Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst (GCFW) Practical Assignment

Version 1.9 (revised January 20, 2002)

Lin Zhu

Abstract

This paper introduces the GIAC enterprise – a future cookie saying company, analyzes its e-commerce business requirements and provides a network security architecture solution. After fully investigated the access restriction, it proposals a front end to back end network components design, particularly chooses CISCO 3620 as a border router and PIX 515E as a primary firewall and VPN terminator. In the second chapter, it illustrates the security policies for key devices and provides a detailed tutorial on how to set up a PIX. Furthermore, a lab is set up to prove its concept and verify the firewall policies. Based on the audit results, it makes couple recommendations. At the end of the paper, it chooses Kent Scott's design to launch three attacks in order to prove the author's knowledge of the threats in current Internet world.

Chapter 1: Assignment 1 - Security Architecture

1.1 About Fortune Company

GIAC enterprise is a global provider of fortune cookie sayings. It develops, designs, manufactures and trades sayings in various languages and styles, and owns about 90% of sayings market share. The company has about 100 employees, 50 international sales partners and 10 suppliers.

Last year's revenue exceeded 10 million Canadian dollars thanks to the newly launched online web transaction applications. The new web applications not only allow a retail customer order sayings online, but also provide an interface for business partners and suppliers to access GIAC's inventory and ordering system.

The detailed business operation modules are discussed in the next section. Particularly, we will emphasise on the access requirements form different type of customers.

1.2 E-business requirements

Retail customers

Companies or individuals could purchase and order bulk fortunes either through a secured portal http://www.giacsayings.com or through traditional methods such as fax, phone, letter or e-mail.

The online ordering system allows customers to register themselves on the site and create a profile. Information that is typically required from a customer includes name, shipping address, contact information, purchase status, and the identity with GIAC in the form of username and password. Comparing with the amount of the saying trade involved and the amount for Internet security investment, GIAC decided not to contain any customer's credit card information. Online payment is accepted through PAYPAL. If a customer doesn't want to enter credit card number on each transaction, he could set up a pre-approved merchandize account with sales representative and get charged after purchase.

Anonymous users could browse company's catalog and general information through unsecured HTTP web pages. When a customer wants to purchase something or check his ordering status, he needs to enter his username and password. After a user enters his password, server will send back its certificate to start the SSL authentication handshake. After the negotiation, any data is encrypted before sending and decrypted before being used. The integrity of the data is also confirmed.

There are two way of shipment. Clients either could order per-made saying through Canada Post, or download image via web (HTTPS) and print themselves later.

GIAC uses Apache web server, JBOSS framework based J2EE application server and Oracle backend database. Communication between the web server and application server runs on TCP port 7000.

From above analyze, we understand that HTTP (port 80/tcp) and HTTPS (port 443 /tcp) services on the web server have to be opened to external retail customers to allow them to access company's web pages. Also, the web server needs to talk to internal application server. In GIAC, application server port 7000/tcp is bind to listen to requests from the web sever. We need to permit traffic from web server to internal application server on that port. Please see detailed access requirement at section 1.5, and the web server requirement at section 1.4 pages 14-16.

Partners

International companies that translate and resell fortunes will access the same web page http://www.giacsayings.com as retail customers. In that web page, there is a special link connecting to partner's secured web instance https://partners.giac.com. Users are required to be authenticated through RSA secure ID tokens. (GIAC will provide RSA tokens to each partner). Since partners have privileges to change the company's database, GIAC believes it is necessary to implement this extra security measure.

After authentication, a secured http tunnel is setup between partner and server through SSL. Through this secured link, a partner could access sayings database with lot of flexibility, he could check sayings' retail and wholesale price, download designs and upload translated image, or delete obsolete units for that region. Upload is only allowed through cutting and paste or through gif format files. Furthermore, the system also allows partners to check the inventory and ordering database so that they could know their custom better and translate/resell more best-selling designs. Finally, like retail clients, partners could finish their purchase online. They have choices either to download image via HTTPS protocol and print locally, or specify the design, language and format, and then ask GIAC to make them and ship to different resell locations. Their payments will use traditional billing method and clear with GIAC once a month.

On GIAC's web server, there is another web component which is specially designed for this B2B application. Its responsibility is to authenticate RAS user, assign different privilege levels to different partners and produce dynamic web information accordingly. B2C and B2B system will share the same application server and oracle database to increase the components reusability and simplicity. The connection between the web server to internal application server is also through TCP protocol port 7000.

For partners, besides the same access requirement as retail customers, traffic from web server to internal RSA server port also need to be permitted for token authentication.

RSA server port 8000/tcp is opened to answer the query for user authentication. Firewall should allow request from web server to RAS server port 8000/tcp. Please see section 1.5 for detailed description.

Business partners could also use traditional methods to conduct business through phone, fax or e-mail.

Having a dedicated lease line or VPN connection between partners and GIAC network not only cost dollars, but also increase the complexity of the design. Most international partners have only one to two sales representatives. The web service should provide them enough functionality and security.

Suppliers

For people who supply GIAC enterprises with their fortune cookie sayings, they access GIAC web portal the same way as partners do through https://partners.giacsayiings.com.

However, after RSA authentication, they will gain different user privilege as of partners'. Through SSL tunnel, a supplier could check inventory and ordering database to decide its production direction, upload new image and design, change old sayings' design or delete the unpopular ones. Of course, a supplier could only view/change/delete his own designs. Upload is only allowed through cut and paste or through gif format files.

The web component used for partners is also suitable for suppliers. Both partners and suppliers accounts are pre-defined by GIAC. In oracle database, their access permission (read, writer and delete) to different sayings is clearly stated. Web component on the web server will use this list dynamically produce corresponding web content.

On the other side, GIAC will connect to suppliers through suppliers' business-to-business web services. By this, GIAC could access supplier's catalogue database, make purchase and track the shipping and payment status. That again is through secured HTTP channel to suppliers' web portal. This traffic could be treated as part of the internal traffic.

Above all, there will be no extra access requirement particularly for suppliers through firewall.

Internal users

GIAC enterprise is located in Toronto. Employees at head office need to access to the Internet to send e-mail, browse web, host web-conferencing, access external suppliers web services and download business related documentations.

To improve the security and performance, GIAC employees will not have direct access

to the Internet; instead they will have to go through various application proxies first. For messaging, all the incoming mail will first be examined by a mail server sits at DMZ. This mail server will not only have anti-Spam and anti-rely function, but also has mailwash function built in to block the possible malicious attachment and virus. After external mail server's filtering, the messages will be forwarded to internal mail server and then delivered to users. Outgoing mail will take the reverse path. Mail transaction between internal and external mail server uses protocol SMTP (port 25/tcp). Detailed mail servers requirement please see section 1.4 page15.

For web browsing and streaming application (video/audio application), internal users access a web proxy first (through proxy server port 8080/tcp). The proxy sever then goes to the Internet to retrieve the content. This way the accessible websites are monitored and restricted, and also saved the bandwidth should more then 2 users accessing the same source. Certain MIME types such as .exe are prohibited. Ftp download also trough the same proxy on port 8079/tcp. To access this proxy instance, user authentication is required. This instance also provides unrestricted http access to the Internet for administration purpose. This way the downloads are scanned and controlled. Detailed proxy servers requirement please see section 1.4 page15.

If an internal user wants to query a public DNS name, the query will first send to a internal DNS server and then forward to the external DNS on DMZ. ExDNS then retrieves the answer from Internet. ExDNS is also authoritative for public domain giacsayings.com. The public query traffic to ExDNS for that domain should be allowed. Port 53/udp is used to transfer DNS information. Detailed DNS server's analysis also sees section 1.4 page16.

Section 1.5 gives out the detailed technical specification for access list.

Mobile users

Mobile sales person and telecommuter are required to use VPN clients to access corporate network. In the future, GIAC will set up VoIP through VPN and move office phone number to users' remote desktop. Mobile users will gain Internet access through cell phone data modem (or air card) connection and then use VPN to access corporation LAN.

Cisco VPN client 3.6 will be used as client software. Client authentication is through RSA Ace/Server and RSA SecurID combination. After a VPN client gains permission, he enjoys the same network privilege as an internal user does in the head office.

All the remote desktops are required to have latest personal firewall and anti-virus software installed.

1.3 Architecture

From above business requirements and budget restraint, GIAC designed a network as showed in Figure 1-1.

Network Address Schema

Public Address: 205.205.205.0/24
DMZ zone: 192.168.1.0/24
Touchdown segment: 192.168.0.0/24
Internal Server: 192.168.30.0/24
Internal Desktop: 192.168.40.0/24
VPN client virtual internal ip: 192.168.20.0/24

Public addresses and ISP's IP are imaginary IPs used here for demonstration purpose.

NAT Table For PIX Firewall:

	NAT	REAL
WebSvr	205.205.205.30	192.168.1.30
ExDNS	205.205.205.40	192.168.1.40
ExMailSvr	205.205.205.10	192.168.1.10
SysLog Svr	205.205.205.11	192.168.1.50
VPN Partner	205.205.205.50	192.168.30.50
InMailSvr	192.168.1.110	192.168.30.10
AppSvr	192.168.1.112	192.168.30.12
RSASvr	192.168.1.116	192.168.30.16

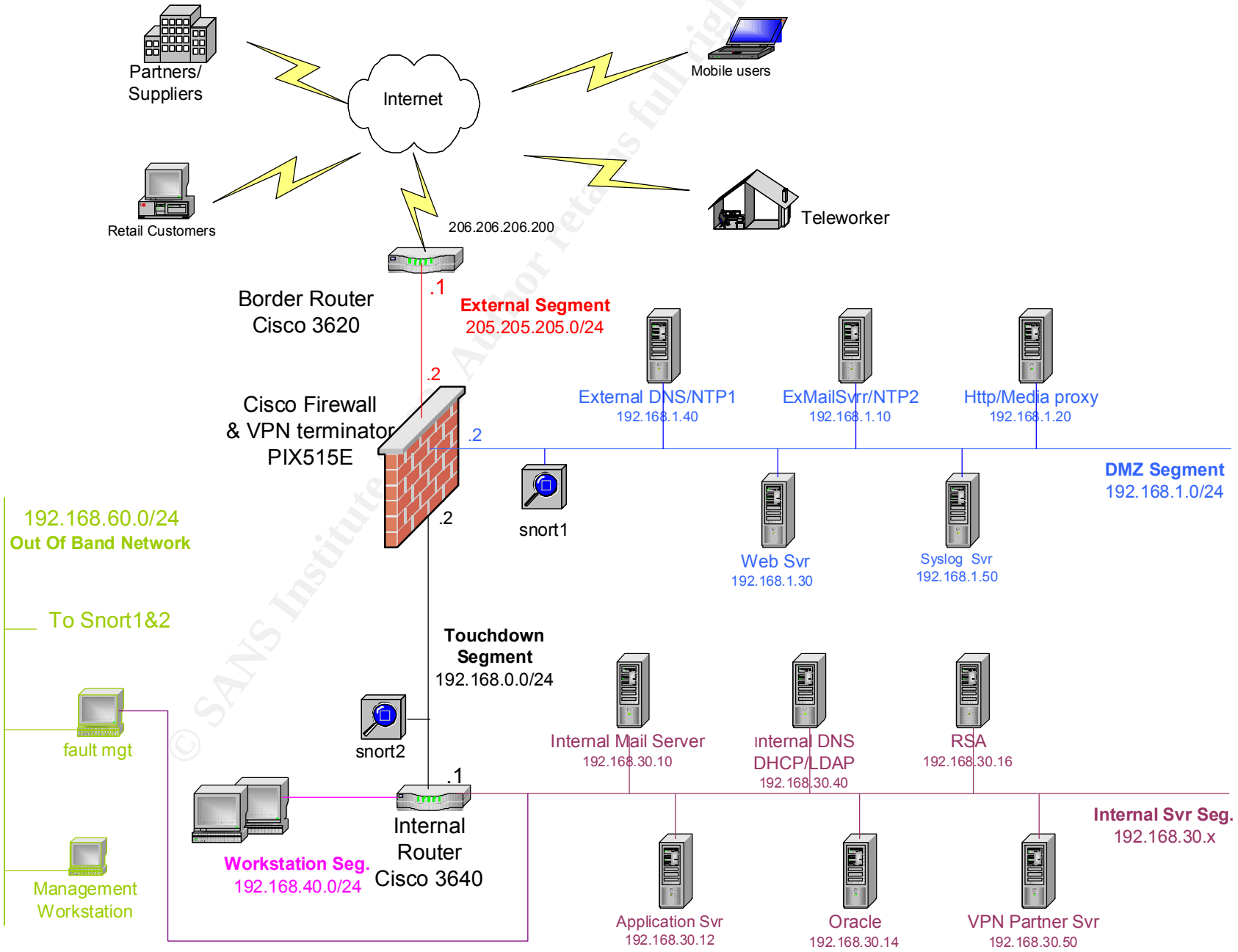


Figure 1-1 GIAC NETWORK DIAGRAM

The following is the consideration that GIAC faced during the design period.

Redundancy and High Availability

Site redundancy is not in the scope of this phase of the design.

Due to the nature of the business, overall application availability level is not required as high as that of e-banking or other online web transaction applications. If the network is down, customers and partners can still call/fax to purchase or check the order.
All the crucial devices such as border router, switch and pix will have gold contract with Cisco. The four-hour hardware turn around time should be sufficient to the current business requirement.

In the future, if there is a need to realize five nine up time, GIAC could easily add a backup firewall into the current design. Not only will Cisco provide up to 60% of discount for second unit, but also after the release 6.2, new LAN fail over feature expends the peers' physical distance which makes site redundancy feasible financially and physically. (Prior to Ver6.2, serial cable is the only choice).

GIAC could also consider using HSRP (Hot standby Redundancy Protocol) to provide redundancy between two dual homed BGP routers. This solution not only provides site redundant, but also dramatically improves the network up time, in the event of connectivity failure towards one ISP, the traffic will be rerouted dynamically to another backup ISP.

Load Balancing

From current traffic profile analyzing and business requirement, GIAC doesn't require load balancing at network level. Current design should be sufficient for GIAC's business growth in the next 3-5 years. (Assuming the network volume increases at 10% per year). Load balancing will only introduce the complexity, not to mention the initial capital cost.

However, it is required to have clustering architecture for application servers, such as web servers, mail servers, database servers to improve the performance.

Demilitarized Zone Firewall Architecture

Even GIAC web application will not contain any credit payment information. To protect privacy of customer's information and fortune sayings' design, and also to mitigate the threats coming from the Internet, GIAC still need a media-level security strategy to protect its internal network. Three-layer firewall architecture is the best fit for GIAC. It is relatively easy to setup with one PIX. All the servers which have direct Internet exposure, will be placed on an separated DMZ zone. In the case of penetration or

attack, the internal network is still protected.

All the servers on DMZ zone have only minimal packages installed with the latest patch updates. Also it is required to have tcp wrapper and netfilter installed. As a rule of thumb, all the unnecessary services such as finger, who, telnet, ftp, rpc will be disabled. Remote management is done through openSSH. Those countermeasures don't require any extra dollars; nevertheless they enhance the overall security features.

