Global Information Assurance Certification Paper

GIAC Enterprises Firewall Overview and Audit

GCFW Practical Version 1.8

Sean Heare
February 18, 2003

Assignment 1 - Security Architecture

1.0 Abstract

Founded in 2000, GIAC Enterprises, a Washington DC based e-business that sells fortune cookie sayings has grown quickly and now has 25 employees and annual revenue of $7.4 million dollars. GIAC's Board of Directors investigated what would be required to continue this growth and determined that due to the companies extreme reliance on it's network, revisiting Network Security was a paramount concern.

GIAC commissioned SPH Network Security to observe the day-to-day business operations of the company. Based upon those observations, SPH Network Security has defined a network security architecture.

The network security architecture includes descriptions of work flow and required access, descriptions of key and some secondary security elements of the architecture, IKE policy, IPSec policy a tutorial on the setup of the VPN Concentrator.

A technical audit will be conducted with internal staff and SPH network consultants ensuring that the policies implemented above are being enforced.

1.1 Best Practices and Guidelines

- The budget for the purchase of perimeter defense equipment is limited to $25,000. The old architecture will be entirely scrapped except for a Cisco 3640.

- Since Information Technology resources are stretched both in knowledge and manpower at GIAC, the network and its security components must be simple and easy to maintain. Furthermore while there is a budget constraint, they would rather use the entire budget on a reliable security solution than come in under budget but have unexpected security consequences.

- The network will have several layers of protection surrounding hosts to protect them from Internet based threats following a defense-in-depth strategy. Many of these layers of protection are from VISA's e-business partner requirements. These layers of protection include but are not limited to: Installing and maintaining a working network firewall to protect confidential and proprietary data accessible via the Internet. Keeping security patches up-to-date. Encrypting stored data accessible from the Internet. Encrypting data sent across networks. Using and regularly updating anti-virus software. Restricting access to data by business "need to know." Assigning unique IDs to each person with computer access to data. Tracking access to data by unique ID. Not using vendor-supplied defaults for system passwords and other security parameters and regularly testing security systems and processes.[1]

- Essential functions such as customer information databases and network management will be further protected from threats by having internal firewalls in place to restrict unauthorized access.

- GIAC's connection to the Internet is currently via one ISP. They would like to increase redundancy at some point in the future by adding a second ISP as a possible connection to the Internet; hence this should be taken into account in the design of the network.

- FTP access into giac.com is forbidden.

1. The SANS Institute. Network Design and Troubleshooting, SANS Firewall Track 2.5.2. Bethesda, MD: SANS Press, p. 74 (2001).

- Dial-up services into or out of GIAC's internal networks are not allowed. GIAC employees outside of the internal network should access the internal network solely via VPN.

- GIAC's ISP has assigned giac.com the IP Address range XXX.234.209.160/27. All public IP addresses in this document are also sanitized.

1.2 Business Operations

After investigating the company's business operations, the following communication relationships and needs have been defined:

1.2.1 Customers

GIAC has two customers. They are Lumbago Incorporated, a fortune cookie manufacturer and Dumb Luck Restaurants a Chinese food franchise in the Midwest.

The customers place orders through their SSL encrypted web browsers to the GIAC website. Customers receive fortune packages solely through HTTPS download (TCP 443). Fortune Packages are stored in a PostgreSQL database on the internal network segment dedicated to non-office traffic. PostgreSQL was chosen for its combination of price, reliability, asset transaction and stored procedure support.

The customer website (customer.giac.com) allows customers to update contact and billing information. Customers can change passwords on their accounts. New customers can create accounts on the website but cannot place orders until they authenticate their accounts by responding to an e-mail sent from the site administrator.

In order for customers to access the customer website TCP ports 80 and 443 will need to be accessible from the Internet to customer.giac.com. Customer billing and contact information is stored in a PostgreSQL Database. This database is also located on another hardened host on the network segment dedicated to databases.

1.2.2 Suppliers

A variety of writers working as independent contractors off-premises supply GIAC with fortune cookie sayings. The writers are paid on a per file basis and submit their fortunes by the hundreds to the editors at GIAC by PGP encrypted e-mail. The editor edits these fortunes for grammar, syntax and content.

The editor then packages the fortunes by subject into zip files. The editor copies the files into a directory on partner.giac.com so that partners can automatically

access the file at any time. Finally, the zipped fortunes are then inserted into GIAC's fortune database using pgadmin II utilizing SSH over port 5432 TCP.[2]

1.2.3 Partners

Malfortuna SA and Sorte má SA partnered with GIAC to capture overseas markets. Malfortuna SA translates the fortunes received into Spanish and resells the fortunes throughout Latin America except Brazil. Sorte má SA does the same for Brazil.

Partners access fortunes directly from partner.giac.com. The web portal allows them access to the fortune database (a PostgreSQL database) directly. Ports TCP 443, TCP 80 and TCP 5432 will need to be opened to the partner web portal. Access to the partner portal is by setting Apache's mod_access module to only accept traffic from IP addresses the partners have defined. Each partner has their own portal in a pre-agreed upon sub-directory.

1.2.4 Teleworkers

GIAC's sales force and teleworkers remotely access information resources in the home office over the VPN. SecurID and unique user accounts for each user grant token+password authentication for VPN access. VPN access will require IPSec with Encapsulating Security Payload (ESP) (IP 50) mode and Internet Key Exchange (IKE) (UDP 500) to be allowed to come in from the Internet to the External Network so that the VPN concentrator can be accessed. Since GIAC remote users already by definition have some means of using the Internet when connecting to the GIAC VPN, they will not be allowed to split tunnel while accessing GIAC.

GIAC employees need to perform queries, add and edit records on the databases (TCP 5432). They need to update and test the web sites using SSH and they will need to view the results of those edits (TCP 22, 80, 443). They will also need to check e-mail (TCP 25, 110).

The remote users utilize company assigned laptops running Windows XP Professional with the latest vulnerability patches installed. All company Windows workstations have Norton Anti-Virus 2003 running with the latest virus updates. Teleworkers are expected to use their own Internet connections to use Liveupdate to keep the virus scanners up to date.

Laptops, due to the increased threat they receive, have ZoneAlarm Pro 3.5 installed. An upgrade to Zone Labs Integrity is being considered.

Since laptops are often the most vulnerable information asset in the company all employees have been familiarized with laptop safe practices guidelines.

---

2. Yankowski, Fred. "How do I...use pgAdmin II via a secure (encrypted) connection?" 20 December 2001. URL:http://pgadmin.postgresql.org/pgadmin2.php?ContentID=11. (17 February 2003).

Employees are provided with a cable locking system to secure their laptops, and training on how to use the cable lock system.[3] Employees assigned with laptops are further advised to lock laptops in a drawer at night if they are to be left in the GIAC office overnight. Each teleworker has signed a security policy agreeing to secure the laptop and keep its patches and virus database up to date.

1.2.5 On-site Employees

GIAC employees at the office use Windows XP Professional desktop workstations. GIAC employees need to perform queries, add and edit records on the databases using pgadmin II (TCP 5432). They also need to update and test the web sites using SSH (TCP 22, 80, 443). They will also need to check e-mail (TCP 25, 110). Since they are using PCs inside of the network they each run Norton Anti-Virus 2003 running with the latest virus updates (downloaded using LiveUpdate via port 80).

1.2.6 Support Services

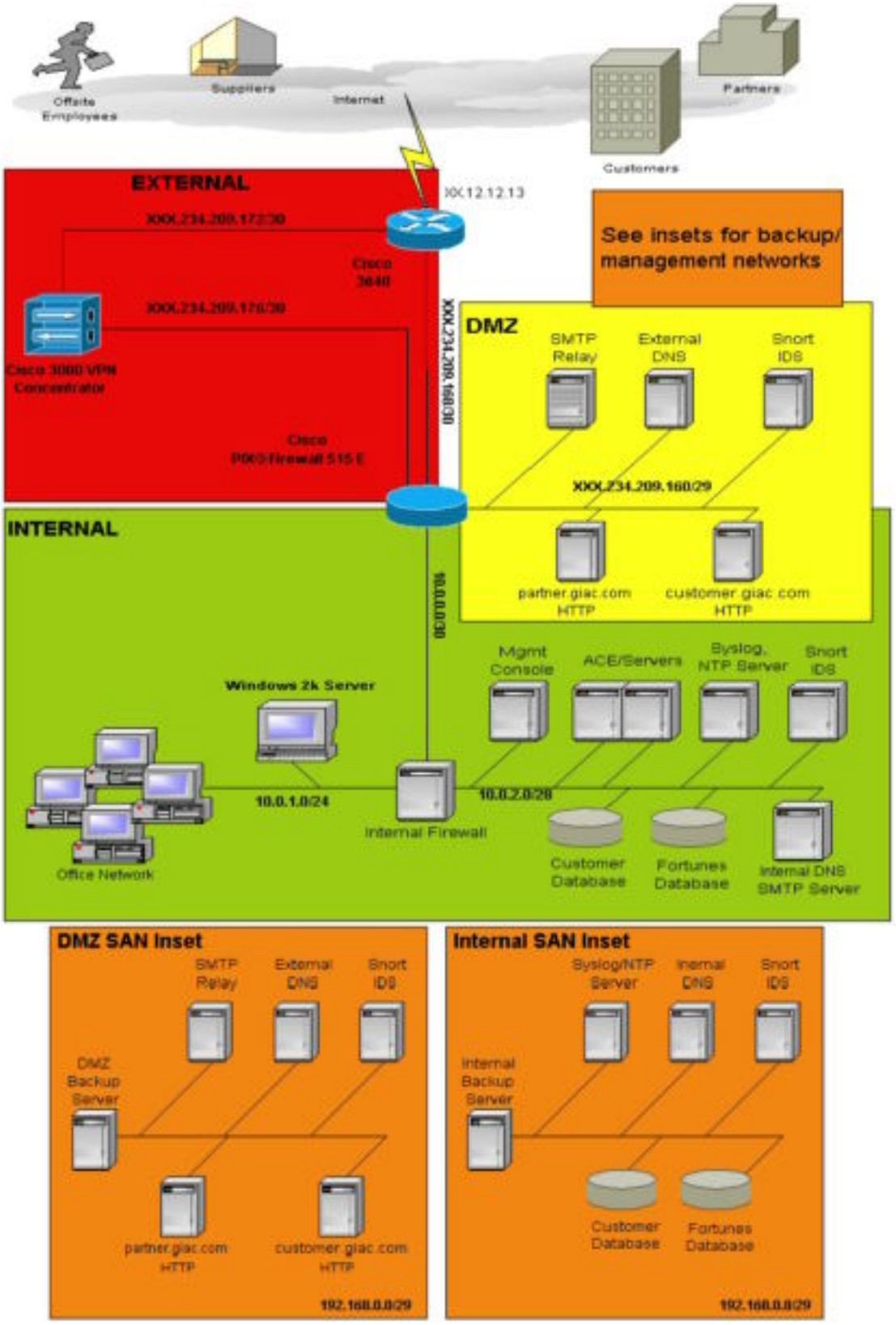
All parties will require UDP port 53 to be opened to the external DNS from the Internet to answer name queries for both the Web and SMTP servers. All parties denoted above communicate via e-mail. Port TCP 25 from the Internet will need to be opened to the SMTP relay for inbound mail. Other Internet services may be permitted on a case-by-case basis but will be blocked by default.

Ports Required

Category	TCP	UDP
Customers	25, 80, 443, (Server needs 5432)	53
Suppliers	25, (Editor needs 5432)	53
Partners	25, 80, 443, (Server needs 5432)	53
Teleworkers	22, 25, 50, 80, 110, 443, 500, 5432	50, 53, 5500
On-site employees	22, 25, 80, 110, 443, 5432	53

3. Childers, Richard. "Laptop Computer Security." Sans Info Sec Reading Room. 30 October 2000. URL: http://www.sans.org/rr/homeoffice/laptop.php (20 January 2003).

1.3 Network Diagram



1.4 IP Address Table

ISP Connection

Address/Address Block	Purpose	Notes
XX.12.12.13	3640 (ISP)	Interface e0

Public IP Address Space (XXX.234.209.160/27)

External Network (XXX.234.209.168/30)

Address/Address Block	Purpose	Notes
XXX.234.209.169	PIX (3640)	Interface e2
XXX.234.209.170	3640 (PIX)	Interface e1
XXX.234.209.171	Broadcast	Broadcast Address

External Network (XXX.234.209.172/30)

Address/Address Block	Purpose	Notes
XXX.234.209.173	VPN (3640)	Interface e0
XXX.234.209.174	3640 (VPN)	Interface e2
XXX.234.209.175	Broadcast	Broadcast Address

External Network (XXX.234.209.176/30)

Address/Address Block	Purpose	Notes
XXX.234.209.177	PIX (VPN)	Interface e1
XXX.234.209.178	VPN (PIX)	Interface e1
XXX.234.209.179	Broadcast	Broadcast Address

(Concentrator assigned 10.0.3.0/24 to distribute via DHCP to VPN users)

DMZ Network (XXX.234.209.160/29)

Address/Address Block	Purpose	Notes
XXX.234.209.161	PIX (DMZ Network)	Interface e2
XXX.234.209.162	Syslog, NTP Server	Interface e0
XXX.234.209.163	Snort IDS	Interface e0
XXX.234.209.164	Partner Web Server	Interface e0
XXX.234.209.165	Customer Web Server	Interface e0
XXX.234.209.166	Ext. DNS/SMTP Relay	Interface e0
XXX.234.209.167	Broadcast	Broadcast Address

DMZ SAN (192.168.0.0/28)

Address/Address Block	Purpose	Notes
192.168.0.1	Backup	Interface e0
192.168.0.2	Syslog, NTP Server	Interface e1
192.168.0.3	Snort IDS	Interface e1
192.168.0.4	Partner Web Server	Interface e1
192.168.0.5	Customer Web Server	Interface e1
192.168.0.6	Ext. DNS/SMTP Relay	Interface e1
192.168.0.7	Management Console	Interface e0
192.168.0.15	Broadcast	Broadcast Address

Private IP Address Space (10.0.0.0/30)

Address/Address Block	Purpose	Notes
10.0.0.1	PIX (Internal Network)	Interface e3
10.0.0.2	Internal Firewall	Interface e0
10.0.0.3	Broadcast	Broadcast Address

Private IP Address Space – Office Network (10.0.1.0/24)

Address/Address Block	Purpose	Notes
10.0.1.1	Internal Firewall	Interface e1
10.0.1.2	Windows 2000 Server	
10.0.1.3 – 10.0.1.200	DHCP Range	For Office machines only
10.0.1.201 – 10.0.1.254	Static Range	For Office Servers and devices requiring static assignment.
10.0.1.255	Broadcast	Broadcast Address

Private IP Address Space – Customer Service Network (10.0.2.0/28)

Address/Address Block	Purpose	Notes
10.0.2.1	Internal Firewall	Interface e2
10.0.2.2	Syslog	Interface e0
10.0.2.3	Snort	Interface e0
10.0.2.4	Customer Database	Interface e0
10.0.2.5	Fortunes Database	Interface e0
10.0.2.6	Internal DNS/SMTP	Interface e0
10.0.2.7	RSA Ace/Server	Interface e0
10.0.2.8	Ace/Server (Replica)	Interface e0
10.0.2.9	Management Console	Interface e0
10.0.2.15	Broadcast	Broadcast Address

Internal SAN (192.168.0.16/28)

Address/Address Block	Purpose	Notes
192.168.0.17	Backup	Interface e0
192.168.0.18	Syslog	Interface e1
192.168.0.19	Snort	Interface e1
192.168.0.20	Customer Database	Interface e1
192.168.0.21	Fortunes Database	Interface e1
192.168.0.22	Internal DNS	Interface e1
192.168.0.31	Broadcast	Broadcast Address

1.5 Explanation of Network Diagram

The GIAC Enterprises network is divided into three different layers: external (red), DMZ (yellow), and internal (green). The external (red) network has one layer of packet filtering provided by the Cisco 3640 from the Internet and has no hosts in it except those that determine access to the rest of the network.

The DMZ (yellow) network is behind the PIX which provides stateful inspection of packets that attempt to traverse it. This network has hosts in it that require public IP addresses.

The internal (green) network is behind all the filtering and inspection encountered in the other layers and is also protected by a Linux host running IPTables. This network has two subnetworks in it: office and customer service. The office network holds all the employees within it. The customer service network holds confidential and proprietary information, and support servers for office and VPN users (employees).

All devices on the red and yellow networks are housed in a secured data center with 2 APC Smart-UPS 3000VA 100V (Part Number: SU3000J) UPS systems for power management. For all Cisco equipment the redundant power supply option has been purchased. The redundant power supplies and UPS increase the availability of the network and its servers.

The DMZ bastion hosts and internal servers and databases all have second interfaces connected to DMZ and internal storage area networks. The DMZ and Internal SAN are stub networks isolated from all other traffic on their own network providing the ability to backup critical servers without impacting other traffic.

1.5.1 External Network

The red network is the network directly behind the perimeter router that borders the ISP network.

Brand and Version:	Cisco 3640 running IOS 12.2
Purpose:	Perimeter Router
Security Function:	First layer of filtering for packets coming into the GIAC network. As the first line of defense its function is to prevent obvious unwanted packets from entering the network, such as attacks from spoofed private addresses using proxy-arp or IANA reserved addresses and unwanted ICMP messages.[4]

4. The SANS Institute. Network Design and Troubleshooting, SANS Firewall Track 2.2.3. Bethesda, MD: SANS Press, p.83 (2001).

It is also the last layer of egress filtering for packets departing the GIAC network. As such it is the final chance to intercept outbound packets from machines compromised by trojans.

Network Placement:	Due to its security function, the 3640 must sit on the edge of the network demarcating where GIACs network ends and the ISP network begins.

The perimeter router is a Cisco 3640 running IOS 12.2. The router has an AUI connecting it to the ISP's T1 and 2 FE interfaces, one connecting it to the PIX and another connecting it to the VPN concentrator.

Brand and Version:	Cisco PIX515E (Software Version 6.1, 64MB RAM, Pentium 433)
Purpose:	Firewall
Security Function:	Utilizing PAT (Port Address Translation) the PIX conceals the layout of the Internal network from the outside world. It provides stateful filtering of traffic passing through it evaluating the state of the packet, the sequence number as well as the source and destination IPs. This allows the PIX to block invalid attempts at using crafted packets to gain access to the networks behind it.
Network Placement:	The Cisco PIX515E straddles all three of the networks having one interface into each of the networks. It has an additional interface connected to the VPN Concentrator. This allows it to shape traffic going from any one sub-network to any other.

The PIX515E Firewall Chassis has PIX failover software that allows another PIX to take over if the first PIX fails. The PIX also has 2 FE ports onboard, a 2-port FE card and an unrestricted license to allow for expansion and support for four Ethernet ports. A second PIX might be purchased in the future depending on network expansion to take advantage of the failover feature and increase network availability.

Brand and Version:	Cisco 3000 VPN Concentrator
Purpose:	Provide secure remote access to the Internal Network via a VPN traversing the Internet. Instead of having to use expensive dedicated lines the company can use public networks and VPN clients outside the

	firewall to access the internal networks while maintaining privacy.
Security Function:	Authenticate, verify and terminate encrypted network traffic from remote sites. IPSec will use ESP (Encapsulated Security Payload) to provide encryption and Authentication. Further authentication will be provided by SecurID. Since SecurID is supported natively on the Cisco 3000 VPN concentrator it is a logical choice for providing token, or token+password authentication.
Network Placement:	The concentrator needs to be placed on the external portion of the network so that it can be reached from the Internet. It could be placed on the edge of the network but placing it behind the perimeter router filters out some undesired traffic. The PIX also needs to be between it and the internal network to ensure that traffic coming from the concentrator undergoes stateful inspection.

The concentrator is the most expensive piece in the design. Its purchase is justified by it's native support of SecurID authentication.

1.5.2 Yellow Network (DMZ)

The yellow network is the network behind the PIX router with the least security. Servers that need to interact with the outside world are placed here.

Brand and Version:	Syslog/NTP (DMZ Network)
Purpose:	Collect Syslog messages from and synchronize bastion hosts and external network hosts.
Security Function:	This host accepts Syslog messages from the other hosts attached to the DMZ SAN. The Syslog traffic is exclusively sent over the SAN. This allows for a central point of collection for logs. This host also synchronizes the surrounding hosts, which establishes the exact time a security event occurred. This is invaluable in incident response because legal issues may arise where being able to prove the time an action was committed is vital to prosecuting a hacker.

Network Placement:	This host is placed in the DMZ to monitor all traffic coming into the DMZ. It straddles the SAN so that it can be managed from the SAN instead of being managed from the DMZ. Like snort it does not allow remote console access from the DMZ, hence it is more difficult to penetrate from the outside.
Brand and Version:	Snort (DMZ Network)
Purpose:	Monitor network for known attack signatures being launched in the DMZ.
Security Function:	Placing snort at this point detects all known attack signatures that have passed successfully through the perimeter router and the PIX to get into the DMZ. Snort provides GIAC with a means of real-time traffic analysis, packet logging, and most importantly, detecting reconnaissance and penetration attacks such as port scans, CGI attacks, OS fingerprinting and buffer overflow attacks.
Network Placement:	This host is placed in the DMZ to monitor all traffic coming into the DMZ. It straddles the SAN so that it can be managed from the SAN instead of being managed from the DMZ. Since it accepts no commands from the DMZ it is more difficult to penetrate from the outside.

Initially, Snort is left in seeking default signatures. Rules will be added and removed as necessary as needed. Logs are reviewed twice a week for anomalies and signature re-configuration and once a week a comparison is done between logs collected in the DMZ and the internal network.

Brand and Version:	Bastion hosts (RH Linux 8 running services described below.)
Purpose:	Provide a service to authorized users.
Security Function:	Hardening each host increases the difficulty for hackers attacking the GIAC network. All hosts are hardened to the following checklist. Patches are applied on a weekly basis or within 24 hours of a security notice being issued by a vendor. User accounts on each server have been audited and reduced to only those necessary to run the server.

	The services on each server have been compartmentalized into chroot()ed jails. This prevents the whole server from being compromised if the service is compromised. Hosts are audited weekly to verify that they are only running authorized services. IPTables runs on each server and is set up to prevent packets from being forwarded from the DMZ into the DMZ SAN. All bastion hosts that have SSH access on the DMZ interface have TCP Wrappers installed. This restricts access to SSH to internal and VPN IP address. The web servers are set up with swatch. When swatch is presented with a recognized attempt to hack the web server it will execute a perl script. The perl script will block access to the offending IP address by appending it to a deny list read by IPTables and restarting it (a poor man's reactive firewall). The alert will page the system administrator on call once an hour to examine the attempt.
Network Placement:	All bastion hosts are placed in the DMZ to provide the advantages of stateful inspection via the PIX and a layer of filtering from the 3640 while at the same time allowing them to be accessible from the rest of the world.

Each of the bastion hosts running on this network uses a 2Ghz Pentium 4 PC, with 1 GB of RAM, 2 100 GB HD mirrored. The hosts all run Redhat Linux 8.0 hardened for the application that they are meant to serve. Each of the Web servers runs Apache 2.0.44.

1.5.3 SAN (DMZ)

The DMZ SAN provides a network exclusively devoted to backup traffic of the bastion hosts and management of the servers. The only hosts on this privately addressed network are the bastion hosts and the backup server. The backup server and the SAN facing interfaces of the hosts in the DMZ have IPTables set to only allow services as needed for backup (and SSH in the case of Syslog and Snort).

Brand and Version:	Backup Server (RH Linux 8.0 running Amanda 2.4.2p2)
Purpose:	Provide daily backup of the bastion hosts.

Security Function:	Increase availability of the DMZ servers by providing a rapid means of recovery from catastrophic loss of a server.
Network Placement:	The backup server has only one interface to the isolated DMZ SAN. This means that one of the DMZ servers must first be compromised before attempting to gain access to the backup server.

1.5.4 Green Network (Internal)

The green network is the internal network of the company and it is privately addressed. It has the most protection. In addition to the countermeasures of the last two zones, the internal network's configuration is hidden from the outside by private addressing. The green network also has another firewall providing further protection and dividing assets into two subnetworks, one more protected than the other.

Brand and Version:	Internal Firewall running RH Linux 8 and IPTables
Purpose:	Filter internal traffic. Separate the office broadcast domain from the internal Customer Service broadcast domain.
Security Function:	This internal firewall prevents unauthorized employees from gaining access to the systems in the Customer Service networks especially the fortunes and the customer database. It increases availability to the Customer Service network by separating office traffic from Customer Service traffic.
Network Placement:	By being placed right behind the PIX but right in front of the various internal networks, this firewall can block unwanted internal traffic. On this firewall one interface goes to the PIX and the other two go to each of the internal networks: Office and Customer Service.
Brand and Version:	Internal Servers (RH Linux 8 running services described below.)
Purpose:	Provide a service to authorized internal users.
Security Function:	Hardening each host increases the difficulty for hackers attacking the GIAC network. All hosts are hardened to the following checklist. Patches are applied on a weekly basis or within 24 hours of a security notice being issued by a vendor. User

	accounts on each server have been audited and reduced to only those necessary to run the server. The services on each server have been chroot()ed to prevent the whole server from being compromised if the service is compromised. Hosts are audited weekly to verify that they are only running authorized services. IPTables runs on each server and is set up to prevent packets from being forwarded from the internal network into the internal SAN. All internal servers that have SSH access to the Customer Service network have TCP Wrappers installed. This restricts access to SSH to internal and VPN IP address.
Network Placement:	These hosts were placed in the Customer Service network because they require the greatest protection from the outside and some protection from the office network. The hosts are all have a second interface connected to the Internal SAN.

The hardware on these hosts is identical to the hardware installed on the bastion hosts. The software is identical. The internal DNS/SMTP relay server runs eXtrememail 1.5.5. (with IMAP shut down) and BIND 9.2.1.

Brand and Version:	RH Linux 8, Snort 1.9 IDS/Syslog/NTP (Internal Network)
Purpose:	Monitor network for known attack signatures. Collect Syslog messages from and synchronize internal hosts.
Security Function:	This server is hardened using the same checklist as the other servers on the network. Placing the IDS at this point detects all known attack signatures that have passed successfully through other defenses to access the internal network. Snort provides GIAC with a means of real-time traffic analysis, packet logging, and most importantly, detecting reconnaissance and penetration attacks such as port scans, CGI attacks, OS fingerprinting and buffer overflow attacks. This host accepts Syslog messages from the other hosts attached to the internal SAN. The Syslog traffic is exclusively sent over the SAN. This allows for a central point of collection for logs.

This host also synchronizes the surrounding hosts, which establishes the exact time a security event occurred. This is invaluable in incident response.

Network Placement: This host is placed in the Customer Service network to monitor all traffic coming into the Customer Service network. It straddles the Internal SAN so that it can be managed from the Internal SAN instead of being managed from the Customer Service network. Since it accepts no commands from the Customer Service network it is more difficult to penetrate from the outside.

Initially, Snort is left in seeking default signatures. Rules will be added and removed as necessary as needed. The logs on this snort server are checked with the same frequency and tests that the logs on the DMZ snort server are.

The Customer Service network holds the most mission critical servers in the company. The database server holding the fortunes and the database server holding the customer information inhabit this network. For extra redundancy on top of the normal backup routine both databases are backed up nightly onto tape drives attached to their respective machines. These backups are stored in a secured locker outside the data center in a room secured by badge reader with no other outside access. The backups are stored for 30 days.

Brand and Version: RH Linux 8, Syslog

Purpose: Provide Syslog collection exclusively for the PIX.

Security Function: Since the PIX is the heart of the network and since logging is a noted weakness of the PIX it needs a server devoted to collecting statistics from it. This server solely accepts Syslog messages from the PIX. It is hardened, as the other Linux servers have been hardened.

Network Placement: It is placed on the internal network because it needs to be well protected since the data it receives will almost definitely be critical in incident response.

Brand and Version: Windows 2000 Servers, RSA ACE/Server 5.0

Purpose: Provide SecurID authentication for the VPN.

Security Function: The VPN Concentrator uses the RSA ACE/Server to provide strong authentication for remote users connecting over the VPN. Users have a PIN, which they have been instructed to memorize.

Users also have a token (in this case an SD520 Pinpad) which provides a pseudo-random generated 6-digit number that expires every 60 seconds. The ACE/Server using the same algorithm generates the same 6-digit number. This provides token-based authentication with the PIN protecting the VPN if the token is stolen. [5]

The ACE/Server also provides individual time synchronization. This prevents the token from falling out of sync with the server and also defends against replay attacks.[6]

Network Placement: Since these hosts (primary and replica) provide authentication for the VPN they must be placed in the best-protected area of the network. This does everything possible to prevent hackers from crashing these servers. (It is assumed that if a hacker can reach these servers that the network is penetrated to the point that the hacker need not worry about obtaining VPN access).

