Global Information Assurance Certification Paper

GIAC CERTIFIED FIREWALL ANALYST
Version 3.0

By Jesús Berto
Date: April 20th, 2004

Table of content

ASSIGNMENT 1: SECURITY ARCHITECTURE

1 GIAC BUSINESS OVERVIEW

GE is planning to expand the business in the online of fortune cookie sayings.
GE main offices are located in lima – Peru and all the business is located in this city. They consider expanding the business to other important cities in the country as Ica, Arequipa, Cuzco, Huaraz and Trujillo.

GE is planning to modernize its infrastructure and create an e-business service to facilitate the communication, that is, permits an interaction between users, sellers, buyers, partners, etc in an environment that is not immovable and not even physical.
For that reason, GE has hired our services to implement a solution that protect the information against the misuse of this and prevent that the operations of GE can be interrupted by a hostile attack.

For budget of this year, GE considers to give more important for this first phase to protect internal network from internet rather than internal network from inside.

2 ENTITIES OF THE GIAC BUSINESS

2.1 CUSTOMERS

Giac Enterprise has actually 320 customers registered in GE Data base Servers.
The following table shows services, port or protocol that GE permits Customers to access.

Port/Protocol	Services	Description
80/tcp	Http	Customers' access to GE Web Site, using a web browser, to consult promotions, prices and information about the business.
443/tcp	Ssl	Customers' access to GE Web Site, using a secure web transfer (https) for transactions. Login and password are required.

Table 1. Customers' connectivity

2.2 SUPPLIERS

Giac Enterprise has actually 3 Suppliers registered in GE Data base.

The following table shows services, port or protocol that GE permits Suppliers to access.

Port/Protocol	Services	Description
80/tcp	Http	Suppliers' access to GE Web Site, using a web browser, to consult information about the business.

Table 2. Suppliers' connectivity

2.3 PARTNERS

Giac Enterprise has actually 4 Partners registered in GE Data base servers.
They promote the business of GE cookies sayings in its location, assist customers, and assist GE with the translation of cookie sayings.
As Partner of Giac Enterprise, they translate the sayings for cookies in its location if it is necessary.
The following table shows services, port or protocol that GE permits Partners to access.

Port/Protocol	Services	Description
80/tcp	Http	Partners access GE web site, using a web browser to consult news; promotions and information that can be used for gain new customers in their locations.
443/tcp	Ssl	Customers' access to GE web site, using a secure web transfer (https) for product request and transactions. Login and password are required.

Table 3. Partners' connectivity

2.4 GIAC ENTERPRISES EMPLOYEES LOCATED ON GIAC ENTERPRISE'S INTERNAL NETWORK

Giac Enterprise has actually 25 employees located in the internal network and distributed in different areas of the company.
The following table shows services, port or protocol that GE permits internal employees access to internet.

Port/Protocol	Services	Description

80/tcp	Http	Access to all websites in internet using their web browser (Microsoft Internet Explorer). Access to antivirus servers of the provider.
443/tcp	Ssl	As some suppliers websites needs GE's employees to establish a secure web transfer (https) for transactions, permit access to https. They establish connection using ther web browser: Microsoft Internet Explorer.
25/tcp	SMTP	Access to mail servers in internet to send and receive mails using Outlook Express
53/tcp 53/udp	Dns	Access to dns servers to translate between domain names and ip addresses. GE's external dns server communicates with the two dns servers of the internet service provider.

Table 4. GE's employees' connectivity to internet

Section 1.3.2 shows services in separated machines that compose the GE's internal network.

2.5 GIAC ENTERPRISES MOBILES SALES FORCE AND TELEWORKERS

Giac Enterprise has actually 5 mobile sales force and 3 teleworkers that access to internal network using a security medium.
Mobile sales force and teleworkers need to perform operations to perform his work. They need to access to OMEGA application located in the internal web site of GE. Strong political is implemented for these users, for example, change their password weekly.
Access to GE antivirus update server is needed too.

Port/Protocol	Services	Description
500/tcp 50/ip 51/ip	Vpn	These protocols need to be permitted to establish a vpn between their desktops and the firewall.
80/tcp	http	Mobile sales and teleworkers access to internal web server to make operations according to user privileges.
80/tcp	http	Mobile sales and teleworkers access to GE Antivirus Update Server to download antivirus updates.

Table 5. Remote users connectivity

2.6 THE GENERAL PUBLIC

The following table shows services, port or protocol that Giac Enterprise permits to general public to access.

Port/Protocol	Services	Description
80/tcp	Http	General Public access to GE's web site for information. There isn't any transaction between them and GE.

Table 6. General Public connectivity

3 DESIGN OF THE NETWORK SECURITY ARCHITECTURE FOR GE.

3.1 NETWORK DIAGRAM

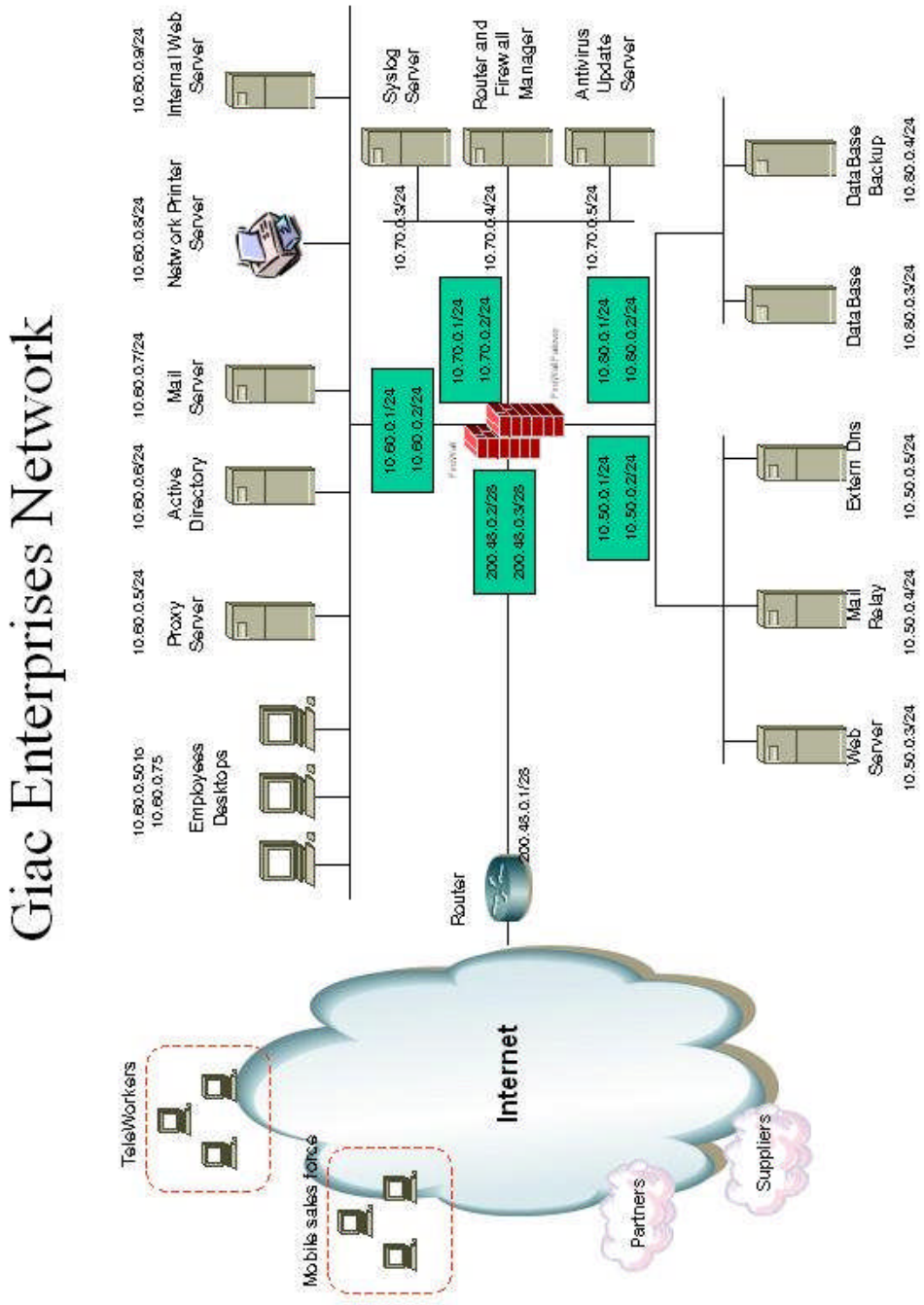


Fig 1

3.2 NETWORK COMPONENTS

3.2.1 FILTERING ROUTER

Model	Version IOS
CISCO2610XM[1]	Cisco IOS Software Release 12.3

Table 7. Border Router Summary

Router name: SCS04100.

The primary purpose of this component is to direct data between GE's internal network and internet. Also the router will be the first line of defense allowing some data packets to pass. The router will be configured to send logs to a internal server when it denies. Logs are very useful to find out possible attacks and bad operation of the router.

GE's technical staff have decided for this router for the following reasons:

- Complete hardware/software solution, no additional OS vulnerabilities or boot-time errors to worry about.
- Cisco support, which is generally very good.
- Performance, probably the best in the business.
- Free upgrades

3.2.2 FIREWALLS

Model	Version IOS
PIX 515E[2]	PIX v6.3(3) Software for the 515E, 525 and 535 Chassis

Table 8. Firewall Summary

Firewall name: SCS04200
Firewall failover name: SCS04201

Pix 515E with Unrestricted Software License.
The purpose of this component on the network is to set up a boundary between the known trustable users on one side and the potentially hackers/crackers on the other.
Additionally to this purpose, the pix firewall has enabled a VPN option to permit GE's mobiles sales and teleworkers access to GE's internal network using a secure connection.
A Vpn Accelerator Card plus is included for a better performance.

Between other features, the firewall permits network address translation (NAT), increasing network privacy by hiding internal IP addresses from internet.
The Pix firewall will generate syslog messages from system events. It will send this messages for document security, resources, system and accounting issues to a syslog server.

The firewall and the firewall failover will have five interfaces that divide the network into five zones: outside, inside, dmz , mngmt and data

- Dmz: This Demilitarized zone is a separate network connected to the firewall for servers available to the public access. Components of this network are web server, mail relay and extern dns.
- Outside: This zone is a separate network with low security. In this zone will be Internet.
- Inside: This zone is a separate network connected to the firewall with high security. Components of this network are desktop computers of GIAC Enterprises employees, networks printers, domain controller servers, mail server, internal dns and internal web servers.
- Mngmt: This zone is a separate network that contains the syslog server and management of router and firewalls. In this zone is permitted to download antivirus update
- Data: This zone is a separate network that contains important servers that GE want to protect for internal users. Components of this network are database servers.

An optional interface is added for failover use.

GE's technical staff have decided for this firewall for the following reasons:

- Complete hardware/software solution, no additional OS vulnerabilities or boot-time errors to worry about.
- Cisco support, which is generally very good.
- Performance, probably the best in the business.
- Free upgrades
- The stateful fail-over option permits not to lost active internet connections.

3.2.3 VIRTUAL PRIVATE NETWORKING (VPN)

The GE's Pix Firewall will be configured as a VPN enabled device.
This VPN consist of a secure, private tunnel between GE's mobile sales force and teleworkers devices and GE's internal network.
The VPN offers a private communication channel over the public access internet, this is, providing confidentiality, integrity and authentication services of the communication between GE's mobile sales force and teleworkers devices and GE's internal network.
Internet wasn't designed to have a lot of security, and more and more people are using it each and every day both for private and business use. For that reason

VPN exists and it is a very well security solution and cost effective for communication between remote sites (teleworkers and mobile sales force) and GE's internal network.
GE considers take advantage of the capacity that Pix Firewall and its failover option has to. Considering this technical issue and also the low number of vpn needed, GE choices to use Pix firewall as a VPN enabled device.

VPN tunnels: 8 (5 mobiles sales and 3 teleworkers). considering to increase this number in the future to 18 tunnels (13 mobiles sales and 5 teleworkers).

3.2.4 OTHER COMPONENTS

Components of GE's network are internal user desktops, internal servers and additionally, desktops or laptops used for the mobiles sales force and teleworkers that communicate with GE's internal network using a VPN tunnel.

All the following components share the following features:

- Microsoft Technology.
- Windows 2000 Operating System. Patched with the latest security hot fixed and hardened according with the Microsoft Windows 2000 security guide. Microsoft provides a security program that regularly delivers service packs, security rollup packages, and security patches in http://www.microsoft.com/windows2000/security/
- Antivirus Software: Etrust Antivirus for desktops and servers. All desktops and server have an agent installed inside, and according to a schedule, connect to the GE antivirus update server with port 80 to update their antivirus database.
- Look at the network diagram (section 1.3.1) to locate the component in the network.

MAIL RELAY

Server name: SCS04400.

The Mail Relay has one main component:

- SMTP content filtering engine

The purpose of this server is to process outgoing and incoming mail, acting as a relay server. It identifies spam from blacklisted sources, scans for viruses, extracts compressed attachments, and performs mime analysis-filtering mail based on keywords in the email header, email body, and email attachments. This accepts mail on behalf of the GE mail server and then delivers the e-mail to GE mail server. Accepts mails from GE mail server using port 25/tcp and then

delivers the mails to other mail servers in internet. More detail of the functionality of this software can be found in the web site of the Etrust SCM[3]

A Mail Relay develops an important role to secure the GE's internal network providing protection against: employee misuse of email, exposure to email legal liability, unsolicited email (spam) and viruses.

Port/Protocol	Services	Description
25/tcp	SMTP	GE Mail Relay accesses to internet using SMTP GE Mail Relay accesses to GE Mail Server using SMTP

Table 9. Mail relay access

PROXY SERVER

Server name: SCS04410

The Proxy Server has one main components:

- Http content filtering engine

The purpose of this server is to control HTTP content, filtering rules and other criteria such as HTML keywords, URL category, file name, and file type (determined by the content signature).

All this functionality can be obtained with Etrust Secure Content Manager[4], a software that is not expensive and has a very good performance.

A Proxy Server develops an important role to secure the GE's internal network providing protection against employee misuse of web, confidentiality breaches, viruses and other offensive material.