Network Management and IDS

PIX has no build-in storages for loggings. On DMZ zone, GIAC needs to build an external syslog server. Firewall logging is the base for intrusion detection. Since building a syslog server is an unavoidable process, it makes sense to consolidate other logs from devices (border router, and servers in DMZ zone) into one big logging server. Having a centralized syslog system not only reduces administration overhead, but also helps administrators to be able to pin-point problems faster. Administrators could also pre-set certain filter rules; if the criteria are met, the system can send an SNMP trap to fault management console.

For GIAC's internal network, an Out of Band Network should be build. It will make management and troubleshooting extremely easy. Especially for fault management, in the case of network breakdown, administrators will still have immediate access to network devices. Detailed discussion on network management is out of the scope of this paper. Briefly, GIAC uses free SNMP monitoring tools such as Scotty or Mrtg for fault management. Monitored objects should include not only network devices but also all the critical application servers. SNMP is the key technology for network management; however, SNMPv1 has been reported with lot of vulnerability.[1] To minimums the risk, GIAC will choose version 2, in the future upgrade to SNMPV3 when it becomes mature. V3 supports authentication and secured tunnel communication. Default community string should be changed.

Intrusion detection system should also be built in this network. GIAC could use snort as a real-time traffic analyzer and packet-logging tool for security and troubleshooting purposes. The caveat of IDS is that it's easy to setup, but requires consistent monitoring and tuning. Otherwise, it is just another piece of furniture in the computer room.

Centralized Backup

No need to mention how important the backup is for operations. Even through the initial set up for a centralized backup requires an administrator's huge amount of effort; however, since all the jobs can be scheduled, the real operation after setup is actually brain-less. GIAC installed a centralized backup ARKEIA server in internal network with

[1] http://www.cert.org/advisories/CA-2002-03.html

a DLT library. ARKEIA will backup multi favored OS. Configuration files on DMZ Servers will be sftped (secured ftp, one feature of secure shell) to backup server first.

1.4 Network Components

Not only has Cisco a huge range of high quality products to chose from, it also has superior after-sale support and services. Taking the current IT staff 's knowledge into consideration, GIAC chose Cisco products as its border router and firewall. GIAC's existing network devices are all from Cisco; learning curve for staff should be relatively low if devices are from the same vendor. At the rest of the section, we will examine each component in details, give out the hardware and software specifications, and the reasons why that's the best choice for GIAC's enterprise.

Connection to ISP

GIAC will use LAN Extension - Ethernet 3Mbps.
Public IP: 205.205.205.0/24

From GIAC premise to ISP the connection is standard LAN interfaces. This setup doesn't require WAN technology, which is welcomed by GIAC staff since they are already familiar with LAN configurations. Furthermore, in the future, if GIAC ever needs to increase the gateway bandwidth, they could simply increase to 4M, 5M up to 100M without hardware change. Current investments (both capital and knowledge) get protected.

From analysis in session 1.3, 3Mbps full-duplex connection should meet current traffic requirement and the volume growth within the next three years. (Estimated peek traffic in and out: 1M from internal, 1M for partners and 1M from e-customer).

Border Router

Hardware: Cisco 3620 with 1 NM-4E (Four ports Ethernet Network Module) Card.
Software: Cisco IOS 12.2(12a) Enterprise Plus: c3620-jk8o3s-mz.122-12a.bin
ENTERPRISE/FW/IDS PLUS IPSEC 56
IP: 205.205.205.1 (Interface facing internal)
206.206.206.200 (interface connecting to ISP)

The list price for Cisco3620 and 2620 are almost same; however, 3620 can process packets at 40 kilo-packets per second while 2620 has only about half of the capacity. GIAC will choose 3620 as its border router gateway to the Internet.

Firewall/VPN

Hardware: Cisco PIX515E with one PIX-4FE (four ports 10/100 Fast Ethernet interface) card.
Software: Version 6.3

IP: 205.205.205.2 (interface connecting to border router)
192.168.0.2 (interface connecting to internal campus network)
192.168.1.2 (interface connecting to DMZ)

GIAC would like to use some appliance type of firewall. Software firewalls not only have speed issue (even though it is not a big issue under GIAC's traffic pattern), but also require a lot of administration overhead for underlying OS. Besides firewall software, administrators have to consistently patch and upgrade the Operation System which obviously will double IT department's load. From current market available appliances (such as Cyberguard, PIX, Netscreen), GIAC chooses PIX515E for the good cost/performance rate. PIX515E has 200M processor with 64M memory; up to 6 network interfaces and can handle 26000pkcts/sec (120Mbs throughput). It has all the features that GIAC looks for, stateful inspection firewall with application awareness, build-in VPN acceleration and wired speed. Moreover, PIX's similar look and feel with other Cisco devices is easy for GIAC's staff to master comparing with other appliances.

515E will also function as a VPN terminator. Considering the volume passing through the firewall, there should be no performance issues by using 515E as a firewall and VPN terminator at the same time.

Internal Router

Hardware: Cisco 3640 with 1 NM-4E (Four ports Ethernet Network Module) Card.
Software: Cisco IOS 12.2(12a) Enterprise Plus: c3620-jk8o3s-mz.122-12a.bin
ENTERPRISE/FW/IDS PLUS IPSEC 56
IP: 192.168.0.1 (Interface connecting to PIX)
192.168.40.1 (interface connecting to workstation segment switch)
192.168.30.1 (interface connection to server segment switch)

Use layer 3 instead of layer 2 MPLS architecture could improve the overall campus network stability. From security point of view, it also improves the network safety. End users' desktops are very easily infected by worms or virus. If servers are separated from workstation network, even the workstation network is under attacked by virus such as Code Red, the connection between servers network to external network is still unaffected. It is also easier for administrator to contaminate the impact in certain network by blocking the malicious traffic through the router. Internal router also blocks chatty NetBios traffic leave the internal network.

Server

Hardware: Intel based server type
Software: Linux Redhat 8.0
Internal Severs sit at Network 192.168.30.0/24
External DMZ servers sit at Network 192.168.1.0/24

GIAC's web applications are JBOSS framework based J2EE application servers. All the servers sit on Linux Redhat distribution platform. By using Linux distribution on INTEL architecture, GIAC could save huge amount of OS license fee and hardware cost. It also enjoys a lot of free open source applications.

All internal servers will be able to access DMZ servers through openSSH. Servers in DMZ zone have only the minimal OS packages installed with the latest patch updates. Tcp wrapper and netfilter are the mandatory packages. Unnecessary services such as finger, who, telnet, ftp, rpc will be disabled.

Only explicit outgoing traffic from DMZ is allowed. The Internet exposed servers such as web server, external mail relay and proxy server will have build in netfilter to act as second layer defense in depth protection.

Mail Server

Software: SendMail8.12.7
Internal mail server: 192.168.30.10
External mail relay: 192.168.1.10

Extra layer of mail relay sever will enhance the overall security of messaging system. It sets up an extra barrier between external and internal network. GIAC will setup mailwash system on external mail server to filter out the virus, suspicious attachment file and SPAMed messages. Internal mailing system uses LDAP for user authentication.

Proxy Server

Software: Squid2.5
IP: 192.168.1.20

The proxy server will have two instances. One is filtered for general users. Ftp is disabled; and for http and https, it will block certain MIME file types such as .exe or .bin to enhance the security. Another instance has no filtering which is for administration purpose. FTP is enabled and user authentication is required. Only small amount of people have privileges to download which limits the possible Trojan and virus download.

Public Web Server

Software: Apache 2.0.40
IP: 192.168.1.30

Web server will use clustering technology to provide load balance and redundancy. In ideal situation, all the web traffic should go through reverse proxy first to improve the security and performance. Nevertheless, the initial setup should satisfy GIAC's requirements. Web server will communicate with internal application server through port

7000/tcp. Also for partners' web authentication, it needs to talk with RSA server on port 8000/tcp.

Domain Name Server

Software: BIND 9.2.1
Internal DNS: 192.168.30.40
External DNS: 192.168.1.40

GIAC will have spilt DNS setting. External DNS only answers query for its public domain -- giacsayings.com; and it is non-recursive to prevent BIND buffer overflow vulnerabilities. It only allows zone transfer from GIAC ISP, since GIAC use their DNS as secondary to increase the availability. Internal DNS only answers query form internal network.

NTP servers

Two NTP servers sit on DMZ will synchronize with 3 external public NTP servers. In turn, the rest of DMZ servers and all internal servers/desktops will sync with those two.

On OBN, there will have one NTP server too; however, this NTP only sync with its own machine clock and provides relative correct time to OBN.

RSA Server

Software: RSA ACE/Server 5.0
IP: 192.168.30.16

The combination of ACE/Server(Agent) and SecurID tokens provide two-factor authentication method.

RSA ACE/Server will be hided well in Internal network and should be hardened as DMZ servers.

Intrusion Detection Servers

Software: Snort 1.9
IP: 192.168.60.21
192.168.60.22

Snort is a very good traffic analyzer and packet-logging tool. Two snort severs will be placed. One connects to DMZ and the other connects to touchdown internal network. The interfaces connecting to monitored networks will be set at promiscuous mode without ip address and arp updates. Those interfaces will be connected to switches' mirrored ports so that all the traffic on those vlans could be monitored.

LDAP

Software: openLDAP2
IP: 192.168.30.40

GIAC uses openLDAP as single point sign-on solution. LDAP co-exists with DNS and DHCP server.

Database

Software: Oracle9i
IP: 192.168.30.14

Access to Human Resource and Web Client database' should be restricted at least at database level by using user accounts and different privilege levels.

File Sharing

Software: Samba
IP: 192.168.30.15

GIAC will setup a big samba server to host internal users home directory and other common applications. This way all the users have only one home directory no matter which platform they choose to use.

Backup

Software: ARKEIA
IP: 192.168.30.17

ARKEIA is a multi-platform network backup utility.

Desktop (including telecommuter's desktop)

Hardware: Intel based Desktop PC
Software: Windows2000 with Norton antivirus installed
IP: 192.168.40.0/24

Remote desktop will also install personal firewall such as ZoneAlarm or BlackIce, and remote access software VPN client 3.6.

1.5 Access requirements in detail

The detailed business analysis please sees section 1.2.

- Public Web server

  HTTP (port 80/tcp) and HTTPS (port 443 /tcp) services on the web server have to be opened to external retail customers to allow them access company's web page. Internal web application server listening on port 7000/tcp. Since the web server needs to talk to internal application server, traffic from web server to internal application server port 7000/tcp needs to be permitted, too. For partners and suppliers RSA authentication, traffic from web server to internal RSA server port 8000/tcp also needs to be allowed.

Application	Port	Destination	Source
HTTPS	443/tcp	WWW (205.205.205.30)	External Any
HTTP	80/tcp	WWW (205.205.205.30)	External Any

Public web server to internal servers

Application	Port	Destination	Source
TCP	7000/tcp	Appsvr(192.168.30.12)	WWW(192.168.1.30)
TCP	8000/tcp	RSA(192.168.30.16)	WWW(192.168.1.30)

- Proxy server

  There are two proxy instances. One listens on port 8080/tcp, provides strict access for general internal users. Another listens on port 8079/tcp, provides unrestricted access to internet (including ftp download). Internal users need to access both ports. This proxy server on DMZ requires unlimited access to the Internet.

Application	Port	Destination	Source
Proxy (secured)	8080/tcp	Proxy (192.168.1.20)	Internal all
Proxy (Unsecured)	8079/tcp	Proxy (192.168.1.20)	Internal all
ALL	ALL	External ALL	Proxy (192.168.1.20)

- Mail Server

Messages transacted between mail servers uses protocol SMTP (port 25/tcp). Mail server on DMZ zone (ExMailSvr) should be able to accept mails from Internet and send mails to any public mail servers. Internal mail server (InMailSvr) should be permitted to talk with ExMailSvr on port 25/tcp and vers-versa.

Application	Port	Destination	Source
SMTPIncoming	25	ExMailSvr(205.205.205.10)	External ALL

SMTPoutgoing	25	External ALL	ExMailSvr(205.205.205.10)
SMTP relay	25	ExMailSvr(192.168.1.10)	InMailSvr(192.168.30.10)
SMTP relay	25	InMailSvr(192.168.30.10)	ExMailSvr(192.168.1.10)

- DNS

  DNS server sits on DMZ (ExDNS) answers query for its authoritative domain – giacsayings.com. Firewall has to allow everybody access port 53/udp on ExDNS. UDP can only carry less then 512 bytes answer, for any bigger size query, TCP protocol has to be used. Giacsayings.com domain will not contain any record longer then 500bytes, UDP protocol should be sufficient.

  Since GIAC's ISP is also ExDNS's secondary, zone transfer has to be allowed from ISP DNS to ExDNS (on port 53, protocol tcp).

Application	Port	Destination	Source
DNS	53/udp	ExDNS(205.205.205.40)	External all
DNS	53/tcp	ExDNS(205.205.205.40)	ISP(206.206.206.31)

  If an internal user wants to query a public DNS name, the query will first send to an internal DNS server and then forward to the external DNS on DMZ. ExDNS then retrieves the answer from Internet. From DMZ to External network, ExDNS should be allowed query public DNS servers through Internet both on tcp and udp.

Application	Port	Destination	Source
DNS	53/udp&tcp	External all	ExDNS(192.168.1.40)
DNS	53/udp&tcp	ExDNS(192.168.1.40)	Internal all

- NTP

  In order to synchronize the time, GIAC will adjust its time with three public time servers through NTP protocol. NTP uses port 123/udp.

Application	Port	Destination	Source
NTP	123/udp	ExDNS(205.205.205.40) ExMailSvr(205.205.205.10)	Public NTP server 199.212.17.34 128.100.102.201 142.3.100.15

- ICMP

  ICMP is useful but also a little evil which could be used as mapping and DoS attack tool. It has to be handled carefully. ICMP between external network and

DMZ/internal is strictly blocked except limited error messages such as packet-too-big to allow ensure the traffic flow quality. ICMP between DMZ and internal zone should be permitted for troubleshooting.

Ping from ISP's edge router to GIAC's border router should also be permitted for ISP monitoring and troubleshooting purpose.

Application	Permission	Destination	Source
ICMP packet-too-big Time-exceeded	permit	DMZ	External all
ICMP	Deny	Internal	External all
ICMP	Permit	Internal	DMZ
ICMP	Permit	DMZ	Internal
ICMP	Permit	Border router (205.205.205.1)	ISP edge router (206.206.206.10)

- Border Router Network Management

Manage the border router is a trick business. PIX should allow syslog information to be sent from router to the syslog server. That information is sent in the clear text. GIAC believes the chance that someone will sit between the router and PIX to sniff the packet is remotely possible. Rather, GIAC wants to take the risk to monitor the router's health and collect logging information.

For router management SSH is used for remote secure access. It is only allowed SSH from syslog server.

Application	Permission	Destination	Source
Syslog (514/udp)	Permit	NetMgt Svr (205.205.205.11)	Border Router (205.205.205.1)
SSH(22/tcp)	Permit	BorderRouter (205.205.205.1)	NetMgt Svr 192.168.1.50)

Chapter 2: Assignment 2 - Security Policy and Tutorial

2.1 Border Router

Border router will do some basic filtering and spoof mitigation, but its main function is to pass packets as fast as possible. IOS12 has firewall and IDS features built in. Those features; however, require a lot of CPU and memory power. In this design, PIX and snort are used to fulfill those functions.

