0
(Disables network address translation on our inside interfaces since we have NIC-registered addresses. It also requires that traffic initiates from an inside host unless explicitly given by a STATIC statement.)

Static (DMZ, outside) 190.1.1.254 190.1.1.254 netmask 255.255.255.255
Static (DMZ, outside) 190.1.1.253 190.1.1.253 netmask 255.255.255.255
Static (DMZ, outside) 190.1.1.252 190.1.1.252 netmask 255.255.255.255

Static (DMZ, outside) 190.1.1.250 190.1.1.250 netmask 255.255.255.255
Static (DMZ, outside) 190.1.1.249 190.1.1.249 netmask 255.255.255.255
(These 'static' commands define addresses in the DMZ that access can be initiated to from the outside.)

Route outside 0.0.0.0 0.0.0.0 190.1.254.1
(Configures a static route for all traffic outside bound to use the border router's ethernet interface as the next hop. Similar static routes should be used for the other interfaces.)

Inbound ACL Start
Access-list inbound permit TCP any host 190.1.1.253 EQ domain
Access-list inbound permit TCP any host 190.1.1.252 EQ domain
(These two statements allow all DNS requests to reach our external DNS servers.)

Access-list inbound permit TCP any host 190.1.1.250 EQ www
Access-list inbound permit TCP any host 190.1.1.249 EQ www
Access-list inbound permit TCP any host 190.1.1.250 EQ 443
Access-list inbound permit TCP any host 190.1.1.249 EQ 443
Access-list inbound permit TCP any host 190.1.1.250 EQ FTP
Access-list inbound permit TCP any host 190.1.1.249 EQ FTP
(These allow access to our web servers using HTTP, SHTTP, and FTP.)

Access-list inbound permit TCP any host 190.1.1.254 EQ SMTP
(This allows SMTP traffic to reach the external email server.)

Access-list inbound permit TCP any host 190.1.20.252 EQ www
Access-list inbound permit TCP any host 190.1.20.251 EQ www
Access-list inbound permit TCP any host 190.1.20.252 EQ 443
Access-list inbound permit TCP any host 190.1.20.251 EQ 443
(These permit HTTP and SHTTP traffic to get to the internal proxy servers.)

Outbound ACL Start
Access-list outbound permit TCP host 190.1.20.252 any EQ www
Access-list outbound permit TCP host 190.1.20.251 any EQ www
Access-list outbound permit TCP host 190.1.20.252 any EQ 443
Access-list outbound permit TCP host 190.1.20.251 any EQ 443
Access-list outbound permit host 190.1.20.252 any EQ FTP
Access-list outbound permit host 190.1.20.251 any EQ FTP
Access-list outbound permit host 190.1.20.252 any EQ SMTP
Access-list outbound permit host 190.1.20.251 any EQ SMTP
(Allow the two proxy servers access using FTP, HTTP, SMTP, and SHTTP.)

Access-list outbound permit TCP host 190.1.20.240 190.1.1.250 any

Access-list outbound permit TCP host 190.1.20.240 190.1.1.249 any
Access-list outbound permit TCP host 190.1.20.241 190.1.1.250 any
Access-list outbound permit TCP host 190.1.20.241 190.1.1.249 any
(Let the two database servers communicate with the two web servers.)

Access-list outbound permit TCP 190.1.30.0 255.255.255.0 190.1.1.0 255.255.255.0 any
Access-list outbound permit TCP 190.1.30.0 255.255.255.0 190.1.254.0 255.255.255.0 any
Access-list outbound permit ICMP 190.1.30.0 255.255.255.0 190.1.1.0 255.255.255.0 any
Access-list outbound permit ICMP 190.1.30.0 255.255.255.0 190.1.254.0 255.255.255.0 any
(Allow hosts on the IT-VLAN to access all devices in the DMZ and the perimeter zone.)

DMZOUT ACL Start
Access-list dmzout permit TCP host 190.1.1.250 any EQ www
Access-list dmzout permit TCP host 190.1.1.250 any EQ 443
Access-list dmzout permit TCP host 190.1.1.250 any EQ FTP
Access-list dmzout permit TCP host 190.1.1.249 any EQ www
Access-list dmzout permit TCP host 190.1.1.249 any EQ 443
Access-list dmzout permit TCP host 190.1.1.249 any EQ FTP
(Allow the two web servers access using HTTP, SHTTP, or FTP.)

Access-list dmzout permit TCP host 190.1.1.254 any EQ SMTP
(Allow the external mail server access using SMTP.)

Access-list dmzout deny TCP host 190.1.1.253 190.1.0.0 255.255.0.0 EQ domain
Access-list dmzout deny TCP host 190.1.1.252 190.1.0.0 255.255.0.0 EQ domain
(Deny the DNS servers access to the intranet using domain.)

Access-list dmzout permit TCP host 190.1.1.253 any EQ domain
Access-list dmzout permit TCP host 190.1.1.252 any EQ domain
(Allow the DNS server all other access using domain.)

Access-group inbound in interface outside
(This statement binds the ACL "inbound" to the outside interface and applies to incoming traffic.)
Access-group outbound in interface intranet
(This statement binds the ACL "outbound" to the intranet interface and applies to incoming traffic.)
Access-group dmzout in interface DMZ

(This statement binds the ACL "dmzout" to the DMZ interface and applies to incoming traffic.)

Route outside 0.0.0.0 0.0.0.0 190.1.254.1 1
Route DMZ 190.1.1.0 0.0.0.255 1
Route intranet 190.1.0.0 0.0.255.255 190.1.20.10 1
(These statements enter static routes into the table for faster and more secure routing of packets. They specify an interface, traffic destined for it and the next hop address followed by a metric.)

Policy for the VPN

There are two types of virtual private networks (VPN's) that we need to support for our company. The first scenario is the VPN that supports our suppliers and partners. The second is the VPN that supports our remote employees. They both require secure and encrypted connectivity, the difference between them is the access to corporate resources they require. Telecommuting employees need access to all of the intranet resources they have when in the office, while partners and suppliers need only hit some DMZ devices and some intranet database servers.

There are two approaches for configuring site-to-site VPN's. Those are using pre-shared keys or using certificates. This example demonstrates the setup using certificates with Verisign as the certificate authority. The following code would be applied to our PIX Firewalls. This example was copied from the following Cisco web site and has been modified somewhat to fit this assignment's criteria:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/config/sit2site.htm#xtocid7

A similar but complimentary configuration must be setup on the VPN device of the example partner 'partner1'.

Domain-name GIAC.com
(Defines or domain)

CA Generate RSA key 1024
(Generates the PIX firewall RSA key pair. This command is not stored in the configuration.)
CA identify GIAC.com 209.165.202.130
CA configure GIAC.com ca 2 20 crloptional
(These are Verisign related enrollment commands)

CA authenticate GIAC.com

(Authenticates the CA by obtaining its key and certificate. This command is not stored.)

CA enroll GIAC.com pxbn8903rq
(Request signed certificates from your CA for your PIX Firewall's RSA key pair. Before entering this command, contact your CA administrator because they will have to authenticate your PIX Firewall manually before granting its certificate. This command is not stored in the configuration.)

Show ca certificate
(Check that you actually got a certificate. This command is not stored.)

CA save all
Write memory
(Save the keys, certificates and CA commands to flash memory.)

Static (inside, outside) 190.1.1.0 190.1.1.0
(Creates a static one-to-one translation rule.)

Isakmp enable outside
Isakmp policy 8 auth rsa-sig
(Configures an Internet key exchange (IKE) policy.)

Access-list 90 permit IP 190.1.1.0 255.255.255.0 10.0.0.0 255.0.0.0
(Create a partial ACL)

Crypto IPSec transform-set strong esp-3des esp-has-hmac
(Configures a transform set that defines how the traffic will be protected)

Crypto map topartner1 20 IPSec-isakmp
Crypto map topartner1 20 match address 90
Crypto map topartner1 20 set transform-set strong
Crypto map topartner1 20 set peer 200.201.134.100
(These define a crypto map to partner1 who has an outside firewall address of 200.201.134.100.)

Crypto map topartner1 interface outside
(Applies the map to the outside interface)

Sysopt connection permit-ipsec
(Tell the PIX firewall to accept IPSec traffic)

The following setup procedure is for configuring the Cisco VPN Client Version 1.1 on our remote employees pc. It assumes that the client is already installed on the pc. It was copied from the following Cisco web site and slightly modified to fit this assignment:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/config/basclnt.htm#17261

Step 1 Click **Start**>**Programs**>**Cisco Secure VPN Client**>**Security Policy Editor**.

Step 2 Click **Options**>**Secure**>**Specified Connections**.

Step 3 In the Network Security Policy window, click **Other Connection** and then click **Non-Secure** in the panel on the right.

Step 4 Click **File**>**New Connection**. Rename New Connection. For example, GIAC.

Step 5 Under **Connection Security**, click **Secure**.

