

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 Certification
GCFW Practical Assignment

Firewalls, Perimeter Protection, and VPNs
Version 1.7

William Chan

October 2002

Table of Contents

Introduction and Scope 3

Assignment 1 Security Architecture 4

1.1 Business Operation 4
1.2 Data Classification 4
1.3 Business Applications and Network Services 5
1.4 Access Requirements 8
1.5 Design Guidelines and Considerations 11
1.6 Existing Perimeter Network Design 12
1.7 Proposed Secure Perimeter Network Design 14
1.8 IP Addressing 21
1.9 Cost Summary and Justification 23

Assignment 2 Security Policy and Tutorial 24

2.1 Border Router Security Policy 24
2.2 External Firewall Security Policy 29
2.3 VPN Security Policy 41
2.4 Tutorial on Border Router Implementation 49

Assignment 3 Verify the Firewall Policy 59

3.1 Plan the Audit 59
3.2 Conduct the Audit 64
3.3 Evaluate the Audit 73

Assignment 4 Design Under Fire 75

4.1 Information Gathering 76
4.2 Known Vulnerabilities 78
4.3 Attacks 84
4.3.1 An Attack Against the Firewall Itself 84
4.3.2 A Denial of Service Attack 86
4.3.3 An Attack Plan to Compromise an Internal System 87

Endnotes 89

Introduction

GIAC Enterprise is a small but well-established company in the fortune cookie business. In order to expand its customer base, GIAC has been experimenting with e-commerce over the Internet for a couple of years and business has been growing steadily. However, GIAC has also learned, through a series of incidents including virus infection and denial of service attacks, that security must be a fundamental component of any e-business strategy. As a result, GIAC has formalized a security project to review its business and security requirements and to propose a proper security infrastructure with enough details for budget approval by senior management. The goal of this project is to deliver a cost effective and robust security infrastructure design with room for growth. Existing network and firewall equipment will be re-used wherever appropriate in order to lower the capital cost of the project.

Scope

Primary focus of this project is on perimeter security[1], i.e. to protect privacy, to mitigate risk and to provide logs for auditing purpose. High availability and high fault tolerance requirements have been carefully considered but, due to budget constraint, remain as options for future enhancement. In the worst case scenario, downtime due to hardware outage is estimated at about 4 hours including software and configuration restoration as the local hardware vendor can guarantee a one-hour turn around time for hardware replacement.

Other issues such as physical security, application security, host security, encryption key management, anti-virus strategies, disaster recovery etc. are outside the scope of this project.

Assignment 1 Security Architecture

1.1 Business Operation

GIAC Enterprise (GIAC) is a small but well-established company and has been a leader in the business of fortune cookie for over twenty years. One of the keys to its success is the early adoption of new technology to facilitate business growth, as demonstrated by their attempts to growth their business over the Internet. As revenue and profit increase, the number of customer, supplier, partner and employee also grows but so is the complexity and risk of doing business online. Their current defense strategy of using Network Address Translation (NAT) to hide their internal network from the Internet is starting to fall apart as hacker are growing in numbers and skills. In order to better protect itself against fraud and business loss, GIAC has decided that it is now the time to review and implement correct security architecture to meet their present and foreseeable future business needs.

Technology-wise, GIAC has standardized, like many other corporations, on Microsoft Windows 2000 platform and applications including Microsoft Office, Exchange and IIS Web Server and Cisco network equipment. There is also some expertise in Linux operating system and database application development. On the governance side, GIAC has a well-defined information security policy providing high-level guidelines on how confidential information should be protected.

1.2 Data Classification

As per GIAC's Enterprise Information Security Policy, internal data are classified into the following three classes:

> **Confidential Restricted** – the most sensitive, confidential information resources intended for the exclusive use of a strictly limited number of authorized employees who have the right and need to know. This class includes, but not limited, to the following:
>
> - Strategic information of GIAC;
> - Information that has a significant impact on GIAC's well-being or is highly newsworthy;
> - Unannounced GIAC financial performance and Operational Information
>
> **Confidential -** information resources that, if disclosed to or modified by an unauthorized individual, could adversely impact GIAC performance, customers trust or employee confidence. Examples in this class include:
>
> - Customers' financial information and records;
> - Customers' transaction and payment methods;

- Confidential product information such as fortune cookie sayings

Internal Use Only – the information resources that are used and modified during normal course of business, the disclosure or unauthorized change of which has little adverse impact on GIAC. Examples include:

- Non-sensitive operational data;
- Internal policies, standards and procedures;
- General internal memoranda and emails

1.3 Business Applications and Network Services

All servers on GIAC networks are hardened using best practice guidelines including those recommended by SANS[2] and CERT[3].

Web Server
GIAC's web application is designed with a tiered structure using an iPlanet web server as the presentation interface to users, a BEA Weblogic server as the application layer, and an Oracle server at the backend to keep all confidential data in databases. Purpose of the application server is to support applications that share data and resources with other systems, and generate information for web pages and other user interfaces. The web server and application server do not store any confidential customer or financial information in their hard drives. The BEA Weblogic server uses JDBC (Java Database Connectivity), an API for connecting programs written in Java, and communicates with the Oracle server using SQL*Net v2 over TCP port 1521[4]. (Note that port 1521 is the default port used by Oracle for SQL*Net, however, this value does not agree with IANA port assignments[5]). SQL*Net is Oracle's client/server middleware product that offers transparent connection from one database to another, or from client tools to the database.

Mail
GIAC's Mail system also has a split-architecture with an external mail server serving external clients and an internal mail server serving internal users. The external mail server will relay mail messages to and from the internal mail server for external communications. Internal users will not be able to bypass the internal mail server to send and receive mail to the outside world, so the internal mail server provides a choke point for virus scanning and content filtering as required.

FTP/SSH Server
An FTP server is available on the External Service for those customers, suppliers and partners who have an ftp account setup to transfer files in batch mode. A login ID and password are required, no anonymous login is allowed.

For more confidential information, secure file transfer can be done by SSH to the same server. Secure Shell (SSH), also known as Secure Socket Shell, is a

UNIX-based command interface and protocol used for secure access to a remote computer. GIAC's has implemented OpenSSH[6] 3.4 server as the corporate standard for Secure Socket Shell. OpenSSH is a free version of the SSH protocol suite of network connectivity tools that encrypts all traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks. The OpenSSH suite includes the ssh program which replaces rlogin and telnet, scp (secure copy) which replaces rcp, and sftp (secure ftp) which replaces ftp. Although OpenSSH supports SSH protocol versions 1.3, 1.5, and 2.0, only version 2.0 is used for the GIAC network because it is more robust, free of any restrictive license and its richness in features.

For GIAC security network implementation, vulnerabilities against SSH and OpenSSH have been checked and patched including the recently discovered Trojan exposure[7]. Port 22 is required for SSH.

Note: Cisco products including PIX firewall and VPN 3000 Series Concentrators only support the SSH remote shell functionality as provided in SSH version 1. SSH v2 is not supported at this time.

DNS

DNS service is provided using a split DNS architecture. External DNS service is provided by a major national service provider because they have demonstrated that best current practices have been followed, including their compliance with RFC 2827[8] on ingress filter and RFC 3013[9] on security services and procedures. The ISP's DNS server has an IP address of 196.196.196.250.

An internal DNS server resolves DNS queries from the internal networks, and forwards unresolved queries for external domain names to the ISP DNS server for resolution. Zone transfer is not allowed on the ISP's DNS server to the public, but it is allowed if the request is from customers' internal DNS servers. DNS uses UDP port 53 for queries/replies and TCP 53 for zone transfer[10].

Network Monitoring and Message Logging

An existing SNMP based network management server is used to monitor the performance and up/down status of all servers and network devices except the UDP port 161 is required for SNMP queries and UDP port 162 is used for SNMPTRAP for the monitored devices to send traps to the management server. The network management server is also serving as a syslog server for all servers to provide a single focal point for monitoring and event correlation. Syslog protocol uses UDP port 514.

Authentication Server
An existing Radius server is used by the VPN gateway to perform authentication for remote users. Note that Cisco PIX firewall listens for Radius on ports 1645 and 1646, not 1812 and 1813 as assigned by IANA. Cisco PIX firewall also permits the use of TCP literal names for a number of services, including domain, ftp, ftp-data, http, smtp, sqlnet, tacacs and telnet[11].

Tape Backup Server
Veritas Netbackup BusinessServer[12] is used for server back and recovery purpose. For the server on the External Service Network to be backed up to the Tape Backup server on the Internal Service Network through the PIX firewall, the following TCP ports are required[13]:

Source	Ports	Data Flow	Destination	Ports
Client	900-999, 4900-4999	---->	Master	800-899, 4800-4899, 13720-13721
Master	900-999, 4900-4999	---->	Client	13782-13783

Network Time Protocol (NTP) Service
Time synchronization on all servers and network devices by NTP[14] is critical in correlating event log entries from different devices. The Directory server is also serving as an internal master timeserver for all hosts on GIAC internal networks. The internal timeserver itself is synchronized to two public NTP secondary (stratum 2) timeservers over the Internet. UDP port 123 is required for NTP. The border router and all servers on the external service network synchronize directly to the Internet stratum 2 servers.

TFTP
Trivial File Transfer Protocol[15] (TFTP), an Internet software utility for transferring files that is simpler to use than the File Transfer Protocol (FTP) but less capable and secure, is used for IOS upgrade for Cisco devices. It is used where user authentication and directory visibility are not required. TFTP uses the User Datagram Protocol (UDP) rather than the Transmission Control Protocol (TCP). In the proposed architecture, the design team has decided not to allow TFTP traffic to go through the external firewall. When IOS software on the Border Router needs an upgrade, a temporary subnet will be setup with a local TFTP server for file transfer.

Network Address Translation (NAT)[16] and Network Addressing
With the explosion of the Internet and the increase in business and home networks, the number of available IP addresses provided by IPv4 address scheme is simply not enough. While IPv6 is being developed and deployed, it will take several years to implement because it requires modification of the entire

infrastructure of the Internet. In the mean time, use of NAT allows a single device, such as a router or firewall at the border of a corporate network, to act as an agent between the Internet (or public network) and a local (or private) network. NAT gateway handles the traffic by translating the source network address to that of its Internet connected interface. When the remote host replies, the NAT device forwards the traffic to the computer on the internal network that established the session. Since computers on the Internet cannot access the internal computers directly, they cannot initiate a session with them, and thus cannot attack them easily. RFC1918[17] provides guideline and information on using private network addresses.

GIAC has been assigned a class C network address of 192.73.235.0/24 that has a range of 254 routable and assignable host addresses for external communications over the Internet. GIAC is also using a private Class B network address of 172.20.0.0/16 for its private internal networks. Out of the 172.20.0.0/16 network, range of subnets 172.20.2.0/24 to 172.20.3.0.0/24 will be used for internal resources and user networks, while subnets 172.20.129.0/24 and 172.20.13.0/24 will be used for VPN NAT address pools for Partners and GIAC mobile users respectively.

The outside interface of the VPN concentrator as well as all servers on the external service network, including the web server, Weblogic application server, SSH server and the Mail Relay server, are assigned with public network addresses for public access. All internal servers and printers are assigned with static addresses from the private class B network address. DHCP is used to assign dynamic IP addresses to all workstations from the private address.

The serial interface of the border router is assigned by its ISP an ip address of 196.196.196.242/30 while the IPS router at the next hop is at 196.196.196.241 /30.

Note: Both class C network addresses 192.73.235.0 and 196.196.196.0 have not been assigned to any party as of September 2002 as per ARIN's record.

1.4 Access Requirements

- Customers - Customers are companies or individuals that purchase or plan to purchase bulk online fortunes. As such, customers will need to:

    - Access to GIAC's web servers for viewing online catalog which is available to anyone from any country,
    - Login or create account and change profile including password,
    - Submit their orders with account and payment information when they are ready to purchase,

- Download the purchased fortune cookie sayings when their payment method is approved
- Send e-mail to GIAC for support, product information and complaints.

Access to all except general marketing and product information will need proper authentication. New customers will be able to open accounts by submitting their credentials on line using secure http (or SSL for Secure Socket Layer) for approval. As the account and payment information contains confidential data, they need to be protected by encryption during storage and transit. Customers do not need direct access to any other internal applications. In summary, customers will need web access by HTTP (TCP 80), secure web access by HTTPS (TCP 443), E-Mail access by SMTP (TCP 25).

- Suppliers – Suppliers are authors of fortune cookie sayings that that GIAC can purchase by placing order by Email. They already have their on-line accounts established with GIAC. To complete orders from GIAC, suppliers will use SSL for secure file transfer to deliver their new sayings to GIAC and submit their invoices online for billing purpose. All access will need authentication, and contents of transfer are protected by encryption in transit and in storage. Suppliers do not need access to any other internal applications. Access protocols required for suppliers are pretty well the same as those for customers, namely HTTP (TCP 80), HTTPS (TCP 443), and SMTP (TCP25).

- Partners - Partners are international companies that translate and resell fortunes. With proper legal agreement in place with these trusted partners, GIAC allows individual staff from these Partners networks to use SSH for secure file transfer via VPN tunnels over the Internet, and to have limited read-write access to the Fortune Cookie Sayings Partner Database, which also provides on-line SQL query and language translation services. The Partner Database is a separate database from the Master Database even though they are physically residing on the same server. Access control is further enforced at OS layer by tcp wrapper[18] and at application layer by Oracle[19] database application software.

  The VPN tunnel is established between the VPN client software at the remote end and the VPN gateway at GIAC's end. Two-factor authentication (something you know and something you have) is also required before access is granted. Each approved remote user uses a RSA SecurID Token Card[20] provided by GIAC, and the ID and password entered are authenticated against a Radius server. GIAC's database server is further hardened to restrict and authenticate access at operating system and application level. In summary, access protocols required for Partner connections are HTTP (TCP 80), HTTPS

(TCP 443), SMTP (TCP25), FTP (TCP 20), SSH (TCP 22) and SQL*Net 2 (TCP 1521).

- There are about 150 GIAC Enterprises employees located on GIAC Enterprise's internal network, including about 8 support and database development staff. All staff will have (i) Read-only access to all databases for various business functions, (ii) E-mail access via internal mail server to communication with internal users, customers, suppliers and partners, (iii) web and ftp access to GIAC public web and ftp servers, and (iv) web and ftp access to the Internet to perform their tasks including competitive analyses, credit check, and product research and development. Database developers and support staff will need all of the above access plus administrative access to all databases for product development and support purpose. For support staff, secure Telnet and FTP capabilities are also required to all servers on the External Service Network. All other services including telnet and NNTP are not allowed as they are deemed as not required for business purposes. Internet access is restricted to business related activities, even though this is largely enforced by company policy. In summary, access protocol requirements for GIAC internal employees are outbound HTTP (TCP 80), HTTPS (TCP 443), FTP (TCP 21), SSH (TCP 22) and SQL*Net 2 (TCP 1521). SMTP (TCP 25) is only required for the internal E-Mail server to communicate through the firewall to the E-Mail Relay server on the External Service network.

- GIAC Enterprises mobile sales force and teleworkers – will need VPN connections similar to that available to staff on Partners' networks. Once connected, they need the same access to internal resources as for users on internal networks. No split tunneling is allowed because it is difficult to enforce the same security standards on remote computers. Split tunneling allows for secure access to corporate resources through an encrypted tunnel while allowing Internet access directly through the ISP's resources (eliminating the corporate network from the path for web access) but this practice imposes an exposure of the corporate network to the Internet via the remote computers. All laptops or home computers need to be protected by personal firewall and anti-virus software. For those computers that will store confidential information on their local drives, use of encryption via Microsoft EFS is enforced.

1.5 Design Guidelines and Considerations

1. The design should deliver a secure solution to support all current business requirements with flexibility to scale up in the future.
2. Budget is tight this year. If the capital cost of the project, excluding cost of training and service contract, exceeds 5% of the total IT budget, there will be no chance of getting approval. Knowing that the IT budget this year has been reduced this year by 20% to $500,000. The target cost of the project is set at $25,000.
3. The defense must follow the Defense in Depth[21] principle, with which multiple layers of protection are established combining capabilities of people, operations and security technologies.
4. Web server protected by a firewall will be used to provide insecure (port 80) and secure (port 443) access from Internet. Via an application server, the web server will be sending and retrieving product and financial information to/from database server on the internal network. No confidential information is stored in the local drive of the web server or application server.
5. Confidential information in transit over the Internet will be encrypted using SSL and VPN technology. Maximum strength of encryption will be used as permitted by local regulations.
6. Access to any confidential or confidential restricted information requires authentication with the use of a centralized authentication server. All failed attempts and other abnormal behavior will be logged and alarms will be sent to a centralized log server.
7. Use single purpose components where possible.
8. Use Cisco equipment where appropriate to leverage existing expertise and training on Cisco products.
9. Re-use existing equipment where possible due to budget constraint.
10. Redundancy and fault tolerance are nice to have, but can be added later on when budget is available.
11. Services to external clients are provided via servers in a service network[22]. Trusted and authorized users including partners and mobile employees can access internal network resources via VPN.
12. Where feasible, use SSL as the standard security control for web applications instead of using other different special software.
13. All routers, firewalls, VPN gateways, IDS, and servers are hardened with unnecessary services removed by default. Connectivity to any switch ports is locked down by MAC addresses. Security patches must be kept up-to-date.
14. Dial-up modem directly accessing any host on the service network or the internal networks is not allowed.
15. Except for VPN connections, external connections will not be permitted to directly access any of the facilities inbound to the internal network. The servers in the DMZ will control access from there initially.
16. Routing on all firewalls and VPN gateway must only be static.

17. A warning must be issued on any computer against unauthorized access and must precede or be included in the logon challenge issued by the system at login.
18. The console of any computer must be locked after 5 minutes of inactivity.
19. Network devices must have system logging turned on. System logs may not be stored on the network device that creates them.
20. System logs as well as alerts should be sent to central Logging servers located on firewalled Management LANs.

1.6 Existing Perimeter Network Design

Most of the network components and servers are already in place on the existing network, including hubs, switches, routers and all application servers. As shown in Figure 1 below, the existing network consists of a border router and an internal router where NAT is performed to hide the internal private network. Access control lists are also used to control access by source and destination addresses. There is also a Shiva Remote Access Server to provide dial up access to internal network for mobile users and partners.

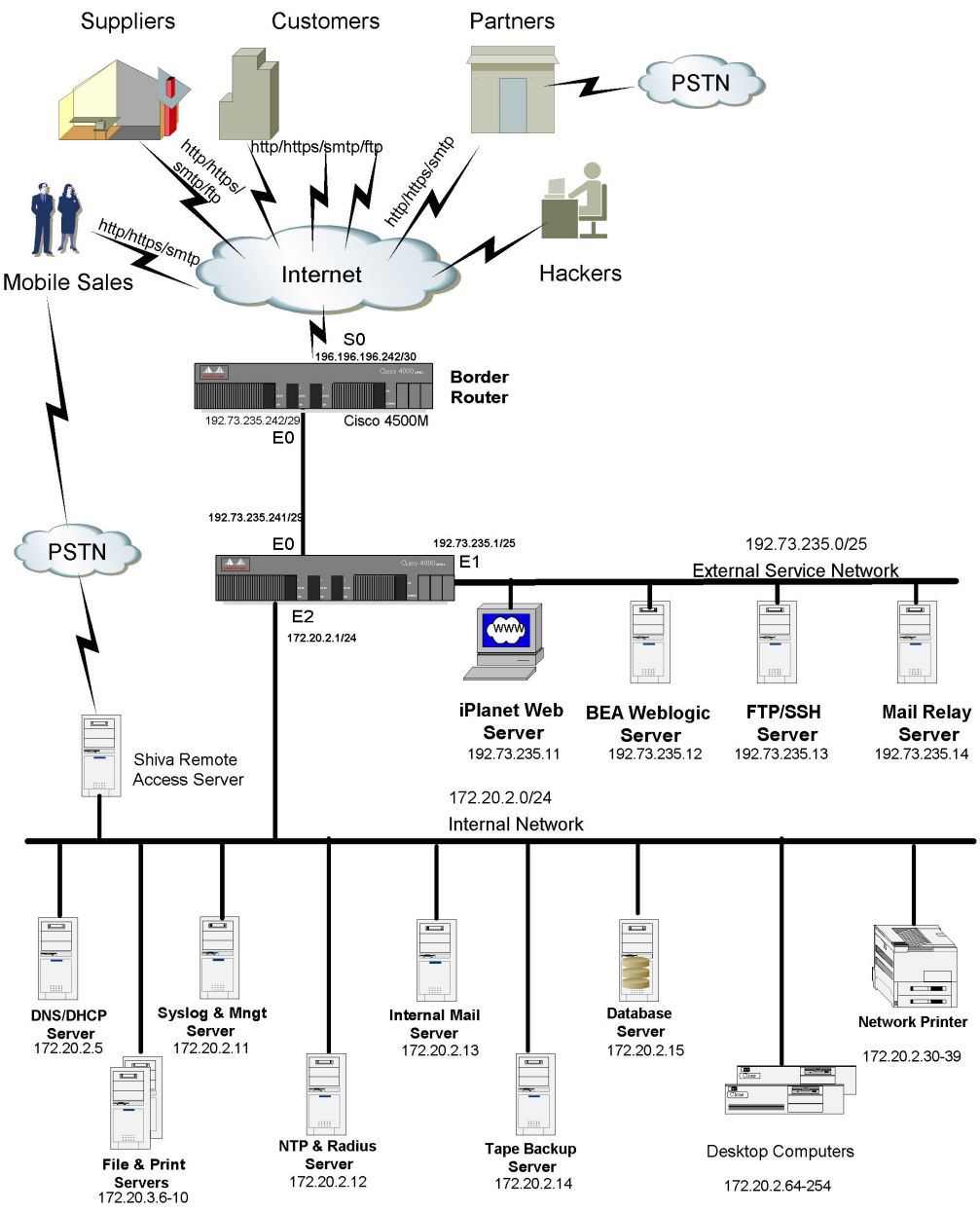


Figure 1 GIAC's Existing Networks

1.7 Proposed Secure Perimeter Network Design

Components required for the proposed perimeter infrastructure include:

- A border router (must have)
- An external firewall (must have)
- A VPN gateway (must have, can be standalone or integrated with firewall)
- Intrusion Detection Systems (following the Defense-in-Depth approach)
- An internal firewall (following the Defense-in-Depth approach)

After thorough discussion with users, security staff and senior management, the design team has decided to implement only the first four components on the above list, while postpone the implementation of an internal firewall to a later time when budget is available. However, the team also decides that an existing router can be used in the design where the internal firewall is going to be. Even though the primary function of this internal router in the design is to route packets (as opposed to control access), it will make the migration to firewall much easier with all the internal servers and resources in the right place with the right IP network addresses.

