Global Information Assurance Certification Paper

GIAC GCFW Practical Assignment
Version 1.6

Securing GIAC Enterprises
Rocky Mountain SANS

By

Patrick Thibeault

August 21, 2001

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

Background

GIAC Enterprises is a growing company that provides fortunes for fortune cookie companies. Its strong Internet presence is used as the means for communicating with customers, suppliers and partners. They have international partners and clients. Due to a recent acquisition, GIAC Enterprises is revamping its current architecture to provide for increased security and scalability. As always, cost is a factor. Preliminary analysis has indicated that there will be no budget for redundancy or high availability this year. It will be addressed in next year's budget.

GIAC's recent acquisition of "Quirky Quotes" (QQ) has created a need to increase network capacity and integrate QQ's existing network with GIAC's. By eliminating QQ's Internet presence and using a private network between the two offices, they can have the full access they need to utilize internal systems and increase security. By having one point of presence to the Internet, costs can be saved by eliminating the need for duplicate perimeter security systems. Since GIAC Enterprises has a security policy in place which states that "Internet access will only be provided at the corporate level," it was easy to convince them to cancel their current Internet service.

GIAC Enterprises needs to provide an Internet accessible web page for their customers in addition to Internet access, email and DNS services for their employees. They also need to provide an HTTPS site for their authors and partners so they can have the ability to download and upload fortunes.

Security Policy Overview

The security policy eluded to earlier was created in anticipation of this project. It covers many aspects of internal security and the perimeter security requirements. Some highlights from that document that will be pertinent to this project are:

- GIAC Enterprises will be protected by a firewall.
- There will be no direct connections from the Internet to systems on the internal network.
- Internet security will be layered with IDS systems at each layer watching for breaches at any and all layers.
- Remote access will be provided only through a VPN. No modems.
- GIAC will be a good citizen and prevent egress spoofing filtering from their network.
- Software patches will be installed in a timely manner. A weekly maintenance window will be provided for these patches. If deemed necessary, patches can be and should be applied immediately.
- Virus protection will be done on two levels, at the server/desktop level, and on the email servers.
- Logging will be done on all systems accessed from the Internet, systems used for

Internet access and any other key systems where accountability is needed.
- No clear text passwords of any kind will be transmitted across the Internet. This means no POP3.
- Banners for restricted access systems shall be changed to state the fact that access is restricted.
- Names for servers and systems will be arbitrary and will not disclose the OS or purpose of the system. (Since GIAC Enterprises is located in Denver, Colorado, USA, systems are named after ski resorts.)
- Systems accessed from outside of the company will be locked down to only allow needed services.
- Delivery of all fortunes must be made across an encrypted link or through traditional mail.
- Syslog and IDS will actively report configuration changes and attacks to the administrator.

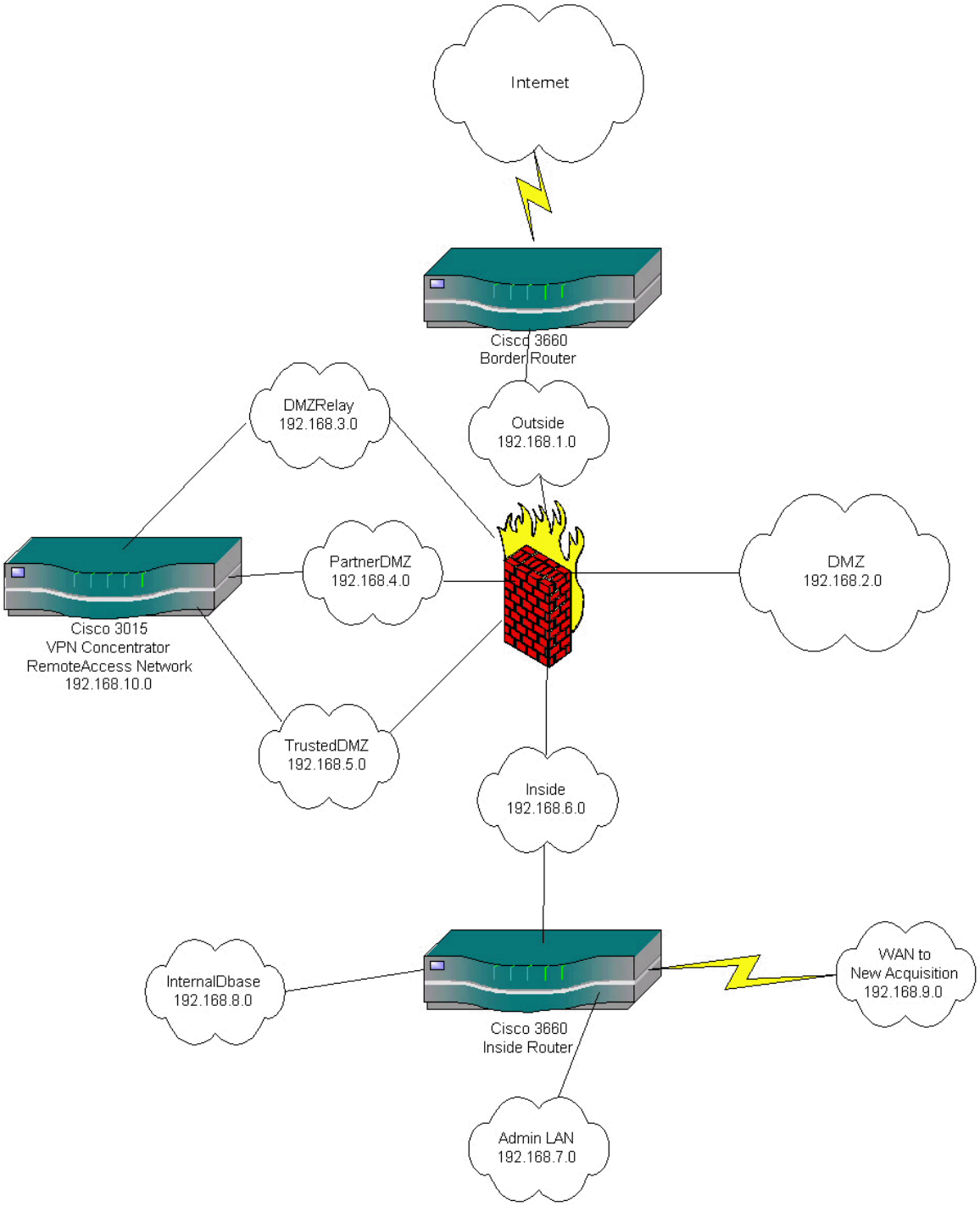
Hardware/Software Solutions

GIAC Enterprises has strong technical experience with Cisco devices and Microsoft operating systems. There is some knowledge of Unix flavors but a decision has been made to use Microsoft wherever possible. This is because it is easier to find consultants and employees familiar with Microsoft than the Unix type systems. Linux with Snort will be run as the IDS system for cost reasons. The corporate firewall will be a Cisco PIX.

Network Design

The network design is multi-layered. It involves a primary firewall, a border router, an internal screening router, and multiple DNS, mail and IDS servers. IIS 5 will be used as the web server, MS Exchange 2000 will be used as the mail servers and MS DNS will be used for DNS services. The VPN solution will be a Cisco 3015 concentrator.

GIAC's Network



Network Diagram Explanation

The network diagram depicts clouds for Local Area Networks. The following is a description of the purpose of each of those networks.

- Outside

The outside network will use private addresses for obscurity. It will host the border router, PIX Outside interface, syslog, and IDS servers.

System	IP
Border Router	192.168.1.254
PIX	192.168.1.1
Syslog	192.168.1.5

- DMZ

The DMZ LAN is for all Internet accessible systems that do not need access into the private network. This prevents vulnerabilities on these systems from affecting other systems that do have access into the private network.

System	IP	Public IP
PIX	192.168.2.1	
WWW	192.168.2.5	100.100.100.1
ExtDNS1	192.168.2.6	100.100.100.2
ExtDNS2	192.168.2.7	100.100.100.3

- DMZRelay

The DMZRelay LAN is for Internet accessible systems that need to pass information onto the private network.

System	IP	Public IP
PIX	192.168.3.1	
Mail1	192.168.3.5	100.100.100.4
Mail2	192.168.3.6	100.100.100.5
VPNPublic	192.168.3.7	100.100.100.6

- PartnerDMZ

The Partner DMZ is used to host the two web servers for partners and authors to access via the VPN. They will have no access to the Inside, DMZ, DMZRelay, TrustedDMZ or the Outside networks. The only connection to the private network from this LAN will be from the transactional database server to the internal database server.

System	IP
PIX	192.168.4.1
WWWA	192.168.4.5
WWWB	192.168.4.6
Dbase	192.168.4.7
VPNDMZ	192.168.4.254

- TrustedDMZ

The trusted DMZ is a LAN where VPN users will connect to the internal network. It will have full permissions into the network for Remote Access VPN users, but will be monitored by the firewall.

Systems	IP
PIX	192.168.5.1
VPN	192.168.5.254

- Inside

The inside network is where the internal corporate servers will reside including email, Internal DNS, and WebSense. This is where the bulk of the users at GIAC's Denver office will connect.

System	IP
PIX	192.168.6.1
Syslog	19.168.6.4
IntMail1	192.168.6.5
WebSense	192.168.6.7
Internal DNS	192.168.6.8
PDC	192.168.6.10
InternalRouter	192.168.6.254

- Admin LAN

The Admin LAN will be protected by IOS firewall rules from the rest of the network.

This is where the payroll server and sensitive HR data is stored. This is also the LAN the administration employees will attach their computer systems to.

- Internal Database LAN

The Internal Database LAN's sole purpose is to protect the database from internal users.

System	IP
Internal Dbase	192.168.8.5
Router	192.168.8.254

Device Architecture

Internet Access

A Tier 1 provider will be chosen to provide Internet access for GIAC Enterprises. This will help ensure response times for customers from around the globe. Since redundancy is not feasible in this year's budget, only a single T1 will be installed. Since most of our data transfers are text documents and not huge binary files, a T1 has been deemed sufficient until usage increases.