Step 6 Under **Remote Party Identity and Addressing,** set the following preferences in the panel on the right:

a. ID Type—Click **IP address**.

b. Enter the IP address of the internal host within the PIX Firewall unit's internal network to which the VPN client will have access. Enter **190.1.20.100**.

c. Click **Connect using Secure Gateway Tunnel**.

d. ID Type—Click **IP address**.

e. Enter the IP address of the outside interface of the PIX Firewall. Enter **190.1.254.1.**

Step 7 In the Network Security Policy window, click the plus sign beside the GIAC entry to expand the selection, and click **My Identity**. Set the following preferences in the panel on the right:

a. Select Certificate—Click **None**.

b. ID Type—Click **IP address**.

c. Port—Click **All**.

d. Local Network Interface—Click **Any**.

e. Click **Pre-Shared Key**. When the Pre-Shared Key dialog box appears, click **Enter Key** to make the key field editable. Enter **cisco1234** and click **OK**.

Step 8 In the Network Security Policy window, expand Security Policy and set the following preferences in the panel on the right:

a. Under **Select Phase 1 Negotiation Mode,** click **Main Mode**.

b. Select the **Enable Replay Detection** check box.

Leave any other values as they were in the panel.

Step 9 Click **Security Policy**>**Authentication (Phase 1)**>**Proposal 1** and set the following preferences in the panel on the right:

a. Authentication Method—Click **Pre-shared Key**.
b. Encrypt Alg—Click **Triple DES**.
c. Hash Alg—Click **MD5**.
d. SA Life—Click **Unspecified** to accept the default values.

e. Key Group—Click **Diffie-Hellman Group 1**.

Step 10 Click **Security Policy**>**Key Exchange (Phase 2)**>**Proposal 1** and select the following values in the panel on the right:

a. Select the **Encapsulation Protocol (ESP)** check box.

b. Encryption Alg—Click **Triple DES**.

c. Hash Alg—Click **SHA-1**.

d. Encapsulation—Click **Tunnel**.

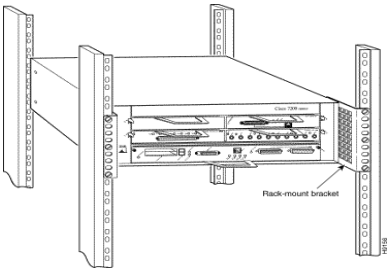
Step 11 Click **File**>**Save Changes**.

The VPN client is now activated.

Tutorial for Implementing the Border Router

This section of the assignment is a soup-to-nuts guide for getting your border router up and running. The first step is to get it physically installed. The packing material should contain an installation guide for installing your new Cisco 7204 router. If it does not, the following web link contains all the information you need to help you rack mount, ground the chassis, and connect the port and cables.

http://www.cisco.com/univercd/cc/td/doc/product/core/7204/7204ig/inst4icg.htm



It also includes important information on the power requirements, the environmental conditions you need to safely operate your router, and a checklist of things to do before you start the router. There is also a section that describes the meaning of the LED's on the router and a link to a 'trouble-shooting guide' should the steps fail.

The next step is to connect a console terminal or pc to the console port on the router and load the configuration. It is best to have the console connected to the router the first time you turn on the power to ensure that the router initializes properly. Directions for connecting a console to the router are found in the previous link, "Installing the Cisco 7204". The initial system boot-up loads from Flash memory and you should see the following messages on the console:

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-J-M), Released Version 11.1(17)CA
Copyright (c) 1986-1996 by Cisco Systems, Inc.
Compiled Sun 21-Apr-96 04:10 by
Image text-base: 0x60010890, data-base: 0x605F0000

ROM: System Bootstrap, Version 11.1(17)CA, RELEASED SOFTWARE
ROM: 7200 Software (C7200-J-M), Released Version 11.1(17)CA

```
router uptime is 8 minutes
System restarted by reload
System image file is "c7200-j-mz", booted via tftp from 1.1.10

Cisco 7204 (NPE 150) processor with 12288K/4096K bytes of memory.
R4700 processor, Implementation 33, Revision 1.0 (Level 2 Cache)
Last reset from power-on
Bridging software.
SuperLAT software copyright 1990 by Meridian Technology Corp).
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
TN3270 Emulation software (copyright 1994 by TGV Inc).
4 Ethernet/IEEE 802.3 interfaces.
2 FastEthernet/IEEE 802.3 interfaces.
4 Token Ring/IEEE 802.5 interfaces.
4 Serial network interfaces
125K bytes of non-volatile configuration memory.
1024K bytes of packet SRAM memory.

20480K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
4096K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x0

         --- System Configuration Dialog ---

At any point you may enter a questions mark `?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets `[]'.

continue with configuration dialog? [yes]:
```

The messages displayed describe the hardware and software versions that the router booted with, as well as some copyright and system uptime information. The last message displayed comes from the "Setup Utility". It is prompting you continue configuring the router using the Setup Utility with "Yes" as the default answer. I think the best way to understand the process is to do it manually, so you should type in "No" and press enter.

NOTE: As with most things, practice is the best way to become proficient at configuring Cisco routers. It is highly recommended that you obtain an unused router to practice with, or practice with this one for several days or weeks before you install any production routers! Investigate and become familiar with all of the "Show" commands and their output. Try saving files using different methods and installing them from different sources. Perform IOS upgrades and backups until you are comfortable with the procedures. Understanding these things can make a huge difference during an outage or crisis!

After you exit the Setup Utility you will then get the prompt: **Router>**

Examining the prompt will tell you a few things. First, it displays the routers hostname, which out of the box is "Router". The hostname is followed by a symbol that shows you the current mode. The ">" symbol means that you are in "user exec" mode. If you type a question mark "?" and press enter, it will show you a list of available commands for the mode you are in. For a complete list of the Cisco IOS commands and more information on their function reference this link:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122mindx/index.htm

The next step is to enter into "privileged exec" mode. Do this by entering "enable" at the prompt:

Router> Enable
Router#

Since there is no default password set, it does not prompt you for one and takes you directly into privileged exec mode. Notice that the prompt changed to a "#" to indicate mode change. From here you can enter into configuration mode by entering:

Router# Config terminal
Router (config)#

Notice the prompt change again to indicate you are in configuration mode. You are now able to enter router configuration commands. Another important configuration mode to know about is the "interface configuration" mode, which lets you enter commands specific to a certain interface. You do this from the "config" prompt by entering:

Router (config)# interface ethernet0
Router (config-int)#

You are now able to enter configuration commands for the ethernet interface in slot 0. The form of the command is "Interface type slot/port", where "interface" is a key word, "type" indicates the interface type (i.e.: ethernet, serial, atm), and "slot/port" indicate the physical slot and port numbers of the interface in the router. Entering the command "end" will take you out of configuration mode and put you back into privileged exec mode.

At this point, I will just copy and paste the configuration file that was created in policies section for the border router above. Most of the commands were described in that section already, so I will just highlight and describe the additional commands.

Hostname GIAC-inetrouter1

(This gives the router a name that will now be displayed in the prompt and on a telnet connection screen. Very useful to give it a meaningful name!)

!

Service timestamps debug datetime localtime

Service timestamps log datetime localtime

Service password-encryption

!

Clock timezone EST –5

Clock summer-time EDT recurring

(These two commands set the internal clock rules for its time zone and daylight savings time offsets. This helps when reviewing logs too.)

No CDP

No service tcp-small-servers

No service upd-small-servers

No service finger

No SNMP server

No IP unreachables

No IP direct-broadcasts

No IP source-route

No IP http server

No IP bootp server

!

AAA new-model

AAA authentication login it-staff tacacs+ enable

AAA authentication enable it-staff tacacs+ enable

AAA accounting exec default stop-only tacacs+

AAA accounting commands 0 default start-stop tacacs+

AAA accounting commands 1 default start-stop tacacs+

AAA accounting commands 15 default start-stop tacacs+

AAA accounting system default start-stop tacacs+

(The AAA accounting commands provide system level information about commands entered at different privilege modes to the log file.)

Enable password 7 24598wq300asd832

IP Domain-name GIAC.com

(Defines that domain name this router is part of)

IP Name-server 190.1.20.253

(Provides the IP address of the DNS server)

!

Interface Loopback0

IP address 190.1.253.1. 255.255.255.255

No IP directed-broadcast

(These commands define a logical interface called the "Loopback" interface. It is useful for connecting to with telnet because this interface is always up.)