1.5.5 SAN (Internal)

The Internal SAN provides a network exclusively devoted to backup traffic of the Customer Service hosts, the management of the Internal Snort server and the management of the Internal Syslog server. The only hosts on this privately addressed network are the internal servers and databases and the backup server. The backup server and the SAN facing interfaces of the hosts in the Customer Service network have IPTables set to only allow services as needed for backup (and SSH in the case of Syslog and Snort).

Brand and Version: Backup Server (RH Linux 8.0 running Amanda 2.4.2p2)

5. Jakobsson, Markus "How Does SecurID Work?"
URL:http://www.rsasecurity.com/rsalabs/staff/bios/mjakobsson/teaching/How%20does%20SecurID%20work_files/frame.htm. (12 February 2003).

6. Gutmann, Peter. "Encryption and Security Tutorial Part 4: Authentication" p.17.
URL:http://www.cryptoengines.com/~peter/part4.pdf. (12 February 2003).

Purpose:	Provide daily backup of the internal servers and databases.
Security Function:	Increase availability of the internal hosts by providing a rapid means of recovery from catastrophic loss of a server.
Network Placement:	The backup server has only one interface to the isolated internal SAN. This means that one of the internal servers must first be compromised before attempting to gain access to the backup server. Because they use private addressing and perform no internal routing, each of the SANs could use the same IP address space. They do not share the same address space to simplify the matter of referring to the network hosts by their IP address.

1.5.6 Network Management Center

The Network Management Center (NMC) is in a room adjacent to the data center. The NMC is secured through badge reader allowing only administrators access to the center. The same level of physical security applies to the NMC as the Data Center especially since one of the management consoles is in the Customer Service network. The backup machines and management consoles reside in the NMC. This allows staff to monitor events, check logs, burn CDs to compare logs from different networks on a non-networked machine and run backups without entering the data center.

1.6 Business Justification

The Security Architecture above is within budget and uses off-the-shelf technologies in standard configurations. It is feasible to maintain this network with two or three employees devoted to administrating and maintaining systems.

Bill of materials.

#	***Description***	***Cost***
1	Cisco 3640 with an AUI a built in WAN port and FE port	$2495
1	Cisco PIX515E Firewall with 2 FE ports onboard, a 2-port FE card and an unrestricted license	$3200
1	Cisco 3030 VPN Concentrator	$9000
1	Linux Firewall Server running IPTables	$300
1	Ace Server Base License v5.1 25 Users (incl. 1 replica)	$3700
25	SD-520 PinPad Token 4 year, 6 digit, 60 second	$2125

Since the Cisco 3640 is capable of supporting aT3 connection it provides the ability to expand GIAC's connectivity to the outside world in the next couple of years without changing routing gear. The 3640 also supports logging violations

of its extended ACLs. The Cisco PIX515E Firewall uses Cisco's Adaptive Security Algorithm (ASA). ASA offers stateful, connection-oriented inspection of packets that passed through the ACLs on the 3640. It is capable of handling the same amount of traffic as the router above, that means the PIX will also meet GIAC's network capacity needs in the medium term.

The Cisco 3030 VPN Concentrator provides 3DES encryption for GIAC's VPN Traffic. It provides a spectrum of methods of authentication including: RADIUS, Windows NT, TACACS+, SecurID and it's own internal database. Although only client-to-LAN connections are planned with the Concentrator thus far it is capable of establishing IPSEC connections to partner or remote if it is deemed necessary in the future.

Assignment 2 – Security Policy and Tutorial

2.0 Scope and Caveats

This document will define the security policy for the Perimeter Router, Firewall and VPN Concentrator (Hereafter denoted as Firewall Security Policy). It will define the ACLs, ruleset and IPSec policy (as needed) for the device.

It is assumed that the Firewall Security Policy is part of a comprehensive Network Security Policy. This Firewall Security Policy should be updated as business or technical needs warrant by GIAC's CIO after ratification of the policy by the board of directors.

It is also assumed these devices are physically secured in a room without dropped ceilings, with a solid door, no windows and access restricted at least by a lock and preferably a badge reader. If any of this equipment needs to be moved, installed, or removed approval must come from GIAC's CIO. This Firewall Security Policy is based on section 3.3.4 of the NSA's Router Security Configuration Guide.[7]

Performing hardware maintenance, changing the physical configuration of the router, and physically connecting to the router are activities restricted to the IT department of GIAC. The console ports of the devices in question are not to be connected to any out-of-band connections.

All equipment on the network shall be set to use UTC time. Equipment will synchronize with NTP where supported (the PIX does not support NTP). Where not supported, GIAC staff will have to manage synchronization as needed.

Since packets test against access lists from top to bottom[8], security rules with more specific criteria will be placed before rules covering general criteria. Wherever possible, rules that are used more often will be placed closer to the front of a list. These two policies should optimize the speed by which packets test against the access list.

Changes to the Firewall configuration (and the tests that come with such changes) will only be made between the hours of 0400 and 0700 Tuesday through Thursday (except in the case of emergency patches). This will prevent sudden changes and mistaken configurations from unduly impacting the enterprise. A bad configuration can be backed out of if it cannot be corrected before 0700. Firewall changes and maintenance will be reviewed weekly on Friday to plan what changes will be made in the next week. All

7. Antonine, Vanessa, et al. Router Security Configuration Guide. Fort Meade: National Security Agency, 2002. p. 45-50.

8. Chapell, Laura. Introduction to Cisco Router Configuration. Indianapolis: Macmillan Technical Publishing, 1999. p. 316.

changes to the defensive configurations of GIAC's networks must be tested to ensure that the changes put in place to indeed perform as intended.

2.1 Perimeter Router Security Policy

2.1.1 Login Banner

A login banner, which includes a legal notice, is placed on the perimeter router warning anyone who accesses the router of the legal implications of unauthorized use. Issuing the following command in global configuration mode (GIAC_3640(config)#) configures the GIAC banner:

```
GIAC_3640(config)# banner motd #
This system is the property of GIAC Enterprises. It is for authorized
use only. Users (authorized or unauthorized) have no explicit or
implicit expectation of privacy.

Any or all uses of this system and all files on this system may be
intercepted, monitored, recorded, copied, audited, inspected, and
disclosed to authorized site, GIAC Enterprises, and law enforcement
personnel.

By using this system, the user consents to such interception,
monitoring, recording, copying, auditing, inspection, and disclosure at
the discretion of authorized site or GIAC Enterprises personnel.

Unauthorized or improper use of this system may result in
administrative disciplinary action and civil and criminal penalties. By
continuing to use this system you indicate your awareness of and
consent to these terms and conditions of use. LOG OFF IMMEDIATELY if
you do not agree to the conditions stated in this warning.[9]
#
```

2.1.2 Restrict Console and Auxiliary Port Access

Since there is a restriction on placing console ports on an out of band network, the console is safe from network breaches. However if there is a breach in physical security access to the console port of the perimeter router could easily provide opportunity for a breach. The following commands should be issued so that console access is restricted. [10]

The first command sets a username and password for authentication on the console. The 0 after password means that the password string is unencrypted as it is entered into the box.

9. Computer Incident Advisory Capability. "Information Bulletin J-043g: Creating Login Banners." CIAC. 9 May 2000. URL: http://www.ciac.org/ciac/bulletins/j-043.shtml (20 January 2003).

10. Cisco Tech Notes. "Improving Security on Cisco Routers." Cisco Systems. 29 December 2002. URL: http://www.cisco.com/warp/public/707/21.html#pass (20 January 2003)

The command after that drops the router into configuration mode for the console. The next line reduces the default timeout on the console from ten minutes to two-and-a-half. Finally the login local command is set so that authentication comes from the user database on the router itself instead of from remote authentication. The auxiliary port will not be used and hence has been disabled in the configuration.

```
GIAC_3640(config)#username sheare password 0 sanj0se32cats
GIAC_3640(config)# line con 0
GIAC_3640(config-line)# exec-timeout 2 30
GIAC_3640(config-line)# login local
GIAC_3640(config-line)# end
GIAC_3640(config)# line aux 0
GIAC_3640(config-line)# no exec
GIAC_3640(config-line)# transport input none
```

2.1.3 Restrict VTY Access

Virtual Terminal access to the router from a remote site can be just as damaging as a console breach. The following commands should be issued so that vty access is restricted. [11] The first command creates an access list that only permits access to traffic coming from the management net. The next addition to the access list denies all other IP traffic.

The next commands restricting the virtual terminals to only accepting traffic from SSH require line configuration mode. Set login to local authentication. Set time out to two-and-a-half minutes, also set the router to disconnect after three failed login attempts. Finally set the access list in operation for incoming traffic on the virtual terminals.

```
GIAC_3640(config)# access-list 1 permit 10.0.2.0 0.0.0.255
GIAC_3640(config)# access-list 1 deny ip any any log
GIAC_3640(config)# line vty 0 4
GIAC_3640(config-line)# transport input ssh
GIAC_3640(config-line)# login local
GIAC_3640(config-line)# ip ssh time-out 150
GIAC_3640(config-line)# ip ssh authentication-retries 3
GIAC_3640(config-line)# access-class 1 in
GIAC_3640(config-line)# end
```

2.1.4 Disable Services not in use

The following commands should disable services that the router will not need in normal operation. The commands are issued from global configuration mode.

"Cisco Discovery Protocol (CDP) is primarily used to obtain protocol addresses of neighboring devices and discover the platform of those devices. CDP can also be

11. Ibid.

used to show information about the interfaces your router uses."[12] Since CDP is such a great reconnaissance tool and since the network and the equipment on it is already well known CDP must be disabled.

```
GIAC_3640(config)# no cdp run
```

The router will not be assigning IP addresses to other routers using bootp. If it were enabled it could potentially allow a hacker to receive a trusted IP address.

```
GIAC_3640(config)# no ip bootp server
```

```
Late versions of IOS have a web server onboard for management of the
router. The web server is an extra service for configuring the router
that since it is not in use should be shutdown.
```

```
GIAC_3640(config)# no ip http server
```

Squelch the option in IP packets for the sender of the packet to dictate the route back to the source address. This will make it harder to penetrate the network by spoofing the IP address.[13]

```
GIAC_3640(config)# no ip source-route
```

Finger, the small services (on both TCP and UDP) and SNMP must be disabled. The small services and finger have no use on the network. Disable SNMP, the network is small enough that the vulnerabilities do not outweigh the troubleshooting advantages.

```
GIAC_3640(config)# no service finger
GIAC_3640(config)# no service tcp-small-servers
GIAC_3640(config)# no service udp-small-servers
GIAC_3640(config)# no snmp
```

For each interface the following commands should be issued:

There should be no need to proxy arps. If ip proxy arps are enabled they could be used to spoof by sending packets from outside the network into the network with addresses from inside the network.

```
GIAC_3640(config-if)# no ip proxy-arp
```

Disabling directed broadcasts mitigates SMURF attacks. It must be used on all routers on the network and not on just the perimeter router to be effective[14]

12. Cisco Documentation. "Configuring Cisco Discovery Protocol." Cisco Systems. 15 January 2002. URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/fcprt3/fcd301c.htm (20 January 2003)

13. Internet FAQ Consortium. "What Can I Do About Source Routing?" Internet FAQ Consortium. 17 January 2003. URL:http://www.faqs.org/faqs/cisco-networking-faq/section-23.html (20 January 2003).

```
GIAC_3640(config-if)# no ip-directed-broadcasts
```

Squelching the following three commands prevents reconnaissance hackers from gaining information from ICMP messages.

```
GIAC_3640(config-if)# no ip unreachable
GIAC_3640(config-if)# no ip redirect
GIAC_3640(config-if)# no ip mask-reply
```

2.1.5 ACLs

The extended access list command on the Cisco 3640 router looks like this:

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} protocol source source-wildcard destination
destination-wildcard [precedence precedence] [tos tos] [log | log-
input] [time-range time-range-name]
```
[15]

GIAC staff will review firewall lists weekly (as part of the change control meeting on Friday). This ensures that there are not contradictory, ineffective or duplicate rules.[16]

2.1.6 Inbound Access Control Lists (Ingress Filtering)

The ingress filters will be placed upon the Internet facing serial interface. The first commands configure and load the access list onto that interface.

```
GIAC_3640(config)# int serial 0/0
GIAC_3640(config-int)# ip address XYZ.12.12.13 255.255.255.252
GIAC_3640(config-int)# ip access-group 100 in
```

The ingress filter begins with the most common attacks with specific rules to deny any inbound IP packet that contains an IP address from GIAC's network to mitigate the risk of spoofing. Next all private (per RFC 1918), Class D (Multicast) and Class E (Experimental) IP addresses coming from the Internet are denied.

Next, the less common attack possibilities are eliminated such as the Default DHCP network, localhost, default network address, and addresses IANA has reserved that should not be in use[17].

---

14. CERT Coordination Center. "CERT® Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks." CERT. 13 March 2000 URL:http://www.cert.org/advisories/CA-1998-01.html (20 January 2003).

15. Cisco CCO, "Configuring Commonly Used IP ACLs." Cisco Systems. 20 November 2002 URL: http://cco-rtp-1.cisco.com/en/US/tech/tk648/tk361/technologies_configuration_example09186a0080100548.shtml (20 January 2003.)

16. The SANS Institute, Building a Rule Base: Defense In-Depth, SANS Firewall Track 2.3.2, Bethesda, MD: SANS Press, p. 68 (2001).

17. IANA, "Internet Protocol V4 Address Space." IANA. 10 December 2002 URL: http://www.iana.org/assignments/ipv4-address-space (20 January 2003)

Ports well known to have services that could threaten the enterprise as defined in the SANS/FBI 20 Most Critical Internet Security Vulnerabilities are denied at this firewall. These include: rpc, NFS, lockd, NetBIOS, SNMP. Syslog, and TFTP should not come into the corporate network from the outside.

There must be nothing inside the corporate network running a high level port normally chosen for HTTP. So those have been disabled.
Finally, certain ports have to be left open. These ports are necessary for the day-to-day operation of the enterprise and include: The web servers, mail servers, DNS, and the VPN concentrator.

Cisco 3640 Allowed Checklist

From	To	Service	Port
Everywhere	customer.giac.net	www	80/TCP
Everywhere	customer.giac.net	ssl	443/TCP
Everywhere	partner.giac.net	www	80/TCP
Everywhere	partner.giac.net	ssl	443/TCP
Everywhere	External DNS	DNS	53/UDP
ISP DNS	External DNS	DNS (Zone Xfer)	53/TCP
Everywhere	SMTP Server	SMTP	25/TCP
Everywhere	VPN Concentrator	SecurID	5500/UDP
Everywhere	VPN Concentrator	IKE	500/UDP
Everywhere	VPN Concentrator	ESP	50/IP

All ICMP not specifically for MTU discovery is denied. Only established TCP sessions are allowed through to mitigate DoS attacks. After all the other filters only traffic destined for GIAC addresses is allowed through. All other addresses are denied and logged.

```
! - GIAC's subnet should not come from the outside.
access-list 100 deny ip XXX.234.209.160 0.0.0.31 any log

! - Private addresses
access-list 100 deny ip 10.0.0.0 0.255.255.255 any log
access-list 100 deny ip 172.16.0.0 0.15.255.255 any log
access-list 100 deny ip 192.168.0.0 0.0.255.255 any log

! - Multicast and Experimental
access-list 100 deny ip 224.0.0.0 31.255.255.255 any log

! - DHCP default network.
access-list 100 deny ip 169.254.0.0 0.0.255.255 any log

! - localhost
access-list 100 deny ip 127.0.0.0 0.255.255.255 any log

! - IANA reserved
access-list 100 deny ip 1.0.0.0 0.255.255.255 any log
access-list 100 deny ip 2.0.0.0 0.255.255.255 any log
access-list 100 deny ip 5.0.0.0 0.255.255.255 any log
access-list 100 deny ip 7.0.0.0 0.255.255.255 any log
```

```
access-list 100 deny ip 23.0.0.0 0.255.255.255 any log
access-list 100 deny ip 27.0.0.0 0.255.255.255 any log
access-list 100 deny ip 31.0.0.0 0.255.255.255 any log
access-list 100 deny ip 36.0.0.0 1.255.255.255 any log
access-list 100 deny ip 39.0.0.0 0.255.255.255 any log
access-list 100 deny ip 41.0.0.0 0.255.255.255 any log
access-list 100 deny ip 42.0.0.0 0.255.255.255 any log
access-list 100 deny ip 58.0.0.0 1.255.255.255 any log
access-list 100 deny ip 60.0.0.0 0.255.255.255 any log
access-list 100 deny ip 70.0.0.0 1.255.255.255 any log
access-list 100 deny ip 72.0.0.0 7.255.255.255 any log
access-list 100 deny ip 80.0.0.0 15.255.255.255 any log
access-list 100 deny ip 96.0.0.0 31.255.255.255 any log
access-list 100 deny ip 197.0.0.0 0.255.255.255 any log
access-list 100 deny ip 222.0.0.0 1.255.255.255 any log

! - Ports
! - NetBIOS in Win NT 135(tcp & udp),137, 138(udp),139(tcp).
access-list 100 deny tcp any any range 135 139 log
access-list 100 deny udp any any range 135 139 log

! - Windows 2000 also uses 445(tcp and udp)
access-list 100 deny tcp any any eq 445 log
access-list 100 deny udp any any eq 445 log

! - SNMP, Syslog, TFTP, FTP
access-list 100 deny udp any any range 161 162 log
access-list 100 deny udp any any eq 514 log
access-list 100 deny udp any any eq 69 log
access list 100 deny tcp any any eq 21 log

! - RPC and NFS(111/tcp and 111/udp)
access-list 100 deny tcp any any eq 111 log
access-list 100 deny udp any any eq 111 log

! - NFS (2049/tcp and 2049/udp)
access-list 100 deny tcp any any eq 2049 log
access-list 100 deny udp any any eq 2049 log

! - lockd (4045/tcp and 4045/udp)
access-list 100 deny tcp any any eq 4045 log
access-list 100 deny udp any any eq 4045 log

! - X Windows 6000/tcp - 6255/tcp
access-list 100 deny tcp any any range 6000 6255 log

! - high HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp)
access list 100 deny tcp any any eq 8000 log
access list 100 deny tcp any any eq 8080 log
access list 100 deny tcp any any eq 8888 log

! - Deny hacker tools
access list 100 deny ip any any eq 31337 log
access list 100 deny tcp any any range 12345 12346 log
access list 100 deny tcp any any eq 20034 log
access list 100 deny tcp any any eq 27665 log
```

```
access list 100 deny udp any any eq 27444 log
access list 100 deny udp any any eq 31335 log

! - Permissions
! - Allow HTTP/S traffic to Customer
access-list 100 permit tcp any XXX.234.209.165  eq www
access-list 100 permit tcp any XXX.234.209.165  eq 443

! - and Partner
access-list 100 permit tcp any XXX.234.209.164  eq www
access-list 100 permit tcp any XXX.234.209.164  eq 443

! - Permit inbound email traffic to the mail server.
access-list 100 permit tcp any host XXX.234.209.166 eq smtp

! - Permit DNS traffic from the ISP
access-list 100 permit udp any host XXX.234.209.166 eq domain

! - Zone transfers from ISP only.
access-list 100 permit tcp host XYZ.12.12.13 host XXX.234.209.166 eq
domain
access-list 100 deny tcp any any eq 53 log

! - VPN Concentrator Traffic.
access list 100 permit udp any XXX.234.209.173 eq 5500
access list 100 permit udp any XXX.234.209.173 eq 500
access list 100 permit esp any XXX.234.209.173

! - Deny ICMP packets, MTU discovery(type 3, type 4)
access-list 100 permit icmp any XXX.234.209.160 0.0.0.31 3 4
access-list 100 deny icmp any XXX.234.209.160 0.0.0.31 log

! - Permit only established traffic to mitigate DoS attacks
access-list 100 permit tcp any any established

! - Permit only traffic for GIAC's ip range.
access-list 100 permit ip any XXX.234.209.160 0.0.0.31 any

! - Explicitly deny all other addresses
access-list 100 deny ip any any log-input
```

2.1.7 Outbound Access Lists (Egress Filtering)

The egress filter is placed on the Fast Ethernet interface facing the internal network. It tracks traffic that is moving through that interface out to the Internet. First the FastE interface is configured. ICMP for any MTU discovery is permitted outbound, as it was inbound so that local hosts can resend smaller packets. All ECHO replies and time exceeded are dropped. All outbound IP traffic from a source not on the GIAC network is dropped. Finally addresses not specifically permitted are denied.

```
GIAC_3640 (config)# interface fastethernet 0/1
GIAC_3640 (config-int)ip address XXX.234.209.170 255.255.255.224
GIAC_3640 (config-int)# ip access-group 101 in
```

```
! - MTU size discovery
access-list 101 permit icmp XXX.234.209.160 255.255.255.224 any packet-
too-big
access-list 101 permit icmp XXX.234.209.160 255.255.255.224 source-
quench

! - Deny echo-replies and time exceeded out of the local network.
access-list 101 deny icmp any any echo-reply
access-list 101 deny icmp any any time exceeded

! - Deny outbound IP packet unless address is a GIAC address.
access-list 101 permit ip XXX.234.209.160 0.0.0.31 any

! - Explicit deny
access-list 101 deny ip any any log-input
```

2.1.8 Logging

Before logging is set up, time synchronization is set up with the organization's NTP server. Logging is buffered with a timestamp and then set to send all logs to the syslog server. While testing the network the logs will be set as verbose as possible. Once traffic becomes more predictable logs will be reduced to maintenance levels.

```
GIAC_3640(config)# ntp server XXX.234.209.162
GIAC_3640(config)# service timestamps debug datetime msec localtime
show-timezone
GIAC_3640(config)# service timestamps log datetime msec localtime show-
timezone
GIAC_3640(config)#logging XXX.234.209.162
GIAC_3640(config)#logging trap debugging
GIAC_3640(config)#logging console debug
```

2.1.9 Passwords and Privileges

Following the principle of least privilege, individual accounts are assigned to Network administrators at GIAC allowing them each the least amount of privilege needed to manage the routers. The `enable secret` command provides encryption for the enable password. The service password-encryption protects VTY, AUX and Console passwords with MD5 encryption. Clear-text passwords are encrypted by this service and are stored in configuration. This means the encrypted password is visible via the `show conf` command. Here are examples of the commands that would be issued:

```
GIAC_3640(config)# enable secret 0 chicken7thoughts
GIAC_3640(config)# service password-encryption
GIAC_3640(config)# username sheare password sanj0se32cats
GIAC_3640(config)# username sheare privilege 1
GIAC_3640(config)# privilege exec level 15 show ip
GIAC_3640(config)# privilege exec level 15 show
GIAC_3640(config)# username csmith password nosun6nomoon
GIAC_3640(config)# username csmith privilege 15
GIAC_3640(config)# privilege exec level 15 show access-list
GIAC_3640(config)# privilege exec level 15 show ip accounting
```

```
GIAC_3640(config)# username avasquez password alphatomato1
GIAC_3640(config)# username avasquez privilege 1
GIAC_3640(config)# privilege exec level 1 show access-list
GIAC_3640(config)# privilege exec level 1 show ip accounting
```

Once these tasks are completed the configuration should be saved to NVRAM and a copy of the configuration should be cut and pasted from the console and labeled with the date, type of router and version of IOS. For example: `20030104Cisco_3640v12.2.`

2.2 Firewall Policy (PIX 515E)

After the first layer of packet filtering provided by the external router the Cisco PIX 515E will provide stateful packet inspection for inbound and outbound traffic. Before configuring the PIX Firewall, the network diagram has been drafted with IP addresses that will be assigned to the PIX Firewall and those of routers on each interface. The Security Level for each interface has been noted. [18]

2.2.1 Access Control, Logging and disabling unwanted services

First the enable password must be set for the Cisco PIX 515E to ensure secure access while configuring the firewall. As with the router, syslog has been enabled to provide timestamped logs to syslog. NTP is not supported by the PIX so time has to be manually checked at least once every six months to account for daylight savings and weekly to ensure no drift has occurred that may affect the logs.[19] Since no SNMP is used on site that is disabled as well.

```
pixfirewall(config)# enable password helena3rats
pixfirewall(config)# logging buffered debugging
pixfirewall(config)# logging timestamp
pixfirewall(config)# logging host XXX.234.209.162 udp
pixfirewall(config)# no snmp-server location
pixfirewall(config)# no snmp-server contact
pixfirewall(config)# snmp-server community public
```

2.2.2 Interface Configuration

On this network there are four interfaces on the PIX firewall – Outside, DMZ, VPN and Inside. With PIX there are security levels set on each interface that you name with the nameif command.

ASA security levels control access between systems on different PIX interfaces. The relative security levels of the interfaces either enable or restrict access.

```
pixfirewall(config)# nameif e0 outside security0
pixfirewall(config)# nameif e1 dmz security50
pixfirewall(config)# nameif e2 vpn security25
pixfirewall(config)# nameif e3 inside security100
```

18. Cisco Systems, “Basic Firewall Configuration.” 10 June 2002.

URL:http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/config/bafwcfg.htm (20 January 2003).

19. Chapman, David W., Fox Andy, Cisco Secure Pix Firewalls, Indianapolis: Cisco Press, 2002, p. 107

The IP address and mask for each interface is set with the following commands.

```
pixfirewall(config)# ip address outside XXX.234.209.169 255.255.255.252
pixfirewall(config)# ip address dmz     XXX.234.209.161 255.255.255.252
pixfirewall(config)# ip address vpn     XXX.234.209.177 255.255.255.252
pixfirewall(config)# ip address inside  10.0.0.1        255.255.255.252
```

PIX interfaces are shutdown by default. The interface command enables the interface. Auto-negotiation is disabled on the three interfaces where there is no possibility of other traffic. The DMZ does not have a switch and so half-duplex needs to be used because more than two systems share the same network segment. By default MTU is set at 1500.

```
pixfirewall(config)# interface ethernet0 100full
pixfirewall(config)# interface ethernet1 100basetx
pixfirewall(config)# interface ethernet2 100full
pixfirewall(config)# interface ethernet3 100full
```

The default `fixup protocol` values installed on the PIX need to be changed to reflect the GIAC security policy. The `fixup protocol` command identifies which protocols are to be examined by Cisco's Adaptive Security Algorithm (ASA), which stores that information in a hash in the state table.[20]

.

The ASA hash contains information such as: source and destination address, port number, TCP flags and sequence numbers. When the reply returns, the hash is checked against the state table. If there is a match then the packets are allowed, otherwise the packet is dropped.

To conform to the security policy the following commands must be issued. First h323 and sip can be removed (they are fixup protocols by default). FTP has an extra command keyword in it to fix a vulnerability regarding Malicious HTML Tags Embedded in Client Web Requests[21]. Next NTP, and DNS need to flow through the PIX and hence are added to the fixup protocol list. HTTP, SMTP, and SQLNet are also fixup protocols by default.[22]

```
pixfirewall(config)# fixup protocol ftp strict 21
pixfirewall(config)# no fixup protocol rsh 514
pixfirewall(config)# no fixup protocol h323 1720
pixfirewall(config)# no fixup protocol sip 5060
pixfirewall(config)# fixup protocol domain 53
pixfirewall(config)# fixup protocol ntp 123
```

20. The SANS Institute, Firewalls 102: Perimeter Protection with Firewalls, SANS Firewall Track 2.2.5, Bethesda, MD: SANS Press, p. 189 (2001).

21. Cisco Security Advisory, "Cisco Secure PIX Firewall FTP Vulnerabilities." Cisco Systems. 27 June 2000. URL:http://www.cisco.com/warp/public/707/pixftp-pub.shtml (20 January 2003).

22. Chapman and Fox, p. 93.

2.2.3 Firewall Routing Configuration

Route and RIP information must be configured on the PIX firewall interfaces. Route information specifies the interface to which packets should be forwarded. The PIX also examines RIP traffic to passively ascertain the location of devices of the network.

The outside interface facing the perimeter router (e0) should be configured first.

```
pixfirewall(config)# route outside XXX.234.209.168 255.255.255.252
XXX.234.209.170 1
```

The default route to the perimeter router (209.170) is through the outside interface 1 hop away from the PIX. The 0 0 in the command is shorthand for broadcasting the packets out to that subnet using the default mask. The other interfaces have other subnets behind them and must be set up differently. The PIX should broadcast an ARP into the DMZ and hence the DMZ needs no route.

```
pixfirewall(config)# route inside 10.0.0.0 255.255.255.252 10.0.0.2 1
pixfirewall(config)# route vpn XXX.234.209.176 255.255.255.252
XXX.234.209.178 1
```

Accessing lower security level interfaces from a higher-level interface requires the `nat` and `global` commands. Network Address Translation (NAT) translates a local range of addresses into a global range of addresses, in effect keeping GIAC's internal IP addresses unknown to the external networks. Port Address Translation (PAT) translates a private session from an internal address to a port on an outside address. The PIX at GIAC is configured to use NAT until the IP addresses are exhausted at which point it switches over to using PAT. To use PAT issue the global command with one IP address instead of a range of addresses.