Border router also sends logs to the syslog server on DMZ for central logging and monitor purpose. GIAC would like to know what happens to the router, what kind of traffic passes through, and get alerts if something goes wrong. Syslog server will install a simple netfilter firewall, which only allows the syslog connection from the router.

Set up encrypted enable secret

```
service password-encryption
enable secret "realpasswd"
```

VTY Security

Even passwords that are encrypted in the configuration are not encrypted on the wire as an administrator type the password. Thus GIAC will use ssh as remote access method to manage router itself. Who can access to vty should also be controlled. Only connections from syslog management console are allowed to access router directly. (205.205.205.11 is Nat ip address for network management console 192.168.1.50).

```
 crypto key generate rsa                    ←Enable SSH
access-list 1 permit  host 205.205.205.11  log
access-list 1 deny  any log
line vty 0 15
        access-class 1 in           ←control access source
        exec-timeout30 0            ←Setup default timeout to 30mins
        transport input ssh         ←enable ssh as input transport
        transport output none
        transport preferred none
```

Physical access to the console port means no password needed upon reboot, at least console port need login password protection. Console should be used for last resort admin only.

```
line con 0
        login
```

exec-timeout 30 0
password 7 005C161E055C0408

Configure hostname and banner information

Even though warning banner cannot stop the intrusion, at least clearly warns the unlawful attempts.

```
hostname BorderRouter
    banner motd ^
    ********************************************************************
    * This is a private computer facility. Access to the facility        *
    * must be specifically authorized. If you are not authorized,        *
    * your continued access and further inquiry will expose you to       *
    * criminal and/or civil proceedings.                                 *
    ********************************************************************
     ^
```

Global Services

Add time stamping service facility for logging and debugging.

service timestamps debug datetime localtime
service timestamps log datetime localtime

Some services turn on by default, should be turned off to prevent security breach

no service finger
no service udp-small-servers
no service tcp-small-servers
no service pad ← *disable* all packet assembler/disassemble
no ip bootp server ← disable access the BOOTP service available from hosts on the network
no ip http server ← disable remote http access
no ip source-route ← IP has a provision to allow source IP host to specify route through Internet. Should turn off
no ip domain-lookup ← don't use DNS
no ip identd ← The ip identd command returns accurate information about the host TCP port, should be disable to prevent unauthorized queries.
no ip rcmd rsh-enable)
no ip rcmd rcp-enable) ←disabled by default double check

Enable router forward packets destined for a subnet of a network that has no network default route.

Ip classless

Enable the use of subnet 0 for interface addresses and routing updates.

ip subnet-zero

Logging and snmp setup

Log to centralized syslog server on DMZ. 205.205.205.11 is NATed ip address for syslog server 192.168.1.50.

SNMP is a useful network management tool; however, the protocol is not secure and the messages are sent in clear text. On border router, SNMP will be disabled. Since syslog information is going to be sent out to management console, logging analyzing tools could be used to monitor log entries and generate alerts to administrators.

no snmp-server

logging host 205.205.205.11
logging trap warnings
logging history warnings
logging buffered 16384 debugging
logging console emergencies

Specify the method of event notification,

ip audit notify log
ip audit po max-events 100

Access Lists

The access list is a series of address comparisons and in may cases port and protocol comparisons as well. Access list processing starts on the first line of an access list. If a match is made, a permit or deny action is taken and the process of that list ends. As a rule of thumb, policy should be written in the order of deny first and permit after. The moment a single ACL is added, all traffic is dropped except that which is expressly permitted. [2]

GIAC chose to use Extended Name access list. Extended ACL exams almost every part of a packet header, while Standard ACL only checks the IP source. Reflexive ACL provides stateful packet filtering at the cost of CPU utilization. GIAC wants border router to pass the traffic as soon as possible with some basic filtering functions.

[2] Sans Track 2.3 Firewalls 102: Perimeter Protection and Defence In-Depth Pg.13-31

Extended ACL is the best fit for GIAC. Meanwhile, Name ACL allows admin to define a descriptive name for the filters and save some typing for a long list.

Filters will be placed inbound on the both sides of the router. Filtering the unnecessary packets before they get routed not only saves the CPU resource, but also makes sense if packets would be denied later by the filter on another interface's outbound side.

Denied packets will also be logged and sent to centralized logging console. Over there, the more detailed security analysis and baseline trend could be achieved.

Interface facing ISP [3]

The default settings for a Cisco router do not check routing paths or stop illegitimate traffic. They also permit ARP traffic to pass through its interfaces. On each interface, we need to disable some network services that could be used for reconnaissance.

interface Ethernet0/1
ip address 206.206.206.200 255.255.255.0
no cdp enable ←Cisco discovery protocol should not be actived on public *facing interface*
no ip redirects ←disable resent packets through the same interface
no ip directed-broadcast ← should be applied to every LAN interface that isn't known to forward legitimate directed broadcasts.
no ip proxy-arp ← To prevent internal addresses from being revealed
no ip unreachables ← prohibit IP unreachable responses
no ip helper-address ← Disable UDP broadcast destinations
ip access-group GIACISP in

ip access-list extended GIACISP

deny ip 10.0.0.0 0.255.255.255 any log-input *deny ip 172.16.0.0 15.255.255.255 any log-input* *deny ip 192.168.0.0 0.0.255.255 any log-input*	Deny all RFC1918 netblocks[4]
deny ip 1.0.0.0 0.255.255.255 any log-input *deny ip 2.0.0.0 0.255.255.255 any log-input* *deny ip 5.0.0.0 0.255.255.255 any log-input* *……..* *deny ip 233.0.0.0 0.255.255.255 any log-input*	1) Deny all IANA unallocated netblocks[5] 2) This list changes consistently and needs to monitor closely. 3) Sometimes this is the root cause of the complain that GIAC web pages are not accessible for certain users.

[3] Securing Cisco Routers: Step-by-Step pg33-37
[4] http://www.ietf.org/rfc/rfc1918.txt
[5] http://www.iana.org/assignments.ipv4-address-space

	Because their newly assigned IPs fall into these blocks.
deny ip 224.0.0.0 31.255.255.255 any log-input	Deny multicast sources
deny ip 240.0.0.0 15.255.255.255 any log-input	Deny Class E networks
deny ip 0.0.0.0 0.255.255.255 any log-input *deny ip 169.254.0 0.0..255.255 any log-input* *deny ip 192.0.2.0 0.0.0.255 any log-input* *deny ip 127.0.0.0 0.255.255.255 any log-input*	Deny IANA reserved networks
deny ip 205.205.205.0 0.0.0.255 any log-input	Deny traffic inbound from GIAC's public address blocks to prevent spoof
permit icmp any any packet-too-big *Permit icmp host 206.206.206.10 205.205.205.0 0.0.0.255* *Deny icmp any any log-input*	Filter ICMP 1) Packet-too-big should be allowed for IP fragmentation requests. 2) ICMP from ISP's edge router is also allowed for troubleshooting 3) Other ICMP such as TTL exceed, will be filtered to prevent attackers from using this technique to probe our network
deny udp any any rang 161 162 log-input *deny tcp any any rang 161 162 log-input* *deny udp any any eq 69 log-input* *deny udp any any eq 514 log-input*	Deny inbound attempts to certain services where GIAC doesn't provide; while a hacker frequently uses (snmp,tftp,syslog). This part should be checked regularly. For instance, when under SQL slammer attack , blocking should happen here.
permit ip any 205.205.205.0 0.0.0.255	Permit Legitimate traffic
deny ip any any log-input	The final rule catches all the packets not otherwise specified.

Interface facing internal network

interface Ethernet0/0
ip address 205.205.205.1 255.255.255.0

ip access-group GIACINTRA in
no ip redirects
half-duplex
no ip unreachables
no ip redirects
no ip directed-broadcast
no ip helper-address
no ip proxy-arp

ip access-list extended GIACINTRA

deny icmp any any echo-reply log-input *deny icmp any any time-exceeded log-input* *deny icmp any any host-unreachable log-input*	First, deny ICMP response traffic which would otherwise reveal our network information for hackers
permit ip 205.205.205.0 0.0.0.255 any	Permit Legitimate traffic out
deny ip any any log-input	The final rule catches all the packets not otherwise specified.

Other Interfaces

All other unused interfaces should be in the shutdown state.

2.2 Primary Firewall

CiscoWorks2000 VMS module is designed to provide a GUI interface for PIX and VPN configuration; it is helpful for complicated Cisco environment. Nevertheless, it is an expensive add-on and doesn't cover all the PIX functions. At GIAC, command line will be chosen as primarily configuration method. Administrators will try to keep the configuration simple and robust which wouldn't require constant change after initial setup.

HTTPS PDM is helpful; however, it does not cover all the functionality either. Moreover GIAC don't want to open another hole, which has direct access to the primary firewall. GIAC believe the less connectivity, the safer it is.

GIAC's PIX is going to have three interfaces, which connects to the border router, internal network and DMZ. Same syslog server for the border router will be used for PIX logging. Netfilter rules on syslog server will be setup allowing syslog and snmp traffic from firewall. TCP syslog protocol is chosen over UDP since GIAC wants to make sure all the logs are transferred. To prevent possible DoS because of logging space issue, a cron job is scheduled to monitor and clean the file system on that server.

Please see the detailed explanation on section 2.4 tutorial.

Interface setup

Three interfaces are enabled; and auto negotiation is used to discover their speed and duplex status. Internal interface has the highest security level.

```
nameif e0 outside security 0
nameif e1 inside security 100
nameif e2 dmz security50
interface e0 auto
interface e1 auto
interface e2 auto
ip address inside 192.168.0.2 255.255.255.0
ip address outside 205.205.205.2 255.255.255.0
ip address dmz 192.168.1.2 255.255.255.0
```

Routing

Static routing is used because of the size of the network. Hence, RIP will be disabled. Using static routing also simplifies the troubleshooting and maintenance.

```
route outside 0.0.0.0  0.0.0.0 205.205.205.1 1
route inside 192.168.30.0 255.255.255.0 192.168.0.1 1
route inside 192.168.40.0 255.255.255.0 192.168.0.1 1
route inside 192.168.20.0 255.255.255.0 192.168.0.1 1
```

Disable RIP attributes

```
no rip inside passive
no rip outside passive
no rip inside default
no rip outside default
```

Remote administration

The only direct access to PIX is through SSH from centralized syslog server.

```
ssh 192.168.1.50 255.255.255.0 dmz
ssh timeout 30
```

SNMP and logging

SNMP is the key technology for network management; however, SNMPv1 has been reported with lot of vulnerability.[6] To minimums the risk, GIAC will choose version 2, in the future upgrade to SNMPV3 when it becomes mature. V3 supports authentication and secured tunnel communication. Default community string will be changed. And SNMP pulling is only allowed from SYSLOG server on DMZ.

Integrated Cisco Secure IDS will be enabled and logged; however GIAC will avoid using dynamic shunning because of possible false positives.

```
snmp-server community g1ac
snmp-server enable traps
snmp-server host 192.168.1.50 mgt

logging on
logging timestamp
logging buffered debugging
logging trap warnings
logging history warnings
logging host mgt 192.168.1.50
ip audit name attackpolicy attack action alarm
ip audit name infopolicy info action alarm
ip audit interface outside infopolicy
ip audit interface outside attackpolicy
ip audit interface inside infopolicy
ip audit interface inside attackpolicy
ip audit interface dmz infopolicy
ip audit interface dmz attackpolicy
ip audit info action alarm
ip audit attack action alarm
```

System configuration related to security

PIX has several methods to protect against various DoS attack. In GIAC, Flood defender is enabled to monitor SYN connections. This can prevent a possible SYN flood attack. Frag Guard will be disabled since GIAC accept modem user's web request, which might require fragmentation.

```
floodguard enable
no sysopt route dnat
```

[6] http://www.cert.org/advisories/CA-2002-03.html

Application fixup

Only necessary protocols are enabled to save resources.

fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720

Establishing Outbound Connectivity with NAT and PAT

To establish the connectivity, first we will have to deal with the outbound traffic. NAT and PAT are the only means to allow inside traffic to get out of a PIX. NAT allows a private address range to be translated into a pool of public addresses. This hides the inside addressing scheme from the outside world. PAT allows the translating of a range of internal addresses to one external IP in case of NAT address shortage. [7]

nat (dmz) 1 0 0
nat (inside) 2 0 0

global (outside) 1 205.205.205.241-205.205.205.254 netmask 255.255.255.0
global (outside) 1 205.205.205.240 netmask 255.255.255.0
global (dmz) 2 192.168.1.241-192.168.1.254 netmask 255.255.255.0
global (dmz) 2 192.168.1.240 netmask 255.255.255.0

Every interface will have one unique NATID. Since we only want internal user access DMZ but not external network.

However the NAT ID in the Nat command has to be the same NAT ID for the corresponding global command.

Access Lists

GIAC applies ACL on every interface of PIX firewall. On lower security level interfaces, static and access-list mush be used to allow requests from an outside host to the inside network. For higher security level interfaces, even though PIX automatically allow traffic to flow from high security level to low security level, GIAC uses ACL as an addition to control the traffic.

PIX only allows to specify one access group per interface. Access lists work on a first-match basis. For each access list, the order of each policy is important. As a rule of thumb, the rule matches the most core business traffic should be allowed to pass PIX first to speed up the process. In GIAC's case, web portal flow should be examined first and then SMTP and other applications flows.

[7] SANS Track.2.2 page 190

- External Interface

Since GIAC provides WWW services, external users have to be allowed to access web server's port 80/tcp and 443/tcp. See detailed access requirement at section 1.5. Traffic control for VPN will be discussed in section 2.3.

name 192.168.1.10 exmail
name 192.168.1.30 websvr
name 192.168.1.40 dnssvr
name 192.168.1.50 mgtsvr

static(dmz,outside) 205.205.205.10 exmail
static(dmz,outside) 205.205.205.30 websvr
static(dmz,outside) 205.205.205.40 dnssvr
static (dmz,outside) 205.205.205.11 mgtsvr

access-list acl_outside permit tcp any host 205.205.205.30 eq 80
access-list acl_outside permit tcp any host 205.205.205.30 eq 443

Public needs to access external DNS server's port 53/udp for giacsayings.com's query. ISP DNS's zone transfer needs to be allowed since it is our secondary DNS backup.

access-list acl_outside permit udp any host 205.205.205.40 eq 53
access-list acl_outside permit tcp 206.206.206.31 host 205. 205.205.40 eq 53

The above four rules examine the core traffic to GIAC network, they should be placed at the beginning of the ACL list. Mail (SMTP) probably is the next biggest application through PIX, the access to external Mail server 25/tcp should be placed right after.

access-list acl_outside permit tcp any host 205.205.205.10 eq 25

Border router's syslog information has to be logged into management console. Border router management is a trick business. On the one side, GIAC wants to monitor device health and network activity; on the other hand, GIAC has to risk security by allowing untrusted device sending traffic to DMZ.

access-list acl_outside permit udp host 205.205.205.1 host 205.205.205.11 eq 514

Inbound ICMP through the PIX is denied by default; outbound ICMP is permitted, but the incoming reply is denied by default.[8] GIAC needs to get ICMP reply messages such as packet-too-big back to ensure the traffic moves as smoothly as possible.

access-list ext permit icmp any any unreachable

Last rule, deny all the traffic otherwise not explicated above.