!

```
Interface FastEthernet0
  Description Perimeter Zone segment-X
  IP address 190.1.254.1 255.255.255.0
  No mop enabled
  No IP redirects
  No IP proxy-arp
  No CDP
  Standby 1 IP 190.1.254.250
  Standby 1 priority 110
  Standby 1 preempt
  Standby 1 authentication 9yodude
```

(The "standby" commands are added under the interface and work to establish hot standby routing protocol HSRP. This is done also on the ethernet interface of the counterpart router.)

```
!
Interface Serial0
  Description T1 line to ISP
  IP address 12.13.14.15 255.255.255.252
  Bandwidth 1544
  IP access-group 101 in
  IP access-group 102 out
  No IP redirects
  No IP proxy-arp
  No CDP
!
Router rip
  Version 2
  Passive-interface Serial0
  Network 190.1.0.0
  No auto-summary
```

(This section turns on the routing protocol RIP version 2, and denies the serial interface from updating the routing table for RIP.)

```
!
Router BGP 98707
  BGP router-id 190.1.253.1
  BGP log-neighbor-changes
  Network 190.1.0.0 mask 255.255.0.0
  Neighbor 12.13.12.30 remote-as 4321
  Neighbor 12.13.12.30 ebgp-multihop 4
  Neighbor 12.13.12.30 update-source loopback0
  Neighbor 190.1.254.10 remote-as 98707
  Neighbor 190.1.254.10 update-source loopback0
  Maximum-paths 4
```

(This section turns on the routing protocol BGP 'border gateway protocol'. It is a common and secure routing protocol to use on the edge of your network. Many of the parameters must be coordinated with the ISP's router on the other end of the serial link. The ones shown here are fictitious.)

```
!
Access-list 101 deny IP 190.1.0.0 0.0.255.255 any log
Access-list 101 deny IP 10.0.0.0 0.255.255.255 any log
Access-list 101 deny IP 172.16.0.0 0.15.255.255 any log
Access-list 101 deny IP 192.168.0.0 0.0.255.255 any log
Access-list 101 deny IP 127.0.0.0 0.255.255.255 any log
Access-list 101 deny IP 255.0.0.0 0.255.255.255 any log
Access-list 101 deny IP 224.0.0.0 7.255.255.255 any log
Access-list 101 deny IP host 0.0.0.0 any log
Access-list 101 permit tcp any host 190.1.1.254 EQ SMTP log
Access-list 101 permit TCP any any established log
Access-list 101 permit TCP any host 190.1.1.250 EQ WWW log
Access-list 101 permit TCP any host 190.1.1.249 EQ WWW log
Access-list 101 permit TCP any host 190.1.1.250 EQ 443 log
Access-list 101 permit TCP any host 190.1.1.249 EQ 443 log
Access-list 101 permit TCP any host 190.1.1.250 EQ FTP log
Access-list 101 permit TCP any host 190.1.1.249 EQ FTP log
Access-list 101 permit TCP any host 190.1.1.250 GT 1023 established log
Access-list 101 permit TCP any host 190.1.1.249 GT 1023 established log
Access-list 101 permit UDP any host 190.1.1.253 EQ DOMAIN log
Access-list 101 permit TCP any host 190.1.1.252 EQ DOMAIN log
Access-list 101 permit UDP any host 190.1.1.253 EQ DOMAIN log
Access-list 101 permit TCP any host 190.1.1.252 EQ DOMAIN log
Access-list 101 deny IP any any log
!
Access-list 102 deny ICMP any any log
Access-list 102 permit IP 190.1.0.0 0.0.255.255 any log
Access-list 102 deny IP any any log
!
Logging trap debugging
Logging 190.1.20.254
NTP Server 190.1.20.254
Tacacs-server host 190.1.20.254 key zztop81
!
Banner motd ^C

    Unauthorized Access Here is Prohibited!! All activity is monitored
    and Unauthorized Users will be Prosecuted!!!

    Terminate your connection NOW!
```

```
^C
Access-list 5 deny 0.0.0.0 255.255.255.255
Access-list 7 permit 190.1.30.0 0.0.0.255
!
Line aux 0
  Access-class 5 in
  Transport input all
Line VTY 0 4
  Access-class 7 in
  Exec-timeout 15 0
  Password 7 A34589jn2398UU4e3
!
End
```

When finished loading the config file, save it in memory and to other locations for backup and swift retrieval (i.e. a flash card or tftp server.) It is a good idea to save the Cisco IOS file to the flash card as well.

Router# Copy running-config startup-config
(Copies the current configuration from RAM into NVRAM for use at next reload. See the 'Copy' command for ways to save the configuration to other locations.)
Router# Show running-config
(Displays the current configuration stored in RAM.)

Now that the router has been configured and backed-up, it is a good idea to test its operation. Some things you might want to try would include:

- Execute the command "**show interface"** to make sure all interfaces are up and packets are flowing.
- Ping all of the interfaces from another location on the network.
- Try logging into the router to check that you are getting challenged by TACACS+ for a signon and password.
- Check that the **"enable"** command password challenges you.
- Test using telnet to access the router; is there a password challenge? Did you see the banner message?
- Examine the routing table with the **"show route"** command.
- Show the log file and look for any problems.
- Ensure that the access-lists are applied to the interfaces with **"show access-list"**.

The following links provide more good information regarding configuration and ongoing maintenance of your router respectively:
http://www.cisco.com/univercd/cc/td/doc/product/core/7204/7204ig/cfig4icg.htm
http://www.cisco.com/univercd/cc/td/doc/product/core/7204/7204ig/main4icg.htm

Part 3 – Verify the Firewall Policy

This section of the assignment deals with conducting an audit of GIAC's primary firewall. It is not an exhaustive audit of all company security practices, but simply a technical audit of the primary firewall and the policies it enforces. A real audit would test the entire security architecture implemented across all layers to more closely simulate a hacker's viewpoint. It would also take into consideration security on all levels, network, physical, social engineering, etc. This is because the firewall is more than just one piece of hardware; it is a collection of systems and an ongoing cycle. It is a journey with no endpoint. However, the focus of this part of the assignment is tightly specked out to concentrate solely on the Cisco PIX firewall and policies it is programmed to enforce.

The Audit Game Plan

As an outside consultant hired by GIAC to audit their primary firewall, I will work closely with the engineers responsible for maintaining the firewalls and the IT management team. The first order of business will be to get a written contract of what GIAC expects from the audit and have those expectations specifically and clearly stated. I would also expect to sign a non-disclosure agreement with GIAC.

For the audit I will employ a suite of scanning tools, utilities, and methods to test for weaknesses. As part of the process I would work with the technical staff. This would allow them to oversee the methods used first hand and would provide valuable training for the staff. This insight would help the staff learn techniques that could be beneficial in the future when network changes are made or new attacks are discovered. The results and recommendations will be documented for the management team. At which point they will have the option to continue to pay me for overseeing the recommended changes. The actual testing should take no more than one week (40 hours). The majority of the testing can be done during normal hours. Some testing, however, has the potential to adversely affect network operations and should be scheduled for after hours during slow periods. The management team will always be kept informed as to the testing schedule. Along with the 40 hours of testing and training, I require approximately three more working days to prepare a formal report of the findings and recommendations.

The management team must approve the testing schedule before actual probing begins. It will be the responsibility of the management team to have staff available if they wish to take part and learn. My hourly rate is $225.00 an hour, with estimated time being 64 hours for a total of $14,400. The rate will be the same if GIAC wished me to work on implementing any outstanding recommended changes.

Audit Execution

Whois Audit

The first phase of the audit is conducted from an Internet connected computer to assess the outward defenses posture. The first test is to execute a series of "Whois" commands on the GIAC.com domain. Many times you can find valuable information in this type of query such as the IP addresses of any DNS severs, physical location addresses, or even contact names. Contact names of actual employees are especially dangerous in that it leaves you susceptible to social engineering type attacks. An example response to the Whois command for GIAC looks like:

Search results for: NET-GIAC

```
GIAC Enterprises Corporation (NET-GIAC)
   10 Fortune Cookie Road
   Happy Town, CA 54321
   US

   Net name: GIAC
   Net block: 190.1.0.0 - 190.1.255.255

   Coordinator:
      GIAC Enterprises Corporation (WF34-ARIN)
         domains@GIAC.com
      800-555-1234

   Domain System inverse mapping provided by:

   DNS1.GIAC.COM          190.1.1.253
   DNS2.GIAC.COM          190.1.1.252

   Record last updated on 14-Jan-2002.
   Database last updated on 1-May-2002 20:02:50 EDT.
```

From the example we can see that the information provided is sterile and provides no contact names to exploit. About the only extra precaution we could make here would be to hide our IP addresses with some form of NAT.

Traceroute

Traceroute is a great diagnostic utility used to map out the path taken by packets across a network. It is usually used for trouble-shooting connectivity problems but can also be used to identify all the router hops between you and a target resource.

It relies upon the ICMP protocol and information it gets from "time-to-live" messages to identify "next hops". An attacker could use this command to create a map of your network to aid in his mission. For example he enters the command:

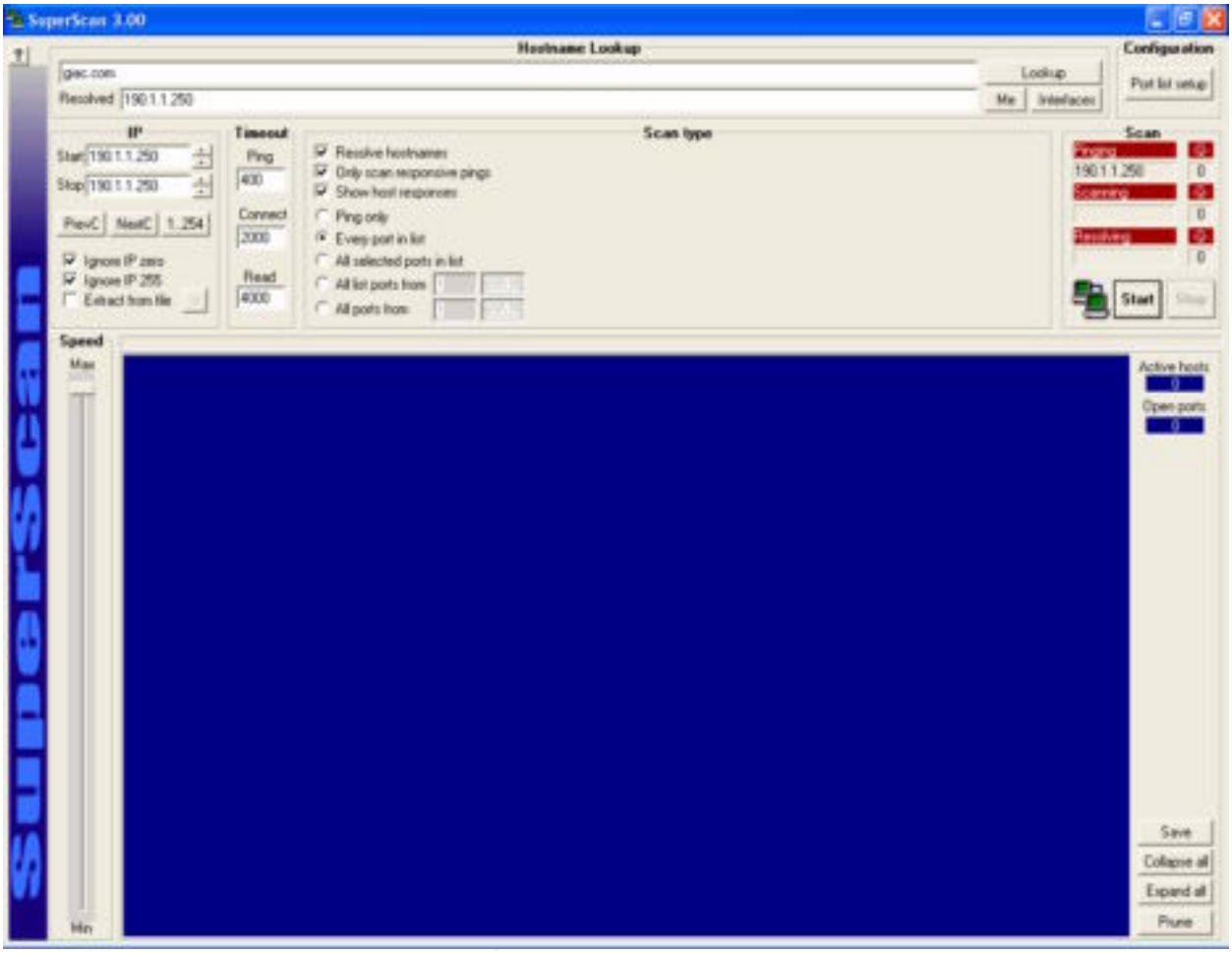
$ Traceroute webserver.giac.com

Tracing route to webserver.giac.com (190.1.1.250) over a maximum 30 hops:
1 < 6 ms yocalisp (1.2.3.4)
2 < 4.5 ms border-router (12.13.14.15)
3 < 1 ms giac-fw (190.1.254.1)
4 < 1 ms giac-webserver (190.1.1.250)

This example makes it easy for the attacker to create the layout of our network. However, GIAC has configured the border router to deny all ICMP commands from the Internet so we pass this test. For diagnostics, it is common to allow ICMP Ping responses only from the IP address of the ISP connected to the border router.

Port Scanning

Another common method attackers employ is port scanning. This type of probing tells the attacker the state of TPC and UDP ports on Internet reachable devices. Knowing which ports are available and which are closed allows the enemy to narrow the focus of his attacks to vulnerabilities associated with those specific ports. Thus it is a best practice only to expose those ports, which are necessary and block all others. There is several port scanning utilities available for this purpose. Common ones include: (PortScan, UltraScan, and the venerable Nmap) just to list a few. Being partial to attractive graphical interfaces, I'll use on called SuperScan V3.0, which is owned by Foundstone (http://www.foundstone.com). The following is an example screen shot of the SuperScan utility:



The above example shows the utility ready to scan all TCP ports on the server at address 190.1.1.250. Had this been a real address, I could have started the scan and the available ports would appear in the blue portion of the screen. The ports it would have shown are: 21 (FTP), 80(HTTP), and 443(SHTTP). This is the necessary minimal amount of ports required for the web server. This type of scan would be performed on every DMZ device and across all three firewall interfaces in order to check the firewall rules in all directions.

This utility could also perform a 'ping sweep' of the network 190.1.1.0 to discover what other machines are available, fortunately our border router blocks ICMP ping requests and would give the foe no additional information. For purposes of illustrating this example SuperScan is sufficient, however other utilities such as Nmap are more robust in their port scanning features and I would probably use them in an actual audit.

Telnet

Telnet is a remote console program used for administering systems. Most networking equipment supports it and it is a freely distributed utility. This gives an intruder an available backdoor into your systems to attempt. Especially if no authentication is required! After identifying as many target systems as he can, the attacker will try to telnet to all of them. A successful connection would allow him to launch further attacks from behind your firewall.

An example of an attempted telnet connection to the GIAC firewall would look like:

```
$ telnet 190.1.254.1
  Trying 190.1.254.1… Could not open connection to the host, on port 23.
  A socket operation was attempted to an unreachable network.
$
```

Here we can see that the effort to establish a telnet connection failed because it was blocked by the firewall. By our firewall rules we know that telnet connections are only permitted when sourced from the 190.1.30.0 network. Trying to telnet from that segment is allowed but is further secured by tacacs+ authentication. It is important to note also that if the authentication service is down, it will resort to authentication by prompting for the password that is encrypted in the running configuration. The factory default has been changed.

Spoofing

The spoof attack is a method used to gain entry into your network by altering the source address of attacking packets to that of an internal network address. This is an attempt to fool the firewall into believing that the traffic originated from the corporate intranet. Fortunately for GIAC, the border router filters out this type of ploy before it ever gets to the actual firewall. (See the border router configuration for details on the incoming ACL.)

This may seem like an obvious precaution to take, but the SANS institute lists the "Spoofing" on their "Top 20 Most Critical Internet Security Vulnerabilities" that affect all systems. This implies that it is a common security configuration mistake made by system administrators, and that it is an easy attack to execute. In addition to the companies internal network numbers, the border router should block private addresses (RFC 1918), Loopback, broadcast, and multicast addresses. Get more information about the SANS top 20 list at: http://www.sans.org/top20.htm

DNS Audit

As was stated earlier, the DNS is a service that maps hostnames to IP addresses for ease of use. Auditing the domain name server (DNS) is a matter of checking two areas. First, to ensure that it is not leaking important information to potential intruders, and second, to prove that it is secure against know DNS threats.

One of the biggest information type threats is a zone transfer. A zone transfer is basically copying the entire DNS database to another machine. This information can be used to create a topology map of your network. There are two countermeasures against this information-gathering tool. First is to segregate your DNS into an internal server and an external server. The external DNS contains only information about Internet available devices in the DMZ and no intranet hosts. Thus, even if a zone transfer occurs, the attacker will have only public information. Second is to limit zone transfers to only specific intranet host devices. These two countermeasures are already implemented so GIAC passes that part of the audit.

Another high impact attack against the DNS is called cache poisoning. This is the situation where an enemy is able to trick your DNS server into storing incorrect information into cache memory. If he succeeds, DNS queries from legitimate customers could be routed to a fake site to obtain information, or to a null site for a denial of service attack. Preventative steps against cache poisoning and other attacks against our BIND DNS can be found at: http://www.sans.org/top20.htm. The following list is an excerpt from that website:

The following steps should be taken to defend against the BIND vulnerabilities:

1. Disable the BIND name daemon (called "named") on all systems that are not authorized to be DNS servers. Some experts recommend you also remove the DNS software.
2. On machines that are authorized DNS servers, update to the latest version and patch level. Use the guidance contained in the following advisories:
3. For the NXT vulnerability: http://www.cert.org/advisories/CA-99-14-bind.html
   For the QINV (Inverse Query) and NAMED vulnerabilities: http://www.cert.org/advisories/CA-98.05.bind_problems.html
   http://www.cert.org/summaries/CS-98.04.html
4. Run BIND as a non-privileged user for protection in the event of future remote-compromise attacks. (However, only processes running as root can be configured to use ports below 1024 – a requirement for DNS. Therefore you must configure BIND to change the user-id after binding to the port.)
5. Run BIND in a chroot()ed directory structure for protection in the event of future remote-compromise attacks.
6. Disable zone transfers except from authorized hosts.
7. Disable recursion and glue fetching, to defend against DNS cache poisoning.
8. Hide your version string.

Banner Grabbing

Banner grabbing is simply an attempt to identify a host (firewall, router, server) by attempting a connection to it and reading the information given in the banner message. Default banners usually list the manufacturer and model of the device connected to via telnet or FTP. Knowing this information gives an attacker the ability to focus his attention directly on vulnerabilities associated with that equipment. This saves him a lot of time and effort.

Fortunately, most equipment allows you to change this default information to whatever you wish. In our case, we used the MOTD feature on the Cisco routers to display threatening warnings. So GIAC passes this audit test.