Below is the proposed secure perimeter network design (Figure 2) showing the location of each security component. It also shows how networks in three zones (the Red zone for un-trusted networks, the Blue zone for the DMZ network and the Green zone for the trusted internal networks) are connected together. Purpose, security function, placement and make/model of each security component are discussed as well.

Border Router

The primary function of the border router is to move packets between the GIAC networks and the Internet to meet business requirements. As the border router is the first line of defense against any attack from the Internet, the first fundamental security requirement on a border router is to lock down the router itself so it will not be easily compromised. Once the router is hardened, ingress and egress traffic flow can be controlled with the use of access control lists to deny spoofed IP packets from any unused and private IP ranges, to filter out source routed packets and IP unreacheable and time exceeded ICMP messages. Use of static packet filtering will also improve the overall performance by reducing the amount of traffic that firewall(s) has to handle. Stateful inspection and filtering functions are not required on the border router because they will be performed by the firewall.

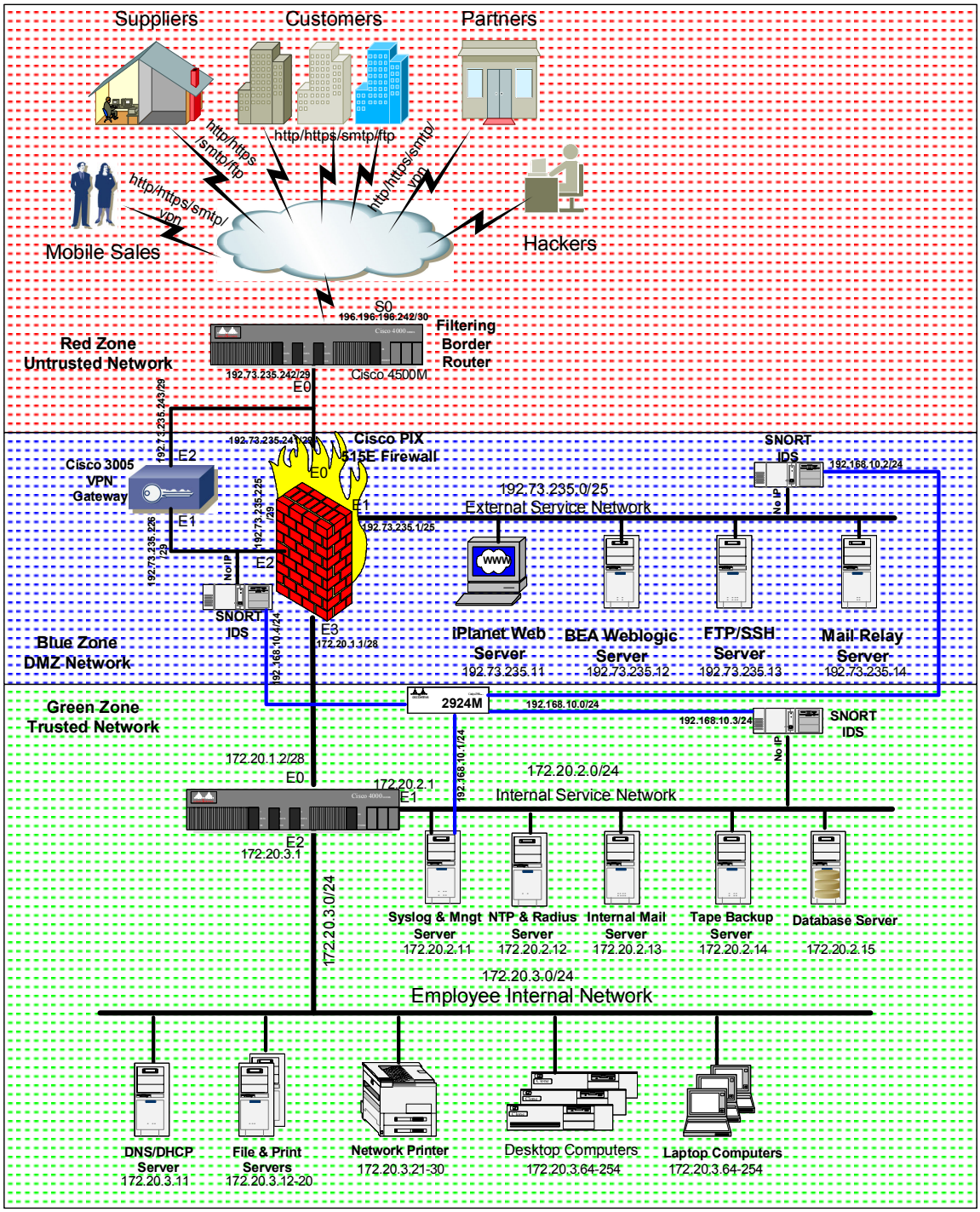


Figure 2 Proposed Secure Perimeter Network Design Diagram

As mentioned earlier, GIAC has standardized on Cisco platform for their networking devices including routers and switches. In the existing network configuration, a Cisco 4500M, with four Ethernet ports for LAN connections and an HSSI serial interface for high-speed WAN connections, is used as the border router. Even though Cisco had announced the end of sale of the 4500 series router in June 2001, they will continue to provide TAC support until end of 2005. Considering the fact that it can still run the latest (12.1.17) GD version of IOS, and the additional purchase cost of a new 3640 router as a replacement, the design team has decided to re-use it as the border router for now. There should not be any issue with hardware replacement as there are a couple more units of the same available for parts. As security and performance requirements on the Secure Perimeter Infrastructure will be reviewed annually, re-use of the existing Cisco 4500M as border router at this time makes perfect sense. Currently, a 5Mbps fractional T3 connection to the Internet is in place and peak utilization seldom exceeds 25% of the maximum bandwidth.

External Firewall

The concept of the firewall is much like the Great Wall of China, which was built to keep intruders out and to protect the residents within. Gates were used to provide limited access points and to control the entry and exit of those allowed. In today's environment, protecting data and network resources is critical to successful e-business, and firewalls are mandatory network security devices.

After spending sometime researching firewall features and functions, GIAC security team has come to the conclusion that there is no perfect firewall because a firewall by itself is not a complete defense system. The best firewall balances functionality, risk reduction, cost, manageability and vendor support as a tool that implements a security policy along with other devices applying the concept of "Defense in Depth".

There are many publications on firewall ranging from very general to very technology or product specific. Some articles worth reading include SANS' "Choosing The Best Firewall"[23], and "Internet Firewall: Frequently Asked Questions"[24]. There are also papers and articles comparing different firewall products, including a GCFW Practical Assignment by Clear Seders[25] where a brief comparison is done between Cisco PIX and CheckPoint FW-1 firewalls, the two major products in corporate environment.

GIAC's design team has decided, based on the above considerations and on Cisco's track record for technical support, to have Cisco PIX as their external firewall of choice. The PIX firewall, a purpose-built appliance that offers a high level of protection, is tightly integrated with a proprietary, hardened operating system combining stateful firewall and IP security (IPSec) VPN capabilities. Checkpoint Firewall-1 remains an option, when budget is available, for the

implementation of an internal firewall because this will provide additional challenge to hackers to break through two firewalls of different platforms before they can get access to the critical resources on the internal network. With a budget of about $25,000, it is just not enough to have two firewalls in the design.

It is further decided that the Cisco PIX 515E firewall at a purchase cost of $10,000 is the right equipment at the right price point for this project. PIX 515E is intended for small to medium business and enterprise environment s, provides up to 188 Mbps of firewall throughput with the ability to handle as many as 125,000 simultaneous sessions. Included in the purchase price is an additional 4-port 10/100 Ethernet interface, unrestricted software license (required for four or more interfaces) for the firewall, software release 6.2, a 64MB memory upgrade for better performance and for the stateful high availabilities capabilities which GIAC may need in the future. Also included in the price is the 56-bit DES VPN feature license. Because of the additional cost for the 168-bit 3DES VPN feature license and because of the design team's preference to use purpose-built component, it is decided that a separate VPN gateway will be purchase for the infrastructure.

More than just controlling access by stateful packet filtering, PIX firewalls can also provide other network services such as Network Address Translation (NAT), Port Address Translation (PAT), TACACS+ and Radius support, content filtering, attack detection and prevention, and many other features[26].

As shown in the proposed design diagram, the four interfaces on the PIX firewall allow physical separation of devices grouped by their risks and functions. The four networks connecting to the four interfaces of the firewall are:

- External network – a network with only 2 devices: the border router and the firewall itself. Even though this network is somewhat protected by the access control lists on the border router, it is still considered as an un-trusted external network.
- External Service Network – sometimes also called DMZ. All public accessible servers are located on this networks, including web server and the Weblogic application server for all web-based applications, SSH server to provide secure file transfer function, and mail relay server which allows for virus and content scanning to deny all undesirable traffic. Content of SSH server is scanned, moved and cleaned up everyday. No confidential data is ever permanently stored in any server on this network. Access from External Service Network to the internal network is tightly restricted to only those services required.
- VPN Network – a network established between the VPN concentrator and the external firewall. Connections from the trusted remote users to the internal or DMZ network will be terminated on the VPN concentrator, decrypted and passed over to the firewall for the permit/deny decision
- Internal Network – In the proposed design, the existing Internal Network is split from a flat topology into two network – one for the critical servers

including the database server, internal mail server and the management server, and another one for the internal users in general. The reason for splitting up is due to the difference in impact upon exposure between the 2 groups of devices. Access control can be better enforced with the physical separation.

VPN Gateway

Virtual Private Networks (VPNs) provide a way to set up a secure network connection between sites or nodes over the Internet. A VPN is basically an encrypted communication channel between to compatible devices, either standalone or integrated into a firewall, that can send encrypted messages and decrypt received messages from each other. Data privacy, encryption, authentication and integrity are the foundation for secure VPNs. With confidential information protected when passing through the ubiquitous public Internet, VPN provides a low cost solution to traditional dedicated connections.

As GIAC is already a Cisco shop with expertise developed on Cisco routers and soon-to-be-there PIX firewall, the design team has come the decision that a Cisco 3000 series VPN concentrator is a logical and sensible choice. The major benefit of using a standalone VPN Concentrator as opposed to using the integrated VPN function on a PIX firewall is that encrypted traffic will be decrypted at the concentrator, and therefore contents can be scanned and monitored, before entering the firewall.

Both Cisco 3005 and 3015 VPN Concentrators are designed for small to medium sized organizations with bandwidth requirements up to full-x T1/E1 (4Mbps maximum performance) and up to 100 simultaneous sessions. The 3015 will be the preferred choice because it is field-upgradeable to models 3030, 3060, and 3080 where hardware based encryption is used for consistent performance throughput. However, because of the significant cost difference between the two models ($4,000 for 3005 and $12,500 for 3015), 3005 with no built-in upgrade capability becomes the final choice of VPN gateway in order to meet the budget limit for the project. The 3000 Series Concentrator also comes with free and unlimited license for Cisco's cross-platform VPN client. It also supports wide range of VPN client software implementations including Cisco VPN client, VPN 3002 hardware client, the Microsoft Windows 2000 L2TP/IPSec client and the Microsoft PPTP for Windows 95, 98, NT and 2000.

With the Cisco VPN 3000 Concentrator software version 3.0 and later, address pool for NAT (Network Address Translation) can be configured on a group basis. This will allow separation of partners and mobile users into separate groups with different access privileges and restrictions.

As shown in the proposed design, the external interface of the VPN concentrator will be connected to the network between the border router and the external firewall, where all IPSec tunneled connections from remote users will be terminated. The VPN concentrator will then authenticate the users, decrypt the traffic and forward the packets via the second interface to the PIX firewall for access to appropriate resources as permitted by firewall policy.

Intrusion Detection System

An intrusion detection system (IDS) analyzes traffic for attacks. It examines individual packets within the data stream to identify threats from authorized users, back-door attacks and hackers who have thwarted the control systems to exploit network connections and access valuable data. There are two types of Intrusion Detection Devices: Host based (HIDS) and Network based (NIDS). Host based IDS monitor security within a network component, such as a server or a workstation. Network based IDS monitor the traffic over networks. Some IDS are strictly single purpose, while others are a combination of both network and host based.

NIDS also add a new level of visibility into the nature and characteristics of the network. They provide information about the use and usage of the network -- information that can be used to:

- Increase the value and efficacy of the control systems like firewalls and routers
- Produces hard evidence for the altering of the enterprise security policy
- Provides decision support for network management

In the proposed design for GIAC, SNORT[27] is chosen because it is open source based, and it is capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more.

SNORT network intrusion detection systems will be deployed in three critical segments – the VPN network and the internal and external service networks. IDS will not be deployed on the network between the border router and the external firewall because there will be excessive alerts which may not be relevant to GIAC at all. Also a NIDS on the external network will not be able to examine encrypted VPN traffic anyway.

In the proposal, SNORT 1.8.6 is installed on Dell PowerEdge 1500SC (with single PIII 1.13GHz processor, 1G RAM, 36GB hard drive at a list price of $2,150 each) on Red Hat Linux 7.2 platform. Each SNORT HIDS is configured with two

10/100BaseT Ethernet cards. The first one connects to the network being monitored and runs in promiscuous mode with no IP address. The second NIC connects to a subnet also shared by a second NIC on the syslog/management server so that all alerts and events from the NIDSs can be centrally monitored and managed.

Internal Firewall

Following the Defense in Depth approach, a second firewall is desirable to further protect the critical resources on the internal service network as well as the internal employee network. However, due to budget constraint at this time, the internal firewall will not be implemented as part of this design. It will be reviewed again as an enhancement when next year's infrastructure and security review comes up.

1.8 IP Addressing

The following table summarizes the subnet and host addresses being used in the proposed secure perimeter network design:

Network Name	Interface/Host Name	Description	Network Address
BROutside		Border Router to ISP Network	196.196.196.242/30
Public Address Networks			
PIXOutside		Firewall External Network – to Border router	192.73.235.240/29
	fwoutside	Interface Ethernet 0 on PIX firewall	192.73.235.241/29
	brinside	Interface Ethernet 0 on Border Router	192.73.235.242/29
	vpnoutside	Interface Ethernet 2 on VPN gateway	192.73.235.243/29
PIXExtService		External Service Network – public servers	192.73.235.0/25
	fwservice	Interface Ethernet 1 on PIX firewall	192.73.235.1/25
	webserver	iPlanet Web Server Ethernet interface	192.73.235.11/25
	appserver	Weblogic server Ethernet interface	192.73.235.12/25
	ftpserver	FTP server Ethernet interface	192.73.235.13/25
	Mailrelayserver	Mail Relay server Ethernet interface	192.73.235.14/25
PIXVPN		VPN Internal Network – VPN to Firewall	192.73.235.224/29
	fwvpn	Interface Ethernet 2 on PIX firewall	192.73.235.225/29
	vpninside	Interface Ethernet 1 on VPN gateway	192.73.235.226/29
Private Address Networks			
PIXInside		Firewall Internal Network – to internal router	172.20.1.0/28
	fwinside	Interface Ethernet 3 on PIX firewall	172.20.1.1/28
	iroutside	Ethernet 0 on Internal router	172.20.1.2/28
GIACIntService		GIAC Internal Service Network	172.20.2.0/24
	ir-server	Internal router interface for Internal Service network	172.20.2.1/24
	syslog-mngt	Syslog & Management Server	172.20.2.11/24
	ntp-radius	NTP & RADIUS Server	172.20.2.12/24
	internal-mail	Internal mail server	172.20.2.13/24
	tape-backup	Tape Backup Server	172.20.2.14/24
	db-server	Database Server	172.20.2.15/24
GIACIntUsers		Internal User Network – internal users	172.20.3.0/24
	ir-users	Internal router interface for GIAC	172.20.3.1/24

		users network	
	internal-dns	Intenal DNS/DHCP Server	172.20.3.11/24
GIACSnort		SNORT IDS to Syslog Server Network	192.168.10.0/24
VPNPartners		VPN – NAT address pool for Partners	172.20.129.0/24
VPNMobile		VPN – NAT address pool for Mobile Users	172.20.130.0/24

Table 1 IP Network Addresses

1.9 Cost Summary and Justification

The table below shows the capital cost of all the components required for the implementation of the proposed design. As the grand total meets the 5% of IT budget guideline that the design team found out earlier (see Design Guidelines and Consideration section), it is very likely that the project will be approved.

Component	Function	Qty	Product #	Components Cost
Cisco 4500M	Border router performing static packet filtering	1	No purchase required – existing equipment IOS 12.1.17	$0
Cisco PIX 515E Firewall with 4 interfaces and unrestricted software license	External firewall performing stateful inspection and stateful packet filtering functions	1	PIX-515E-UR-BUN PIX-4FE PIX-VPN-DES SF-PIX-6.2 (upgrade to 6.2(1), see Section 3.2)	$10,000
Cisco 3005 VPN	VPN concentrator supporting up to 100 simultaneous sessions	1	CVPN3005-E/FE-BUN	$4,000
Dell PowerEdge 1500SC	IDSs running SNORT on Red Hat Linux 7.2	3	Single 1.13GHz processor, 1GB RAM, 36GB Hard disk	$6,500
Cisco 2924M 24-port switch	New subnet for the SNORT IDSs connecting to the syslog server	1	WS-C2924M-XL-EN	$2,700
Cisco 4000 Router	Connecting internal networks to the external firewall	1	No purchase required – existing equipment	$0
Miscellaneous	Small Contingency fund for UPS, patch cables, etc.			$1,800
Total				**$25,000**

Table 2 Cost of Security Components

Assignment 2 – Security Policy and Tutorial

2.1 Border Router Security Policy

The border router is a Cisco 4500M with 4 Ethernet and a high-speed serial interfaces, 16MB Flash and 16MB RAM running IOS 12.1.17, a stable GD[28] (General Deployment) release.

There are four basic functions[29] that a border router performs:

- Blocking specific IP addresses to prevent spoofing traffic and traffic from private and unused network addresses
- Augmenting firewall policy
- Control ICMP traffic
- Blocking absolutes such as source routing and broadcast

As the border router is the first line of defense against attacks from the Internet, there are also other security areas that need to be tightened, including:

- Password Management
- Controlling interactive access via console port, TTYs and VTYs
- Proper warning banners
- Commonly configured management services including SNMP and HTTP
- Management and Interactive Access
- Logging
- Disabling all unnecessary services
- Staying up-to-date with latest security patches

The border router is configured following the guidelines from Cisco[3031], the National Security Agency Router Security Configuration Guide[32], and the SANS training course material[33].

A major national service provider is selected to provide the Internet connection with DNS services for GIAC because they have demonstrated that best current practices have been followed, including the compliance with RFC 2827 on ingress filter that denies any traffic that does not have the source address that was expected on a particular interface. For example, if an ISP is providing a connection to the IP address 192.73.235.0/24, the ISP could filter traffic so that only traffic sourced from address 192.73.235.0/24 can enter the ISP router from that interface. Note that unless all ISPs implement this type of filtering, its effectiveness is significantly reduced. Also, the further you get from the devices you want to filter, the more difficult it becomes to do that filtering at a granular level.

When defining access control lists, It is important to keep the order of rules in the correct sequence because Cisco devices, including routers and PIX firewall, read

the rules from top to bottom, and as soon as a match is found, they will stop reading any other rules still on the lists.