[8] http://www.cisco.com/warp/public/110/31.html#messtype

access-list acl_outside deny ip any any log-input

- DMZ Interface

From DMZ to internal network, web sever access application server at port 7000/tcp and RSA server at port 8000/tcp. (See access requirement in details on section 1.5.)

static(inside,dmz) 192.168.1.110 192.168.30.10
static(inside,dmz) 192.168.1.112 192.168.30.12
static(inside,dmz) 192.168.1.116 192.168.30.16

access-list acl_dmz permit tcp host 192.168.1.30 host 192.168.1.112 eq 7000
access-list acl_dmz permit tcp host 192.168.1.30 host 192.168.1.116 eq 8000

Web portal is GIAC's core, any portal traffic should have first priority through PIX. The next big application is internal users web browsing. For internal user, the speed of the Internet is very important. PIX should be able to pass those packets as quickly as possible. For GIAC, internal users access web through Proxy server. The third rule should check against proxy. Since it needs to access various services in the Internet; instead of explicate every port, GIAC permits all outbound traffic from proxy. Of course, GIAC is going to make sure the NETFILER is properly setup in the proxy server.

access-list acl_dmz permit ip host 192.168.1.20 any

Mail traffic usually has big volume, PIX should be optimized to process those packets too. Thus, the next rule should check flows through external mail server. ExMailSvr has to be able to send messages to internal mail sever and other mail servers in the net.

access-list acl_dmz permit tcp host 192.168.1.10 any eq 25

From DMZ to External network, ExDNS should be allowed query public DNS servers through Internet both on tcp and udp.

access-list acl_dmz permit tcp host 192.168.1.40 any eq 53
access-list acl_dmz permit udp host 192.168.1.40 any eq 53

NTP protocol has to be allowed from two dedicated DMZ severs to three public time servers (GIAC uses three local university servers).

access-list acl_dmz permit udp host 192.168.1.40 host 199.212.17.34 eq 123
access-list acl_dmz permit udp host 192.168.1.40 host 128.100.102.201 eq 123
access-list acl_dmz permit udp host 192.168.1.40 host 142.3.100.15 eq 123
access-list acl_dmz permit udp host 192.168.1.10 host 199.212.17.34 eq 123
access-list acl_dmz permit udp host 192.168.1.10 host 128.100.102.201 eq 123
access-list acl_dmz permit udp host 192.168.1.10 host 142.3.100.15 eq 123

Syslog server is the only server that has direct ssh access to border router.

access-list acl_dmz permit tcp host 192.168.1.50 host 205.205.205.1 eq 22

Any ICMP request is allowed to the internal network for troubleshooting.

access-list acl_dmz permit icmp any 192.168.30.0 255.255.255.0
access-list acl_dmz permit icmp any 192.168.40.0 255.255.255.0

ICMP reply should also be allowed.

access-list dmz permit icmp any any echo-reply
access-list dmz permit icmp any any unreachable
access-list dmz permit icmp any any source-quench
access-list dmz permit icmp any any time-exceeded

Finally, block everything else.

access-list acl_dmz deny ip any any log-input

- Inside Interface

Internal servers and desktops are allowed to access any servers and services on DMZ zone. This setting is designed for easy management and troubleshooting. To prevent internal users to abuse this privilege, GIAC uses user account/password to limit the access to DMZ servers; only authorized users are granted the permission. No internal server or workstation has direct access to Internet. All the access to the Internet goes through application proxies first to get content filtered. This setting will prevent internal users setup some kind of tunnels to external workstation, in turn let foreign machines gain access to the corporation network. Of course it doesn't eliminate the possibility that few internal users use httptunnel bypassing proxy server.

Nobody is going to have access to Internet directly.

Even though outbound traffic to DMZ is wide open, GIAC doesn't want internal users to probe firewalls. Only icmp to firewall interfaces is allowed for troubleshooting.

access-list acl_inside permit icmp any host 192.168.0.2
access-list acl_inside permit icmp any host 192.168.1.2
access-list acl_inside permit icmp any host 205.205.205.2

access-list acl_inside deny ip any host 192.168.0.2
access-list acl_inside deny ip any host 192.168.1.2
access-list acl_inside deny ip any host 205.205.205.2

From Internal to DMZ, all the traffic is allowed.

access-list acl_inside permit ip 192.168.30.0 255.255.255.0 192.168.1.0 255.255.255.0
access-list acl_inside permit ip 192.168.40.0 255.255.255.0 192.168.1.0 255.255.255.0
access-list acl_inside permit ip 192.168.0.0 255.255.255.0 192.168.1.0 255.255.255.0

Then, block everything else:

access-list acl_inside deny ip any any log-input

At last, access-list has to be applied to each interface properly.

access-group acl_inside in interface inside
access-group acl_outside in interface outside
access-group acl_dmz in interface dmz

2.3 VPN

GIAC will use VPN to provide secured channel between remote teleworkers or wireless users to corporation network.

Since VPN feature supported by PIX, GIAC will use PIX firewall as its VPN server. Having VPN and firewall combined in same device, not only cut the cost, but also enhance the security. Otherwise the firewall has to open couple holes to facility the VPN channels. PIX515E has VPN accelerator build-in, the performance should be acceptable for the size of GIAC's traffic.

RSA solution will be implemented for user authentication. GIAC will allocate a class C ip addresses (192.168.20.0/24) to be used as virtual internal address to make security and access-list tighter. Remote users will be assigned a virtual address automatically when they sign on. VPN is terminated at the outside interface of the PIX.

Setup ACL to bypass NAT for VPN traffic

Do not use Network Address Translation for inside–to–pool. VPN traffic should not go through as NAT. GIAC will allow vpn users access almost all the internal network.

nat (inside) 0 access-list 101

access-list 101 permit ip 192.168.30.0 255.255.255.0 192.168.20.0 255.255.255.0
access-list 101 permit ip 192.168.40.0 255.255.255.0 192.168.20.0 255.255.255.0

Use RSA authentication

aaa-server partner-auth protocol radius
aaa-server partner-auth (inside) host 192.168.30.16 MYSECRET timeout 20

Config IKE

IKE will be enabled on the outside interface of the PIX. GIAC's IKE policy: using des encryption algorithm, md5 for hash, pre-shared key (giac1234). Client 3.x use Diffie-Hellman group 2 instead of default group 1. Security association's lifetime will use default value (one day).

Since GIAC uses RSA authentication, it is recommended to set each participating peer's identity to hostname. Otherwise, the ISAKMP security association to be established during Phase 1 of IKE may fail.

isakmp enable outside
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 authentication pre-share
isakmp policy 10 group 2
isakmp key giac1234 0.0.0.0 netmask 0.0.0.0
isakmp identity hostname

For VPN Client 3.x (Easy VPN framework)

For the Cisco VPN Client version 3.x, we need add another policy. After remote clients log in, PIX is going to assign it an internal ip address with internal DNS server information. Split tunnel will not be used at the moment since it involves much more complicated access control process. Considering the size of GIAC enterprise (30 – 40 VPN users in total), the VPN users' Internet connection will go through corporation proxy. This traffic overhead is not expected to be significant.

vpngroup giacremote address-pool giacpool
vpngroup giacremote dns-server 192.168.30.40
vpngroup giacremote default-domain giacsayings.com
vpngroup giacremote password g1ackey

Config IPSEC

IPSEC provides data confidentiality, data integrity and original authentication.

- First, we have to permit IPSEC connections through firewall.

  syopt connection permit-ipsec

- Defines how the traffic will be protected through transform set. GIAC has a set called fu-set with two transforms.

  crypto IPSec transform-set fu-set esp-3des esp-sha-hmac

- Define crypto map

  Assign the pre-defined transform set. Dynamic map can ease IPSec configuration and are recommended for use with networks where the peers are not always predetermined, such as mobile users who obtain dynamically assigned IP address.[9]

  crypto dynamic-map fumap 10 set transfrom-set fu-set

  Define a crypto map "fusmap" to enable the ISAKMP policy. The policy number should user higher number than dynamic map.

  crypto map fusmap 20 IPSec-isakmp dynamic fumap

  Make sure PIX Firewall will attempt to set IP addresses for each peer; and will accept requests for IP addresses from any requesting peer since the remote users ip is unknown.

  crypto map fusmap client configuration address initiate
  crypto map fusmap client configuration address respond

  Apply crypto map to the interface.

  crypto dynamic-map fumap interface outside

Config IKE mode

By using IKE mode, PIX will be able to automatically assign an internal IP address to a VPN client.

ip local pool giacpool 192.168.20.1-192.168.20.254
crypto map fusmap client configuration address initiat
isakmp client configuration address-pool local giacpool outside

[9] http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v50/config/ipsec.htm#xtocid20

VPN Client 3.6

GIAC will use Cisco VPN Client 3.x as vpn client software. Not only does Client 3.x support multi-platforms, it also has stronger encryption ability than Secure Client 1.1, not to mention it is easy to use and configure. All the VPN desktop users are required to use antivirus and personal firewall software.

The steps to set up a Client are as simple as the following, the detailed procedure please refer to Cisco manual. [10]

Create a new connectivity entry
Enter remote server as : 205.205.205.2 which is PIX's ip address on external interface.
Group Access name: giacremote
Password: giackey

After finishing the connectivity wizard, choose the connection just built and click the connect. An authentication window will pop up. Use SecurID token to enter the username and one time PIN to connect to corporation network.

For test, you could start a telnet session and look at logs and trace the traffic.
You should be able to see the logs on client side:

```
13:22:34.225 giac - Deleting IKE SA
13:23:23.677 giac - SENDING>>>> ISAKMP OAK MM (SA)
13:23:23.787 giac - RECEIVED<<< ISAKMP OAK MM (SA)
13:23:23.877 giac - SENDING>>>> ISAKMP OAK MM (KE, NON)
13:23:23.997 giac - RECEIVED<<< ISAKMP OAK MM (KE, NON, VID)
13:23:24.067 giac - SENDING>>>> ISAKMP OAK MM *(ID, HASH)
13:23:24.117 giac - RECEIVED<<< ISAKMP OAK MM *(ID, HASH)
13:23:24.167 giac - SENDING>>>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID)
13:23:24.227 giac - RECEIVED<<< ISAKMP OAK TRANS *(HASH, ATTR)
13:23:24.227 giac - Received Private IP Address = IP ADDR=192.168.20.2
13:23:24.277 giac - SENDING>>>> ISAKMP OAK TRANS *(HASH, ATTR)
13:23:24.327 giac - RECEIVED<<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID,
NOTIFY:STATUS_RESP_LIFETIME)
13:23:24.378 giac - SENDING>>>> ISAKMP OAK QM *(HASH)
13:23:24.498 giac - Loading IPSec SA keys...
13:23:24.498
```

From PIX log:

```
602301: sa created,
  (sa) sa_dest= 205.205.205.2, sa_prot= 50,
    sa_spi= 0x36c3cb1c(918801180),
```

[10] http://www.cisco.com/warp/customer/110/B.html

```
   sa_trans= esp-des esp-sha-hmac , sa_conn_id= 1
602301: sa created,
  (sa) sa_dest= 206.206.206.101, sa_prot= 50,
    sa_spi= 0xb1eb041b(2984969243),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2
302001: Built inbound TCP connection 121 for faddr 192.168.20.2/1040 gaddr 205.
205.205.50/23 laddr 192.168.30.50/23
```

206.206.206.101 is client's public ip address

If you trace traffic on internet, you only see the ESP traffic and IKE negotiation between client's public ip to PIX's external ip (206.206.206.101 to 205.205.205.2). Which is exact what we expected.

2.4 Tutorial for PIX Firewall

PIX setup is not difficult if administrators have a clear network and security topology of the designed network. Cisco configuration forms are used to better understand GIAC's infrastructure. This extra process will make the installation process easier and faster (The original document could be found at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v50/config/cfgforms.htm#41850). Those forms are particularly designed for PIX firewall version 5.0; they are also applicable to other versions.

This tutorial will focus on security related topics. For detailed instruction on how to setup and management PIX 6.2, please refer to http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_62/index.htm

Connect to PIX

As any other Cisco device, first of all, a terminal connection to PIX is needed for initial setup. In the case of hyper terminal, the configuration for serial port is: 9600 bits per second, 8 data bits, no parity, 1 stop bits and hardware flow control.

Get the latest Software

Make sure GIAC gets the latest software. Usually the default installation is one or two release behind due to the delay on shipment. Go to Cisco software center and download the latest image. The software installation only takes about couple minutes.

Configure PIX Firewall interfaces

GIAC PIX Firewall has four physical network interfaces. Table 2-1 provides a form for entering PIX Firewall network interface information. From this form it is very easy to get the setup as shown in the session 2.2 for interface configuration.

Table 2-1

Interface Name	Interface Type	Hardware ID	Interface IP Address	Interface Speed	MTU Size	Interface Security Level
Outside	Ethernet	0	205.205.205.2	Auto	1500	0
Inside	Ethernet	1	192.168.0.2	Auto	1500	90
DMZ	Ethernet	2	192.168.1.2	Auto	1500	50

Use **ip address** command to assign an ip address and netmask. **Interface** *hardware_id hardware_speed* to identify the interface type. Each interface has a unique name and security level that you can change using the nameif command. Security levels let you control access between systems on different interfaces and the way you enable or restrict access depends on the relative security level of the interfaces. In configuration mode, enter the following:

pix***# config t***
pix(config)***# nameif e0 outside security 0***
pix(config)***# nameif e1 inside security 100***
pix(config)***# nameif e2 dmz security50***
pix(config)***# interface e0 auto***
pix(config)***# interface e1 auto***
pix(config)***# interface e2 auto***
pix(config)***# ip address inside 192.168.0.2 255.255.255.0***
pix(config)***# ip address outside 205.205.205.2 255.255.255.0***
pix(config)***# ip address dmz 192.168.1.2 255.255.255.0***

For interfaces with a higher security level such as the inside interface, or a DMZ interface relative, use the **nat** and **global** commands to let users on the higher security interface access a lower security interface. For the opposite direction, from lower to higher, you use the **static** and **access-list** command. We will discuss this in great details later.

Routing

Each inside or perimeter PIX Firewall interface is configurable for route and Routing Information Protocol (RIP) information. Only one default route is permitted. This command statement sends any packets destined for the default route, IP address 0.0.0.0 (abbreviated as 0, and 0 for the netmask), to the router 205.205.205.1. The "1" at the end of the command statement indicates that the router is the router closest to

the PIX Firewall; that is, one hop away.

pix(config)# ***route outside 0.0.0.0 0.0.0.0 205.205.205.1 1***

In addition, add static routes for the networks that connect to the inside router as follows:

pix(config)# ***route inside 192.168.30.0 255.255.255.0 192.168.0.1 1***
pix(config)# ***route inside 192.168.40.0 255.255.255.0 192.168.0.1 1***
pix(config)# ***route inside 192.168.20.0 255.255.255.0 192.168.0.1 1***

Since we use static routing, there is no need for RIP updates

pix(config)# ***no rip inside passive***
pix(config)# ***no rip outside passive***
pix(config)# ***no rip inside default***
pix(config)# ***no rip outside default***

Estabilsh outbound connectivity

In interface **nameif** definition, we give interface different security level. PIX uses NAT and PAT to establish connectivity from hosts on high security level to hosts on lower level.