```
pixfirewall(config)# nat(inside) 1 0.0.0.0 0.0.0.0
pixfirewall(config)# nat(dmz) 2 XXX.234.209.160 255.255.255.248
pixfirewall(config)# nat(vpn) 3 XXX.234.209.172 255.255.255.252
pixfirewall(config)# global(outside) 1 XXX.234.209.185-XXX.234.209.189
255.255.255.248
pixfirewall(config)# global(outside) 1 XXX.234.209.190 255.255.255.248
pixfirewall(config)# global(outside) 2 XXX.234.209.160 255.255.255.248
pixfirewall(config)# global(outside) 3 XXX.234.209.172 255.255.255.252
```

The interface name in parenthesis is the source interface. The following number is the NAT ID. The IP address represents the mapping between an address on the private network (in the case of the `nat` command) and an address or range of addresses on the perimeter or external network (in the case of the `global` command). The `nat(inside)` command here says to take any address from the inside interface and translate it to an address in the range listed in the `global(outside)` command.

Access to higher security level interfaces than the one the packet entered requires the static and access-list commands. The static command protects zones with higher security levels by not providing access to them without explicitly specification of the IP address space or service. The access-list command allows the inside host to be accessed from the outside much like with a firewall.

The servers in the DMZ must be accessible from the Internet.

```
pixfirewall(config)# static (dmz, outside) XXX.234.209.164
XXX.234.209.164 netmask 255.255.255.255
pixfirewall(config)# static (dmz, outside) XXX.234.209.165
XXX.234.209.165 netmask 255.255.255.255
pixfirewall(config)# static (dmz, outside) XXX.234.209.166
XXX.234.209.166 netmask 255.255.255.255
```

VPN users need to be able to access the Internal Network from the Internet.

```
pixfirewall(config)# static (inside, vpn) 10.0.0.0 10.0.0.0 netmask
255.0.0.0
```

The access lists still need to be put in place to complete access to the devices. The outside_in access list will control traffic inbound from the interface facing the perimeter router.

```
! - Internet to Web Server and SSL
access-list outside_in permit tcp any host XXX.234.209.164 eq www
access-list outside_in permit tcp any host XXX.234.209.164 eq 443
access-list outside_in permit tcp any host XXX.234.209.165 eq www
access-list outside_in permit tcp any host XXX.234.209.165 eq 443

! - Internet to SMTP Proxy
access-list outside_in permit tcp any host XXX.234.209.166 eq smtp

! - Internet to External DNS
access-list outside_in permit udp any host XXX.234.209.166 eq domain

! - ISP DNS to External DNS (zone transfer)
access-list outside_in permit tcp host XYZ.12.12.14 host
XXX.234.209.166 eq domain

! - Public Stratum 2 NTP to NTP Server
access-list outside_in permit udp host XZ6.200.93.8 host
XXX.234.209.162 eq ntp
access-list outside_in permit udp host XW0.162.8.3 host XXX.234.209.162
eq ntp
access-list outside_in permit udp host X8.82.161.227 host
XXX.234.209.162 eq ntp

! - Perimeter Router to Syslog
access-list outside_in permit udp host XXX.234.209.170 host
XXX.234.209.162 eq 514
```

```
access-list outside_in permit udp host XXX.234.209.170 host
XXX.234.209.162 eq ntp
access-list outside_in deny ip any any log-input
```

The dmz_in access list will control traffic inbound from the interface facing the dmz

```
! - smtp proxy to smtp internal
access-list dmz_in permit tcp host XXX.234.209.166 host 10.0.2.6 eq
smtp

! - web server to db access
access-list dmz_in permit tcp host  XXX.234.209.165 host 10.0.2.4 eq
5432
access-list dmz_in permit tcp host  XXX.234.209.165 host 10.0.2.5 eq
5432
access-list dmz_in permit tcp host XXX.234.209.164 host 10.0.2.5 eq
5432

! - external to internal DNS
access-list dmz_in permit udp host  XXX.234.209.166 host 10.0.2.6 eq
domain

access-list dmz_in deny ip any any log-input
```

The vpn_in access list will control traffic inbound from the interface facing the vpn

```
! - Remote Employees can access the database via the VPN
access-list vpn_in permit tcp 10.0.3.0 255.255.255.0  host 10.0.2.4 eq
5432
access-list vpn_in permit tcp 10.0.3.0 255.255.255.0  host 10.0.2.5 eq
5432

! - Get and receive e-mail
access-list vpn_in permit tcp 10.0.3.0 255.255.255.0 host 10.0.2.6 eq
smtp
access-list vpn_in permit tcp 10.0.3.0 255.255.255.0 host 10.0.2.6 eq
pop3

! - DNS and secondary DNS for the VPN
access-list vpn_in permit udp 10.0.3.0 255.255.255.0 host 10.0.2.6 eq
domain
access-list vpn_in permit udp 10.0.3.0 255.255.255.0 host
XXX.234.209.166 eq domain

! - Secure copy new web pages.
access-list vpn_in permit tcp 10.0.3.0 255.255.255.0 host
XXX.234.209.164 eq ssh
access-list vpn_in permit tcp 10.0.3.0 255.255.255.0 host
XXX.234.209.165 eq ssh

! - Syslog and NTP
access-list vpn_in permit tcp XXX.234.209.176 255.255.255.252 host
XXX.234.209.162 eq 514
```

```
access-list vpn_in permit tcp XXX.234.209.176 255.255.255.252 host
XXX.234.209.162 eq ntp

! - VPN RSA Ace/Server access
access-list vpn_in permit udp XXX.234.209.176 255.255.255.252 host
10.0.2.7 eq 5500
access-list vpn_in permit udp XXX.234.209.176 255.255.255.252 host
10.0.2.8 eq 5500


access-list vpn_in deny ip any any log-input
```

The internal_out access list will control traffic inbound from the interface facing the internal network.

```
! - Allow out of the internal office network HTTP/S, FTP traffic
! - POP3, and Secondary DNS.
access-list internal_out permit tcp 10.0.1.0 255.255.255.0 any eq www
access-list internal_out permit tcp 10.0.1.0 255.255.255.0 any eq 443
access-list internal_out permit tcp 10.0.1.0 255.255.255.0 any eq ftp
access-list internal_out permit tcp 10.0.1.0 255.255.255.0 any eq pop3
access-list internal_out permit tcp 10.0.1.0 255.255.255.0 any eq
domain

! - Allow the internal SMTP gateway to speak to the external gateway
access-list internal_out permit tcp host 10.0.2.6 host XXX.234.209.166
eq smtp

! - Allow the internal DNS server to speak to the DMZ DNS Server to
pick up zone transfers and queries
access-list internal_out permit ip 10.0.2.6 255.0.0.0 host
XXX.234.209.166 eq domain

! - Allow the on-site employees to edit the web pages
access-list internal_out permit tcp 10.0.1.0 255.255.255.0 host
XXX.234.209.164 eq ssh
access-list internal_out permit tcp 10.0.1.0 255.255.255.0 host
XXX.234.209.165 eq ssh
access-list internal_out deny ip any any log-input
```

We will need to apply these access lists to the appropriate interfaces using the following commands:

```
access-group outside_in in interface outside
access-group dmz_in in interface dmz
access-group vpn_in in interface vpn
access-group internal_out in interface internal
```

The PIX should be managed from the 10.0.1.0 network using SSH.[23] To do this the PIX must be set up to run SSH first by generating and saving an RSA key

23. Chapman and Fox, p. 306-307

then by specifying what hosts can access the PIX via SSH and setting the inactivity timeout. Telnet service to the console is denied.

```
pixfirewall(config)# hostname GIAC_pix_1
GIAC_pix_1(config)# domain-name giac.com
GIAC_pix_1(config)# ca generate rsa key 2048
GIAC_pix_1(config)# ca save all
GIAC_pix_1(config)# ssh 10.0.1.0 255.255.255.0 inside
GIAC_pix_1(config)# ssh timeout 5
```

Once again write the whole thing to memory.

```
GIAC_pix_1(config)# write mem
GIAC_pix_1(config)# tftp-server dmz ext-services /20030106pix515w.conf
GIAC_pix_1(config)# write net :
Building configuration...
TFTP write '/20030106pix515w.conf' at ext-services on interface 2
[OK]
```

2.3 VPN Policy

GIAC teleworkers and offsite salespeople will connect to the network from the Internet using Cisco's VPN Client software to form a VPN tunnel to the Cisco VPN Concentrator 3030. GIAC has no need to allow partner or supplier traffic to come across a VPN. Each of those groups accesses their required information through an encrypted web browser. So the IPSec policy only has to be set to allow through traffic for employees and sales force to access required resources. Remote users need to retrieve email, access and edit the web servers, access and edit the customer and fortunes database.

2.3.1 IKE Policy

The IKE (Internet Key Exchange) policy determines how IKE will authenticate peers, negotiate IPSec SAs (Security Associations) and which kind of IPSec keys will be utilized. IKE eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers. IKE also specifies a lifetime for the IPSec security association, allows encryption keys to change during IPSec sessions without having to break the session and provides anti-replay services.[24] There are a myriad of options to choose from. Choices must be made for an encryption algorithm, a hash algorithm and an authentication provider. Here is a list of the choices supported by the Cisco 3030 VPN Concentrator:

Encryption Algorithm: The packets need to be encrypted to ensure confidentiality. The choices for encrypting are DES and 3DES:

DES: The Data Encryption Standard (DES) published in 1977. DES applies a 56-bit key to every 64-bit block of data.

3DES: A variant on DES uses three DES keys in succession to provide a 168-bit key. It is stronger encryption than DES, but it is processor intensive.

A tip regarding encryption: All the IKEs in place use at least the 56-bit DES (Data Encryption Standard) as their method of encryption most use 168-bit 3DES, which while slower provides even stronger encryption. The encryption ensures an outsider does not easily read traffic sent to and delivered from GIAC. Since DES can in fact be broken in a realistic amount of time using today's computers only 3DES IKE candidates should be selected.[25]

---

24. Cisco Documentation, "Configuring Internet Key Exchange Security Protocol." Cisco Systems. 20 November 2001. URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt4/scike.htm (20 January 2003).

25. SearchSecurity Definition, "Data Encryption Standard - a searchSecurity definition - see also: DES." TechTarget. 19 January 2001. URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213893,00.html (20 January 2003).

Hash Algorithm: The packets need to be checked to ensure they have not been altered in route. A one-way hash algorithm, where the data being sent is run against the algorithm to produce a message that cannot easily be forged, is used to provide integrity assurance. The choices for hash algorithms are MD5 and SHA-1.

MD5: According to searchsecurity.com, "MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input."[26] Since the data itself is put through the algorithm to create the digest, MD5 involves no keys.

SHA-1 (Secure Hash Algorithm) likewise involves no keys but produces a 160-bit message digest. Hence SHA-1 is slower than MD5, but more secure against attacks.[27] Authentication Method: The hosts have to know who each other are. To this end a digital signature of some kind is required. There are three options:

RSA signature: RSA key pairs can be utilized when encrypting and signing IKE key management messages. The hosts obtain digital certificates from a Certification Authority (CA) when this is used as the authentication method.

RSA encrypted non-ces: RSA encrypted non-ces uses no third party certificate authority. You enter the other host's RSA public key. It allows for a compromise between relying on a third party for network authentication and the relatively unsafe method of using a pre-shared key.

Preshared Key: Involves sharing individual secrets to authenticate encrypted tunnels. A preshared key must be configured on each participating host. If one of the hosts is does not possess the same preshared key, the SA cannot be established.

Diffie-Hellman: Also called exponential key agreement, it is a method of exchanging a shared secret key securely over a public network. To this end you must use one of the Diffie-Hellmann (DH) groups. IKE uses Diffie-Hellman to establish session keys. The concentrator supports (DH) groups 1 (768-bit), 2 (1024-bit), 5 (2048-bit)[28]. The more bits a group uses the longer it takes to process.

---

26. SearchSecurity Definition, "MD5 - a searchSecurity definition." TechTarget. 4 April 2002. URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci527453,00.html (20 January 2003).

27. NIST, "FIPS 180-1 - Secure Hash Standard." NIST. 17 April 1995. URL: http://www.itl.nist.gov/fipspubs/fip180-1.htm (20 January 2003).

28. Cisco Systems, "CiscoWorks Management Center for VPN Routers Defining IKE Policies – Cisco Systems." Cisco Systems. 17 January 2003. URL: http://www.cisco.com/en/US/products/sw/cscowork/ps3994/products_user_guide_chapter09186a00800e45ce.html#1048412 (20 January 2003).

Finally the SA's lifetime parameter has to be configured. The SA has a limited lifetime because given enough time and enough data any key is hackable. Before the security association's lifetime is expired, a new security association is set up. When the security association expires, the traffic must be forwarded on the new security association.

The IKE Policy for GIAC is as follows:

Parameter	Accepted Values	Keyword
Encryption Algorithm	3DES	3des
Hash Algorithm	MD5	md5
Authentication Method	RSA non-ces	rsa-encr
Diffie-Hellman	2 (1024-bit)	2
SA Lifetime	3600 (1 hour)	3600

TripleDES was selected because the encryption it provides is stronger than the encryption provided by DES and the TripleDES encryption on the concentrator is hardware based. MD5 was chosen because it is faster than SHA-1.

RSA non-ces was chosen to provide a more secure means of authentication than shared keys while at the same time maintaining independence from a third party certificate authority. DH Group 2 was chosen because while it is processor intensive it is also concealing the session keys that are vital to maintaining the VPN. Setting the SA Lifetime to 1 hour (3600 seconds) keeps the SA changing frequently while allowing sessions to not be overwhelmed by fresh key exchanges.

2.3.2 IPSec Policy

GIAC will support ESP-3DES-MD5 as its SA. Since peer-to-peer VPNs are not being established with any other providers SA compatibility is not a concern. The SA will be configured as follows.

The IP Address range 10.0.3.0/24 has been reserved for VPN connections. Giving VPN users their own range of addresses rather than using the internal DHCP server will assist in isolating VPN traffic on the internal network. This allows administrators an easy means of discerning which traffic is from the VPN and which is from the office.

Since employees, especially the sales force, could be literally anywhere, the VPN will accept IPSec traffic from anywhere. The only requirement being the traffic passes through the perimeter firewall first. The Cisco VPN 3030 Concentrator will authenticate remote users using SecurID. A RSA ACE/Server is located on the internal network. Each user will be assigned a SecurID Token.

All employee accounts on the VPN will be in the RemoteUser group. Each employee will be assigned a unique account within this group. To ensure the non-triviality of cracking passwords the minimum password length is set to 8 characters and alphabetic-only passwords are not allowed. To ensure that sessions are not left open while unattended the idle timeout is set for 10 minutes and the maximum connection time is set to 8 hours. Split tunnel is denied to all VPN users.

Perfect Forward Secrecy provides extra protection by ensuring that each key is derived from a shared secret value. As the keys change, this value changes. So if a key is compromised, data encrypted by neighboring keys remain safe. PFS is enabled on all GIAC connections and DH Group 2 will be utilized (1024-bit).

2.4 Tutorial configuring the VPN Concentrator

This tutorial will concentrate solely on configuring the Cisco 3030 VPN Concentrator to accept client-to-lan connections per GIACs stated VPN Policy.

Here is an overview of the IKE-IPSec process by Rhys Haden.[29]

1. Peer P detects that traffic wishes to use an IPsec tunnel to peer Q.
2. Peer P initiates an IKE SA with peer Q.
3. A transform set is issued by peer P for the IKE SA
4. A transform set is issued by peer Q for the IKE SA
5. On agreement of the transform set, peer P sends their digital certificate across the IKE SA
6. Peer Q sends their digital certificate across the same bi-directional IKE SA.
7. Peer P and Peer Q then exchange Diffie-Hellman numbers that are digitally signed so that they can establish a shared key that they can be confident genuinely comes from the other peer.
8. Peers P and Q verify each other's signature using each other's public key.
9. The shared key is calculated using the Diffie-Hellman numbers.
10. The IKE SA is now established
11. Peer P sends a transform set on the IKE SA.
12. Peer Q sends a transform set on the IKE SA and peers P and Q decide the lowest common set.
13. Peer P now initiates a uni-directional IPsec SA for data transfer
14. If Peer Q needs to send data then peer Q initiates its own uni-directional IPsec SA.
15. The Diffie-Hellman key exchange is used again for P and Q to negotiate a shared key, because IKE is being used, the shared key derived at this stage is totally independent of the IKE shared key.
16. Data is now sent over the IPsec SAs.
17. As the IPsec SAs near expiration as defined by their timers, IKE creates new IPsec SAs and data transfer continues seamlessly.

2.4.1 VPN Concentrator Configuration

To complete this configuration the GIAC test laptop, a console cable and a crossover cable are required. Verify that the test laptop is set to the IP address XXX.234.209.177 with a subnet mask of 255.255.255.252. This will be important when it comes time to access the VPN Concentrator through the VPN Concentrator Manager.

29. Haden, Rhys, "IPSec", 2002. URL: http://www.rhyshaden.com/ipsec.htm (20 January 2003)

Before beginning it is essential that the concentrator is not hooked up to the production network until ready to be placed into operation. The concentrator should be hooked up via its console port to the laptop's COM 1 port. A crossover cable will be required later in the tutorial.

Once all the cables are hooked up power up the laptop and the concentrator. A terminal emulation program must be run from the laptop in order to access the console port. For this exercise HyperTerminal will be used.

Click the start button and then click on run.
Type the phrase hypertrm in the run box and click OK
HyperTerminal will appear. A window labeled Connection Description will appear, in the name field of the window type in VPN3030 Console. This should look something like this:

Click OK. A window labeled Connect To will appear. Select “Direct to Com1” in the Connect Using dropdown then Click OK. The COM1 Properties Window will appear. Select the following settings:
Bits Per Second: 9600
Parity: None
Data Bits: 8
Stop Bits: 1
Flow Control: None
When properly configured it should look like this:

Click OK. Hit Enter a couple of times. You should now see a prompt:[30]

```
Login:
```

Type in the default username and password, which are both admin and then hit enter. You should then see the following:

```
Welcome to
Cisco Systems
VPN 3000 Concentrator Series
Command Line Interface
Copyright (C) 1998-2001 Cisco Systems, Inc.

-- : Set the time on your device. ...

> Time
```

30. Cisco Systems, “Cisco VPN 3000 Series Concentrators Installing and Powering Up the VPN Concentrator.” URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_getting_started_guide_chapter09186a00800bf698.html#1050259 (20 January 2003)

```
Quick -> [ 17:26:14 ] _
```

Type the correct time in 24-hour format and then hit enter. The next screen should ask you to enter the correct date in MM/DD/YYYY format:

```
-- : Enter the date ...

> Date

Quick -> [ 03/26/2001 ] _
```

Once the correct date has been input hit enter again. The time zone needs to be set. In the case of GIAC the time zone should be set to –5. Enter –5 and then hit enter.

```
-- : Set the time zone on your device. ...

-- : Enter the time zone using the hour offset from GMT: ...

> Time Zone

Quick -> [ 0 ] _
```

Daylight Savings Time Support should be disabled so input 2 and hit enter.

```
1) Enable Daylight Savings Time Support
2) Disable Daylight Savings Time Support

Quick -> [ 2 ] _
```

The next screen that will appear will ask for the IP address for interface 1. Interfaces on the VPN are numbered starting from 1 (as opposed to 0).

```
This table shows current IP addresses.

    Interface            IP Address/Subnet Mask    MAC Address
-------------------------------------------------------------
| Ethernet 1 - Private  |    0.0.0.0/0.0.0.0     |
| Ethernet 2 - Public   |    0.0.0.0/0.0.0.0     |
| Ethernet 3 - External |    0.0.0.0/0.0.0.0     |
-------------------------------------------------------------

** An address is required for the private interface. **

> Enter IP Address

Quick Ethernet 1 -> [ 0.0.0.0 ] _
```

Type in the following IP Address for Ethernet 1, the private interface, XXX.234.209.178 then hit enter. The concentrator will prompt for the subnet mask. Input 255.255.255.252 and then hit enter again.

```
> Enter Subnet Mask
```

```
Quick Ethernet 1 -> [ 255.0.0.0 ] _
```

The concentrator will prompt for the line speed. Select 2 and hit enter.

```
1) Ethernet Speed 10 Mbps
2) Ethernet Speed 100 Mbps
3) Ethernet Speed 10/100 Mbps Auto Detect

Quick -> [ 2 ] _
```

Select full duplex on the next screen by typing 2 and hitting enter.

```
1) Enter Duplex - Half/Full/Auto
2) Enter Duplex - Full Duplex
3) Enter Duplex - Half Duplex

Quick -> [ 2 ] _
```

The next screen should look like this:

```
1) Modify Ethernet 1 IP Address (Private)
2) Modify Ethernet 2 IP Address (Public)
3) Modify Ethernet 3 IP Address (External)
4) Configure Expansion Cards
5) Save changes to Config file
6) Continue
7) Exit

Quick -> _
```

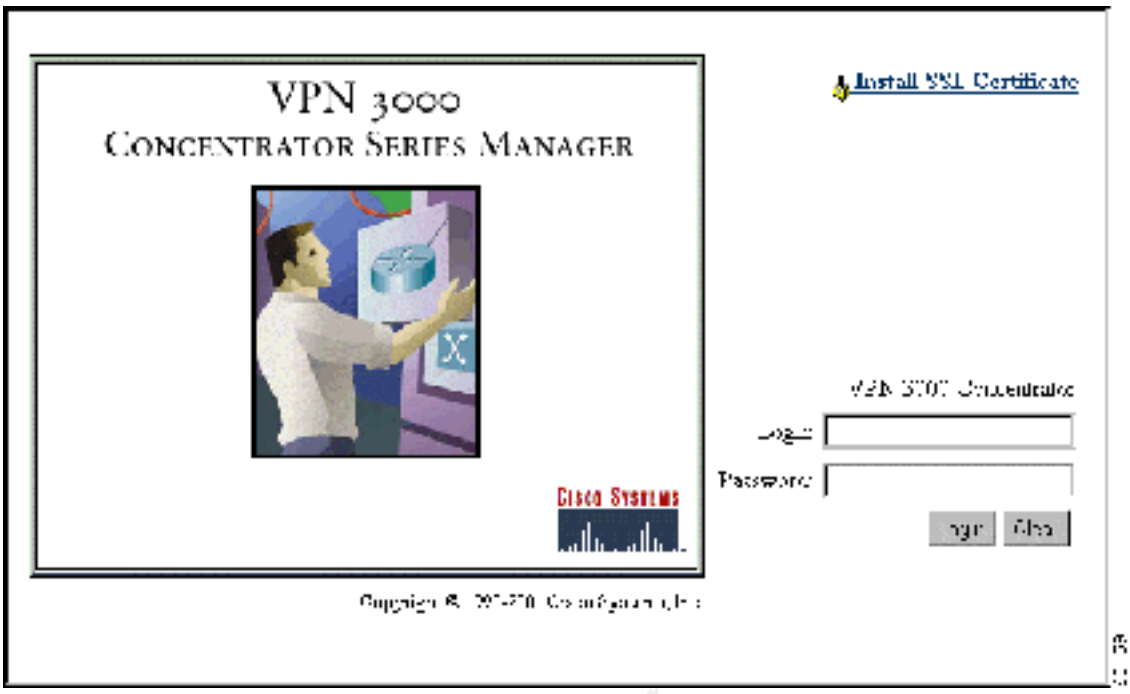
Type 5 and hit enter to save changes. Then type 7 to exit. Now place the crossover cable into the private interface and hook it into the laptop.

Once the basic connectivity to the VPN has been configured, accessing the following website will launch the VPN 3000 Concentrator Series Manager:

```
http://XXX.234.209.178/access.html
```

The screen that appears should look like this[31]:

31. Cisco Documentation, "Using the VPN Concentrator Manager for Quick Configuration." Cisco Systems. 26 September 2002. URL: http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/3_6/getting/gs3mgr.htm (20 January 2003).



Type the default login and password into the appropriate boxes. Both of them are admin. All the letters are lower case. Click the login button.

Select the hyperlink labeled “Click Here to Start Quick Configuration.” This should bring up the screen that has the interfaces listed in a table that should at this moment look like this.

Interface	Status	IP Address	Subnet Mask
Ethernet 1 (Private)	UP	XXX.234.209.178	255.255.255.252
Ethernet 2 (Public)	Not Configured	Not Configured	Not Configured
Ethernet 3 (External)	Not Configured	Not Configured	Not Configured

Click the Ethernet 2 interface. The “Configuration | Quick | IP Interfaces | Ethernet 2” Screen should appear. Click the “Static IP” radio button. Fill in the following parameters to configure Ethernet 2:

IP Address: XXX.234.209.173
Subnet Mask: 255.255.255.252
Filter: None
Speed: 100

Duplex: Full

Make certain that the Public Interface checkbox is checked. Ethernet Interface 2 will be the interface facing the Internet.

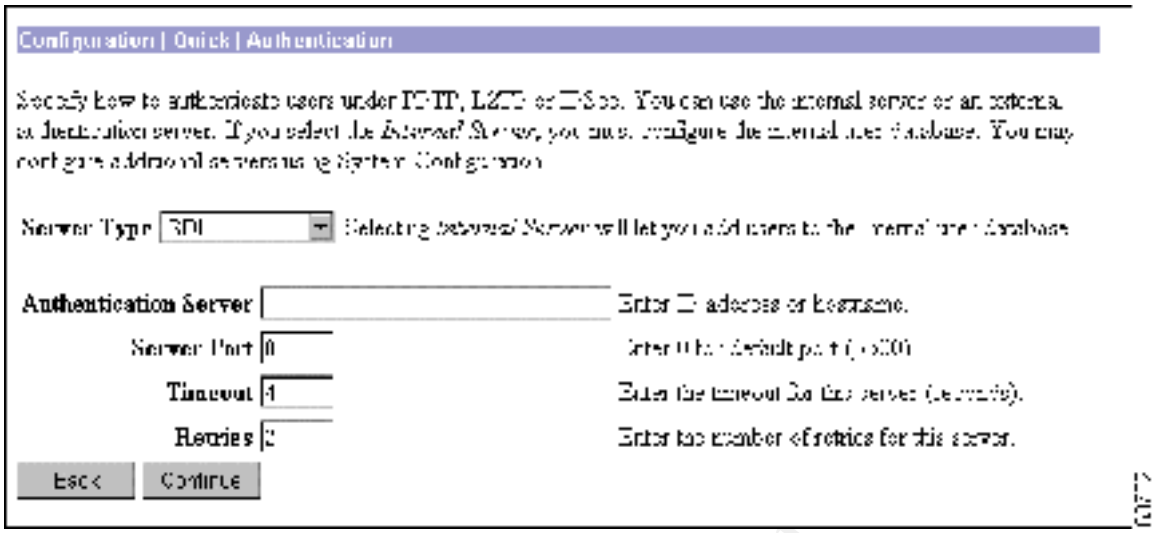
Click Apply, the Interfaces menu of the "Configuration | Quick | IP Interfaces" screen should now look like this:

Interface	Status	IP Address	Subnet Mask
Ethernet 1 (Private)	UP	XXX.234.209.178	255.255.255.252
Ethernet 2 (Public)	UP	XXX.234.209.173	255.255.255.252
Ethernet 3 (External)	Not Configured	Not Configured	Not Configured

Click continue. The next screen that appears will be the "Configuration | Quick | System Info Screen." On this screen the following parameters need to be loaded.

DNS Server: XXX.234.209.166
Domain: giac.com
Default Gateway: XXX.234.209.174

Click continue. The Configuration | Quick | Protocols" screen will appear. On this screen only leave IPSec checked then click continue. The next screen will be the "Configuration | Quick | Address Assignment" screen. On this screen the Configured Pool checkbox should be selected. In the Range Start field, type in the IP Address 10.0.3.1, and in the Range End field, 10.0.3.254 should be input. Click Continue.



The “Configuration | Quick | Authentication” Screen will appear next. Internal Server is the authentication set by default. Click the drop down and select SDI. GIAC’s ACE/Server IP address is 10.0.2.7. Set the port number to 5500. Click Continue.

The next screen is “Configuration | Quick | IPSec Group”. This screen sets the IPSec Group. The Group Name is RemoteUser. The password should again conform to the password policy and again has to be verified. Click continue.

“Configuration | Quick | Admin Password” allows for the password to be reset. This should be done at this point. The password should be 16 characters and consist of no dictionary crackable words. Verify the password then click continue.

The final screen in quick configuration is “Configuration | Quick | Done”. Click “Save Needed” icon at the upper right corner of the window to save the active configuration. A web browser window should appear with the words “Save Successful”. Click OK in that window to dismiss it and then click the hyperlinked labeled “Configuration” on the “Configuration | Quick | Done” screen.

To bring the concentrator in line with policy some other settings need to be set that cannot be set in Quick Configuration. The IKE proposal, how the remote host and the VPN share private information over public channels, is the first item to be configured.

Under Configuration select System, Tunneling Protocols, IPSec, and then IKE Proposals. The Configuration | System | Tunneling Protocols | IPSec | IKE Proposals screen should appear. It looks like this:

This screen supports the activation and priority setting of multiple IKE proposals. These proposals establish how users will exchange certificates to authenticate both origin and identity information before establishing a VPN.

In GIAC's case only remote access clients are supported. All Active Proposals must be removed except CiscoVPNClient-3DES-MD5-RSA by highlighting each client in the Active Proposals list and then clicking deactivate until CiscoVPNClient-3DES-MD5-RSA is left active.

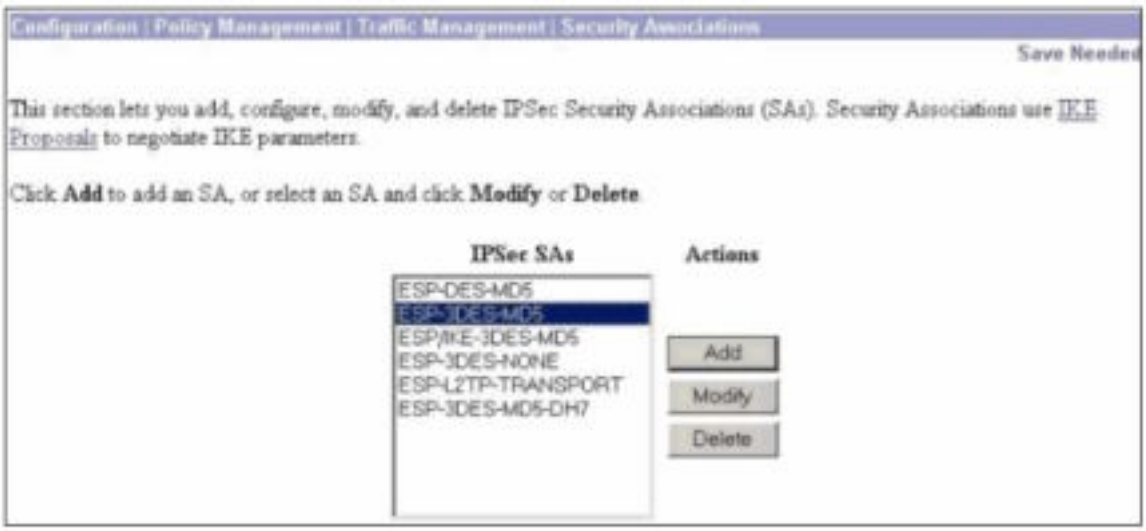
In GIAC's case MD5 is selected to favor speed over having too much security.

RSA is selected over generic XAUTH authentication to allow a means of fingerprinting what computer the user is using when utilizing the VPN. RSA uses public and private keys from the RSA Algorithm to generate the certificate hence the key is not based on the username and password, which is how the key is generated in the default IKE proposal CiscoVPNClient-3DES-MD5. So RSA is used to authenticate both the user and the origin. The RSA public key for the VPN is pre-loaded onto each user's VPN Client software on their laptop when integrated allowing the user to merely need their username and password to access the VPN.

GIAC uses CiscoVPNClient-3DES-MD5-RSA as it's only IKE proposal. This limits the vectors of attack on IKE proposals, but the weakness is that there is no fallback proposal. CiscoVPNClient-3DES-MD5-RSA provides the RSA Digital Certificate, User/Password as its Authentication mode, MD5/HMAC-128 as its

Authentication Algorithm, 3DES-168 as its Encryption Algorithm and Diffie-Hellman group 5 (2048-bits) for session establishment.

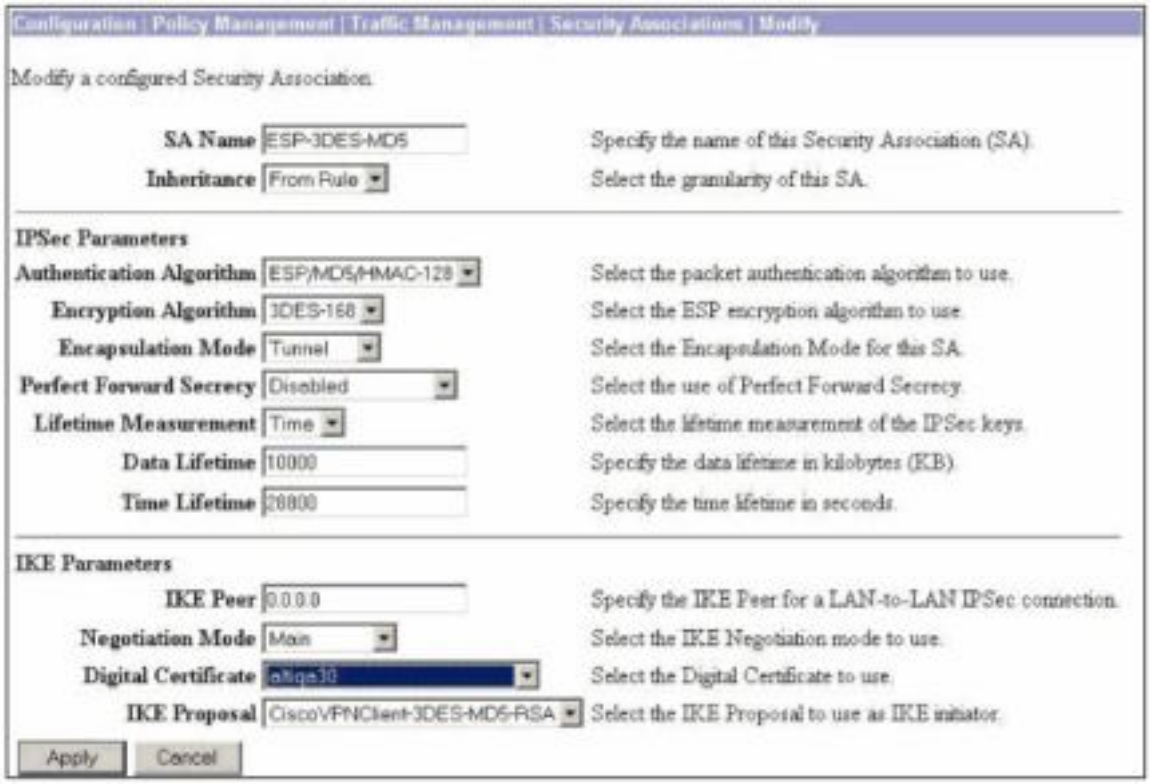
Each user will have their own individual account with which to access the VPN all set up in the same IPSec group with the settings above. Doing this places accountability upon the individual when accessing the internal network over the VPN. Also if an employee leaves the company without returning the laptop revoking the ex-employee's account will prevent the ex-employee from accessing the VPN.



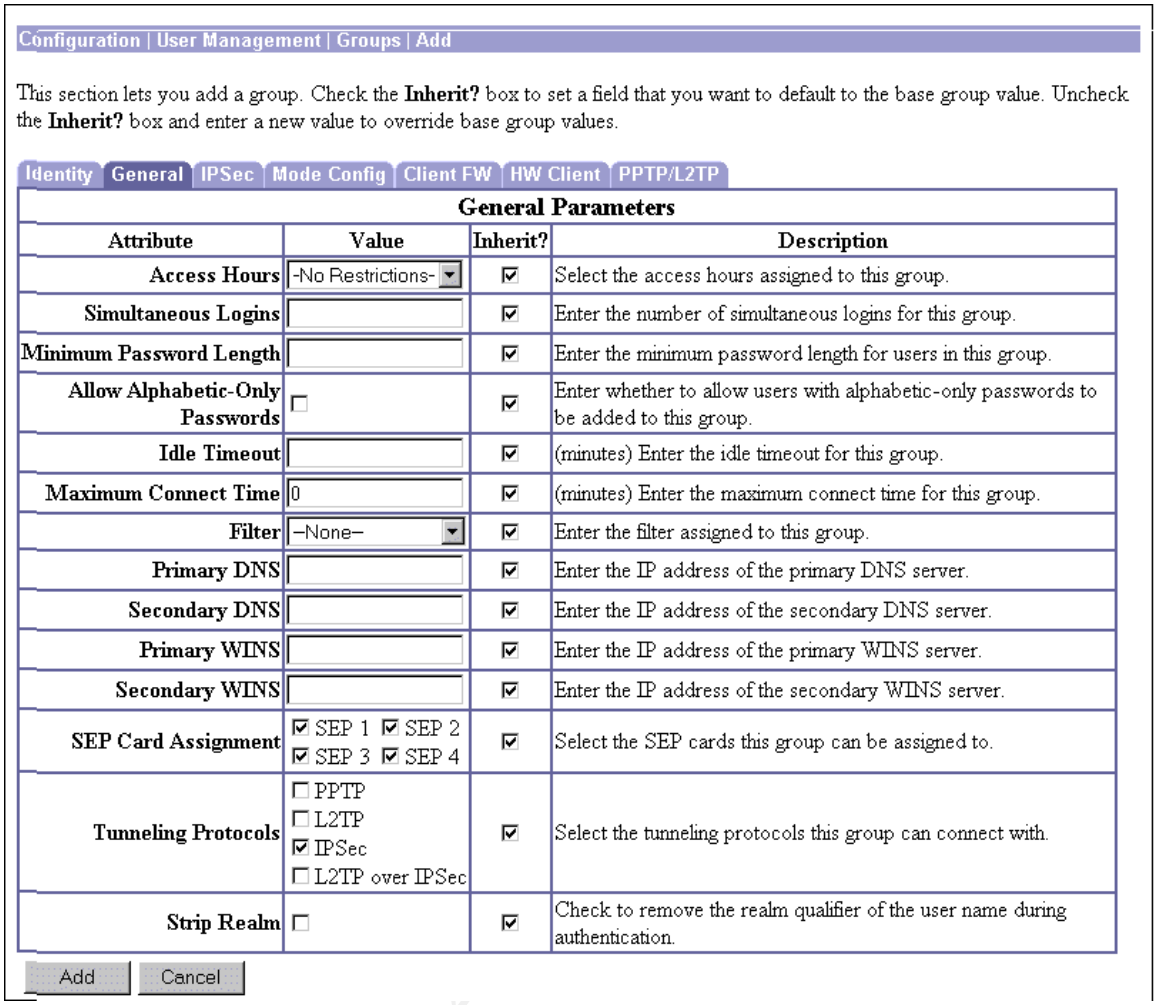
The IPSec Security Associations must next be set. The window can be found under Configuration | Policy Management | Traffic Management | Security Associations. Security Associations are a connection between IPSec peers that determine the services available between the peers.[32] ESP-DES-MD5 should be the only proposal set.

Once the other IPSec SA's have been deleted, highlight ESP-3DES-MD5 and click Modify. The Configuration | Policy Management | Traffic Management | Security Associations | Modify screen should appear.

32. Chapman and Fox p.198



This screen has a number of parameters that can be changed. Perfect Forward Secrecy should be set to Group 2 (1024-bits). The Time Lifetime should be modified to 3600 to conform to the policy. Everything else should be left on the default setting. Then click apply. Next navigate to the Configuration | User Management | Groups. Verify that the group name is RemoteUser is highlighted then click the Modify Group button.



Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPSec | Mode Config | Client FW | HW Client | PPTP/L2TP

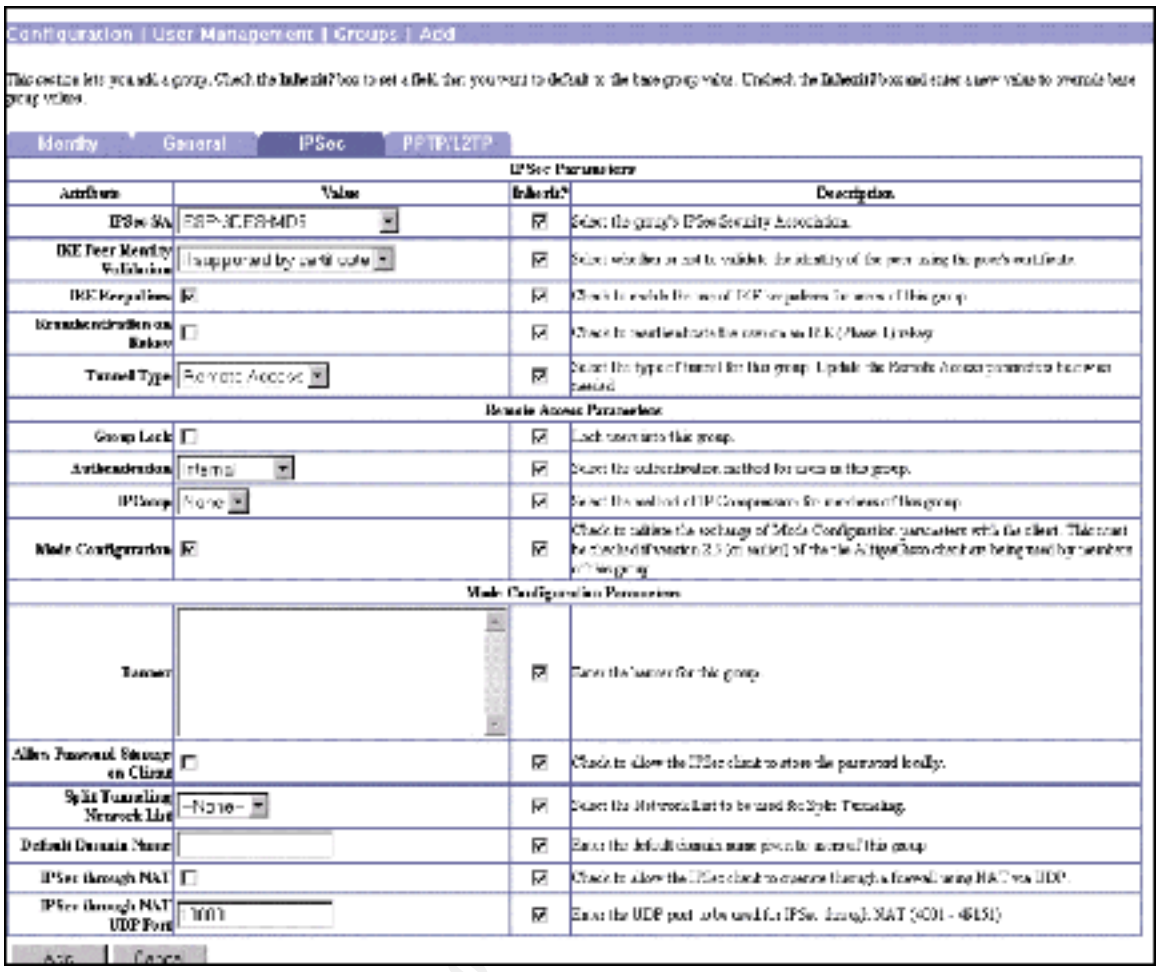
General Parameters

Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	☑	Select the access hours assigned to this group.
Simultaneous Logins		☑	Enter the number of simultaneous logins for this group.
Minimum Password Length		☑	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	☐	☑	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout		☑	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	☑	(minutes) Enter the maximum connect time for this group.
Filter	-None-	☑	Enter the filter assigned to this group.
Primary DNS		☑	Enter the IP address of the primary DNS server.
Secondary DNS		☑	Enter the IP address of the secondary DNS server.
Primary WINS		☑	Enter the IP address of the primary WINS server.
Secondary WINS		☑	Enter the IP address of the secondary WINS server.
SEP Card Assignment	☑ SEP 1 ☑ SEP 2 ☑ SEP 3 ☑ SEP 4	☑	Select the SEP cards this group can be assigned to.
Tunneling Protocols	☐ PPTP ☐ L2TP ☑ IPSec ☐ L2TP over IPSec	☑	Select the tunneling protocols this group can connect with.
Strip Realm	☐	☑	Check to remove the realm qualifier of the user name during authentication.

Add | Cancel

On this screen[33] select the “Simultaneous Logins” and raise it to 25 (for snow days). Unchecking “Allow Alphabetic-Only Passwords” enforces the password policy. The password policy is eight or more characters that has at least numbers and letters and is not dictionary crackable. Reduce the “Idle Timeout” to 10 minutes and change the “Maximum Connect Time” to 480 minutes. Next select the IPSec Tab.

33. Cisco Systems, “User Management.” 2 May 2001. URL: http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/vpn3kco/vcoug/usr_3_0/usermgt.htm#xtocid28958 (20 January 2003)



The IPSec screen needs to have the following parameters verified: Verify that the IPSEC SA selected is ESP-3DES-MD5, the Tunnel Type is set to "Remote Access" and the authentication is set to SDI (not Internal). Set the Default Domain Name to giac.com. Click Add.

Next navigate to the Identity tab. For each GIAC user the following information must be entered:

- ✓ User Name (first letter of first name and the entire last name)
- ✓ A default password that conforms to the password policy
- ✓ Verification of that password

Then click the Add button. Continue doing this until all employees have been entered. Next navigate to Configuration | System | Servers | Authentication. The replica RSA ACE/Server needs to be added to this list. Click the Add Button, type in 10.0.2.8 for the server IP address.

The concentrator should now be configured to accept traffic. The next step is to secure it so it can be placed on the production network.

Assignment 3 – Verify the Firewall Policy

3.0 Introduction

In order to manage risk and as part of the overall security policy at GIAC a firewall audit will be performed once every six months. Some portions of the audit will be checked on a quarterly basis. The results of each audit will be compared to the initial audit, which will be performed as soon as possible by outsourced consultants. Outside consultants were selected because of their impartiality and specialization in performing audits.

3.1 Plan the audit.

3.1.1 Ground Rules

The consultants and GIAC management have agreed upon the following ground rules for the audit in writing:[34]

- ✓ This exercise is focused on the primary firewall (PIX).
- ✓ Although this exercise is focused on the primary firewall attempts are obviously being made to access hosts behind it. Hence, no hosts are restricted from being scanned by this exercise. Attacks on the hosts themselves are not to be mounted.
- ✓ Acceptable testing techniques are restricted to attacks against the firewall itself (i.e. no social engineering). No attacks are to occur outside of the prescribed times of the audit.
- ✓ tcpdump will be run on hosts within the DMZ and internal networks (both customer service and office) during work hours for two days before the audit. This will then be reviewed to assess if any office traffic is in violation of the firewall or the security policy.
- ✓ The audit is to be performed between 8pm Saturday and 4am Sunday to ensure that the impact upon the Enterprise by the audit is minimized. Backups and other network-intensive activity will have been performed before the audit commences. This way if anything is broken by the audit it can be quickly restored to operation.
- ✓ The consultants will denote the addresses from which they will launch their attacks beforehand to GIAC. Administrators will be instructed to ignore attacks from those ranges within the prescribed audit period.

34. Tracey, Miles and Wack, John, DRAFT Special Publication 800-42, Guideline on Network Security Testing. Washington: USGPO, 2001. p. 16

- ✓ GIAC and Audit technical staff have exchanged contact information.

- ✓ Since auditing the firewall looks exactly like an attack upon the firewall, all GIAC management and technical staff have been informed when the audit will be performed and the implications of such an audit. If GIAC technical staff are not informed in advance then law-enforcement agencies could be called in on a false alarm sent by a well meaning but ignorant employee (in violation of the security policy).

- ✓ The GIAC CIO will present the results of the audit to GIAC management. The information will then be kept off network in a tape backup cartridge in a locked office. The consulting group will not retain a copy of the results of the audit.

- ✓ Each scan performed on the GIAC network is logged and attached to the audit. Scan files are to conform to the following nomenclature: a timestamp followed by the location of the laptop building the log. e=external, i=internal, d=dmz, v=vpn, 2=direction, example: 200301150111_e2i_fw_01.log would be the first log at 1:11am on the 15th of January 2003 going from the external network to the internal network through the firewall. All time codes are UTC.

3.1.2 Technical Approach

Before the audit the consultants will verify that the firewall is in a physically secure location, check firewall change control processes, and firewall backup and recovery procedures. The consultants will also check the current firewall configurations including account levels, password policies, and services running on the firewall.

According to Shake Communications, the firewall audit itself will consist of the following reviews:[35]

- Software and hardware versions
- Rulebase:
  - Traffic to internal and external networks
  - Internal and external services passing through your firewall
- Software configuration, including:
  - Known hosts
  - IP addresses
  - Implied rules
  - NAT
  - Proxy configurations
  - Content filtering

35. Shake Communications, "Firewall Auditing." URL: http://www.shake.net/firewall.cfm (20 January 2003)

    - Firewall management
    - Remote connections (i.e. dialup/VPN clients)
- Operating System – including file permissions, applications, user accounts, security patches and hotfixes
- Log files
- Verification that the firewall configuration meets your Gateway and Information Security Policies
- Verification that access control policies perform properly limiting who can effect and test changes on the firewall and when.

3.1.3 Estimate costs and level of effort.

The consulting group has outlined three positions required to conduct the audit:

Senior Auditor: The Senior Auditor will coordinate all activities and provide the final inspection of all aspects of the audit. He will ensure compliance with the ground rules of the audit and verify proper handling of the results of the audit. He will solely perform the pre-checks before the audit, perform post-audit analysis, issue recommendations and generate the final report.

Junior Auditors: Junior Auditors will perform the actual tests and document whether the tests have passed or failed.

1 Senior Consultant	$250/hr * 40 hours = $10000
2 Junior Consultants	$150/hr * 20 hours = $3000

The cost for labor to conduct the audit will be $11,000.00[36]. GIAC or the consulting firm will already own the equipment used.

GIAC technical staff will be working on the audit preparations and the audit itself. They will be providing access to systems, monitoring the audit, assisting in the audit, and answering questions the consultants have regarding procedures.

Senior Network Engineer	$50/hr * 20 hours = $1000
System Administrator	$40/hr * 20 hours = $800

The labor costs for GIAC staff for the audit will be $1800 dollars[37].

3.1.4 Identify risks and considerations and how they are addressed.

There are several risks in conducting an audit on the firewall:

36. SBC, "Internet-Pacific Bell Dedicated Rider C Final." URL: https://ebiznet.sbc.com/calnetinfo/RiderC/Other_Svcs/10_C_Hourly_Consulting.htm (13 February 2003).

37. washingtonpost.com, "washingtonpost.com: Jobs." URL: http://www.washingtonpost.com/ac2/wp-dyn/jobs/salarysurvey (13 Feburary 2003).

1. Sensitive information will be gathered throughout the audit. This will include at least the network architecture. It may also include proprietary intellectual property and confidential customer records.

   To mitigate this risk audit staff will be required to sign Non-Disclosure Agreements. GIAC staff should be present on both sides of any network test to verify that any data gathered is solely for use in the audit.

2. Denial of Service to critical business functions will occur during the audit. This may prevent business from being conducted. Worse yet, it is in the realm of possibility that GIAC's ISP may misinterpret tests from outside the GIAC network as an attack. The ISP may contact law enforcement or engage defenses, which would defeat the test.

   Partners, Suppliers, Employees and Customers are notified that a regular maintenance may impact availability to the GIAC network between the hours of 8pm Saturday and 4am on Sunday. The same notification will be on the website for customers and by e-mail to suppliers and partners. No other information is disseminated to people outside the company regarding the audit. This should mitigate the risk of any essential function by any other interested party being performed during the hours of the audit.

   Administrators have been notified to verify their backups and be on-call during the audit to circumvent any outages and resolve any problems that may occur because of the audit. GIAC's ISP has been notified of the audit so they do not inadvertently mistake the audit for an attack

3. A hacker could attack GIAC during the audit. Depending upon the attack this could be very difficult to discern from the audit.

   If an unexpected attack is detected during the audit then auditing will cease and be resumed at a later date. This will allow GIAC staff to focus their efforts upon the security incident.

3.2 Primary Firewall Audit

The goal of the primary firewall audit is to verify that the firewall is indeed executing the policy defined. To this end the auditors will scan the network from both the inside and outside to verify that the rulebase is indeed allowing the services prescribed to pass through the firewall.

3.2.1 Tools

As mentioned above in the ground rules, nmap will be the tool primarily used to conduct the audit. nmap is a port scanner that crafts IP packets utilizing them to determine host availability, services offered, operating system, and firewall in

use.[38] tcpdump, a packet sniffer, will be used to monitor nmap and verify that the firewall is treating traffic in accord with the firewall policy. Telnet will be used to test connectivity to the applications residing on hosts as needed.

3.2.2 Software and Hardware Versions

Attempts to establish telnet connections to the PIX from both the external and the internal network failed. In order to verify the software and hardware versions of the Firewall the following command is issued from within the data center at the console port of the firewall.

```
GIAC_pix_1# show ver
```

This yielded the following results:

```
Cisco PIX Firewall Version 6.2(1)
Cisco PIX Device Manager Version 2.0(1)
Compiled on Wed 27-Dec-02 21:18 by morlee
pix515E up 2 days 20 hours 10 mins 32 secs
Hardware: PIX-515E, 64 MB RAM, CPU Pentium 433 MHz
Flash i28F640J5 @ 0x300
BIOS Flash AT29C257 @ 0xfffd8000
0: ethernet0: address is 00aa.xxxx.0032, irq 11
1: ethernet1: address is 00aa.xxxx.0033, irq 10
2: ethernet2: address is 00a0.xxxx.d029, irq 9
3: ethernet3: address is 00a0.xxxx.b5f7, irq 7
Licensed Features:
Failover: Disabled
VPN-DES: Enabled
VPN-3DES: Enabled
Maximum Interfaces: 6
Serial Number: 123 (0x7b)
Activation Key: 0xc5233151 0xb429f6d0 0xda93739a 0xe15cdf51
```

The software found on the PIX is up to date in conformance with the security policy. The hardware conforms to the description in the documentation provided by GIAC.

3.2.3 Reconnaissance Scans

Ping Sweep

Using a ping sweep, nmap can discover hosts on the GIAC network without port scanning. The following command is issued from the auditor's network somewhere on the Internet:[39]

```
nmap -sP –PI –p 1-65535 -O -v -T 2 XXX.234.209.160/27
```

38. Nmap, "Nmap -- Free Stealth Port Scanner For Network Exploration & Security Audits." 10 August 2002.URL:http://www.insecure.org/nmap/ (20 January 2003).

39. Fyodor, "Nmap network security scanner man page." 2001. URL:http://www.insecure.org/nmap/data/nmap_manpage.html (20 January 2003)

-sP means perform a ping sweep without actually performing any port scanning. –PI means to specifically use only ICMP (not ACK). –O means attempt to identify the host OS. –v means to be verbose.

–T 2 is actually polite timing behavior. It is used so as to minimize the chances of choking up network resources. nmap can be set to sweep faster or slower than this. Since the perimeter router is blocking certain ICMP responses only one host is shown to be up. The ICMP ping sweep performed as expected.

SYN Stealth

The next command –sS tells nmap to use TCP SYN if a SYN/ACK is returned then the service is up. If an RST is returned then the service is down. This is used to detect services running on hosts within the domain. –PT is issued to perform a sweep using TCP ACK + ping sweep. –p tells nmap what port numbers to test.

```
nmap -sS -PT –p 1-65535 -v -T 3 XXX.234.209.160/27
```

The output follows:

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on  (XXX.234.209.173):
(The 65534 ports scanned but not shown below are in state: closed)
Port       State       Service
50/tcp     filtered    Remote Mail Checking Protocol
[500]
Remote OS guesses: Cisco VPN 3000 or 3COM 4924 GigE Switch

Interesting ports on  (XXX.234.209.164):
(The 65533 ports scanned but not shown below are in state: closed)
Port       State       Service
80/tcp     filtered    World Wide Web HTTP
443/tcp      filtered    secure http (SSL)
Remote OS guesses: Linux Kernel 2.4.3 SMP (RedHat)

Interesting ports on  (XXX.234.209.165):
(The 65533 ports scanned but not shown below are in state: closed)
Port       State       Service
80/tcp     filtered    World Wide Web HTTP
443/tcp    filtered    secure http (SSL)
Remote OS guesses: Linux Kernel 2.4.3 SMP (RedHat)
Nmap run completed -- 256 IP address (4 hosts up) scanned in 137
seconds

Interesting ports on  (XXX.234.209.166):
(The 65534 ports scanned but not shown below are in state: closed)
Port       State       Service
25/tcp     filtered    Simple Mail Transfer
Remote OS guesses: Linux Kernel 2.4.3 SMP (RedHat)
```

This scan conforms to the GIAC security policy in that only services that need to be visible to the outside world through the firewall actually are namely web, ssl,

smtp. ESP (ip/50) is visible for VPN users and this traffic does not pass through the PIX firewall.