The following security related lines of configuration on the border router are grouped together with comments on functions:

```
! Make sure accurate local time (instead of GMT) is used in all log entries
        service timestamps debug datetime msec localtime show-timezone
        service timestamps log datetime msec localtime show-timezone

! Set hostname of the border router
        hostname giac-br1

! Setting up password encryption. The first statement provides only a minimum
! protection for configured password because it uses a simple Vigenere cipher. It
! does not apply to passwords set with the “enable secret” command, but it does
! apply to passwords set with “enable password”, if any. The second line uses
! Type 5 encryption with MD5 hashing for strong protection.
        service password-encryption
        enable secret <secret-password>
        no enable password

! Setting buffer size and logging level to log server
        logging 172.20.2.11
        logging facilities syslog
        logging buffered 16384 informational
        logging trap informational
        no logging console

! Avoid using these services (DEC): Discard, Echo, and Chargen.
        no service tcp-small-servers
        no service udp-small servers

! Use the following global commands to explicitly disable the following services:
        no ip source-route
        no service pad
        no service finger
        no ip http server
        no ip bootp server
        no ip domain-lookup
        no cdp run

! Configure an ACL for TCP Intercept to protect the servers on the DMZ from
! SYN flood attacks
        access-list 101 permit tcp any 192.73.235.0 0.0.0.128

! Enable TCP Intercept to protect against SYN flooding, watch the "flow" for only
! 60 seconds (not the default 24 hours), keep half-open sockets only 10 seconds,
! set the low water mark to 1500 active opens per minute, and set the high water
```

```
! mark to 6000 active opens per minute:
        ip tcp intercept list 101
        ip tcp intercept connection-timeout 60
        ip tcp intercept watch-timeout 10
        ip tcp intercept one-minute low 1500
        ip tcp intercept one-minute high 6000

! Use the following interface command to configure IP address on the interfaces
! and to disable the unnecessary services:
        interface serial 0
        ip address 196.196.196.242 255.255.255.252
        no cdp enable
        no ip directed-broadcast
        no ip redirects
        no ip unreachales
        no ip proxy-arp
        no ip mroute-cache
        !
        interface ethernet 0
        ip address 192.73.235.242 255.255.255.248
        no cdp enable
        no ip directed-broadcast
        no ip redirects
        no ip unreachales
        no ip proxy-arp
        no ip mroute-cache

! Configure an basic ACL to allow snmp access only from the Management Server to the
! Border Router
        access-lsit 10 permit 172.20.2.11
        access-list 10 deny any any log

! On the serial interface facing the Internet, an extended ACL is used to deny any
! inbound traffic spoofing router's own addresses, GIAC's public address, loop
! back address, private network addresses, and multicast addresses as source
! addresses:

        access-list 110 deny ip host 196.196.196.242 host 196.196.196.242 log
        access-list 110 deny ip host 192.73.235.242 host 192.73.235.242 log
        access-list 110 deny ip 192.73.235.0 0.0.0.255 any log
        access-list 110 deny ip 127.0.0.1 0.255.255.255 any log
        access-list 110 deny ip 10.0.0.0 0.255.255.255 any log
        access-list 110 deny ip 172.16.0.0 0.15.255.255 any log
        access-list 110 deny ip 192.168.0.0 0.0.255.255 any log
        access-list 110 deny ip 224.0.0.0 15.255.255.255 any log
        access-list 110 deny ip 240.0.0.0 15.255.255.255 any log

! On the same ACL, we also need to block certain undesirable services initiated
! from outside to come in, including telnet (TCP 23), tftp (UDP 69), sunrpc
! (TCP/UDP 111), Windows Netbios (TCP/UDP 135 – 139), TCP Direct for
```

```
! Windows 2000 (TCP/UDP 445), snmp (UDP 161-162), and X11 (TCP 6000-
! 6063):
        access-list 110 deny tcp any any eq telnet log
        access-list 110 deny udp any any eq tftp log
        access-list 110 deny tcp any any eq 111 log
        access-list 110 deny udp any any eq 111 log
        access-list 110 deny tcp any any range 135 139 log
        access-list 110 deny udp any any range 135 139 log
        access-list 110 deny tcp any any eq 445 log
        access-list 110 deny udp any any eq 445 log
        access-list 110 deny udp any any range 161 162 log
        access-list 110 deny tcp any any range 6000 6063 log
        access-list 110 deny udp any any range 6000 6063 log

! Finally we need to let all other IP traffic in to the GIAC public address space,
! and let the firewall to do further stateful access control:
        access-list 110 permit ip any 192.73.235.0 0.0.0.255

! An outbound extended ACL on the serial 0 interface can be used to restrict
! undesirable traffic such as ICMP responses by specifying the ICMP type and
! code, some of them are listed below:
```

Type	Name	Code
3	Destination unreacheable	0 Net Unreachable 1 Host Unreachable 2 Protocol unreacheable 3 Port unreacheable 4 Fragmentation needed 13 Communication administratively prohibited
4	Source Quench	No code
11	Time Exceeded	0 Time to Live exceeded in transit
18	Address Mask Reply	No code

```
        access-list 111 deny icmp any any 3 0
        access-list 111 deny icmp any any 3 1
        access-list 111 deny icmp any any 3 2
        access-list 111 deny icmp any any 3 3
        access-list 111 deny icmp any any 3 4
        access-list 111 deny icmp any any 3 13
        access-list 111 deny icmp any any 4
        access-list 111 deny icmp any any 11 0
        access-list 111 deny icmp any any 18

! Now we can allow all traffic with GIAC's public address as source address to
! communicate with the outside world :
        access-list 111 permit ip 192.73.235.0 0.0.0.255 any
```

```
! ACL 110 and 111 are then applied to the serial 0 interface in the inbound and
! outbound direction respectively:
        interface serial 0
        ip access-group 110 in
        ip access-group 111 out

! Go IP classless and setting up static routes:
        ip route 0.0.0.0 0.0.0.0 196.196.196.241
        ip route 192.73.235.0 0.0.0.128 192.73.235.241
        ip route 192.73.235.224 0.0.0.8 192.73.235.241

! Configure snmp read-only with non-default community string
        snmp-server community <hard-to-guess-password> RO 10

! Login banner
        banner motd c
        +---------------------------------------------------------------------------------------------+
        |                          WARNING                                                            |
        |                          ---------------                                                    |
        |                                                                                             |
        | The programs and data stored on this system are licensed to and/or are |
        | private property of this company and are lawfully available only to          |
        | authorized users for approved purposes.  Unauthorized access to any   |
        | program or data on this system is not permitted, and any unauthorized  |
        | access beyond this point may lead to prosecution. This system may be  |
        | monitored at any time for operational reasons, therefore, if you are       |
        | not an authorized user,                                                                     |
        |                    DO NOT ATTEMPT TO LOG IN.                                |
        +---------------------------------------------------------------------------------------------+|
        c

! Disabling remote access to aux port and VTY lines
        line aux 0
        transport input none
        line vty 0 4
        transport input none

! Setting automatic timeout to 5 minutes and set password on the console port
        line con 0
        exec-timeout 5 0
        password 0 <password>

! Finally NTP is configured by pointing directly to 2 Stratum 2 servers in the
! Internet, This will avoid the need to open a port on the firewall for NTP traffic in
! order to point to the internal NTP server:
        ntp server 65.211.109.1
        ntp server 192.73.48.6
```

2.2 External Firewall Security Policy

Policy Requirements

The policies to be defined on the PIX firewall have to reflect those business needs discussed in Assignment One, as summarized in the following table:

Requirements	Source	Destination	Service	Direction
Inbound from Internet				
Insecure access to web server	Any	Web server	http	Internet to External Service Network
Secure access to web server	Any	Web server	https/ssl	Internet to External Service Network
Mail	Any	Mail Relay Server	smtp	Internet to External Service Network
File upload/download (For Partners and mobile users)	Any (Need ID and password)	FTP Server	ftp	Internet to External Service Network
Inbound snmptrap and syslog	Inside interface of border router	Syslog/Management Server	Snmptrap, syslog	Border router to Internal Service Network
ICMP responses	Any	Any	Four types of ICMP replies	Internet to other networks
Services for External Service Network				
Application server to Database server	Weblogic App Server	Oracle DB Server	SQL*Net v2	External Service Net to Internal Service Net
Backup all servers on External Service Network to Tape Backup Server	External Service Network	Tape Backup Server	800-899 4800-4899 13720-13721	External Service Network servers to Tape Backup Server
Backup all servers on External Service Network to Tape Backup Server	Tape Backup Server	External Service Network	13782-13783	Tape Backup Server to External Service Network servers
Snmptrap and syslog to manage't server	External Service Net	Syslog&mngt server	Snmptrap syslog	External Service Network to management server
DNS lookup to ISP DNS	External Service Net	Syslog&mngt server	Domain (udp)	External Service Network to ISP DNS
NTP service from external stratum 2 servers	External Service Net	Internet Time Servers	ntp	External Service Network to Internet
Exchange mail with Internal Mail server	Mail Relay server	Internal Mail server	smtp	Mail Relay server to Internal Mail server
Exchange mail with the Internet	Mail Relay server	Internet	smtp	Mail Relay server to the Internet
ICMP for support purpose	External Service Network	The rest of GIAC networks	icmp	External Service Network to the other networks

VPN Users				
Mobile Users to Internal Network	GIAC user group by NAT address	Internal networks	all	GIAC VPN users to Internal networks
Mobile Users to External Service Network	GIAC mobile user group by NAT addresses	External Service Network	All except smtp	GIAC VPN users to External Service networks
Mobile Users to the Internet	GIAC user group by NAT address	Internet	http, https, ftp	GIAC Mobile users to the Internet
Partner VPN users to External Service Network	GIAC Partner user group by NAT addresses	Service Network	http, https, ftp, ssh	VPN to External Service networks
Partner VPN users to Database Access	Partner user group by NAT address	Database Server	SQL*Net v2	VPN to Internal Service Network
Network Services for VPN Concentrator	VPN Internal interface	Internal Network	Ntp, dns (utp), radius, syslog, snmptrap	VPN Concentrator to Internal Network
Allow ping from VPN users, and make VPN inside interface pingable	VPN internal network	Any	Ping, and ping response	VPN internal network to any
Inside Networks				
Denying outbound connection to the VPN clients	Internal networks	VPN NAT networks	Deny any	Internal to VPN clients
Internal mail server to send and receive mail via Mail Relay Server	Internal Mail Server	Mail Relay Server	smtp	Internal mail server to Mail Exchange Server
Internal users to servers on External Service Network	Internal networks	External Service Network	http, https, ssh	Internal networks to External Service Network
Internal users to Internet	Internal Networks	Internet	http, https, ssh, ftp, telnet	Internal networks to Internet (including to Border router)
Tape Backup for servers on External Service Network	Tape Backup Server	External Service Network	13782-13783	Tape Backup server to External Service Network
DNS for internal DNS server	Internal DNS Server	ISP DNS Server	dns (udp & tcp)	Internal DNS server to Internet
NTP for Internal NTP server	Internal NTP Server	Internet	ntp	Internal NTP server to stratum 2 servers

Snmp polling to the VPN internal interface	Syslog & mngt server	VPN internal interface	snmp	Internal management server to VPN inside interface
SNMP management of public servers	Manageme nt server	External Service Network	snmp	Management server to External Service Network
Allow ICMP	Internal network	Any	icmp	Ping from internal networks to any net

Identifying Each Interface

Note: with PIX v5.3 and later software release, it is no longer necessary to use Ethernet 1 as the inside network port and Ethernet 2 outside network port. Any port, whether fixed or a PCI expansion port, and any interface type can be assigned to be the inside or outside network port.

The syntax for ACL rules on the PIX is similar to IOS ACLs on Cisco routers:

```
access-list ID {action} protocol source_addr source_mask [operator port]
destination_addr destination_mask [operator port]
```

or in the case of access-list for ICMP packets:

```
access-list ID {action} icmp source_addr
source_mask destination_addr destination_mask icmp_type
```

where

ID	= Number or name of access-list
action	= Either permit or deny, -whether to drop or pass the packet
protocol	= The protocol, either ip, tcp, udp or icmp
source_addr	= The host part of the packet's source IP address
source_mask	= The network mask of the packet's source IP address
destination_addr	= The host part of the packet's destination IP address
destination_mask	= The network mask of the packet's destination IP address
operator port	= any of eq, gt, lt, or range, to describe the following port #
icmp_type	= An ICMP type code or name, e.g. echo, echo-reply

Note: Unlike ACLs on Cisco routers, ACLs on PIX are applied inbound only.

The first step in configuring a PIX Firewall is to use the nameif command to identify and set the security level of each interface on the firewall:

```
nameif ethernet0 fwoutside security0
nameif ethernet1 fwservice security40
nameif ehternet2 fwvpn security60
nameif ethernet3 fwinside security100
```

The purpose of assigning a security level to each interface is to identify the relative degree of trust-worthiness of networks connecting to each interface. For interfaces with a higher security level such as the inside interface, or a perimeter interface relative to the outside interface, use the NAT and global commands to let users on the higher security interface access a lower security interface. For the opposite direction, from lower to higher, use the access-list command.

The next step is to assign an ip address to each interface in the PIX firewall:

```
ip address fwoutside 192.73.235.241 255.255.255.248
ip address fwservice 192.73.235.1 255.255.255.128
ip address fwvpn 192.73.235.225 255.255.255.248
ip address fwinside 172.20.1.1 255.255.255.240
```

Note: Always specify a network mask with the ip address command. If you let PIX firewall assign a network mask based on the IP address, you may not be permitted to enter subsequent IP addresses if another interface's address is in the same range as the first address.

Enable Fixup Protocols and Create a Default Route

Cisco muffles each of the supported fixup protocols with wrapper, the so-called ASA (Adaptive Security Algorithm). Once enabled it is valid for inbound and outbound traffic and there is no extra commands needed to configure it except for one or the other direction.

```
fixup protocol ftp 21
fixup protocol http 80
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
```

Use the **route** command to set a default route to the outside router.

```
route fwoutside 0 0 192.73.235.242 1
```

This command states that the default router is on the fwoutside interface, as defined above. The 0 0 information is an IP address of 0.0.0.0 and mask of 0.0.0.0, which the PIX Firewall associates with the default route. The route command could be read as "if I have a packet intended for IP address 0.0.0.0, send it to 192.73.235.242 instead." The "1" at the end is the number of hops that the router is from the PIX Firewall. Hops are number of routers, so 1 hop is the router nearest the PIX Firewall, in this case, on the fwoutside interface. And there can only be one default route for the PIX firewall.

Defining Host Names

Host names can be used in ACLs instead of their IP addresses, and they are defined with the use of the name command:

```
name 192.73.235.241 fwoutside
name 192.73.235.242 brinside
name 192.73.235.243 vpnoutside
name 192.73.235.1 fwservice
name 192.73.235.11 webserver
name 192.73.235.12 appserver
name 192.73.235.13 ftpserver
name 192.73.235.14 mailrelayserver
name 192.73.235.225 fwvpn
name 192.73.235.226 vpninside
name 196.196.196.250 isp-dns
name 172.20.1.1 fwinside
name 172.20.1.2 iroutside
name 172.20.2.1 ir-servers
name 172.20.2.11 syslog-mngt
name 172.20.2.12 ntp-radius
name 172.20.2.13 internal-mail
name 172.20.2.14 tapebackup
name 172.20.2.15 dbserver
name 172.20.3.1 ir-users
name 172.20.3.11 internal-dns
```

Configuring ACLs on the Outside Network (acl_fwoutside)

The ACL fwoutside allows inbound connection requests from the Internet to the public servers on the External Service Network, as identified on Table in Section 2.2:

```
Access-list acl_fwoutside permit tcp any host webserver eq http
Access-list acl_fwoutside permit tcp any host webserver eq https
Access-list acl_fwoutside permit tcp any host mailrelayserver eq smtp
Access-list acl_fwoutside permit tcp any host ftpserver eq ftp
```

Note: “any” in the access-list stands for any host in any network, or “0.0.0.0 0.0.0.0”

Note: PIX firewall permits the following TCP literal names[34]: bgp, chargen, cmd, daytime, discard, domain, echo, exec, finger, ftp, ftp-data, gopher, h323, hostname, http, ident, irc, klogin, kshell, lpd, nntp, pop2, pop3, pptp, rpc, smtp, sqlnet, sunrpc, tacacs, talk, telnet, time, uucp, whois, and www. Permitted UDP literal names are biff, bootpc, bootps, discard, dnsix, echo, mobile-ip, nameserver, netbios-dgm, netbios-ns, ntp, rip, snmp, snmptrap, sunrpc, syslog, tacacs, talk, tftp, time, who, and xdmcp.

The next two lines allows the border router to send snmptrap and syslog to the syslog&mngt server on the internal network:

```
Access-list acl_fwoutside permit udp brinside host syslog-mngt eq snmptrap
Access-list acl_fwoutside permit udp brinside host syslog-mngt eq syslog
```

With PIX software release 5.0.1 or higher, inbound ICMP through the PIX is denied by default; outbound ICMP is permitted, but the incoming reply is denied by default.

Note: Ping and trace route access should not be allowed from the Internet to any hosts on the internal networks to avoid information leakage..

However, to permit responses to ICMP requests initiated by all devices on GIAC’s networks to the Internet, four types of unrestricted ICMP reply messages[35] need to be allowed as shown below:

```
Access-list acl_fwoutside permit icmp any any echo-reply
Access-list acl_fwoutside permit icmp any any unreacheable
Access-list acl_fwoutside permit icmp any any source-quench
Access-list acl_fwoutside permit icmp any any time-exceeded
```

The following line ends the access-list “outside” by explicitly denying any packets not allowed by the lines above:

```
Access-list acl_fwoutside deny ip any any
```

Finally, apply the access list to the interface:

```
Access-group acl_fwoutside in interface fwoutside
```

Configuring ACLs on the External Service Network (acl_fwservice)

To allow Weblogic server on the External Service Network to access the Database server on the Internal Service Network:

```
Access-list acl_fwservice permit tcp host appserver host dbserver eq sqlnet
```

The following lines allow for tape backup service from the External Service Network to the Tape Backup Server:

```
Access-list acl_fwservice permit tcp 192.73.235.0 255.255.255.128 host
tapebackup range 800 899
Access-list acl_fwservice permit tcp 192.73.235.0 255.255.255.128 host
tapebackup range 4800 4899
Access-list acl_fwservice permit tcp 192.73.235.0 255.255.255.128 host
tapebackup range 13720 13721
```

Note: PIX Firewall uses a subnet mask, whereas Cisco IOS software uses a wildcard mask. (In Cisco IOS software, the inverse mask in the above lines would be specified with the 0.0.0.255 value. For an explanation on Inverse Mask, please see Section 2.4 on Border Router Implementation Tutorial).

The following lines allow snmptrap, syslog, and DNS lookup and for the servers on the External Service Network:

```
Access-list acl_fwservice permit udp any host syslog-mngt eq snmptrap
Access-list acl_fwservice permit udp any host syslog-mngt eq syslog
Access-list acl_fwservice permit udp any host isp-dns eq domain
```

Note: tcp domain is not required, as these servers are not expected to make zone transfer request from the ISP DNS server.

Mail exchange by smtp is allowed from the Mail Relay Server to the Internal Mail Server with the following line:

```
Access-list acl_fwservice permit tcp host mailrelayserver host internal-mail eq
smtp
```

Once the specific inbound requirements to the internal networks are defined as stated above, we can now allow general ntp and mail access to the Internet but not to the rest of the GIAC networks:

```
Access-list acl_fwservice deny ip 192.73.235.0 255.255.255.128 172.20.0.0
255.255.128.0
Access-list acl_fwservice deny ip 192.73.235.0 255.255.255.128 192.73.235.128
255.255.255.128
Access-list acl_fwservice permit udp any any eq ntp
Access-list acl_fwservice permit tcp host mailrelay any eq smtp
```

Note: The order of the rules are important, otherwise the traffic flows intended for the Internet may also show up on the internal networks, and causing security and performance issues.

To allow ICMP traffic ping and trace route) to the internal networks for trouble-shooting purposes, the following lines are required:

```
Access-list acl_fwservice permit icmp any 172.20.0.0 255.255.128.0
Access-list acl_fwservice permit icmp any 192.73.235.128 255.255.255.128
Access-list acl_fwservice permit icmp any any echo-reply
Access-list acl_fwservice permit icmp any any unreacheable
Access-list acl_fwservice permit icmp any any source-quench
Access-list acl_fwservice permit icmp any any time-exceeded
access-list acl_fwservice permit udp any range 32769 65535 172.20.0.0
255.255.128.0range 33434 33523
access-list acl_fwservice permit udp any range 32769 65535 192.73.235.128
255.255.255.128 range 33434 33523
```

And the following closing line for this ACL will stop all other traffic:

```
Access-list acl_fwservice deny ip any any
```

Finally, apply the access list to the interface:

Access-group acl_fwservice in interface fwservice

Configuring ACLs on the VPN Network (acl_fwvpn)

There are three groups of source address on packets coming to the fwvpn interface of the PIX firewall: the NAT pool of addresses for GIAC Partners (172.20.129.0/24), that for GIAC mobile employees and teleworkers (172.20.130.0/24) and the internal Ethernet interface of the VPN itself (192.73.235.226/29).

The following lines allow GIAC mobile employees and teleworkers to have the same access rights, after proper authentication on the VPN, to the resources on the internal networks and the External Service Network, except smtp access to the Mail Relay Server:

```
Access-list acl_fwvpn deny tcp 172.20.130.0 255.255.255.0 host mailrelayserver
eq smtp
Access-list acl_fwvpn permit ip 172.20.130.0 255.255.255.0 172.20.0.0
255.255.128.0
Access-list acl_fwvpn permit ip 172.20.130.0 255.255.255.0 192.73.235.0
255.255.255.128
```

GIAC Mobile users are also allowed to access the Internet once they are connected to GIAC's network via VPN:

```
Access-list acl_fwvpn permit tcp 172.20.130.0 255.255.255.0 any eq http
Access-list acl_fwvpn permit tcp 172.20.130.0 255.255.255.0 any eq https
Access-list acl_fwvpn permit tcp 172.20.130.0 255.255.255.0 any eq ftp
```

For the Partners VPN users, access are much more restrictive:

```
Access-list acl_fwvpn permit tcp 172.20.129.0 255.255.255.0 host webserver eq
http
Access-list acl_fwvpn permit tcp 172.20.129.0 255.255.255.0 host webserver eq
https
Access-list acl_fwvpn permit tcp 172.20.129.0 255.255.255.0 host ftpserver eq
ftp
Access-list acl_fwvpn permit tcp 172.20.129.0 255.255.255.0 host ftpserver eq
ssh
Access-list acl_fwvpn permit tcp 172.20.130.0 255.255.255.0 host dbserver eq
sqlnet
```

The following lines will provide proper network services for the VPN concentrator:

```
Access-list acl_fwvpn permit udp host vpninside host ntp-radius eq ntp
Access-list acl_fwvpn permit udp host vpninside host ntp-radius eq radius
Access-list acl_fwvpn permit udp host vpninside host syslog-mngt eq syslog
Access-list acl_fwvpn permit udp host vpninside host syslog-mngt eq snmptrp
Access-list acl_fwvpn permit udp host vpninside host internal-dns eq domain
```

Finally, the following lines allow any users to ping and trace route anywhere, and allow the VPN internal interface to respond to ping:

```
Access-list acl_fwvpn permit icmp any any
Access-list acl_fwvpn permit icmp host vpninside any echo-reply
Access-list acl_fwvpn permit icmp host vpninside any unreacheable
Access-list acl_fwvpn permit icmp host vpninside any source-quench
Access-list acl_fwvpn permit icmp host vpninside any time-exceeded
access-list acl_fwvpn permit udp any range 32769 65535 any range 33434
33523
```

A deny all statement is again required at the end of the access list:

```
Access-list acl_fwvpn deny ip any any
```

Finally, apply the access list to the interface:

```
Access-group acl_fwvpn in interface fwvpn
```

Configuring ACLs on the Inside Network (acl_fwinside)

The access list acl_fwinside controls all traffic leaving the internal networks to the outside world via the PIX firewall.