Denial of Service

As the name of the attack implies, DOS attempts to shut down and deny your service to legitimate customers. DOS attacks accomplish this by either flooding your available bandwidth, or by taking advantage of a weakness in an application, a protocol, or an operating system. There are several countermeasures to employ against DOS attacks; many of them have already been stated early in this assignment. Some of those include; use of redundant equipment where single points of failure existed, maximum amount of RAM used in all equipment, latest software and operating system patches, multiple high speed data transmission lines, and good physical security. Some of the more specific types of DOS are listed as follows:

Syn Flood: This is the method of overloading the connection queue by sending numerous incomplete connection requests. It takes advantage of the TCP three-way handshake by only sending the SYN packet and ignoring the SYN/ACK responses. All Cisco gear using IOS 11.3 or above is protected against this type of attack so our firewall and routers are immune. Most other vendors offer patches or upgrades to protect against this as well.

Smurf: "The Smurf attack is on of the most frightening DOS attacks in existence due to the amplification effects of the attack. The amplification effect is a result of sending a directed broadcast ping request to a network of systems that will respond to such requests. An attacker sends spoofed ICMP ECHO packets to the broadcast address of the amplifying network. The source address of the packet is forged to make it appear as if the victim system has initiated the request. Since the ECHO packet was sent to the broadcast address, all the systems on the amplifying network will respond to the victim. If the amplifying network has 100 systems that respond to

a broadcast ping, the attacker has effectively multiplied the DOS attack by a magnitude of 100." [4]

All of our Cisco networking equipment can thwart this type of attack internally by using the **no IP directed-broadcast** command. Check out this CERT advisory: http://www.cert.org/advisories/CA-1998-01.html for other vendor information.

Of course, this does not help us externally against these attacks if our wide area network links are saturated by another attacking network. In this case, you could work with your ISP to either block the attacking network or identify them for contact and help.

Incorrectly Configured ACL's:

Another part of the audit involves reviewing the firewall and router access control lists. The Cisco IOS provides a number of commands for checking the ACL's. The first is to show a specified ACL (**show access-lists "acl-number")** and is executed from the privileged mode:

```
Router# show access-lists 101

Extended IP access list 101
    permit tcp host 198.92.32.130 any established                    (4304 matches) check=5
    permit udp host 198.92.32.130 any eq domain                       (129 matches)
    permit icmp host 198.92.32.130 any
    permit tcp host 198.92.32.130 host 171.69.2.141 gt 1023
    permit tcp host 198.92.32.130 host 171.69.2.135 eq smtp          (2 matches)
    permit tcp host 198.92.32.130 host 198.92.30.32 eq smtp
    permit tcp host 198.92.32.130 host 171.69.108.33 eq smtp
    permit udp host 198.92.32.130 host 171.68.225.190 eq syslog
    permit udp host 198.92.32.130 host 171.68.225.126 eq syslog
    deny   ip 150.136.0.0 0.0.255.255 224.0.0.0 15.255.255.255
    deny   ip 171.68.0.0 0.1.255.255 224.0.0.0 15.255.255.255        (2 matches) check=1
    deny   ip 172.24.24.0 0.0.1.255 224.0.0.0 15.255.255.255
    deny   ip 192.82.152.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.122.173.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.122.174.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.239.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.240.0 0.0.7.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.248.0 0.0.3.255 224.0.0.0 15.255.255.255

An access list counter counts how many packets are allowed by each line of the
access list. This number is displayed as the number of matches. Check denotes how
many times a packet was compared to the access list but did not match.
```

This example obtained from:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_r/iprprt1/1rdip.htm#1020059

Two more privileged mode commands are: **show IP accounting** and **show IP accounting access-violations**. Examples of these and explanations of their content are shown below. Again, these examples were obtained at the Cisco URL: **http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_r/iprprt1/1rdip.htm#1020059**

Examples

The following is sample output from the **show ip accounting** command:

```
Router# show ip accounting

   Source           Destination      Packets               Bytes
 131.108.19.40    192.67.67.20             7                 306
 131.108.13.55    192.67.67.20            67                2749
 131.108.2.50     192.12.33.51            17                1111
 131.108.2.50     130.93.2.1               5                 319
 131.108.2.50     130.93.1.2             463               30991
 131.108.19.40    130.93.2.1               4                 262
 131.108.19.40    130.93.1.2              28                2552
 131.108.20.2     128.18.6.100            39                2184
 131.108.13.55    130.93.1.2              35                3020
 131.108.19.40    192.12.33.51          1986               95091
 131.108.2.50     192.67.67.20           233               14908
 131.108.13.28    192.67.67.53           390               24817
 131.108.13.55    192.12.33.51        214669             9806659
 131.108.13.111   128.18.6.23          27739             1126607
 131.108.13.44    192.12.33.51         35412             1523980
 192.31.7.21      130.93.1.2              11                 824
 131.108.13.28    192.12.33.2             21                1762
 131.108.2.166    192.31.7.130           797              141054
 131.108.3.11     192.67.67.53             4                 246
 192.31.7.21      192.12.33.51         15696              695635
 192.31.7.24      192.67.67.20            21                 916
 131.108.13.111   128.18.10.1             16                1137
```

Example: Show IP accounting access-violations

The following is sample output from the **show ip accounting access-violations** command. The output pertains to packets that failed access lists and were not routed:

```
Router# show ip accounting access-violations


   Source           Destination      Packets         Bytes         ACL
131.108.19.40    192.67.67.20             7           306          77
131.108.13.55    192.67.67.20            67          2749         185
131.108.2.50     192.12.33.51            17          1111         140
131.108.2.50     130.93.2.1               5           319         140
131.108.19.40    130.93.2.1               4           262          77
Accounting data age is 41
```

Table 15 describes the fields shown in the displays.

Table 15: show ip accounting (and access-violation) Field Descriptions Field	**Description**
Source	Source address of the packet.
Destination	Destination address of the packet.
Packets	Number of packets sent from the source address to the destination address. With the **access-violations** keyword, the number of packets sent from the source address to the destination address that violated an access control list.
Bytes	Sum of the total number of bytes (IP header and data) of all IP packets sent from the source address to the destination address. With the **access-violations** keyword, the total number of

	bytes sent from the source address to the destination address that violated an access-control list.
ACL	Number of the access list of the last packet sent from the source to the destination that failed an access list filter.

Another useful audit command is the **Show Route** command used in privileged mode. This will display the current routing tables contained in memory. Check the table to ensure that the information is correct and that no bogus entries have been added.

Once you have compiled all the information from the above commands you can use it to tune your ACL's. Rules that seem to be getting hit more often should be moved up the access list since they are executed in a top down fashion. However, do not move the rule up if changing the order will alter your security policy. For instance, don't move a general rule up to the top that would preclude the need for a more specific rule that follows.

In addition to using the tools built into the system, I would check the logs of the firewall and of the Intrusion Detection scanners. They could provide valuable information about what traffic is actually getting through and point to weaknesses in the firewall's configuration. Finally, I would use some traffic generator programs that allow me to send packets to specific devices using specific IP port numbers. This would be an acid test to see how far the firewall allows me to penetrate.

Eavesdropping and Session Hijacking:

These two dangers exist because of the publicly shared lines used by the Internet. Eavesdropping is simply the act of 'listening or observing' the packets of some one else's conversion. Session hijacking takes advantage of your ability to eavesdrop and of a weakness in the TCP protocol. This allows the hijacker to jump into and take over one side of a connection without the other party's knowledge.

Both of these attacks can be made extremely difficult to perform when strong encryption is employed. GIAC currently is using IPSec for its tunneling security encryption to its partners and remote employees. GIAC is also encrypting communication with its customers using secure sockets layer (SSL) or commonly implemented as SHTTP. We can verify that encryption is indeed taking place with the aid of a protocol analyzer. A protocol analyzer is the ultimate diagnostic or spying tool, depending on your motives, for analyzing network traffic. Once the

analyzer is connected to the same network it records the packets going by in their raw format. This allows you to view the entire contents of each packet at each protocol layer. If the payload data is not encrypted, then you will be able to read the clear text information it contains.

One of my favorite protocol analyzers is made by Network Associates and is named the Sniffer. Visit either of these web sites for more product information: http://www.sniffer.com or http://www.nai.com.

Ping of Death, Teardrop, WinNuke:

These three common and easily obtainable DOS attacks take advantage of the way the IP stack is implemented on different operating systems. Patches for the various operating systems have long been available to negate these three (and several others like them) DOS attack programs. My only point in listing them here is to underscore the need to diligently apply the latest software patches and to be vigilant of new attacks.

You should frequently check your vendor's web page to determine if new patches are available for software you utilize. Also it is wise to stay current on new threats and vulnerabilities. You can do this by checking these two excellent sites: http://www.sans.org or http://www.cert.org. Both of them offer an automated e-mail service to give up-to-the-minute updates regarding the latest security holes.

Audit Analysis and Recommendations

It is pleasing to note that GIAC passed several of the audit tests. However, there is always room for improvement. The following is a list of recommended security enhancements for GIAC Enterprises.

1. Use network address translation (NAT) for the devices in the DMZ and segment-X. As part of a layered security approach, disguising the internal IP numbers adds one more hurdle for an attacker to overcome. This is akin to locking your car doors to prevent auto theft. It serves only slow the thief down and perhaps makes him change targets to easier prey.

2. Confuse potential enemies with disinformation. "Use a program like RotoRouter from packetstorm.com to generate fake responses to incoming traceroute probes." [4] Replies, or non-replies, from the firewall to probes can reveal information about its configuration. Confuse hackers with bogus replies.