3.2.4 Traffic from External Networks to Internal Networks

SYN Stealth Port Scans

Our first Firewall Rulebase tests involve testing for services using a SYN stealth scan without ping. The following command issued from a laptop on the Auditor's Network will perform port scans on devices residing in the DMZ.

```
nmap -sS -P0 -p 1-65535 -O -v -T 3 XXX.234.209.160/29
```

The same command is run from a laptop resident on the VPN and Internal networks. In each case the results comply with the accepted firewall policy.

Next the VPN subnet is tested in the same way. Laptops residing in the DMZ, the Internet and the Internal Network run the following command.

```
nmap -sS -P0 -p 1-65535 -O -v -T 3 XXX.234.209.172/30
```

Again the same command is run with the addresses reserved for the Internal subnet as the target. No open ports were detected from this test.

```
nmap -sS -P0 -p 1-65535 -O -v -T 3 XXX.234.209.184/29
```

Scanning outward from each of the networks will test the egress filters.

```
nmap -sS -P0 -p 1-65535 -O -v -T 3 XXX.234.209.160/27
```

Finally, the firewall itself needs to be scanned for any open ports. –p0 tells nmap to not ping at all but merely scan for open ports. –sT is for TCP, -sU is for udp.

```
nmap -sT -P0 -p 1-65535 -v -T 3 XXX.234.209.169
nmap -sU -P0 -p 1-65535 -v -T 3 XXX.234.209.169
```

From the outside the firewall itself responds to no services.

3.2.5 Traffic from Internal Networks to External Networks

Traffic flow conforming to the firewall policy from the Internal to the External Network needs to be verified. The process is much the same as above the difference being the commands are run from the trusted network.

```
nmap -sP –PI -O -v -T 2 XXX.234.209.160/27
nmap -sS -PT –p 1-65535 -v -T 3 XXX.234.209.160/27
```

The VPN does not show up on this side as having any ports open from the PIX side. Other than that this scan looks much the same as the last one.

Once again we would scan for any open ports, by pointing nmap at the external interface of the firewall this time and testing all ports on UDP and TCP.

```
nmap -sT -P0  -p 1-65535 -v -T 3 XXX.234.209.169
nmap -sU -P0  -p 1-65535 -v -T 3 XXX.234.209.169
```

The auditor has set up a test web server on their network. Scanning it from the internal network will verify that the traffic is indeed arriving at that site on the Internet from the internal network.

```
nmap -sT -P0  -p 1-65535 -v -T 3 XXX.114.201.19
nmap -sU -P0  -p 1-65535 -v -T 3 XXX.114.201.19
```

3.2.6 Internal and External Services Passing Through the Firewall

Each rule in the firewall policy must be tested to determine whether it is actually performing as expected. Each rule is validated by tcpdumps from hosts monitoring the connection on the segments in question.

tcpdumps for some of the connections are provided in Appendix A. The number in the rule column in the tables below corresponds to the number of a tcpdump in Appendix A.

Items that are verified receive a check and are working as expected. Those that fail receive an x and the failure will be noted in the comments below the table. If there is an asterisk next to the check then there are comments in the Auditor's post-analysis recommendations regarding a particular rule.

Internal_out

Unless otherwise noted, tcpdumps in this section are taken from a host inside the GIAC internal network and from a host in the destination segment.

Rule	Allow out of the internal office network HTTP/S, FTP traffic POP3, and Secondary DNS.	Verified
1	access-list internal_out permit tcp 10.0.1.0 255.255.255.0 any eq www	✔
2	access-list internal_out permit tcp 10.0.1.0 255.255.255.0 any eq 443	✔
3	access-list internal_out permit tcp 10.0.1.0 255.255.255.0 any eq ftp	✔
4	access-list internal_out permit tcp 10.0.1.0 255.255.255.0 any eq pop3	✔ *
5	access-list internal_out permit tcp 10.0.1.0 255.255.255.0 any eq domain	✔ *

The auditors contact the test server at the auditor site for web and ftp traffic. The auditors contact the pop3 and domain server in the DMZ to test the other rules. Upon further examination of the rules in this list, they also contact their own test server to test pop3 and domain.

Rule	Internal SMTP and DNS to Allow the internal SMTP gateway to speak to the external gateway	Verified
6	access-list internal_out permit tcp host 10.0.2.6 host XXX.234.209.166 eq smtp	✔
7	access-list internal_out permit ip 10.0.2.6 255.0.0.0 host XXX.234.209.166 eq domain	✔

Sending e-mail from the Internal Network tests the SMTP relay. Performing a zone transfer and querying the DMZ DNS from the Internal DNS test the DNS.

```
[avasquez@int-dns01 /]dig www.somewhere.org
; <<>> DiG 9.2.1 <<>> www.somewhere.org
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27825
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.somewhere.org.              IN      A

;; ANSWER SECTION:
www.somewhere.org.       10800   IN      CNAME   somewhere.org.
somewhere.org.           10800   IN      A       XXX.183.228.194

;; AUTHORITY SECTION:
somewhere.org.           10800   IN      NS      dns1.someisp.com.
somewhere.org.           10800   IN      NS      dns2.someisp.com.

;; ADDITIONAL SECTION:
dns1.someisp.com.     10800   IN      A       XXX.183.205.35
dns2.someisp.com.     10800   IN      A       XXX.183.192.65

;; Query time: 16 msec
;; SERVER: XXX.234.209.166#53(XXX.234.209.166)
;; WHEN: Sat Feb 15 22:26:54 2003
;; MSG SIZE  rcvd: 147
```

In both cases, the tcpdumps are collected from the customer service network and the DMZ. The e-mail arriving at the destination outside of GIAC verifies that the service is actually working.

Rule	Allow the on-site employees to edit the web pages	Verified
8	access-list internal_out permit tcp 10.0.1.0 255.255.255.0 host XXX.234.209.164 eq ssh	✔
9	access-list internal_out permit tcp 10.0.1.0 255.255.255.0 host XXX.234.209.165 eq ssh	✔

Attempting to reach either of the websites using the SSH port from the auditor's network failed:

```
telnet XXX.234.209.164
Trying XXX.234.209.164...
```

```
telnet: connect to address XXX.234.209.164: Connection timed out
```

SSH access is tested by using Telnet to connect on the SSH port to each of the sites in question.

```
telnet customer.giac.com 22
Trying XXX.234.209.164...
Connected to customer.giac.com.
SSH-2.0-OpenSSH_3.5p1
Protocol Mismatch.

telnet partner.giac.com 22
Trying XXX.234.209.165...
Connected to partner.giac.com.
SSH-2.0-OpenSSH_3.5p1
Protocol Mismatch.
```

Outside_In

Tests from the outside of the network to the inside of the network were conducted from the auditor's networks. tcpdump data gathered from these links were taken from the auditor's networks and the segment that the auditors were accessing.

Rule	Internet to Web Server and SSL	Verified
10	access-list outside_in permit tcp any host XXX.234.209.164 eq www	✔
11	access-list outside_in permit tcp any host XXX.234.209.164 eq 443	✔
12	access-list outside_in permit tcp any host XXX.234.209.165 eq www	✔
13	access-list outside_in permit tcp any host XXX.234.209.165 eq 443	✔

From the auditor's network each of the web sites is contacted using a web browser. Along with the tcpdumps this verifies that they can be accessed from outside the GIAC network using http and https.

Rule	Internet to SMTP Proxy	Verified
14	access-list outside_in permit tcp any host XXX.234.209.166 eq smtp	✔

Using telnet to open a connection from the auditor's network to the GIAC SMTP server in the DMZ yielded the following session.

```
telnet smtp.giac.com 25
Trying XXX.234.209.166...
Connected to smtp.giac.com.
Escape character is '^]'.
220-smtp.giac.com -- Server ESMTP ("SMTP-GIAC-01")
220 Unsolicted bulk mail prohibited; spammers will be prosecuted
HELO somewhere.net
250 smtp.giac.com OK, auditors-host.somewhere.net [XXX.114.201.20].
```

Rule	Internet to External DNS	Verified
15	access-list outside_in permit udp any host XXX.234.209.166 eq domain	✔

Running DiG against the DNS in the DMZ yields

```
; <<>> DiG 9.2.1 <<>> www.somewhere.org
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27825
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.somewhere.org.              IN      A

;; ANSWER SECTION:
www.somewhere.org.       10800   IN      CNAME   somewhere.org.
somewhere.org.           10800   IN      A       XXX.183.228.194

;; AUTHORITY SECTION:
somewhere.org.           10800   IN      NS      dns1.someisp.com.
somewhere.org.           10800   IN      NS      dns2.someisp.com.

;; ADDITIONAL SECTION:
dns1.someisp.com.        10800   IN      A       XXX.183.205.35
dns2.someisp.com.        10800   IN      A       XXX.183.192.65

;; Query time: 44 msec
;; SERVER: XXX.234.209.166#53(XXX.234.209.166)
;; WHEN: Sat Feb 15 22:15:38 2003
```

Rule	Perimeter Router to Syslog	Verified
16	access-list outside_in permit udp host XXX.234.209.170 host XXX.234.209.162 eq 514	✔
17	access-list outside_in permit udp XXX.234.209.170 255.255.255.252 host XXX.234.209.162 eq ntp	✔

While using Kiwi Syslog Message Generator from the auditor's network, attempts to send the syslog server log messages failed. A UDP Port Scan directed at port 514 from the auditor's network. (CMD: -sU -PT -PI -p 514 -O -T 3 XXX.234.209.162)

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
The 1 scanned port on  (XXX.234.209.162) is: closed
Remote OS guesses: Linux Kernel 2.4.0 - 2.5.20, Linux 2.4.19-pre4 on
Alpha, Linux Kernel 2.4.0 - 2.5.20 w/o tcp_timestamps, Gentoo 1.2 linux
(Kernel 2.4.19-gentoo-rc5), Linux 2.5.25 or Gentoo 1.2 Linux 2.4.19
rc1-rc7), Linux 2.4.7 (X86)
Nmap run completed -- 1 IP address (1 host up) scanned in 10 seconds
```

Temporarily turning down the 3640's .170 interface, the same test is performed using the Perimeter Router's IP address (host XXX.234.209.170). It succeeded. The message on the server looked like this:

```
Feb 15 22:49:30 XXX.234.209.170 XXX.234.209.170 SyslogGen This is a
test message generated by the 'Syslog Message Generator'
```

The same UDP port scan from this IP address yields:

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
Interesting ports on  (XXX.234.209.162):
Port       State       Service
514/udp    open        syslog
Remote OS guesses: Linux Kernel 2.4.0 - 2.5.20, Linux 2.4.19-pre4 on
Alpha, Linux Kernel 2.4.0 - 2.5.20 w/o tcp_timestamps, Gentoo 1.2 linux
(Kernel 2.4.19-gentoo-rc5), Linux 2.5.25 or Gentoo 1.2 Linux 2.4.19
rc1-rc7), Linux 2.4.7 (X86)
Nmap run completed -- 1 IP address (1 host up) scanned in 7 seconds
```

Performing the same UDP port scan for NTP (as opposed to syslog) on the host from the external network failed, and from the Perimeter Router's IP address revealed an open port on NTP. Running ntpdate from the laptop hooked using the Perimeter Router's IP address yielded the following information

```
ntpdate –b XXX.234.209.162
15 Feb 22:52:00 ntpdate[18599]: step time server XXX.234.209.162 offset
-0.001460 sec
```

Rule	Deny and Log – Outside_In	Verified
18	access-list outside_in deny ip any any log-input	✔

SYN Stealth, and UDP Port scans verify that the firewall is indeed blocking any other traffic attempting to traverse the firewall from this interface. The PIX's stateful inspection features denied FIN and ACK scans passage to hosts in the DMZ. tcpdumps on the other networks did not discover any of the the port scan packets passing through the PIX from outside networks on unexpected ports. The PIX successfully logged all denied attempts.

DMZ_In

Rule	smtp proxy to smtp internal	Verified
19	access-list dmz_in permit tcp host XXX.234.209.166 host 10.0.2.6 eq smtp	✔

Testing the connection from the SMTP server on the DMZ network using Telnet results in the following:

```
telnet 10.0.2.6 25
Trying 10.0.2.6...
Connected to smtp2.giac.com.
Escape character is '^]'.
220-smtp2.giac.com -- Server ESMTP ("SMTP-GIAC-02")
220 Unsolicted bulk mail prohibited; spammers will be prosecuted
HELO somewhere.net
250 smtp2.giac.com OK, smtp.giac.net [XXX.234.209.166].
^]
telnet> quit
Connection closed.
```

Testing the connection from other addresses on the DMZ results in the following:

```
telnet 10.0.2.6 25
Trying 10.0.2.6...
telnet: connect to address 10.0.2.6: Connection refused
```

Attempting to connect to it from the auditor's network obviously yields:

```
telnet 10.0.2.6 25
Trying 10.0.2.6...
telnet: connect to address 10.0.2.6: No route to host
```

Rule	web server to db access	Verified
20	access-list dmz_in permit tcp host XXX.234.209.165 host 10.0.2.4 eq 5432	✔
21	access-list dmz_in permit tcp host XXX.234.209.165 host 10.0.2.5 eq 5432	✔
22	access-list dmz_in permit tcp host XXX.234.209.164 host 10.0.2.5 eq 5432	✔

Running nmap from the web machines

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
Interesting ports on  (10.0.2.4):
Port       State       Service
5432/tcp   filtered    postgres
Too many fingerprints match this host for me to give an accurate OS
guess
Nmap run completed -- 1 IP address (1 host up) scanned in 47 seconds

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
Interesting ports on  (10.0.2.5):
Port       State       Service
5432/tcp   filtered    postgres
Too many fingerprints match this host for me to give an accurate OS
guess
Nmap run completed -- 1 IP address (1 host up) scanned in 43 seconds
```

Testing the connection using Telnet from the web machines

```
telnet 10.0.2.4 5432
Trying 10.0.2.4...
Connected to 10.0.2.4.
Escape character is '^]'.
asdf
EFATAL 1:  invalid length of startup packet
Connection closed by foreign host.

telnet 10.0.2.5 5432
Trying 10.0.2.5...
Connected to 10.0.2.5.
Escape character is '^]'.
asdf
EFATAL 1:  invalid length of startup packet
Connection closed by foreign host.
```

Testing the connection from other addresses on the DMZ results in the following:

```
telnet 10.0.2.4 5432
Trying 10.0.2.4...
telnet: connect to address 10.0.2.4: Connection refused
```

Attempting to connect to it from the auditor's network obviously yields:

```
telnet 10.0.2.4 5432
Trying 10.0.2.4...
telnet: connect to address 10.0.2.4: No route to host
```

The same results were yielded with 10.0.2.5.

Rule	external to internal DNS	Verified
23	access-list dmz_in permit udp host XXX.234.209.166 host 10.0.2.6 eq domain	✔

Running DiG from the DMZ DNS host to the Internal DNS host yields the following result:

```
<<>> DiG 9.2.1 <<>> www.somewhere.org
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27825
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.somewhere.org.              IN      A

;; ANSWER SECTION:
www.somewhere.org.       10800   IN      CNAME   somewhere.org.
somewhere.org.           10800   IN      A       XXX.183.228.194

;; AUTHORITY SECTION:
somewhere.org.           10800   IN      NS      dns1.someisp.com.
somewhere.org.           10800   IN      NS      dns2.someisp.com.

;; ADDITIONAL SECTION:
dns1.someisp.com.        10800   IN      A       XXX.183.205.35
dns2.someisp.com.        10800   IN      A       XXX.183.192.65

;; Query time: 29 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Sat Feb 15 22:33:19 2003
```

Rule	Deny and Log	Verified
24	access-list dmz_in deny ip any any log-input	✔

SYN Stealth, and UDP Port scans verify that the firewall is indeed blocking any other traffic attempting to traverse the firewall from this interface. The PIX's stateful inspection features denied FIN and ACK scans. tcpdumps on the internal network did not discover any of the the port scan packets passing through the PIX from dmz networks on unexpected ports. The PIX successfully logged all denied attempts.

VPN_In

Rule	Remote Employees can access the database via the VPN	Verified
25	access-list vpn_in permit tcp 10.0.3.0 255.255.255.0 host 10.0.2.4 eq 5432	✔
26	access-list vpn_in permit tcp 10.0.3.0 255.255.255.0 host 10.0.2.5 eq 5432	✔

```
telnet 10.0.2.4 5432
Trying 10.0.2.4...
Connected to 10.0.2.4.
Escape character is '^]'.
asdf
EFATAL 1:  invalid length of startup packet
Connection closed by foreign host.

telnet 10.0.2.5 5432
Trying 10.0.2.5...
Connected to 10.0.2.5.
Escape character is '^]'.
asdf
EFATAL 1:  invalid length of startup packet
Connection closed by foreign host.
```

Rule	Get and receive e-mail	Verified
27	access-list vpn_in permit tcp 10.0.3.0 255.255.255.0 host 10.0.2.6 eq smtp	✔
28	access-list vpn_in permit tcp 10.0.3.0 255.255.255.0 host 10.0.2.6 eq pop3	✔

```
telnet 10.0.2.6 25
Trying 10.0.2.6...
Connected to smtp2.giac.com.
Escape character is '^]'.
220-smtp2.giac.com -- Server ESMTP ("SMTP-GIAC-02")
220 Unsolicted bulk mail prohibited; spammers will be prosecuted
HELO somewhere.net
250 smtp2.giac.com OK, pc12.giac.net [10.0.3.12].

telnet pop3.comcast.net 110
Trying 10.0.2.6...
Connected to pop3.comcast.net.
Escape character is '^]'.
+OK 11 -- ("SMTP-GIAC-02") Abuse prohibited; abusers will be prosecuted
```

Rule	DNS and secondary DNS for the VPN	Verified
29	access-list vpn_in permit udp 10.0.3.0 255.255.255.0 host 10.0.2.6 eq domain	✔
30	access-list vpn_in permit udp 10.0.3.0 255.255.255.0 host XXX.234.209.166 eq domain	✔

Running DiG against the DNS in the DMZ yields

```
<<>> DiG 9.2.1 <<>> www.somewhere.org
;; global options:  printcmd
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27825
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.somewhere.org.              IN      A

;; ANSWER SECTION:
www.somewhere.org.       10800   IN      CNAME   somewhere.org.
somewhere.org.           10800   IN      A       XXX.183.228.194

;; AUTHORITY SECTION:
somewhere.org.           10800   IN      NS      dns1.someisp.com.
somewhere.org.           10800   IN      NS      dns2.someisp.com.

;; ADDITIONAL SECTION:
dns1.someisp.com.        10800   IN      A       XXX.183.205.35
dns2.someisp.com.        10800   IN      A       XXX.183.192.65

;; Query time: 49 msec
;; SERVER: XXX.234.209.166#53(XXX.234.209.166)
;; WHEN: Sat Feb 15 22:54:18 2003
```

Running DiG against the DNS in the Customer Service network yields

```
; <<>> DiG 9.2.1 <<>> www.somewhere.org
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27825
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.somewhere.org.              IN      A

;; ANSWER SECTION:
www.somewhere.org.       10800   IN      CNAME   somewhere.org.
somewhere.org.           10800   IN      A       XXX.183.228.194

;; AUTHORITY SECTION:
somewhere.org.           10800   IN      NS      dns1.someisp.com.
somewhere.org.           10800   IN      NS      dns2.someisp.com.

;; ADDITIONAL SECTION:
dns1.someisp.com.        10800   IN      A       XXX.183.205.35
dns2.someisp.com.        10800   IN      A       XXX.183.192.65

;; Query time: 24 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Sat Feb 15 22:55:34 2003
```

Rule	Secure copy new web pages.	Verified
31	access-list vpn_in permit tcp 10.0.3.0 255.255.255.0 host XXX.234.209.164 eq ssh	✔
32	access-list vpn_in permit tcp 10.0.3.0 255.255.255.0 host XXX.234.209.165 eq ssh	✔

Tests from the auditor network for this case were already performed in Rules 8 and 9. SSH access is tested by using Telnet to connect to the SSH port to each of the sites in question.

```
telnet customer.giac.com 22
Trying XXX.234.209.164...
Connected to customer.giac.com.
SSH-2.0-OpenSSH_3.5p1
Protocol Mismatch.

telnet partner.giac.com 22
Trying XXX.234.209.165...
Connected to partner.giac.com.
SSH-2.0-OpenSSH_3.5p1
Protocol Mismatch.
```

Rule	VPN Concentrator to Syslog and NTP	Verified
33	access-list vpn_in permit udp XXX.234.209.176 255.255.255.252 host XXX.234.209.162 eq 514	✔
34	access-list vpn_in permit udp XXX.234.209.176 255.255.255.252 host XXX.234.209.162 eq ntp	✔

Temporarily turning down the VPN Concentrator's .176 interface, the same test is performed using the VPN Concentrator's IP address (host XXX.234.209.176). It succeeded. The message on the server looked like this:

```
Feb 15 22:49:30 XXX.234.209.176 XXX.234.209.176 SyslogGen This is a
test message generated by the 'Syslog Message Generator'
```

The same UDP port scan from this IP address yields:

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
Interesting ports on  (XXX.234.209.162):
Port       State      Service
514/udp    open       syslog
Remote OS guesses: Linux Kernel 2.4.0 - 2.5.20, Linux 2.4.19-pre4 on
Alpha, Linux Kernel 2.4.0 - 2.5.20 w/o tcp_timestamps, Gentoo 1.2 linux
(Kernel 2.4.19-gentoo-rc5), Linux 2.5.25 or Gentoo 1.2 Linux 2.4.19
rc1-rc7), Linux 2.4.7 (X86)
Nmap run completed -- 1 IP address (1 host up) scanned in 4 seconds
```

Performing the same UDP port scan for NTP (as opposed to syslog) from the VPN Concentrator's IP address revealed an open port on NTP. Running ntpdate from the laptop hooked using the VPN Concentrator's IP address yielded the following information

```
ntpdate –b XXX.234.209.162
15 Feb 23:34:20 ntpdate[18599]: step time server XXX.234.209.162 offset
-0.021367 sec
```

Rule	VPN RSA Ace/Server access	Verified
35	access-list vpn_in permit udp XXX.234.209.176 255.255.255.252 host 10.0.2.7 eq 5500	✔
36	access-list vpn_in permit udp XXX.234.209.176 255.255.255.252 host 10.0.2.8 eq 5500	✔

Connecting to the VPN Concentrator from the auditor's network using SecurID to authenticate along with tcpdumps from the auditor's network and the customer service network verified that traffic was passing through the concentrator to the RSA ACE/Server along the expected port.

Running a UDP scan for port 5500 on the PIX's VPN facing address yielded:

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
Interesting ports on  (XXX.234.209.177):
Port       State       Service
5500/udp   open        securid
Too many fingerprints match this host for me to give an accurate OS
guess
Nmap run completed -- 1 IP address (1 host up) scanned in 21 seconds
```

Rule	Deny and Log	Verified
37	access-list vpn_in deny ip any any log-input	✔

SYN Stealth, and UDP Port scans from the VPN Concentrator IP address verify that the firewall is indeed blocking any other traffic attempting to traverse the firewall from the VPN Concentrator facing interface. The PIX's stateful inspection features denied FIN and ACK scans. tcpdumps on the internal network did not discover any of the the port scan packets passing through the PIX from vpn networks on unexpected ports. The PIX successfully logged all denied attempts.

3.2.7 Audit of Office Traffic using tcpdump

Some traffic rules cannot be tested because neither GIAC nor the auditing company owns the hosts that are allowed to access. The tcpdumps gathered from monitoring traffic in and out of GIAC for two days were used to verify these rules.

Rule	ISP DNS to External DNS (zone transfer)	Verified
38	access-list outside_in permit tcp host XYZ.12.12.14 host XXX.234.209.166 eq domain	✔

```
16:35:17.590056 XYZ.12.12.14.33228 > XXX.234.209.166.domain: S
3562218001:3562218001(0) win 5840 <mss 1460,sackOK,timestamp
69149026[|tcp]> (DF)

16:35:17.590210 XXX.234.209.166.domain > XYZ.12.12.14.33228: S
3128929:3128929(0) ack 3562218002 win 32120 <mss 1360,nop,nop,sackOK>
(DF)
```

```
16:35:17.590311 XYZ.12.12.14.33228 > XXX.234.209.166.domain: . ack 1
win 5840 (DF)

16:35:17.596891 XXX.234.209.166.domain > XYZ.12.12.14.33228: P 1:65(64)
ack 1 win 32120 12333 notify$ [21037a] [22337q] [18004n]
[20548au][|domain] (DF)...
```

Rule	Public Stratum 2 NTP to NTP Server	Verified
39	access-list outside_in permit udp host XZ6.200.93.8 host XXX.234.209.162 eq ntp	
40	access-list outside_in permit udp host XW0.162.8.3 host XXX.234.209.162 eq ntp	
41	access-list outside_in permit udp host X8.82.161.227 host XXX.234.209.162 eq ntp	