GE's employees connect to the GE Proxy Server to access internet using http and https

Port/Protocol	Services	Description
80/tcp	http	GE Proxy Server accesses to internet using http
443/tcp	Ssl	GE Proxy Server accesses to internet using https

Table 10. Proxy Server access

EXTERNAL WEB SERVER

Server name: SCS04420.

GE's Web Site ORIUS is a web-based marketing, sales and transactions. Customers, suppliers, partners, and public in general access to GE Web Server services as it have been mentioned in previous section. Catalogues and on-line stores are designed so customers can look over the wires and fill up a shopping cart and pay by credit card. Business partners obtain information that helps them manage stocks, expansion and finances. To develop these operations, GE Web Server needs to access GE Data Base.

Software Installed:

- Microsoft Internet Information Service 5.0
- E-business applications : ORIUS

Port/Protocol	Services	Description
1433/tcp	Msql	GE Web Server accesses to GE Data Base Servers using port 1433

Table 11. Web Server access

INTERNAL WEB SERVER

Server name: SCS04421

GE's Internal Web Server contains a web based application, and according to privileges, GE internal users login and access to financial, human resources, inventory and so on. To develop these operations, GE Internal Web Server needs to access GE Data Base.
In this design, internal employees and vpn users access to this server.

Software Installed:

- Microsoft Internet Information Service 5.0.
- Web based application : OMEGA

Port/Protocol	Services	Description
1433/tcp	Msql	GE Internal Web Server accesses to GE Data Base Servers using port 1433

Table 12. Web Server access

MAIL SERVER

Server name: SCS04430.
Software Installed:

- Microsoft Exchange 2000.

GE's employees use their Microsoft Outlook Express to send and receive e-mail through this server. This server communicates with the GE Mail Relay Server to interact with internet.

Port/Protocol	Services	Description
25/tcp	SMTP	GE Mail Server accesses to GE Mail Relay Server using SMTP

Table 13. GE Mail Server access

EXTERNAL DNS SERVER

Server name: SCS04450.

For address resolution, two dns servers are implemented; public accessible DNS server on the DMZ and a second DNS server on the internal network side of the firewall. The second dns server is installed in GE Active Directory. GE doesn't have to worry about external network users in internet compromising the internal dns server because people in internet will never see it. The only dns contact external users will have is with the GE External Dns Server

Software Installed:

- Microsoft Domain Name Server.

Following Sans recommendation this is a:
External Dns Server will be non-recursive.
Zone transfer are only allowed to ISP Dns servers
Respond to queries and reverse queries is allowed.

Port/Protocol	Services	Description
53/tcp, 53/udp	domain	GE External Dns Server accesses to ISP Dsns Servers.

Table 14. GE External Dns Server access

DATA BASE SERVER

Server name: SCS04460

Server Backup name: SCS04701.
Software Installed:

- Microsoft SQL Server 2000.

Stores confidential information of the GE's business. GE web server uses information stored in GE Data Base Server or GE Data Base Backup if it is necessary. For that reason it's important to save information of this server. A second database server is implemented as backup.

Port/Protocol	Services	Description
1600/tcp, 2600/tcp	RPC static port for Sql Server replication	GE Data Base Server Backup accesses to GE Data Base Server using port 1600 and 2600 for traffic replication GE Data Base Server accesses to GE Data Base Backup Server using port 1600 and 2600.

Table 15. GE Data Base Servers access

ACTIVE DIRECTORY

Server name: SCS04470

An active directory is implemented to store information about objects on the network making it easier to locate resources for clients and maintain resources for administrators. It is integrated with Kerberos to provide more secure authentications and DNS to locate network services as well to store DNS resource records as AD objects. The internal dns server queries the external DNS when it can not resolve a name. It's recursive and don't allow any zone transfer so there isn't a secondary dns server.

Software Installed:

- Microsoft Active Directory 2000.

Port/Protocol	Services	Description
53/udp	DNS	GE Active Directory accesses to GE External DNS Server using port DNS.

Table 16. GE Active Directory server access

SYSLOG SERVER

Server name: SCS04490

A central point of administration for auditing and alarming is implemented with a syslog server.

Software Installed:

- Syslog Server.

The syslog server receive logging packets from:

- Router
- Firewalls

Port/Protocol	Services	Description
514/tcp	syslog	Router and firewalls to GE Syslog Server access.

Table 17. GE Syslog Server access

ROUTER AND FIREWALL MANAGER.

Desktop name: SCS04510.

The router and firewall have addressed the administration via ssh to the ip address of this desktop. Ssh permits that traffic between the manager and the router or firewall be encrypted.

NETWORK PRINTER SERVER

Server name: SCS04500.
Hewlett Packard LaserJet 4000.
GE's employees share this only printer server.

ANTIVIRUS SERVER.

Desktop name: SCS04600.
Desktops and servers access to this server to maintain their antivirus signature updated. The antivirus update server must to have his antivirus signature updated too, and it's made, accessing to antivirus provider server in internet. Due to the amount of traffic generated by this tasks, they must be made in hours of minor traffic, between 1:00 am to 6:00am

Port/Protocol	Services	Description
80/tcp	http	Antivirus Update Server to antivirus servers in internet. Desktops and server in GE internal network access to

		this server using port 80 to download antivirus update.

Table 18. GE Antivirus Update Server access

EMPLOYEES'S DESKTOPS

Desktops name: SCS08001,SCS08002,SCS08003,SCS08004,….SCS08025
Employees have user rights in their desktops, to prevent of installing software or modify settings. They can read, make, print documents through Microsoft Office and adobe reader, send and receive mails using Microsoft Outlook, access to web sites in internet and to web-base applications for his daily work with internet explorer.

Operating System: Microsoft windows 2000 Professional.
Main software installed:

- Outlook Express
- Microsoft Office 2000
- Adobe Reader 6.0.
- Internet Explorer 6.0

LAPTOPS AND DESKTOPS FROM MOBILES SALES FORCE AND TELEWORKERS

Desktops and Laptops name:
SCS09001,SCS09002,SCS09003,SCS09004,….SCS09008
Operating System: Microsoft windows 2000 Professional.

Main software installed:

- A personal firewall ZoneAlarm
- Cisco Vpn Client.
- Outlook Express
- Microsoft Office 2000
- Adobe Reader 6.0,

3.3 IP ADDRESSING SCHEME

Non-routable addresses internally (RFC 1918) and routable addresses externally

Private Addressing Scheme	10.50.0.0/24 : dmz 10.60.0.0/24 : inside 10.70.0.0/24: mngmt

	10.80.0.0/24: data 10.90.0.0/24: vpn users
Public Addressing Scheme	200.48.0.0/28 : 16 IP address provided for the internet service provider

Table 19. IP Address Scheme

Network Device	Private IP Address	Public IP Address
Router	****	200.48.0.1
Firewall	****	200.48.0.2
Firewall Failover	****	200.48.0.3

Table 20. IP distribution in the outside zone

Network Device	Private IP Address	Public IP Address
Firewall	10.50.0.1	****
Firewall Failover	10.50.0.2	****
Web Server	10.50.0.3	200.48.0.4
Mail Relay	10.50.0.4	200.48.0.5
External Dns	10.50.0.5	200.48.0.6

Table 21. IP distribution in the dmz zone

Network Device	Private IP Address	Public IP Address
Firewall	10.60.0.1	****
Firewall Failover	10.60.0.2	****
Proxy Server	10.60.0.5	****
Active Directory	10.60.0.6	****
Mail Server	10.60.0.7	****
Network Printer	10.60.0.8	****
Internal Web Server	10.60.0.9	****
Employees Desktops	10.60.0.50-10.60.0.75	Nat: 200.48.0.10-200.48.0.11

Table 22. IP distribution in the inside zone

Network Device	Private IP Address	Public IP Address

Firewall	10.70.0.1	****
Firewall Failover	10.70.0.2	****
Syslog Server	10.70.0.3	200.48.0.7
Router and Firewall Manager	10.70.0.4	****
Antivirus Server	10.70.0.5	200.48.0.8

Table 23. IP distribution in the mngmt zone

Network Device	Private IP Address	Public IP Address
Firewall	10.80.0.1	****
Firewall Failover	10.80.0.2	****
DataBase	10.80.0.3	****
Database Backup	10.80.0.4	****

Table 24. IP distribution in the data zone

Network Device	Private IP Address	Public IP Address
Mobile sales force and teleworkers desktops and laptops	10.90.0.1-10.90.0.8	****

Table 25. IP distribution Remote Users

ASSIGNMENT 2: SECURITY POLICY AND COMPONENT CONFIGURATION

1 GE BORDER ROUTER (SCS04100)

1.1 GENERAL

The following commands are used to armor the router itself and add traffic control according to sans recommendations and NSA Security Recommendation guides[5]. I don't have a router available, however in cisco web site can be found a lot of manuals, configuration examples about this router, so this help me to make the configuration.

Hardening the router:

a. Choose a name that does not make it clear what the device is to be used for. A difficult name will make difficult to know what device is.

   Hostname: SCS04100

b. Use a secure encryption password. Useful for keeping unauthorized individuals from viewing the password in the configuration file. (<password>, here, I introduce the password without <>)

   service password-encryption
   enable secret <password>

c. Display a warning so it will prevent unauthorized users

   banner login ^C
   Unauthorized access is prohibited. You are being monitored.
   ^C

d. Turn on the router's logging capability, and use it to log errors and blocked packets to GE internal (trusted) syslog host. Useful for the management of faults.

   logging on
   logging 200.48.0.7
   no logging console

e. Shut down unneeded services on the router. Servers that are not running cannot break and compromise the system. It prevents denial of service attack. Also more memory and processor slots are available.

```
no service tcp-small servers
no service udp-small servers
no ip bootp server
no service  finger
no ip http server
no snmp server
no ip source-route
no service dhcp
```

f. Shut down unneeded services on the router. These services allow certain packets to pass through the router, or send special packets, or are used for remote router configuration.

```
no cdp run
no service config
no ip source-route
no ip domainlookup
no ip classless
no service pad
```

g. Secure interfaces on the router by using certain commands in the configurate interface mode.

```
no ip directed-broadcast
no ip mask-reply
no ip proxy-arp
no ip unreachables
no ip redirects
```

h. Enable SSH (version 1) for management of the router from a host inside GE's network. With this method the management is more secure because traffic is encrypted.

```
crypto key generate rsa
ip ssh time-out 60
ip ssh authentication-retries 5
```

1.2 FILTERING ROULES

The border router acts as the first line of defense, so GE implements access list in the border router to provide basic filtering, permitting and denying traffic across the router.

The syntax of the access list used in this configuration is resumed as follows:

access-list <number 100-199> <permit|deny> <protocol> <source> <sourcemask> <source-port> <destination> <destination-mask> <destination port> <log>

number 100-199 : Extended access-list can take a number between 100 and 199
permit|deny : Permit traffic or deny it
protocol : Protocols being requested, for example: TCP, UDP, ICMP
source : Identity of the source of the packet (ip address, any, range of ip address)
sourcemask : Mask of the source network
source-port : Services I permit or deny access to in source address
destination : Identity of the destination of the packet (ip address, any, range of ip address)
destination-mask : Mask of the destination network
destination port : Services I permit or deny access to in destination address
log :To enable or disabled (if it is omitted) logging of the occurrence. I consider only logging deny occurrences because of the importance to know possible attacks.

Considering the level of security of each interface, rules are needed to permit traffic for one zone to other when is needed and deny traffic when is not necessary. The order of the rules applied in each interface must to be considered due to the top-to-bottom reading of the firewall. When one rule is matched it finished and don't read the next rule. For a better performance of the firewall the order of the rules are important. Rules that are frequently matched go first and then the following and so on.

1.2.1 INCOMING TRAFFIC THROUGH SERIAL 0/0 INTERFACE

a. There are packets whose source ip address are not normal to travel in internet. These packets will be spoofing packets that are trying to exploit a vulnerability. For that reason is convenient to block the entire address space at GE's perimeter.

   Block all traffic with source IP address corresponding to GE's address assignment
   access list 101 deny ip 200.48.0.0 0.0.0.240 any log

   Block loopback address

```
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log

Block broadcast address.
access-list 101 deny ip 255.0.0.0 0.255.255.255 any log

Block packets coming from private RFC1918
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 172.16.0.0 1.15.255.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log

Block packets coming from IANA reserved, private and multicast addresses
access-list 101 deny ip 0.0.0.0 0.255.255.255 any log
access-list 101 deny ip 1.0.0.0 0.255.255.255 any log
access-list 101 deny ip 2.0.0.0 0.255.255.255 any log
access-list 101 deny ip 5.0.0.0 0.255.255.255 any log
access-list 101 deny ip 7.0.0.0 0.255.255.255 any log
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 14.0.0.0 0.255.255.255 any log
access-list 101 deny ip 23.0.0.0 0.255.255.255 any log
access-list 101 deny ip 27.0.0.0 0.255.255.255 any log
access-list 101 deny ip 31.0.0.0 0.255.255.255 any log
access-list 101 deny ip 36.0.0.0 0.255.255.255 any log
access-list 101 deny ip 37.0.0.0 0.255.255.255 any log
access-list 101 deny ip 39.0.0.0 0.255.255.255 any log
access-list 101 deny ip 41.0.0.0 0.255.255.255 any log
access-list 101 deny ip 42.0.0.0 0.255.255.255 any log
access-list 101 deny ip 71.0.0.0 0.255.255.255 any log
…..
access-list 101 deny ip 79.0.0.0 0.255.255.255 any log
access-list 101 deny ip 89.0.0.0 0.255.255.255 any log
…..
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny ip 173.0.0.0 0.255.255.255 any log
…..
access-list 101 deny ip 173.0.0.0 0.255.255.255 any log
…..
access-list 101 deny ip 187.0.0.0 0.255.255.255 any log
access-list 101 deny ip 189.0.0.0 0.255.255.255 any log
access-list 101 deny ip 190.0.0.0 0.255.255.255 any log
access-list 101 deny ip 197.0.0.0 0.255.255.255 any log
access-list 101 deny ip 223.0.0.0 0.255.255.255 any log
…..
access-list 101 deny ip 255.0.0.0 0.255.255.255 any log

Block packets with no IP address.
```

access-list 101 deny ip host 0.0.0.0 any log

b. Permit valid traffic goes into GE's network and finish denying the rest.