3. Generate a disaster recovery plan for your mission critical services. Catastrophic disasters do occur and can ruin even a well-insured business. A plan for quick recovery at a remote site can save a business. Generate the plan and periodically practice the drill.

4. Staff a full time security position. This person would be responsible for keeping current on new threats and vulnerabilities, coordinating upgrades and patches, creating and maintaining a corporate security policy, managing future network audits, and archiving and analyzing all security related logs.

5. Tune the Intrusion detection systems to watch for slow and distributed scans.

6. Where possible, disable the use of telnet by all employees in favor of SSH. Telnet has a major weakness in that it transmits login and password information in clear text format. Anyone connected to the intranet with a packet analyzer would be able to pick that information off the line for improper use. Especially if it were an administrators password. SSH is supported by most networking equipment transmits only encrypted information.

7. Block java applets at the incoming port of the firewall and on all employee browsers. Also configure employee browsers to disallow cookies.

8. Add a rule to the firewall that allows the external mail server to communicate only with a mail relay server located on Segment-Z of the Intranet. Currently it is allowed to inwardly communicate with the entire intranet.

9. Employ Tripwire products on the web servers. See: http://www.tripwire.com for product information. Its primary function is to alert you to file changes. Since we are running the accounting feature on all our Cisco routers, switches, and firewalls, we don't need to duplicate that function on those devices.

10. Use a product like "Antisniff" to protect your intranet from rogue protocol analyzers. It does this by detecting network interface cards that are in promiscuous mode, a sign the computer has either been compromised or that protocol analyzer software is being used.

Part 4 – Design Under Fire

The concluding section of this practical assignment involves researching and designing an attack on a GCFW practical assignment that was previously posted within the last six months. The specifics entail three different attack scenarios. In order they are: an attack against the firewall itself, a denial of service attack originating from 50 compromised broadband systems, and an assault against any internal system through the perimeter.

I have selected the practical assignment by Michael Desrosiers submitted in April of 2002. The URL is: http://www.giac.org/practical/Michael_Desrosiers_GCFW.zip. His network diagram is depicted as follows:

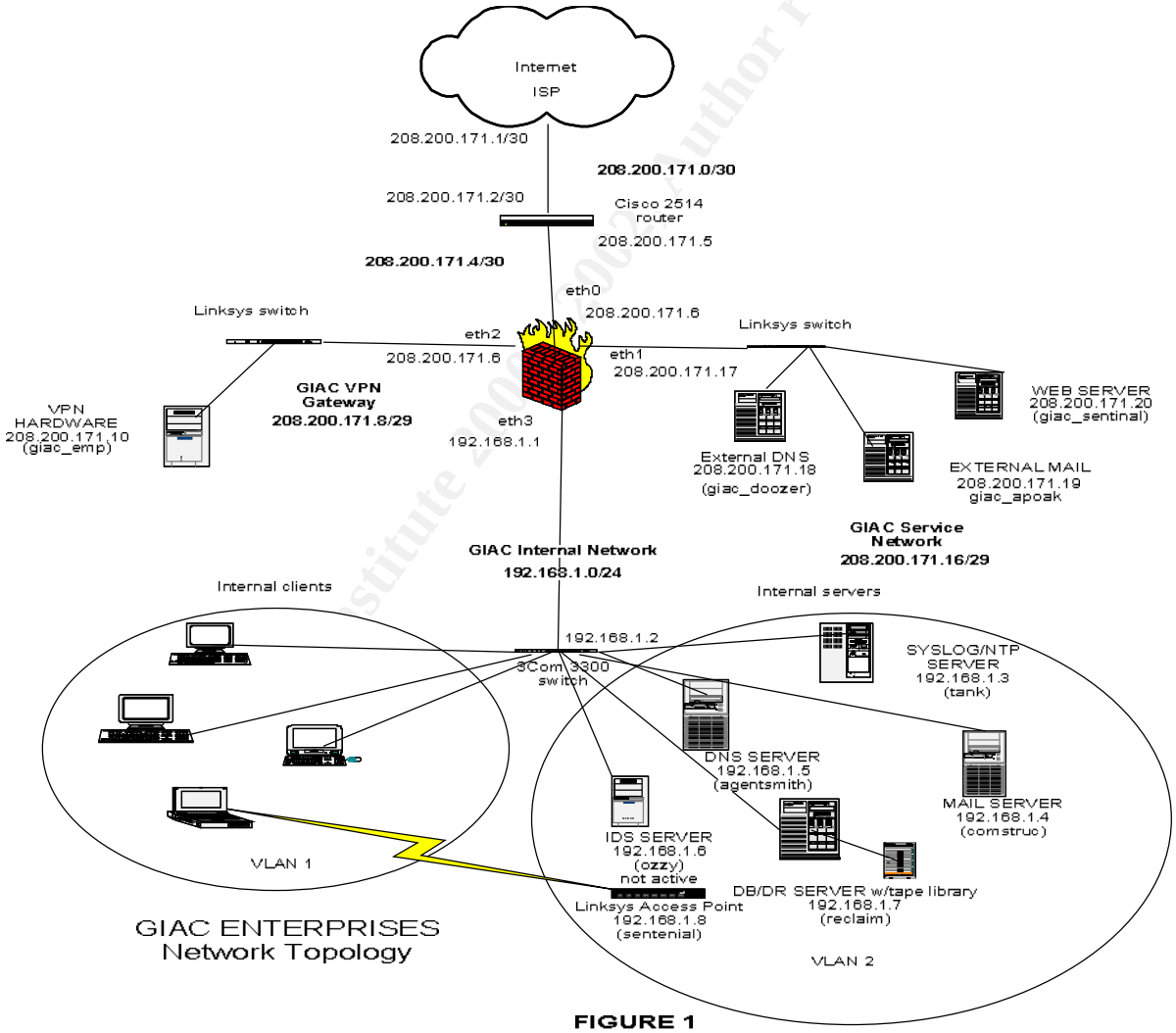


FIGURE 1

Reconnaissance Phase

It would be wise to gain as much information as possible on our enemy's camp before we attempt any offensive against our target. This provides us with huge advantages that can make the difference between having to 'carpet bomb' our foes position versus sending in a lone sniper. Moreover, our information gathering techniques should be as surreptitious as possible. We don't want to telegraph our intentions and give them the opportunity to plug a hole before our attack. We also don't want to give away our identity through sloppy tactics like ping sweeping or full port scanning. Such actions would raise alarms on their IDS and firewall logs. Therefore we shall use as much stealth as possible in our data-gathering mission.

We'll begin with using many of the same tools used to conduct our own design audit. The **Whois** utility will be our first step in trying to glean some information. Even though he didn't mention sterilizing the registration information in his practical, I'll give him the benefit of the doubt and suppose that I was only able to pick up some generic information such as a business mailing address, a contact position like 'network administrator', a phone number for the contact person, a domain name (GIAC.COM), and a block of network addresses used by GIAC Enterprises (208.200.171.0/28). No other domain names or subsidiary information was found.

Another sometimes-useful technique is to view the **source code** from their Internet web pages. Thanks to careless or egotistical programmers, they sometimes contain further data for our recon mission. Again, I'll give the benefit of the doubt here and say that it related nothing of additional use.

It was determined also that **Telnet** was locked down from external use.

Using **nslookup** I was able to determine the DNS server as having an address of 208.200.171.18. Zone transfers have been blocked so I'm unable to collect any further intelligence. However, given the small range of IP addresses I can some educated guesses. It's likely that one interface on the firewall is on the same segment as the DNS server and also a web server or mail exchange server. Further, he may be using variable length subnet masking (VLSM) on his registered addresses for his WAN links.

The **traceroute** tool is the next bullet in my gun. By trace routing to the DNS server using port 53 (DNS queries which are allowed to pass) I'm able to map out a good section of the GIAC service network:

```
$ Traceroute 208.200.171.18
Tracing route to (208.200.171.18), over a maximum of 30 hops:
    1 my-isp  (5.6.7.8) 17ms
```

2 GIAC-isp (12.13.14.15) 37ms
3 GIAC-border-router (208.200.171.2) 42ms
4 GIAC-firewall (208.200.171.17) 55ms
5 GIAC-DNS (208.200.171.18) 64ms

Trace complete.

I now try to identify the software and operating systems of his network equipment. I give his equipment the **Finger** command but to his credit he has disabled the finger service on all devices. **Banner grabbing** is also stymied and leaks no useful data. So I resort to the next level of tools to detect the operating system like **Queso, SS,** and **NMAP**. Nmap provides a large variety of methods to detect the O/S with several different switches. Using just a couple of them I'm quickly able to get what I need to help focus my attacks:

Commands:

Nmap –sS –p 80 –O –v GIAC.com
Nmap –sS –F –o giac.log –v –O www.giac.com//28

Revelations: GIAC-border-router is a Cisco 2514 running Cisco IOS version 12.0.
GIAC-firewall is Linux Red Hat 7.2 probably running it's own Netfilter/IPtables.
The GIAC DNS and Web Server are RS/6000 boxes running AIX 5100-01.