Add a **nat** command statement for each higher security level interface from which you want users to start connections to interfaces with lower security levels:

nat [(if_name)] nat_id local_ip [**netmask** [max_conns [em_limit]]] [norandomseq]

Syntax Description

if_name The internal network interface name.

nat_id Specify 0 to indicate that no address translation be used with *local_ip*. All nat command statements with the same *nat_id* are in the same nat group.

local_ip Internal network IP address to be translated. You can use 0.0.0.0 to allow all hosts to start outbound connections. The 0.0.0.0 *local_ip* can be abbreviated as 0.

netmask Network mask for *local_ip*. You can use 0.0.0.0 to allow all outbound connections to translate with IP addresses from the global pool.

Table2-2 maps internal (inside) or perimeter network addresses with global network addresses on other interfaces in the PIX Firewall.

Table 2-2: Inside (Local) or Perimeter Network Address Translation

Inside or Perimeter Name from Table2.4-1	NAT ID Number (1 to 65,000)	Network Address Mapped to the NAT ID	Network Mask for This Address
Inside	2	Any	Any
Dmz	1	Any	Any

Let inside users start connections on any lower security interface.

pix(config)# ***nat (inside) 2 0 0***

To let DMZ users start connections to the outside.

pix(config)# ***nat (dmz) 1 0 0***

We use different natid because we only want insider users to access the DMZ interface but not the outside interface. However the nat id in the nat command must be the same natid we use for the corresponding global command.

Add **global** command statement for each lower security interface which you want users to have access to; on GIAC case, on the outside and dmz interface. The global addresses in the pool provide an IP address for each outbound connection, and for those inbound connections resulting from outbound connections. Because there are limited outside IP addresses, add a PAT global to handle overflow. Translation (PAT) is realized by using **global** command statement, which specifies a single IP address. For better performance, make sure PAT ip address number is lower then the global ip address number. Also ensure that associated **nat** and **global** command statements have the same *nat_id*.

global [(*if_name*)] *nat_id global_ip*[-*global_ip*] [**netmask** *global_mask*]

Syntax Description

if_name The external network where you use these global addresses.
Nat_id A positive number shared with the **nat** command
Global_ip If the external network is connected to the Internet, each global IP address must be registered with the Network Information Center (NIC).
netmask Reserved word that prefaces the network *global_mask* variable.
Global_mask The network mask for *global_ip*.

Table 2-3: Global Network Address Range for GIAC

Outside or Perimeter Interface Name	NAT ID Number	Beginning of IP Address Range	End of IP Address Range
Outside	1	205.205.205.241	205.205.205.254
DMZ	2	192.168.1.241	192.168.1.254

Translate above form to words:

pix(config)# ***global (outside) 1 205.205.205.241-205.205.205.254***
pix(config)# ***global (outside) 1 205.205.205.240***
pix(config)# ***global (dmz) 2 192.168.1.241-192.168.1.254***
pix(config)# ***global(dmz) 2 192.168.1.240***

Access lists

By default, PIX deny any connectivity from lower security level interface to higher level interface. GIAC has to let outside user to access its server and servers in DMZ zone has to access internal servers. Any server on a network that has a higher security level than the current interface requires a **static** and **access-list** command statement. Static address translation creates a permanent, one-to-one mapping between a host on a higher security level interface and a global address on a lower security level interface. Static address translation hides the actual address of the server from users on the less secure interface, making casual access by unauthorized users less likely.

static [(*internal_if_name*, *external_if_name*)] *global_ip local_ip* [**netmask** *network_mask*]

Syntax Description

internal_if_name	The internal network interface name. The higher security level interface you are accessing.
external_if_name	The external network interface name. The lower security level interface you are accessing.
Global_ip	A global IP address. This address cannot be a PAT (Port Address Translation) IP address. The IP address on the lower security level interface you are accessing.
local_ip	The local IP address from the inside network. The IP address on the higher security level interface you are accessing.
Netmask	Reserve word required before specifying the network mask.

network_mask The network mask pertains to both *global_ip* and *local_ip*

Table 2-4 is the list of what services need to be accessed.

Table 2-4: Static Address Mapping

Interface on Which the Host Resides	Interface Name Where the Global Address Resides	Host IP Address	Static IP Address	Comments
Dmz	Outside	192.168.1.10	205.205.205.10	exMailSvr
Dmz	Outside	192.168.1.30	205.205.205.30	WebSvr
Dmz	Outside	192.168.1.40	205.205.205.40	DnsSvr
Inside	Dmz	192.168.30.10	192.168.1.110	InMailSvr
Inside	Dmz	192.168.30.12	192.168.1.112	AppSvr
Inside	Dmz	192.168.30.16	192.168.1.116	RSASvr
DMZ	Outside	192.168.1.50	205.205.205.11	MGTSvr

Translate to command line:

pix(config)# ***static(dmz,outside) 205.205.205.10 192.168.1.10***
pix(config)# ***static(dmz,outside) 205.205.205.30 192.168.1.30***
pix(config)# ***static(dmz,outside) 205.205.205.40 192.168.1.40***
pix(config)# ***static (dmz,outside) 205.205.205.11 192.168.1.50***

pix(config)# ***static(inside,dmz) 192.168.1.110 192.168.30.10***
pix(config)# ***static(inside,dmz) 192.168.1.112 192.168.30.12***
pix(config)# ***static(inside,dmz) 192.168.1.116 192.168.30.16***

Access-list specifically allows inbound connections.

Syntax Description [11]

acl_ID	Name of an access list. You can use either a name or number.
permit/deny	When used with the access-group command, the permit option selects a packet to traverse the PIX Firewall. While the deny option does not allow a packet to traverse the PIX Firewall. By default, PIX Firewall denies all inbound or outbound packets unless you specifically permit access..
Port	Services you permit or deny access to.
Protocol	Name or number of an IP protocol. It can be one of the keywords icmp, ip, tcp, or udp, or an integer in the range 1 to 254 representing an IP protocol number. To match any Internet protocol, including ICMP, TCP, and UDP, use the keyword ip.
source_addr	Address of the network or host from which the packet is being sent.
source_mask	Netmask bits (mask) to be applied to *source_addr*, if the source address is for a network mask.
Remote_addr	IP address of the network or host remote to the PIX Firewall.
Remote_mask	Netmask bits (mask) to be applied to *remote_addr*, if the remote address is a network mask.

Access list works on a first-match basis, so for inbound access, we must deny first and then permit after. Also the order is important. Most of the requests from external are web access related connection, we should let the connections to the web to get processed first and then pass mail traffic and dns query.

From section 1.5, GIAC need the following access requirement on each interface.(Not include VPN)

Table 2-5

- External Interface

[11] http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/cmdref/ab.htm

Permit /Deny a Connection	Network Protocol	Static IP Address from Table 2.4-4	Ports (Services) Authorized for the Static IP Address	Foreign Host or Network IP Address and Network Mask	Ports (Services) Foreign IP Address[2]
Permit	Tcp	205.205.205.10	25	Any	Any
Permit	Tcp	205.205.205.30	80&443	Any	Any
Permit	Udp	205.205.205.40	53	Any	Any
Permit	Tcp	205.205.205.40	53	206.206.206.31	Any
Permit	Udp	205.205.205.11	514	205.205.205.1	Any
Permit	ICMP unreachable	Any		Any	

- DMZ interface

Permit	Tcp	192.168.1.110	25	192.168.1.10	Any
Permit	Tcp	192.168.116	8000	192.168.1.30	Any
Permit	Tcp	192.168.112	7000	192.168.1.30	any
Permit	Tcp&udp	Any	53	192.168.1.40	Any
Permit	Tcp	Any	25	192.168.1.10	Any
Permit	Udp	199.212.17.34 128.100.102.201 142.3.100.15	123	192.168.1.10 192.168.1.40	Any
Permit	Ip	Any	Any	192.168.1.20	any
Permit	ICMP echo-reply	Any		any	

	Unreachable Source-quench Time-exceeded				
Permit	Icmp	Any	Any	192.168.30.0/24 192.168.40.0/24	any

- Inside Interface

Permit	icmp	192.168.1.2 192.168.0.2 205.205.205.2		Any	
Deny	ip	192.168.0.2 192.168.1.2 205.205.205.2	any	Any	any
Permit	Ip	192.168.1.0/24	Any	192.168.30.0/24 192.168.40.0/24 192.168.0.0/24	any

From above table, easily we got three groups of access-list as stated on section 2.2 Access-lists part. Cut and past those ACL in configuration command line. For each access group, the last rule will always be deny any any to catch all the inexplicit traffic.

access-group commands bind corresponding access list to the appropriate interface. The access list is applied to traffic inbound to an interface. If you enter the permit option in an access-list command statement, the PIX Firewall continues to process the packet. If you enter the deny option in an access-list command statement, PIX discards the packet immediately.[12]

pix(config)# ***access-group acl_dmz in interface dmz***
pix(config)# ***access-group acl_outside in interface outside***
pix(config)# ***access-group acl_inside interface inside***

At the end of the configuration, don't forget to save the configuration and reboot the PIX to active the ACL immediately.

PIX(config)# ***wr mem***
PIX(config)# ***reload***

[12] http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/cmdref/ab.htm#1025611

Chapter 3: Assignment 3 - Verify the firewall

Auditing is a verification of the integrity of a system. Without auditing, the security policy of that company is not comprehensive. Without auditing, the implemented rules cannot be confirmed. A thorough audit includes vulnerability assessment, penetrating test, perimeter and server system auditing. Here, we will focus on auditing the primary firewall.

After initial setup or rule modification on the firewall, it's recommended to audit that device once. It ensures that the change is implemented as suppose to be and doesn't break any other application functions.

3.1 Plan the audit

What

Primary firewall auditing is different from vulnerability auditing. The main purpose of the procedure is to verify that the policy we want to apply is actually implemented. The packets that supposed to be blocked are blocked and there is no leakage. The rule that has to allow packets is truly passing the traffic.

The detailed procedure will be discussed in the next section. As a summary, first, we are going to scan every firewall interface to search the available services. Ensure that only services intended to run will response to the scan, any other services should be turned off. Second, we will conduct ingress filtering test to ensue that any non-routable addresses or internal address do not pass the firewall. Fragmentation through firewall will also be tested. Third, audit outbound traffic. We will make sure that there is no chatty services leak into the Internet. Last, we will verify that the direct access to the firewall is designed as it supposes to be -- only accessible through syslog server.[13]

When

The actual audit will be conducted on one of the weekends. The test will start from Saturday morning 8:00am, and is expected to finished by Sunday morning within 24 hours.

Most of scans used in auditing will have the same traffic pattern that GIAC will normally confront at day-to-day base. (Any public services are under constant scan and attack attempts). GIAC's network should be able to handle the extra traffic. Of cause, some brutal scans and nessus vulnerability checks could be destructive. To be precautious, the audit will be conducted at a period when the traffic has the lowest volume. Analyzing from web logs, GIAC notices that weekends have the least web transactions. Moreover,

[13] SANS Track 2.5 text book pg 80-116

traffic through primary firewall during that period has minimum volume too. After discussion with management team and business unit, GIAC audit team decides to conduct the auditing on one of the Saturdays.

About week early, audit team will pass the memo to internal users to notify the incoming audit on the next Saturday. Furthermore, they will also post a maintenance web page on the test day. It announces that the company is undergoing network maintenance and users might experience service interruption during the day. Finally, audit team will ask operations and the primary technical support for that weekend to have extra cautious. Primary support technicians should not loose their precautious just become there is a massive audit going on. They should be able to distinguish whether the attack/problem is the real incident or because of the audit. If there is a real attack, support and audit team should be able to stop the audit and response quickly.

Cost and Effort

The software/hardware cost for this audit is almost nil. The only cost is the labor cost for planning and execution. To ensure the operation success, administrators need careful plan and thorough preparation.

GIAC is going to use free software to conduct the audit. Since free tools normally don't come with a single GUI interface that generates pretty management chart, administrators might have to take a week or two to install and configure various packages. Nevertheless, GIAC could benefit from this practice on the long run. Whenever there is a major change on the firewall, GIAC could use this procedure to audit the implementation.

As to hardware, GIAC is going to use administrators' laptops or desktops.

GIAC decides to ask security control team to conduct the actual audit. Choosing someone who is not involved in the implementation or daily support, will make this audit more accurate and close to the reality. Auditors look at the network in a fresh and third party point view, avoid technicians' possible "white lies". Of cause, in the planning stage, technical group has to be heavily involved to provide the necessary network and security information.

Audit team estimates that the audit proximate takes 24 hours, at least two shifts to finish. They will also make sure on that day, there is good communication channel setup with primary support and operation group. In the case of system crash due to the massive scan, there is immediate support. Moreover, if a hacker knows in advance that GIAC is undergoing audit, they might disguise themselves in the massive scan to do some real attack and hope that their traffic will not get noticed. The GIAC security specialist has to take extra cautious when analyze the IDS alerts and other loggings from perimeter devices. He should be able to distinguish the real attack from audit scan.

How

Figure 3-1 is the actual audit diagram. Three scan machines are ExSvr, InSvr and DMZSvr. GIAC needs 3 machines to conduct this audit, one on external 205.205.205.0/24 segment, one on internal touchdown segment 192.168.0.0/24, and one on DMZ192.168.1.0/24 network. All those machines will have tcpdump, nmap, hping2 and nessus installed.

Basically, GIAC is going to use tcpdump as a sniffer tool. It has two function, one is to ensure that the packets the scan tools suppose to generate are actually send out to the designed interface; another is to verify whether the packets pass through the firewall. Nmap, nessus and hping2 will be used as scan tools.

- **Tcpdump**
  www.tcpdump.org

  A powerful tool for network sniffering. This program allows you to see the traffic on a network. It can be used to print out the headers of packets on a network interface that matches a given expression. You can use this tool to track down network problems, to detect "ping attacks" or to monitor the network activities. The manual for tcpdump could go on forever. GIAC is going to use the following:

  tcpdump -i eth0 -n -w /tmp/eth0.tcpdump src or dst host 205.205.205.200

  -i which interface to monitor
  -n use ip address and port number instead of resolved to dns name and service name
  -w dump to a file
  option: *src or dst host* dump any thing to or from that host
  205.205.205.200 target host

- **Nmap**
  www.nmap.org

  Nmap is a powerful security audit tool, of course it could also be used as a step stone for black hat's attack. It could conduct a fast tcp/udp/icmp port scan, OS detection and ping sweep. It also has a windows version available. GIAC is going to use nmap as a scan tool to verity firewall's rule.

  nmap -v –R -g53 -sS -sR -P0 -p 1-65535 -o firewall.out ip_address

  -v verbose
  -R don't resolve dns and service
  -g53 set the source port number utilized for the scans
  -sS conducts SYN scan
  -sR conducts RPC scan all the ports found

-P0 no ping
-p 1-65535 ports to be scan
-o output result to firewall.out
ip_addres: Address of the host to be scanned

- **Nessus**
  www.nessus.org

Nessus is a remote security scanner. It has a very comprehensive service vulnerability check database(over thousand plugin checks). Also it has a so-called smart service recognition – it will recognize a telnet server running on a non-standard port (3333) or a smtp server running on port 2500. Moreover, it has a very nice report function. Not only give you the vulnerability list, it also provide the solution and risk level.