Allow HTTP /HTTPS traffic from partners, customers, suppliers and public in general to GE Web Site.
access-list 101 permit tcp any host 200.48.0.3 eq 80
access-list 101 permit tcp any host 200.48.0.3 eq 443

Allow SMTP traffic from Internet to the GE Mail Relay Server.
access-list 101 permit tcp any host 200.48.0.4 eq SMTP

Allow DNS traffic from Provider DNS Servers to the GE External DNS Server.
access-list 101 permit udp host 200.38.23.11 host 200.48.0.5 eq domain
access-list 101 permit udp host 200.38.23.12 host 200.48.0.5 eq domain
access-list 101 permit tcp host 200.38.23.11 host 200.48.0.5 eq domain
access-list 101 permit tcp host 200.38.23.12 host 200.48.0.5 eq domain

Allow VPN traffic to the firewall
access-list 101 permit tcp any host 200.48.0.2 eq 500
access-list 101 permit ip any host 200.48.0.2 eq 50
access-list 101 permit ip any host 200.48.0.2 eq 51

Allow ICMP protocols that are required for normal network operations and are allowed to any address in GIAC public address. All other ICMP packets are dropped.
access-list 101 permit icmp any 200.48.0.0 0.0.0.240 source-quench
access-list 101 permit icmp any 200.48.0.0 0.0.0.240 parameter-problem
access-list 101 permit icmp any 200.48.0.0 0.0.0.240 time-exceeded
access-list 101 permit icmp any 200.48.0.0 0.0.0.240 unreachable

Deny and log the remaining traffic not matched here
access-list 101 deny ip any any log

c. Apply ACLS to outsider: serial0/0

ip access-group 101 in

1.2.2 OUTCOMING TRAFFIC THROUGH ETHERNET 0/0 INTERFACE

The filter we have applied on the ethernet interface is Access List 102:

a. Permit GE internal networking components, with a valid address, access to internet. So, it will block outbound spoofing.

   access-list 102 permit 200.48.0.0 0.0.0.240 any

b. Deny and log the remaining traffic not matched here

   access-list 102 deny any any log

c. Apply ACLS to ethernet0/0

   ip access-group 102 out

1.3 GE FIREWALL (SCS04200 –SCS04201) AND VPN

After install and connect the two firewall units, the primary unit must to be configured. The secondary firewall is updated with the configuration of the first one when the primary is saved.
A tutorial for the configuration of the firewall can be found in the Appendix A. A more complete syntax for all commands used to configure the firewall can be found in cisco web site[6].

1.3.1 BASIC CONFIGURATION

a. Assign names and set security level for the firewall interfaces. Access from one network to other depends of their security level. Traffic from higher levels to lower levels is permitted by default, the inverse is not permitted. According to the importance of the components distributed in the GE network, mngmt is the zone with a hight level of security, follow by data, inside, dmz and outside, in this order.

   nameif ethernet0 outside security0
   nameif ethernet1 dmz security50
   nameif ethernet2 inside security60
   nameif ethernet3 data security80
   nameif ethernet4 mngmt security100

b. Set each ethernet interface the speed and type of operation. I use auto mode because It will be more flexible when the firewall connects to differents models of hubs and switches.

   interface ethernet0 auto
   interface ethernet1 auto
   interface ethernet2 auto
   interface ethernet3 auto

interface ethernet4 auto

c. Set an encrypted password for the configuration. Useful for keeping unauthorized individuals from viewing your password in your configuration file . As (<password>, here, I introduce the password without <>)

enable password <password> encrypted
passwd <password> encrypted

d. Assign hostname of the firewall. As router name assign, the name must not be easy.

hostname SCS04200
domain-name cisco.com

e. Enable application inspection for the protocols. Inspect the application-layer commands being passed over these protocols: http and smtp

fixup protocol http 80
fixup protocol SMTP 25

The following command specifies the maximum DNS packet length. DNS requires application inspection so that DNS queries will not be subject to the generic UDP handling based on activity timeouts. Instead, the UDP connections associated with DNS queries and responses are torn down as soon as a reply to a DNS query has been received. This functionality is called DNS Guard. [7]

fixup protocol dns maximum-length 1500

no fixup protocol h323 h225 1720
no fixup protocol h323 ras 1718-1719
no fixup protocol ils 389
no fixup protocol rsh 514
no fixup protocol rtsp 554
no fixup protocol sip 5060
no fixup protocol skinny 2000

f. According the address table in the previous assignment, GE defines the IP address for each interface.

ip address outside 200.48.0.2 255.255.255.240
ip address dmz 10.50.0.1 255.255.255.0
ip address inside 10.60.0.1 255.255.255.0
ip address data 10.80.0.1 255.255.255.0
ip address mngmt 10.70.0.1 255.255.255.0

g. Enable the "flood defender" to protect against flood attacks. The floodguard command lets us reclaim PIX Firewall resources if the user authentication (uauth) subsystem runs out of resources. If an inbound or outbound uauth connection is being attacked or overused, the PIX Firewall will actively reclaim TCP user resources[8]

```
floodguard enable
```

h. Enable sending notification messages to The GE syslog server. (messages: emergencies, alerts, critical, errors, warnings, notifications). Specify that the messages send to the syslog server has a time stamp value. Disable logging console if it's enable, that is, to avoid degradation of the firewall performance.

```
logging timestamp
logging trap notifications
no logging console
logging host mngmt 10.70.0.3
logging on
```

i. Disable firewall to send SNMP traps because GE doesn't have a system to receive them.

```
no snmp-server
no snmp-server location
no snmp-server contact
no snmp-server enable traps
```

j. Set the default route to be 200.48.0.1. All traffic that is not defined to route to another network are sent by default to internet thought the router.

```
route outside 0.0.0.0 0.0.0.0 200.48.0.1 1
```

k. Permit GE Router and Firewall Management workstation accesses to the firewall using SSH version 1 . SSH is more secure than telnet because data travels encrypted[9]. First I generate RSA key pairs for the PIX Firewall and then assign my host 10.70.0.4 who will initiate the SSH connection.

```
ca generate rsa key 1024
ca save all
ssh 10.70.0.4 255.255.255.255
ssh timeout 60
```

1.3.2 FILTERING RULES

Syntax of access list implemented in pix firewall is similar to the syntax of access list used in router configuration. The top-to-bottom reading and the importance of the order of the access rules are applied here too.

OUTSIDE ACCESS

In this zone, there are some public services that are accessible to internet. There is a web server, mail server and the dns server. It is clear that before the mails server that is located in the internal zone, exist a mail relay that will forward the traffic to the mail server located in another zone. Also, the firewall must permit that log traffic generated by the router can arrive to the syslog server.

a. Define a static nat translation to permit traffic from internet to public servers in the dmz zone and mngmt zone. By default the number of embryonic connection per host and the maximum number of simultaneous TCP and UDP connections for the entire subnet are zero[10] To prevent denial of service of these public servers, these numbers are applied.

   GE web server translation
   static (dmz, outside) 200.48.0.4 10.50.0.3 netmask 255.255.255.255 0 0 300 500

   GE Mail Relay server translation
   static (dmz, outside) 200.48.0.5 10.50.0.4 netmask 255.255.255.255 0 0 300 500

   GE External DNS server translation
   static (dmz, outside) 200.48.0.6 10.50.0.5 netmask 255.255.255.255 0 0 300 500

   GE Syslog server translation
   static (mngmt, outside) 200.48.0.7 10.70.0.3 netmask 255.255.255.255 0 0 300 500

b. Permit HTTP/HTTPS traffic from anywhere to GE web server.

   access-list 101 permit tcp any host 200.48.0.4 eq 80
   access-list 101 permit tcp any host 200.48.0.4 eq 443

c. Permit SMTP traffic from anywhere to GE Mail Relay server.

   access-list 101 permit tcp any host 200.48.0.5 eq 25

d. Permit traffic from provider dns servers to GE external dns server.

access-list 101 permit udp host 200.38.23.11 host 200.48.0.6 eq 53
access-list 101 permit udp host 200.38.23.12 host 200.48.0.6 eq 53
access-list 101 permit tcp host 200.38.23.11 host 200.48.0.6 eq 53
access-list 101 permit tcp host 200.38.23.12 host 200.48.0.6 eq 53

e. Permit SYSLOG traffic from the border router to GE syslog server.

   access-list 101 permit udp host 200.48.0.1 host 200.48.0.7 eq 514

f. Deny and log the remaining traffic not matched here.

   access-list 101 deny ip any any

g. Apply the access-list 101 on the outside interface

   access-group 101 in interface outside

DMZ ACCESS

The firewall must permit that traffic generate by servers in this zone can arrive to their destination.

a. Define a static nat translation to permit traffic from dmz to servers in the inside zone, data zone and mngmt zone.

   GE Data Base Servers translation
   static (data, dmz) 10.80.0.3 10.80.0.3 netmask 255.255.255.255 0 0
   static (data, dmz) 10.80.0.4 10.80.0.4 netmask 255.255.255.255 0 0

   GE Mail Server translation
   static (inside, dmz) 10.60.0.7 10.60.0.7 netmask 255.255.255.255 0 0

   GE Antivirus Server translation
   static (mngmt, dmz) 10.70.0.5 10.70.0.5 netmask 255.255.255.255 0 0

b. Permit SQL traffic from GE web server to GE Data Base and GE Data Base Backup.

   access-list 102 permit tcp host 10.50.0.3 host 10.80.0.3 eq 1433
   access-list 102 permit tcp host 10.50.0.3 host 10.80.0.4 eq 1433

c. Permit SMTP traffic from GE Mail Relay to GE Mail Server

access-list 102 permit tcp host 10.50.0.4 host 10.60.0.7 eq 25

d. Permit antivirus download traffic (HTTP) from dmz zone to GE antivirus server.

   access-list 102 permit tcp 10.50.0.0 255.255.255.0 host 10.70.0.5 eq 80

e. Deny and log the remaining traffic not matched here.

   access-list 102 deny ip any any

f. Apply the access-list 102 on the dmz interface

   access-group 102 in interface dmz

INSIDE ACCESS

In this zone, desktops of employees access to internet through a proxy server, mail server needs to access to the mail relay to receive clean mails and send mails to internet through this mail relay. Internal and remote users access to the application OMEGA in the internal web server. This server accesses to database server located in other zone to send and received data necessary to perform operations.

a. Traffic generated by internal zone of the GE network can go out to internet with the origin ip address translated by one of this pool of legal IP addresses.

   global (outside) 1 200.48.0.10-200.48.0.11 netmask 255.255.255.240
   nat (inside) 1 10.60.0.0 255.255.255.0 0 0

b. Define a static nat translation to permit traffic from inside zone to servers in the data zone and mngmt zone.

   GE Data Server translation
   static (data, inside) 10.80.0.3 10.80.0.3 netmask 255.255.255.255 0 0
   static (data, inside) 10.80.0.4 10.80.0.4 netmask 255.255.255.255 0 0
   GE Antivirus Server translation
   static (mngmt, inside) 10.70.0.5 10.70.0.5 netmask 255.255.255.255 0 0

c. Permit users on the inside zone access to internet through a proxy server. The PCs in the internal zone must to be configured to use a proxy server in the LAN and don't use a proxy with local addresses.

   access-list 103 permit tcp host 10.60.0.5 any eq 80

access-list 103 permit tcp host 10.60.0.5 any eq 443

d. Permit SMTP traffic from GE Mail Server to GE Mail Relay.

   access-list 103 permit tcp host 10.60.0.7 host 10.50.0.4 eq 25

e. Permit recursive dns queries from GE internal dns (a service in GE active directory server) to GE external dns server.

   access-list 103 permit udp host 10.60.0.6 host 10.50.0.5 eq 53

f. Permit SQL traffic from GE internal web server to GE database servers.

   access-list 103 permit tcp host 10.60.0.9 host 10.80.0.3 eq 1433
   access-list 103 permit tcp host 10.60.0.9 host 10.80.0.4 eq 1433

g. Permit antivirus download traffic (HTTP) from inside zone to GE antivirus server.

   access-list 103 permit tcp 10.60.0.0 255.255.255.0 host 10.70.0.5 eq 80

h. Deny and log the remaining traffic not matched here.

   access-list 103 deny ip any any

i. Allow traffic, access-list 103, with no nat use when this traffic is where zones with high level to low level of security.

   Nat (inside) 0 access-list 103

j. Apply the access-list 103 on the inside interface

   access-group 103 in interface inside

MNGMT ACCESS

In this zone, the management host access to the router and firewall for administration purposes, antivirus server performs updates of desktops and servers in the GE network.

a. Define a static nat translation to permit traffic from the router to the syslog server and from the provider antivirus servers to the GE antivirus server.

   GE syslog server translation
   static (mngmt,outside) 200.48.0.7 10.70.0.3 netmask 255.255.255.255 0 0

GE antivirus server translation
static (mngmt,outside) 200.48.0.8 10.70.0.5 netmask 255.255.255.255 0 0

b. Permit HTTP traffic from GE antivirus server to the provider antivirus server to download antivirus updates.

access-list 104 permit tcp host 10.70.0.5 host 200.23.21.22 eq 80
access-list 104 permit tcp host 10.70.0.5 host 200.23.21.33 eq 80

c. Permit HTTP traffic from GE antivirus server to GE desktops and servers in the dmz zone, inside zone and data zone.

access-list 104 permit tcp host 10.70.0.5 10.50.0.0 255.255.255.0 eq 80
access-list 104 permit tcp host 10.70.0.5 10.60.0.0 255.255.255.0 eq 80
access-list 104 permit tcp host 10.70.0.5 10.80.0.0 255.255.255.0 eq 80

d. Permit SSH traffic from GE router and firewall management to the router

access-list 104 permit tcp host 10.70.0.4 host 200.48.0.1 eq 22

e. Deny and log the remaining traffic not matched here.

access-list 104 deny ip any any

k. Allow traffic, access-list 104, with no nat use when this traffic is where zones with high level to low level of security.

Nat (inside) 0 access-list 104

f. Apply the access-list 104 on the mngmt interface

access-group 104 in interface mngmt

DATA ACCESS

In this zone antivirus update is needed in the data base servers.

a. Define a static nat translation to permit traffic from the data base servers to the antivirus server in the mngmt zone.