```
16:44:15.163711 XXX.234.209.162.ntp > XW0.162.8.3.ntp:  v4 bcast strat
3 poll 6 prec -6 (DF)
16:44:15.163778 XXX.234.209.162.ntp > XZ6.200.93.8.ntp:  v4 bcast strat
3 poll 6 prec -6 (DF)
16:44:15.181150 XW0.162.8.3.ntp > XXX.234.209.162.ntp:  v4 bcast strat
3 poll 6 prec -18 [tos 0x10]
16:44:15.186429 XZ6.200.93.8.ntp > XXX.234.209.162.ntp:  v4 bcast strat
3 poll 6 prec -18 [tos 0x10]
16:44:15.364820 XXX.234.209.162.ntp > X8.82.161.227.ntp:  v4 bcast
strat 3 poll 6 prec -6 (DF)
16:44:15.377348 X8.82.161.227.ntp > XXX.234.209.162.ntp:  v4 bcast
strat 3 poll 6 prec -18 [tos 0x10]...
```

3.2.8 Application Testing

A series of applications were run in the Internal Network to see if they could reach the Internet. AOL Instant Messenger (AIM) and GoToMyPC were found to be able to operate in the office in violation of the firewall policy. AIM and GoToMyPC's ability to use ports that are commonly left open in a firewall configuration allowed them to evade detection during the tcpdump of all office traffic. The only way they would have been detected would be if they were initially negotiating a connection port at which time the tcpdump would have reported a series of SYN packets without response on different ports until a connection was finally established on a port that is open on the firewall.

3.2.9 Service Testing

Specific services must be tested to see if they conform to the firewall policy. From the inside network and the VPN network access to the following services that pass through the firewall are tested: Web browsing to the Internet, SSH connections to customer and partner sites are tested, FTP to the Internet.

The DMZ has several services that must be accessible from the outside world. GIAC personnel from the consultant's site test each of the accounts. partner.giac.com is tested for secure database access using a test account from the consultant's site. The test fails because the ACL only allows access to partner from the partners sites. www.giac.com is tested for secure customer

ordering from the consultant's site. The order works indicating the firewall is allowing packets to pass through to the website from the web. Mail is sent into the giac.com domain to test the SMTP server. Mail is sent from the giac.com domain to the consultants to verify outbound rules. An attempt to make a zone transfer will be attempted from the consultant's domain. This will test the rule prohibiting transfers from the external DNS to any address except the ISPs DNS. Sam Spade will be used to test the rule. To enable zone transfers the following checkbox needs to be checked in options.

Sam Spade Options Screen

To perform a zone transfer, click the Zone Transfer menu item found under the "Tool" menu bar item. The information for GIACs DNS is filled into the Zone Transfer window.

Sam Spade Zone Transfer

The zone transfer is unsuccessful. All syslogs are checked and logs of each audit session are copied from the syslogs and attached to the audit. Finally the PIX log for the audit is copied and attached to the audit.

3.2.10 Access Control Policy Verification

GIAC has a change control policy in place for access to the firewall. Access to the PIX is through either SSH or through the console port inside the data center. Access by both means was tested and verified. When the PIX was accessed an adequate warning banner was issued. SSH connections time have been verified to timeout after five minutes of inactivity. Access via other means was tested (e.g. Telnet) and denied.

Rule	ssh timeout	Verified
42	ssh timeout 5	✔

Each administrator has an individual account on the PIX by which to make changes. All activity on the PIX is logged to a syslog server. Changes made to the firewall rules and policies are agreed upon in advance at a weekly change control meeting. All changes and tests of those changes are documented in a departmental blog on a workstation in the Network Management Center. The workstation is backed up to tape nightly. This preserves the change control logs in case of hardware failure.

3.3 Audit Results

Software and Hardware	Result	Service Testing	Result
Physically Secure	Passed	Internal Web	Passed
Redundant Power Supply and UPS	Passed	Internal FTP	Passed
Console Secured	Passed	Internal SSH to Websites	Passed
Documentation Checked	Passed	Internal SMTP	Passed
Configuration Files Checked	Passed	Internal POP3	Passed
Latest patches installed on Firewall	Passed	VPN Web	Passed
Redundant Firewall	Failed	VPN FTP	Passed
Only needed services running	Passed	VPN SSH to Websites	Passed
Password Policy for Firewall	Passed	VPN SMTP	Passed
Ping Sweeps & Port Scans	**Result**	VPN POP3	Passed
ICMP traffic denied by Firewall	Passed*	Internet to partner.giac.com	Passed
TCP ACK ping denied	Passed**	Internet to www.giac.com	Passed
Inbound Port Scan (TCP)	Passed	Internet SMTP	Passed
Inbound Port Scan (UDP)	Passed	Zone Transfer Test	Passed
Outbound Port Scan (TCP)	Passed	Internal/VPN AIM	Failed
Outbound Port Scan (UDP)	Passed	Internal/VPN Telnet	Passed
Firewall Rulebase Testing	**Result**	**Logs**	**Result**
Internet to DMZ	Passed	partner syslog	Passed
Internal to DMZ	Passed	www syslog	Passed
VPN to DMZ	Passed	SMTP syslog	Passed
Internet to VPN	Passed	DNS syslog	Passed
Internal to VPN	Passed	PIX logs	Passed
DMZ to VPN	Passed		
Internet to Internal	Passed		
DMZ to Internal	Passed		
VPN to Internal	Passed		
Internal to Internet	Passed		
DMZ to Internet	Passed		
VPN to Internet	Passed		

The firewall ruleset and actions taken by GIAC staff generally map to the stated GIAC Firewall Policy. As always there are suggestions as to how to improve the ability of the firewall to protect GIAC.

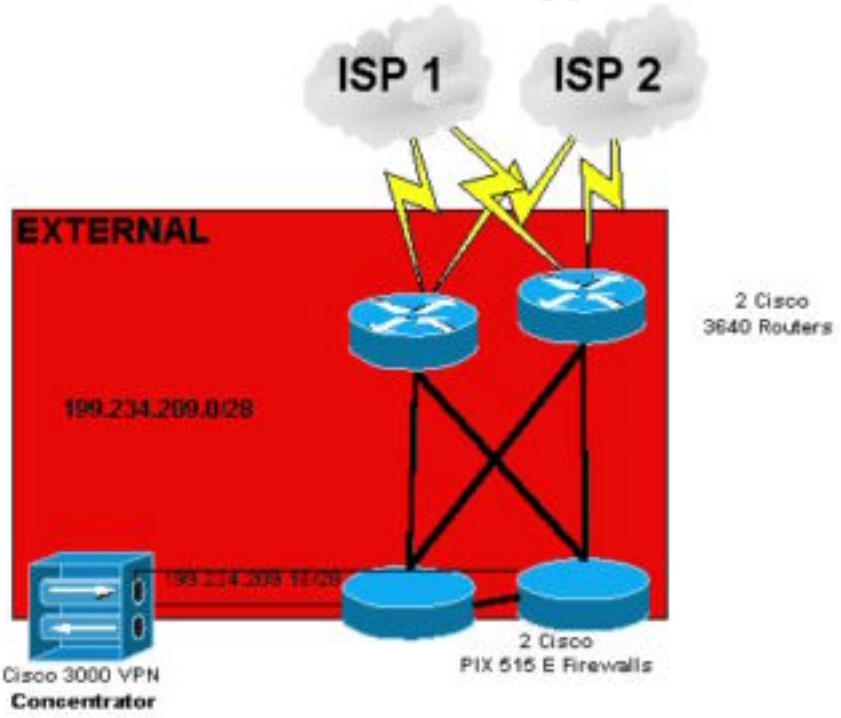
3.4 Auditor Recommendations

The auditors made several recommendations to assist GIAC in protecting its assets.

3.4.1 Redundant Networks and Network Devices

The current network architecture has only one primary firewall and one perimeter router attached to one ISP. This creates bottlenecks at both the firewall and the PIX. The risk here is twofold: 1.) The system lacks fault tolerance. If either the perimeter router or the PIX encounters a fault that severs it from the network GIAC's connection to the Internet is lost, and 2.) The system could be trivially brought down by a concerted DoS attack at either bottleneck.

Recommendation 1: Subscribe to a second ISP. Purchase a redundant Cisco 3640 and redundant PIX. Place them in a redundant configuration that connects each 3640 to both providers and each PIX to each 3640.



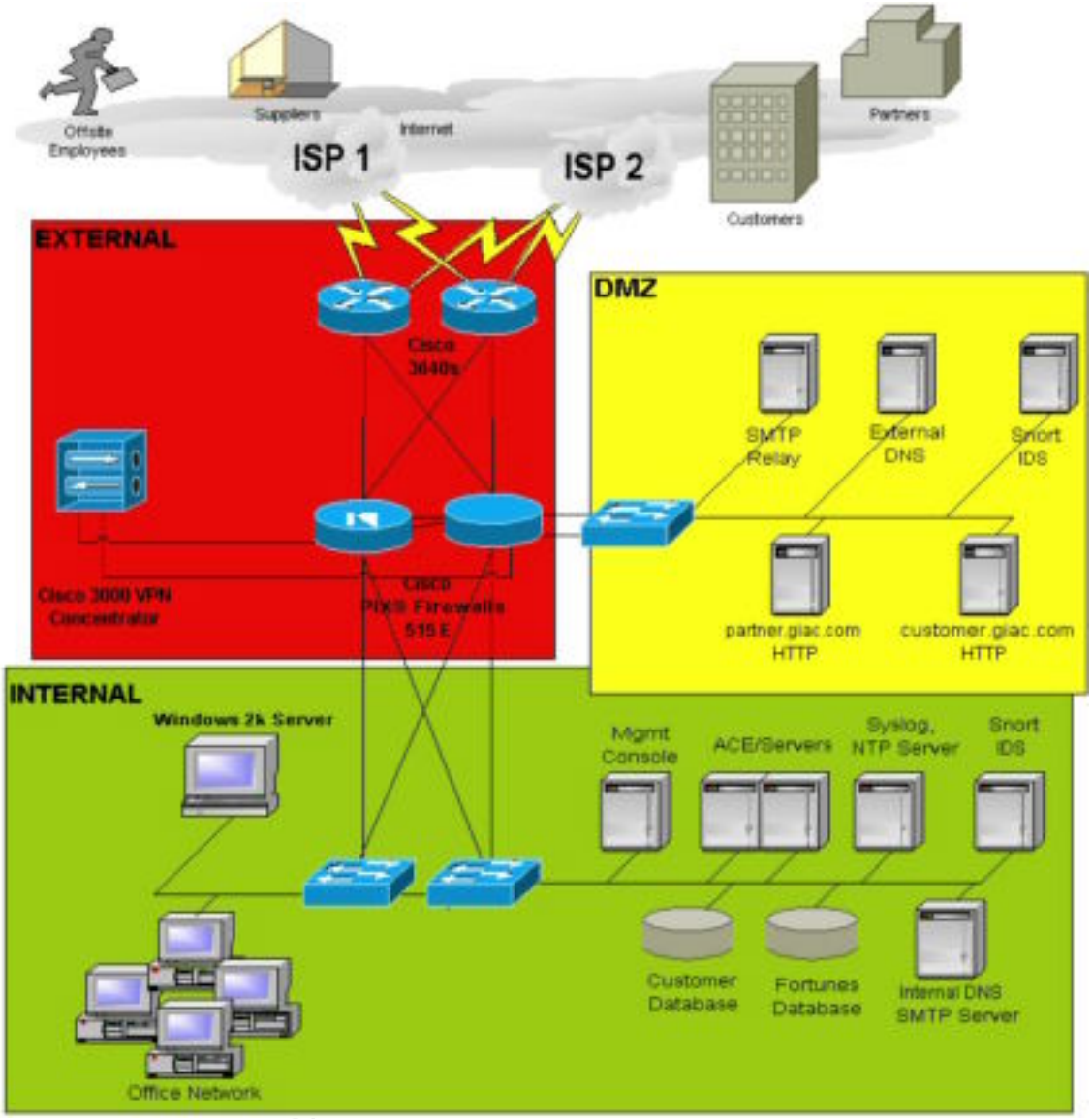
Recommendation 1 Architecture

3.4.2 Switching

Although it is not an issue now bandwidth utilization in the future could be an issue.

Recommendation 2: Place 3 Cisco Catalyst 2950 48PT 10/100 switches one on the Yellow Network borders the PIXs through the hub, one behind the internal firewall on the office network, and one on the non-office network behind the internal firewall. These switches provides a performance enhancement by breaking each host behind it into it's own collision domain. Hence the switches also increase the availability of the host. Placing the switch at these points of the network allows for the greatest benefit to the most hosts. Also, since the office PCs exclusively use IP using a WINS server residing on the Windows 2000 server to resolve where other PCs are located bandwidth efficiencies can be realized in acting on this strategy[40]

40. The SANS Institute. Network Design and Troubleshooting, SANS Firewall Track 2.5.2. Bethesda, MD: SANS Press, p. 58,59 (2001).



Architecture with Recommendation 1 and Recommendation 2 implemented

3.4.3 Disabling AOL Instant Messenger

Although the policy denies AOL Instant Messenger (AIM) traffic from Internal Networks, the firewall allowed AIM traffic to pass through. This is because AIM scans for open ports. It finds the open port and uses it to login to the host login.oscar.aol.com.

Recommendation 3: Add an access list entry denying access to login.oscar.aol.com. Create a DNS entry in the internal DNS that points login.oscar.aol.com to an internal address. This should prevent most users from accessing AIM. Some users will be proficient enough manipulating the AIM client to place the actual IP address for login.oscar.aol.com into the host field of the connection preferences window on their client (they would get this from an

outside DNS). The host login.oscar.aol.com has changed IP addresses at least once but it may be worth adding an entry in the routing tables of the firewall that would make the current IP address unreachable from GIAC. Some have suggested blocking the entire netblock for AOL.[41]

3.4.4 Disabling GoToMyPC and Windows Remote Desktop

Although the policy denies any other VPNs being setup. GoToMyPC.com has a client that will breach the firewall using ports 80, 443, and 8200.[42] Microsoft Windows 2000 and later has the Remote Desktop Protocol which uses port 3389.[43]

Recommendation 4: Add an access list entry denying access to poll.gotomypc.com. Create a DNS entry in the internal DNS that points the netblock for gotomypc.com to an internal address.[44] Place an egress filter on the ephemeral ports 3389 and 8200.

3.4.5 Further Restricting DNS and POP3

Rules 4 and 5 above allowed access to Domain Name Servers and POP3 Servers on the Internet. This could allow an employee to download mail from a site that is not controlled by GIAC. Which would be information brought into GIAC without first passing through a GIAC server. The rule should be tightened to allowing access only to the GIAC's DNS and POP3 Server.

41. Shockley, Steven "Blocking AIM, ICQ and Yahoo! Messenger with ipf." URL: http://www.shockley.net/ipf-block-aim.asp (20 January 2003).

42. ISS X-Force Database, "http-gotomypcdotcom-connection (9166): Detects a login from the gotomypc.com site to a local host running the server software" URL: http://www.iss.net/security_center/static/9166.php (20 January 2003).

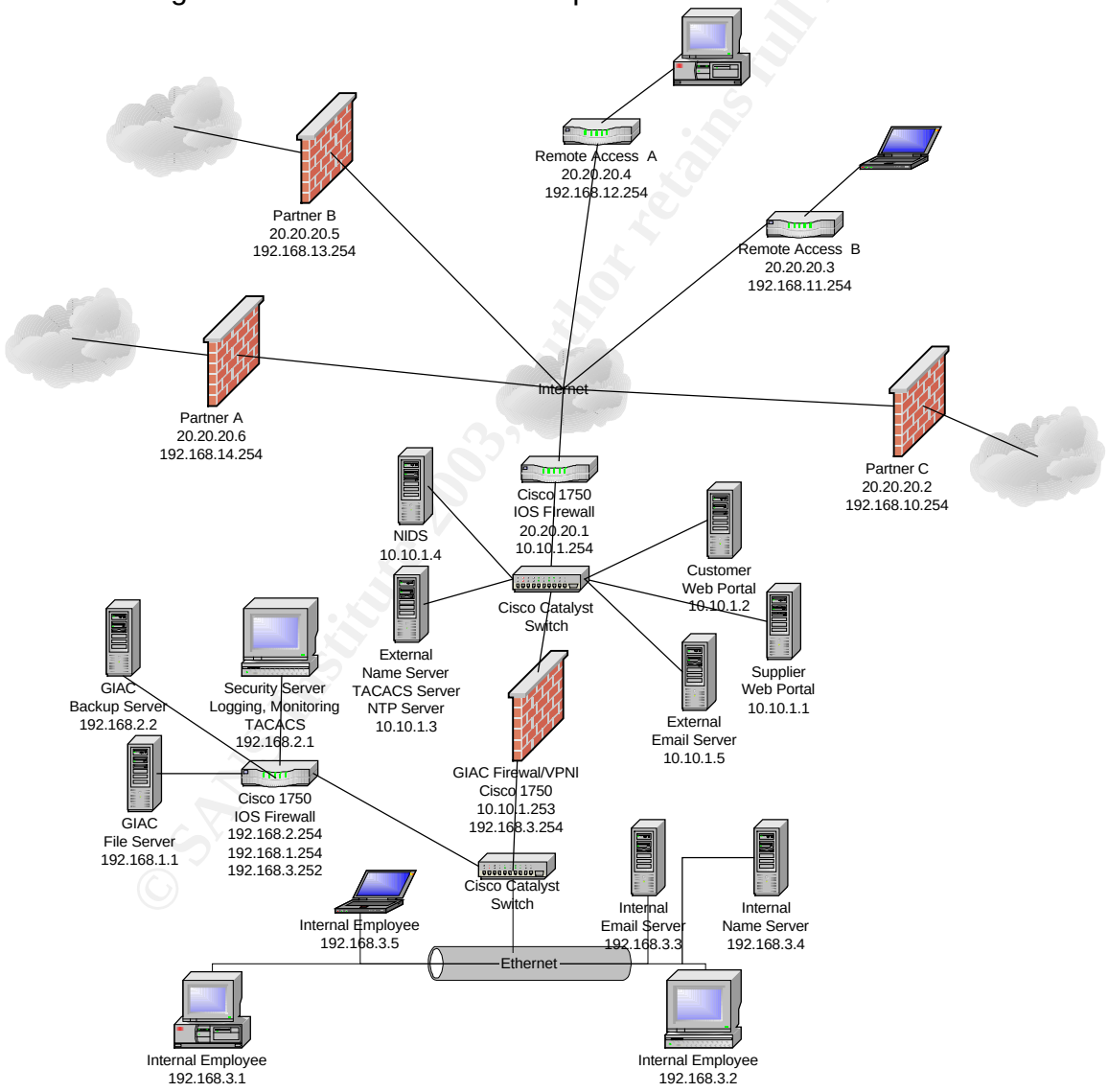
43. Akerman, Richard, "TCP/IP Ports" URL: http://www.chebucto.ns.ca/~rakerman/port-table.html#Table (20 January 2003).

44. ISS X-Force Database, "http-gotomypcdotcom-connection (9166): Detects a login from the gotomypc.com site to a local host running the server software" URL: http://www.iss.net/security_center/static/9166.php (20 January 2003)..

Assignment 4 – Design Under Fire

4.0 Design Under Fire Introduction

For the rest of the paper, I will be working to pierce the security of another GIAC Enterprises the one described in great detail by Keith Pachulski. (http://www.giac.org/practical/Keith_Pachulski_GCFW.doc) I will first attack his firewall utilizing a vulnerability for the firewall he chose. Then I will perform a denial of service attack and describe some countermeasures that could be put in place against such attacks. Finally, I will select an internal system to compromise and describe the process by which it will be attacked. Here is the Network Diagram from Mister Pachulski's practical.[45]



45. Pachulski, Keith, "Keith_Pachulski_GCFW.doc", 17 October 2002 URL: http://www.giac.org/practical/Keith_Pachulski_GCFW.doc. (20 January 2003).

4.1 Attacking the Firewall

I chose to engage Mister Pachulski's firewall with a recent attack. The Cisco Systems Product Security Incident Response Team issued an advisory regarding "SSH Malformed Packet Vulnerabilities" on December 20th 2002. This attack relies on the being able to initiate an SSH session with the router. Authentication is not necessary because the attack acts upon either the greeting or the Key Exchange portion of the SSHv2 process. The attack itself is comprised of sending various forms of malformed data at the SSH daemon.[46]

Poor implementation of SSH on a wide variety of platforms led to various potentials for buffer overflow exploits. The results of the attack differ for various types of daemons. In the case of this router it would reload IOS and still be vulnerable after reload.[47]

Using DiG or NSLookup, I determined the publicly accessible IP addresses of giac.com. Using Traceroute, I determined the IP address of the giac's border router.

Rapid7 released the SSHredder test suite as a free download which I downloaded using a one time email address from a public computer. Once I downloaded SSHredder, I used netcat to project the various SSHredder tests at the firewall from a spoofed address from the GIAC internal network again from a public computer.

```
[cosmic]> nc -v 20.20.20.1 22 < *.pdu
```

Downloads:

Netcat: http://www.atstake.com/research/tools/network_utilities
SSHredder: http://www.rapid7.com/perl/DownloadRequest.pl?PackageChoice=666

The attack failed because Mister Pachulski has limited SSH access to the host to a single IP address from within his domain. The attack relied on being able to access the SSH daemon.

If the attack succeeded, I could have then isolated which attacks reset the router and performed a DoS or with a little programming a DDoS attack based on the vulnerability. The DoS attack would have effectively brought traffic going into and departing GIAC to a standstill. This would have disrupted the connections that GIAC has with customers and partners on the Internet. Performed at the right time it could shatter confidence in the company's ability to operate effectively on the Internet.

---

46. Rapid7, "http://www.rapid7.com/advisories/R7-0009.txt." URL: http://www.rapid7.com/advisories/R7-0009.txt. (16 February 2003).

47. Cisco Systems, "Cisco Security Advisory: SSH Malformed Packet Vulnerabilities." URL:http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml. (16 February 2003).

4.2 DDoS, Distributed Denial of Service Attack

The second portion of the client entails attacking the above network architecture with 50 Windows machines on Broadband SOHO (Small Office/Home Office) Connections.

4.2.1 DDoS Attack

A ubiquitous (and now classic) approach to launching distributed denial of service attacks involves semi-customizing (hex editing) existing trojan packages (in my case evilbot) that use IRC as a control channel for the zombie.[48]

Reconnaissance is limited to using traceroute to determine the ip address of GIACs border router. If traceroute fails then scanning GIAC's public IP block with nmap should suffice in lending me an educated guess.

According to the parameters of the assignment, I have obtained 50 Windows 9x/2000/XP machines that have cable/dsl connections with which I can launch my DDoS attack upon giac.com. I obtained these zombies by uploading a customizied version of the Subseven trojan to various Yahoo! Groups and e-mailing the trojan to several hundred e-mail addresses in domains with DSL or cable modem subscribers. The victims thought they were downloading and installing a virus cleaner.

I have pre-programmed my zombies to meet me on secret channel #FOMC on a secluded IRC server. From my secret IRC channel #FOMC I issue the following commands:[49]

```
<greenspan> !r
<knnby56> zombie 1.0 ready for action…
<xcvdf43> zombie 1.0 ready for action…
<lqrty_32> zombie 1.0 ready for action…
…
```

This verifies that my fifty zombies are indeed ready to launch to the attack. Next, I issue the command that will launch a DDoS attack upon grc.com's perimeter router.

```
<greenspan> !udp 20.20.20.1 9999999 0
```

The !udp command issued into the IRC channel instructs the Zombies to target the IP address with 9,999,999 UDP datagrams sent to random ports and to not

48. Merchant, Corey and Stewart, Joe, "SecurityFocus HOME Infocus: Detecting and Containing IRC-Controlled Trojans:" 10 July 2002. URL:http://online.securityfocus.com/infocus/1605 (20 January 2003).

49. Gibson, Steve, "The Attacks on grc.com." 5 March 2002. URL:http://grc.com/dos/grcdos.htm (20 January 2003).

delay at all the time between sending datagrams. The zombies all respond back to the channel with the following message.

```
<lqrty_32> PRIVMSG #FOMC Attacking host 20.20.20.1, 9999999, 0
```

So, calculating 50 cable/DSL connections times the average connection speed of 500k I come up with 25mb of traffic overwhelming that T1. Unless he is blocking all UDP inbound (he isn't) then his perimeter router should be overwhelmed. The perimeter router is the only means of GIAC.COM accessing the Internet. Therefore GIAC.COM is out of commission and the attack is successful.

4.2.2 Defending against DDoS

Although there is no magic bullet to defend against DDoS there are several things that can be done to mitigate the risk.

- ✓ **Policy**: Have a policy on hand giving step-by-step people to call (Executives, Engineers, Law Enforcement) and things to do (Forensics to isolate the kind of attack,

- ✓ **Know your ISP**: - You should know a technical and administrative contact. Also find out what their response to DDoS attacks has been in the past and get a response policy written into the service level agreement with the provider regarding addressing DDoS attacks.

- ✓ **Filtering**: - It is unlikely these days but if the attack is pointing at a single port or even a predictable group of ports you can block that port, or have your ISP block that port. Already you should have private addresses denied inbound, and addresses that are not sourced as your own denied outbound.[50]

- ✓ **TCP Intercept**: IOS has a function called TCP Intercept. This function intercepts and validates TCP connection requests. It intercepts SYN packets from clients to servers matching an extended access list tied to TCP Intercept.

- ✓ **Increase connection tables**: Increase connection tables and decrease TCP timeout times set on web servers.[51]

- ✓ **Bandwidth Throttling**: You could throttle bandwidth to a service that is under attack. Again this isn't so much a solution as a method of letting other services survive the onslaught.

---

50. Cisco Systems, "Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks." 17 February 2000. URL:http://www.cisco.com/warp/public/707/newsflash.html#prevention (20 January 2003).

51. Scheneider, Bill, "P R E S S R E L E A S E." 14 February 2000. URL:http://www.arena.no/nyheter/wsa-ddos.htm (20 January 2003).

4.3 Penetration Attack

The last attack is to penetrate the perimeter of the network above and gain access to an asset on the interior.

Reconnaissance and Target Selection

After reading some press releases on their website regarding partnerships in which GIAC is engaged. I first test the partner sites for vulnerabilities that would allow me to exploit any possible VPN connection and find nothing.

Running a SYN port scan on the well-known ports from nmap in sneaky mode from my machine, I discover the open services at giac.com. Running nmap in Sneaky mode tests a port once every 15 seconds. This takes awhile (over 4 hours) but the benefit is that the scan is so infrequent that it is likely to get buried in the logs. A tcpdump of the scan would look like this.

```
16:20:15.322517 my.evil-hacking-machine.com.58663 > 20.20.20.1.11253: S
115169870:115169870(0) win 4096
16:20:15.322582 20.20.20.1.11253 > my.evil-hacking-machine.com.58663: R
0:0(0) ack 115169871 win 0 (DF)...
16:20:30.657547 my.evil-hacking-machine.com.58663 > 20.20.20.1.10547: S
115169870:115169870(0) win 4096
16:20:30.657792 20.20.20.1.10547 > my.evil-hacking-machine.com.58663: R
0:0(0) ack 115169871 win 0 (DF)
```

I simultaneously run a UDP port scan (from one of my other hosts) of the well-known ports in sneaky mode as well and with both of them have discovered the services that can be accessed from the Internet. The open services are as follows:

TCP 80, TCP 443, TCP 53, UDP 53, TCP 123, TCP 25

Out of the services available, I conclude that the easiest and most desirable services to penetrate would be https and http. If I can gain access to these services I may be able to gain access to the internal databases, which store proprietary and confidential information. nmap also determined that the system in question is running a form of Linux.

Continuing with reconnaissance, the web server is first tested using Nikto (v 1.2.3) is a vulnerability assessment tool for webservers. At this point it tests "over 2000 potentially dangerous files/CGIs, versions on over 130 servers, and problems on over 200 servers."[52] I set Nikto here to scan for webservers on the ports where I found services.

```
Nikto.pl -h 20.20.20.1 -p 80,443
```

52. cirt.net, "Nikto." URL: http://www.cirt.net/code/nikto.shtml (20 January 2003).

Nikto will probably generate many logs at the target site when it operates. I make a point of performing this scan on a weekend or holiday (actually a three-day weekend would be ideal) when it will likely be some time before someone looks at the logs. Either way, Nikto would tell me that the servers are running Apache 1.3.26.

Vulnerability Search
A search through the possible exploits brings up several that come close but fail for different reasons. I chose to take advantage of the fact he is running Apache 1.3.26 and hopefully and outdated version of OpenSSL.

The vulnerability detailed in http://www.cert.org/advisories/CA-2002-23.html exploits a buffer overflow in the SSLv2 and/or SSLv3 handshake process. For version 2, the weakness is found in the fact that OpenSSL allows the client to set the key length to any size. The exploit overwrites variables in the SSL_Session structure with whatever code the hacker desires.[53]

In version 3, the same trick is performed with the SESSION_ID variable. I, of course, don't really have to know any of this; Solar Eclipse kindly wrote an exploit script that will grant shell access as the Apache UID on a vulnerable machine. I downloaded openssl-too-open from this site: http://packetstormsecurity.nl/0209-exploits/openssl-too-open.tar.gz

Impact
If I am able to get shell access to the host, then I will possibly be able to use other exploits to escalate my privileges to root. If the system is not chroot()ed I may be able to get information about the internal network by accessing logs. I can search for core dumps on the computer in an attempt to discover user account information. Depending on permissions, I may be able to download the /etc/passwd and /etc/groups cracking them at my leisure.

Penetration Attempt
To attempt the penetration on the server I first have to untar, compile and install the openssl-to-open source code. Once that is done, I decide that the most likely Linux for the host to be running is Red Hat version 7.3

To attack this version on this host, I issue the following command:

```
./openssl-to-open -a 0x0b 20.20.20.1
```

The following results appear:

```
: openssl-too-open : OpenSSL remote exploit
```

53. Eclipse, Solar. "openssl-too-open.c - OpenSSL remote exploit" 2001. URL: http://packetstormsecurity.nl/0209-exploits/openssl-too-open.tar.gz. (17 February 2003).

```
  by Solar Eclipse <solareclipse@phreedom.org>

: Opening 30 connections
  Establishing SSL connections

: Using the OpenSSL info leak to retrieve the addresses
  ssl0 : 0x810b3a0
  ssl1 : 0x810b360
  ssl2 : 0x810b4e0

* Addresses don't match...
```

It goes on like this twice more opening ten more connections each time. It fails to break into the server. I test all the different hardware platforms, and none of the exploits execute. Next I run openssl-scanner to see if I missed something.