Now that I have identified the firewall, it's IP address, and its operating system; I would like to learn more about its rule base and configuration. Specifically, I want to learn the state (open, closed, filtered) of the firewall's service ports. Once again, there are several scanning tools available to me for this task. A few of them being: **Hping, Nmap,** and **Firewalk.**

Swiftly I discover that **TCP ports 25, 53, 80, 113, 443 and that UPD ports 53 and 500 are open. I also learn that all ICMP ports are open!**

What a wealth of information I now possess about my intended target! In a short amount of time I have a nice map of their network topology, the equipment they are using for their Internet services (hardware, software, and operating systems), some phone and address information (for attacks that I will discuss in a later section!), and even a list of open service ports on their firewall. I am now prepared for a much more focused attack on my target and have greatly increased my chances for success.

Firewall Assault

Armed with the knowledge from the recon phase, I can search the Internet for known vulnerabilities and tools that exploit them. Several organizations keep track of bugs and weaknesses in software and hardware. A few of the site I checked are: http://www.cert.org/, http://lists.insecure.org/#bugtraz, and http://lists.insecure.org/#vuln-dev

Even when narrowing my search down to specifics like "Linux Red Hat 7.2", "Netfilter", and "IPTables" I was still overwhelmed by hundreds of documented vulnerabilities. The following are just three examples that I quickly found.

Copied from: http://lists.insecure.org/#bugtraz

Bugtraq Full Disclosure Security list Web Archive [CARTSA-20020402] Linux Netfilter NAT/ICMP code information leak

From: Philippe Biondi (*biondi@cartel-securite.fr*)
Date: May 08 2002

- **Next message:** secure@conectiva.com.br: "[CLA-2002:481] Conectiva Linux Security Announcement - imlib"
- **Previous message:** Ulf Harnhammar: "CRLF Injection"

Cartel Sécurité --- Security Advisory
Advisory Number: CARTSA-20020402
Subject: Linux Netfilter NAT/ICMP code information leak
Author: Philippe Biondi <biondi@cartel-securite.fr>
Discovered: April 2, 2002
Published: May 8, 2002

Problem description
==========
The following bug exists in the netfilter NAT implementation: When the first packet of a connection is hitting a NAT rule, and this packet causes the NAT box itself to reply with an ICMP error message, the inner IP packet inside the ICMP error message is not un-NAT'ed correctly. This leads to the ability to discover which ports of a host are NATed and where the packet will really go. This can also lead to those ICMP error packets being dropped by stateful firewalls not recognizing the related connection.
Vulnerable versions
==========
All kernel patches from iptables package < ipables-1.2.6a are vulnerable.
All versions of kernel >= 2.4.4 and up to (at least) 2.4.19-pre6 use a vulnerable version.

These two advisories are copied from: http://www.cert.org/

Red Hat Information for VU#230307

Date Notified 02/28/2002

Date Modified 04/24/2002 04:00:15 PM

Status Summary Vulnerable

Vendor Statement

The Netfilter IRC DCC module is distributed with kernels in Red Hat Linux 7.1 and 7.2, although it is not used in default installations. Updated kernel packages with a fix for this issue are available from the Red Hat Network or linked from our advisory:

Red Hat Information for VU#234971

Date Notified 02/28/2002

Date Modified 04/22/2002 04:44:40 PM

Status Summary Vulnerable

Vendor Statement

Red Hat Linux 7.0, 7.1, 7.2 as well as Red Hat Secure Web Server 3.2 contain a vulnerable version of mod_ssl. However to exploit the overflow, the server must be configured to require client certificates, and an attacker must obtain a carefully crafted client certificate that has been signed by a Certificate Authority which is trusted by the server. Users who use client certificate authentication would be wise to upgrade or switch to the superior shared memory session cache, shmcb, which is not vulnerable to this issue. Updated mod_ssl packages will be available shortly at the following URL. Users of the Red Hat Network can use the 'up2date' tool to update their systems at the same time.

I suspect it will be easier to attack the underlying operating system (Linux) than the smaller and hardened firewall software. Especially gauging from the large difference in the number of known vulnerabilities. Attacking the O/S is even more insidious if successful. This would allow us not only to bypass the firewall, it would give us an inside platform from which to launch strikes against other internal targets. In addition we could cover our tracks since we could control all logging from that box to the logging server.

Again I turn to the World Wide Web to aid in my research for known exploits against Linux. Also, since I am not a coder, I will need sites that provide me with either the source code or the compiled executable programs. Once again my quest was quick and astonishingly easy. I list only two locations for exploits, but many more exist.

The first site alone I visited: http://www.insecure.org/sploits_linux.html listed 98 exploits with 65 of the giving you ROOT ACCESS! Incredible.

The next one I linked to was:
http://anticode.antionline.com/download.php?dcategory=linux-exploits&sortby
It contained 145 Linux exploits with the code scripts included. Jackpot!

I have merely to sort these lists by category, date, or popularity and then decide which ones match up with my intended desires. I can choose simply disrupt service all the way up to taking root control of the box. Furthermore, examination of the border router shows that they are NOT filtering out packets originating from private address networks (RFC-1918), Loopback addresses, broadcast or multicast networks. This leaves us the opportunity to further cover our tracks by sourcing all our attack packets as originating from their internal private address!

Conclusion: I was astonished at the amount of information you can learn about an organization and their network using Internet provided tools. Equally surprising are the vast amount of hacking tools available for even "script kiddies" level attackers. I would recommend that they reconfigure the border router to packet filter the network addresses I listed above as well as filter ICMP packets.

Denial of Service Attack

The assumption for this part of the attack is that we have gained control of 50 broadband type (cable modem or DSL) systems. As the title suggests, our intention here is to deny legitimate customers or employees the online services provided by GIAC Enterprises. This can be accomplished by either crashing one or more of the vital pieces in their online network, or by overwhelming the service with so many requests that legitimate users are locked out or become too frustrated by response time issues.

Once again, a quick check on the Internet for DOS attacks yields several ready to use tools. The fire site I visited was:
http://anticode.antionline.com/download.php?dcategory=distributed-attack-tools&sortby

It lists five distributed DOS style attacks. They are:

- **Blitznet:** A SYN flood attack method.
- **Slurpie:** A distributed password file cracker.
- **TFN:** Is a Tribal Flood - distributed flood network client & server type attack tool.
- **Trinoo:** Is a DDOS attack tool.
- **Saltine-cracker:** is a distributed password audit tool.

For this attack I'm not looking to crack their password files so I won't use Slurpie or Saltine-cracker. I will also pass on Blitznet since it employs a SYN flood method of DOS. Being a well-known attack, several operating system patches and many other countermeasures can be in place to mitigate or eliminate the SYN flood attempt.

> **For example: Increases in system RAM and in the size of the connection queue for SYN requests, lowering the timeout period for connection establishment, and O/S patches. In addition, some IDS systems can help relieve the attack by sending Reset commands to the system being attacked when it detects a flood occurring.**

I'm not suggesting that either of those attack methods won't get the job done, it's just that I think I will have a better chance of victory by saturating their WAN links. Simple math will prove my case.

I have control of fifty DSL modems at an average speed each of say, 768Kbs. This gives me (50 x 768Kbs) a crushing 38.4Mbs worth of bandwidth to overwhelm his paltry (1.54Mbs) T1 line. Imagine a water main trying to drain into a pipe 25 times smaller than itself! It's going to back up and be messy.

There is virtually nothing GIAC could do to avoid this attack the first couple of times. They could increase their ISP WAN links to help mitigate the problem, or they could work with their ISP and the authorities to help trace, capture and prosecute the offender. Both will take a significant amount of time and effort. And neither solution fully guarantees their future security from these aggressions.

Internal Target Strike

For this last part of the assignment, I thought I would try an approach that is both different and fun. I could use the same tools and techniques that I employed against the firewall and produce similar results. However, I want to highlight an area of security that often goes overlooked and unattended. Security breaches by external hackers seem to get all the media attention yet FBI crime statistics show that the much larger threat comes from internal sources. Employee carelessness, gullibility, and dissatisfaction can be far more damaging. The following excerpt is from an FBI congressional report on cyber threats from the URL listed below it:

> "Insider Threat
> The disgruntled insider is a principal source of computer crimes. Insiders do not need a great deal of knowledge about computer intrusions, because their knowledge of victim systems often allows them to gain unrestricted access to cause damage to the system or to

steal system data. The 1999 Computer Security Institute/FBI report notes that 55% of respondents reported malicious activity by insiders."

http://www.fbi.gov/search?NS-search-page=document&NS-rel-doc-name=/congress/congress99/nipc10-6.htm&NS-query=computer+hacking&NS-search-type=NS-boolean-query&NS-collection=FBI_Web_Site&NS-docs-found=7&NS-doc-number=7

I will demonstrate some frighteningly easy social engineering attacks to compromise an internal system. Human beings are both the strongest and weakest points in network security. Strong because of our cognitive powers, and weak because of our, well, humanness. In pointing out some of our fallibilities I hope to both entertain and teach you about some of the most overlooked security holes any organization faces; its own trusted employees.

I can start by using the address and phone numbers I obtained during the reconnaissance phase. Couple those along with a little Internet searching about their partners and I am ready to start the scheme. The following are fictional excerpts from supposed telephone calls I made over a several day period.

Scenario #1

After calling the companies switchboard and having them forward my calls to places like "the operations center", "the web site administrator", or "someone in the IT network group" I quickly compile a list of names, titles and extensions. Next, posing as a recruiter, I directly call some of the engineers…

Me: Hi Tom, this is Harry Headhunter calling from HH Recruiting and Associates. I was given your name by [coworker] who said you are someone who is knowledgeable in networking and might be looking for new opportunities.