GE antivirus server translation
static (mngmt,data) 10.70.0.5 10.70.0.5 netmask 255.255.255.255 0 0

b. Allow traffic, access-list 105, with no nat use when this traffic is where zones with high level to low level of security.

   Nat (inside) 0 access-list 105

c. Permit traffic HTTP from all servers in the data zone to the antivirus update server.

   access-list 105 permit tcp 10.80.0.0 255.255.255.0 host 10.70.0.5 eq 80

d. Deny and log the remaining traffic not matched here.

   access-list 105 deny ip any any

e. Apply the access-list 104 on the data interface

   access-group 105 in interface data

1.3.3 CONFIGURATION OF THE FAILOVER OPTION

For stateful failover, GE considers to add a 6th interface in the pix, "sfa", to be used exclusively for passing state information between the two firewalls units. More detail of the configuration of the failover option can be found in cisco web site[11]. A tutorial for the implementation of this option can be found in the appendix A.

Assign IP address to each interface of the failover and configure stateful failover. In this configuration, GE assigns the maximum value (15) for the transmission of the failover packets between the primary and the secondary firewalls.

```
failover
failover poll 15
failover ip address outside 200.48.0.3
failover ip address dmz 10.50.0.2
failover ip address inside 10.60.0.2
failover ip address mngmt 10.70.0.2
failover ip address data 10.80.0.2
failover ip address sfa 10.90.0.2
failover link sfa
```

1.3.4 CONFIGURATION OF THE VPN OPTION

Because of the number of people (8 in total), and similar access to GE network, I will create only one group called groupmobile. A tutorial for the implementation of this option can be found in the appendix A.

The IOS version 6.3 of the pix has the following methods:

- encryption algorithm: aes, aes-192, aes-256, des, 3des,
- hash algorithm: md5 y sha
- authentication method: pre-share y rsa-sig

Actually, GE don't have a CA available. In the future, it will be consider because it's more secure than pre-share.

Considering the strong of the method and then the speed, GE chooses the following configuration:

Protocols	Encryption Algorithm	Hashing algorithm	Authentication method
Ipsec	Aes-256	SHA	Pre-shared

Table 26. VPN Tunnel Configuration

a. Permit VPN users in internet connects to GE internal web server and GE antivirus server. Traffic to both servers are HTTP. Do not use NAT for inside-to-pool traffic as this should not go through NAT

   access-list 106 permit tcp 10.90.0.0 255.255.255.0 host 10.60.0.9 eq 80
   access-list 106 permit tcp 10.90.0.0 255.255.255.0 host 10.70.0.5 eq 80
   Nat (inside) 0 access-list 106

b. Create a pool of addresses from which IP addresses are assigned dynamically to the remote VPN Clients. This pool was determined in the previous assignment.

   ip local pool vpnpool1 10.90.0.1 - 10.90.0.8

c. Permit encrypted traffic

   sysopt connection permict-ipsec

d. Define the transform set to be used during IPSec security association (SA) negotiation. Specify the configuration as show in table ZZZZ.

crypto ipsec transform-set trmset1 esp-aes-256 esp-sha-hmac

e. Create a dynamic crypto map entry and add it to a static crypto map. For mobile users is convenient to create a dynamic crypto map entry.

crypto dynamic-map map2 10 set transform-set trmset1
crypto map map1 10 ipsec-isakmp dynamic map2

f. Bind the crypto map to the outside interface.

crypto map map1 interface outside

g. Enable Internet Security Association and Key Management Protocol (ISAKMP) negotiation on the interface on which the IPSec peer communicates with the PIX firewall.

isakmp enable outside
isakmp identity address

h. Define an ISAKMP policy to be used while negotiating the ISAKMP SA. Specify AES as the encryption algorithm.

isakmp policy 10 authentication pre-share
isakmp policy 10 encryption AES
isakmp policy 10 hash SHA
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400

i. Create a VPN group: groupmobile, and configure the policy attributes: pool of address created in step (a), idle timeout to shutdown the connection (30 minutes) and password for the group created (<password>, here, I introduce the password without <>).
For better perfomance, enable split-tunnel applied to access-rule 106 It permits GE's mobiles sales and teleworkers to forward the Internet-destined traffic directly without forwarding it over the encrypted tunnel.

vpngroup groupmobile address-pool vpnpool1
vpngroup groupmobile split-tunnel 106
vpngroup groupmobile idle-time 1800
vpngroup groupmobile password <password>

ASSIGNMENT 3: DESIGN UNDER FIRE

For this section of the practical, I choose the practical assignment v3.0 from Jared McLaren[12].
http://www.giac.org/practical/GCFW/Bien_Jared_McLaren_GCFW.pdf

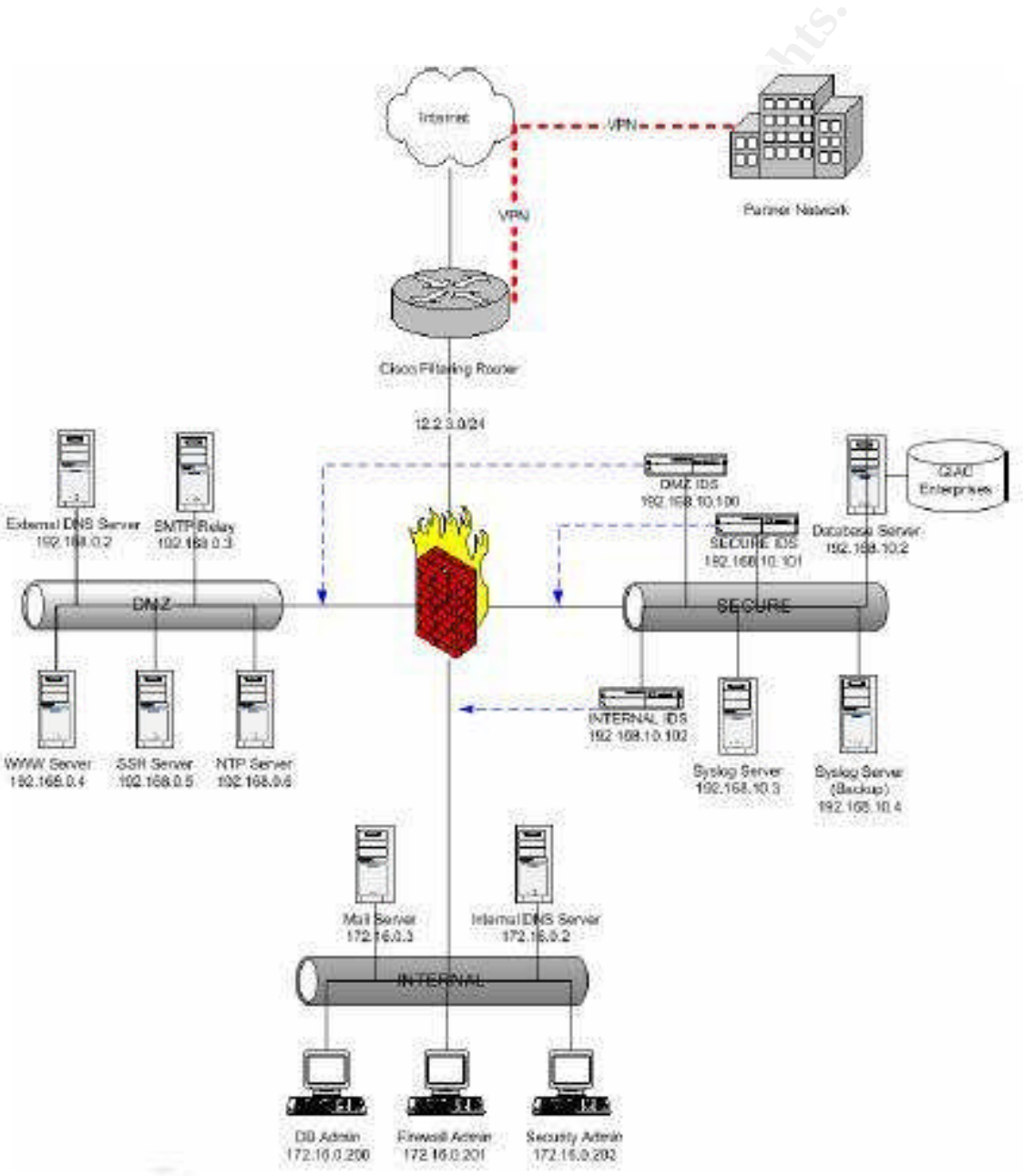


Fig 2.

1 COMPROMISE AN INTERNAL SYSTEM

The purpose of this design is to compromise an internal server from the internal network of GE.

Located in internet, I will began, first making a reconnaissance of external services provided by the victim. Depending of the results of this reconnaissance I will find design an attack to compromise a server.
I only know this parameter:

- URL of the web server: www.giac.com

With nslookup I can find, besides other information, the ip address of the web server. Use nslookup with the name of the web server.

```
C:\>nslookup www.giac.com
*** No se puede encontrar el nombre de servidor para la direcci¢n XX.XXX.X.XX: Non-existent domain
*** No se puede encontrar el nombre de servidor para la direcci¢n XX.XXX.X.XX: Non-existent domain
*** Los servidores predeterminados no están disponibles
Servidor:  UnKnown
Address:  X.XXX.X.XX

DNS request timed out.
    timeout was 2 seconds.
Respuesta no autoritativa:
Nombre:  www.giac.com
Address:  12.2.3.4
```

The information displayed will give us in the last line the ip address of the web server. However to verify this, I can use another method what can also give me more information; mails, telephones of administrative contacts, ip address information.

```
Domain ID:D20796732-LROR
Domain Name:GIAC.COM
Created On:26-Feb-2000 23:08:23 UTC
Last Updated On:18-Jan-2004 04:53:38 UTC
Expiration Date:26-Feb-2007 23:08:23 UTC
Sponsoring Registrar:R63-LROR
Status:CLIENT TRANSFER PROHIBITED
Registrant ID:37152111-NSI
Registrant Name:The GIAC
Registrant Organization:The GIAC
Registrant Street1:1163 E. Ogden Ave
Registrant Street2:Suite 705-174
Registrant City:Naperville
Registrant State/Province:IL
Registrant Postal Code:60563
Registrant Country:US
Registrant Phone:+1.7085576006
Registrant Email:hostmaster@giac.com
Admin ID:16815046-NSI
Admin Name:Lance Spitzner
Admin Street1:1163 E OGDEN AVE STE 705-174
Admin City:NAPERVILLE
Admin State/Province:IL
Admin Postal Code:60563-1687
Admin Country:US
```

```
Admin Email:hostmaster@GIACCOM
Tech ID:5358805-NSI
Tech Name:Network Solutions, LLC.
Tech Organization:Network Solutions, LLC.
Tech Street1:13200 Woodland Park Drive
Tech City:Herndon
Tech State/Province:VA
Tech Postal Code:20171-3025
Tech Country:US
Tech Phone:+1.18886429675
Tech Email:customerservice@giac.com
Name Server:NS53.WORLDNIC.COM
Name Server:NS54.WORLDNIC.COM
```

The results in the whois site: http://www.whois.net/ give me information of people in this organization. This information can help me to make social engineering calling by telephone to Lance Spitzner and trying to obtain valuable information: for example; operating system of the pcs in the internal network. Obviously Lance Spitzner, in the other side of the call, will not suspect that I am deceiving him.

More information about the web server can be found in the following web site: http://uptime.netcraft.com

Fig 3.

It displays information about its operating system. In this case, web server of McLaren is running apache over linux. (The assignment of McLaren don't mention about the operating system of its web server, so this will be assumed) The version of the operating system is displayed too.

Next, I will try to find out what services, besides the web service, is running in the web server. Maybe it can be found that mail, ftp and other services are running in the same machine, so it will be more possibilities to find more vulnerabilities.

```
# nmap 3.50 scan initiated Mon Jul 12 14:52:11 2004 as: nmap -sT -n -v -p 80 -P0 -oN nmap1.txt 12.2.3.4
Interesting ports on 12.2.3.4:
PORT   STATE SERVICE
80/tcp open  http
443/tcp open  ssl

# Nmap run completed at Mon Jul 12 14:52:11 2004 -- 1 IP address (1 host up) scanned in 0.125 seconds
```

The result in running the nmap command shows me that two services are running in that machine.

The next step is to find out vulnerabilities in the operating system or in the apache application. I will look for in http://packetstormsecurity.org or in http://www.securityfocus.com. Also, knowing the version of apache 1.3.29, the following web site will be useful too :
http://www.apacheweek.com/features/security-13

Since, this web server is running apache and linux, I will suspect that important servers in the internal network are running the same operating system. So, once the web server is compromised with an exploit extracted by one of the url describe before, I covers the attack; changing the services that are running in the web server for other ones modified and that can help me to compromise other systems. I will install a sniffer (tcpdump) in the server to steal more information that can be useful to compromise an internal server. The data server located in the secure zone of the firewall is my final target.

However, it is probably that this last step to compromise a system can be detected by the administrator of GIAC, because the dmz, secure and internal zones of the network of McLaren are monitored by an ids.

Another way to compromise an internal system without be monitored by an IDS, will be making social engineering. So, as I found telephones, mails of persons who works in Giac, I will find out others person working in the GIAC enterprise, and then what operating system is running in their machines. Knowing that McLaren is working in this company and his telephone, I will call him asking for a person whose name is very common for example Peter, John, and telling him that I want to communicate with him. If I am lucky, he will tells me his last name, due to that I can not remember him. Then I will asking him if he can give me telephone number of Peter. In the same way, I try with Peter to get other names of people working in the company.
I will calling Peter and telling that I trying to update his antivirus but I don't remember what version of the operating system have, so I will expect his help So, this way I can obtain what version of operating system are running in desktops.

From the same way, he can give me his mail address with another story invented: I will tell him that I am a sender and I will sending a mail with information of new promotions.