```
./openssl-scanner 20.20.20.1
: openssl-scanner : OpenSSL vulnerability scanner
  by Solar Eclipse <solareclipse@phreedom.org>

Opening 255 connections . . . . . done
Waiting for all connections to finish . . . . . done

20.20.20.1: Not Vulnerable
```

Apparently the server has been patched or updated to a later version of OpenSSL.

Works Cited

1. The SANS Institute. Network Design and Troubleshooting, SANS Firewall Track 2.5.2. Bethesda, MD: SANS Press, p. 74 (2001).

2. Yankowski, Fred. “How do I...use pgAdmin II via a secure (encrypted) connection?“ 20 December 2001. URL:http://pgadmin.postgresql.org/pgadmin2.php?ContentID=11. (17 February 2003).

3. Childers, Richard. "Laptop Computer Security." Sans Info Sec Reading Room. 30 October 2000. URL: http://www.sans.org/rr/homeoffice/laptop.php. (20 January 2003).

4. The SANS Institute. Network Design and Troubleshooting, SANS Firewall Track 2.2.3. Bethesda, MD: SANS Press, p. 83 (2001).

5. Jakobsson, Markus “How Does SecurID Work?” URL:http://www.rsasecurity.com/rsalabs/staff/bios/mjakobsson/teaching/How%20does%20SecurID%20work_files/frame.htm. (12 February 2003).

6. Gutmann, Peter. “Encryption and Security Tutorial Part 4: Authentication” p.17. URL:http://www.cryptoengines.com/~peter/part4.pdf. (12 February 2003).

7. Antonine, Vanessa, et al. Router Security Configuration Guide. Fort Meade: National Security Agency, 2002. p. 45-50.

8. Chapell, Laura. Introduction to Cisco Router Configuration. Indianapolis: Macmillan Technical Publishing, 1999. p. 316.

9. Computer Incident Advisory Capability. "Information Bulletin J-043g: Creating Login Banners." CIAC. 9 May 2000. URL:http://www.ciac.org/ciac/bulletins/j-043.shtml. (20 January 2003).

10. Cisco Tech Notes. “Improving Security on Cisco Routers.” Cisco Systems. 29 December 2002. URL: http://www.cisco.com/warp/public/707/21.html#pass (20 January 2003)

11. Ibid.

12. Cisco Documentation. “Configuring Cisco Discovery Protocol.” Cisco Systems. 15 January 2002. URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/fcprt3/fcd301c.htm. (20 January 2003).

13. Internet FAQ Consortium. “What Can I Do About Source Routing?” Internet FAQ Consortium. 17 January 2003. URL:http://www.faqs.org/faqs/cisco-networking-faq/section-23.html. (20 January 2003).

14. CERT Coordination Center. “CERT® Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks.” CERT. 13 March 2000 URL: http://www.cert.org/advisories/CA-1998-01.html. (20 January 2003).

15. Cisco CCO, “Configuring Commonly Used IP ACLs.” Cisco Systems. 20 November 2002 URL: http://cco-rtp-1.cisco.com/en/US/tech/tk648/tk361/technologies_configuration_example09186a0080100548.shtml. (20 January 2003.)

16. The SANS Institute, Building a Rule Base: Defense In-Depth, SANS Firewall Track 2.3.2, Bethesda, MD: SANS Press, p. 68 (2001).

17. IANA, “Internet Protocol V4 Address Space.” IANA. 10 December 2002 URL: http://www.iana.org/assignments/ipv4-address-space. (20 January 2003).

18. Cisco Systems, “Basic Firewall Configuration.” 10 June 2002. URL:http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/config/bafwcfg.htm. (20 January 2003).

19. Chapman, David W., Fox Andy, Cisco Secure Pix Firewalls, Indianapolis: Cisco Press, 2002, p. 107

20. The SANS Institute, Firewalls 102: Perimeter Protection with Firewalls, SANS Firewall Track 2.2.5, Bethesda, MD: SANS Press, p. 189 (2001).

21. Cisco Security Advisory, “Cisco Secure PIX Firewall FTP Vulnerabilities.” Cisco Systems. 27 June 2000. URL:http://www.cisco.com/warp/public/707/pixftp-pub.shtml. (20 January 2003).

22. Chapman and Fox, p. 93.

23. Chapman and Fox, p. 306-307

24. Cisco Documentation, “Configuring Internet Key Exchange Security Protocol.” Cisco Systems. 20 November 2001. URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt4/scike.htm. (20 January 2003).

25. 1 SearchSecurity Definition, “Data Encryption Standard - a searchSecurity definition - see also: DES.” TechTarget. 19 January 2001. URL:

http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213893,00.html. (20 January 2003).

26. 1 SearchSecurity Definition, “MD5 - a searchSecurity definition.” TechTarget. 4 April 2002. URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci527453,00.html. (20 January 2003).

27. NIST, “FIPS 180-1 - Secure Hash Standard.” NIST. 17 April 1995. URL: http://www.itl.nist.gov/fipspubs/fip180-1.htm (20 January 2003).

28. 1 Cisco Systems, “CiscoWorks Management Center for VPN Routers Defining IKE Policies – Cisco Systems.” Cisco Systems. 17 January 2003. URL: http://www.cisco.com/en/US/products/sw/cscowork/ps3994/products_user_guide_chapter09186a00800e45ce.html#1048412. (20 January 2003).

29. Haden, Rhys, “IPSec”, 2002. URL: http://www.rhyshaden.com/ipsec.htm. (20 January 2003).

30. Cisco Systems, “Cisco VPN 3000 Series Concentrators Installing and Powering Up the VPN Concentrator.” URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_getting_started_guide_chapter09186a00800bf698.html#1050259. (20 January 2003).

31. Cisco Documentation, “Using the VPN Concentrator Manager for Quick Configuration.” Cisco Systems. 26 September 2002. URL:http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/3_6/getting/gs3mgr.htm. (20 January 2003).

32. Chapman and Fox p.198.

33. Cisco Systems, “User Management.” 2 May 2001. URL: http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/vpn3kco/vcoug/usr_3_0/usermgt.htm#xtocid28958. (20 January 2003).

34. Tracey, Miles and Wack, John, DRAFT Special Publication 800-42, Guideline on Network Security Testing. Washington: USGPO, 2001. p. 16

35. Shake Communications, “Firewall Auditing.” URL: http://www.shake.net/firewall.cfm. (20 January 2003).

36. SBC, “Internet-Pacific Bell Dedicated Rider C Final.“ URL: https://ebiznet.sbc.com/calnetinfo/RiderC/Other_Svcs/10_C_Hourly_Consulting.htm. (13 February 2003).

37. washingtonpost.com, “washingtonpost.com: Jobs.” URL: http://www.washingtonpost.com/ac2/wp-dyn/jobs/salarysurvey. (13 Feburary 2003).

38. Nmap, “Nmap -- Free Stealth Port Scanner For Network Exploration & Security Audits.” 10 August 2002.URL:http://www.insecure.org/nmap. (20 January 2003).

39. Fyodor, “Nmap network security scanner man page.” 2001. URL: http://www.insecure.org/nmap/data/nmap_manpage.html. (20 January 2003).

40. The SANS Institute. Network Design and Troubleshooting, SANS Firewall Track 2.5.2. Bethesda, MD: SANS Press, p. 58,59 (2001).

41. Shockley, Steven “Blocking AIM, ICQ and Yahoo! Messenger with ipf.” URL: http://www.shockley.net/ipf-block-aim.asp. (20 January 2003).

42. ISS X-Force Database, “http-gotomypcdotcom-connection (9166): Detects a login from the gotomypc.com site to a local host running the server software” URL:http://www.iss.net/security_center/static/9166.php. (20 January 2003).

43. Akerman, Richard, “TCP/IP Ports” URL: http://www.chebucto.ns.ca/~rakerman/port-table.html#Table. (20 January 2003).

44. ISS X-Force Database, “http-gotomypcdotcom-connection (9166): Detects a login from the gotomypc.com site to a local host running the server software” URL:http://www.iss.net/security_center/static/9166.php. (20 January 2003).

45. Pachulski, Keith, “Keith_Pachulski_GCFW.doc”, 17 October 2002 URL: http://www.giac.org/practical/Keith_Pachulski_GCFW.doc. (20 January 2003).

46. Rapid7, “http://www.rapid7.com/advisories/R7-0009.txt.” URL: http://www.rapid7.com/advisories/R7-0009.txt. (16 February 2003).

47. Cisco Systems, “Cisco Security Advisory: SSH Malformed Packet Vulnerabilities.” URL:http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml. (16 February 2003).

48. Merchant, Corey and Stewart, Joe, “SecurityFocus HOME Infocus: Detecting and Containing IRC-Controlled Trojans:” 10 July 2002. URL:http://online.securityfocus.com/infocus/1605. (20 January 2003).

49. Gibson, Steve, “The Attacks on grc.com.” 5 March 2002. URL:http://grc.com/dos/grcdos.htm. (20 January 2003).

50. Cisco Systems, “Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks.” 17 February 2000. URL:http://www.cisco.com/warp/public/707/newsflash.html#prevention. (20 January 2003).

51. Scheneider, Bill, “P R E S S R E L E A S E.” 14 February 2000. URL:http://www.arena.no/nyheter/wsa-ddos.htm. (20 January 2003).

52. cirt.net, “Nikto.” URL:http://www.cirt.net/code/nikto.shtml. (20 January 2003).

53. Eclipse, Solar. “openssl-too-open.c - OpenSSL remote exploit” 2001. URL: http://packetstormsecurity.nl/0209-exploits/openssl-too-open.tar.gz. (17 February 2003).

Appendix A

Dumps 1 – 5, Internal Office to Internet

Dump 1 - http

```
20:24:51.790737 10.0.1.34.3198 > XXX.114.201.19.http: S
73237820:73237820(0) win 32120 <mss 1360,nop,nop,sackOK> (DF
)
20:24:51.804345 XXX.114.201.19.http > 10.0.1.34.3198: S
2349476281:2349476281(0) ack 73237821 win 34000 <nop,nop,sac
kOK,mss 1360> (DF)
20:24:51.804425 10.0.1.34.3198 > XXX.114.201.19.http: . ack 1 win 32120
(DF)
20:24:51.804880 10.0.1.34.3198 > XXX.114.201.19.http: . 1:1361(1360)
ack 1 win 32120 (DF)
20:24:51.804913 10.0.1.34.3198 > XXX.114.201.19.http: P 1361:1712(351)
ack 1 win 32120 (DF)
```

Dump 2 - https

```
20:24:49.874395 10.0.1.34.3199 > XXX.114.201.19.https: S
73235903:73235903(0) win 32120 <mss 1360,nop,nop,sackOK> (D
F)
20:24:49.892633 XXX.114.201.19.https > 10.0.1.34.3199: S
554005921:554005921(0) ack 73235904 win 34000 <nop,nop,sack
OK,mss 1360> (DF)
20:24:49.892795 10.0.1.34.3199 > XXX.114.201.19.https: . ack 1 win
32120 (DF)
20:24:49.895522 10.0.1.34.3199 > XXX.114.201.19.https: P 1:97(96) ack 1
win 32120 (DF)
```

Dump 3 - ftp

```
20:39:19.362131 10.0.1.34.32809 > XXX.114.201.19.ftp: S
3618851230:3618851230(0) win 5840 <mss 1460,sackOK,timestamp
37938413[|tcp]> (DF)
20:39:19.362290 XXX.114.201.19.ftp > 10.0.1.34.32809: S
74105408:74105408(0) ack 3618851231 win 32120 <mss 1360,nop,nop,sackOK>
(DF)
20:39:19.362393 10.0.1.34.32809 > XXX.114.201.19.ftp: . ack 1 win 5840
(DF)
20:39:19.368649 XXX.114.201.19.ftp > 10.0.1.34.32809: P 1:65(64) ack 1
win 32120 (DF)
20:39:19.368758 10.0.1.34.32809 > XXX.114.201.19.ftp: . ack 65 win 5840
(DF) [tos 0x10]
...
20:41:02.889123 10.0.1.34.32809 > XXX.114.201.19.ftp: P 4860:4866(6)
ack 16486 win 5840 (DF) [tos 0x10]
20:41:02.896455 XXX.114.201.19.ftp > 10.0.1.34.32809: P 32486:32527(41)
ack 2466 win 31024 (DF)
20:41:02.896595 10.0.1.34.32809 > XXX.114.201.19.ftp: . ack 32527 win
5840 (DF) [tos 0x10]
```

```
20:41:02.896707 10.0.1.34.32809 > XXX.114.201.19.ftp: F 4866:4866(0)
ack 16527 win 5840 (DF) [tos 0x10]
20:41:02.896813 XXX.114.201.19.ftp > 10.0.1.34.32809: . ack 4867 win
31024 (DF)
20:41:02.907572 XXX.114.201.19.ftp > 10.0.1.34.32809: F 32527:32527(0)
ack 2467 win 31024 (DF)
20:41:02.907650 10.0.1.34.32809 > XXX.114.201.19.ftp: . ack 32528 win
5840 (DF)
```

Dump 4 – POP3

```
20:44:46.483533 10.0.1.34.32904 > XXX.234.209.166 .pop3: S
49338796:49338796(0) win 5840 <mss 1460,sackOK,timestamp
38290219[|tcp]> (DF) [tos 0x10]
20:44:46.495265 XXX.234.209.166 .pop3 > 10.0.1.34.32904: S
3384915805:3384915805(0) ack 49338797 win 33304 <nop,nop,timestamp
1282057896 38290219,nop,[|tcp]> (DF)
20:44:46.495359 10.0.1.34.32904 > XXX.234.209.166 .pop3: . ack 1 win
5840 <nop,nop,timestamp 38290225 1282057896> (DF) [tos 0x10]
20:44:46.511404 XXX.234.209.166 .pop3 > 10.0.1.34.32904: P 1:84(83) ack
1 win 33304 <nop,nop,timestamp 1282057898 38290225> (DF)
20:44:46.511475 10.0.1.34.32904 > XXX.234.209.166 .pop3: . ack 84 win
5840 <nop,nop,timestamp 38290234 1282057898> (DF) [tos 0x10]
20:44:51.773006 10.0.1.34.32904 > XXX.234.209.166 .pop3: F 1:1(0) ack
84 win 5840 <nop,nop,timestamp 38292928 1282057898> (DF) [tos 0x10]
20:44:51.784312 XXX.234.209.166 .pop3 > 10.0.1.34.32904: . ack 2 win
33304 <nop,nop,timestamp 1282058425 38292928> (DF)
20:44:51.790397 XXX.234.209.166 .pop3 > 10.0.1.34.32904: R
3384915889:3384915889(0) win 33304 (DF)
```

Dump 4a – POP3 (Elsewhere!!)

```
20:44:25.278163 10.0.1.34.32905 > XXX.114.201.19.pop3: S
39799463:39799463(0) win 5840 <mss 1460,sackOK,timestamp
38279362[|tcp]> (DF) [tos 0x10]
20:44:25.291268 XXX.114.201.19.pop3 > 10.0.1.34.32905: S
323355607:323355607(0) ack 39799464 win 33304 <nop,nop,timestamp
925967577 38279362,nop,[|tcp]> (DF)
20:44:25.291354 10.0.1.34.32905 > XXX.114.201.19.pop3: . ack 1 win 5840
<nop,nop,timestamp 38279369 925967577> (DF) [tos 0x10]
20:44:25.308938 XXX.114.201.19.pop3 > 10.0.1.34.32905: P 1:84(83) ack 1
win 33304 <nop,nop,timestamp 925967579 38279369> (DF)
20:44:25.309014 10.0.1.34.32905 > XXX.114.201.19.pop3: . ack 84 win
5840 <nop,nop,timestamp 38279378 925967579> (DF) [tos 0x10]
20:44:32.133365 10.0.1.34.32905 > XXX.114.201.19.pop3: P 1:7(6) ack 84
win 5840 <nop,nop,timestamp 38282872 925967579> (DF) [tos 0x10]
20:44:32.149047 XXX.114.201.19.pop3 > 10.0.1.34.32905: . ack 7 win
33304 <nop,nop,timestamp 925968263 38282872> (DF)
20:44:32.151193 XXX.114.201.19.pop3 > 10.0.1.34.32905: P 84:106(22) ack
7 win 33304 <nop,nop,timestamp 925968263 38282872> (DF)
20:44:32.151254 10.0.1.34.32905 > XXX.114.201.19.pop3: . ack 106 win
5840 <nop,nop,timestamp 38282881 925968263> (DF) [tos 0x10]
20:44:35.110065 10.0.1.34.32905 > XXX.114.201.19.pop3: P 7:10(3) ack
106 win 5840 <nop,nop,timestamp 38284396 925968263> (DF) [tos 0x10]
```

```
20:44:35.124944 XXX.114.201.19.pop3 > 10.0.1.34.32905: P 106:128(22)
ack 10 win 33304 <nop,nop,timestamp 925968560 38284396> (DF)
20:44:35.125013 10.0.1.34.32905 > XXX.114.201.19.pop3: . ack 128 win
5840 <nop,nop,timestamp 38284404 925968560> (DF) [tos 0x10]
20:44:43.168116 10.0.1.34.32905 > XXX.114.201.19.pop3: F 10:10(0) ack
128 win 5840 <nop,nop,timestamp 38288522 925968560> (DF) [tos 0x10]
20:44:43.180640 XXX.114.201.19.pop3 > 10.0.1.34.32905: . ack 11 win
33304 <nop,nop,timestamp 925969366 38288522> (DF)
20:44:43.182468 XXX.114.201.19.pop3 > 10.0.1.34.32905: R
323355735:323355735(0) win 33304 (DF)
```

Dump 5 – DNS (DMZ)

```
20:45:00.806845 10.0.1.34.32780 > XXX.234.209.166.domain:
23255+[|domain] (DF)
20:45:00.808861 10.0.1.34.32781 > XXX.234.209.166.domain:
22796+[|domain] (DF)
20:45:00.816597 XXX.234.209.166.domain > 10.0.1.34.32780:  23255
3/2/2[|domain] (DF)
20:45:00.825699 XXX.234.209.166.domain > 10.0.1.34.32781:
22796[|domain] (DF)
20:45:00.828047 10.0.1.34.32781 > XXX.234.209.166.domain:
22797+[|domain] (DF)
20:45:00.838575 XXX.234.209.166.domain > 10.0.1.34.32781:  22797
NXDomain[|domain] (DF)
```

Dump 5a – DNS (Elsewhere!!)

```
20:46:09.636679 10.0.1.34.32781 > ns01.elsewhere.org.domain:
14487+[|domain] (DF)
20:46:09.636679 10.0.1.34.32781 > ns01.elsewhere.org.domain:
14487+[|domain] (DF)
20:46:09.638673 10.0.1.34.32782 > ns01.elsewhere.org.domain:
45363+[|domain] (DF)
20:46:09.648602 ns01.elsewhere.org.domain > 10.0.1.34.32781:  14487
3/2/2[|domain] (DF)
20:46:09.653563 ns01.elsewhere.org.domain > 10.0.1.34.32782:
45363[|domain] (DF)
20:46:09.654537 10.0.1.34.32782 > ns01.elsewhere.org.domain:
45364+[|domain] (DF)
20:46:09.667909 ns01.elsewhere.org.domain > 10.0.1.34.32782:  45364
NXDomain[|domain] (DF)
```

Dumps 6 – 7, Connections from the Internal DNS and SMTP sites to the DMZ DNS and SMTP sites.
Dump 6 - UDP

```
20:48:25.185588 10.0.2.6.32777 > XXX.234.209.166.domain:
4440+[|domain] (DF)
20:48:25.187580 10.0.2.6.32778 > XXX.234.209.166.domain:
15886+[|domain] (DF)
20:48:25.197362 XXX.234.209.166.domain > 10.0.2.6.32777:  4440[|domain]
(DF)
```

```
20:48:25.202135 XXX.234.209.166.domain > 10.0.2.6.32778:
15886[|domain] (DF)
20:48:25.202935 10.0.2.6.32778 > XXX.234.209.166.domain:
15887+[|domain] (DF)
20:48:25.214011 XXX.234.209.166.domain > 10.0.2.6.32778:  15887
NXDomain[|domain] (DF)
20:48:49.132972 10.0.2.6.32778 > XXX.234.209.166.domain:
18332+[|domain] (DF)
20:48:49.146014 XXX.234.209.166.domain > 10.0.2.6.32778:
18332[|domain] (DF)
```

Dump 6a – TCP

```
20:58:54.109665 10.0.2.6.32803 > XXX.234.209.166.domain: S
1558112605:1558112605(0) win 5840 <mss 1460,sackOK,timestamp 34853
484[|tcp]> (DF)
20:58:54.109812 XXX.234.209.166.domain > 10.0.2.6.32803: S
68080042:68080042(0) ack 1558112606 win 32120 <mss 1360,nop,nop,sa
ckOK> (DF)
20:58:54.109904 10.0.2.6.32803 > XXX.234.209.166.domain: . ack 1 win
5840 (DF)
...
21:02:01.104265 10.0.2.6.32803 > XXX.234.209.166.domain: F 1236:1236(0)
ack 191 win 5840 (DF) [tos 0x10]
20:02:01.104375 XXX.234.209.166.domain > 10.0.2.6.32803: . ack 1237 win
32085 (DF)
21:02:01.107923 XXX.234.209.166.domain > 10.0.2.6.32803: F
20191:20191(0) ack 37 win 32085 (DF)
21:02:01.107999 10.0.2.6.32803 > XXX.234.209.166.domain: . ack 20192
win 5840 (DF)
```

Dump 7 - SMTP

```
21:32:14.189100 10.0.2.6.2953 > XXX.234.209.166.smtp: S
70080160:70080160(0) win 32120 <mss 1360,nop,nop,sackOK> (DF)
21:32:14.204682 XXX.234.209.166.smtp > 10.0.2.6.2953: S
2974489942:2974489942(0) ack 70080161 win 34000 <nop,nop,sackOK,mss
1460> (DF)
21:32:14.204800 10.0.2.6.2953 > XXX.234.209.166.smtp: . ack 1 win 32120
(DF)
21:32:14.255544 XXX.234.209.166.smtp > 10.0.2.6.2953: P 1:139(138) ack
1 win 34000 (DF)
21:32:14.259264 10.0.2.6.2953 > XXX.234.209.166.smtp: P 1:13(12) ack
139 win 31982 (DF)
21:32:14.271268 XXX.234.209.166.smtp > 10.0.2.6.2953: . ack 13 win
34000 (DF)
21:32:14.273008 XXX.234.209.166.smtp > 10.0.2.6.2953: P 139:219(80) ack
13 win 34000 (DF)
21:32:14.281920 10.0.2.6.2953 > XXX.234.209.166.smtp: P 13:47(34) ack
219 win 31902 (DF)
21:32:14.297083 XXX.234.209.166.smtp > 10.0.2.6.2953: P 219:242(23) ack
47 win 34000 (DF)
21:32:14.300358 10.0.2.6.2953 > XXX.234.209.166.smtp: P 47:75(28) ack
242 win 31879 (DF)
21:32:14.314794 XXX.234.209.166.smtp > 10.0.2.6.2953: P 242:273(31) ack
75 win 34000 (DF)
21:32:14.320889 10.0.2.6.2953 > XXX.234.209.166.smtp: P 75:81(6) ack
273 win 31848 (DF)
```

```
21:32:14.334260 XXX.234.209.166.smtp > 10.0.2.6.2953: P 273:313(40) ack
81 win 34000 (DF)
21:32:14.341932 10.0.2.6.2953 > XXX.234.209.166.smtp: P 81:1240(1159)
ack 313 win 31808 (DF)
21:32:14.454433 XXX.234.209.166.smtp > 10.0.2.6.2953: . ack 1240 win
34000 (DF)
21:32:14.454541 10.0.2.6.2953 > XXX.234.209.166.smtp: P 1240:1245(5)
ack 313 win 31808 (DF)
21:32:14.549860 XXX.234.209.166.smtp > 10.0.2.6.2953: P 313:328(15) ack
1245 win 34000 (DF)
21:32:14.556819 10.0.2.6.2953 > XXX.234.209.166.smtp: P 1245:1251(6)
ack 328 win 31793 (DF)
21:32:14.569335 XXX.234.209.166.smtp > 10.0.2.6.2953: P 328:362(34) ack
1251 win 34000 (DF)
21:32:14.569864 XXX.234.209.166.smtp > 10.0.2.6.2953: F 362:362(0) ack
1251 win 34000 (DF)
21:32:14.569926 10.0.2.6.2953 > XXX.234.209.166.smtp: . ack 363 win
31759 (DF)
21:32:14.570340 10.0.2.6.2953 > XXX.234.209.166.smtp: F 1251:1251(0)
ack 363 win 31759 (DF)
21:32:14.587989 XXX.234.209.166.smtp > 10.0.2.6.2953: . ack 1252 win
34000 (DF)
```

Dumps 8 – 9, SSH from Internal host to GIAC Websites
Dump 8 - customer.giac.com

```
21:52:06.445386 10.0.1.23.2999 > customer.giac.com.ssh: S
71272440:71272440(0) win 32120 <mss 1360,nop,nop,sackOK> (DF)
21:52:06.445560 customer.giac.com.ssh > 10.0.1.23.2999: S
631456727:631456727(0) ack 71272441 win 5840 <mss 1460,nop,nop,sackOK>
(DF)
21:52:06.445692 10.0.1.23.2999 > customer.giac.com.ssh: . ack 1 win
32120 (DF)
21:52:06.456123 customer.giac.com.ssh > 10.0.1.23.2999: P 1:23(22) ack
1 win 5840 (DF)
21:52:06.572107 10.0.1.23.2999 > customer.giac.com.ssh: . ack 23 win
32098 (DF)
21:52:08.322209 10.0.1.23.2999 > customer.giac.com.ssh: P 1:3(2) ack 23
win 32098 (DF)
21:52:08.322363 customer.giac.com.ssh > 10.0.1.23.2999: . ack 3 win
5840 (DF)
21:52:08.322499 customer.giac.com.ssh > 10.0.1.23.2999: P 23:42(19) ack
3 win 5840 (DF)
21:52:08.322551 customer.giac.com.ssh > 10.0.1.23.2999: F 42:42(0) ack
3 win 5840 (DF)
21:52:08.322652 10.0.1.23.2999 > customer.giac.com.ssh: . ack 43 win
32079 (DF)
21:52:09.989406 10.0.1.23.2999 > customer.giac.com.ssh: F 3:3(0) ack 43
win 32079 (DF)
21:52:09.989507 customer.giac.com.ssh > 10.0.1.23.2999: . ack 4 win
5840 (DF)
```

Dump 9 - partner.giac.com

```
22:52:19.074400 10.0.1.23.3000 > partner.giac.com.ssh: S
71285069:71285069(0) win 32120 <mss 1360,nop,nop,sackOK> (DF)
22:52:19.074519 partner.giac.com.ssh > 10.0.1.23.3000: S
640821470:640821470(0) ack 71285070 win 5840 <mss 1460,nop,nop,sackOK>
(DF)
22:52:19.074643 10.0.1.23.3000 > partner.giac.com.ssh: . ack 1 win
32120 (DF)
22:52:19.083197 partner.giac.com.ssh > 10.0.1.23.3000: P 1:23(22) ack 1
win 5840 (DF)
22:52:19.271865 10.0.1.23.3000 > partner.giac.com.ssh: . ack 23 win
32098 (DF)
22:52:30.976074 10.0.1.23.3000 > partner.giac.com.ssh: P 1:3(2) ack 23
win 32098 (DF)
22:52:30.976238 partner.giac.com.ssh > 10.0.1.23.3000: . ack 3 win 5840
(DF)
22:52:30.976377 partner.giac.com.ssh > 10.0.1.23.3000: P 23:42(19) ack
3 win 5840 (DF)
22:52:30.976430 partner.giac.com.ssh > 10.0.1.23.3000: F 42:42(0) ack 3
win 5840 (DF)
22:52:30.976529 10.0.1.23.3000 > partner.giac.com.ssh: . ack 43 win
32079 (DF)
22:52:33.799287 10.0.1.23.3000 > partner.giac.com.ssh: F 3:3(0) ack 43
win 32079 (DF)
22:52:33.799384 partner.giac.com.ssh > 10.0.1.23.3000: . ack 4 win 5840
(DF)
```

Dumps 10 – 13, Connections to giac.com websites from the Internet using http and https

Dump 10 - https, customer.giac.com

```
20:11:26.601087 XXX.114.201.20.2255 > customer.giac.com.https: S
54432284:54432284(0) win 32120 <mss 1360,nop,nop,sackOK> (D
F)
20:11:26.615755 customer.giac.com.https > XXX.114.201.20.2255: S
4206192688:4206192688(0) ack 54432285 win 34000 <nop,nop,sa
ckOK,mss 1460> (DF)20:11:27.044960 XXX.114.201.20.2255 >
customer.giac.com.https: . ack 1708 win 32053 (DF)
20:11:27.078908 XXX.114.201.20.2255 > customer.giac.com.https: P
274:1256(982) ack 1708 win 32053 (DF)
20:11:27.078933 XXX.114.201.20.2255 > customer.giac.com.https: P
1256:1410(154) ack 1708 win 32053 (DF)
20:11:27.107906 customer.giac.com.https > XXX.114.201.20.2255: . ack
1410 win 34000 (DF)
20:11:27.381512 customer.giac.com.https > XXX.114.201.20.2255: .
1708:3068(1360) ack 1410 win 34000 (DF)
20:11:27.382663 customer.giac.com.https > XXX.114.201.20.2255: P
3068:4428(1360) ack 1410 win 34000 (DF)
20:11:27.382753 XXX.114.201.20.2255 > customer.giac.com.https: . ack
4428 win 32120 (DF)
20:11:27.383704 customer.giac.com.https > XXX.114.201.20.2255: P
4428:5663(1235) ack 1410 win 34000 (DF)
20:11:27.384707 customer.giac.com.https > XXX.114.201.20.2255: P
5663:6793(1130) ack 1410 win 34000 (DF)
20:11:27.384772 XXX.114.201.20.2255 > customer.giac.com.https: . ack
6793 win 32120 (DF)
```

Dump 11 - http, customer.giac.com

```
20:12:22.921920 XXX.114.201.20.2097 > customer.giac.com.http: S
54368603:54368603(0) win 32120 <mss 1360,nop,nop,sackOK> (DF)
20:12:22.935931 customer.giac.com.http > XXX.114.201.20.2097: S
1422373497:1422373497(0) ack 54368604 win 9520 <nop,nop,sackOK,mss
 1360> (DF)
20:12:22.936034 XXX.114.201.20.2097 > customer.giac.com.http: . ack 1
win 32120 (DF)
20:12:22.941490 XXX.114.201.20.2097 > customer.giac.com.http: P
1:439(438) ack 1 win 32120 (DF)
20:12:22.960854 customer.giac.com.http > XXX.114.201.20.2097: . ack 439
win 9520 (DF)
20:12:22.963891 customer.giac.com.http > XXX.114.201.20.2097: P
1:201(200) ack 439 win 9520 (DF)
20:12:23.141162 XXX.114.201.20.2097 > customer.giac.com.http: . ack 201
win 31920 (DF)
20:12:23.154711 customer.giac.com.http > XXX.114.201.20.2097: FP
201:355(154) ack 439 win 9520 (DF)
20:12:23.154820 XXX.114.201.20.2097 > customer.giac.com.http: . ack 356
win 31766 (DF)
20:12:23.161584 XXX.114.201.20.2097 > customer.giac.com.http: F
439:439(0) ack 356 win 31766 (DF)
20:12:23.174599 customer.giac.com.http > XXX.114.201.20.2097: . ack 440
win 9520 (DF)
```

Dump 12 - https, partner.giac.com