Since GIAC Enterprises does not have a routable IP address block of its own, it will be required for GIAC to obtain a /24 block of addresses from their ISP. With the use of Network Address Translation, there will be plenty of addresses to provide the needed presence on the Internet with room to grow.

Border Router

The border router is the device sitting between the Internet connection and GIAC Enterprises' private network. It is the first line of defense to protect from unauthorized attempts at the network. The Cisco 3660 router has been chosen. It will be configured with 256MB of RAM, 32 MB of Flash memory, and the 2 Fast Ethernet Network Module with the two CSU/DSU T1 wan cards. With a single LAN connection to the internal network and a single T1, the additional cards provide room to grow. The 3660 was chosen over the 3620 and 3640 because of processor speed and the ability to add more than 128MB of main memory. With BGP a possibility in the future, the extra memory and processor will help keep the router running with increased loads in the future. There are no General Deployment IOS versions for the 3660, so IOS 12.0.7T IP/FW/IDS has been chosen. Since there will be a high-end processor and extra memory in this router, GIAC will be able to take advantage of the features of the IOS and provide some preliminary firewall and IDS support at this point in the network.

Network Switch

The network switch chosen for the connection between the border router and the PIX firewall can be any 100 MB switch with at least 4ports. The first two ports will be used for the router and then the firewall, and the others will be used for an IDS server and syslog server. All other unused ports on the switch will be disabled.

Firewall

A Cisco PIX firewall was chosen for the primary firewall system. It provides stateful packet inspection with its Adaptive Security Algorithm. Being a hardened appliance, GIAC can rely on Cisco to harden the OS so they won't have to. It would be beneficial to have a second firewall from another vendor, but hopefully one can be acquired in the future. Since the IOS firewall and PIX firewall do not use the same type of architecture, it is hoped that both systems will not be vulnerable to the same exploits.

The Cisco PIX 525 was chosen for this network. The PIX is equipped with an extra 4 port 10/100 Ethernet card to provide layering between systems. With the fixed configuration of two interfaces, there will be a total of 6 Fast Ethernet interfaces. Version 6.0.1 software has been chosen. It is the newest version of the software and it does not have any known bugs that could be a problem. It also has some new features that should be implemented.

One interface on the firewall will serve the public Internet connection; the second (in order of security rights) will be used for the untrusted DMZ number 1. It will serve as the network hosting all systems that do not need internal access. These would be the external DNS and the public web site.

The third interface will support the DMZ Relay LAN. This DMZ will be used for the mail relay servers, where Trend Micro's Interscan Virus Wall will be running. In addition, the public interface of the VPN solution will be connected to this network.

The fourth interface will be for the Extranet for web servers used to receive new fortunes from the authors. It will also be the same network where the partners come to retrieve and leave their fortunes. Both systems will be accessed via SSL and require authentication to logon. Each system will query a transactional database and will be granted access on a non-standard port to do ODBC queries to the internal database.

The fifth interface will be used as a trusted network, with no port blocking and giving the firewall one last time to monitor for abnormal activity. This is where the remote access VPN users will enter the network, so this is where the VPN's private interface will be connected. By checking the traffic, GIAC can make sure that remote access users are not unknowingly being used to penetrate the network. This LAN provides an outbound connection to the Internet as well as the internal network.

The sixth interface will serve the purpose of connecting the internal GIAC network to the

Internet. It will filter what the employees do on the Internet.

VPN

The VPN solution for the network will be the Cisco 3015 VPN Concentrator. It is capable of 100 simultaneous connections and is upgradeable if the need arises. Software version 3.1 has been chosen because it has an ability (though it is yet to be seen) to notify client software of software updates. This will help in client administration going forward. The client software will be the 3.1 client because it has support for Windows XP and GIAC needs to support all of its users.

Because the 3015 has a third interface, the same VPN concentrator for remote access, as well as access for our partners and authors, will be used. The partners will be limited to access only on the DMZ port. This is where the SSL web server that they will interact with will be located. They will only have access to HTTPS through this VPN.

Internal Switch

The device connecting the private interface of the firewall to the rest of the Internal network is a Cisco Catalyst 6500. Systems on this LAN will be the WebSense server (used for web filtering), the Internal DNS servers, the Internal Exchange email servers, and other server systems that will perform various functions for internal users. This is the same LAN where most of the user systems will be attached. This LAN will be connected to another Cisco 3660.

Internal Router

The internal router will also be a Cisco 3660. It will be configured with 128MB of RAM, 32 MB of Flash memory, and two network modules that have the 2 Fast Ethernet and 2 WIC slots. It will also have two CSU/DSU T1 wan cards filling two of the WIC slots. IOS version 12.07T with the IP/FW/IDS feature set will be used. This device, with the larger processor, will be used to provide IDS alerting on the Internal networking and limited firewalling to the Internal Database LAN and the Administration LAN.

Other equipment

Other equipment needed for this network include two more LAN switches for the Administration LAN and the Internal Database LAN. Cisco Catalyst 29xx XL switches will also be used here. The port number will vary on how many users need to be attached to these networks. All unused ports will be shutdown.

In addition, a few syslog servers will be used. The first will sit on the LAN between the PIX firewall and the border router. It will collect syslog messages from the border router. The second syslog server will be sitting off of the Catalyst 6500 and will collect messages from The PIX Firewall and the internal routers and switches. Each system will report IDS alerts to the administrator's email.

Also, Snort IDS will be placed on many areas of the network, like off of all six LAN interfaces of the PIX and on the protected networks for Administration and the Internal Database. Since Snort is freeware and runs on Linux, it will enable the use of older Pentium computers to serve as the platforms for these systems. Cost will be minimal.

Software

We will be using Trend Micro's Interscan Wall for the mail relay servers. They will be running on Windows 2000. Care will need to be taken to ensure that the OS is correctly patched.

The web servers will be running IIS 5 on Windows 2000. No domains will be used and each system will be a standalone system.

The DNS servers will also be Windows 2000 systems running Microsoft DNS.

The database systems will be Microsoft SQL 2000, running on Windows 2000.

The syslog servers will be running Windows 2000. The syslog application will be Kiwi Syslog from Kiwi Enterprises.

The Web filtering software will be WebSense. It has a database that compares URL requests to the policy we create. It then allows or disallows web access per that policy. Since it integrates with the PIX, this is transparent to the users.

The only non-Windows OS that will be used are the Linux systems used to support Snort.

The vulnerability assessment tool Cyber Cop will scan all systems to identify vulnerabilities before being placed online. This will provide a final check to verify all patches have been installed.

Architecture Summary

When all of the previous mentioned components are assembled, there will be a layered

defense. The border router will take care of much of the noise, and the PIX firewall will monitor and manage the remaining traffic. Some inbound connections to the DMZ will terminate there and that LAN does not have further inbound access, adding further protection. This will prevent IIS vulnerabilities from giving a hacker access to systems that can then enter the internal network, like email. The email system is on a separate DMZ, and with the proper rule set, only smtp vulnerabilities will be the weakness for that network.

The Extranet DMZ will have SSL and a database server. These systems will only be able to talk to authenticated VPN users. The database will only be allowed to talk to the internal database. This will prevent random Internet access attempts to these systems.

Remote access VPN users will have full access. While they are on the VPN, GIAC will redirect all of their traffic from their home system through the VPN by disabling split tunneling. This will allow the firewall to check their traffic for possible hacking.

The internal router running firewall and IDS IOS will provide some security from Internal hacking.

With two systems logging the router and firewall traffic and eight Snort systems on top of three Cisco IDS systems, redundant logging and intrusion checking will occur.

Applying the Architecture

The following contains descriptions on how to configure some of the devices for the network we have planned.

As with anything, good security practices can help make securing a network easier. It is always beneficial to have training because some of the hackers out there are very skilled. Training will help secure your network and will keep security managers focused on new techniques. It is important to be well trained before attempting a project such as this.

Passwords should be difficult to guess. A good security policy will outline what methods to use when creating passwords. They should be over 6 characters long, both alpha and numeric, and include special characters. Accounts should be locked out after 3 failed attempts and old passwords should not be reused. Also, passwords should expire or be changed every 90 days. Not all systems provide mechanisms to enforce rules like these, but if it is defined in a security policy, people can be reminded of them.

Another part of general security is that password files should be saved to an offline disk like a floppy. If possible, it should be locked in a drawer or lock box where access is limited to authorized personnel.

Physical security means making sure the equipment and systems that are being protected are locked up. In GIAC Enterprises' case, this means having the main systems locked in a secure computer room. Access to this room is via a keypad entry. Only authorized personnel have access to this room.

Power redundancy and climate control will also help keep the systems secure. The possibility of a malicious person shutting off your AC or turning off other vital equipment like the UPS system should be considered. For these reasons, the controls for these systems should also be in a secured room.

Border Router

Once the higher-level security needs are met, equipment security comes into play. For a good start on securing the border Cisco router, visit Cisco's web page at: http://www.cisco.com/warp/public/707/21.html

Note that Cisco configurations do not always show default settings. Also, default settings vary between IOS versions. It is always a good idea to reissue commands even though you know they are enabled by default. This will help ensure security.

After loading the IOS to the router, and assuming it has no configuration, the router needs to be configured for functionality.

One Ethernet and one Serial interface will be configured for use on the network. The serial interface will be assigned an IP address given by the ISP. It will not be from the pool of public addresses assigned to GIAC by the ISP.

The Fast Ethernet interface will be addressed with a private address. This will allow this LAN and the systems on it to be only accessible from this LAN.

Routing on this router will have a default route to the ISP, and a single static route to the PIX's public interface for the block of assigned addresses. No dynamic routing protocols will be enabled.

That is all that is needed to provide a functioning router for this purpose. From here, securing this router will be next.

General Security

Some more commands to enter to restrict access and services on the border router are:

service tcp-keepalives-in

This command makes sure all VTY sessions are still in use and that someone

couldn't lock up all of the VTY sessions. It is vital not to allow VTY access to this router at all. This command will only prevent problems if someone mistakenly does allow VTY access down the road.

no ip http server

This command prevents http management access to the router. This interface is known to have bugs and really does not need to be allowed for an experienced administrator.