Tom Techie: Hello Harry. I'm not actively looking for a new position but I like to keep my options open. What do you have for me?

Me: Well Tom, I've got a company that is looking for a networking leader to manage their Internet infrastructure. The pay range is starting around $120,000 dollars including a yearly bonus and a full load of benefits. Does that sound interesting to you?

Tom Techie: Yeah, sounds great! [Drooling] What company is it?

Me: I can't tell you the name specifically until we agree to and set up an interview. But I will tell you they are a very well know retail chain and their data center

where the position is located is in Maui! Of course a full relocation package would be extended to you. But before I let them know you are interested, I need to get some preliminary information from you about your experience.

Tom Techie: Sure, what do you want to know?

Me: What kind of equipment and software do you work with now?

Tom Techie: Well, I'm in charge of our network security. I configured and administrate the corporate firewall and routers. Our routers are all Cisco and our firewall is Netfilter on Red Hat 7.2.

Me: What models and software versions have you specifically worked with?

Tom Techie: Well our router is a Cisco 2514 running IOS version 12.0.1. The firewall I just upgraded to IPTables version 1.2.4 and I also installed Bastille Linux 1.3.pre10 on the firewall server. I also configured the ACL's and NAT myself.

Me: What other equipment are you directly experienced with?

Tom Techie: I also installed our DNS server. It runs on an RS/6000 with AIX 5100.

Me: Do you work with the web or mail servers?

Tom Techie: No, Dan Disgruntled installed those. He's not been happy lately and I know he would be interested in other opportunities too. Just don't tell him about this one!

Me: Okay, I'll keep him on my list for another time. Tell me about how you configured the firewalls and NAT. Describe any problems you had and how you overcame them…

As you can see, a couple of easy phone calls can take the place of hours or days of using hacking techniques. In a short time I can obtain a ton of information about their networking equipment from the experts who are all to eager to impress me with their knowledge. I've also learned the name of someone who is unhappy with the company and may be willing to divulge even more critical information!

Scenario #2

In this instance, I call into the companies help desk and ask them to forward me to the marketing directors secretary. This will make it appear to her that the call originated from the corporate help desk.

Me: Hi Sally, this is Adam Administrator calling from computer operations. An audit report I ran last night shows we need to upgrade your PC with the latest security patch.

Sally: Okay, when do you want to do it?

Me: If you've got just a couple of minutes right now I can walk you through it over the phone.

Sally: Oh, okay. What do I need to do?

Me: Well first, save your work if you are in the middle of anything. Then I need you to go to a web site and pull down the patch. **(I sound so concerned for her work.)**

Sally: All right, I've saved my documents, now what?

Me: First, pull up your browser and go to www.ulamer.com.

Sally: It's asking me to "login".

Me: Correct. Now just enter your network signon and password. You don't need to tell me what it is. I could have done this for you but then I would have had to change your password and that's a pain for you. **(I'm so nice! And I cleverly defeat their policy of not sharing your password with anyone.)**

Sally: I see. Okay, now it has a message that says, "Download complete, please reboot to continue".

Me: Great! Now just reboot and we're all done.

Sally: Well, that was easy.

Me: Yep, I told you it would only take a couple of minutes. Thanks for your help…

Here we go again. In just a few minutes I have not only captured a valid users signon and password, but I have installed a Trojan horse program on her PC! The

Trojan horse could be a virus, it could be a keystroke logger, or it could be a remote control program that I could connect with and be directly on their intranet!

The number of different attack scenarios possible is limited only by the imagination of the assailant. The best way to help close these types of security holes is through education and motivation. Every employee should receive training about protecting information. They should be made aware of these security threats and the importance of their nature. They should be instructed never to give out information that could potentially cause damage and not to trust anyone who they are not certain of their identity. Finally, each person must feel that security is part of his job description and that he has a vested interest to remain vigilant.

Appendix A: Signon and Password Policy

GIAC Enterprises Password Policy

1. User ID's will be unique.
2. User ID's will be a minimum of six characters.
3. Remote access sessions will automatically time out after 30 minutes of inactivity.
4. Transmission of user ID's and passwords will always be encrypted and never in clear text format.
5. Storage of user ID's and passwords will always be encrypted and never in clear text format.
6. User accounts will be "locked out" after three incorrect signon attempts.
7. Password resets and account lockouts will be handled through the corporate help desk and only after they have authenticated your identity.
8. Passwords must be a minimum of 6 alpha AND numeric characters.
9. Passwords will expire after a maximum of 30 days. (User notification of impending change should be 10 days in advance.)
10. A user cannot change his password to one that was previously used in his last twelve passwords.
11. It is recommended that users utilize upper and lower case letters and special characters within the password. Further, the password should not be contained in a dictionary nor should it be easily guessed (i.e. a pets name).
12. User should be instructed to never disclose his signon or password to anyone. No authorized agent will ever call to ask for this information.
13. User should be educated about the need for password security.

Appendix B: Internet Usage Policy

Note: This policy was copied entirely from reference source [3].

Company network resourced, including those used to gain access to Internet-based sites, are only to be used for the express purpose of performing work-related duties. This policy is to insure the effective use of networking resources and shall apply equally to all employees. Direct supervisors may approve the use of network resources beyond the scope of this limited access policy when said use meets the following conditions:

- The intended use of network resources is incidental.
- The intended use of network resources does not interfere with the employee's regular duties.
- The intended use of network resources serves a legitimate company interest.
- The intended use of network resources is for educational purposes and within the scope of the employee's job function.
- The intended use of network resources does not break any local, state, or federal laws.
- The intended use of network resources will not overburden the network.

Failure to comply with this Internet usage policy can result in disciplinary actions including loss of Internet access privileges or TERMINATION.

References and Acknowledgements

[1] SANS Institute Conference material, Track-2: Firewalls, Perimeter Protection, and VPN's, April 2002, Orlando, FL

[2] Web Commerce Technology Handbook, by Daniel Minoli and Emma Minoli, McGraw-Hill, 1998.

[3] Mastering Network Security, by Chris Brenton, SYBEX Inc., Network Press, 1999.

[4] Hacking Exposed – Second Edition, by Joel Scambray, Stuart McClure, and George Kurtz, Osborne/McGraw-Hill, 2001.

[5] Managing Cisco Network Security, Student Guide Version 1.1, Copyright Cisco Systems Inc, 1998.

[6] Virtual Private Networks for Dummies, by Mark Merkow, IDG Books Worldwide INC, 1999.

[7] Cryptography and Network Security – Principles and Practices – Second Edition, by William Stallings, Prentice Hall, 1999.

World Wide Web Resource Links

http://cisco.com
http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/vac_ds.htm
http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/index.shtml
http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/p515e_ds.htm
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/cmdref/index.htm
http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/tech/nat_wp.htm
http://www.cisco.com/warp/public/cc/pd/si/casi/ca2950/index.shtml
http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/prodlit/ids41_ds.htm
http://www.cisco.com/univercd/cc/td/doc/product/core/7204/index.htm
http://www.cisco.com/univercd/cc/td/doc/pcat/7200.htm
http://www.cisco.com/wwl/export/crypto/
http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/news/vgano_ai.pdf
http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/index.shtml
http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/supcc_ov.htm
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/rbkixol.htm#52290

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/config/sit2site.htm#xtocid7
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_5_4/msfc/acc_list.htm
http://www.cisco.com/univercd/cc/td/doc/product/core/7204/7204ig/main4icg.htm
http://www.cisco.com/univercd/cc/td/doc/product/core/7204/7204ig/cfig4icg.htm
http://www.cisco.com/univercd/cc/td/doc/product/core/7204/7204ig/inst4icg.htm
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122mindx/index.htm
http://www.ibm.com
- http://www-1.ibm.com/servers/aix/products/aixos/
- http://commerce.www.ibm.com/content/home/shop_ShopIBM/en_US/eServer/pSeries/entry/B50_7046B50B.html
- http://commerce.www.ibm.com/content/home/shop_ShopIBM/en_US/eServer/pSeries/entry/B50.html

http://www.microsoft.com
- http://www.microsoft.com/isaserver/
- http://www.microsoft.com/windows2000/server/
- http://www.microsoft.com/exchange/techinfo/default.asp
- http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/virus/virus.asp
- http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/mailexch/default.asp

http://www.arin.net/library/index.html
http://www.iana.org/
http://www.giac.org/
http://www.sans.org/newlook/home.php
http://www.sans.org/top20.htm
http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm
http://www.isc.org/products/BIND/
http://www.coyotepoint.com/equalizer.shtml
http://www.coyotepoint.com/
http://www.pcmag.com\firewalls
http://www.pcmag.com/article/0,2997,s=1470&a=3566,00.asp
http://www.foundstone.com
http://lists.insecure.org/#bugtraz
http://lists.insecure.org/#vuln-dev
http://www.insecure.org/sploits_linux.html
http://www.antionline.com
http://anticode.antionline.com/download.php?dcategory=distributed-attack-tools&sortby

Additional Acknowledgements:

- All manufacturers equipment pictures shown were copied courtesy of their respective web sites.