Then, I will search for a Trojan that will can run in that operating systems and send him with an attractive message as this one that I found some days ago:

From: lizie@com
To: pmarrison@giac.com
Subject: Notify from a Know Person ;-)

Body:

Hey Peter Marrison,
It's me -> (myphoto4.jpeg)
I very much love productive leisure, to prepare for new exotic dishes, at leisure to leave with friends on the nature, to float, I like to go for a drive on mountain skiing, to visit excursions, travel. Very easy going.
For more information see the attached file.
Best wishes, Lizie

Document.vbs

Obviously, the document.vbs will run a Trojan that will give me control over his machine and will continue to compromise other important systems in Giac network. As this design of GIAC don't mention about an antivirus for desktops and servers, this attack can success.

2 SUGESTIONS TO MITIGATE THE ATTACK

To mitigate the attack GIAC must:

- Consult vendor last updates and patches to secure the web server and important servers in the network.
- Install intrusion detection for host. This will be installed in important servers as the web server, data base servers, mail servers and send its alarms to another server in another zone of the network.
- Install antivirus servers in desktops and to be updated all days.
- Consider to have an smtp content filtering in the SMTP relay.
- A Http content filtering will be useful to prevent downloads of infected files.
- Prevent personal of GIAC of the social engineering methods to obtain information.
- According to sans recommendations[13], I can prevent GE's network resources from being used as clients or agents for denial of services. To avoid the GIAC network could be used to damage other networks, do the following:
  - ✓ Egress filtering to stop spoofed ip packets from leaving GE's network, that is, ensuring that routers and firewalls are configured to forward IP packets only if those packets have the correct source ip address for GE's network

- ✓ Stop GE's network from being used as a broadcast amplification site, that is, configuring all of systems (routers, workstations, servers, etc.) so that they do not receive or forward directed broadcast traffic

ASSIGNMENT 4: VERIFY THE FIREWALL POLICY

1 PLANNING THE VALIDATION

1.1 TECHNICAL APPROACH

The verification of the firewall policy consists in testing traffic permitted in the zones created in the firewall: outside, dmz, internal, mngmt, data. Tools that would help me to make this work will be nmap and tcpdump.

Laptops with the following tools are installed:

- tcpdump[14]: With tcpdump, I am going to see traffic traveling between my laptop and the server, who is my target system to analyze. It will be with nmap to see firewall behavior.

  The following command is used for this work:

  "tcpdump host <ip address>"

  This command captures all traffic traveling to and from <ip address>

- nmap[15]: For the proposal of verification of the firewall policy, nmap is use to determine what services are running in the different zones of the firewall. Besides that, nmap will perform test of firewall behavior.

  The following scanning modes are used for this work and can be more explained in insecure web site: the art of port scanning[16]:

  "Nmap –sV <ip_address_of_the_target>"

  -sF, -sX, -sN, -sA : Stealth Fin, Xmas, Null and Ack scan
  -sV: Verify scan probes open ports determining service & app names/version
  -sU: Scan of the UDP ports, the option -P0 is needed.
  -P0: Don't ping hosts before port scanning is required as the firewall blocks ICMP traffic
  -p 1-65535 : scan ports from 1 to 65535. It is omitted, scans from 1 to 1024
  -oN: Write output to a specific file.

These tools are distributed as it can be shown in the following picture Fig 4..
Laptop A with Nmap
Laptop B with tcpdump
Server C, the target
Laptop D with tcpdump

The ip distribution will be make according to the zones of the firewall or servers in the network that I am analyzing. Nmap is applied to the GE server. Tcpdump is applied in both sides of the firewall, listen the traffic between these two zones while the nmap is running.

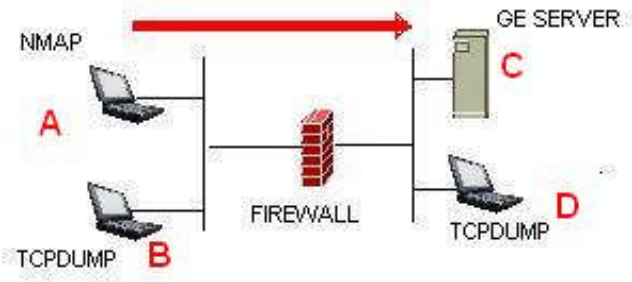


Fig 4.

Results of the test are documented in this format:

Interface of the firewall and server analyzed			
Component	Ip Address	Command	Result

Table 27. Report

1.2 CONSIDERATIONS

- The testing is performed from sunday 6:00am to monday 6:00am. If the case, the testing couldn't finished in this interval, it would continue the next sunday.
- The present testing will include only firewall verification, so the laptop will be located in the different zones that the firewall has created.
- Testing is only over the primary firewall.
- Testing will be performed by personal of GE's staff.

1.3 COST AND LEVEL OF EFFORT

Resource	Cost by Hour (US $)
Team leader	40
Analyst	30

Table 28. Resources

Task	Resource	Hours	Cost per Task (US $)
Planning of the project	Team leader	6	240
Management of the project	Team Leader	3	120
Implementation	Analyst	12	360
Analysis of the results	Team Leader	4	160
Reporting and documentation	Analyst	4	120
Total Cost (US $)		1000	

Table 29. Tasks

1.4 RISKS

- Public and private services will be not able for a period of time. For that reason GE consider to make the audit on a date with a low level of traffic, that is, since sunday at 6:00am to monday 6:00am.
- If the firewall doesn't block malicious traffic, critical servers could be affected and need to be rebuilt, so it's very important that exists a management consent with knowledge of the risks.

2 CONDUCTING THE VALIDATION

Following the scheme of the Fig 4, the distribution and results are:

Laptop A:

Ip address: 200.48.0.14
Command executed: "nmap -sV 200.48.0.4"
Result: Nmap shows that the web server has filtered ports 80 and 443

```
C:\nmap-3.50>nmap -sV 200.48.0.4

Starting nmap 3.50 ( http://www.insecure.org/nmap ) at 2004-07-13 18:51 SA Pacif
ic Standard Time
Interesting ports on 200.48.0.4:
(The 1657 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
80/tcp  closed http
443/tcp closed https

Nmap run completed -- 1 IP address (1 host up) scanned in 130.217 seconds
```

Fig 5.

Laptop B:

Ip Address: 200.48.0.13
Command execute: “tcpdump host 10.50.0.3”
Results: Tcpdump shows packets generated by laptop A are sent to the web server

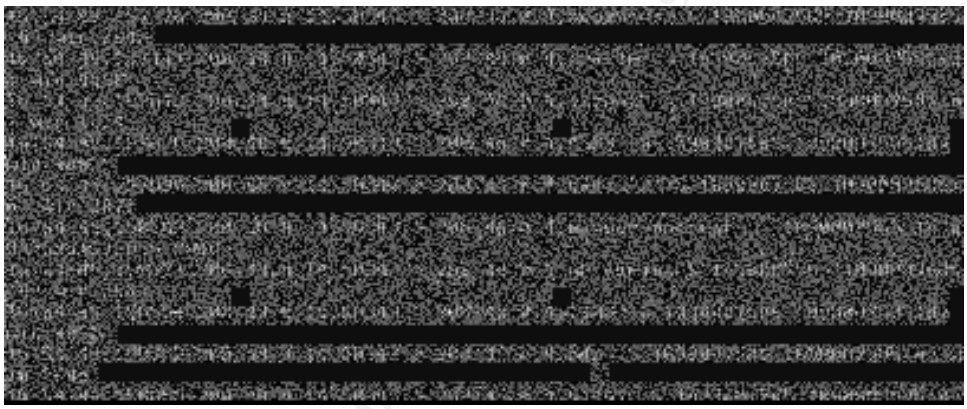


Fig 6.

Servidor C: Ip address: 10.50.0.3
Nombre del servidor: web server
Result: Server is operative and without any damage.

Laptop D: Ip address: 10.50.0.14
Command execute: “tcpdump host 10.50.0.3”
Results: Tcpdump shows packets generated by laptop A and arrived to the web server. The server respond with another packet to laptop A

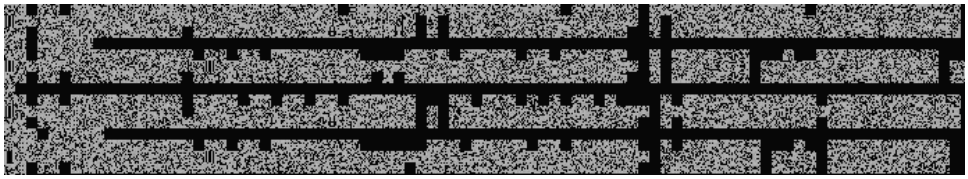


Fig 7.

Fig 5 shows me that some ports are unfiltered and the rest of them are filtered. That's meas the firewall is doing its work.
Fig 6 shows traffic sent from the laptop A to the target server C. Packets are created in the laptop A and send to the server C. The firewall compare these with its rules and drops the ones who service or ip address of the packet origin is not permitted.
Fig 7 confirms this. I can notice that only services that is permitted in the firewall arrives to the server C and the rest of them is denied in the firewall. It shows traffic that arrive to the server C and shows the traffic sent by server C to the laptop A.

The following tables shows a resume of the process of verification of rules in the firewall
I notice, that the results in scanning dns server and syslog server don't shows me that udp ports are unfiltered. It looks like they are in silence. Maybe UDP scan could not complete the scan because it reach the timeout allowed with no responses.

2.1 VERIFY SERVICES AVAILABLE FOR OUTSIDE ZONE

Outside Interface of the firewall – GE Web Server			
Component	Ip Address	Command	Result
Laptop A	200.48.0.14	Nmap -sV –p 1-65535 200.48.0.4	Traffic to the web server has unfiltered ports 80 and 443. The rest of ports are filtered
Laptop B	200.48.0.13	tcpdump host 200.48.0.14	Packets generated by laptop A in Outside zone are sent to the GE Web Server in the Dmz zone
GE Web Server	10.50.0.3 nat: 200.48.0.4	****	Server is operative and without any damage
Laptop D	10.50.0.14	tcpdump host 200.48.0.14	Packets http and https generated by laptop A in Outside zone arrive to the GE Web Server. The server responds to laptop A

Table 30. Outside Interface – GE Web Server

Outside Interface of the firewall – GE Mail Relay			
Component	Ip Address	Command	Result
Laptop A	200.48.0.14	Nmap -sV –p 1-65535 200.48.0.5	Traffic to the Mail Relay has unfiltered port 25. The rest of ports are filtered
Laptop B	200.48.0.13	tcpdump host 200.48.0.14	Packets generated by laptop A in Outside zone are sent to the GE Mail Relay in the Dmz zone
GE Mail Relay	10.50.0.4 nat : 200.48.0.5	****	Server is operative and without any damage
Laptop D	10.50.0.14	tcpdump host 200.48.0.14	Packets smtp generated by laptop A in Outside zone arrive to the GE Mail Relay. The server responds to laptop A

Table 31. Outside Interface – GE Mail Relay

Outside Interface of the firewall – GE External Dns Server			
Component	Ip Address	Command	Result
Laptop A (Dns Server of the Provider)	200.38.23.11 200.38.23.12	Nmap –sU –P0 200.48.0.6 Nmap –sV –P0 200.48.0.6	Traffic to the External Dns Server has filtered all ports with the first command. With the second command, External Dns server has unfiltered the 53/tcp port
Laptop B	200.48.0.13	tcpdump host 200.38.23.11 tcpdump host 200.38.23.12	Packets generated by laptop A in Outside zone are sent to the GE external Dns server in the Dmz zone.
GE Mail Relay	10.50.0.5 nat : 200.48.0.6	****	Server is operative and without any damage
Laptop D	10.50.0.14	tcpdump host 200.38.23.11 tcpdump host 200.38.23.11	With the first command, no Packets generated by laptop A in Outside zone arrived to the GE

			External Dns Server in the Dmz zone. With the second command, there are domain packets tcp.

Table 32. Outside Interface – GE External Dns Server

Outside Interface of the firewall – GE Syslog Server			
Component	Ip Address	Command	Result
Laptop A (Router)	200.48.0.1	Nmap –sU –P0 200.48.0.7	Traffic to the Syslog Server has filtered all ports.
Laptop B	200.48.0.13	tcpdump host 200.48.0.1	Packets generated by laptop A in Outside zone are sent to the GE Syslog server in the mngmt zone.
GE Syslog Server	10.70.0.3 nat : 200.48.0.7	****	Server is operative and without any damage
Laptop D	10.70.0.14	tcpdump host 200.48.0.1	No Packets generated by laptop A in Outside zone arrived to the GE Syslog Server in the Mngmt zone.

Table 33. Outside Interface – GE Syslog Server

2.2 VERIFY SERVICES AVAILABLE FOR DMZ ZONE

The following table shows a resume of the process of verification of rules in the firewall.

Dmz Interface of the firewall – GE Data Base Servers			
Component	Ip Address	Command	Result
Laptop A (GE Web Server)	10.50.0.3	Nmap -sV –p 1-65535 10.80.0.3 Nmap -sV –p 1-65535 10.80.0.4	Traffic from the GE Web Server to the GE Data Base servers has unfiltered port 1433. The rest of ports are filtered

Laptop B	10.50.0.13	tcpdump host 10.50.0.3	Packets generated by laptop A in dmz zone are sent to the GE Data Base servers in the Data zone
GE Data base And GE data base backup server	10.80.0.3 10.80.0.4	****	Server is operative and without any damage
Laptop D	10.80.0.14	tcpdump host 10.50.0.3	Packets sqlnet generated by laptop A in dmz zone arrive to the GE Data Base servers. The server responds to laptop A

Table 34. DMZ Interface – GE Data Base Servers

Dmz Interface of the firewall – GE Mail Server			
Component	Ip Address	Command	Result
Laptop A (GE Mail Relay)	10.50.0.4	Nmap -sV –p 1-65535 10.60.0.7	Traffic from the GE Mail Relay to the GE Mail Server has unfiltered port 25. The rest of ports are filtered
Laptop B	10.50.0.13	tcpdump host 10.50.0.4	Packets generated by laptop A in dmz zone are sent to the GE Mail Server in the inside zone
GE Mail Server	10.60.0.7 nat : 10.60.0.7	****	Server is operative and without any damage
Laptop D	10.60.0.14	tcpdump host 10.50.0.4	Packets smtp generated by laptop A in dmz zone arrive to the GE Mail Server. The server responds to laptop A

Table 35. DMZ Interface – GE Mails Server

Dmz Interface of the firewall – GE Antivirus Server			
Component	Ip Address	Command	Result
Laptop A	10.50.0.14	Nmap –sV –p 1-65535	Traffic to the antivirus

		10.70.0.5	server backup has unfiltered port 80. The rest of ports are filtered
Laptop B	10.50.0.13	tcpdump host 10.50.0.14	Packets generated by laptop A in dmz zone are sent to the GE antivirus server in the mngmt zone
GE Antivirus Server	10.70.0.5 nat: 10.70.0.5	****	Server is operative and without any damage
Laptop D	10.50.0.14	tcpdump host 10.50.0.14	Packets http generated by laptop A in dmz zone arrive to the GE antivirus server. The server responds to laptop A

Table 36. DMZ Interface – GE Antivirus Server

2.3 VERIFY SERVICES AVAILABLE FOR INSIDE ZONE

The following table shows a resume of the process of verification of rules in the firewall.