No snmp-server

This will remove SNMP from the router. SNMP can be used to gather information about the router.

no service udp-small-servers
no service tcp-small-servers
no service finger
no ip bootp server

These all remove services that can only give away information or leave the router susceptible to Denial of Service attacks.

no ip source-route

This command prevents packets with source route information from passing through the router. There are few, if any, real world reasons why someone would need this on their Internet border router.

no cdp run

This disables the Cisco Discover Protocol. This protocol talks to nearby Cisco devices and advertises information about the router. This is handy on private networks, but gives away information to the ISP router and other directly connected devices.

no ip unreachables

This command will keep the router from responding with ICMP unreachables messages. Hackers can use these messages. They tailor their attack to your network configuration based on the information received in those messages. If your router does not provide this information to them, they will have to spend more time finding out for themselves if systems are available.

scheduler interval 500

The scheduler interval command makes sure that the router is not overwhelmed with packet traffic and will process processor interrupts at least every 500 milliseconds.

```
banner motd ^C
Authorized GIAC Enterprises Employees Only!

Unauthorized Access Prohibited by Law and WILL BE Prosecuted!

Use is subject to monitoring!
^C
```

The banner motd command puts the sting of characters between ^c to ^c on the screen when a user connects to the router. This will alert the user that the system is protected and that legal action will be taken if necessary to prosecute inappropriate use. This is a better message than one that simply "Welcomes" any unauthorized user.

Under each network interface the following commands should be issued:

IN GIAC's case the two interfaces are:

```
int fastethernet 0/0
```

and

```
int serial 0/0
```

```
no ip proxy-arp
```

This makes sure the proxy arp feature on Cisco routers are disabled.

```
no ip redirects
```

This command prevents the router from sending ICMP redirects. In this configuration, the router should never have to, but if changes happen to the network design, this will ensure traffic continues to pass through the access control lists on this router.

```
no ip directed-broadcast
```

The no ip directed-broadcast command prevents directed broadcasts. This is the

feature exploited by Smurf attacks.

Passwords and Management

Now let's add passwords and limit who can connect to this router.

From global configuration mode, type:

Service password-encryption

This encrypts the passwords in the configuration so someone looking over your shoulder could not easily read the password from the screen or a printed copy of the configuration. This is not to be considered a secure encryption method and will only limit casual viewing of the password. Limiting access to the configuration files and backups of this file is important.

Enable secret xxxxx

This sets the enable password. The enable password allows changes to the router. Do not use the "enable password" command. That password is also an easy encryption method. "Enable secret" uses MD5 for encryption and is harder to crack. Use a password that is difficult to guess and use numbers and different cases. This will help to make the password harder to crack.

```
Line con 0
Login
Password xxxxxx
```

This sets the password and prompts for a password on the console port of the router. Since GIAC Enterprises has multiple network connections in each office, the console port will be patched through to the serial port of the router administrator's PC. By doing this, telnet to the router will not be allowed at all. This prevents clear text communications to the router, which can be picked up by packet sniffers.

```
Line aux 0
Login
No password
Access-class 18 in
Transport input none
Transport output none
Line vty 0 4
Login
No password
Access-class 18 in
```

```
Transport input none
Transport output none
```

This will lock down the aux port and the VTY ports on the router. First, set the router to prompt for a password, and then with no password set, no one can log on. The access-class statement refers to access control list number 18 which will be defined in the next step. It will limit who can connect to the ports based on the source IP address. The transport input and output commands prevent any access to these ports or the ability to use these ports outbound. This is a good extra step to take when securing VTY and AUX ports.

Then exit back to global configuration, and create the access-list for the VTY ports.

```
access-list 18 deny any
```

This secures the Aux port and VTY ports in case someone turns on the password command. Why the number 18? It is better to be random than predictable.

Logging

Now that services have been shut off and access has been restricted, it is time to set up logging on this router.

The first and most important thing to remember with logging is to have an accurate timestamp. With most computers, this is done with Network Time Protocol (NTP). If each system had a different time, then being able to track a hacker's progress through the network would be thwarted since the time for every log entry would have to be adjusted. NTP ensures that all systems on the network are within 100ths of a second of each other.

To configure NTP, type the following in global configuration mode:

```
ntp server 18.26.4.105 version 2 prefer
ntp server 18.72.0.3 version 2
```

This will set two clock sources on the Internet to be the NTP clock source. These sources are publicly available NTP clock sources. It would be better to bring in a private NTP clock source for the network to insure that the clock source is valid. This is expensive and GIAC has chosen to use two well-known public Internet clock sources.

Next, configure the router to log timestamps correctly and for the correct time zones. Since GIAC is in Denver, the following would be added to the router:

```
clock timezone mst -7
clock summer-time MDT recurring
```

This sets the timezone and offset from GMT time and sets the router to follow Daylight Savings Time every year.

```
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
```

These commands set debugging and logging timestamps to show the date and time for the local time zone and to show the time zone. This makes sure there is no mistake understanding when events occurred.

Now to configure the logging of the events that now have correct timestamps, type the following:

```
logging trap debugging
```

This sets the logging event to debug which means to log all events no matter what severity.

```
logging buffered debugging
```

This allows syslog messages to be stored in memory until that memory space fills and then it overwrites the oldest messages. This is helpful in problem determination.

```
no logging console
```

This prevents all of the logging events from being sent to the console connection. When the firewall and IDS features are enabled, the console port would be overwhelmed, locking you out of the router.

```
logging facility local6
```

This sets the facility level to log events on the syslog server. This is useful to create different log files for different systems on a single syslog server.

```
logging source-interface FastEthernet0/0
```

This sets the syslog message's source IP address to the address assigned the fastethernet interface 0/0.

```
logging 192.168.1.5
```

This will send the syslog messages to the syslog server at that IP address. In this case, the router's LAN, along with the firewall, is on a private address block and will only log messages from this router, so outside connections to this syslog server are limited.

Context Based Access Control

Context Based Access Control (CBAC) is Cisco IOS's firewall feature set. It is an advanced method of access control lists. GIAC Enterprises has bought a "revved up" Cisco router to help provide some security at the border router, without impacting that router's performance.

The first part of CBAC is creating extended access control lists for allowing inbound and outbound permitted traffic.

The inbound access list will be created first. Cisco's access lists are processed from the top down. Knowing that, rules must be placed in the correct order. More specific rules are placed first, and the more general rules second. This could allow services through, that should have been denied. Also, placing the more frequently used rules should go first in the list to minimize processing times.

It is a good idea to simply cut and paste the following into the router with remarks that serve as reminders of each rule's purpose.

```
Access-list 120 remark   FIRST WE BLOCK SPOOFED SOURCE ADDRESSES
Access-list 120 remark   FROM THE INTERNET
access-list 120 deny  ip    100.100.100.0 0..0.0.255 any log
Access-list 120 remark   BLOCK PRIVATE RFC 1918 ADDRESSES
access-list 120 deny   ip 10.0.0.0 0.255.255.255 any log
access-list 120 deny   ip 172.16.0.0 0.15.255.255 any log
access-list 120 deny   ip 192.168.0.0 0.0.255.255 any log
Access-list 120 remark Block invalid inbound source addresses
access-list 120 deny   ip host 255.255.255.255 any log
access-list 120 deny   ip 0.0.0.0 0.255.255.255 any log
access-list 120 deny   ip 127.0.0.0 0.255.255.255 any log
access-list 120 deny   ip 224.0.0.0 15.255.255.255 any log
access-list 120 deny   ip 240.0.0.0 7.255.255.255 any log
access-list 120 remark ALLOW INTERNET SERVICES IN
access-list 120 permit tcp any host 100.100.100.4 eq smtp log
access-list 120 permit tcp any host 100.100.100.5 eq smtp log
access-list 120 permit udp any host 100.100.100.2 eq domain log
access-list 120 permit udp any host 100.100.100.3 eq domain log
access-list 120 permit udp any host 100.100.100.6 eq isakmp log
access-list 120 permit udp any host 100.100.100.6 eq 4444 log
```

```
access-list 120 permit tcp any host 100.100.100.1 eq www log
access-list 120 remark   EXPLICIT DENY ALL
access-list 120 deny   ip any any log
```

This access list by itself will not allow the user traffic from returning to the inside network. This will be handled when CBAC is turned on, in a few steps.

Next, it is time to configure the outbound access list.

```
access-list 150 remark Outbound access List FOR ALL USERS
access-list 150 remark allow outbound www from nat block
access-list 150 permit tcp 100.100.100.0 0.0.0.255 any eq www log-input

access-list 150 remark Allow outbound email
access-list 150 permit tcp host 100.100.100.4 any eq smtp log-input
access-list 150 permit tcp host 100.100.100.5 any eq smtp log-input
access-list 150 remark Allow outbound SSL FOR ALL USERS
access-list 150 permit tcp 100.100.100.0 0.0.0.255 any eq 443 log-input

access-list 150 remark Allow outbound DNS
access-list 150 permit udp 100.100.100.0 0.0.0.255  any eq domain log-input

access-list 150 remark ALLOW OUTBOUND FTP FOR ALL USERS
access-list 150 permit tcp 100.100.100.0 0.0.0.255 any eq ftp log-input

access-list 150 remark Allow outbound NTP for ALL USERS
access-list 150 permit udp 100.100.100.0 0.0.0.255 any eq ntp log-input
access-list 150 permit udp border.router.int.s0/0address 0.0.0.0 any eq ntp log-
input

access-list 150 remark ALLOW OUTBOUND VPN CONNECTIONS for VPN
Only
access-list 150 permit udp host 100.100.100.6 any eq isakmp log-input
access-list 150 permit udp host 100.100.100.6 any eq 4444 log-input

access-list 150 remark EXPLICIT DENY ANY
access-list 150 deny any any log-input

access-list 150 remark BECAUSE OF HOW THIS LIST WAS WRITTEN
access-list 150 remark NO SPOOFED ADDRESSES WILL BE ALLOWED OUT
```

These access lists now need to be applied to the correct interfaces. It has been decided that both access lists will be applied to the WAN interface of the router. This is the first point of entry for traffic into the network. To apply these lists, the following should be typed from global configuration mode:

```
Int s0/0
Ip access-group 120 in
Ip access-group 150 out
```

Now, as mentioned before, these rules by themselves will not allow the user traffic to return data back into the network. This is where CBAC comes in. By applying inspect rules to the same interfaces and by using the extended access lists, traffic will dynamically allow the traffic processes through. With CBAC enabled, there are a few commands that are enabled by default that can affect the performance of the traffic and these commands can be reviewed at:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt3/sccbac.htm

Here are the commands for CBAC:

```
ip inspect audit-trail
```

This allows messages to be sent via syslog.

```
ip inspect name inspectrule cuseeme
ip inspect name inspectrule ftp
ip inspect name inspectrule h323
ip inspect name inspectrule http
ip inspect name inspectrule rcmd
ip inspect name inspectrule realaudio
ip inspect name inspectrule smtp
ip inspect name inspectrule sqlnet
ip inspect name inspectrule streamworks
ip inspect name inspectrule tftp
ip inspect name inspectrule vdolive
ip inspect name inspectrule tcp
ip inspect name inspectrule udp
```

All of the above monitored the application listed and the last two statements monitored the tcp and udp protocols. The router will keep a session table for each stream of traffic and create dynamic access lists to allow this traffic back into the network.