After install the package, add library path first
LD_LIBRARY_PATH=/usr/local/lib:/usr/local/ssl/lib; export LD_LIBRARY_PATH
As root run *nessus-adduser* to add login user account. (We will use open a account called nessus and use password as authentication method)
Start nessus server daemon
/usr/local/sbin/nessusd –D&

- **Hping2**
  www.hping.org

  Hping is a command line based packet assembler and analyzer. It could be used for firewall testing, port scanning and network packets craft. It could also display target replies like ping does with ICMP replies. GIAC is going to use this tool to generate some fragmented packets for test. Basically, it is a ping like tool, very easy to use. However the author recently stopped the development. We certainly hope that someone in the community could continue his work.

  The syntax GIAC is going to use are as following:

  hping2 -V --frag --data 40 --count 3 --syn -p 22 ip_address

  -V verbose
  --frag fragmentation
  --data the size of the data
  --count how many packets we are going to send
  --syn set the flag
  -p 22 scan port 22
  ip_address target address

3.2 Execution

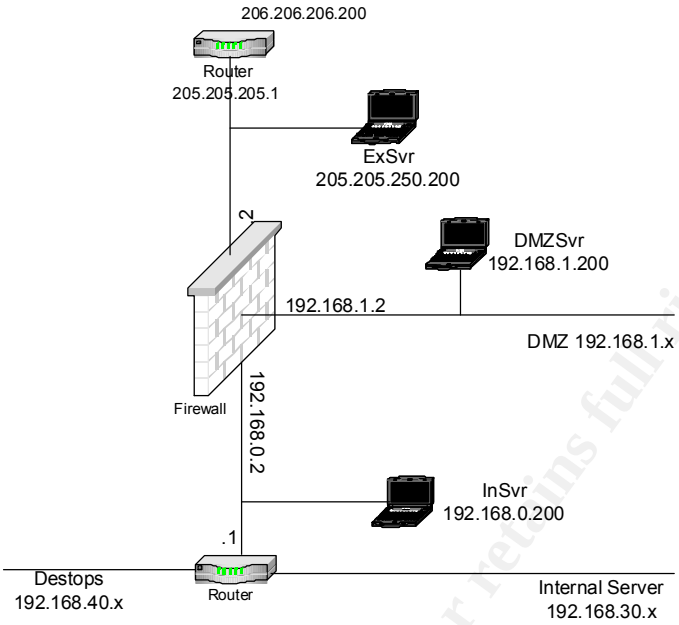


Figure 3-1 Auditing Diagram

Step 1. Verify the rules

First of all, GIAC is going to verify whether the primary firewall fulfills its basic functions. Are allowed services being past through and deny services being blocked? Nmap is used in this case to scan the firewall. This command returns all the services that are being run. Only services intended to run should response to scan. Scan will be conducted on each interface of the firewall. Any services that should not be running should be turned off.

External Scan

From ExSvr, GIAC is going to do a SYN scan to its public segment from port 1 to 65535. We will craft the packets to forge the source port to be 53.

- External SYN Scan

Nmap –v –g53 –sS –sR –P0 –p 1-65535 205.205.205.0/24	Interesting ports on (205.205.205.2): (The 65533 ports scanned but not shown below are in state: closed) Port State Service (RPC) 23/tcp filtered telnet 1467/tcp filtered csdmbase ---------- Interesting ports on (205.205.205.10): (The 65533 ports scanned but not shown below are in state: filter) Port State Service (RPC) 25/tcp open smtp ---------- Interesting ports on (205.205.205.30): (The 65533 ports scanned but not shown below are in state: closed) Port State Service (RPC) 80/tcp open http 443/tcp open https
ExSvr Tcpdump	GIAC confirmed that the corresponded traffic was produced by nmap. Due to the space the output is omitted.
DMZSvr tcpdump	From DMZSvr sniffer, we only see the legitimate traffic coming in and out. Excerpt from tcpdump: # tcpdump –nn 22:03:12.061694 205.205.205.200.53 > 192.168.1.30.80: S 2879827956:2879827956 (0) win 2048 22:03:12.061694 192.168.1.30.80 > 205.205.205.200.53: S 2736631423:2736631423 (0) ack 2879827957 win 5840 <mss 1460> (DF) 22:03:12.061694 205.205.205.200.53 > 192.168.1.30.80: R 2879827957:2879827957 (0) win 0 (DF) 22:07:28.808334 205.205.205.200.32774 > 192.168.1.30.80: S 1928471982:1928471982 (0) win 5840 <mss 1460,sackOK,timestamp 80192785 0,nop,wscale 0> (DF) 22:07:28.808416 192.168.1.30.80 > 205.205.205.200.32774: S 2987798408:2987798408 (0) ack 1928471983 win 5792 <mss 1460,sackOK,timestamp 355406761 80192785,nop, wscale 0> (DF) 22:07:28.808853 192.168.1.30.80 > 205.205.205.200.32774: S 2987798408:2987798408 (0) ack 1928471983 win 5792 <mss 1460,sackOK,timestamp 355406761 80192785,nop, wscale 0> (DF) 22:07:28.809112 205.205.205.200.32774 > 192.168.1.30.80: . ack 1 win 5840 <nop,nop,timestamp 80192785 355406761> (DF) 22:07:28.809116 205.205.205.200.32774 > 192.168.1.30.80: P 1:45(44) ack 1 win 5840 <nop,nop,timestamp 80192785 355406761> (DF) 22:07:28.809264 192.168.1.30.80 > 205.205.205.200.32774: . ack 45 win 5792 <nop,nop,timestamp 355406762 80192785> (DF) 22:07:28.809635 192.168.1.30.80 > 205.205.205.200.32774: . ack 45 win 5792 <nop,nop,timestamp 355406762 80192785> (DF) ……
Log from firewall	302001: Built inbound TCP connection 52 for faddr 205.205.205.200/53 gaddr 205.205.205.100/53 laddr 192.168.1.40/53 302001: Built inbound TCP connection 53 for faddr 205.205.205.200/53 gaddr 205.205.205.30/80 laddr 192.168.1.30/80 302001: Built inbound TCP connection 54 for faddr 205.205.205.200/53 gaddr 205.205.205.30/443 laddr 192.168.1.30/443 302001: Built inbound TCP connection 55 for faddr 205.205.205.200/53 gaddr 205.205.205.10/25 laddr 192.168.1.10/25 Rest: 106019: IP packet from 205.205.205.200 to 205.205.205.100, protocol 6 received

	from interface "outside" deny by access-group "acl_outside" ---------- When destination is to firewall itself (ip) dest_addr= 205.205.205.2, src_addr= 205.205.205.200, prot= 6402106: Rec'd packet not an IPSEC packet didn't pass

The scan conducted on firewall itself though, is a little surprise. First, telnet is not even turned on external interface, but the scan indicates telnet service is still listening. Second, GIAC never know there is anther service available on port 1467. After research, GIAC realizes that network service is PIX Secure Telnet (TCP 1467) for policy manager. Since GIAC doesn't intend to use it, GIAC will try to turn it off. (Details see section 3.3.) The rest of the test goes as what GIAC expected.

From above test, GIAC concludes that (besides the ports on firewall itself) all the firewall rules intended to permit tcp traffic are effectively working. And all the other tcp traffic is being blocked.

- External UDP Scan

Similarly: we are going to lookup at udp packets.

External UDP scan Nmap –v –g53 –sU–P0 –p 1-65535 205.205.205.0/24	Interesting ports on (205.205.205.40): (The 65535 ports scanned but not shown below are in state: closed) Port State Service 53/udp open domain
ExSvr tcpdump	Since they are all udp packets, we could only see packets send out……. 12:02:51.477987 205.205.205.200.53 > 205.205.205.19.34: [|domain] 12:02:51.497005 205.205.205.200.53 > 205.205.205.252.6000: [|domain] ……
DMZSvr tcpdump	On DMZSvr, we could only see packets get into dns server 11:38:22.874862 205.205.205.200.53> 192.168.1.40.53: 0 [0q] (0) 11:38:28.884862 205.205.205.200.53 > 192.168.1.40.53: 0 [0q] (0)
Log from firewall	Other then the packets dedicated to the dns server, the firewall generates the following entry 106007: Deny inbound UDP from 205.205.205.200/0 to 192.168.1.200/59 due to DNS Query

The result tells us that only udp port 53 from 205.205.205.40 is open to the public. That is in the expectation.

- External Ping Scan

Now that we have checked tcp and udp. How about ICMP? Simply we will do a nmap ping scan.

Nmap –sP –R 205.205.205.0/24
It only find border router 205.205.205.1 is up, which is intended open to 205.205.205.0/24 segment for troubleshooting purpose.

We had checked the good packets. How is firewall going to react to craft packets? GIAC is going to do FIN, Xmas Null and ACK scans to the external public network segment. The following is the firewall's response.

- External FIN Scan

Nmap –v –R –g53 –sF -P0 –p 1-65535 205.205.205.0/24	All the ports on 205.205.205.1 are closed ---------- Interesting ports on (205.205.205.2): (The 65533 ports scanned but not shown below are in state: closed) Port State Service 23/tcp open telnet 1467/tcp open csdmbase ---------- To rest of the sever: 65535 scanned ports are filtered
DMZSvr tcpdump	NONE packet goes through
Log from firewall	106015: Deny TCP (no connection) from 205.205.205.200/53 to 192.168.1.200/100 flags FIN …… 106015: Deny TCP (no connection) from 205.205.205.200/53 to 192.168.1.201/4005 flags FIN …… omitted the rest.

- External Xmas Scan

Nmap –v –R –g53 –sX –P0 –p 1-65535 205.205.205.0/24	All the ports on 205.205.205.1 are closed ---------- Interesting ports on (205.205.205.2): (The 65533 ports scanned but not shown below are in state: closed) Port State Service 23/tcp open telnet 1467/tcp open csdmbase ---------- To rest of the sever: 65535 scanned ports are filtered
DMZSvr tcpdump	NONE
Log from firewall	106015: Deny TCP (no connection) from 205.205.205.200/53 to 192.168.1.200/1349 flags FIN PSH URG omitted the rest.

- External Null Scan

Nmap –v –g53 –sN –P0 –p 1-65535 205.205.205.0/24	All the ports on 205.205.205.1 are closed ---------- Interesting ports on (205.205.205.2): (The 65533 ports scanned but not shown below are in state: closed) Port State Service 23/tcp open telnet 1467/tcp open csdmbase ---------- To rest of the sever: 65535 scanned ports are filtered
DMZSvr tcpdump	NONE
Log from firewall	106015: Deny TCP (no connection) from 205.205.205.200/53 to 192.168.1.200/4600 flags Omitted the rest.

- External Ack Scan

Nmap –v –R –g53 –sA –P0 –p 1-65535 205.205.205.0/24	Interesting ports on (205.205.205.2): (The 65533 ports scanned but not shown below are in state: closed) Port State Service 23/tcp open telnet 1467/tcp open csdmbase ---------- To rest of the sever: 65535 scanned ports are filtered
DMZSvr tcpdump	NONE
Log from firewall	106015: Deny TCP (no connection) from 205.205.205.200/53 to 192.168.1.200/3500 flags ACK Omitted the rest.

From above charts, we see that PIX successfully blocked ACK, NULL, Xmas and FIN scan to the servers it protects. The results are what we expected that a primary firewall should do. However, it cannot successfully protect itself from crafted packets.(ports 23/tcp and 1467/tcp). GIAC definitely has to disable secure telnet service and make sure the latest patch fix is installed.

DMZ Scan

At this step, we are going to conduct TCP SYN and UDP scan on DMZ interface to verify the rules. From previous test, GIAC have a very good idea about how firewall is going to guard the protected network from craft packets. FIN, ACK, NULL , XMAS scans will not be repeated since pretty much we know the results. GIAC will only scan ip from 192.168.1.100-254 since that range is NAT/PAT range trough PIX, anything above is the actual severs in DMZ.

- DMZ SYN scan

DNS sever, External mail server, Web and Proxy all will response to the scan at various ports. Here the focus is the traffic from DMZ to internal.

Nmap –v –g53 –sS –sR –P0 –p 1-65535 192.168.1.100-254	scanned ports on all detected hosts are filtered.
InSvr tcpdump	NONE
Log from firewall	…… 106019: IP packet from 192.168.1.200 to 192.168.1.100, protocol 6 received from interface "dmz" deny by access-group "acl_dmz" ……

If we are going to craft the packets to forge the source 192.168.1.10 (mail server) and 192.168.1.30 (Web server), we will see three connections are allowed. The syslog from PIX:

302001: Built inbound TCP connection 100 for faddr 192.168.1.10/53 gaddr 192.168.1.110/25 laddr 192.168.1.10/25
302001: Built inbound TCP connection 101 for faddr 192.168.1.30/53 gaddr 192.168.1.112/7000 laddr 192.168.30.12/7000
302001: Built inbound TCP connection 102 for faddr 192.168.1.30/53 gaddr 192.168.1.116/8000 laddr 192.168.30.16/6000

Those results are exactly what we want. Firewall only allows external web sever connect to internal application servers through port 7000/tcp and 8000/tcp; and permits external mail server send smtp request to the internal mail server.

- DMZ UDP scan

All the UDP ports should be closed. Below are the results. Even if we change the source ip address to be 192.168.1.10 or .30, we still get the same result.

Nmap –v –g53 –sU–P0 –p 1-65535 192.168.1.100-254	scanned ports on all other detected hosts are filtered.
InSvr tcpdump	NONE
Log from firewall	106007: Deny inbound UDP from 192.168.1.10/0 to 192.168.30.10/59 due to DNS Query Omitted the rest

Step 2. Test the services

GIAC is also going to audit the public services on DMZ zone by using nessus. Through the protection of the firewall, those services shouldn't have too much vulnerability from security checks.

On ExSvr, GIAC is going to enable all the security checks including the denial of services plugins since GIAC want to see how the environment is going to response DoS type of attacks. This test is not an IDS evasion test; any IDS related scan would not be conducted. Since the extensive nmap scan has been conducted early, at this stage GIAC will only do a simple snmp port scan. After scan all the servers on 205.205.205.0/24, the following is the result.

- Non-random IP Ids

All the hosts get warning about non-random IP Ids. This may be used for port scanning and other things. Since it's vendor related and has low risk, GIAC will leave as it is.

- Border router

We got one warning for 205.205.205.1 about is icmp services.

> Warning found on port general/icmp
>
> The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols.
>
> Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).
>
> Risk factor : Low CVE : CAN-1999-0524

Since icmp has to be turned on for troubleshooting, GIAC is going to leave it as it is. ICMP will only be permitted from 205.205.205.0/24 anyway.

- PIX

For PIX itself, nessus gives out the following warning:

> Information found on port general/tcp
>
> Nmap found that this host is running Cisco PIX 515 or 525 running 6.2(1)

It detects firewall's vender and software version. By using this information, a hacker could use known PIX vulnerability to launch various attacks against GIAC. Administrator is going to inform Cisco about this.

- External web server

Information found on port http (80/tcp)
The remote web server type is:

Apache/2.0.40 (Red Hat Linux)

Solution : You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

- External DNS server

Information found on port domain (53/tcp)

The remote bind version is :
9.2.1

Above warnings remind GIAC that all the services should only supply bogus version information to the public.