Inside Interface of the firewall –Sites in internet			
Component	Ip Address	Command	Result
Laptop A (GE Proxy Server)	10.60.0.5	Nmap -sV –p 1-65535 200.48.0.1	Traffic from the GE Proxy Server to the outside zone has unfiltered ports 80 and 443 for the GE Proxy Server. The rest of ports are filtered
Laptop B	10.60.0.14	tcpdump host 10.60.0.5	Packets generated by laptop A in inside zone are sent to a site in the outside zone.
Site in internet	200.48.0.1	****	Server is operative and without any damage
Laptop D	200.48.0.14	tcpdump host 10.60.0.5	Packets http and https generated by laptop A in inside zone arrive to the remote site in the outside zone. The server responds to laptop A

Table 37. Inside Interface – Sites in internet

Inside Interface of the firewall – GE Mail Relay			
Component	Ip Address	Command	Result
Laptop A (GE Mail Server)	10.60.0.7	Nmap -sV –p 1-65535 10.50.0.4	Traffic from the GE Mail Server to the GE Mail Relay has unfiltered port 25. The rest of ports are filtered
Laptop B	10.60.0.13	tcpdump host 10.60.0.7	Packets generated by laptop A in inside zone are sent to the GE Mail Relay in the Dmz zone
GE Mail Relay	10.50.0.4	****	Server is operative and without any damage
Laptop D	10.50.0.14	tcpdump host 10.60.0.7	Packets smtp generated by laptop A in inside zone arrive to the GE Mail Relay. The server responds to laptop A

Table 38. Inside Interface – GE Mail Relay

Inside Interface of the firewall – GE External Dns Server			
Component	Ip Address	Command	Result
Laptop A (GE Active Directory)	10.60.0.6	Nmap –sU –P0 10.50.0.5	Traffic from the GE Active Directory to the GE Syslog Server has filtered all ports.
Laptop B	10.60.0.13	tcpdump host 10.60.0.6	Packets generated by laptop A in Inside zone are sent to the GE External Dns server in the dmz zone.
GE External Dns Server	10.50.0.5	****	Server is operative and without any damage
Laptop D	10.50.0.14	tcpdump host 10.60.0.6	No Packets generated by laptop A in inside zone arrived to the GE external dns server in the Dmz

			zone.

Table 39. Inside Interface – GE External Dns Server

Inside Interface of the firewall – GE Data Base Servers			
Component	Ip Address	Command	Result
Laptop A (GE Internal Web Server)	10.60.0.9	Nmap –sV –p 1-65535 10.80.0.3 Nmap –sV –p 1-65535 10.80.0.4	Traffic from the GE Internal Web Server to the GE Data Base Servers has unfiltered port 1433. The rest of ports are filtered
Laptop B	10.60.0.13	tcpdump host 10.60.0.9	Packets generated by laptop A in inside zone are sent to the GE Data Base Servers in the data zone
GE Data Base and GE Data Base Backup	10.80.0.3 10.80.0.4	****	Server is operative and without any damage
Laptop D	10.80.0.14	tcpdump host 10.60.0.9	Packets sqlnet generated by laptop A in inside zone arrive to the GE Data Base Servers. The server responds to laptop A

Table 40. Inside Interface – GE Data Base Servers

Inside Interface of the firewall – GE Antivirus Server			
Component	Ip Address	Command	Result
Laptop A	10.60.0.14	Nmap –sV –p 1-65535 10.70.0.5	Traffic to the GE Antivirus Server has unfiltered port 80. The rest of ports are filtered
Laptop B	10.60.0.13	tcpdump host 10.60.0.14	Packets generated by laptop A in inside zone are sent to the GE Antivirus Server in the mngmt zone
GE Antivirus Server	10.70.0.5	****	Server is operative and without any damage

Laptop D	10.70.0.14	tcpdump host 10.60.0.14	Packets http generated by laptop A in inside zone arrive to the GE Antivirus Server. The server responds to laptop A

Table 41. Inside Interface – GE Antivirus Server

2.4 VERIFY SERVICES AVAILABLE FOR MNGMT ZONE

The following table shows a resume of the process of verification of rules in the firewall.

Mngmt Interface of the firewall – Provider Antivirus Servers			
Component	Ip Address	Command	Result
Laptop A (GE Antivirus Server)	10.70.0.5	Nmap –sV –p 1-65535 200.23.21.22 Nmap –sV –p 1-65535 200.23.21.33	Traffic from the GE Antivirus Server to the Provider Antivirus Servers has unfiltered port 80. The rest of ports are filtered
Laptop B	10.70.0.13	tcpdump host 10.70.0.5	Packets generated by laptop A in mngmt zone are sent to the Provider Antivirus Servers in the outside zone
Provider Antivirus Server	200.23.21.22 200.23.21.33	****	Server is operative and without any damage
Laptop D	200.48.0.14	tcpdump host 10.70.0.5	Packets http generated by laptop A in mngmt zone arrive to the Provider Antivirus Server. This responds to laptop A

Table 42. Mngmt Interface – Providers Antivirus Servers

Mngmt Interface of the firewall – Desktops and Servers in the GE network			
Component	Ip Address	Command	Result
Laptop A (GE Antivirus Server)	10.70.0.5	Nmap –sV –p 1-65535 10.50.0.14 Nmap –sV –p 1-65535 10.60.0.14	Traffic from the GE Antivirus Server to desktops and server in the dmz, internal and data

		Nmap –sV –p 1-65535 10.80.0.14	zones has unfiltered port 80. The rest of ports are filtered
Laptop B	10.70.0.13	tcpdump host 10.70.0.5	Packets generated by laptop A in mngmt zone are sent to the desktops and server in the dmz, internal and data zone
Dmz_Server Int_Desktop Data_Server	10.50.0.14 10.60.0.14 10.80.0.14		Desktops and Servers are operative and without any damage
Laptop D	10.50.0.14 10.60.0.14 10.80.0.14	tcpdump host 10.70.0.5	Packets http generated by laptop A in mngmt zone arrive to the desktop or server. This responds to laptop A

Table 43. Mngmt Interface – Desktops and Servers in the GE Network

Mngmt Interface of the firewall – Router			
Component	Ip Address	Command	Result
Laptop A (GE Router and Firewall Manager)	10.70.0.5	Nmap –sV –p 1-65535 200.48.0.1	Traffic from the GE Router and Firewall Manager to the router has unfiltered port 22. The rest of ports are filtered
Laptop B	10.70.0.13	tcpdump host 10.70.0.5	Packets generated by laptop A in mngmt zone are sent to the router
Router	200.48.0.1		Router is operative and without any damage
Laptop D	200.48.0.14	tcpdump host 10.70.0.5	Packets ssh generated by laptop A in mngmt zone arrive to the router. This responds to laptop A

Table 44. Mngmt Interface – Router

2.5 VERIFY SERVICES AVAILABLE FOR DATA ZONE

Data Interface of the firewall – Antivirus Server			
Component	Ip Address	Command	Result
Laptop A (GE Data Base Servers)	10.80.0.3 10.80.0.4	Nmap –sV –p 1-65535 10.70.0.5	Traffic from the GE Data Base Servers to the GE Antivirus Server has unfiltered port 80. The rest of ports are filtered
Laptop B	10.80.0.13	tcpdump host 10.80.0.3 tcpdump host 10.80.0.4	Packets generated by laptop A in data zone are sent to the GE Antivirus Server
GE Antivirus Server	10.70.0.5		GE Antivirus Server is operative and without any damage
Laptop D	10.70.0.14	tcpdump host 10.80.0.3 tcpdump host 10.80.0.4	Packets http generated by laptop A in data zone arrive to the router. This responds to laptop A

Table 45. Data Interface – GE Antivirus Server

2.6 TCP ATTACKS

The purpose of this section of the test is to verify the behavior of the firewall to the malformed packets that the laptop A sends to the GE Server C. Appendix B, shows the diagrams of this test.

FIN SCAN			
Component	Ip Address	Command	Result
Laptop A	200.48.0.14	Nmap –v –sF –n –P0 –p80 200.48.0.4	Port 80 is in state open.
Laptop B	200.48.0.13	tcpdump host 200.48.0.14	There are packets sent to the target but not packets returned from the target.
GE Web Server	10.70.0.3 nat: 200.48.0.4		GE Web Server is operative and without any damage
Laptop D	10.70.0.14	tcpdump host 200.48.0.14	There isn't any packet that arrived from the

			laptop A

Table 46. Tcp Attacks – Fin Scan

NULL SCAN			
Component	Ip Address	Command	Result
Laptop A	200.48.0.14	Nmap –v –sN –n –P0 –p80 200.48.0.4	Port 80 is in state open.
Laptop B	200.48.0.13	tcpdump host 200.48.0.14	There are packets sent to the target but not packets returned from the target.
GE Web Server	10.70.0.3 nat: 200.48.0.4		GE Web Server is operative and without any damage
Laptop D	10.70.0.14	tcpdump host 200.48.0.14	There isn't any packet that arrived from the laptop A

Table 47 Tcp Attacks – Null Scan

ACK SCAN			
Component	Ip Address	Command	Result
Laptop A	200.48.0.14	Nmap –v –sA –n –P0 –p80 200.48.0.4	Port 80 is in state open.
Laptop B	200.48.0.13	tcpdump host 200.48.0.14	There are packets sent to the target but not packets returned from the target.
GE Web Server	10.70.0.3 nat: 200.48.0.4		GE Web Server is operative and without any damage
Laptop D	10.70.0.14	tcpdump host 200.48.0.14	There isn't any packet that arrived from the laptop A

Table 48 Tcp Attacks – Ack Scan

XMAS TREE SCAN

Component	Ip Address	Command	Result
Laptop A	200.48.0.14	Nmap –v –sX –n –P0 –p80 200.48.0.4	Port 80 is in state open.
Laptop B	200.48.0.13	tcpdump host 200.48.0.14	There are packets sent to the target but not packets returned from the target.
GE Web Server	10.70.0.3 nat: 200.48.0.4		GE Web Server is operative and without any damage
Laptop D	10.70.0.14	tcpdump host 200.48.0.14	There isn't any packet that arrived from the laptop A

Table 49 Tcp Attacks – Xmas Tree Scan

The results in these tables indicate that the firewall dropped these packets sent by the laptop A. For that reason, laptop D monitoring don't show me any traffic from or to laptop A.

3 EVALUATING THE RESULTS

3.1 ANALYSIS OF THE RESULTS

It appears that the GE firewall performs as it is defined. Only the configured unfiltered ports in outside, inside, dmz, mngmt and data interface in the firewall are accessible for services. With this verification, GE can be secure that services are accessed by the ones that must to access.
The second test, tcp attacks, verify that the firewall detects no valid connection and drops it, so in this way, it will avoid that an attacker can bypass the firewall and gather information of the target.

3.2 RECOMMENDATIONS FOR IMPROVEMENTS OR ALTERNATE ARCHITECTURE

- GE can increase network security with an IDS. This will be useful to identify and isolate intrusions against computer systems. This will have one interface monitoring on the outside of the firewall.
- For future expansion of GE, maybe to other nations in south america, GE should have to buy a separate VPN device because of a future increase in the traffic demand to the firewall.
- GE should consider to buy a second firewall from a different technology that the first one, and located inside the GE's network as a second level of defense.

- GE data base servers and other critical servers can behind this second firewall, so it will be protected by internal users and give hackers in internet extra difficulty to access.

APPENDIX A. TUTORIAL FIREWALL

1 BASIC CONFIGURATION AND ACCESS RULES

This tutorial is based in "configuring the pix firewall " document found in cisco web site[17] and "Controlling network access"[18]

1. Start your terminal emulation program.

2. Power on the PIX Firewall. On newer models, the switch is at the back, on older models, at the front.

3. If you are configuring a PIX 506, PIX 515, PIX 525, or PIX 535 and your site downloads configuration images from a central source with TFTP, look for the following prompt in the startup messages:
   Use BREAK or ESC to interrupt flash boot.

   PIX Firewall displays this prompt for 10 seconds. To download an image, press the **Escape** key to start boot mode. If you are not downloading an image, ignore the prompt or press the Space bar to start immediately and PIX Firewall starts normally.

4. After the startup messages appear, you are prompted with the following unprivileged mode prompt:

   pixfirewall>

5. Enter enable and press the **Enter** key.
   The following prompt appears:
   Password:
   Press the **Enter** key.

6. You are now in privileged mode. The following prompt appears:
   pixfirewall#

   Enter configure terminal and press **Enter**. You are now in configuration mode.