Of course, these rules still need to be applied to an interface. The inspection rules will be added to the WAN interface S0/0 since this is where the access lists are configured. To apply these rules, type the following from the global configuration mode:

```
int s0/0
ip inspect inspectrule in
ip inspect inspectrule out
```

Advance traffic filtering has now been added to the border router for improved security. Router performance should be monitored from now on to make sure that this traffic is not overwhelming the router.

Intrusion Detection System

Intrusion detection will be added to the router next. An Intrusion Detection System (IDS) monitors traffic flows and will alert an administrator if certain, abnormal traffic occurs. This is usually an indication of malicious activity on the network. The Cisco router has this feature as part of its Network Operating System.

For starters, again from global configuration mode, type:

```
ip audit notify log
```

This sets the IDS system to send notifications to the Syslog server that was set earlier.

```
ip audit smtp spam 100
```

This sets the maximum number of inbound recipients to 100 before the IDS marks the SMTP traffic as spam. The default is 250 and GIAC has made the decision to limit this to 100.

```
ip audit name auditrule info action alarm
ip audit name auditrule attack action alarm drop reset
```

These two commands create an audit rule called "auditrule" and will alarm on information gathering intrusions and drop and reset connections on attack intrusions.

If the router's processor is overwhelmed because it has to check all traffic in and out bound, the amount of traffic checked can be limited to just traffic not from the source IP address block of the users. This will limit IDS checking to inbound traffic only, but this will still be beneficial. To do this, type:

```
ip audit name auditrule info list 99 action alarm
ip audit name auditrule attack list 99 action alarm drop reset
```

Then, create a standard access list 99 as follows:

```
access-list 99 deny   100.100.100.0  0.0.0.255 log
```

With these commands set, the router will not provide IDS checking on packets

originating from your users. Only do this if the router was overwhelmed with the first set of commands.

As with CBAC, these rules now need to be applied to a router interface. Again, the WAN interface Serial 0/0 was chosen, since this is the interface the untrusted traffic first enters GIAC's network. From global configuration mode, type:

```
Int s0/0
ip audit auditrule in
ip audit auditrule out
```

The border router is now locked down with strong access control and some Intrusion Detection capability. Make sure to save the router configuration before moving on.

Primary Firewall

The PIX firewall is the primary defense against intrusions from outside attackers. GIAC has developed a complicated design that will make the network more secure. It is not being complicated that makes it secure, but the layers implemented. Being complicated increases the chance for a mis-configuration so it is important for GIAC to make sure that it is implemented correctly and that all changes are checked and double-checked.

The primary firewall is the Cisco PIX 525. The PIX has been configured with six 10/100 ethernet interfaces. Assuming the firewall is already loaded with version 6.01, configuration of the firewall can begin. First, label the interfaces:

Interfaces

```
nameif ethernet0 outside security0
nameif ethernet1 DMZ security10
nameif ethernet2 DMZRelay security20
nameif ethernet3 PartnerDMZ security40
nameif ethernet4 TrustedDMZ security80
nameif ethernet5 inside security100
```

Then, set up the IP addresses of the interfaces:

```
ip address outside 192.168.1.1 255.255.255.0
ip address DMZ 192.168.2.1 255.255.255.0
ip address DMZRelay 192.168.3.1 255.255.255.0
ip address PartnerDMZ 192.168.4.1 255.255.255.0
ip address TrustedDMZ 192.168.5.1 255.255.255.0
ip address inside 192.168.6.1 255.255.255.0
```

Nat

Now, turn on Network Address Translation:

Nat (inside) 1 0 0
Nat (TrustedDMZ) 1 0 0
Nat (DMZRelay) 1 0 0
Nat (DMZ) 1 0 0

Global (outside) 1 100.100.100.10–100.100.100.253 netmask 255.255.255.0
Global (outside) 1 100.100.100.254 netmask 255.255.255.0
Global (DMZ) 1 192.168.2.1-192.168.2.254 netmask 255.255.255.0
Global (DMZRelay) 1 192.168.3.1-192.168.3.254 netmask 255.255.255.0
Global (TrustedDMZ) 1 192.168.5.1-192.168.5.254 netmask 255.255.255.0

Routing

Then routing is configured:

Route outside 0.0.0.0 .0.0.0.0 192.168.1.254 1
Route inside 192.168.7.0 255.255.255.0 192.168.6.254 1
Route inside 192.168.8.0 255.255.255.0 192.168.6.254 1
Route inside 192.168.9.0 255.255.255.0 192.168.6.254 1
Route TrustedDMZ 192.168.10.0 255.255.255.0 192.168.5.254 1

General Security

Next, disable RIP:

no rip inside passive
no rip inside default
no rip outside passive
no rip outside default
no rip DMZ passive
no rip DMZ default
no rip DMZRelay passive
no rip DMZRelay default
no rip PartnerDMZ passive
no rip PartnerDMZ default
no rip TrustedDMZ passive
no rip TrustedDMZ default

Now, disable SNMP:

no snmp-server location

```
no snmp-server contact
snmp-server community hardtoguesspassword
no snmp-server enable traps
```

Telnet hosts for management will not be enabled since the PIX is to be managed via console connections.

Allow Traffic

Now, inbound connections need to be allowed:

From the Internet:

```
static (DMZRelay, outside) 100.100.100.4 192.168.3.5 netmask 255.255.255.255 500

static (DMZRelay, outside) 100.100.100.5 192.168.3.6 netmask 255.255.255.255 500

static (DMZ, outside) 100.100.100.2 192.168.2.6 netmask 255.255.255.255 500

static (DMZ, outside) 100.100.100.3 192.168.2.7 netmask 255.255.255.255 500

static (DMZRelay, outside) 100.100.100.6 192.168.3.7 netmask 255.255.255.255 500

static (DMZ, outside) 100.100.100.1 192.168.2.5 netmask 255.255.255.255 500
```

```
access-list outside_in permit tcp any host 100.100.100.4 eq smtp
access-list outside_in permit tcp any host 100.100.100.5 eq smtp
access-list outside_in permit udp any host 100.100.100.2 eq 53
access-list outside_in permit udp any host 100.100.100.3 eq 53
access-list outside_in permit udp any host 100.100.100.6 eq 500
access-list outside_in permit udp any host 100.100.100.6 eq 4444
access-list outside_in permit tcp any host 100.100.100.1 eq www

access-group outside_in in interface outside
```

From the DMZRelay:

```
static (inside, DMZRelay) 192.168.6.5 192.168.6.5 netmask 255.255.255.255
500

Access-list DMZRelay_in permit tcp host 192.168.3.5 host 192.168.6.5 eq smtp
Access-list DMZRelay_in permit tcp host 192.168.3.6 host 192.168.6.5 eq smtp

Access-group DMZRelay_in in interface DMZRelay
```

From the PartnerDMZ:

static (inside, PartnerDMZ) 192.168.8.5 192.168.8.5 netmask 255.255.255.255 500

Access-list PartnerDMZ_in permit tcp host 192.168.4.7 host 192.168.8.5 eq 1433
(Note: this allows queries from our transactional Database server on the SQL port to our internal database.)

access-group PartnerDMZ_in in interface PartnerDMZ

From the TrustedDMZ:

static (inside, TrustedDMZ) 192.168.6.0 192.168.6.0 netmask 255.255.255.0 500
static (inside, TrustedDMZ) 192.168.7.0 192.168.7.0 netmask 255.255.255.0 500
static (inside, TrustedDMZ) 192.168.8.0 192.168.8.0 netmask 255.255.255.0 500
static (inside, TrustedDMZ) 192.168.9.0 192.168.9.0 netmask 255.255.255.0 500

Access-list TrustedDMZ_in permit tcp 192.168.10.0 255.255.255.0 any
Access-list TrustedDMZ_in permit udp 192.168.10.0 255.255.255.0 any

Access-group TrustedDMZ_in in interface TrustedDMZ

From the Inside network:

Access-list Inside_in permit tcp any any eq www
Access-list Inside_in permit tcp any any eq smtp
Access-list Inside_in permit tcp any any eq 443
Access-list Inside_in permit udp any any eq 53
Access-list Inside_in permit tcp any any eq ftp
Access-list Inside_in permit udp any any eq ntp

Access-group Inside_in in interface Inside

This should be all of the access lists needed. The PIX denies all traffic except for what is explicitly allowed.

Additional features used in this configuration are:

Fixup protocol ftp
Fixup protocol http
Fixup protocol h323

```
Fixup protocol rsh
Fixup protocol smtp
Fixup protocol sqlnet
Fixup protocol sip
Fixup protocol domain
```

The fixup statements make the PIX look at the application traffic and verify its purpose.