There is no application requirement for connections initiated from the internal network to the VPN networks:

```
Access-list acl_fwinside deny ip 172.20.0.0 255.255.128.0 172.20.128.0
255.255.255.128
```

The following line allows the internal mail server to exchange mail with the Mail Relay server in the External Service Network:

```
Access-list acl_fwinside permit tcp host internal-mail host mailrelayserver eq
smtp
```

Http, https and ssh can be initiated from anywhere in the internal network to the External Service Network and the Internet:

```
Access-list acl_fwinside permit tcp 172.20.0.0 255.255.128.0 any eq http
Access-list acl_fwinside permit tcp 172.20.0.0 255.255.128.0 any eq https
Access-list acl_fwinside permit tcp 172.20.0.0 255.255.128.0 any eq ssh
```

The clear-text based telnet and ftp are allowed from the internal networks to the Internet but not to the External Service Network:

```
Access-list acl_fwinside deny tcp 172.20.0.0 255.255.128.0 192.73.235.0
255.255.255.128 eq telnet
Access-list acl_fwinside deny tcp 172.20.0.0 255.255.128.0 192.73.235.0
255.255.255.128 eq ftp
Access-list acl_fwinside permit tcp 172.20.0.0 255.255.128.0 any eq telnet
Access-list acl_fwinside permit tcp 172.20.0.0 255.255.128.0 any eq ftp
```

The Netbackup Tape Backup server needs to access the servers on the External Service Network via tcp port 13782-13783:

```
Access-list acl_fwinside permit tcp host tapebackup 192.73.235.0
255.255.255.128 range 13782 13783
```

The internal DNS server needs to be able to send DNS queries and zone transfer to the ISP DNS server:

```
Access-list acl_fwinside permit udp host internal-dns host isp-dns eq domain
Access-list acl_fwinside permit tcp host internal-dns host isp-dns eq domain
```

And the internal NTP server need to synchronize with the stratum 2 Internet time servers:

```
Access-list acl_fwinside permit udp host ntp-radius any eq ntp
```

SNMP management requires snmp polling from the Syslog&Mngt Server to the Border Router, the VPN concentrator (internal interface) and all the servers on the External Service Network.

```
Access-list acl_fwinside permit udp host syslog-mngt host brinside eq snmp
Access-list acl_fwinside permit udp host syslog-mngt host vpninside eq snmp
Access-list acl_fwinside permit udp host syslog-mngt 192.73.235.0
255.255.255.128 eq snmp
```

The following lines allows ICMP ping and trace route from internal networks to any networks:

```
Access-list acl_fwinside permit icmp any any
access-list int permit udp any range 32769 65535 any range 33434 33523
```

Ending the acess list is the deny all statement:

```
Access-list acl_fwinside  deny ip any any
```

Finally, apply the access list to the interface:

```
Access-group acl_fwinside in interface fwinside
```

2.3 VPN Security Policy

Note: Cisco VPN3000 Concentrator software is upgraded from 3.6 to 3.6(1) in order to address the multiple vulnerabilities[36] published in September 2002.

The VPN Concentrator creates a virtual private network by creating a secure connection across a TCP/IP network, such as the Internet, that users see as a private connection. It can create single-user-to-LAN connections or LAN-to-LAN connections.

In the case of GIAC secure perimeter network design, the primary function of the VPN concentrator is to provide strong authenticate and a secure connection for the remote users. For monetary and ease of implementation reasons, it is decided that site-to-site VPN connections will not be implemented this time. For the same reasons, Cisco VPN Client software 3DES Release 3.6.1 is used as the standard VPN client software for all remote users, including GIAC mobile users and teleworkers, as well as those users from Partners.

The Cisco VPN 3005 Concentrator, running software release 3.6.1, performs the following functions:

- Establishes tunnels
- Negotiates tunnel parameters
- Authenticates users
- Assigns user addresses
- Encrypts and decrypts data
- Manages security keys
- Manages data transfer across the tunnel
- Manages data transfer inbound and outbound as a tunnel endpoint or router

To accomplish these functions, Cisco VPN 3000 Series concentrators invokes various standard protocols including:

- Tunneling
  - IPSec
  - GRE
  - PPTP
  - L2TP/PPTP
  - L2TP/IPSec
  - NAT Transparent IPSec
  - IPSec/TCP
- Encryption
  - DES
  - 3DES
  - AES –128 and AES-256

- Authentication
  - Internal Authentication
  - RSA Digital Certificate
  - Radius
  - Microsoft NT Domain authentication
- Integrity
  - HMAC-MD5
  - HMAC-SHA-1
- Key Management
  - Internet Key Exchange (IKE)

One of the features of the Cisco VPN concentrators is its easy of configuration, especially with the Quick Configuration which allows for accepting default values when possible and configuring minimal parameters to make VPN 3005 Concentrator operational. When using Quick Configuration, keep in mind that:

- The quick configuration menus appear only once—and you can go through the steps of quick configuration only once—unless you reboot the system with the Reboot with Factory/Default configuration option.
- Entries are case-sensitive; for example, admin and ADMIN are different passwords.
- The system displays more tips and examples than appear in the dialogue here.
- The system shows current or default entries in brackets; e.g., [0.0.0.0].
- After each entry, press the <Enter> key on the console keyboard.
- Configuration entries take effect as soon as you enter them, and they constitute the active, or running, configuration. Many quick configuration menus let you save the active configuration to the config file, and thus make it the boot configuration. We suggest you do so.
- If you make a mistake, the system displays an Error message and repeats the previous prompt. You can often enter a correct value and proceed, but in some cases you may need to restart the section to correct an earlier error.

Tunneling Protocols and Options

Cisco VPN Concentrators support a number of tunneling protocols, including PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol) with or without Microsoft encryption required, and IPSec (IP security Protocol)[37]. PPTP is probably the most deployed VPN system in terms of market penetration because it is shipped with every copy of Windows operating system software. However it has been proven that PPTP is dated and cryptographically weak[38] [39]. Layer Two Tunneling Protocol (L2TP) is an extension of PPTP and is combining the best features of PPTP from Microsoft and L2F (Layer 2 Forwarding) protocol from Cisco Systems. The two main components that make up L2TP are the L2TP Access Concentrator (LAC), which is the device that physically terminates a call

and the L2TP Network Server (LNS), which is the device that terminates and possibly authenticates the PPP stream.

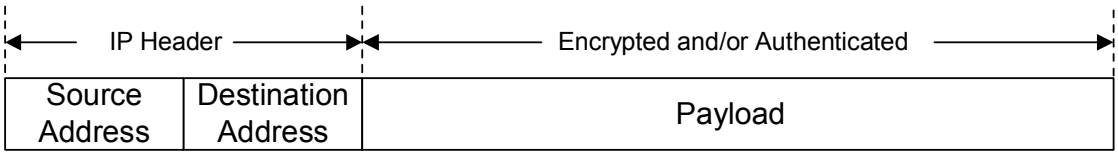
IPSec provides the most complete architecture for VPN tunnels, and it is perceived as the most secure protocol. IPSec is a set of protocol including IKE (Internet Key Exchange)[40], AH (Authentication Header)[41], and ESP (Encapsulating Security Payload)[42]. Together, they add to the network layer security services such as Confidentiality, Authentication, Integrity, Access Control and partial protection against traffic flow analysis. In simple terms, IPSec provides secure tunnels between two peers, such as between a remote client and a router or between two routers, by specifying the keying material and establishing security associations that are defined by protocols and algorithms used to protect sensitive packets. Security associations are unidirectional and are established per security protocol (AH or ESP). When the IPSec peer sees sensitive packets, it sets up the appropriate secure tunnel and sends the packets through the tunnel to the remote peer.

IKE is a standard key negotiation and management mechanism to promote interoperability between devices by allowing for the negotiation of services. IKE is a form of ISAKMP (Internet Security Association Key Management Protocol) /Oakley specifically for IPSec.

The Authentication Header (AH) is a mechanism for providing connectionless data integrity and authentication for IP datagrams, but does not provide confidentiality through encryption. It can also provide non-repudiation, depending on which cryptographic algorithm is used and how keying is performed.

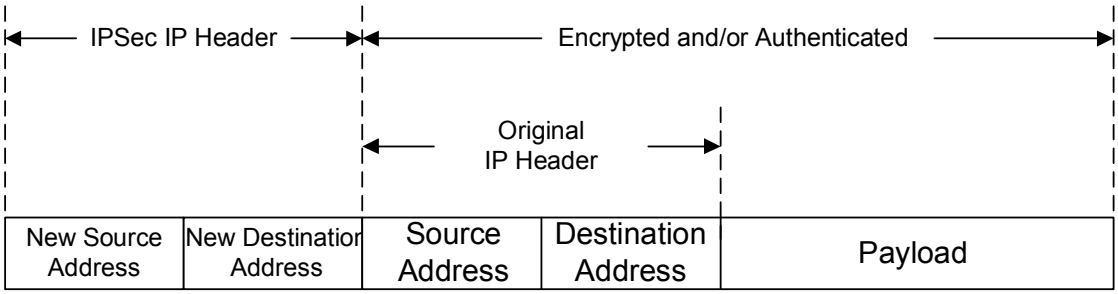
The Encapsulating Security Payload (ESP) is to provide confidentiality and integrity by encrypting data to be protected and placing them in the data portion of the IP Encapsulating Security Payload, but does not protect the new IP header. For strong authentication plus confidentiality, AH and ESP can be deployed in either transport mode or tunnel mode.

In transport mode, only the IP payload is encrypted, and the original IP headers are left unchanged. Tunnel mode can only be used between IPSec hosts but not between security gateways. One advantage of using transport mode is the low overhead because only a few bytes are added to each packet. It also allows devices on the public network to see the final source and destination addresses of the packet. This allows implementation of functions such as quality of service based on the information on the IP header. Below is the format of a transport mode packet:



IPSec Transport Mode

In tunnel mode, the entire original IP datagram is encrypted, and it becomes the payload in a new IP packet with a new header. This allows a network device such as a router to act as an IPSec proxy. The advantage of deploying IPSec with tunnel mode is that it can be implemented between security gateways in the network infrastructure without modifying any operating systems or applications. Below is the tunnel mode packet format:



IPSec Tunnel Mode

There are two distinct phases with IPSec. Initial authentication takes place in the first phase when the two ends of the connection verify to each other that they are in fact who they claim to be. This communication channel is called ISAKMP Security Association. It can be done by as simple as exchanging the hash of a pre-shared secret or as complex as using digital certificate with full deployment of public key infrastructure (PKI). When a shared secret is used, IKE (Internet Key Exchange) protocol handles the negotiation so communications start off using UDP port 500. In phase two, parameters including encryption type, key strength and life cycle, and security services are negotiated. When all parameters are agreed upon, encrypted data can start flowing in a secure tunnel.

For its simplicity of implementation, ease of support and cost effectiveness, GIAC Security team has recommended using IPSec with pre-shared secret for the initial authentication. 3DES will be used for encryption and MD5 for authentication.

Note: Cisco recommends using MD5 hashing in remote-access VPN solutions and SHA-1 in site-to-site VPN solutions. SHA-1 is used for site-to-site solutions because it provides greater security, performing more algorithmic rounds than MD5 and producing 160-bit hash value compared to 128-bit value of MD5. In addition, SHA-1 uses the input message to compute the hash function words, while in MD5 these words are constant.

Configuring the VPN Concentrator

Logon to the VPN console and start configuring:

1. Disabling PPTP

1.1 Configure protocols and encryption options.
This table shows current protocol settings

```
        PPTP                |        L2TP
-------------------------------------------------------------
 Enabled                    | Enabled
 No Encryption Req          | No Encryption Req        |
-------------------------------------------------------------
1) Enable PPTP
2) Disable PPTP
Quick -> [ 1 ]
```

At the cursor, enter **2** to disable PPTP.

1.2 To disable L2TP

```
1) Enable L2TP
2) Disable L2TP
Quick -> [ 1 ]
```

At the cursor, enter **2** to disable L2TP

1.3 To enable IPSec

```
1) Enable IPSec
2) Disable IPSec
Quick -> [ 1 ] _
```

At the cursor, press **<Enter>** to accept the default (1), which enables IPSec.

2. Configuring Authentication

There are four options in server types to authenticate users:

- The internal VPN Concentrator authentication server
- An external RADIUS (Remote Authentication Dial-In User Service) server
- An external NT (Windows NT) Domain server
- An external SDI (RSA Security Inc. SecurID) server

At the VPN console:

Specify how to authenticate users.
1) Internal Authentication Server
2) RADIUS Authentication Server
3) NT Domain Authentication Server
4) SDI Authentication Server
5) Continue
Quick -> _

At the cursor, enter **2** for using Radius Authentication Server.

3. Configuring RADIUS Authentication Server

3.1 Select the external RADIUS authentication server, and the system prompts you to enter its hostname or IP address.

> RADIUS Server (Name/IP Address)
Quick ->

At the prompt, enter IP address **172.20.2.12**

3.2 To enter the RADIUS server secret, also called the shared secret, that allows access to the server.

> RADIUS Server Secret
Quick -> _

At the cursor, enter the RADIUS server secret; **02giac00k1ez**. The system only display asterisks.

3.3 The system prompts you to reenter the RADIUS server secret to verify it.
Verify -> _

At the cursor, reenter the RADIUS server secret, **02giac00k1ez**. The system only display asterisks.

3.4 The system prompts you to enter the UDP port number by which you access the RADIUS server.

> RADIUS Server Port
Quick -> [0] _

At the cursor, enter the RADIUS port number; for example, 1645. To have the system supply the default port number (1645), press **Enter** to accept 0 (the default).

Note that Cisco PIX firewall listens for Radius on ports 1645 and 1646, not 1812 and 1813 as assigned by IANA.

4. Configuring the IPSec Group

This section appears only if the IPSec tunneling protocol is enabled. The remote-access IPSec client connects to the VPN Concentrator via this group name and password. This is the IPSec group that creates the tunnel. Users then log in, and are authenticated, by means of their usernames and passwords.

To configure the IPSec group name and password, follow these steps:

4.1 The system prompts you to enter the IPSec group name.

> IPSec Group Name
Quick -> _

At the cursor, enter the name **giac_mobile** for the Mobile employee group. Maximum is 32 characters, case-sensitive

4.2 The system prompts you to enter the group password.

> IPSec Group Password
Quick -> _

At the cursor, enter a unique password for this group. The minimum is 4, and the maximum is 32 characters, case-sensitive. The system displays only asterisks.

4.3 The system prompts you to reenter the group password to verify it.

Verify -> _
At the cursor, reenter the group password. The system displays only asterisks.

Repeat the above procedure for the **partner** group.

5. Changing the Admin Password

The default admin password supplied with the VPN Concentrator is also **admin**. The password must be changed to improve device security, and it has to be at least eight characters long with a minimum of one numeric and one alphabetical character, as per GIAC Information Security Policy.

5.1 The system prompts you to change the admin password.

We strongly recommend that you change the password
> Reset Admin Password
Quick -> [*****] _

At the cursor, enter a new password for admin. Remember that entries are case sensitive.

5.2 The system prompts you to re-enter the password to verify it.

Verify -> _

At the cursor, reenter the new password. The system displays only asterisks. To keep the default, press **Enter**.

6. Lastly, Saving the Active Configuration

The system displays the final quick configuration menu.

1) Goto Main Configuration Menu
2) Save changes to Config file
3) Exit
Quick -> **2**

At the cursor, enter **2** to save the active configuration in the system config file.

The VPN Concentrator now has enough information to become operational.

2.4 Tutorial on Border Router Implementation

Connecting to the Console Port

Connect the serial port of a PC to the console port using an RJ45-toRJ45 roll-over cable with a DB9 adapter at the PC end.

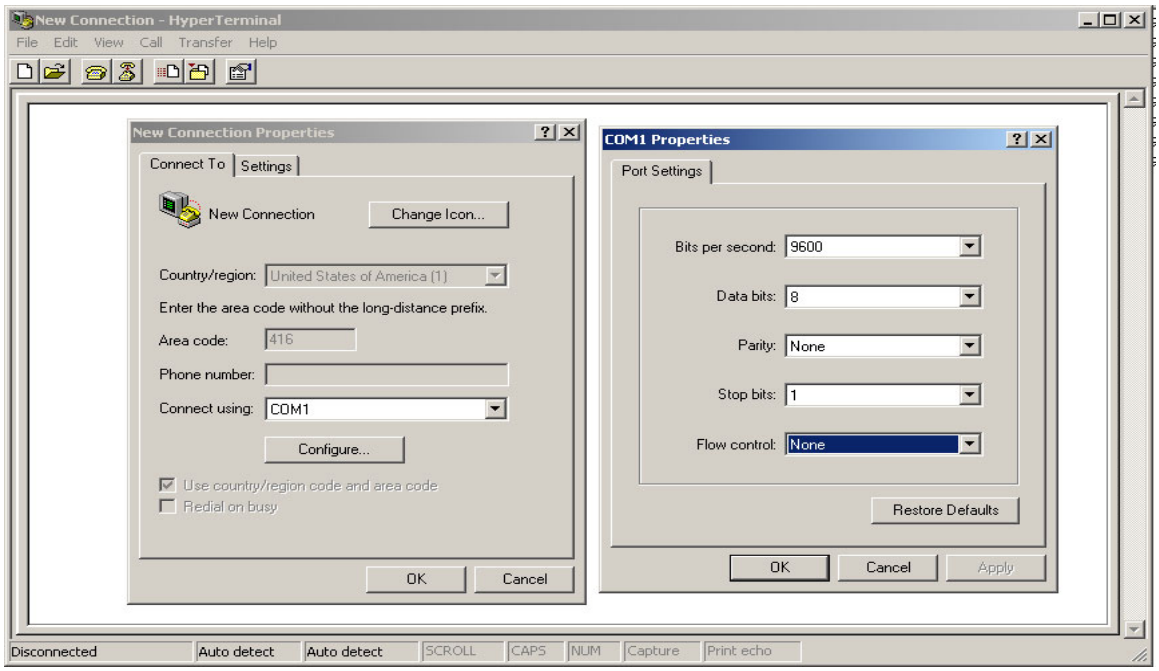
Pin-outs of the roll-over cable is:

Console Port	DB9	Signal	-	NC	NC	TXD	GND	GND	RXD	NC	NC
		Pins	-	1	2	3	4	5	6	7	8
PC COM Port	RJ45	Signal	RI	CTS	DSR	RXD	GND	GND	TXD	DTR	RTS
		Pins	9	8	7	6	5	4	3	2	1

> Tip: Even if it is possible to connect to the router through a telnet session, it is strongly recommended to have a direct connection to the router through the console port. The reason is that if something goes wrong during the configuration change or software upgrade, it might be necessary to be physically located next to the router to power-cycle it. Moreover, you will lose the telnet connection if the router needs a reboot.

Configuration of the PC HyperTerminal Parameters

If Microsoft Windows is the operating system, configure the HyperTerminal with parameters as shown below:



Tip: If there are garbage characters in the HyperTerminal session, this means that the HyperTerminal properties are not configured correctly, or the configuration register of the router is set to a non-standard value for which the console connection speed is higher than 9600 bps. Check the value of the configuration register by using telnet to access the router if possible and use the **show version** command (shown on the last line) to ensure it is set to 0x2102 or 0x102. It is necessary to reload the router to take this change into consideration. Once you are sure the console speed is set to 9600 bps on the router side, you should check that the HyperTerminal properties are set as indicated above. If there is no telnet access, then you may have to try changing the speed and/or the other parameters until there is proper display on screen.

Important Concepts of Access Control List

Inverse Mask

To be able to use ACL effectively, it is important to understand how masks are used with IP addresses in Cisco ACLs to specify the address space to be permitted or denied.

Normally the subnet mask is used to determine where the network number in an IP address ends and the node number in an IP address begins. Because of the way a subnet mask is used to filter an IP address, the bits in a subnet mask have to be set consecutively from left to right. For example a subnet mask of 255.0.0.0 is valid (255 is all eight bits set in the first octet). 255.128.0.0 is also valid (all eight bits set in the first octet, the MSB set in the second octet). 255.64.0.0 is not valid -the first bit (the MSB) in the second octet has been skipped.