7. Assign names and set security level for the firewall interfaces

   nameif ethernet0 outside security0
   nameif ethernet1 dmz security50

```
nameif ethernet2 inside security60
nameif ethernet3 data security80
nameif ethernet4 mngmt security100
```

8. Set each ethernet interface the speed and type of operation

```
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
interface ethernet3 auto
interface ethernet4 auto
```

9. Set an encrypted password for the configuration

```
enable password ZXASASASS encrypted
passwd ZXASASASS encrypted
```

10. Assign hostname of the firewall

```
hostname SCS04200
domain-name cisco.com
```

11. Enable application inspection for the protocols

```
fixup protocol http 80
fixup protocol SMTP 25
no fixup protocol h323 h225 1720
no fixup protocol h323 ras 1718-1719
no fixup protocol ils 389
no fixup protocol rsh 514
no fixup protocol rtsp 554
no fixup protocol sip 5060
no fixup protocol skinny 2000
```

12. define the IP address for each interface

```
ip address outside 200.48.0.2 255.255.255.240
ip address dmz 10.50.0.1 255.255.255.0
ip address inside 10.60.0.1 255.255.255.0
ip address data 10.80.0.1 255.255.255.0
ip address mngmt 10.70.0.1 255.255.255.0
```

13. Enable the “flood defender”

```
floodguard enable
```

14. Enable sending informational messages to a syslog server. Designate a host to receive the messages with the logging host command
    Set the logging level with the logging trap command
    Set the logging facility command to a value other than its default of 20
    Start sending messages with the logging on command

    logging on
    logging timestamp
    logging buffered debugging
    logging trap debugging
    logging facility 5
    no logging console
    logging host mngmt 10.70.0.3

15. Disable firewall to send SNMP traps
    no snmp server
    no snmp-server location
    no snmp-server contact
    no snmp-server enable traps

16. Set the default route to be 200.48.0.1
    route outside 0.0.0.0 0.0.0.0 200.48.0.1 1

17. Use SSH version
    ca generate rsa key 1024
    ca save all
    ssh 10.70.0.4 255.255.255.255
    ssh timeout 60

18. Enable service access with static
    Static Network Address Translation (NAT) creates a permanent, one-to-one mapping between an address on an internal network (a higher security level interface) and a perimeter or external network (lower security level interface)

    The main options of the static command are as follows:

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

- Replace *internal_if_name* with the internal network interface name. In general, this is the higher security level interface you are accessing.

- Replace *external_if_name* with the external network interface name. In general, this is the lower security level interface you are accessing.

- Replace *global_ip* with the outside (global) IP address. In general, this is the interface with the lower security level. This address cannot be a PAT IP address.

- Replace *local_ip* with the internal (local) IP address from the inside network. In general, this is the interface with the higher security level.

- Replace *network_mask* with the network mask that pertains to both *global_ip* and *local_ip*. For host addresses, always use 255.255.255.255. For network addresses, use the appropriate subnet mask for the network.

- (Optional) replace max_conns with the maximum number of concurrent connections permitted through the static address translation.

For example, the following command maps a server with an internal IP address of 10.1.1.3 to the registered IP address 209.165.201.12:

static (inside, outside) 209.165.201.12 10.1.1.3 netmask 255.255.255.255

19. Enable access connections between networks in different zones of the firewall. By default, the PIX Firewall denies access to an internal or perimeter (more secure) network from an external (less secure) network. You specifically allow inbound connections by using access lists. Access lists work on a first-match basis, so for inbound access, you must deny first and then permit after

    The basic syntax for the access-list command is as follows:

    access-list *ID* [line *line-num*] {deny|permit} *protocol* *<source_address* | interface *if_name>*
    [operator *port] destination_address* [operator *port]*

- Replace *ID* with a name or number you create to identify a group of access-list command statements; for example, "acl_inbound," which identifies that the permissions apply to access from the outside interface.
- To insert a remark or an access control entry (ACE), use the line keyword. Replace line-num with the line number at which to make the insertion.
- Use permit or deny depending on whether you want to permit or deny access to the server. By default, all inbound access is denied, so you must permit access to a specific protocol or port.
- Replace *protocol* with the protocol (tcp or udp). For most servers, such as HTTP or email, use tcp.
- Replace *source_address* with the host or network address for those systems on the lower security level interface that must access the *destination_address*. Use any to let any host access the *destination_address*. If you specify a single host, precede the address with host; for example host 192.168.1.2. If you specify a network address, also specify a network mask; for example, 192.168.1.0 255.255.255.0.
- Use the interface keyword if the interface has a dynamically assigned IP address. Replace if_name with the name of the interface configured using the nameif command.
- Use an operator to match port numbers used by the source or destination. This section uses only eq (equal to)
- Use the first *port* parameter after an operator to identify the protocol port used by the source host that initiates the connection.
- Replace *destination_address* with the host or network global address that you specified with the static command statement. For a host address, precede the address with host; for networks, specify the network address and the appropriate network mask.
- Use the second *port* parameter after an operator to specify the protocol port used by the destination host. For example, to identify a web server, use eq http or eq 80. For an email server, use eq smtp or eq 25.

20. The format for the access-group command is as follows:

    access-group *ID* in interface *low_interface*

- Replace ID with the same identifier that you specified in the access-list command statement.
- Replace low_interface with the lower security interface that you specified in the static command statement. This is the interface through which users will access the external (global) address.

  The following example illustrates the three commands required to enable access to a web server with the external IP address 209.165.201.12:

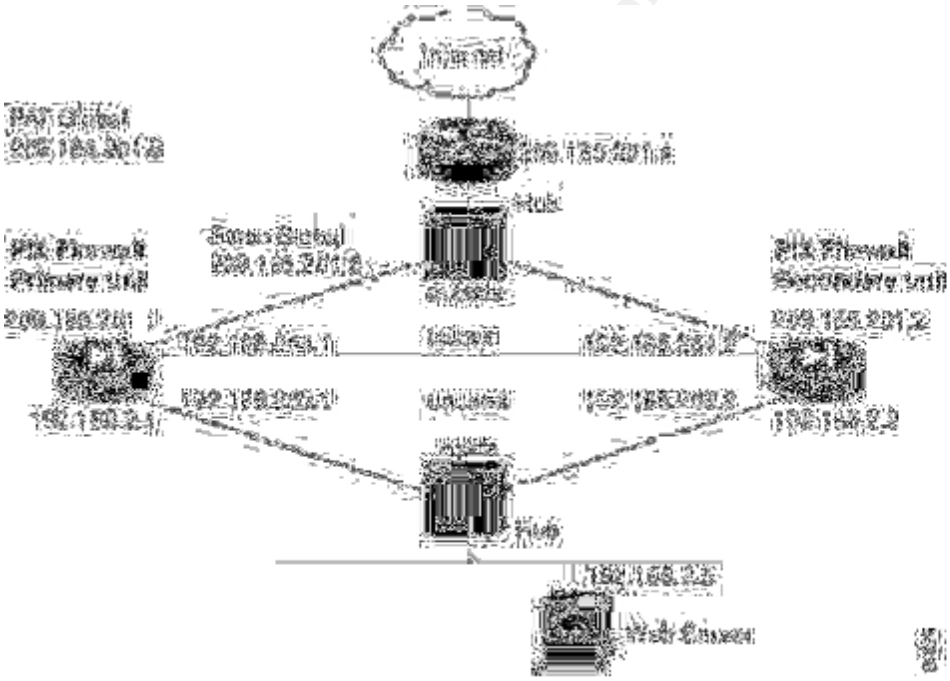
```
static (inside, outside) 209.165.201.12 10.1.1.3 netmask
255.255.255.255 0 0
access-list acl_out permit tcp any host 209.165.201.12 eq www
access-group acl_out in interface outside
```

21. Saving Your Configuration
    When you complete entering commands in the configuration, save it to Flash memory with the **write memory** command.

2 FAILOVER CONFIGURATION

Failover Configuration Examples.

Figure 10-2 lists the network diagram for a failover configuration using a Failover cable.



Follow these steps to configure the PIX Firewall units for use with failover:

1. Set up the PIX Firewall without failover information.
2. Add the failover ip address command for all interfaces including the one for the dedicated failover interface but not for unused interfaces.

3. If there are any interfaces that have not been configured in the non-failover setup, configure them at this time with an IP address and a failover IP address. Also leave the unused interfaces unconnected.
4. If you want to configure Stateful Failover, add the failover link command and specify the interface the Stateful Failover will be using. For Stateful Failover, you should have a dedicated 100BaseTX Stateful Failover interface in addition to all other interfaces.
5. Use the write memory command on the primary unit to save the new configuration.
6. Plug the Failover cable into the primary unit and then power on the secondary unit.

Note If the secondary unit has been previously configured, before you connect it to the Failover cable to the primary unit, boot it up, and enter the write erase command to remove any configuration. This will ensure a smooth synchronization.

7. Enter the write standby command from the active unit to synchronize the current configuration to the Flash memory on the standby unit.

In the example configuration illustrated in Figure 10-2, the Ethernet2 interface (labeled "failover") is used as the dedicated interface for Stateful Failover. The Ethernet3 interface is a previously unconfigured interface and is currently not connected to any active network. There is a cross-over Ethernet cable connecting the unused interface so that the failover check up messages can be sent and received.

Note PIX Firewall requires that unused interfaces be connected to the standby unit and that each unused interface be assigned an IP address. Even if an interface is administratively shut down, the PIX Firewall will try to send the failover check up messages to *all* internal interfaces.

3 VPN CONFIGURATION

This tutotial, extract from cisco web site[19], permits to create a tunnel between remote users and the firewall. There are two phases, describe in this document, the first is the negotitation of the security parameters using Pre-Shared Keys, and the second phase; the exchange of security parameters between the two sides to transmit the data. Configuration of the vpn clients will be make in the desktops and laptops of the remote users. Information about how to configure the cisco vpn client version 4.0 sofware can be found in cisco web site[20]

Using IKE with Pre-Shared Keys

If you use the IKE authentication method of pre-shared keys, manually configure these keys on the PIX Firewall and its peer(s). You can specify the same key to share with multiple peers, but it is more secure to specify different keys to share between different pairs of peers.

To configure a pre-shared key on the PIX Firewall, perform the following steps.

1. Configure the PIX Firewall host name:

   hostname newname

   For example:

   hostname mypixfirewall

   In this example, “mypixfirewall” is the name of a unique host in the domain.
   When two peers use IKE to establish IPSec security associations, each peer sends its identity to its peer. Each peer’s identity is set either to its host name or its IP address. By default, the identity of the PIX Firewall is set to its IP address. If necessary, you can change the identity to be a host name instead.
   As a general rule, set all peers’ identities the same way—either all peers should use their IP addresses or all peers should use their host names. If some peers use their host names and some peers use their IP addresses to identify themselves to one another, IKE negotiations could fail if a peer’s identity is not recognized and a DNS lookup is unable to resolve the identity.

2. Configure the PIX Firewall domain name:

   domain-name name

   For example:

domain-name example.com

3. Specify the pre-shared key at the PIX Firewall:

   isakmp key keystring *address* peer-address [*netmask* mask]

   This is the key that the PIX Firewall and its peer will use for authentication and the peer’s address.

   For example:

isakmp key 1234567890 *address* 192.168.1.100

The pre-shared key is 1234567890, and the peer's address is 192.168.1.100.
Note: Netmask allows you to configure a single key to be shared among multiple peers. You would use the netmask of 0.0.0.0. However, we strongly recommend using a unique key for each peer.

4. Specify the pre-shared key at the remote IPSec peer.

Note: The pre-shared key should be configured at both the PIX Firewall and its peer, otherwise the policy cannot be used. Configure a pre-shared key associated with a given security gateway to be distinct from a wildcard, pre-shared key (pre-shared key plus a netmask of 0.0.0.0) used to identify and authenticate the remote VPN clients.

Basic IPSec Configuration

The following steps cover basic IPSec configuration where the IPSec security associations are established with IKE and static crypto maps are used.
In general, to configure the PIX Firewall for using IPSec, perform the following steps:

22. Create an access list to define the traffic to protect:

access-list access-list-name *{deny* | *permit} ip* source source-netmask destination destination-netmask

For example:

access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0

In this example, the **permit** keyword causes all traffic that matches the specified conditions to be protected by crypto.

23. Configure a transform set that defines how the traffic will be protected. You can configure multiple transform sets, and then specify one or more of these transform sets in a crypto map entry (Step 4d).

crypto ipsec transform-set transform-set-name transform1 [transform2, transform3]

For example:

crypto ipsec transform-set myset1 esp-des esp-sha-hmac
crypto ipsec transform-set myset2 ah-sha-hmac esp-3des esp-sha-hmac

In this example, “myset1” and “myset2” are the names of the transform sets. “myset1” has two transforms defined, while “myset2” has three transforms defined.

24. Create a crypto map entry by performing the following steps:

a. Create a crypto map entry in IPSec ISAKMP mode:

crypto map map-name seq-num *ipsec-isakmp*

For example:

crypto map mymap 10 ipsec-isakmp

In this example, “mymap” is the name of the crypto map set. The map set’s sequence number is 10, which is used to rank multiple entries within one crypto map set. The lower the sequence number, the higher the priority.

b. Assign an access list to a crypto map entry:

crypto map map-name seq-num *match address* access-list-name

For example:

crypto map mymap 10 match address 101

In this example, access-list 101 is assigned to crypto map “mymap.”

c. Specify the peer to which the IPSec protected traffic can be forwarded:

crypto map map-name seq-num *set peer* ip-address

For example:

crypto map mymap 10 set peer 192.168.1.100

The security association will be set up with the peer having an IP address of 192.168.1.100. Specify multiple peers by repeating this command.

d. Specify which transform sets are allowed for this crypto map entry. List multiple transform sets in order of priority (highest priority first). You can specify up to six transform sets.

crypto map map-name seq-num *set transform-set* transform-set-name1 [transform-set-name2, … transform-set-name6]

For example:

crypto map mymap 10 set transform-set myset1 myset2

In this example, when traffic matches access list 101, the security association can use either "myset1" (first priority) or "myset2" (second priority) depending on which transform set matches the peer's transform set.

25. Apply a crypto map set to an interface on which the IPSec traffic will be evaluated:

crypto map map-name *interface* interface-name

For example:

crypto map mymap interface outside

In this example, the PIX Firewall will evaluate the traffic going through the outside interface against the crypto map "mymap" to determine whether it needs to be protected.

26. Specify that IPSec traffic be implicitly trusted (permitted):

sysopt connection permit-ipsec

Note: This command also permits L2TP/IPSec traffic.

Using Dynamic Crypto Maps

Dynamic crypto maps, used with IKE, can ease IPSec configuration and are recommended for use in networks where the peers are not always predetermined. You use dynamic crypto maps for VPN clients (such as mobile users) and routers that obtain dynamically assigned IP addresses.

1. Assign an access list to a dynamic crypto map entry:

crypto dynamic-map dynamic-map-name dynamic-seq-num *match address* access-list-name

This determines which traffic should be protected and not protected.

For example:
crypto dynamic-map dyn1 10 match address 101

In this example, access list 101 is assigned to dynamic crypto map "dyn1." The map's sequence number is 10.