Then provide another layer of egress filtering:

```
Ip verify reverse-path interface outside
```

To configure WWW requests to be authenticated by our Websense server, type:

```
url-server (inside) host 192.168.6.7
filter url http 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

IDS will be activated with the following commands:

```
Ip audit info action alarm
Ip audit attack action alarm drop
```

This concludes the configuration of the primary firewall.

As part of the installation process, each interfaces' configuration should be tested to verify everything works as designed. If necessary, a packet sniffer can be used to verify that traffic is flowing in only the directions planned.

VPN

The VPN device for this network is a Cisco 3015 VPN concentrator. It allows for multiple groups, and allows each group to have limited access.

First, configure the VPN Concentrator with IP addresses for the network:

Public	192.168.3.7
DMZ	192.168.4.254
Private	192.168.5.254

Split tunneling will not be used. The software and information needed to access the network will be delivered to the clients. They will be advised that while connected to GIAC's systems, all of their other communications will be cut off and routed through GIAC's system. Agreeing to this will be part of the authorization form the clients will need to sign before being given access.

Now it is time to connect to the concentrator with our web browser.

The first thing to do is lock down the Concentrator by disabling features that are not needed:

Management

Go to Configuration>System>Management Protocols and click on each protocol and disable them all except HTTPS and SSL. This will mean the Concentrator can only be managed by using a https/SSL connection.

Server Configurations

It is not important to go into great detail on the servers that should be set up, but they are listed here:

Authentication Servers will be the NT Domain controller. When users are disabled from the NT domain, their VPN access is then terminated. GIAC's extranet users will be configured as "Internal Users" on the VPN concentrator. This will be set up shortly.

DNS servers should be set to the internal DNS server at 192.168.6.8.

NTP Host will be the Internal router at 192.168.6.254.

SMTP and Syslog servers should be setup to allow event notifications.

Static routes should be set and OSPF disabled for the concentrator.

Address Assignment

Next the address pools are set up for the remote users.

They will be:

Remote Access	192.168.10.1-254
Author's	192.168.11.1-254
Partner's	192.168.12.1-254

Go to Configuration>System>Address Management>Assignment and place a check in "Use Address Pools."

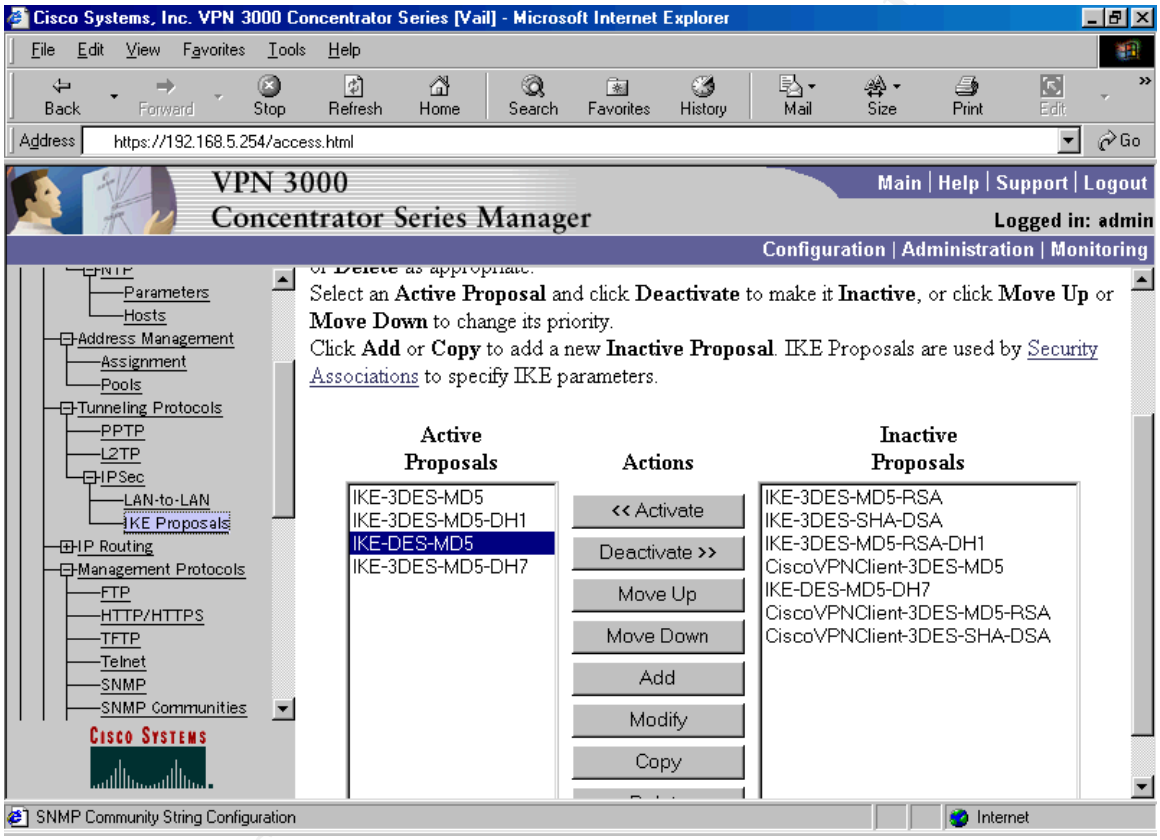
Then go to Configuration>System>Address Management>Pools and add the three pools from 1-254 for the 3 groups that will be attaching to the network.

Tunneling Protocols

Define the tunneling protocols that will be allowed on the network.

Go to Configuration>System>Tunneling Protocols>PPTP and L2TP and disable them. GIAC will only be using IPSec on the network. All authors, partners and remote access users will be given a copy of the Cisco VPN client.

Under IPSec, go to IKE Proposals. This is where to set up what IKE proposals will be used on our network.



With the IKE proposals set, the polices can then be created. This includes security associations.

The only security associations that will be used are the "canned" ones that come already set up on the concentrator. Go to Configuration>Policy Management>Traffic Management>SAs :
(Leave the following and remove any others.)

ESP-3DES-MD5
ESP/IKE=3DES-MD5
ESP-3DES-MD5-DH7

Before adding users and groups, the filter rule for the partner and author users need to be created.

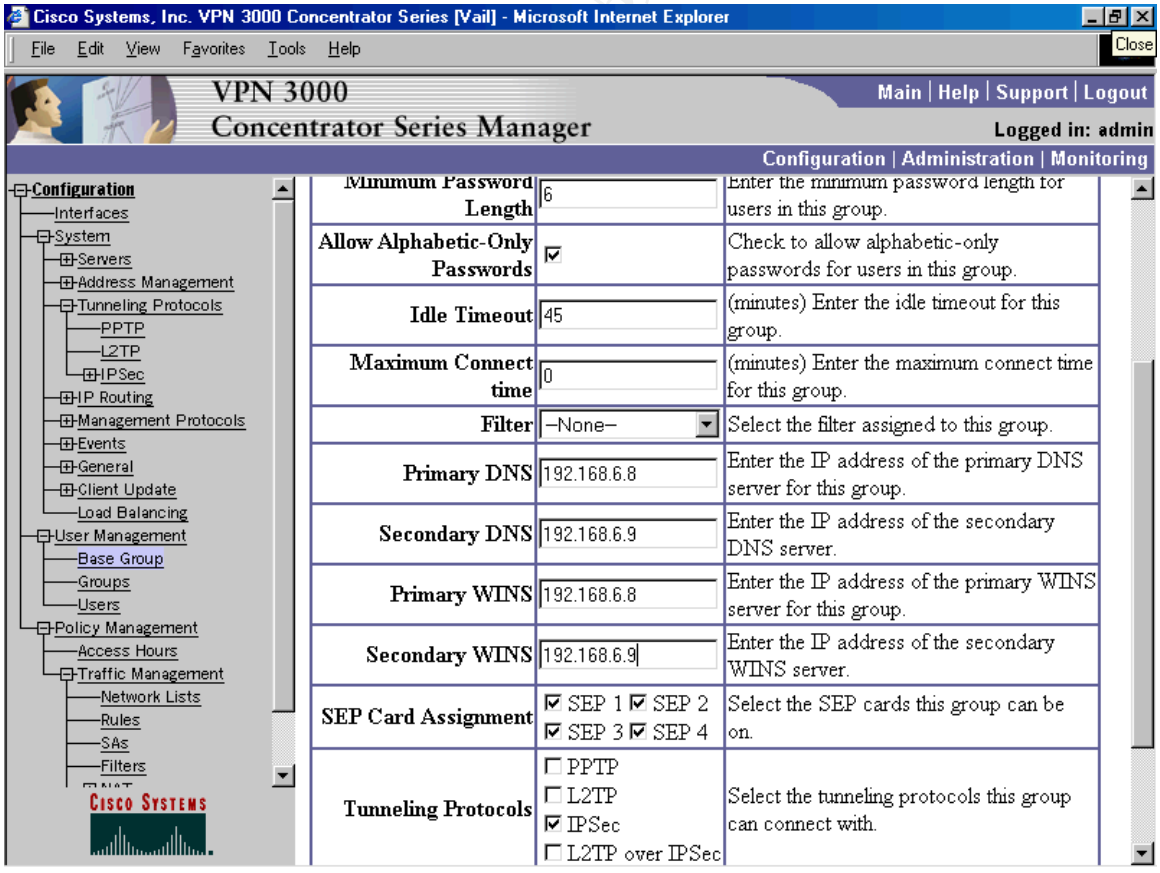
Go to Configuration>Policy Management> Traffic Management>Filters>Add Filter

The settings are:
Call it ALLOWHTTPS
Default Action: Drop and Log
Uncheck Source Routing and Fragments.

Highlight the new filter and click >Assign Rules to Filter.
Add the four rules allowing HTTPS in and out. This will be the only traffic allowed.

Creating Groups

With the Security Associations and filter rules set up, now define a base group for all of the VPN users. Go to Configuration>User Management>Base Group and configure the general tab as follows:



Set the IPSec tab as:

IPSec SA: ESP-3DES-MD5
IKE Keepalives should be checked
Tunnel Type: Remote Access
Group Lock checked.
Authentication: None (This will vary between groups.)
Mode Configuration checked.
Banner:

You are connected to GIAC's Private Network.
Unauthorized use is prohibited.
All use is monitored.

Allow Password Storage on Client Unchecked.
Split Tunneling: None
Domain Name: giac.com
IPSec Through NAT checked.
IPSec UDP port: 4444 (coincides with our firewall rules).
By changing the default port, it is just a little harder for a hacker to guess what GIAC has listening on that port if they do scan the network.

Ignore the PPTP/L2TP tab since those protocols are disabled in the General Tab.

Now that a Base Group has been assigned, this template is used to assign parameters to the other VPN groups: Remote Access, Author, and Partner

A group called TrustedG1AC is created (The name helps protect security.)
A difficult password is assigned. Users only need this when they first setup VPN access.
The type of group is Internal.
These users will authenticate off of the domain directly.
Under the IPSec tab, change Authentication to NT Domain.
Save this group and assign it address pool 192.168.10.1-254.

Then add a group called AuthorAcc355 (author access).
Assign another difficult password.
The group type is Internal.
Under the IPSec tab, change Authentication to Internal.
Save this group and assign it address pool 192.168.11.1-254.
Under the General Tab, change the filter from "None" to "ALLOWHTTPS."

Next, add a group called Partn3rVPN (partner vpn).
Assign another difficult password.
The group type is Internal.
Under the IPSec tab change Authentication to Internal.
Save this group and assign it address pool 192.168.12.1-254.
Under the General Tab, change the filter from "None" to "ALLOWHTTPS."

Now configure a client machine to connect to the VPN and test each group. For the Author and Partner groups, you need to set up an Internal user assigned to the correct group. Test their access.

Internal Router

Basic Configuration

The Internal Router does not need to be as secure as the Border Router, but if given the opportunity, it should be mad as secure as possible. On that note, instead of going into each command one at a time, as was done for the border router, I will first summarize the commands that will carry over from the border router discussion. Then I will list the different commands needed to make the internal router serve its purpose.

Start configuring the IP addresses on each interface first. This router has one WAN interface and 3 Fast Ethernet interfaces. Assign each interface the address listed in the beginning of the document.

Int FastEthernet 0/0 192.168.6.254 for the Inside LAN
Int FastEthernet 0/1 192.168.7.254 for the Admin LAN
Int FastEthernet 1/0 192.168.8.254 for the Internal Database LAN

Then, configure the router to do EIGRP routing with the router at the remote location:

```
Router eigrp1
Network 192.168.6.0
Network 192.168.7.0
Network 192.168.8.0
```

Configure a default route to the firewall for all Internet traffic:

```
Ip route 0.0.0.0 0.0.0.0 192.168.6.1
```

General Security

Now, start securing the router by copying some of the commands that were used on the border router:

```
service tcp-keepalives-in
no ip http server
No snmp-server
no service udp-small-servers
no service tcp-small-servers
```

```
no service finger
no ip bootp server
no ip source-route
no cdp run
no ip unreachables
scheduler interval 500
banner motd ^C
Authorized GIAC Enterprises Employees Only!

Unauthorized Access Prohibited by Law and WILL BE Prosecuted!

Use is subject to monitoring!
^C
```

Under each network interface configuration, the following commands should be issued:

```
no ip redirects
no ip directed-broadcast
```

Back at the global configuration prompt:

```
Service password-encryption
Enable secret xxxxx
Line con 0
Login
Password xxxxxx
Line aux 0
Login
No password
Transport input none
Transport output none
Line vty 0 4
Login
password xxxxxx
exit
ntp server 18.26.4.105 version 2 prefer
ntp server 18.72.0.3 version 2

clock timezone mst -7
clock summer-time MDT recurring
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
logging trap debugging
logging buffered debugging
no logging console
logging facility local6
```

```
logging 192.168.6.4
```

CBAC and Access Control Lists

Now set up the internal router for its firewall role:

Access list 120 and 125 will be used to protect the internal database from the internal users. Only SQL queries will be allowed to this LAN and the server will be able to initiate any outbound communications that it may need. As increased access needs are identified from the rest of the network (i.e. an administrator needing more than just query access to the database), they will be added to list 120.

```
access-list 120 remark ALLOW MS SQL queries
access-list 120 permit tcp any host 192.168.8.5 eq 1433 log
access-list 120 remark   EXPLICIT DENY ALL
access-list 120 deny   ip any any log

access-list 125 remark EXTENDED ACL FOR CBAC
access-list 125 permit ip any any log
```

This will be applied to interface FastEthernet 1/0 as follows:

```
Int f1/0
Ip access-group 120 out
Ip access-group 125 in
```

The Admin LAN needs to be secured next. GIAC does not want any inbound connections from the network into the Admin LAN, but they want the admin users to be free to do what they need to from the Admin LAN. Access lists are set up as follows:

```
access-list 150 remark BLOCK EVERYTHING
access-list 150 remark   CBAC WILL ALLOW THE REST
access-list 150 deny   ip any any log

access-list 155 remark EXTENDED ACL FOR CBAC
access-list 155 permit ip any any
```

This will be applied to interface FastEthernet 0/1 as follows:

```
Int f0/1
Ip access-group 150 in
Ip access-group 155 out
```

Now setup CBAC to monitor this traffic and add access list entries to allow return traffic as needed. To setup CBAC, type:

```
ip inspect audit-trail
ip inspect name inspectrule cuseeme
ip inspect name inspectrule ftp
ip inspect name inspectrule h323
ip inspect name inspectrule http
ip inspect name inspectrule rcmd
ip inspect name inspectrule realaudio
ip inspect name inspectrule smtp
ip inspect name inspectrule sqlnet
ip inspect name inspectrule streamworks
ip inspect name inspectrule tftp
ip inspect name inspectrule vdolive
ip inspect name inspectrule tcp
ip inspect name inspectrule udp
```

These rules still need to be applied to an interface. The inspection rules will be added to the Internal Database LAN and to the Admin LAN interfaces as follows:

```
int f0/1
ip inspect inspectrule in
ip inspect inspectrule out

int f1/0
ip inspect inspectrule in
ip inspect inspectrule out
```

Intrusion Detection System

Now, intrusion detection is added to the router.

```
ip audit notify log
ip audit smtp spam 100
ip audit name auditrule info action alarm
ip audit name auditrule attack action alarm drop reset
```

As with CBAC, apply these rules to the router interfaces:

```
Int f0/1
ip audit auditrule in
ip audit auditrule out

Int f1/0
ip audit auditrule in
ip audit auditrule out
```

This only sets up Context Based Access Controls and Intrusion Detection on the Admin LAN interfaces and on the Internal Database interfaces, leaving the Inside LAN and the WAN susceptible to unmonitored hacking. If after the router has been online for a week or so, GIAC decides that the router has spare processor and memory to be able to add CBAC and IDS to the other interfaces, it would be a good idea. You don't want to overwhelm the router at first, but if the extra capacity is available, you should use it.

Audit

GIAC Enterprises has requested that a security audit of its primary firewall be conducted. They want to verify that the firewall is implementing the security policy as designed. They also want to make sure that there are no documented vulnerabilities still part of their network and that no unneeded services are being permitted through their firewall.

Scope

The scope of this audit, per the practical instructions, is to test the primary firewall only. For this reason, all testing will be done onsite from each of the firewall's interfaces. Vulnerabilities in applications will be noted and will be reported to GIAC.

System logging and the IDS systems will be tested during this audit. They should catch and report the attempts made by this audit. Logs will be analyzed and we will need to verify that the systems behaved as designed.

Tools

The tools for this audit will be Network Associates Cyber Cop Scanner. It has recently been rated as a "Best Buy" by Info Security News Magazine July 2001, www.scmagazine.com. It provides a good tool for vulnerability assessment and for IDS system testing.

The other tool that will be used in this audit is Network Associates' Sniffer Pro packet sniffer. This application can capture all of the traffic on a network and will enable us to verify that traffic is not being passed by the firewall.

Both applications will be loaded onto two laptops. One laptop running Cyber Cop will be on the network we are testing from and the second laptop will be watching traffic with the packet sniffer to see what traffic gets through the firewall.

Time

The time line for this audit is immediately, because this is a new installation and any delay in identifying holes will lead to possible intrusion. Future audits should be conducted randomly at least once a quarter and after any system changes or upgrades. This will help insure the system is working as designed.

The future audits will not be limited to a time of day. Peak periods of the day should be audited to make sure that syslog and IDS systems can keep up with the traffic flow and identify intrusions. For this reason, one peak time period audit should be conducted a year. The other three random audits per year should be conducted at truly random times of the day or night.

Costs

Costs for this audit are not known. It would be easy to say that each audit would require 40-50 man-hours at $100 or more per hour. Each audit may or may not require more time depending on the outcome of the audit. If certain anomalies exist, more time should be spent analyzing and testing.

In GIAC's case, I would charge them for a block of hours. Since the initial audit is all that is being asked for at this time, I would contract for a minimum of 40 hours and then have an hourly fee if more time is needed. I would allow the customer to authorize all hours over 40, if they are needed.

Conducting the Audit

The audit will be conducted from one interface to all of the other networks/interfaces on the network. This will include the one that the auditing system is attached to. This will insure that if one system is compromised that the other systems on that network will not be easily compromised as well.

Cyber Cop Scanner

Cyber Cop Scanner (CCS) is a user friendly software managed by a GUI for Windows systems. It has the ability to test vulnerabilities that have been added to its database against ranges of IP addresses.

For this audit, we will be using two laptops, one testing and the other capturing the traffic.

We will start by setting up Cyber Cop to work correctly for this test. Start by running the application and going to the menu choice: Configure and choose scan settings. Under the scan settings tab we will set the host range to the network we are testing. For all tests, this will involve the following ranges of IP's:

192.168.1.1-254
192.168.2.1-254
192.168.3.1-254
192.168.4.1-254
192.168.5.1-254
192.168.6.1-254
192.168.7.1-254
192.168.8.1-254
192.168.9.1-254
100.100.100.1-254

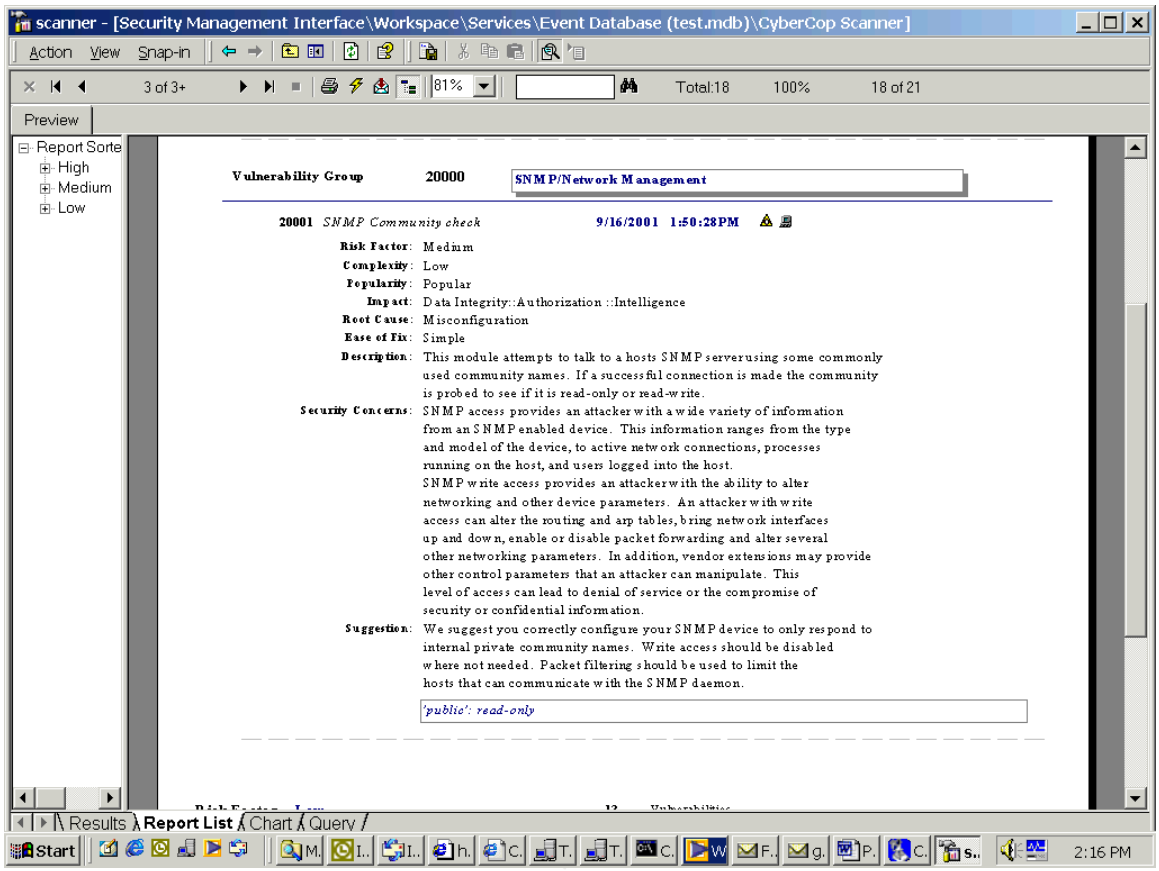
Other settings we need to set under "Scan Settings" are to make sure that under "Scan Options" that the "Allow modules to be disabled based on OS" is not checked.

Under the tab "Engine Options," make sure that the options "Scan Unresponsive Hosts" and "Scan Unroutable Hosts" are both checked. This will make sure that all tests are run on all IP addresses.

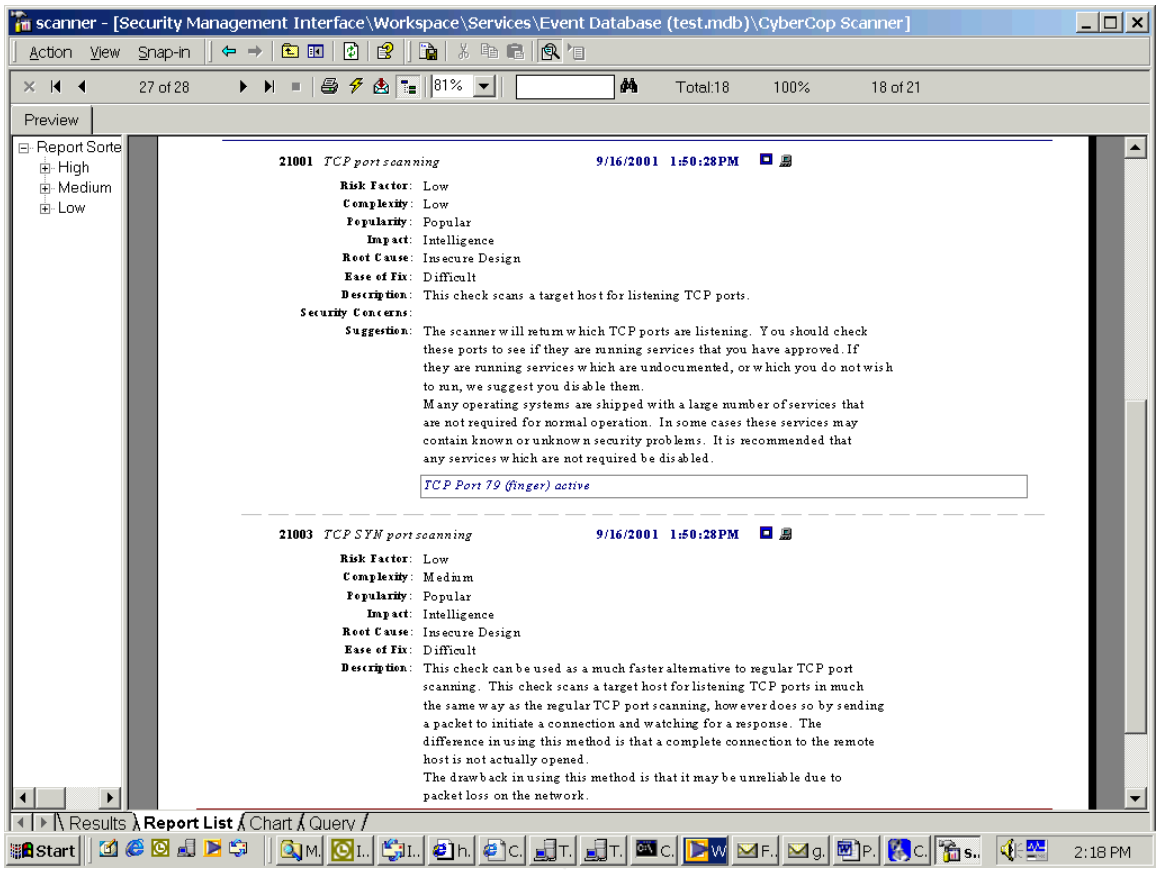
Now we Apply those changes and go to the >Configure>Module Settings. Here we select all tests by choosing the "select all" button. This will run all the tests in the CCS database. Note that some of these tests can crash systems. For the purpose of this audit, all tests will be run. These are the same vulnerabilities that hackers will scan for and it makes sense for you to test for these before they do.

We will first be testing from the Outside network. So we set up the CCS to scan each of the above-mentioned networks, one at a time. We have to give the laptop an IP address from this network. We give each scan an "Output Database" name describing the test (i.e. OutsidetoDMZ). We place the sniffer on each network as we scan to that network. We then review the CCS results, sniffer capture, and IDS and syslog alarms to verify the architecture.

A sample results page looks like:



This first one shows that the SNMP community string was read and lists it as "public." If you see a result like this, you should question why SNMP is turned on and disable it if possible. If SNMP is needed, change the community string to a non-default value that is hard to guess.



This second test shows that the TCP port scanning has revealed that TCP port 79 (finger) is listening. In the GIAC audit, you should only see ports open that the firewall has let through (i.e. SMTP, WWW and DNS where appropriate.) For each host in the CCS results, make sure only the expected ports are open. Investigate anything you cannot explain.

This CCS test will be repeated for each network block, from each of the six interfaces on the PIX (sixty times multiplied by the amount of host results you will need to sift through). The CCS report will tell you what applications are available and what holes and vulnerabilities you have in your network.

From the outside network, you should have only WWW traffic to your public WWW server, DNS UDP traffic to your DNS servers, SMTP traffic to your mail relay servers and VPN related traffic to your VPN box passing through the firewall.

From the DMZ network, you should have no traffic allowed to the DMZRelay, PartnerDMZ, TrustedDMZ or Inside networks. If CCS finds any server vulnerabilities on this network, make a note of them and provide this to GIAC so they can correct these issues.

From the DMZRelay network, you should have no traffic passed through the firewall to

the PartnerDMZ, TrustedDMZ, or Inside networks. This is because the scanner is not configured with the IP address of the mail servers so it should not be allowed to pass traffic to the internal mail servers. It makes sense to test this. First remove the mail relay servers from the network, change the IP address of your CCS laptop to the same IP as the mail relay servers and scan again. This time you should see SMTP traffic allowed. Check to see if there are any SMTP related vulnerabilities on your internal mail servers. If for some reason a hacker has compromised your mail relay servers, this vulnerability, if any, will be important to correct now.

From the PartnerDMZ network, CCS should only report that the transactional database server IP is the only one allowed to do SQL queries into the network.

From the TrustedDMZ, all traffic to lower security level interfaces should be allowed. All traffic to the Inside network should also be allowed.

From the Inside network, test access to the InternalDBase LAN and the Admin LAN. Make sure that the access lists you have set up are working as designed.

Now we should also now setup a VPN user group test. Set up an Internet host to use each of the following VPN groups:

TrustedG1AC
AuthorAcc355
Partn3rVPN