Masks for IP ACLs are in the reverse order, and are therefore called inverse masks or wildcard masks. The inverse mask can be determined by subtracting the normal mask from 255.255.255.255. For example, the inverse mask for network address 192.73.235.0 with a normal mask of 255.255.255.0 can be calculated as:

255.255.255.255 – 255.255.255.0 (normal mask) = 0.0.0.255 (inverse mask)

Other examples:

Source InverseMask of 0.0.0.0 255.255.255.255 = any
Source InverseMask of 192.73.235.11 0.0.0.0 = host 192.73.235.11

Summarizing ACLs

Optimization can be achieved by summarizing a range of networks into a single network, if possible, so that it becomes a smaller list to process. For example, the following eight lines:

```
Access-list test permit ip 192.73.32.0 0.0.0.255
Access-list test permit ip 192.73.33.0 0.0.0.255
Access-list test permit ip 192.73.34.0 0.0.0.255
Access-list test permit ip 192.73.35.0 0.0.0.255
Access-list test permit ip 192.73.36.0 0.0.0.255
Access-list test permit ip 192.73.37.0 0.0.0.255
Access-list test permit ip 192.73.38.0 0.0.0.255
Access-list test permit ip 192.73.39.0 0.0.0.255
```

Can be summarized into a single statement:

```
Access-list test permit ip 192.73.32.0 0.0.7.255
```

Processing ACLs

Traffic entering the router is checked against ACL entries based on the order of the ACL entries. When new statements are added to an ACL, they are added to the end of the list. The router keeps checking until it finds a match. If no matches are found by the time the end of the list is reached, the traffic is denied by an implicitly implied deny all statement. To improve performance of an ACL, the frequently hit entries should be kept at the top of the list. An example below shows that performance can probably be improved by dropping the first 3 lines because the last line actually provides the similar (but looser) control as the first three combine:

```
access-list 101 permit tcp 192.73.235.1 host 192.168.1.1
access-list 101 permit tcp 192.73.235.2 host 192.168.1.1
access-list 101 permit udp 192.73.235.3 host 192.168.1.1
access-list 101 permit ip 192.73.235.0 0.0.0.255 192.168.1.1 0.0.0.0
```

Editing ACLs

As mentioned above, when new statements are added to an ACL, they are added to the end of the list. So be careful with new entries to make sure that all statements in an ACL are in the correct order. Also statements of opposite effect do not cancel each other because of the order of processing. In the following example, all ip traffic will be dropped and the second statement will never be processed:

```
access-list 101 deny ip any any
access-list 101 permit ip any any
```

If there is a need to remove an ACL, use "no" to remove it. For example:

```
No access-list 101 deny ip any any
```

When modifying ACLs, it helps to copy the existing ACL to a notepad, edit with new entries and put all entries in the right order, and then cut and paste into the "config terminal" session after the old ACL is removed.

Defining Ports and Message Types

The question mark "?" can be used to displayed a text description of some well-known ports. For example:

```
Access-list 101 permit tcp host 192.73.235.1 host 192.168.1.1 eq ?
<0-65535>        Port number
bgp              Border Gateway Protocol (179)
chargen          Character generator (19)
cmd              Remote commands (rcmd, 514)
dattime          Daytime (13)
…….
```

Defining In, Out, Source, Destination

These terms are always used as reference by the router. "Out" means that traffic has already been through the router and is leaving the interface to which the ACL is applied. The Source is where it is coming from (on the other side of the router), and the destination is where it is going. "In" is the other way around.

Types of ACLs[43]

There are several types of ACLs with different syntax providing different functions, including:

Standard IP ACLs - number 1 to 99

Standard IP ACLs use source addresses for matching operations.

access-list access-list-number **{permit|deny}** {host|source source-wildcard|**any}**

Extended IP ACLs – number 100 to 199

Extended IP ACLs use source and destination addresses for matching operations and optional protocol type and port numbers for finer granularity of control.

IP

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]]{deny | permit} *protocol source source-wildcard destination destination-wildcard* [precedence *precedence*] [tos *tos*] [log | log-input] [time-range *time-range-name*]

ICMP

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {deny | permit} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* | [[*icmp-type icmp-code*] | [*icmp-message*]] [**precedence***precedence*] [**tos** *tos*] [log | log-input] [time-range *time-range-name*]

TCP

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {deny | permit} **tcp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established**][**precedence** precedence] [**tos** tos] [log | log-input] [time-range *time-range-name*]

UDP

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** minutes]] {deny | permit} **udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** precedence] [**tos** tos] [log | log-input] [time-range *time-range-name*]

Name ACLs

Named ACLs use source addresses for matching operations.
ip access-list {extended|standard} *name*
{**deny** | **permit**} *protocol* {*source source-wildcard* | **host** *source* | **any**} [*operator port*]
{*destination destination-wildcard* | **host** *destination* | **any**} [*operator port*]

Reflexive ACLs

Reflexive ACLs allow IP packets to be filtered based on upper-layer session information. They are generally used to allow outbound traffic and to limit inbound traffic in response to sessions originating inside the router. Reflexive ACLs can be defined only with extended named IP ACLs. They cannot be defined with numbered or standard named IP ACLs, or with other protocol ACLs. Reflexive ACLs can be used in conjunction with other standard and static extended ACLs.

The following is the syntax for various reflexive ACL commands.
interface
ip access-group {*number*|*name*} {in|out}
ip access-list extended *name*
permit *protocol* any any reflect *name* [timeout*seconds*]
ip access-list extended *name*
evaluate *name*

Lock-and-Key ACL[44]

Lock-and-key access allows an external event to place an opening in the firewall. After this opening exists, the router is susceptible to source address spoofing. To prevent this, you need to provide encryption support using IP encryption with authentication or encryption.

Spoofing is a problem with all existing access lists. Lock-and-key access does not address this problem.

Configuring the Router

Once the above concepts on ACLs are understood, router policy implementation becomes easy.

The router can be configured using one of the following procedures:

- Using Configuration Mode—Recommended for those who are familiar with Cisco IOS commands.
- Using AutoInstall—Recommended for automatic installation if another router running Cisco IOS is installed on the network. This configuration method requires knowledge of an advanced Cisco IOS user.
- Using the Setup Facility—Recommended if you are not familiar with Cisco IOS commands. The Setup Facility will bring up the System Configuration Dialog that makes basic configuration more user friendly. However, it may not be intelligent enough for more advance configuration requirements.

With the level of expertise the GIAC Security Team has on Cisco products, Configuration mode will be used for configuring the border router.

Tips in using Configuration Mode

- Most of the commands take effect as soon as they are entered. So be careful with what you type in, especially when working with a device in production network.
- Check the syntax before entering a command. Enter a command and press the <Enter> key to view a quick summary, or precede a command with *help*, as in, *help ip*
- Abbreviate commands. For example, you can use the *config t* command to start configuration mode, the *write t* command statement to list the configuration, and *write m* to write to flash memory. Also, in most commands, *show* can be abbreviated as *sh*. This feature is called command completion.
- After changing or removing the *alias, access-list, conduit, global, nat, outbound*, and *static* commands, use the *clear xlate* command to make the IP addresses available for access.
- Review possible port and protocol numbers at the IANA websites[45].
- Create your configuration in a text editor and then cut and paste it into the configuration. Cisco devices including routers and PIX Firewalls lets you paste in a line at a time or the whole configuration. Always check your configuration after pasting large blocks of text to be sure everything copied.

Since this tutorial is on how to implement the access control policy on the Border Router as outline in Assignment 2, an assumption is make here that the router has already been upgraded to the correct version of IOS software (otherwise a tftp copy is required for software download) and there is no configuration file in NVRAM.

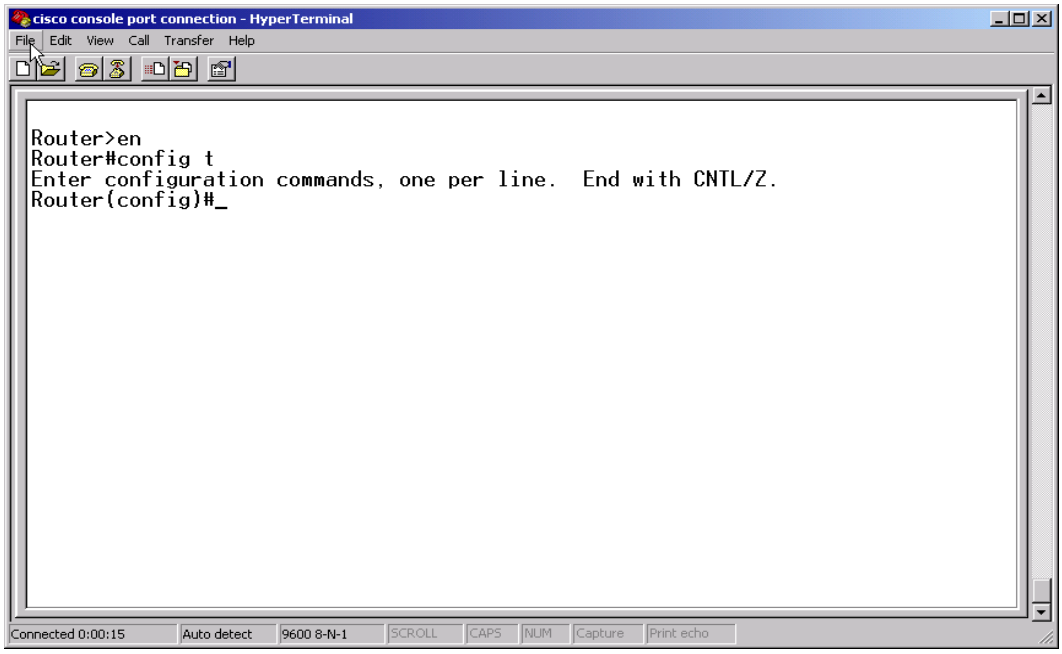
Largely based on the router policy outlined in Assignment 2, we will first put together the following configuration file with a text editor, and then saved it as giac-br.txt:

```
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
!
hostname giac-br1
!
service password-encryption
enable secret <secret-password>
no enable password
!
logging 172.20.2.11
logging facilities syslog
logging buffered 16384 informational
logging trap informational
no logging console
!
no service tcp-small-servers
no service udp-small servers
!
no ip source-route
no service pad
no service finger
no ip http server
no ip bootp server
no ip domain-lookup
no cdp run
!
ip tcp intercept list 120
ip tcp intercept connection-timeout 60
ip tcp intercept watch-timeout 10
ip tcp intercept one-minute low 1500
ip tcp intercept one-minute high 6000
!
interface serial 0
ip address 196.196.196.242 255.255.255.252
no cdp enable
no ip directed-broadcast
no ip redirects
no ip unreachales
no ip proxy-arp
no ip mroute-cache
```

```
ip access-group 110 in
ip access-group 111 out
!
interface ethernet 0
ip address 192.73.235.242 255.255.255.248
no cdp enable
no ip directed-broadcast
no ip redirects
no ip unreachales
no ip proxy-arp
no ip mroute-cache
!
access-lsit 10 permit 172.20.2.11
access-list 10 deny any any log
!
access-list 101 permit tcp any 192.73.235.0 0.0.0.128
!
access-list 110 deny ip host 196.196.196.242 host 196.196.196.242 log
access-list 110 deny ip host 192.73.235.242 host 192.73.235.242 log
access-list 110 deny ip 192.73.235.0 0.0.0.255 any log
access-list 110 deny ip 127.0.0.1 0.255.255.255 any log
access-list 110 deny ip 10.0.0.0 0.255.255.255 any log
access-list 110 deny ip 172.16.0.0 0.15.255.255 any log
access-list 110 deny ip 192.168.0.0 0.0.255.255 any log
access-list 110 deny ip 224.0.0.0 15.255.255.255 any log
access-list 110 deny ip 240.0.0.0 15.255.255.255 any log
access-list 110 deny tcp any any eq telnet log
access-list 110 deny udp any any eq tftp log
access-list 110 deny tcp any any eq 111 log
access-list 110 deny udp any any eq 111 log
access-list 110 deny tcp any any range 135 139 log
access-list 110 deny udp any any range 135 139 log
access-list 110 deny tcp any any eq 445 log
access-list 110 deny udp any any eq 445 log
access-list 110 deny udp any any range 161 162 log
access-list 110 deny tcp any any range 6000 6063 log
access-list 110 deny udp any any range 6000 6063 log
access-list 110 permit ip any 192.73.235.0 0.0.0.255
!
access-list 111 deny icmp any any 3 0
access-list 111 deny icmp any any 3 1
access-list 111 deny icmp any any 3 2
access-list 111 deny icmp any any 3 3
access-list 111 deny icmp any any 3 4
access-list 111 deny icmp any any 3 13
access-list 111 deny icmp any any 4
access-list 111 deny icmp any any 11 0
access-list 111 deny icmp any any 18
access-list 111 permit ip 192.73.235.0 0.0.0.255 any
!
ip route 0.0.0.0 0.0.0.0 196.196.196.241
```

```
ip route 192.73.235.0 0.0.0.128 192.73.235.241
ip route 192.73.235.224 0.0.0.8 192.73.235.241
!
snmp-server community <hard-to-guess-password> RO 10
!
banner motd c
+---------------------------------------------------------------------------------------------+
|                          WARNING                                                            |
|                          --------------                                                     |
| The programs and data stored on this system are licensed to and/or are |
| private property of this company and are lawfully available only to          |
| authorized users for approved purposes.  Unauthorized access to any    |
| program or data on this system is not permitted, and any unauthorized   |
| access beyond this point may lead to prosecution. This system may be   |
| monitored at any time for operational reasons, therefore, if you are         |
| not an authorized user,                                                                     |
|                    DO NOT ATTEMPT TO LOG IN.                                                |
+---------------------------------------------------------------------------------------------+|
c
!
line aux 0
transport input none
line vty 0 4
transport input none
!
ntp server 65.211.109.1
ntp server 192.73.48.6
```

Now upon router bootup and entering into the privileged mode as shown in the diagram below, we can copy and paste the content of the configuration file into the console.



After the configuration file is uploaded, type <exit> or ctrl-z to get out of the config mode, followed by a “write mem” command to copy the running configuration into the startup configuration in the NVRAM.

Now the security policy is implemented on the border router.

Assignment 3 Verify the Firewall Policy

Now that the new secure perimeter network is in place, a technical audit of the primary firewall is necessary to verify the firewall policy is correctly implemented as described in Assignment 2. Upon the completion and analysis of the firewall audit, recommendations for improvements or alternate architectures will be made.

3.1 Plan the Audit

Approach and Budget

The audit will use an "audit-in-depth" approach, meaning that it will be auditing the firewall weakness from different angles using different tool sets. Physical security measures protecting the firewall will also be part of the audit process.

The following table outlines the tasks needed for the audit with estimated man-hours for each task:

Task	Estimated Man-Hours Required
Documentation review and network preparation.	2
Review physical security of firewall.	1
Search for corporate information and firewall hardware and software vulnerabilities from the Internet.	3
Identify and collect/install tools required for firewall audit.	4
Vulnerability Scanning, finger printing, DoS attack and penetration tests against firewall from outside.	8
Check effectiveness of firewall rules by port Scanning from different subnets against hosts protected by firewall.	10
Document findings and generate report.	8
Total Number of Hours	**36**

Preparation works such as reviewing requirements and implementation documentation requires the skill sets of an intermediate security analyst while the actual scanning and attacks as well as the interpretation of the test results requires the expertise of a senior security consultant.

Using $150 per hour as the average unit cost, labor charge for the firewall audit is estimated at $5,400, excluding the cost of tools, if any.

Risk, Timing and other Considerations

Once senior management approves the audit plan and budget, the security team will be responsible for the execution of all the tasks plus communications with other IT staff as well as internal and external users.

One of the major risks when auditing a firewall is the potential negative impact on production business traffic, either in the form of performance degradation or complete network/service outage. This is especially the case for GIAC where, due to the lack of lab facility, the production network will be tested. The firewall with the current design is a single point of failure because redundancy has not been factored in due to budget constraint. For this reason, the period of 18 hours of audit with penetration tests and attacks is scheduled for the next long weekend, starting at 6 am on Saturday and finishing by midnight. As business is expected to be slow over the long weekend, the plan leaves two days for recovery before the next business day if some serious problems ever happen as a result of the audit. During the tests period, network and CPU performance of all nodes impacted will be closely monitored, and utilization thresholds are set at 75% at which point all audit tests have to be slowed down or stopped.

The 10 hours of preparation works including documentation review, vulnerability research and tools installation will be completed before Friday. All systems including the firewall itself will have full tape backup performed between the end of business day on Friday and 6 am on Saturday. This will allow application and data recovery to the end of last business day if necessary. And the report with recommendations will be available 2 business days after the tests are performed.

Server administrators and other support staff are informed of the firewall audit and are required to confirm, either on site or by remote access via VPN, by Sunday at noon on the health and security status of the servers and applications. They are also put on pager standby during the scanning test period so that they can be reached in case any server goes down due to test activities. Partners, the other group of VPN users, have been informed of the maintenance windows on Saturday and thus the VPN Concentrator downtime. Suppliers and customers are not notified because of the small chance of outage and their traffic is expected to be light anyway. GIAC does not deal with consumers at retail level, all customers are companies or individuals that purchase bulk on-line fortunes and business is usually much slower in the weekends. However, contingency plan has been made to have one of the Partners to send notification by Email on behalf of GIAC to all Suppliers and Customers if the outage is longer than 4 hours.

GIAC's ISP will also be informed of the test schedule so that they will not be alarmed with abnormal traffic pattern if detected, even though it is very unlikely because it is not expected to have any scanning test traffic going outbound pass the border router to the Internet.

Another risk coming with the firewall audit is the possibility of not able to detect any real hacking or attack activities over the same period of time. This risk is addressed by closely monitoring the firewall and system logs as well as the IDSs as the audit is taking place.

Confidential data, if obtained inadvertently by the security team during the audit, will be removed and destroyed from all raw data files and they will not appear on any report generated, as required by company information security policy.

Detailed Audit Plan

The first part of the audit is to review the policy and configuration documentation and make sure that all the firewall rules make business and security sense, and there is no syntax or typographical errors in implementation. The firewall policy is further evaluated using reference resources including the SANS top 20[46] vulnerabilities and the Federal Agency Security Practices[47]. Internet sites including ICAT (http://icat.nist.gov/icat.cfm), CVE (http://www.cve.mitre.org/), SecurityFocus (www.securityfocus.org), and Security Advisory notes on the Cisco site are checked for know vulnerabilities. Patches and upgrades, if available, are downloaded an implemented.

Second part of the audit plan is to identify firewall vulnerabilities visible from the external side of the firewall. The public servers on the External Service Network are most likely the potential targets for attacks in the real world, as various lookup services and tools can easily identify their public IP addresses. In order to save time, only public addresses actually in use will be scanned instead of scanning the whole class C network address space, as hackers in real life may do during their reconnaissance phase.

The third part of the audit plan is to port scan the firewall interfaces and the servers to confirm that ports are open only as intended in our policies but nothing else. Since the focus of this audit is on the firewall itself, scanning will only be done against the firewall or networks on the other sides of the firewall. Servers on the local network as the scanning workstation will not be scanned in the audit plan.

Last but not the least, server and firewall logs are examined thoroughly, not only to confirm the tests results but also to ensure that there is no other interesting activities or real attacks happened during our audit period of time.

Scanning Audit Tools

Two scanning tools will be used in our firewall policy audit. The first one, a tool that GIAC security team already has in possession, is CyberCop Scanner v5.5, a commercial vulnerability scanner from Network Associates. The second tool is Nmapwin v1.3.0[48], an open source port scanning utility for network exploration and security audit.

Vulnerability Scanning: CyberCop Scanner v5.5NT (signatures updated to version 5.5-200209)

CyberCop Scanner is a network security assessment tool that can scan devices on networks for more than 700 known vulnerabilities. It can be configured to search for the vulnerabilities that may become security concerns in accordance with security policy. It can identifies security holes to prevent intruders from accessing mission-critical data, unveils weaknesses, validates policies and enforces corporate security strategies. It tests NT and UNIX workstations, servers, hubs and switches and performs thorough perimeter audits of firewalls and routers.

Even though Network Associates recently announced[49] that CyberCop Scanner was reaching the end of life by July 1, 2002, maintenance for the scanner will continue until the end of 2004 with scheduled signature updates performed quarterly.

Port Scanning: Nmap and Nmapwin

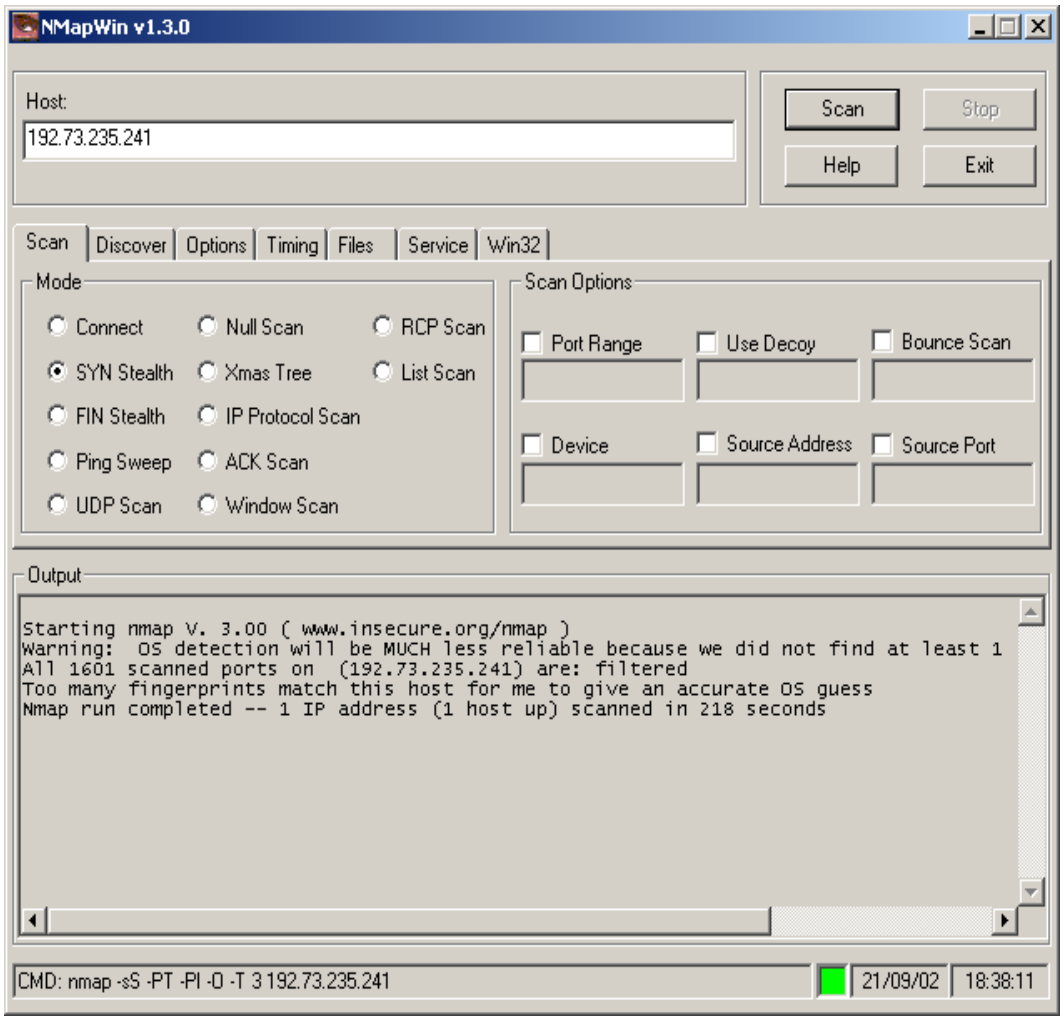
Port scanning is the process whereby every port on a machine is checked to see if anything responds. It is the equivalent of a burglar checking all the doors and windows on a home to see if they open. This is an activity that can be done at an extremely slow pace, making it almost impossible to spot, or an activity that leaves extremely tell tale signs in log files.