Step 3. Ingress filtering audit

GIAC is also going to test that if non-routable address or fragmented packets can pass the firewall. This audit is going to conduct from one of administers home high-speed access modem. This setting is more realistic since non-routable addresses are going to be blocked by the border router instead of the primary firewall. Some people will double the defense by also blocking non-routable addresses on the primary firewall. However, from GIAC's architecture, there is no any other server physically sits on 205.205.205.0/24 network; it is remotely possible that an attack could be initiated directly form that segment. GIAC chooses not to block the non-routable address on its primary firewall's external interface.

- Ingress filter audit

First we will craft the packet to claim that our source ip is 10.10.10.10 and watch the web server if it gets any packets.

From Home Nmap –v –R –sR –S 10.10.10.10 –P0 –p80 205.205.205.30	Port State Service 80/tcp filtered http
Web tcpdump	NONE
Firewall syslog	NONE

- Fragmentation

Second, we will send some fragmented packets to port 22 on web server. All the DMZ severs has port 22 open to internal users for remote access. We want to see if the fragmentized packets could pass through the firewall.

Without fragmentation, of cause the packet will be dropped.

```
#/usr/sbin/hping -V -d 40 -c 3 --syn -p 22 205.205.205.30
using eth0, addr: 206.206.206.200, MTU: 1500
HPING 205.205.205.30 (eth0 205.205.205.30): S set, 40 headers + 40 data bytes

--- 205.205.205.30 hping statistic ---
3 packets tramitted, 0 packets received, 100% packet loss
```

With fragmentation,

hping2 -V --frag --data 40 -c 3 --syn -p 22 205.205.205.30	# /usr/sbin/hping -V --frag -d 40 -c 3 --syn -p 22 205.205.205.30 using eth0, addr: 206.206.206.200, MTU: 1500 HPING 205.205.205.30 (eth0 205.205.205.30): S set, 40 headers + 40 data bytes --- 205.205.205.30 hping statistic --- 3 packets tramitted, 0 packets received, 100% packet loss
DMZSvr tcpdump	1 0.00000 205.205.205.200 -> 192.168.1.30 TCP IP fragment ID=204 Offset=48 MF=0 TOS=0x0 TTL=64 2 0.99848 205.205.205.200 -> 192.168.1.30 TCP IP fragment ID=204 Offset=48 MF=0 TOS=0x0 TTL=64 3 0.99879 205.205.205.200 -> 192.168.1.30 TCP IP fragment ID=204 Offset=48 MF=0 TOS=0x0 TTL=64
Firewall log	106019: IP packet from 206.206.206.201 to 205.205.205.30, protocol 6 received from interface "outside" deny by access-group "acl_outside" 106019: IP packet from 206.206.206.201 to 205.205.205.30, protocol 6 received from interface "outside" deny by access-group "acl_outside" 106019: IP packet from 206.206.206.201 to 205.205.205.30, protocol 6 received from interface "outside" deny by access-group "acl_outside"

Even though PIX claims that it blocked ssh access, web server still gets the second part of fraged packets. PIX has a feature called frag guard could prevent fragmentation. Should GIAC enable this feature, see details on next section.

Step 4. Verify outbound traffic

- Verify NAT and PAT

First of all, GIAC wants to verify that NAT is actually working.

This test is fairly simple; GIAC would do a ping scan from proxy server to ExSvr's port 22(SSH), and monitor the packets getting into ExSvr. The connection should be permitted by the firewall.

```
Proxysvr# nmap –v –sR –sS –p22 205.205.205.200
exsvr#/usr/sbin/tcpdump
tcpdump: listening on eth0
18:14:53.303974 205.205.205.241.61296 > 205.205.205.200.22: S
3182867575:3182867575(0) win 1024
18:14:53.304131 205.205.205.200.22 > 205.205.205.241.61296: S
2589814039:2589814039(0) ack 3182867576 win 5840 <mss 1460> (DF)
```

- Outgoing traffic from DMZ

Secondly, only limited servers has limited connection permission to external network, we going to verify that. We will do a SYN scan from DMZsvr to ExSvr, and monitor if there are packets that reach ExSvr.

```
dmzsvr# nmap –v –sR –sS –p1-65535 205.205.205.200
exsvr#/usr/sbin/tcpdump
tcpdump: listening on eth0
```

ExSvr doesn't see any packets because all are blocked by firewall. If we forge the source ip becomes ExDNS, or ExMailSvr, then we only see ExDNS are allowed to ExSvr's 53/tcp&udp, 123/tcp, and ExMailSvr are allowed to connect to ExSvr's 25/tcp, 123/tcp.

- Chatty protocols

No internal users should have access directly to internet. GIAC is going to test if that is the case.

From internal test machine we will scan external test server.

```
intsvr# nmap –v –sR –sS –p1-65535 205.205.205.200
exsvr#/usr/sbin/tcpdump
tcpdump: listening on eth0
```

ExSvr doesn't see any packets either. Clearly, the rules are properly setup.

Step 5. Access directly to PIX

Direct access to PIX is only allowed through ssh from syslog server. GIAC use ssh and telnet from three test machines and confirmed that is the case.

3.3 Audit report

After the auditing, security control team presents the audit result with couple recommendations.

Audit result

Firewall policy

Overall, the policies implemented on firewall meet business and security requirements. Through TCP SYN and UDP scans, audit concludes that (besides the firewall itself) all the firewall rules intended to permit ip traffic are effectively working. And all the other traffic is being blocked.

Audit also found PIX successfully blocked ACK, NULL, Xmas and FIN scan to the servers it protects. The results are what we expected that a primary firewall should do. Audit team had conduct massive scans with various scan technique, and didn't find any bleach.

PIX itself

The scan conducted on firewall itself though, is a little surprise. During the scan to PIX itself, team discovers that two ports 23/tcp and 1467/tcp response to FIN or NULL scan. However, telnet is not even turned on external interface, but the scan indicates telnet service is still listening. Second, GIAC never know there is anther service available on port 1467. After research, GIAC realizes that network service is PIX Secure Telnet (TCP 1467) for policy manager.

After extensive investigation on PIX documentation, team finds it is a known vulnerability.[14] This may allow certain spoofed packets to pass through the firewall and may allow denial of service. GIAC should contact CISCO as soon as possible to apply the patch.

Furthermore, from analyzing the network architecture, audit concludes that GIAC's network has no redundancy. From border router to internal router, they are all full single failure points. For PIX firewall, GIAC should consider adding a secondary PIX. Not only will it improve the stability of the overall network, but also it is going to ease the administration. Admin could always patch and upgrade the standby peer first to test the procedure, and then touch the production. Since Cisco gives great discount on second unit, audit strongly suggest GIAC network group reconsider its decision. (Please refer to Section 1.3 page 11: Redundancy and High Availability)

Finally in ingress filtering audit, team found that PIX leaks crafted fragmented packets. Even though PIX has frag guard to prevent fragmentation, it will also block legitimate fragmented packets. GIAC's web page needs to be accessed by all kind of users including dial-up. Fragmentation has to be used to accommodate different LAN speed

[14] http://www.securitytracker.com/alerts/2001/Mar/1001127.html

and protocols. Since all the servers have netfilter installed. Iptable configurations should be double checked to ensure that intruded fragmentized packets cannot get to the servers.

Services

From nessus scan, audit doesn't find serious vulnerability on servers. This is the result of tech team's best efforts to always keep the latest software updates.

Nessus reports do correctly give out the various applications' version information. Audit team realizes that some of so called vulnerability checks are based on version information. It is recommended to setup bogus version information for web, e-mail and DNS servers. Even though the bogus information will not block the attack itself, at least it adds an extra layer of protection from hackers.

Outbound traffic

There is no chatty protocol leaving GIAC premise unintentionally. Also the outbound traffic to Internet is properly NATed, which hides GIAC internal network schema.

Recommendation

As analyzed, the following should be implemented immediately:

- Add secondary PIX firewall to reduce the single point failure.
- Enforce the netfilter rules on dmz servers to prevent fragmentation.
- Set up bogus version information for public applications
- Contact PIX support to get latest patch for two "open" ports on PIX

Furthermore, GIAC should consider the following in the long-term planning.
.

- Setup a change control policy

During auditing, our team find that the changes made in our core devices are initiated by tech teams' managers or technicians themselves. There are no authorization or documents to justify the reason. So far, there is no major incident related to unauthorized change yet. When GIAC business grows, network complexity will increase and support team will get expended. One unnecessary change or error might cause the whole network crash. All the changes, particularly the changes on firewall and border router should have risk assessment and management approval before implementation. A comprehensive change control policy is the guarantee towards daily operation success.

- Schedule routing audit regularly

GIAC's network is maintenance by multiple technical groups. To ensure that company's policy is fully implemented and consist, audit is the most effective way. It shouldn't be difficult to schedule a routing audit if the first attempt is well documented.

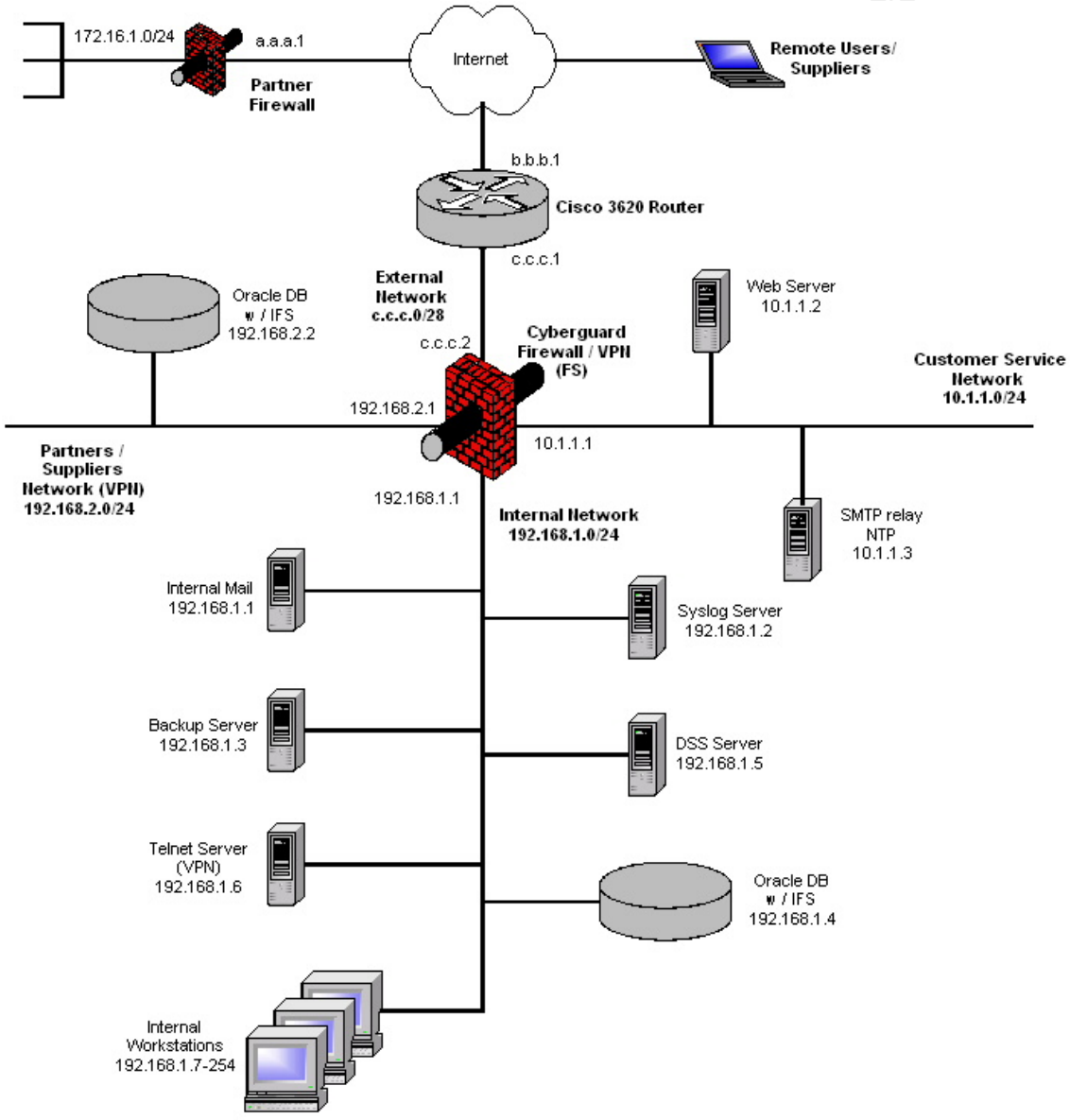
- Enable MAC Address Security on dmz switches

Although there are explicit rules on PIX controlling what kind of traffic could leave DMZ, there is no way to control who can be plugged into the DMZ segment. You never know that one day, one of internal employees might plug his/her desktop into an empty jet port, which is configured to DMZ vlan, and start to download mp3 using web sever's ip address. To make sure our online business goes as smoothly as possible, it is recommended to active Cisco MAC address security feature on switches in the DMZ zone. Media Access Control (MAC) address security allows switch to block input to an Ethernet or Fast Ethernet port when the MAC address of a station attempting to access the port is different from the configured MAC address. [15]

15 http://www.cisco.com/en/US/products/hw/switches/ps679/products_configuration_guide_chapter09186a008007f001.html

Charter 4: Assignment 4 – Design under the fire

We are going to use Kent Stout's practical design for this assignment. The detailed document could be found at http://www.giac.org/practical/Kent_Stout_GCFW.doc. Figure4-1 is his design on visio.



4.1 An attack against firewall

As Kent stated in his document, I haven't seen any security vulnerability related to Cyberguard yet. That is partly due to its unique multi-layered operation system architecture, and partly due to its "popularity" in security community. With its newer released appliance, Ver 4 with PSU5 or Ver5.0 with PSU3, the stability is improved especially for clustered system; however, there are still some bugs. We will try to use these bugs to attack the firewall.

Bug 1: Firewall cannot properly archive the auditing files on HA active peer

To avoid auditing files filling up the file system, Cyberguard has an archiving process to compress audit files and store them to archive directories. Cyberguard provides two methods to control the size of the audit directory. Option one: keep certain days' files. Option two: keep the size of audit file system /var under certain percentage. Whichever criteria is met first, the old audit files will be compressed and moved to /archive directory.

Let's look at the actual scripts from Cyberguard. Two cron jobs were designed to control the archiving process.[16] Auditarc runs daily to compress the n days old (defined in option one) audit files to a big archive file and then move it to /archive directory, the old audit files under /var will then be deleted. Diskarc will run hourly to monitor the size of audit file system /var, if /var exceed 90% full (the default value), auditarc will be executed right away. [17]

The /var partition is 2G bytes on Cyberguard KnightStar appliance. Since diskarc only runs hourly, if anyone could produce over 200M (10%*2G) audit files, he could crash Cyberguard active node easily. Cyberguard is UNIX based software, when /var is full, usually system will change to single user maintenance mode. When the active node crashes, the cluster HA system will fail over to standby.