Use CCS and test to make sure that the access granted for each group is what was designed. Only the TrustedG1AC group should be able to access the internal LAN.

One last test is to try and penetrate the network from the Internet to the 100.100.100.0 network.

Audit Evaluation

Once all of these tests are complete, review the data. Spend time retesting all open ports. Record all system vulnerabilities that have not been corrected to this point.

This data should be compiled and reported to GIAC as your audit results. If any major vulnerabilities exist, regroup and correct them. Bring in additional personnel if necessary.

It may be helpful to classify each vulnerability by its impact (i.e. High, Medium or Low). This will help prioritize which problem should be addressed first.

Design Under Fire

The last task for this practical is to evaluate the design of another GCFW consultant. I will be using the practical by Kevin Oltree at http://www.sans.org/y2k/practical/Kevin_Olree_GCFW.doc. It was chosen because it has the same systems used in my design and I thought it would be a good exercise to learn more about my own vulnerabilities.

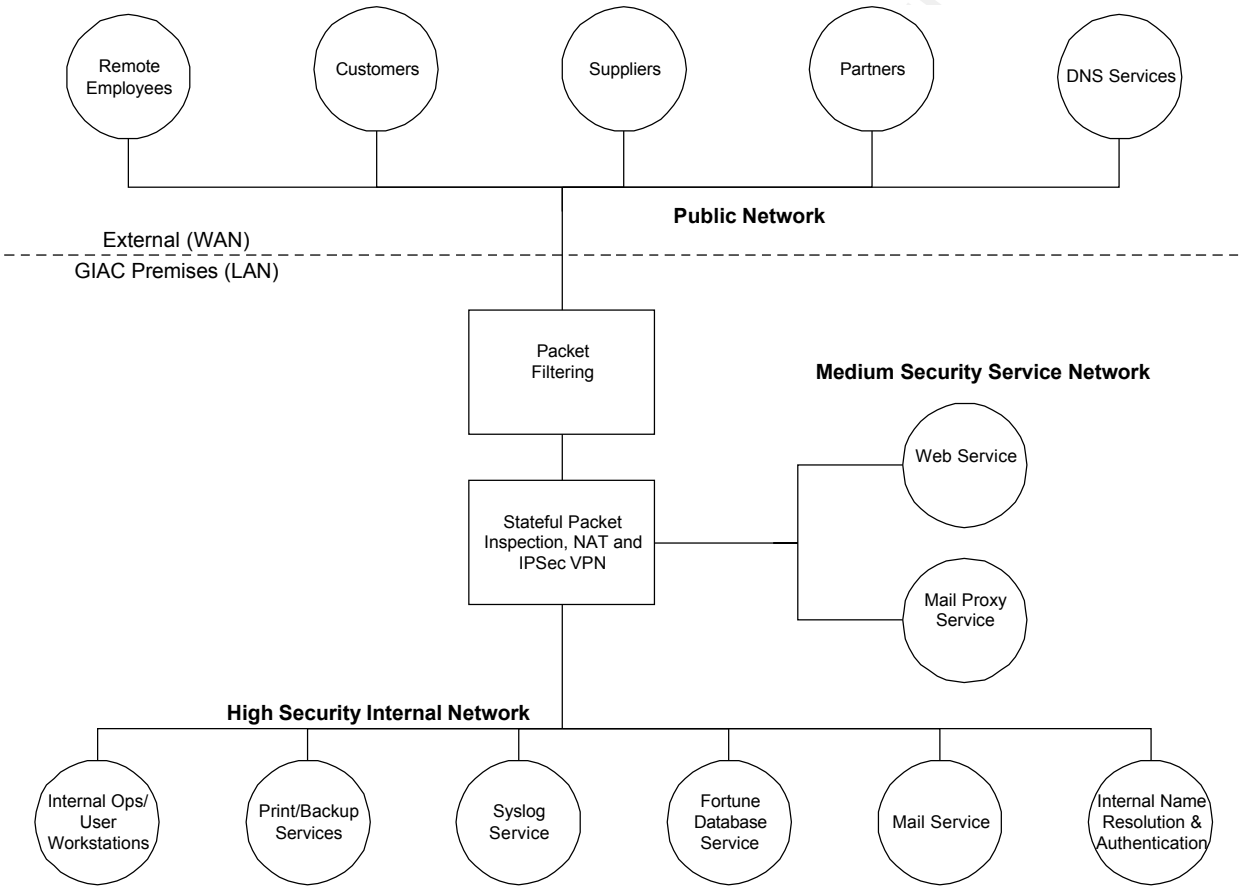


Figure 1.1: Logical Network Design

Overview

The assignment is to mount three different types of attacks against this network design. The attack types are: a direct attack to the firewall, a denial of service attack comprised of 50 cable access systems and an attack compromising an internal system through the perimeter defenses.

Firewall Attack

The Cisco PIX 515 running version 5.3 is a secure system. There are no publicly known attacks that directly affect the firewall in use in his network. This is probably because Cisco uses its own stripped down and hardened operating system on a hardware appliance.

The only possible vulnerability angle I can think of, that does not involve traffic through the PIX, is unauthorized access from the inside network. This is an attack directed to the firewall, but instead of coming from the outside, it occurs from the inside of the network.

First, since there was no telnet configurations listed in the PIX configuration section of Kevin's practical (but he does elude to telnet access to the PIX earlier in the paper), we would simply capture the telnet passwords from the inside of the network. We could use a network sniffer (no switching was indicated) or install a keystroke recorder on the administrator's systems that we assume they access the firewall from.

This would give the attacker full access to the firewall and the ability to make changes. It may require some patience but would be 100% effective. This is more of an attack on the design of the network than an attack toward the firewall solution.

The best way to protect from this is to limit firewall access to the console port only. This will ensure that no network traffic can be intercepted to reveal the PIX access passwords. By using a standalone (no network) system, we can insure that our passwords are secure.

DOS Attack

The other type of attack is a coordinated Denial of Service (DOS) attack from fifty compromised broadband users. This type of attack can degrade the performance of his network.

The first type of attack is the TCP syn attack. Per his configurations, Kevin has taken a good step by limiting the amount of embryonic connections in a half open state for all of his systems. This means that the TCP syn attack would not be successful to take down a service behind his firewall.

The other type of attack is a UDP flood. This type of attack on his network should not work since the only UDP connection he is allowing inbound through his firewall is Syslog from his border router. The border router's IP address is the only address allowed in on that connection. Since he is denying spoofed addresses from the Internet for that address, he has limited a UDP flood attack source to his "outside" network. This is the network between the router and the firewall. To be effective, an attacker needs to be connected to the LAN between his border router and firewall and then send spoofed UDP packets to

the syslog server. Since his network does not have hosts on that network, an attacker would need a physical presence to conduct this attack.

The third type of attack is an ICMP flood. In this scenario, and possibly the scenario where TCP or UDP packets are sent, it is possible for the packets to overwhelm his T1 and the router and/or firewall resources. The firewall will drop ICMP packets (and TCP and UDP packets for invalid services), but the sheer volume of traffic that can be generated by 50 broadband systems can cause a denial of service.

Tools like Trinoo and Tribal Flood network (TFN) can be used to orchestrate this type of attack. With a single command, the zombie machines, in this case the 50 broadband systems, they can generate more traffic than the single T1 can handle. This would take down GIAC's Internet access for employees and customers by not having enough bandwidth available for when legitimate users try to get through the T1.

Information on Trinoo and TFN can be found at:

http://staff.washington.edu/dittrich/misc/trinoo.analysis

and

http://staff.washington.edu/dittrich/misc/tfn.analysis

David Dittrich has authored both sites.

There are two ways for preventing this type of attack. Both involve the assistance of your ISP. The first is only effective after you are under attack. By using a network sniffer or by looking through your logs, you need to identify the source IP addresses. You then must have the ISP drop the traffic from the hosts attacking you by using an access list. By not allowing packets from those source IPs onto the T1, you effectively have freed up your bandwidth until other source IPs start to attack you.

Another proactive way of combating this type of attack is to use Cisco's Committed Access Rate feature. This feature allows you to limit the amount of bandwidth different types of traffic can use on the interface the feature is applied to. Again, this needs to be done on the ISP's router. Here is a Cisco web page describing the configuration of CAR. http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/qos_c/qcpart1/qccar.htm

Using either method to limit traffic on your side of the T1 is too late. By the time the traffic has reached your router, it has already overwhelmed your T1. It is important to have a good relationship with your ISP and make sure that they can provide this service for your network.

Attack on an Internal System

The final attack is one against an internal system. For my attack I chose to attack Kevin's mail server. The reason I have chosen his mail server over his web server is because if I can find a vulnerability in his mail server, I may be able to use the same vulnerability to then attack his internal network. The other reason I chose his mail relay servers is because Kevin did not state what platform he would be using for his web server.

Unfortunately, I found only one vulnerability for the Baltimore Technologies MailSweeper, which Kevin is using on this network. The vulnerability was found on SecurityFocus at the following URL: http://www.securityfocus.com/bid/3027 and is called "Multiple Vendor File Scanner Malicious Archive DoS Vulnerability." This vulnerability allows any malicious person to take a highly compressed ZIP file with other imbedded zip files to crash the server. This happens because once the MailSweeper application finishes unzipping the files to check the contents for viruses, it has become so large that the server runs out of swap space and crashes.

There is a method that can prevent this exploit. It involves creating two partitions on the server. By doing this, the exploit will not crash the system drive and can continue to function.

Other possible vulnerabilities in all of his systems could be found by using a tool like Cyber Cop scanner or NMap. Without having prior knowledge of a network design and the applications that are running, you would need to utilize those tools to help identify the vulnerabilities and systems that exist.

References

Cisco Web Site "Cisco 3600 Series." September 2001. URL: http://www.cisco.com/univercd/cc/td/doc/pcat/3600.htm (Sept 2001).

Cisco Web Site "Configuration Guides and Command References." September 2001 URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/index.htm (Sept 2001).

Cisco Web Site "PIX Firewall Version 6.0." September 2001 URL: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_60/index.htm (Sept 2001).

Cisco Web Site "VPN 3000 Concentrator User Guides." September 2001 URL: http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/vpn3kco/vcoug/index.htm (Sept 2001).

Security Focus "Security Focus Web Page." September 2001 URL: http://www.securityfocus.com/bid/3027 (Sept 2001).