Viewing activity of a port scan is usually a pre-cursor to an attack. While it is not impossible for systems to be scanned by accident or by a rogue service, it is extremely difficult to attack a system without scanning it first. The less ports that are open, the less potential holes an attacker could use. The port scanner of choice for this audit is Nmap.

Nmap is an open source utility for network exploration or security auditing. It is designed to rapidly scan large networks, as well as individual hosts. Nmap uses raw IP packets to determine what hosts are available on the network, what services (ports) they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are

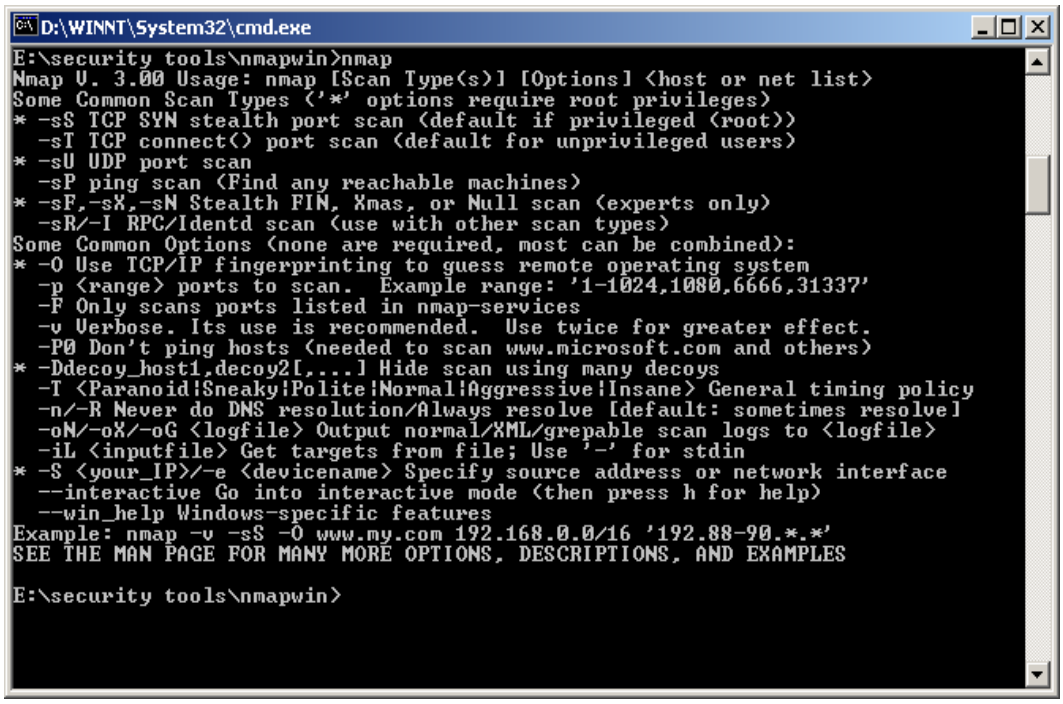
in use, and dozens of other characteristics. Nmap is free software, available with full source code under the terms of the GNU GPL.

Nmapwin is a native Win32 front-end created based on Nmap v2.54beta36 by Jens Vogt, based on the work done by Ryan Permeh (from eEye) and Andy Lutomirski. Main benefit of Nmapwin is the user-friendly interface, as shown below:



Note that at the bottom of the screen, the command line is also displayed showing all the options selected for the scanning session.

Nmap can also be executed in DOS mode, where scripts can be run. The following shows the options available, and more detailed documentation is available from insecure.org[50]:



In order to avoid overloading the production network, timing parameter should be set to 2 for the "polite" mode. Lower value of the timing parameter will also increase the time required to complete the scanning.

For devices that don't response to icmp query, such as the firewall interface or web servers, the –P0 option should be used so Nmap will start the scanning process without waiting for a positive response to ping.

3.2 Conduct the Audit

Documentation Review

Documentation on business requirements for connections and restrictions as outlined in Assignment 1 is fully reviewed and confirmed as matching up-to-date requirements. The design and implementation guidelines described in Assignment 2 are also reviewed. IP addresses of all firewall interfaces and servers are confirmed and recorded.

Switch ports on the four subnets directly connecting to the firewall are made available so scanners and testers can be connected. Ports are also available on the service networks and user networks so that network analyzer and monitor can be used to capture penetrating traffic. All tests devices will have static IP addresses assigned.

Physical Security of Firewall

Firewall together with all other security components of the perimeter network are in a secure room, access to which is properly controlled, logged and monitored. No shared medium hub is used in the entire network. Port security on switches is enabled allowing only nodes with authorized MAC addresses to connect. Use of mirror (or SPAN) ports is tightly controlled.

Information Collection on GIAC (Note: All information below is fictitious)

A Whois search at the InterNic.org[51] for giac.com provides the following information:

> Whois Search Results
>
> Whois Server Version 1.3
>
> Domain names in the .com, .net, and .org domains can now be registered
> with many different competing registrars. Go to http://www.internic.net
> for detailed information.
>
> Domain Name: GIAC.COM
> Registrar: NETWORK SOLUTIONS, INC.
> Whois Server: whois.networksolutions.com
> Referral URL: http://www.networksolutions.com
> Name Server: NS1.GIAC-ISP.ORG
> Name Server: NS2.GIAC-ISP.ORG
> Updated Date: 23-jun-2002
>
> >>> Last update of whois database: Sat, 21 Sep 2002 16:50:15 EDT <<<

Another whois lookup for giac.com at Network Solutions[52] provides further information on corporate address and administrative contact that may be used for social engineering purpose:

> WHOIS Search Results
> Registrant:
> GIAC Fortune Cookie Enterprise
> 99 Enterprise Road, 8th Floor
> New York, New York
> USA
>
> Domain Name: GIAC.COM
>
> Administrative Contact, Technical Contact:
> William Chan (WC12345) William.chan@giac.com
> GIAC Fortune Cookie Enterprise
> 99 Enterprise Road, 9th Floor
> New York, New York
> USA

212-345-6789

Record expires on 01-Dec-2005.
Record created on 02-Dec-1993.
Database last updated on 21-Sep-2002 22:08:33 EDT.

Domain servers in listed order:

NS1.GIAC-ISP.COM	196.196.196.250
NS2.GIAC-ISP.COM	196.196.196.251

The public address of GIAC's web server can be identified with the use of nslookup:

```
D:\>nslookup
Default Server:  ns.uu.net
Address:  137.39.1.3

> www.giac.com
Server:  NS1.GIAC-ISP.COM
Address:  198.6.1.81

Non-authoritative answer:
Name:    www.giac.com
Address:  192.73.235.11
```

Once the public address of the web server is known, the network address registration information can be lookup from ARIN Whois[53]:

```
Search results for: 192.73.235.0

OrgName:    GIAC Fortune Cookie Enterprise
OrgID:      GIAC

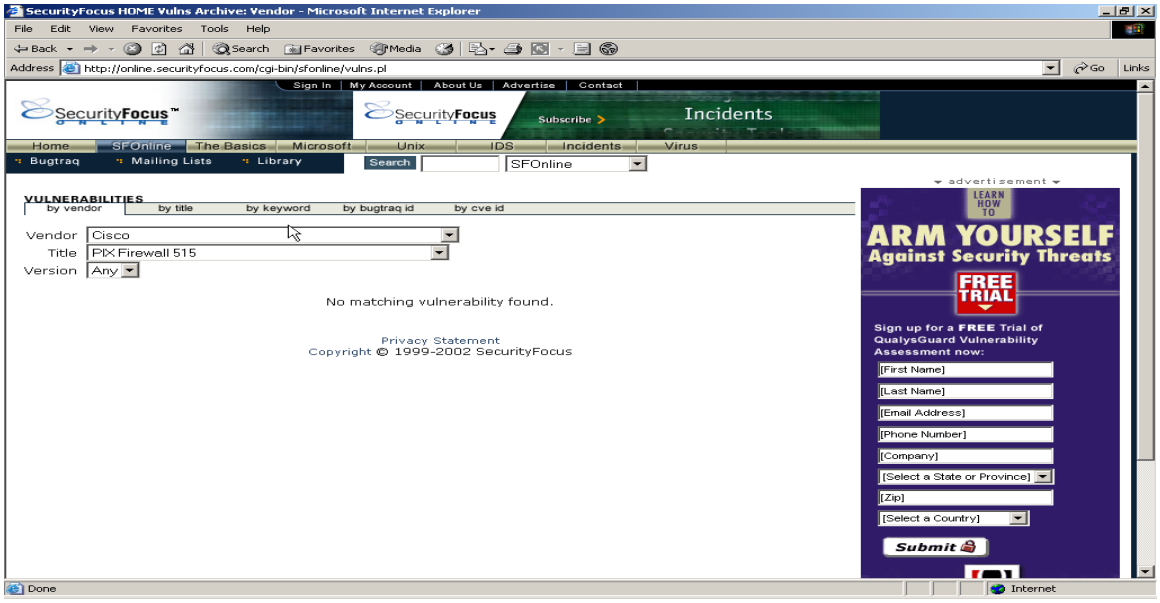
NetRange:   192.73.235.0-192.73.235.255
CIDR:       192.73.235.0/24
NetName:    GIAC
NetHandle:  NET-192-73-235-0-1
Parent:     NET-192-0-0-0-0
NetType:    Direct Assignment
Comment:
RegDate:    1990-08-05
Updated:    2002-01-03

TechHandle: WC12345-ARIN
TechName:   Chan, William
TechPhone:  +1-212-345-6789
TechEmail:  William.chan@giac.com

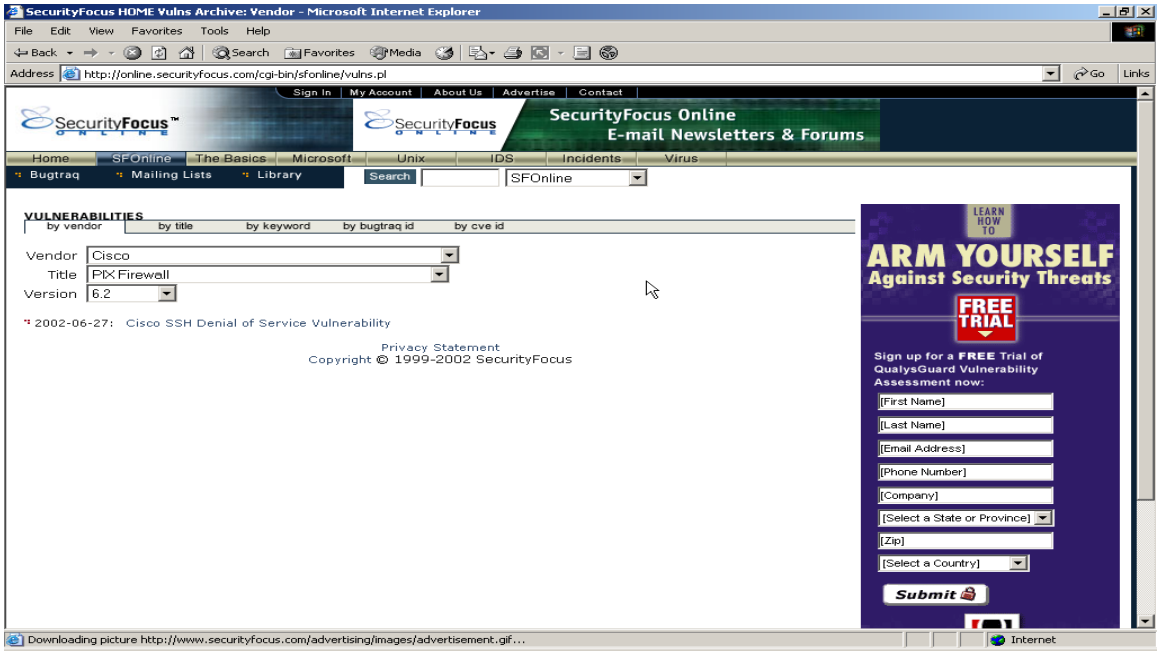
# ARIN Whois database, last updated 2002-09-21 19:05
```

Firewall Vulnerabilities

Hardware and software vulnerabilities can be searched from different sources such as the Bugtraq Information Database from SecurityFocus[54], which shows that there is no known vulnerability as of September 20, 2002 on Cisco PIX Firewall 515:



However, there is one vulnerability is reported on Cisco PIX Firewall software v6.2:



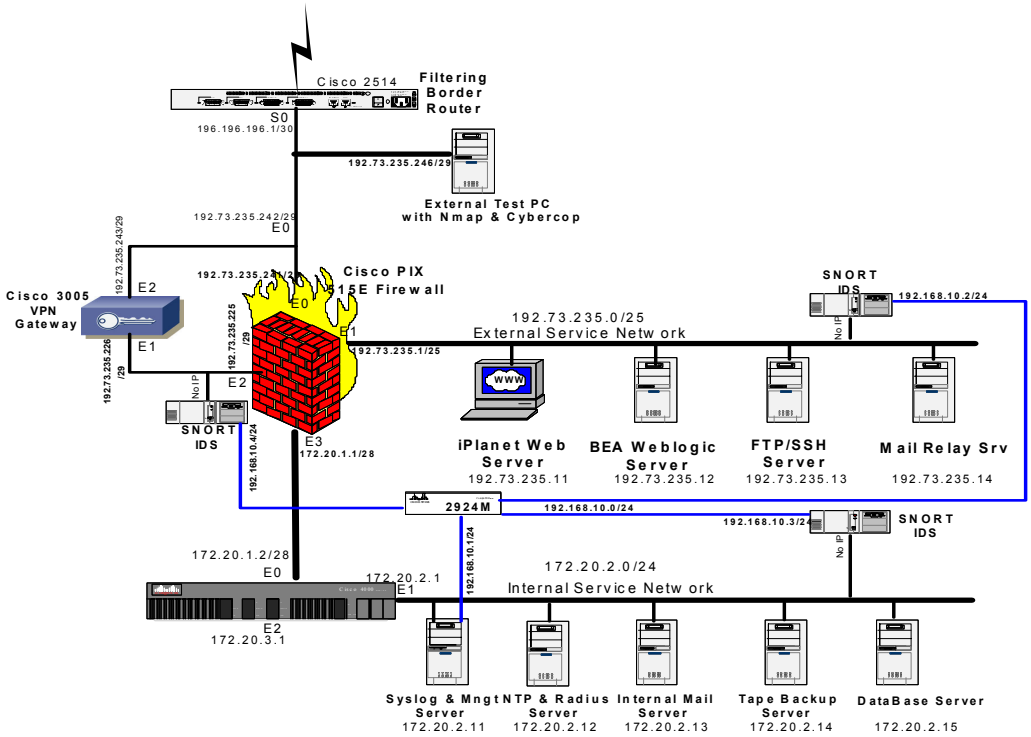
The Cisco SSH Denial of Service Vulnerability, identified as cve[55] CAN-2002-1024[56], will result in a denial of service if there are repeated and concurrent attacks with scanning for SSH vulnerabilities, which will cause excessive CPU consumption. The condition is due to a failure of the Cisco SSH implementation to properly process large SSH packets.

Following the recommendation from Cisco[57], the PIX Firewall software is upgraded to release 6.2(1) in order to address this vulnerability.

Vulnerability Scanning Tests from Outside of Firewall

The purpose of these tests is to simulate the reconnaissance and penetration attempts from a hacker from the Internet, and to confirm the effectiveness of the policies on the primary firewall as seen from outside. Cybercop Scanner v5.5 will be used for this test.

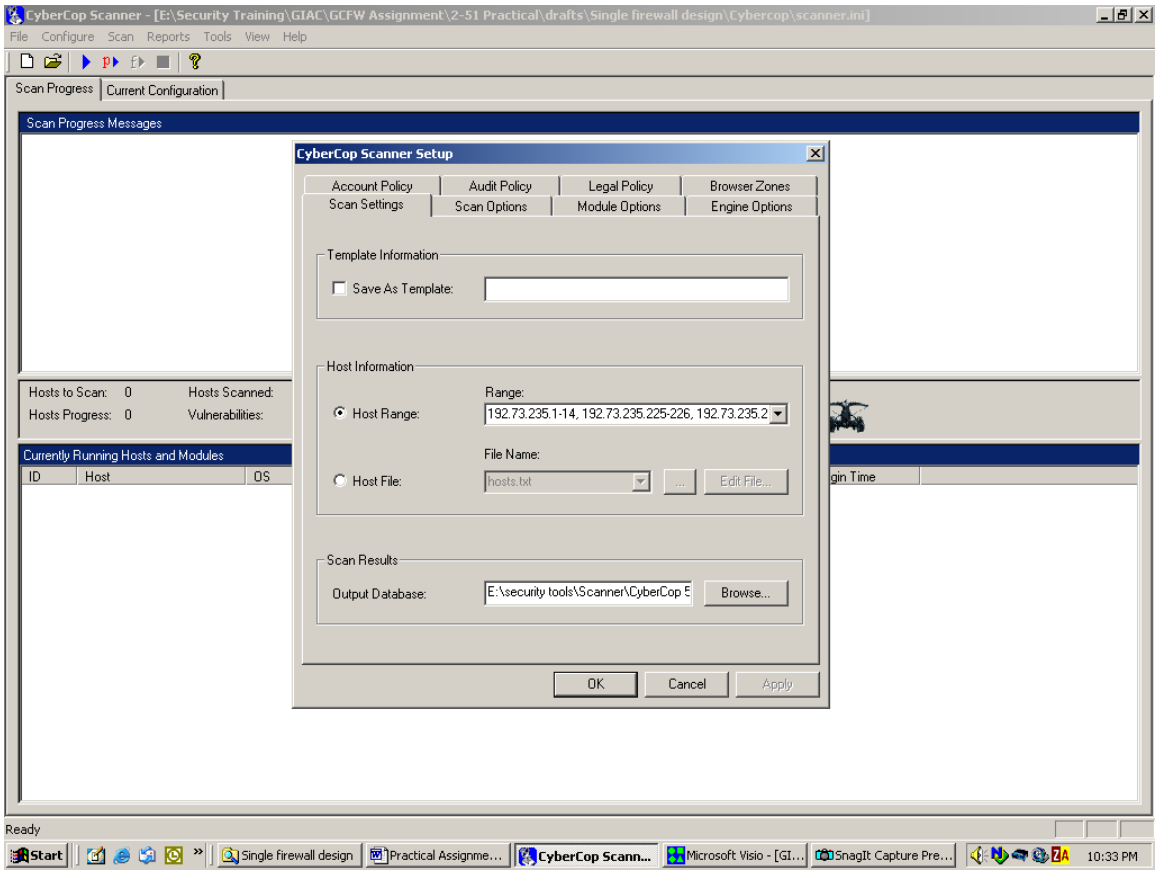
A workstation with Nmapwin and Cybercop installed is connected to the "fwoutside" subnet using an IP address of 192.73.235.246/29. Default gateway is set to 192.73.235.241, the address of the interface E 0 on the PIX Firewall.