```
20:27:11.363097 XXX.114.201.20.2382 > partner.giac.com.https: S
55377063:55377063(0) win 32120 <mss 1360,nop,nop,sackOK> (DF)
20:27:11.376416 partner.giac.com.https > XXX.114.201.20.2382: S
2907818616:2907818616(0) ack 55377064 win 65535 <mss 1460> (DF)
20:27:11.376536 XXX.114.201.20.2382 > partner.giac.com.https: . ack 1
win 32120 (DF)
20:27:11.430798 partner.giac.com.https > XXX.114.201.20.2382: P
1:147(146) ack 97 win 65535 (DF)
20:27:11.437728 XXX.114.201.20.2382 > partner.giac.com.https: P
97:164(67) ack 147 win 31974 (DF)
20:27:11.438046 XXX.114.201.20.2382 > partner.giac.com.https: P
164:1111(947) ack 147 win 31974 (DF)
20:27:11.461141 partner.giac.com.https > XXX.114.201.20.2382: . ack
1111 win 65535 (DF)
20:27:11.537213 partner.giac.com.https > XXX.114.201.20.2382: P
1167:1190(23) ack 1111 win 65535 (DF)
20:27:11.537315 XXX.114.201.20.2382 > partner.giac.com.https: . ack 147
win 31974 (DF)
20:27:11.537337 partner.giac.com.https > XXX.114.201.20.2382: F
1190:1190(0) ack 1111 win 65535 (DF)
20:27:11.537387 XXX.114.201.20.2382 > partner.giac.com.https: . ack 147
win 31974 (DF)
20:27:11.539423 partner.giac.com.https > XXX.114.201.20.2382: P
147:1167(1020) ack 1111 win 65535 (DF)
20:27:11.539513 XXX.114.201.20.2382 > partner.giac.com.https: . ack
1191 win 30931 (DF)
20:27:11.544293 XXX.114.201.20.2382 > partner.giac.com.https: F
1111:1111(0) ack 1191 win 30931 (DF)
20:27:11.562558 partner.giac.com.https > XXX.114.201.20.2382: . ack
1112 win 65535 (DF)
```

Dump 13 - http, partner.giac.com

```
20:28:23.181790 XXX.114.201.20.2099 > partner.giac.com.http: S
54368863:54368863(0) win 32120 <mss 1360,nop,nop,sackO
K> (DF)
20:28:23.196858 partner.giac.com.http > XXX.114.201.20.2099: S
4265933831:4265933831(0) ack 54368864 win 25840 <nop,n
op,sackOK,mss 1460> (DF)
20:28:23.196937 XXX.114.201.20.2099 > partner.giac.com.http: . ack 1
win 32120 (DF)
20:28:23.202063 XXX.114.201.20.2099 > partner.giac.com.http: P
1:439(438) ack 1 win 32120 (DF)
20:28:23.219707 partner.giac.com.http > XXX.114.201.20.2099: . ack 439
win 25840 (DF)
20:28:23.228119 partner.giac.com.http > XXX.114.201.20.2099: P
1:337(336) ack 439 win 25840 (DF)
20:28:23.341147 XXX.114.201.20.2099 > partner.giac.com.http: . ack 337
win 31784 (DF)
20:28:23.356131 partner.giac.com.http > XXX.114.201.20.2099: FP
337:708(371) ack 439 win 25840 (DF)
20:28:23.356231 XXX.114.201.20.2099 > partner.giac.com.http: . ack 709
win 31413 (DF)
20:28:23.356678 XXX.114.201.20.2099 > partner.giac.com.http: F
439:439(0) ack 709 win 31413 (DF)
20:28:23.374381 partner.giac.com.http > XXX.114.201.20.2099: . ack 440
win 25840 (DF)
```

Dump 14 - Internet to DMZ SMTP Server

```
22:05:32.011714 XXX.114.201.20.32804 > XXX.234.209.166.smtp: S
1501796880:1501796880(0) win 5840 <mss 1460,sackOK,timestamp
36900410[|tcp]> (DF) [tos 0x10]
22:05:32.025716 XXX.234.209.166.smtp > XXX.114.201.20.32804: S
2478607386:2478607386(0) ack 1501796881 win 33304 <nop,nop,timestamp
1199343909 36900410,nop,[|tcp]> (DF)
22:05:32.025834 XXX.114.201.20.32804 > XXX.234.209.166.smtp: . ack 1
win 5840 <nop,nop,timestamp 36900417 1199343909> (DF) [tos 0x10]
22:05:32.048766 XXX.234.209.166.smtp > XXX.114.201.20.32804: P
1:139(138) ack 1 win 33304 <nop,nop,timestamp 1199343911 36900417> (DF)
22:05:32.048842 XXX.114.201.20.32804 > XXX.234.209.166.smtp: . ack 139
win 5840 <nop,nop,timestamp 36900429 1199343911> (DF) [tos 0x10]
22:05:46.929016 XXX.114.201.20.32804 > XXX.234.209.166.smtp: P 1:15(14)
ack 139 win 5840 <nop,nop,timestamp 36908047 1199343911> (DF) [tos
0x10]
22:05:46.942785 XXX.234.209.166.smtp > XXX.114.201.20.32804: . ack 15
win 33304 <nop,nop,timestamp 1199345400 36908047> (DF)
22:05:46.943089 XXX.234.209.166.smtp > XXX.114.201.20.32804: P
139:219(80) ack 15 win 33304 <nop,nop,timestamp 1199345400 36908047>
(DF)
22:05:46.943151 XXX.114.201.20.32804 > XXX.234.209.166.smtp: . ack 219
win 5840 <nop,nop,timestamp 36908055 1199345400> (DF) [tos 0x10]
22:06:03.872050 XXX.114.201.20.32804 > XXX.234.209.166.smtp: P 15:20(5)
ack 219 win 5840 <nop,nop,timestamp 36916722 1199345400> (DF) [tos
0x10]
22:06:03.884655 XXX.234.209.166.smtp > XXX.114.201.20.32804: P
219:222(3) ack 20 win 33304 <nop,nop,timestamp 1199347094 36916722>
(DF)
```

```
22:06:03.884726 XXX.114.201.20.32804 > XXX.234.209.166.smtp: . ack 222
win 5840 <nop,nop,timestamp 36916729 1199347094> (DF) [tos 0x10]
22:06:15.648610 XXX.114.201.20.32804 > XXX.234.209.166.smtp: F 20:20(0)
ack 222 win 5840 <nop,nop,timestamp 36922752 1199347094> (DF) [tos
0x10]
22:06:15.661728 XXX.234.209.166.smtp > XXX.114.201.20.32804: . ack 21
win 33304 <nop,nop,timestamp 1199348272 36922752> (DF)
22:06:15.662263 XXX.234.209.166.smtp > XXX.114.201.20.32804: F
222:222(0) ack 21 win 33304 <nop,nop,timestamp 1199348272 36922752>
(DF)
22:06:15.662370 XXX.114.201.20.32804 > XXX.234.209.166.smtp: . ack 223
win 5840 <nop,nop,timestamp 36922759 1199348272> (DF)
```

Dump 15 - Internet to DMZ DNS

```
22:15:38.002360 XXX.114.201.20.32782 > XXX.234.209.166.domain:
62073+[|domain] (DF)
22:15:38.004560 XXX.114.201.20.32783 > XXX.234.209.166.domain:
12945+[|domain] (DF)
22:15:38.018547 XXX.234.209.166.domain > XXX.114.201.20.32783:
12945[|domain] (DF)
22:15:38.019320 XXX.114.201.20.32783 > XXX.234.209.166.domain:
12946+[|domain] (DF)
22:15:38.039052 XXX.234.209.166.domain > XXX.114.201.20.32783:  12946
NXDomain*[|domain] (DF)
22:15:38.041008 XXX.234.209.166.domain > XXX.114.201.20.32782:  62073*
3/2/2[|domain] (DF)
```

Dump 16 - Syslog (Auditor's Network)

```
03:53:11.439046 XXX.114.201.20.3853 > XXX.234.209.162.syslog: udp 110
03:53:12.469172 XXX.114.201.20.3853 > XXX.234.209.162.syslog: udp 110
03:53:13.478770 XXX.114.201.20.3853 > XXX.234.209.162.syslog: udp 109
03:53:14.509264 XXX.114.201.20.3853 > XXX.234.209.162.syslog: udp 108
03:53:15.519517 XXX.114.201.20.3853 > XXX.234.209.162.syslog: udp 110
03:53:16.553614 XXX.114.201.20.3853 > XXX.234.209.162.syslog: udp 109
03:53:17.598690 XXX.114.201.20.3853 > XXX.234.209.162.syslog: udp 110
03:53:18.617990 XXX.114.201.20.3853 > XXX.234.209.162.syslog: udp 109
03:53:19.693597 XXX.114.201.20.3853 > XXX.234.209.162.syslog: udp 110
```

Dump 16a - Syslog (DMZ)

```
[no data]
```

Dump 16b - Syslog (From the proper host)

```
03:29:00.842675 XXX.234.209.170.3706 > XXX.234.209.162.syslog: udp 6
03:29:03.328151 XXX.234.209.170.3707 > XXX.234.209.162.syslog: udp 6
03:29:05.600618 XXX.234.209.170.3708 > XXX.234.209.162.syslog: udp 7
03:29:07.796080 XXX.234.209.170.3709 > XXX.234.209.162.syslog: udp 7
```

Dump 16b - Syslog (From the DMZ)

```
03:29:01.012547 XXX.234.209.170.3706 > XXX.234.209.162.syslog: udp 6
03:29:03.652991 XXX.234.209.170.3707 > XXX.234.209.162.syslog: udp 6
03:29:05.943032 XXX.234.209.170.3708 > XXX.234.209.162.syslog: udp 7
03:29:08.034238 XXX.234.209.170.3709 > XXX.234.209.162.syslog: udp 7
```

Dump 17 – NTP (3640 to PIX)

```
23:38:41.864063 XXX.234.209.170.ntp > XXX.234.209.172.ntp:  v4 client
strat 0 poll 4 prec -6 (DF)
23:38:41.865948 XXX.234.209.172.ntp > XXX.234.209.170.ntp:  v4 server
strat 1 poll 4 prec -18 [tos 0x10]...
```

Dump 17a – NTP (PIX to DMZ)

```
23:38:41.866063 XXX.234.209.170.ntp > XXX.234.209.172.ntp:  v4 client
strat 0 poll 4 prec -6 (DF)
23:38:41.866148 XXX.234.209.172.ntp > XXX.234.209.170.ntp:  v4 server
strat 1 poll 4 prec -18 [tos 0x10]...
```

Dump 18 – (Testing Deny All) SYN Scan on PIX from Outside

```
23:40:49.989647 XXX.114.201.20.10997 > XXX.234.209.169.51318: S
786591601:786591601(0) win 3072
23:40:49.989788 XXX.114.201.20.10997 > XXX.234.209.169.54235: S
786591601:786591601(0) win 3072
23:40:49.989889 XXX.114.201.20.109977 > XXX.234.209.169.63984: S
786591601:786591601(0) win 3072
```

Dump 18a – Connect Scan on PIX from Outside

```
23:41:29.479535 XXX.114.201.20.5218 > XXX.234.209.169.12396: S
45673765:45673765(0) win 32120 <mss 1360,nop,nop,sackOK> (DF)
23:41:29.479742 XXX.114.201.20.5219 > XXX.234.209.169.31765: S
45673765:45673765(0) win 32120 <mss 1360,nop,nop,sackOK> (DF)
23:41:29.479941 XXX.114.201.20.5220 > XXX.234.209.169.2547: S
45673765:45673765(0) win 32120 <mss 1360,nop,nop,sackOK> (DF)
```

Dump 18b – UDP Scan on PIX from Outside

```
23:42:54.782979 XXX.114.201.20.4365 > XXX.234.209.169.15374: udp 0
23:42:54.782436 XXX.114.201.20.4365 > XXX.234.209.169.2716: udp 0
23:42:54.782542 XXX.114.201.20.4365 > XXX.234.209.169.1238: udp 0
23:42:54.782645 XXX.114.201.20.4365 > XXX.234.209.169.35671: udp 0
```

Dump 18c – FIN Scan on PIX from Outside

```
23:45:21.348822 XXX.114.201.20.42756 > XXX.234.209.169.54235: F 0:0(0)
win 4096
23:45:21.349241 XXX.114.201.20.42756 > XXX.234.209.169.13249: F 0:0(0)
win 4096
23:45:21.349678 XXX.114.201.20.42756 > XXX.234.209.169.6571: F 0:0(0)
win 4096
23:45:21.349997 XXX.114.201.20.42756 > XXX.234.209.169.4183: F 0:0(0)
win 4096
23:45:21.350124 XXX.114.201.20.42756 > XXX.234.209.169.26609: F 0:0(0)
win 4096
```

Dump 19 – DMZ SMTP to Internal SMTP Server

```
22:32:14.189100 XXX.234.209.166.smtp > smtp.comcast.net.smtp: S
70080160:70080160(0) win 32120 <mss 1360,nop,nop,sackOK> (DF)
22:32:14.204682 smtp.comcast.net.smtp > XXX.234.209.166.smtp: S
2974489942:2974489942(0) ack 70080161 win 34000 <nop,nop,sackOK,mss
1460> (DF)
```

```
22:32:14.204800 XXX.234.209.166.smtp > smtp.comcast.net.smtp: . ack 1
win 32120 (DF)
```

Dump 20 – 22

Dump 20 – Customer to Customer Database

```
23:08:25.099890 XXX.234.209.165.53258 > 10.0.2.4.postgres: S
483270785:483270785(0) win 4096
23:08:26.230980 XXX.234.209.165.53259 > 10.0.2.4.postgres: S
1496074632:1496074632(0) win 4096
23:08:28.241235 XXX.234.209.165.53260 > 10.0.2.4.postgres: S
1055013047:1055013047(0) win 4096
23:08:29.439021 XXX.234.209.165.53261 > 10.0.2.4.postgres: S
483270785:483270785(0) win 4096
23:08:31.290832 XXX.234.209.165.53262 > 10.0.2.4.postgres: S
1496074632:1496074632(0) win 4096
23:08:35.472358 XXX.234.209.165.53263 > 10.0.2.4.postgres: S
1055013047:1055013047(0) win 4096
```

Dump 21 – Customer to Fortunes Database

```
23:08:55.366280 XXX.234.209.165.53264 > 10.0.2.5.postgres: S
483270785:483270785(0) win 4096
23:08:56.370739 XXX.234.209.165.53265 > 10.0.2.5.postgres: S
1496074632:1496074632(0) win 4096
23:08:58.377614 XXX.234.209.165.53266 > 10.0.2.5.postgres: S
1055013047:1055013047(0) win 4096
23:08:59.388520 XXX.234.209.165.53267 > 10.0.2.5.postgres: S
483270785:483270785(0) win 4096
23:09:01.396882 XXX.234.209.165.53268 > 10.0.2.5.postgres: S
1496074632:1496074632(0) win 4096
23:09:03.404768 XXX.234.209.165.53269 > 10.0.2.5.postgres: S
1055013047:1055013047(0) win 4096
```

Dump 22 – Partner to Fortunes Database

```
23:08:55.366280 XXX.234.209.164.23528 > 10.0.2.5.postgres: S
483270785:483270785(0) win 4096
23:08:56.370739 XXX.234.209.164.23529 > 10.0.2.5.postgres: S
1496074632:1496074632(0) win 4096
23:08:58.377614 XXX.234.209.164.23530 > 10.0.2.5.postgres: S
1055013047:1055013047(0) win 4096
23:08:59.388520 XXX.234.209.164.23531 > 10.0.2.5.postgres: S
483270785:483270785(0) win 4096
23:09:01.396882 XXX.234.209.164.23532 > 10.0.2.5.postgres: S
1496074632:1496074632(0) win 4096
23:09:03.404768 XXX.234.209.164.53269 > 10.0.2.4.postgres: S
1055013047:1055013047(0) win 4096
```

Dump 23 – External to Internal DNS

```
00:39:19.953815 XXX.234.209.166.domain > 10.0.2.6.32805:
54934[|domain] (DF)
00:39:19.954506 10.0.2.6.32805 > XXX.234.209.166.domain:
54935+[|domain] (DF)
00:39:19.965337 XXX.234.209.166.domain > 10.0.2.6.32805:  54935
NXDomain[|domain] (DF)
```

```
00:39:19.965864 10.0.2.6.32805 > XXX.234.209.166.domain:
54936+[|domain] (DF)
00:39:19.975482 XXX.234.209.166.domain > 10.0.2.6.32805:  54936
NXDomain[|domain] (DF)
```

Dump 24 – Deny and Log (DMZ)

```
23:12:57.819293 XXX.234.209.162.46807 > XXX.234.209.161.5516: S
786591601:786591601(0) win 3072
23:12:57.872921 XXX.234.209.162.46807 > XXX.234.209.161.52735: S
786591601:786591601(0) win 3072
23:12:57.889134 XXX.234.209.162.46807 > XXX.234.209.161.13689: S
786591601:786591601(0) win 3072
```

Dump 25 – Remote Employee to Customer Database

```
00:51:55.637960 10.0.3.16.33358 > 10.0.2.4.postgres: S
1722228734:1722228734(0) win 5840 <mss 1460,sackOK,timestamp
128746991[|tcp]> (DF)
00:51:55.638118 10.0.2.4.postgres > 10.0.3.16.33358: S
60201993:60201993(0) ack 1722228735 win 32120 <mss 1360,nop,nop,sackOK>
(DF)
00:51:55.638225 10.0.3.16.33358 > 10.0.2.4.postgres: . ack 1 win 5840
(DF)
```

Dump 26 – Remote Employee to Fortunes Database

```
00:53:01.520909 10.0.3.16.33360 > 10.0.2.5.postgres: S
1790147379:1790147379(0) win 5840 <mss 1460,sackOK,timestamp
128780723[|tcp]> (DF)
00:53:01.521069 10.0.2.5.postgres > 10.0.3.16.33360: S
60267875:60267875(0) ack 1790147380 win 32120 <mss 1360,nop,nop,sackOK>
(DF)
00:53:01.521178 10.0.3.16.33360 > 10.0.2.5.postgres: . ack 1 win 5840
(DF)
```

Dump 27 – Remote Employee to SMTP

```
00:46:30.622852 10.0.3.16.2839 > 10.0.2.6.smtp: S 59877011:59877011(0)
win 32120 <mss 1360,nop,nop,sackOK> (DF)
00:46:30.636744 10.0.2.6.smtp > 10.0.3.16.2839: S
315493436:315493436(0) ack 59877012 win 34000 <nop,nop,sackOK,mss 1460>
(DF)
00:46:30.636857 10.0.3.16.2839 > 10.0.2.6.smtp: . ack 1 win 32120
(DF)...
```

Dump 28 – Remote Employee to POP3

```
00:48:37.315626 10.0.3.16.2845 > 10.0.2.6.pop3: S 60003698:60003698(0)
win 32120 <mss 1360,nop,nop,sackOK> (DF)
00:48:37.328809 10.0.2.6.pop3 > 10.0.3.16.2845: S
2558704105:2558704105(0) ack 60003699 win 34000 <nop,nop,sackOK,mss
1460> (DF)
00:48:37.328939 10.0.3.16.2845 > 10.0.2.6.pop3: . ack 1 win 32120
(DF)...
```

Dump 29 – 30 Remote Employee to DNS

Dump 29 – Remote Employee to Internal DNS

```
00:37:54.252707 10.0.3.16.2813 > 10.0.2.6.domain:  1+[|domain]
00:37:54.266914 10.0.2.6.domain > 10.0.3.16.2813:  1[|domain] (DF)
```

Dump 30 – Remote Employee to DMZ DNS

```
00:39:19.935114 10.0.3.16.2818 > XXX.234.209.166.domain:  2+[|domain]
00:39:20.020521 XXX.234.209.166.domain > 10.0.3.16.2818:  2*
2/2/2[|domain] (DF)
```

Dump 31 – 32 Remote Employee SSH to Websites

Dump 31 – Remote Employee SSH to customer.giac.com

```
00:12:36.445386 10.0.3.16.2999 > customer.giac.com.ssh: S
71272440:71272440(0) win 32120 <mss 1360,nop,nop,sackOK> (DF)
00:12:36.445560 customer.giac.com.ssh > 10.0.3.16.2999: S
631456727:631456727(0) ack 71272441 win 5840 <mss 1460,nop,nop,sackOK>
(DF)
00:12:36.445692 10.0.3.16.2999 > customer.giac.com.ssh: . ack 1 win
32120 (DF)...
```

Dump 32 – Remote Employee SSH to partner.giac.com

```
00:15:30.074400 10.0.3.16.3000 > partner.giac.com.ssh: S
71285069:71285069(0) win 32120 <mss 1360,nop,nop,sackOK> (DF)
00:15:30.074519 partner.giac.com.ssh > 10.0.3.16.3000: S
640821470:640821470(0) ack 71285070 win 5840 <mss 1460,nop,nop,sackOK>
(DF)
00:15:30.074643 10.0.3.16.3000 > partner.giac.com.ssh: . ack 1 win
32120 (DF)
00:15:30.083197 partner.giac.com.ssh > 10.0.3.16.3000: P 1:23(22) ack 1
win 5840 (DF)
00:15:30.271865 10.0.3.16.3000 > partner.giac.com.ssh: . ack 23 win
32098 (DF)...
```

Dump 33 - Syslog (VPN to PIX)

```
21:29:10.246245 XXX.234.209.177.3426 > XXX.234.209.162.syslog: udp 6
21:29:11.527851 XXX.234.209.177.3427 > XXX.234.209.162.syslog: udp 6
21:29:26.456200 XXX.234.209.177.3428 > XXX.234.209.162.syslog: udp 7
21:29:27.796080 XXX.234.209.177.3429 > XXX.234.209.162.syslog: udp 7
```

Dump 33a - Syslog (From the DMZ)

```
21:29:10.812547 XXX.234.209.177.3426 > XXX.234.209.162.syslog: udp 6
21:29:11.972871 XXX.234.209.177.3427 > XXX.234.209.162.syslog: udp 6
21:29:26.712439 XXX.234.209.177.3428 > XXX.234.209.162.syslog: udp 7
21:29:28.114538 XXX.234.209.177.3429 > XXX.234.209.162.syslog: udp 7
```

Dump 34 – NTP (VPN to PIX)

```
22:01:55.134063 XXX.234.209.177.ntp > XXX.234.209.172.ntp:  v4 client
strat 0 poll 4 prec -6 (DF)
22:01:55.135948 XXX.234.209.172.ntp > XXX.234.209.177.ntp:  v4 server
strat 1 poll 4 prec -18 [tos 0x10]...
```

Dump 34a – NTP (PIX to DMZ)

```
22:01:55.136063 XXX.234.209.177.ntp > XXX.234.209.172.ntp:  v4 client
strat 0 poll 4 prec -6 (DF)
22:01:55.136148 XXX.234.209.172.ntp > XXX.234.209.177.ntp:  v4 server
strat 1 poll 4 prec -18 [tos 0x10]...
```

Dump 35 – 36 ACE/Server

Dump 35 – ACE/Server – [VPN Network]

```
00:14:16.120865 XXX.114.201.20.2743 > XXX.234.209.173.5500: udp 124
00:14:16.121316 XXX.234.209.173.5500 > XXX.114.201.20.2743: udp 124...
```

Dump 35a – ACE/Server – [Customer Service Network]

```
00:16:31.942086 XXX.234.209.177.3905 > 10.0.2.7.5500: udp 124
00:16:31.989721 10.0.2.7.5500 > XXX.234.209.177.3905: udp 124...
```

Dump 36 – ACE/Server – [VPN Network]

```
00:14:16.129878 XXX.114.201.20.2749 > XXX.234.209.173.5500: udp 124
00:14:17.146527 XXX.234.209.173.5500 > XXX.114.201.20.2749: udp 124...
```

Dump 36b – ACE/Server – [Customer Service Network]

```
00:16:32.019222 XXX.114.201.20.3946 > 10.0.2.8.5500: udp 124
00:16:32.034533 10.0.2.8.5500 > XXX.114.201.20.3946: udp 124...
```

Dump 37 – (Testing Deny All) SYN Scan on PIX from VPN Concentrator

```
20:51:37.413647 XXX.234.209.178.46807 > XXX.234.209.177.55318: S
786591601:786591601(0) win 3072
20:51:37.413788 XXX.234.209.178.46807 > XXX.234.209.177.54735: S
786591601:786591601(0) win 3072
20:51:37.413889 XXX.234.209.178.46807 > XXX.234.209.177.39689: S
786591601:786591601(0) win 3072
```

Dump 37a – Connect Scan on PIX from VPN Concentrator

```
20:49:58.022535 XXX.234.209.178.2183 > XXX.234.209.177.23294: S
45673765:45673765(0) win 32120 <mss 1360,nop,nop,sackOK> (DF)
20:49:58.022742 XXX.234.209.178.2184 > XXX.234.209.177.3743: S
45673765:45673765(0) win 32120 <mss 1360,nop,nop,sackOK> (DF)
20:49:58.022941 XXX.234.209.178.2185 > XXX.234.209.177.45527: S
45673765:45673765(0) win 32120 <mss 1360,nop,nop,sackOK> (DF)
```

Dump 37b – UDP Scan on PIX from VPN Concentrator

```
20:48:23.692279 XXX.234.209.178.50065 > XXX.234.209.177.18277: udp 0
20:48:23.692436 XXX.234.209.178.50065 > XXX.234.209.177.33020: udp 0
20:48:23.692542 XXX.234.209.178.50065 > XXX.234.209.177.11282: udp 0
20:48:23.692645 XXX.234.209.178.50065 > XXX.234.209.177.38201: udp 0
```

Dump 37c – FIN Scan on PIX from VPN Concentrator

```
20:42:35.578841 XXX.234.209.178.39739 > XXX.234.209.177.60075: F 0:0(0)
win 4096
20:42:35.578981 XXX.234.209.178.39739 > XXX.234.209.177.18982: F 0:0(0)
win 4096
20:42:35.579091 XXX.234.209.178.39739 > XXX.234.209.177.7971: F 0:0(0)
win 4096
20:42:35.579191 XXX.234.209.178.39739 > XXX.234.209.177.42283: F 0:0(0)
win 4096
20:42:35.579299 XXX.234.209.178.39739 > XXX.234.209.177.36609: F 0:0(0)
win 4096
```

Dump 38 – ISP DNS to DMZ DNS

```
16:35:17.590056 XYZ.12.12.14.33228 > XXX.234.209.166.domain: S
3562218001:3562218001(0) win 5840 <mss 1460,sackOK,timestamp
69149026[|tcp]> (DF)

16:35:17.590210 XXX.234.209.166.domain > XYZ.12.12.14.33228: S
3128929:3128929(0) ack 3562218002 win 32120 <mss 1360,nop,nop,sackOK>
(DF)

16:35:17.590311 XYZ.12.12.14.33228 > XXX.234.209.166.domain: . ack 1
win 5840 (DF)

16:35:17.596891 XXX.234.209.166.domain > XYZ.12.12.14.33228: P 1:65(64)
ack 1 win 32120 12333 notify$ [21037a] [22337q] [18004n]
[20548au][|domain] (DF)...
```

Dump 39 – 41 External NTP Server to Internal NTP Server

```
16:44:15.163711 XXX.234.209.162.ntp > XW0.162.8.3.ntp:  v4 bcast strat
3 poll 6 prec -6 (DF)
16:44:15.163778 XXX.234.209.162.ntp > XZ6.200.93.8.ntp:  v4 bcast strat
3 poll 6 prec -6 (DF)
16:44:15.181150 XW0.162.8.3.ntp > XXX.234.209.162.ntp:  v4 bcast strat
3 poll 6 prec -18 [tos 0x10]
16:44:15.186429 XZ6.200.93.8.ntp > XXX.234.209.162.ntp:  v4 bcast strat
3 poll 6 prec -18 [tos 0x10]
16:44:15.364820 XXX.234.209.162.ntp > X8.82.161.227.ntp:  v4 bcast
strat 3 poll 6 prec -6 (DF)
16:44:15.377348 X8.82.161.227.ntp > XXX.234.209.162.ntp:  v4 bcast
strat 3 poll 6 prec -18 [tos 0x10]...
```