2. Specify which transform sets are allowed for this dynamic crypto map entry. List multiple transform sets in order of priority (highest priority first).

   crypto dynamic-map dynamic-map-name dynamic-seq-num *set transform-set* transform-set-name1, [transform-set-name2, … transform-set-name9]

   For example:

   crypto dynamic-map dyn 10 set transform-set myset1 myset2

   In this example, when traffic matches access list 101, the security association can use either "myset1" (first priority) or "myset2" (second priority) depending on which transform set matches the peer's transform sets.

3. Specify security association lifetime for the crypto dynamic map entry, if you want the security associations for this entry to be negotiated using different IPSec security association lifetimes other than the global lifetimes:

   crypto dynamic-map dynamic-map-name dynamic-seq-num *set security-association lifetime {seconds* seconds | *kilobytes* kilobytes}

   For example:

   crypto dynamic-map dyn1 10 set security-association lifetime 2700

   This example shortens the timed lifetime for dynamic crypto map "dyn1 10" to 2700 seconds (45 minutes). The time volume lifetime is not changed.

4. Specify that IPSec should ask for PFS when requesting new security associations for this dynamic crypto map entry, or should demand PFS in requests received from the peer:

crypto dynamic-map dynamic-map-name dynamic-seq-num *set pfs [group1 | group2]*

For example:

crypto dynamic-map dyn1 10 set pfs group1

5. Add the dynamic crypto map set into a static crypto map set.
Be sure to set the crypto map entries referencing dynamic maps to be the lowest priority entries (highest sequence numbers) in a crypto map set.

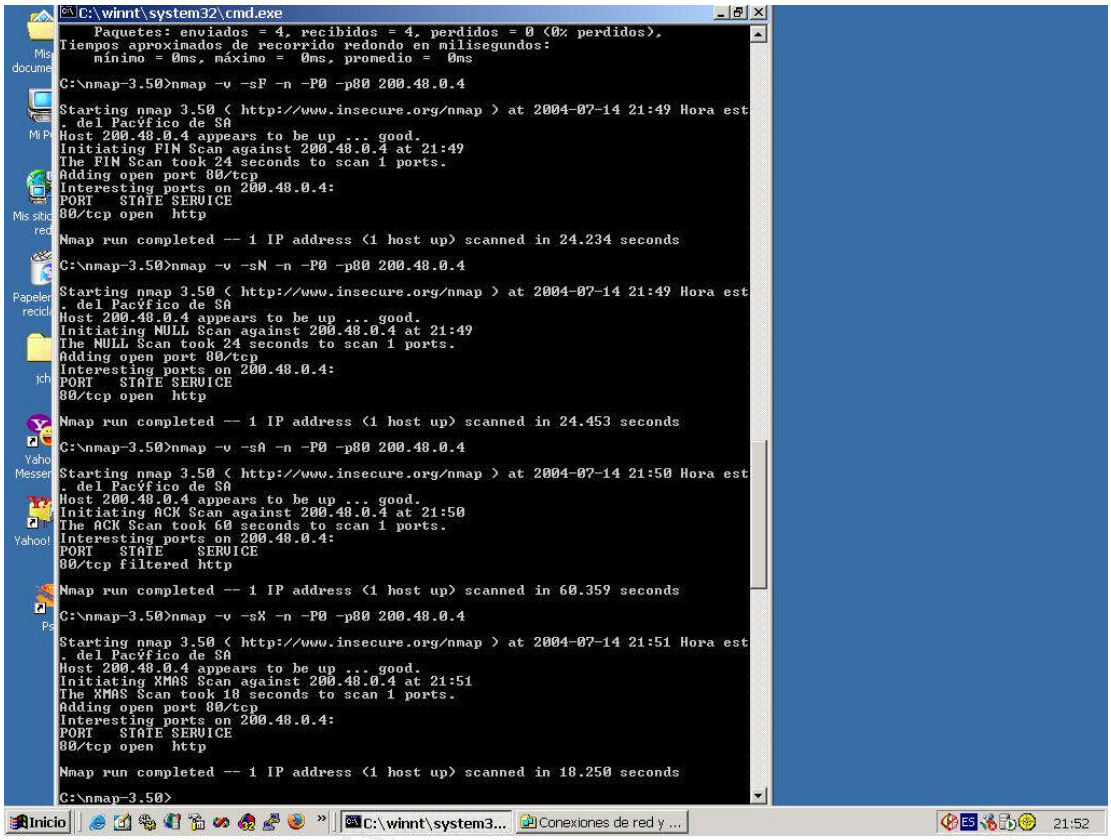
crypto map map-name seq-***num ipsec-isakmp dynamic*** dynamic-map-name

For example:

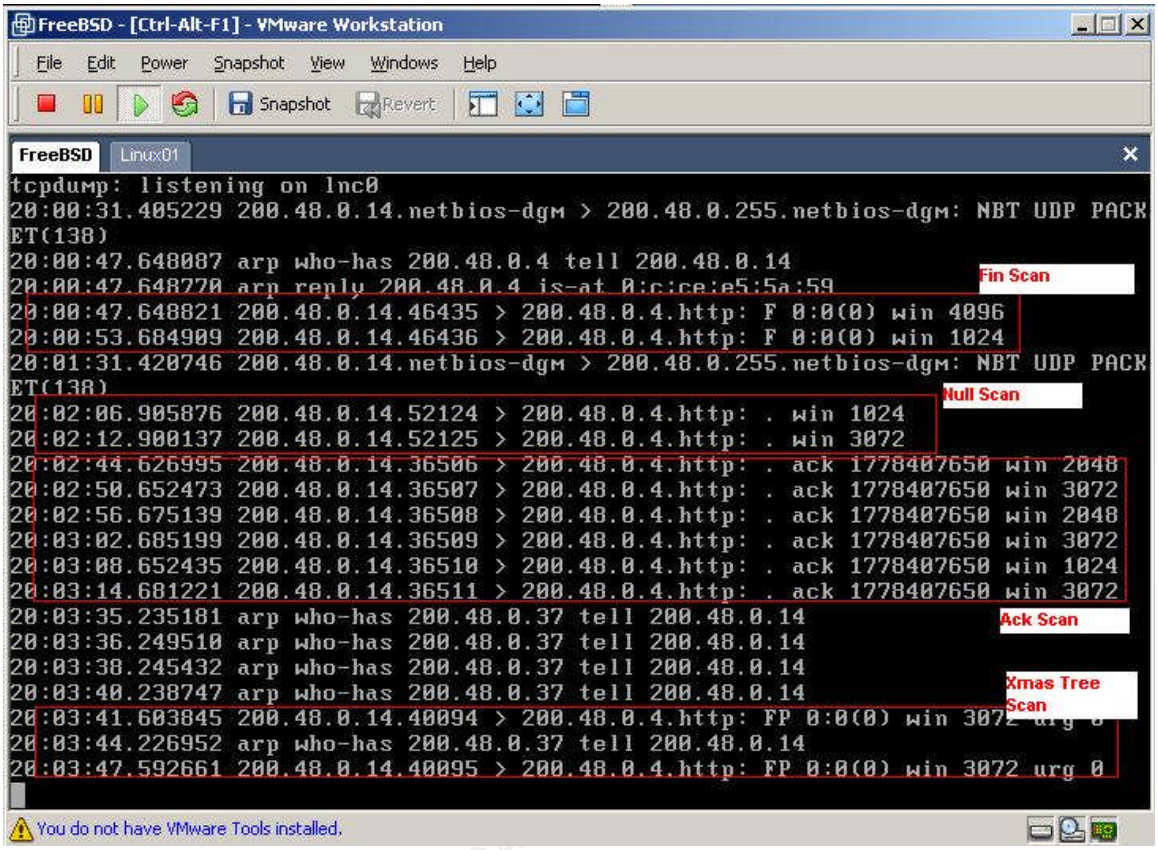
crypto map mymap 200 ipsec-isakmp dynamic dyn1

APPENDIX B. RESULTS OF TCP ATTACKS

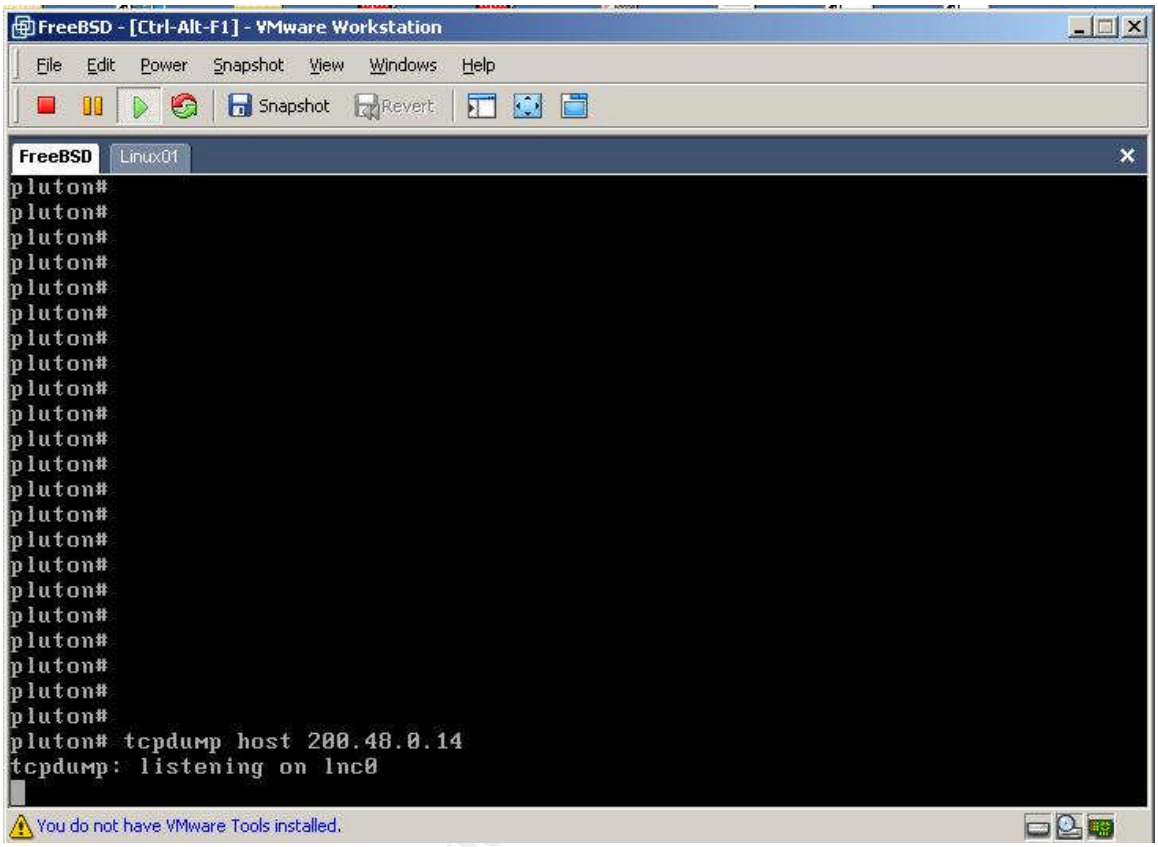
Laptop A. Commands use to test the firewall, in the following order: Fin Scan, Null Scan, Ack Scan, Xmas Tree Scan.



Laptop B. Results.



Laptop D. Results.



DEFINITIONS

Term	Meaning
GE	Giac Enterprise
NAT	Network address translation
ESCM	Etrust Secure Content Manager
VPN	Virtual Private Network
IDS	Intrusion detection system
DNS	Domain name service

BIBLIOGRAPHY

1. Sans Institute Books “Track 2 – Firewalls, Perimeter Protection & Virtual Private Networks”
2. “Building Internet Firewalls” Author: D. Brent Chapman and Elizabeth D. Zwicky

REFERENCES

[1] Cisco Web Site "Cisco 2600 Series Modular Access Routers" URL: http://www.cisco.com/en/US/products/hw/routers/ps259/products_data_sheet09186a00801761b1.html

[2] Cisco Web Site "Cisco PIX 515E Security Appliance" URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b15.html

[3] Etrust Secure Content Manager "Distinctive Features and Funcionalities" URL: http://www3.ca.com/Files/DataSheets/etrust_scm_datasheet.pdf

[4] Etrust Secure Content Manager "Brochure eTrust Secure Content Manager" URL: http://www3.ca.com/Files/Brochures/etrust_scm_brochure.pdf

[5] National Security Agency "Security Recommendation Guides" URL:http://nsa2.www.conxion.com/

[6] Cisco Web Site "Cisco PIX Firewall Command Reference, Version 6.3" URL: http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_book09186a008017284e.html

[7] Cisco Web Site "fixup protocol dns" URL: http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a00801727a8.html#wp1067379

[8] Cisco Web Site "Cisco Pix Firewall - Floodguard" URL: http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a00801727a8.html#wp1029632

[9] Cisco Web Site "Configuring Secure Shell" URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7d5.html

[10] Cisco web site "static" URL: http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a00801cd841.html#wp1026694

[11] Cisco web site "Using Pix Firewall Failover" URL: http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a008017278a.html

[12] Sans Institute "Christopher Reining Practical Assignment" URL: http://www.giac.org/practical/GCFW/Bien_Jared_McLaren_GCFW.pdf

[13] Sans Institute "Help Defeat Denial of Service Attacks: Step-by-Step" URL: http://www.sans.org/dosstep/

[14] Slac Home Page "Monitoring with tcpdump" URL: http://www-iepm.slac.stanford.edu/monitoring/passive/tcpdump.html

[15] Insecure Web Site "Nmap Security" URL: http://www.insecure.org/

[16] Insecure Web Site "The Art of Port Scanning" URL: http://www.insecure.org/nmap/nmap_doc.html

[17] Cisco Web Site "Basic Firewall Configuration" URL:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a00800eb0b0.html

[18] Cisco Web Site "Controlling Network Access" URL:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a008017278e.html

[19] Cisco Web Site "Basic VPN Configuration" URL:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a00800eb0b2.html

[20] Cisco Web Site "Cisco VPN Client – Configuring and managing connection entries" URL:
http://www.cisco.com/en/US/products/sw/secursw/ps2308/products_user_guide_chapter09186a008015e271.html#1000328