On configuring CyberCop, the following Scan Settings are used or enabled:

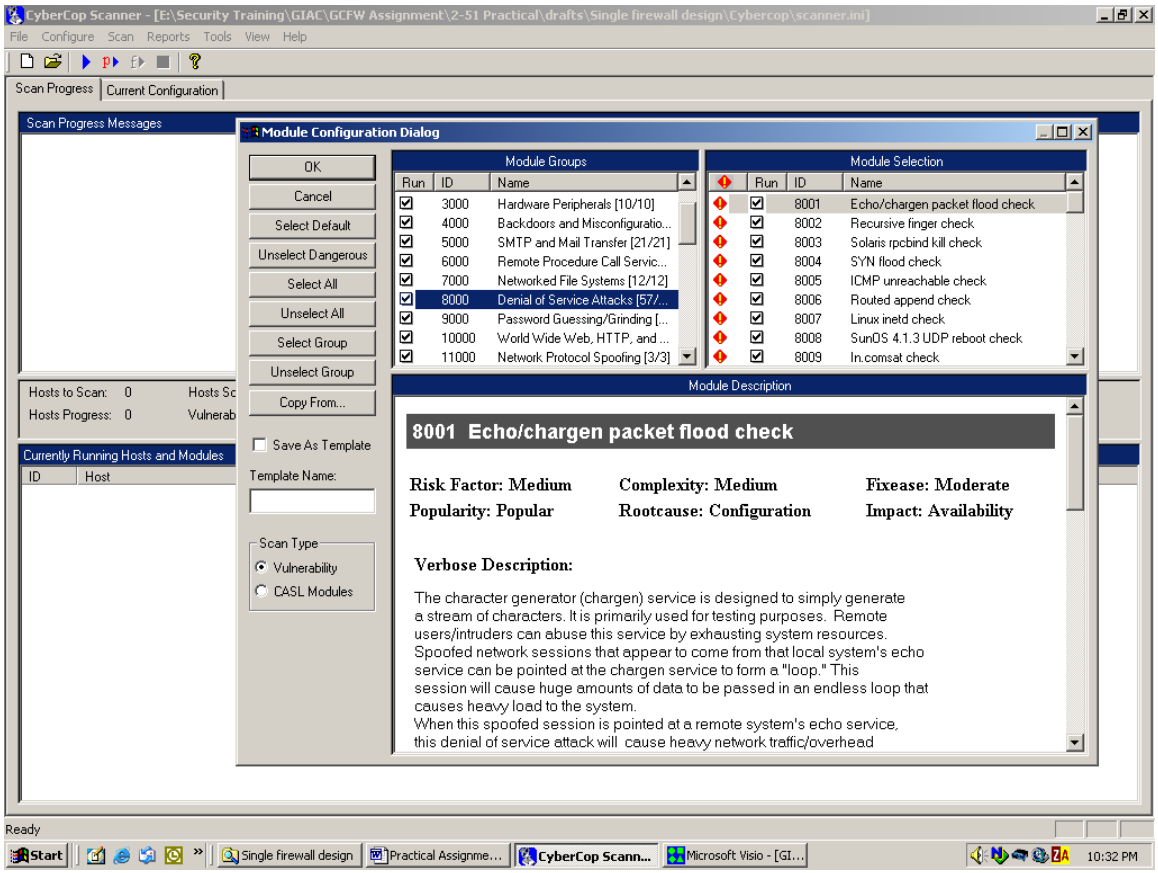
Host Range:	192.73.235.1-14, 192.73.235.225-226, 192.73.235.241-243,
Scan Options	Enable Operating System Identification
	Allow modules to be disabled based on detecting OS
Host Query	Hostname Lookup
	Scan Unresponsive Hosts

Below is a screen capture of the Host Range setup:



On Module Settings, all modules are selected including the dangerous ones such as Denial of Service Attacks because the audit team is interested to find out how robust the systems are. With security, server and application support staff all on

standby and the network load being closely monitored, downtime, if any, will be kept to a minimum.



At the end of the vulnerability scanning, reports can be generated based on a number of different criteria, including by complexity, ease of fix, host, impact, popularity risk factor, and others.

Port Scanning Tests with Nmap:

The Nmap scanner will run scripts from a scanning workstation on each of the four networks directly connected to the firewall to scan against the firewall itself and all the networks on the other sides of the firewall. The default (for privileged users) SYN scan will be used because it is one of the more frequently used scan type by hackers. The primary advantage to this scanning technique is that fewer sites will log it.

Other options used in the script settings include:

-P0 Do not try and ping hosts at all before scanning them. This allows the scanning of networks that don't allow ICMP echo requests (or responses) through their firewall.

-n don’t do reverse DNS resolution on the active IP addresses it finds. Since DNS is often slow, this can help speed things up.

-O This option activates remote host identification via TCP/IP fingerprinting. In other words, it uses a bunch of techniques to detect subtleties in the underlying operating system network stack of the computers you are scanning. It uses this information to create a ´fingerprint´, which it compares with its database of known OS fingerprints (the nmap-os-fingerprints file) to decide what type of system you are scanning.

-r Do not randomize the order in which ports are scanned.

-T n This option identifies the timing policies by defining scanning modes to Nmap. Paranoid mode (T 1) scans very slowly in the hopes of avoiding detection by IDS systems. It serializes all scans (no parallel scanning) and generally waits at least 5 minutes between sending packets. Sneaky is similar, except it only waits 15 seconds between sending packets. Polite (T2) is meant to ease load on the network and reduce the chances of crashing machines. It serializes the probes and waits at least 0.4 seconds between them. Normal (T 3) is the default Nmap behavior, which tries to run as quickly as possible without overloading the network or missing hosts/ports. Aggressive mode (T 4) adds a 5-minute timeout per host and it never waits more than 1.25 seconds for probe responses. Insane (T 5) is only suitable for very fast networks or where you don't mind losing some information. It times out hosts in 75 seconds and only waits 0.3 seconds for individual probes. It does allow for very quick network sweeps though. Here the Polite mode is used because we are trying to avoid overloading the firewall in production network.

-S <ip address> is used to define the source address of the scanner. Note that in the scripts used for this audit, the use of source address is just to point out the right IP address of the scanning station used for each test, but not to hide the real source address, as it may be the case in real life attacks.

-oN <logfilename> is used to identify the path and the file name of the log file.

-p <port range> is used to specify the port range to scan. The default is to scan all ports between 1 and 1024 plus any ports listed in the services file that comes with nmap. In the scripts prepared for this audit, we will also include udp port range 1 to 1024 to identify ports open for services such

as snmp, dns and tftp and netbios; the higher tcp port ranges used for Netbackup are also included:

-p U:1-1024,T:1-1024,4800-4899,13720-13721,13782-13783

Below are the scripts used to scan from each of the four firewall-connected networks:

Nmap Script used from PIXOutside Network:

Nmap -sS -P0 -n -O -r -T 2 -p U:1-1024,T:1-1024,4800-4899,13720-13721,13782-13783 -S 192.73.235.244 -oN pixoutside.log 192.73.235.11-14, 192.73.235.225-226, 172.20.1.1-2, 172.20.2.11-15

Nmap Script used from PIXExtService Network:

Nmap -sS -P0 -n -O -r -T 2 -p U:1-1024,T:1-1024,4800-4899,13720-13721,13782-13783 -S 192.73.235.21 -oN pixextservice.log 192.73.235.241-243, 192.73.235.225-226, 172.20.1.1-2, 172.20.2.11-15

Nmap Scripts used from PIXVPN Network:

Nmap -sS -P0 -n -O -r -T 2 -p U:1-1024,T:1-1024,4800-4899,13720-13721,13782-13783 -e eth0 -S 192.73.235.228 –oN pixvpn1.log 192.73.235.241-243, 192.73.235.11-14, 172.20.1.1-2, 172.20.2.11-15

Nmap -sS -P0 -n -O -r -T 2 -p U:1-1024,T:1-1024,4800-4899,13720-13721,13782-13783 -S 172.20.129.5 -oN pixvpn2.log 192.73.235.241-243, 192.73.235.11-14, 172.20.1.1-2, 172.20.2.11-15

Nmap -sS -P0 -n -O -r -T 2 -p U:1-1024,T:1-1024,4800-4899,13720-13721,13782-13783 -S 172.20.130.5 -oN pixvpn3.log 192.73.235.241-243, 192.73.235.11-14, 172.20.1.1-2, 172.20.2.11-15

Nmap Script used from PIXInside Network:

Nmap -sS -P0 -n -O -r -T 2 -p U:1-1024,T:1-1024,4800-4899,13720-13721,13782-13783 -S 172.20.2.5 -oN pixinside.log 192.73.235.241-243, 192.73.235.225-226, 192.73.235.11-14

Note: The source addresses in the above scripts represent node address of the scanner on the public addressed VPN network, the NAT subnet for Partners VPN and the NAT subnet for the Mobile Users VPN, respectively.

3.3 Evaluate the Audit

Findings:

1. There is no issue on physical security on the PIX firewall.
2. PIX Firewall software is upgraded from 6.2 to 6.2(1) upon Cisco's recommendation to address the Cisco SSH Denial of Service Vulnerability.
3. There is no vulnerability on the PIX Firewall identified by CyberCop Scanner. There are, however, some issues identified on the servers including the need to patch the software on the iPlanet web server. Warning banners, either missing or not worded properly, on some of the servers are also identified as issues that need to be addressed.
4. Results from Nmap port scanning confirm that the firewall rules are behaving as designed.
5. There are no interesting or abnormal activities in the firewall log over the test period of time.

Recommendations:

1. Priority should be given to address the issue of Single-Point-of-Failure. This will prevent loss of business due to component failure or Denial of Service attacks. Financial impact upon service outage should be reviewed to justify the extra cost in security infrastructure.
2. Consider the use of a second firewall to provide an extra layer of protection as required by the defense-in-depth principle.
3. Security can be further improved by using a proxy server in the External Service Network. A proxy server acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service.
4. Consider using a certificate-based authentication for VPN connections instead of using pre-shared password to tighten the security process. There is also a need to investigate the use of site-to-site VPN connections as the number of staff on Partners' networks grows.
5. When the border router(s) get replaced with more up-to-date hardware, consider purchasing the IOS with firewall feature set so that it can further protect the perimeter network in general, and the VPN gateway(s) in particular.

The following diagram shows an enhanced design based on the above recommendations:

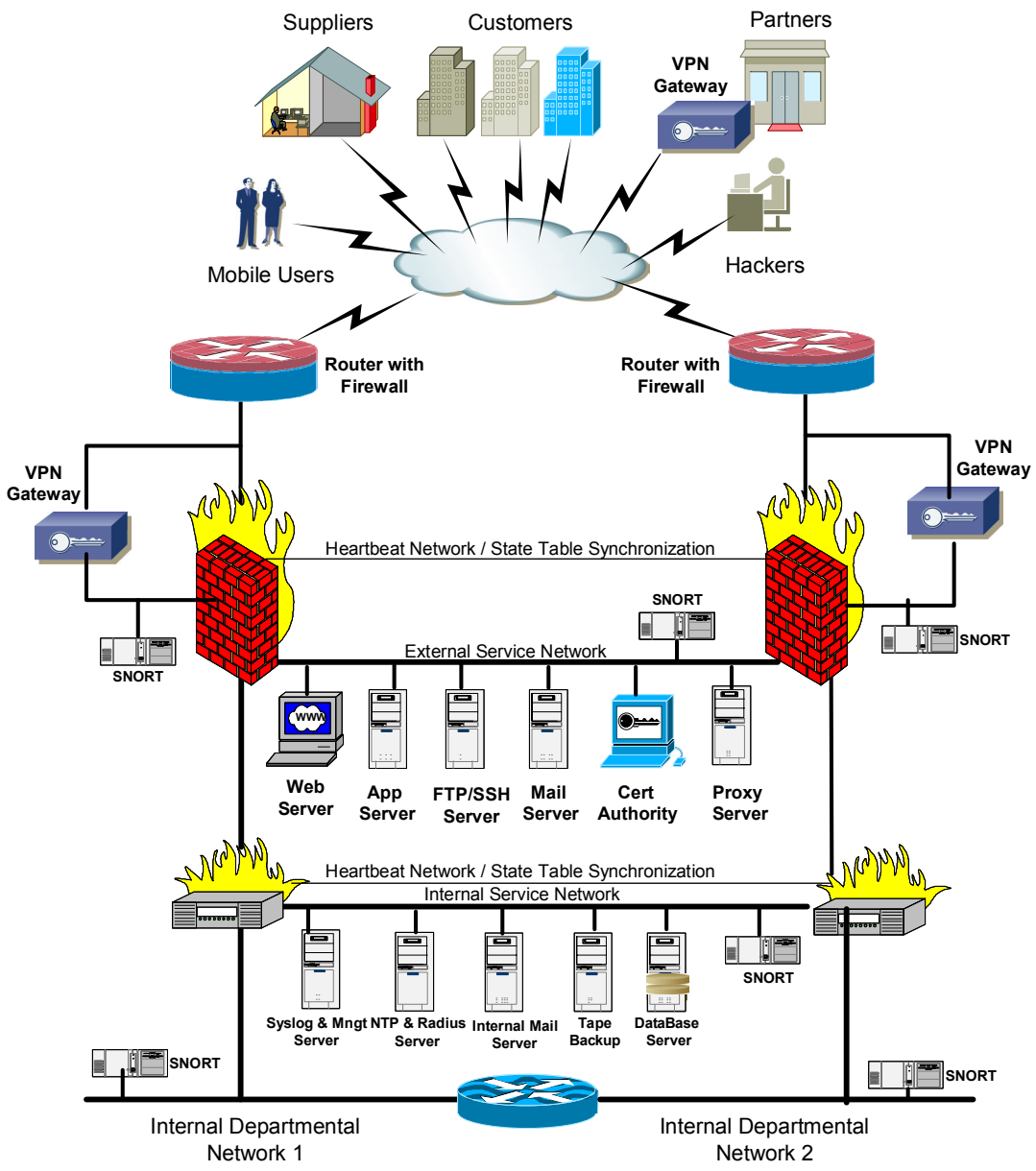
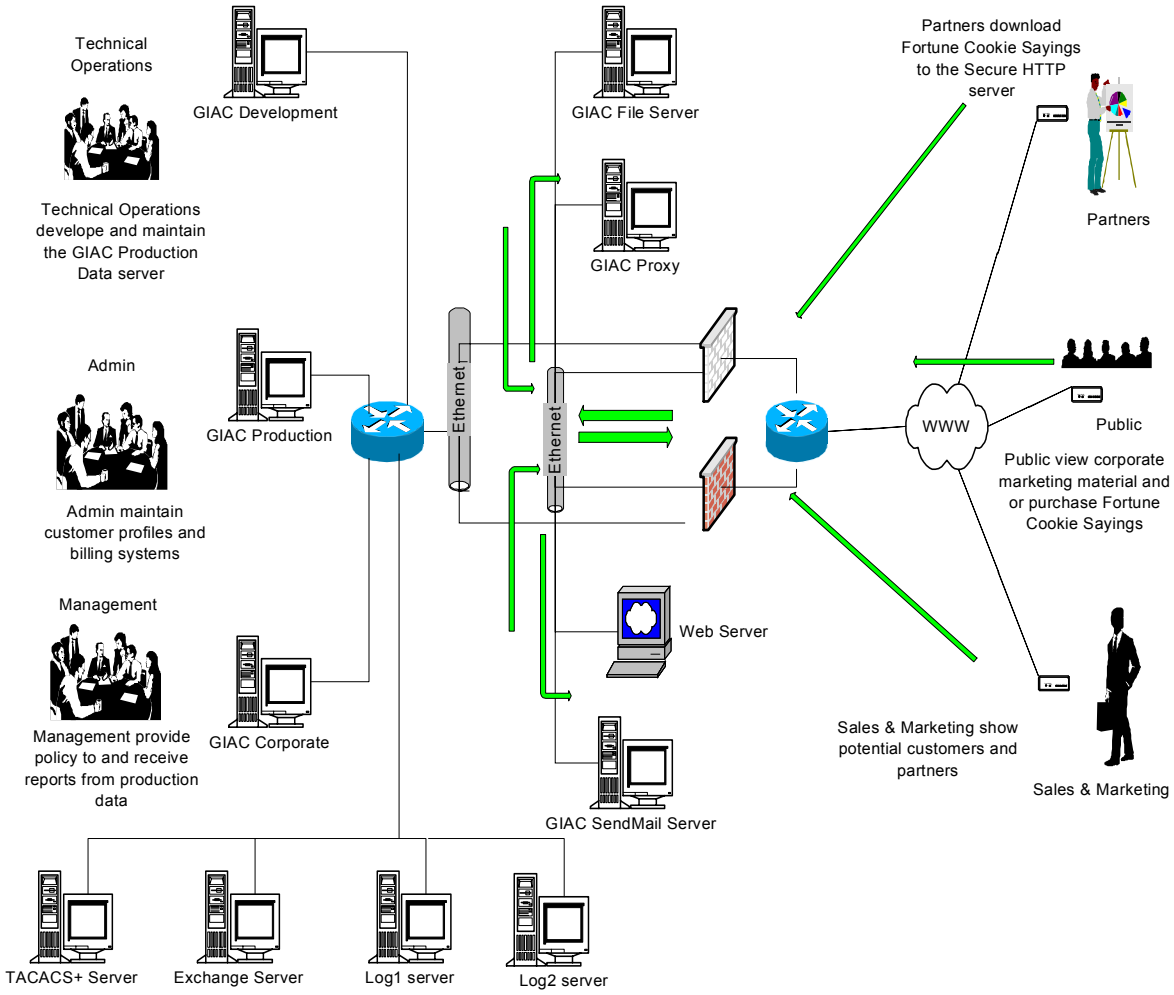


Fig. 3 Enhanced Secure Perimeter Network Design Diagram

Assignment 4 Design Under Fire

The network design by Stephen Monahan is selected to demonstrate the potential risks due to the vulnerabilities of various hardware and software components or the design itself. The design was published in April/May 2002 and can be found at http://www.giac.org/practical/Stephen_Monahan_GCFW.doc.

The following diagram shows the key components of the perimeter network design proposed by Stephen:



4.1 Information Gathering

The following information can be found from Stephan's document:

1. The table below summarizes the information on the key security components as described in the document:

Component	Hardware	Software	Other Information
Border Router	Dual Cisco 3620	IOS 12.0(5)	HSRP
Primary Firewall	Dual Cisco PIX 515	5.2	IDS, NAT, SYN Flood Guard and IP Fragment Guard are enabled.
VPN	Dual Cisco PIX 515	5.2	Client-initiated tunnels

   Note: Vulnerabilities on PIX firewall are search for version 5.2, since there is no detailed version number available (for example, 5.2(3)).

2. Part of the anti-spoofing statements in ACL 107 to restrict in-bound access is not properly configured on the border router. In stead of specifying the GIAC registered public address 208.10.2.0/24 as identified in other parts of the configuration file, the anti-spoofing statements restrict the 208.10.1.0/24:

```
! Outside link to ISP
    interface Serial0/0
    description Serial link to ISP
    ip address 208.10.2.137 255.255.255.248
    ip access-group 107 in

! Deny GIAC registered addresses
    access-list 107 deny   ip 208.10.1.0 0.0.0.255 any log
    access-list 107 deny   udp 208.10.1.0 0.0.0.255 any log
```

   The network address entry of 208.10.1.0 is probably just a typographical error. However, just like any careless mistakes made in real life, this can posed serious risk to the security of the enterprise network. Unfortunately, this error in address spoofing restriction also escaped detection during the audit phase because the only attempt to test the effectiveness of the perimeter router network address filtering was against a private address 192.168.1.15 (it is not clearly documented as to what device is this and why is it selected for audit):

   Command: nmap -sS -S192.168.1.15 -e0 –p80 208.10.2.3

   Because of this implementation error, the border router in Stephan's design is open to spoofing attack from outside.

3. There are also several configuration errors in the access control implementation on the PIX firewall. The most serious one is the lack of access control list applied to the interface “Ethernet 0 dmz”. Although the following command seems to be there to do the job,

   Access-group acl_dmz_int out interface dmz

   The fact that the “access-list acl_dmz_int” is completely missing effectively means that the traffic from the dmz to the Internet or the corporate networks will be dropped by the implicit “deny all” command. Another observation on the above statement is that, even if the access-list acl_dmz_int does exist, it will not take effect anyway if applied in the “out” direction on a PIX interface.

   On controlling inbound access from the Internet, the access list “acl_int_dmz” in the configuration allows only web traffic; while others including smtp, DNS and https will be dropped by the implicit “deny all” function because they are not defined in the access-list:

   !Allow any host to access the web server
   Access-list acl_int_dmz permit tcp any host 208.10.2.3 eq www

   Access-group acl_int_dmz in interface outside

4. There are also duplications in the use of IP addresses. For example, 208.10.2.2 is used for both the GIAC_PIX1/PIX2 (as the HSRP address) and the Sendmail server; IP address 208.10.2.3 is used for the GIAC_PIX1 and the Web server, and again 208.10.2.4 is used for both GIAC_PIX2 and the Proxy Server / DNS:

Comment	GIAC_CORP1	GIAC_PIX1	GIAC_PIX2	GIAC_PER1	GIAC_PER2
Management LAN	192.168.1.0/26				
Administration LAN	192.168.1.64/26				
Technology LAN	192.168.1.128/26				
Shared Systems LAN	192.168.1.192/26				
GIAC_CORP/ GIAC_PIX	192.168.2.248/29				
Shared Services LAN	208.10.2.0/25	208.10.2.2/25* 208.10.2.3/25	208.10.2.2/25* 208.10.2.4/25		
GIAC_PIX /GIAC_PER		208.10.2.129/29* 208.10.2.130/29	208.10.2.129/29* 208.10.2.131/29	208.10.2.132/29* 208.10.2.133	208.10.2.132/29* 208.10.2.134
GIAC_PER /Internet				208.10.2.137* 208.10.2.138	208.10.2.137* 208.10.2.139
Proxy Server/DNS	208.10.2.4				
File Server	208.10.2.5				
Web Server	208.10.2.3				
Sendmail Server	208.10.2.2				

* HSRP address

4.2 Known Vulnerabilities

Below are some of the web sites providing up-to-date information on vulnerabilities and attacks on a broad range of devices including firewalls:

www.securityfocus.org
www.cert.org
www.incidents.org
www.cve.mitre.org
icat.nist.gov
archives.neohapsis.com
www.sans.org/newlook/digests/SAC.htm

The following vulnerabilities are found from the above sites on Cisco PIX Firewall version 5.2 used in Stephan's design:

2002-06-27 Cisco SSH Denial of Service Vulnerabilities[58]

Bugtraq ID	5114
Class	Fail to Handle Exceptional Conditions
CVE	CAN-2002-1024
Published	June 27, 2002
Cisco Vulnerability ID	
	CSCdw29965 for PIX
	CSCdw33027 for IOS
Description:	While addressing vulnerabilities described in http://www.cisco.com/warp/public/707/SSH-multiple-pub.html, a denial of service condition has been inadvertently introduced into firmware upgrades. Firmware for routers and switches (IOS), Catalyst 6000 switches running Catalyst OS, Cisco PIX Firewall and Cisco 11000 Content Service Switch devices may be vulnerable. Cisco has reported[59] that when an attacker tries to exploit the vulnerability VU#945216 (described in the CERT/CC Vulnerability Note at http://www.kb.cert.org/vuls/id/945216) the SSH module will consume too much of the processor's time, effectively causing a DoS. As many of these devices are critical infrastructure components, more serious network outages may occur. This vulnerability is located in a segment of code that was introduced to defend against exploitation of CRC32 weaknesses in the SSH1 protocol (see VU#13877). The attack detection function (detect_attack, located in deattack.c) makes use of a dynamically allocated hash table to store connection information that is then examined to

detect and respond to CRC32 attacks. By sending a crafted SSH1 packet to an affected host, an attacker can cause the SSH daemon to create a hash table with a size of zero. When the detection function then attempts to hash values into the null-sized hash table, these values can be used to modify the return address of the function call, thus causing the program to execute arbitrary code with the privileges of the SSH daemon, typically root.
In some cases the device will reboot. The condition is due to a failure of the Cisco SSH implementation to properly process large SSH packets. In order to be exposed SSH must be enabled on the device.