Bug 2: /var file system fill up on HA standby peer

Even though the standby doesn't pass any traffic, audit process is still up running. It makes sense in a way that it would log any activities on the standby. However, Cyberguard seems to forget that if audit process is up, then archive process should also

[16] Excerpt from cron job:
```
00 02 * * * /usr/sbin/firewall/auditarc
01 * * * * /usr/sbin/firewall/diskarc
```

[17] NETWORK> more /usr/sbin/firewall/diskarc
```
#!/usr/bin/ksh
CURCAP=`df -k /var | awk '/var/ {print $5}' | cut -d % -f1`
export CURCAP
if   [ $CURCAP -ge $CAPACITY ]; then
    /usr/sbin/firewall/auditarc
```

be activated to clean and compress audit files.[18] Depends on the traffic volume and log options on the standby, /var partition (where audit file get stored) will become full in just couple weeks in normal circumstance. Since the OS is built on UNIX, when /var is full, the system cannot provide any resources to the OS, the system will crash.

From Kent's practical, we assume that the firewall audit log will be stored locally. Since this firewall is also acted as application proxies, this firewall should have fairly extensive log options turned on.

The actual attack

1. Reconnaissance

First of all, we have to find out what kind of firewall GIAC is using. From www.netsol.com whois column, we get DNS and mail server's ip addresses for domain giac.org. Against that ip range, we do a nessus scan from port 1 to 65535. Luckily, we found the external DNS server's underlying operation system is SCO UnixWare. Also on the same server, ports 80,443 and 3443 are open. It seems this server is some sort of gatekeeper. It could be SCO UnixWare based Intel server or Cyberguard appliance. Any way, if it is Unix based operation system, we could try to fill the /var to crash the system.

2. Attack

We are going to use hping2 to send 1000 UDP packets/per second to one of the blocked port on firewall. On a 1GHz CPU redhat machine, run the following script

```
While ( 0 < 1 )
    >do
    >hping2 --udp --count 100000 --i u100 –p 1440 –a a.a.a.a
    >done
```

a.a.a.a is a spoofed address. We want to hide our real ip address. –i u100 will send 1000 packets per second.

We keep this simple spoofed port scan continuously for couple hours to fill up the active node's /var directories. How feasible this attack is? Can this simple UDP scan generate 200M audit file in a hour? Well, as an example, I had an environment with Cyberguard firewalls. Three weeks ago, two of internal SQL servers affected SQL worm. They flooded our network by sending hundreds of UDP packets per second to

[18] Excerpt from the script to clean audit file. If the machine is on standby mode, no archive.

```
if [ "$HASTATUS" = "HBM_STANDBY" ] ; then
        ONHA=Standby
      exit 1
     else
```

various hosts' port 1434/udp. The packets sent to public IPs were simply blocked by our firewall (we have policy block all outbound traffic except explicated, 1434/udp outbound is not allowed). In short 20 minutes, they contributed more then 500M audit files on Cyberguard firewall!!!!

When the audit directory is full, the system crashes. The standby supposed to take over when primary is down. However, the backup server is already at single user mode because /var was full a long time ago (Bug 2). Even standby takes over successfully; we could continually scan until the second one crashes. There will be no firewall services unless somebody turns on the magic power button and clean the /var manually. Since the source ip is spoofed , the detection will be very difficult.

3. The Result

The attempt of this hping2 scan is to fill both Cyberguard HA peers' /var partition and then cause underlying OS SCO UnixWare crash. By default, the binary audit logs are stored at /var directory and the system only check the size of the directory every hour. There is great possibility that this approach will success. If both peers are crashed and change to single user mode, there will be no firewall services available. As a result, GIAC network gets disconnected from Internet.

Countermeasure

We strongly recommend GIAC setup a more frequent cron job to make sure the /var and archive directory never become 100% full. Alternatively, GIAC could send all the audit files to an external logging sever (through ftp). Not only could GIAC avoid above bugs, but also could keep the log files' centralized.

4.2 DDOS

We are going to use TFN2K UDP flood to launch a DoS attack against GIAC's DNS server.

There are a lot of DDoS tools available these days such as Trinoo, stacheldracht and TFN…. We prefer TFN2K (a successor of Tribal Flood Network tool) because the communication between the slave and the master is encrypted and silent (No response back from slave), which makes slaves very difficult to be spotted. This tool can launch spoofed UDP, ICMP and TCP SYN flood. Since the GIAC has Cyberguard TCPSYN flood guard enabled, the TCPSYN Flood simply will not work. We tried couple different methods and finally get success from UDP flood attack.

Figure 4-1 illustrates how TFN2K works.

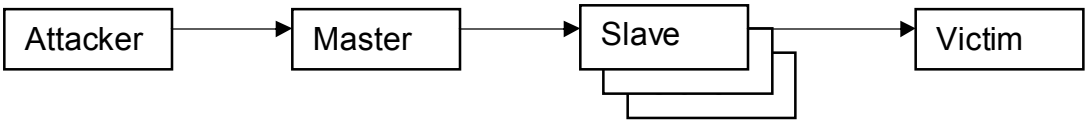


Figure 4-1. How TFN2K works

On all the 50 DSL systems we compromised, install TFN2K slave software and root kits to better hide ourselves. After installation, all the slaves should have td daemon running waiting master to send them the command to start attack.

On master, initiate tfn [19]command to start flood:

```
#./tfn   -c 4  -i c.c.c.1 –p 53

Syntax for tfn is as following
Usage: ./tfn
 [-i target string] Contains options/targets separated by '@',
[-p port] A TCP destination port can be specified for SYN floods
<-c command ID> 4 -  UDP flood
```

The attack will flood firewall's port 53/udp, and consume Cyberguard 100% of the CPU resources to response those crafted packets. Standby will try to take over since the primary freezes; however as long as the continues flood exists, standby will hang in a short period of time. As a result, there will be no firewall services available and GIAC network gets disconnected from the Internet.

Countermeasure

There is no effective way to defeat DDoS attack unless every system on the Internet has comprehensive security feature built in. However, we could take following steps to mitigate the impact.

- Deploy NIDS probes and DDoS filters

  Setup DDos filter devices at the ingress to GIAC network. DDos filters such as Riverhead Guard[20], provide intelligent diversion and adaptive filtering which removes only the malicious traffic while securing Internet availability and ensuring business continuity for legitimate users.

  Deploy DDoS detector or NIDS probes at edge connection points to the Internet. Once probe is connected, it "learns" the normal traffic patterns over the network links, creating baseline thresholds. If a probe identifies a potential threat on a targeted IP, it activates DDoS filter in order to protect the targeted entity.

[19] http://info.hkntec.net/workshop/2002/wk3/day5.html
[20] http://www.riverhead.com

To be more effective, deploy DDoS filters upstream at the ISPs peering or access points while place probes in GIAC premise.

- Setup anti-DDoS channel with ISP

  It will be more effective to defeat DDoS if local Internet Service Provider could get involve in the process. First of all, they could take action to prevent the attack from spreading. Secondly, it will be more bandwidth efficient if local ISP could setup egress/ingress filter on their edge routers (to customers). This way the bandwidth between ISP to good customer is rationalize. Most of the time, even there are filters setup on customer's side, the flood could still fill up the pipe between ISP and the customer.

- Be a good Internet citizen[21]
  Make sure that directed broadcasts is disabled on GIAC network to prevent it from amplifying denial of service attacks. On Kent's design, ICMP is disabled from internal server to public addresses.

- Ingress/egress filter

  Make sure that egress filter on border router drop spoofed ip address leave GIAC network. Or, if using ingress filter, make sure firewall or border router deny private or reserved source ip address. Both actions have been taken by Kent's practical.

- Disallow unnecessary ICMP, TCP, and UDP traffic.

  Disallow UDP and TCP, except on a specific list of ports. For ICPM, only type 3 (destination unreachable) packets should be allowed.

4.3 Attack an internal server through perimeter system

We are going to comprise a remote telecommuter's desktop to access internal database. Internal database server stores lots of contract information with its suppliers and partners which is crucial to GIAC's saying trading business, if we could get hands on to those documents, probably we can sell them to its competitors.

On Kent's design, we could find very good virus and security protection at server level; however, there is no place clearly states prevention at end user level. VPN allows remote user set up an encrypted channel to corporation network through cheap public network infrastructure, but VPN itself protects neither the internal network nor the data transmitted through.

[21] http://www.sans.org/dosstep/index.php

If the remote user doesn't have personal firewall or latest anti-virus software installed, his/her computer is very easily get infected by virus or Trojan software through Microsoft applications. Through Trojan software, an attack could easily gain access to the corporation network.

The following will be our attack attempt:

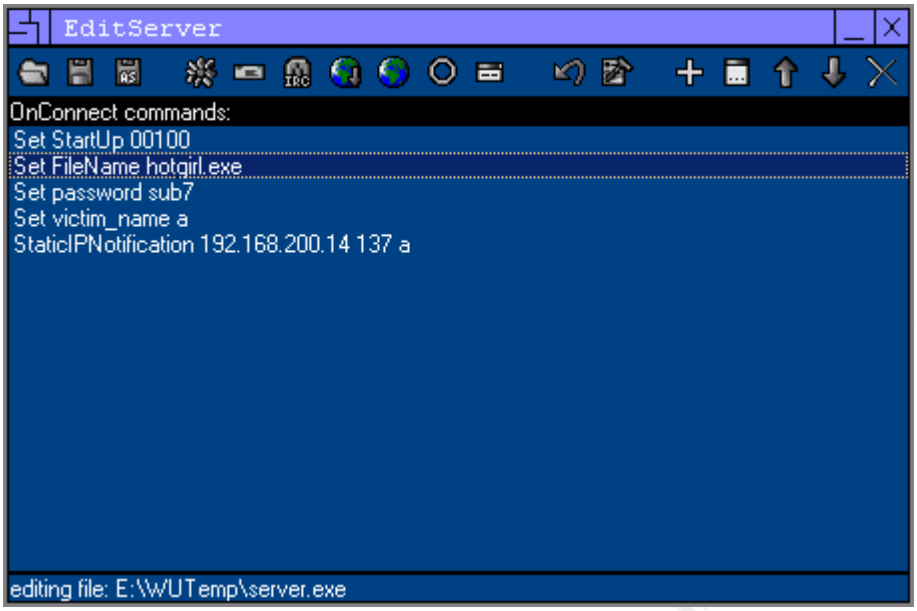
First of all, we are going to comprise couple DSL systems and using them as the base for attacking. Simply, we don't want to get caught when probing GIAC's network. DSL systems without firewall are easy to comprise, use tool such as L0phtCrack[22] to crack the administrator password and we gain full control of those DSL systems.

Second, we are going to find as many valid GIAC e-mail address as possible. From its web site, phone book, yellow page, annual reports, we harvest valid e-mail addresses or employee information. A company like GIAC, the sales people's (nine of ten are telecommuter) information should be easy to get hands on. As a fact, an e-mail address usually is the combination of employee's first and last name.

Thirdly, using social engineer technique send spam messages to GIAC. Those SPAM e-mail will be sent from a DSL system we control. The content of the mail has to be appealing. Since it's close to Valentines Day; we are going to send one of those game link such as "10 ways to test if you are romantic " or "hotgirl". Our hope is to draw some of GIAC employees' curiosity and hopefully they will download that game. The link is crafted and is going to be looks like: http://games.yahoo.com@a.b.c.d/hotgirl.exe. It will be redirect to machine a.b.c.d which we have control of. The link is crafted to looks like from a big commercial site. People usually trust those resources without doubts.

This game actually is a disguised sub7 executable. It could be downloaded from http://www.securityfocus.com/tools/1405. After unpack, run editserver program to configure executable file -- server.exe's setting. Server.exe is the actual Trojan software. Editserver has a feature to bind server.exe with other executables. See the figure below. Since the remote commuter doesn't have anti-virus or firewall software installed, he will not notice that this game he just download actually is a Trojan.

[22] http://www.atstake.com/research/lc4



See, there is one remote GIAC employee is interested to this game. Since he knows that he cannot download executables through VPN connection, he will drop the VPN connection and download that game thorough his Internet connection.

This disguised Trojan uses mail notification to alert us that it has been successfully installed on a victim's desktop. (A hotmail account is used here).

If we got notification, we know we are half way through.

We connect to the sub7 server and start to monitor this VPN user. Sometime later, he re-establishes connection back to GIAC through VPN. Since GIAC didn't use split VPN, we are going to loose him. But Sub7 will actually log the keyboard stroke even off-line.

When we are able to connect to sub7 sever again, we get a fairly good length of log to analyze. If he didn't do too much work and the log didn't catch too much information, we will wait until we collect enough data. At the end, we find that GIAC use static password for VPN authentication; also we harvest some GIAC's internal network information and user login name and password, particularly database account and password! Using the VPN password, we are going to VPN to GIAC through a DSL system. As a salesman, his privilege as a database user probably has read only permission. Nevertheless, that is already good enough for us. From GIAC database, we got internal information such as wholesale prices, contracts with other suppliers etc. GIAC's competitors are willing to pay anything to get these information. We might be able to sell them at a good price.

The attack heavily relies on social engineering. How feasible the attempt it is? Nevertheless, it is worth the try.

Countermeasure[23]

- Setup a policy that requires end users especially remote and mobile users to use properly configured and updated firewall and anti-virus software. Norton anti-virus and Black Ice will be a good choice for GIAC.

- Enforce the policy when end user startup VPN session. There are two purposes. One is to force end user automatically check and download latest virus signature; Two is to check if desktop firewall policy matches with pre-defined VPN client policy.

- Setup network intrusion detection system internally to catch possible Trojan or virus intrusion.

[23] http://www.networkmagazine.com/article/NMG20020603S0004/2

References

Cisco. “CS: Cisco IOS Command Summary, Release 12.2.” URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122sup/122csum/csfindxa.htm#49696

Cisco. “Configuration Forms.” Cisco PIX Firewall Configuration Guide, Version 5.0. URL: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v50/config/cfgforms.htm

Cisco. Cisco PIX Firewall and VPN Configuration Guide, Version 6.2. URL: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_62/config/index.htm

Cisco. “IPSec - PIX to VPN Client Wild-card, Pre-shared, Mode Configuration with Extended Authentication” URL: http://www.cisco.com/warp/customer/110/B.htm

Cisco. Cisco Switches. URL: http://www.cisco.com/en/US/products/hw/switches/ps679

“Distributed Denial-Of-Service (DDoS):TFN2K - An Analysis.” (4 Jun. 2002) URL: http://info.hkntec.net/workshop/2002/wk3/day5.htm

Farrow, Rik. “VPN Vulnerabilities” (6 May, 2002) NetworkMagzine.com URL: http://www.networkmagazine.com/article/NMG20020603S0004/2

Kent Stout. “GCFW Practical assignment - 0338” (Oct. 31, 2002) URL: http://www.giac.org/practical/Kent_Stout_GCFW.doc

SANS. “Help Defeat Denial of Service Attacks: Step-by-Step “ (23 Mar. 2000) URL: http://www.sans.org/dosstep/index.php

SANS. Track 2 – Firewalls, Perimeter protection and VPNs Text Book. The Sans Institute, October 2002

Security tracker. Archives. (20 Mar. 2001) URL: http://www.securitytracker.com/alerts/2001/Mar/1001127.html

Wentzel,James. “What is SubSeven? Giving away control of your machine!” (16Feb. 2001) URL:http://www.sans.org/rr/malicious/subseven2.php

Wright, Joshua; Stewart, John. Securing Cisco Routers: Step-by-Step, Version 1.0. The Sans Institute, August, 2002.