Solution Patches and upgrades to eliminate this vulnerability can be found at http://www.cisco.com/warp/public/707/SSH-scanning.shtml#Software.

Usability for Attack Purpose:
Potentially this recently identified vulnerability can be used for a denial of service attack against the PIX firewall.

2002-06-21. Weak Cisco Password Encryption Algorithm[60]

CVE CAN-2002-0954
Published June 21, 2002
Cisco Vulnerability ID N/A (see Cisco Response below)
Description: The encryption algorithm used by Cisco PIX Firewall software to encrypt passwords for "enable" and "passwd" commands is very fast...too fast. An off-line password guessing attack could be really effective against this kind of passwords.

The following details is available from http://archives.neohapsis.com/archives/vulnwatch/2002-q2/0121.html:

Cisco PIX passwords are limited to a length of 16 Bytes, so in theory there are 255^16 possible passwords, but in real life there are about 80^16 useful password combinations, take a look at your keyboard to verify, even if strong passwords are used. Cisco's password encryption is based on base64 encoded MD5 hashes. Routers IOS uses 1000 MD5 Update rounds to make password brute forcing attacks harder, but the PIX firewall uses only one MD5 update and then the digest is base64 encoded.

For base64 encoding Cisco uses the _crypt_to64() Function of the FreeBSD libcrypt library.

Here's the code to compute PIX password hashes:

```
==========================================
        MD5Context ctx1;
        unsigned char final[MD5_SIZE+1];
        unsigned char cleartext [16+1];
        unsigned char cisco_encoded [16+1];

        memset(cisco_encoded,0,sizeof(cisco_encoded));
        memset(cleartext,0,sizeof(cleartext));
        strcpy((char*) cleartext,"test");

        MD5Init2(&ctx1);
        MD5Update2(&ctx1,(unsigned char*) cleartext,16);
        MD5Final2(final,&ctx1);

        char* p = (char*) cisco_encoded;
        _crypt_to64(p,*(unsigned long*) (final+0),4); p += 4;
        _crypt_to64(p,*(unsigned long*) (final+4),4); p += 4;
        _crypt_to64(p,*(unsigned long*) (final+8),4); p += 4;
        _crypt_to64(p,*(unsigned long*) (final+12),4); p += 4;
```

Due to some weaknesses in the MD5 hash algorithm (den Boer and Bosselaers found a so called pseudo-collision) there may be more effective attacks in the future.

Exploit — Password crackers can be used for off-line password attacks.

Cisco Response (by Damir Rajnovic <gaus@cisco.com>)
http://online.securityfocus.com/archive/1/282037/2002-08-25/2002-08-31/0
When considering the published report one must take the following into the account:
*) The password length and quality is very important.

Using passwords with ten characters or more will make brute force attack much harder up to the point when they become computational infeasible using the present algorithms and general purpose computers. Using passwords which are not easy to guess, with a mixture of lower and upper case letters and numbers, will make off line dictionary attack much harder.
*) This attack is effective only if an attacker can capture the Configuration file.

In order to prevent interception of the configuration files for the PIX particularly during transfer between devices, customers should review their policies and practices concerning storage and transfer of PIX configuration files.

Critical points of review should include firewall management systems and backup procedure (including media and disposal).
*) By default PIX will not accept interactive connections on any port except the console port.

Even if an attacker possesses the password, an interactive administrative session must be established to the trusted/ protected (or externally via IPSEC) interface of the PIX, in order to take advantage of this. Cisco configuration guides recommend explicit and careful configuration of permitted administrative hosts, and default configuration requires the administration hosts to be explicitly configured.
*) Users are encouraged to use the local database that uses "salted" passwords. The example of a configuration is present here:

```
username <user> password <secret password>
aaa authentication enable console LOCAL
```

Alternatively, users can consider using TACACS+ or Radius for authentication.
The practice of having a single, shared enable password should be discouraged in favor of creating a separate usernames with the appropriate privilege level. Additionally, a practice of sharing the same configuration file among multiple PIXes should be reconsidered. For the exact syntax of PIX command consult http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_62/cmdref/ index.htm

Usability for Attack Purpose:

To exploit this vulnerability, attackers have to somehow obtain a copy of the configuration file with the encrypted/hashed password. Furthermore, even with a cracked password, an attack from outside will be successful only if remote telnet or administration from outside is allowed by the firewall policy that usually is not true if best security practices are followed.

2001-09-26 Cisco PIX Firewall SMTP Content Filtering Evasion Vulnerabilities Re-Introduction[61]

Bugtraq ID 3365
Class Fail to Handle Exceptional Conditions
CVE CVE-MAP-NOMATCH
Published Sept 26, 2001
Cisco Vulnerability ID
CSCdu47003

Description. An old vulnerability (Bugtraq ID 1698, cve CVE-2000-1022) that allowed for bypassing of SMTP content filtering has been re-introduced into PIX firmware.

Information below is from (http://online.securityfocus.com/bid/1698/discussion/).
Like other firewalls, the Cisco PIX Firewall implements technology that reads the contents of packets passing through it for application-level filtering. In the case of SMTP, it can be configured so only certain SMTP commands can be allowed through. When receiving messages, it allows all text through between "data" and "<CR><LF><CR><LF>.<CR><LF>", as this is where the body of the message would normally go and there could be words in it that are SMTP commands which shouldn't be filtered. Due to the nature of SMTP and flaws in exceptional condition handling of PIX, it is reportedly possible to evade the SMTP command restrictions by tricking the firewall into thinking the body of the message is being sent when it isn't. During communication with an SMTP server, if the "data" command is sent before the more important information is sent, such as "rcpt to", the SMTP server will return error 503, saying that rcpt was required. The firewall, however, thinks everything is all right and will let everything through until receiving "<CR><LF><CR><LF>.<CR><LF>". It is then possible for the attacker to do whatever he wishes on the email server.

Exploit From http://online.securityfocus.com/bid/1698/exploit/
naif <naif@inet.it>'s Bugtraq post:

> Here an example of what could be done exploiting this bug:
>
> helo ciao
> mail from: pinco@pallino.it
> data (From here pix disable fixup)
> expn guest (Now i could enumerate user
> vrfy oracle and have access to all command)
> help

```
        whatever command i want
        quit
```

Solution Cisco as of 09/26/2001 released an advisory on this vulnerability titled "Cisco Secure PIX Firewall Mailguard Vulnerability" at http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-pub.shtml.

Usability for Attack Purpose:

To exploit this vulnerability, attackers must be able to make connections to an SMTP mail server protected by the PIX firewall. As noted in Section 4.1, access-list acl_int_dmz allows only Web (www) traffic only from the Internet via the PIX firewall to the dmz network, while all other traffic including smtp will be dropped. For this reason, this vulnerability cannot be used to attack Stephan's design, even though no customers or suppliers can ever send any mail to GIAC, but that is not a vulnerability issue.

2000-10-03 Cisco PIX PASV Mode FTP International Address Disclosure Vulnerabilities[62]

Bugtrag ID 1877
Class Fail to Handle Exceptional Conditions
CVE CVE-2000-1027
Published Oct 03, 2000
Description : It is possible to configure the PIX so that it hides the IP address of internal ftp servers from clients connecting to it. By sending a number of requests to enter passive ftp mode (PASV) during an ftp session, the IP address will eventually be disclosed. It is not known what exactly causes this condition.
This has been verified on versions 5.2(4) and 5.2(2) of the PIX firmware and probably affects other versions.
Exploit: The following exploit was submitted by Fabio Pietrosanti (naif) <naif@inet.it> (/data/vulnerabilities/exploits/pixpasv.sh).

```
# sent by: Fabio Pietrosanti (naif) <naif@inet.it>
# try to dos pix using PASV bomb

echo "USER ftptest99"
sleep 2
echo PASS ftptest99
sleep 2
echo SYST
while true
    do
        echo PASV
        sleep 1
        echo PASV
        echo PASV
        sleep 1
```

```
                echo PASV
                echo PASV
                sleep 1
                echo PASV
               echo PASV
                sleep 1
        done
```

It must be run repeatedly on the target server before the internal IP address will be disclosed.

Solution: Currently there is no security patch that SecurityFocus is aware of.

Usability for Attack Purpose:

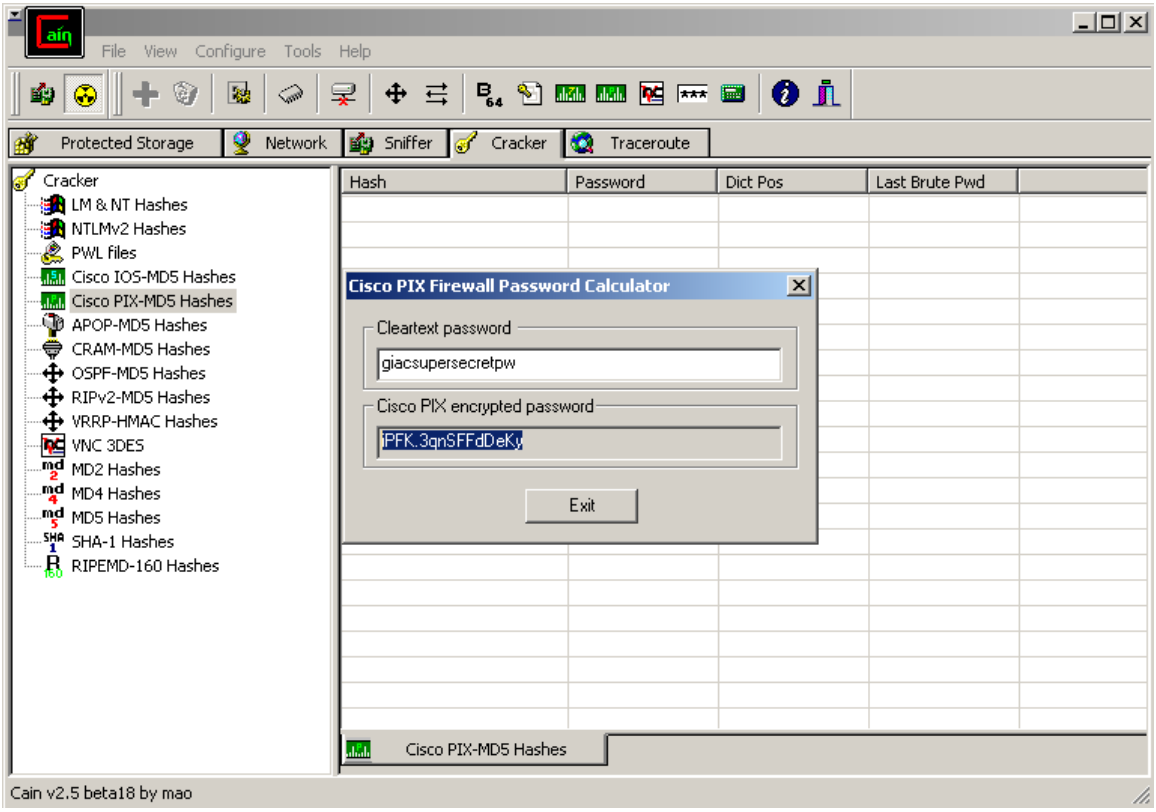
This vulnerability will not be useful for attack purpose against Stephan's design for two reasons. Firstly, the design has no indication that there is an internal ftp server whose address is hidden by the PIX firewall. Even if there is an ftp server, it is most likely to be the one shown as "file server" located in the dmz on the diagram with a public address of 208.10.2.5 as listed on the IP address table (see section 4.1). Secondly, as noted in Section 4.1, access-list acl_int_dmz allows only Web (www) traffic only from the Internet via the PIX firewall to the dmz network, while all other traffic including ftp will be dropped by the implicit deny command. In real life, this means that no customers or suppliers can transfer files to GIAC via ftp, but that is a different story.

4.3 Attacks

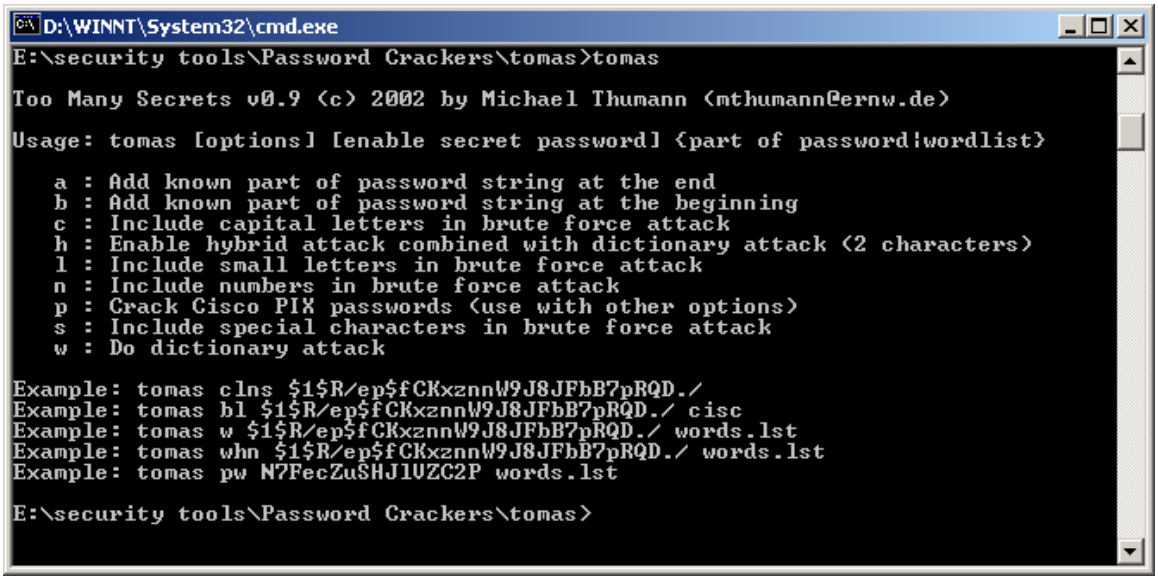
4.3.1 An Attack Against the Firewall Itself - Attacking the Weak Cisco PIX Enable Password Encryption Algorithm

Attempts are made to attack the Weak Cisco PIX Enable Password Encryption Algorithm vulnerability by using the password recovery utilities Cain & Abel v2.5 Beta18[63] and Too Many Secrets v0.9[64]. As described in Section 4.2, the weakness is due to the fact that Cisco PIX passwords are limited to a length of 16 bytes, so in theory there are 255^16 possible passwords, but in real life there are about 80^16 useful password combinations, (counting only the unique key characters available on the keyboard), even if strong passwords are used. Also, Cisco's password encryption is based on base64 encoded MD5 hashes. Routers IOS uses 1000 MD5 Update rounds to make password brute forcing attacks harder, but the PIX firewall uses only one MD5 update and then the digest is base64 encoded.

The following diagram shows the use of Cisco PIX firewall Password Calculator from Cain & Abel:



And the next diagram shows the use of Too Many Secrets v0.9:



As pointed out correctly by Damir Rajnovic of Cisco Systems, the chance of successful password cracking attacks largely depends on the quality and the

length of the passwords. A high quality password using 10 or more alphanumeric characters consisting of upper and lower cases is not likely to be cracked in a practical sense. Furthermore, if there are proper security policy and procedure in place for firewall administration and for password and configuration file protection during transit or storage, it will mitigate significantly the risk coming this vulnerability.

The above exercise demonstrates clearly the importance of the Defense in Depth principle.

4.3.2 A Denial of Service Attack - Attacking the SSH Denial of Service Vulnerability

Attempt will be made to attack the PIX firewall on the Cisco SSH Denial of Service Vulnerability (Cisco Vulnerability CSCdw29965). Chance of success is relatively high because it was only published since June 2002.

Information below on the SSH vulnerability is extracted from the article "SSH1 remote root exploit" [65] from Korpinen Pekka and Lyytikäinen Kalle which provides an excellent explanation on the SSH vulnerability as well as the development and implement of an exploit.

The SSH (Secure Shell) protocol provides a standardized way to communicate on a secured channel. All communications between SSH client and SSH daemon are encrypted. The encryption is done using a symmetric cipher (DES, 3DES and Blowfish, for example). The encryption key is exchanged at the beginning of the connection using RSA keys.

The (SSH) client creates a connection to the (SSH) server that is listening on a specific port, usually 22. The server accepts the connection and responds by sending back its version identification string. The client sends its own identification. After both sides have been identified they switch to a packet based binary protocol. The server sends its host key. The host key is a unique RSA key used to authenticate the host and it is regenerated every hour. The client generates a 256-bit session key, encrypts it using both RSA keys, and sends the encrypted session key and selected cipher type to the server. Now both sides turn on encryption using the selected encryption algorithm and key. Finally the server sends an encrypted confirmation message. At this point the channel is secured. The client then tries to authenticate itself using any of the available authentication methods (password, RSA authentication etc). After successful authentication, the client can allocate a pseudo tty, start port forwarding, or execute a shell command.

When the client or the server receives an encrypted packet, it checks if the packet is tampered with using the crc32 compensation attack detector. The

detection algorithm checks the packet before it is parsed in any way. The first case when this algorithm is used is when the client sends its authentication request. Maximum packet length is about 256k bytes.

The crc32 compensation attack detector in various implementations of SSH1 protocol, including Cisco's, has a bug that allows an attacker to write to memory locations on the server side. The attack detection function (detect_attack, located in deattack.c) makes use of a dynamically allocated hash table to store connection information that is then examined to detect and respond to CRC32 attacks. By sending a crafted SSH1 packet to an affected host, an attacker can cause the SSH daemon to create a hash table with a size of zero. When the detection function then attempts to hash values into the null-sized hash table, these values can be used to modify the return address of the function call, thus causing the program to execute arbitrary code with the privileges of the SSH daemon, typically root.

An exploit implementation by Korpinen Pekka and Lyytikäinen Kalle describes the exploit application uxp2, which is based on a proprietary exploit called "shack"[66]. With uxp2.c downloaded, configure the target host address to be the PIX firewall outside interface address

```
// Target Host
Char host [ ] = "208.10.2.129
```

And the target port to be 22

```
// Target port
int port = 22
```

When the exploit application is compiled with the above configuration, attach can be executed by running the command "./uxp2", and it will cause the SSH module to consume too much of the processor's time, effectively causing a Denial of Service attack.

4.3.3 An Attack Plan to Compromise an Internal System through the Perimeter System

As mentioned Section 4.1, there is no access list in the PIX firewall configuration to allow traffic from the public servers in the dmz to communicate to the Internet, so attack to an internal system will be a real challenge. There is, however, one rule in the internet to dmz ACL allowing inbound traffic to the web server:

```
!Allow any host to access the web server
        Access-list acl_int_dmz permit tcp any host 208.10.2.3 eq www

Access-group acl_int_dmz in interface outside
```

As there is no information on the hardware and software versions of the web server, an assumption is made here that we have it finger-printed, through scanning from outside, as Microsoft IIS 5.0 running on Windows 2000 platform. With that information, a search on SecurityFocus shows that there is a Malformed HTTP Host Header Field Denial of Service Vulnerability[67] reported very recently (Oct 7, 2002). This remotely exploitable denial of service occurs upon receipt of a malformed HOST field in a HTTP request for 'shtml.dll'. It is possible to reproduce this condition by sending an HTTP POST request with a HOST header field that is composed of an excessive number of slashes (/). Once again, the web server becomes a potential target for DOS attack as there is a very good chance that latest security patch has not been applied.

Endnotes

[1] SANS Institute, Track 2 – Firewall, Perimeter Protection and VPNs, "Firewall 101: Perimeter Protection with Firewalls", 2002, p18

[2] SANS Institute, "System Administrator – Security Best Practices", August 16, 2001, URL: http://rr.sans.org/practice/sysadmin.php

[3] CERT Coordination Center, "Securing Network Servers", URL: http://www.cert.org/security-improvement/modules/m10.html

[4] Oracle Networking Services FAQ, Dec 15, 2001, URL: http://www.orafaq.com/faqnet.htm#WHAT

[5] IANA, Port Numbers, URL: http://www.iana.org/assignments/port-numbers

[6] Open SSH, URL: http://www.openssh.org/

[7] OpenSSH Security Advisory (adv.Trojan), URL: http://www.openssh.org/txt/trojan.adv

[8] RFC 2827, Network Ingress Filter, URL: http://www.faqs.org/rfcs/rfc2827.html

[9] RFC 3013 Recommended Internet Service Provider Security Services and Procedures, URL: http://www.faqs.org/rfcs/rfc3013.html

[10] SANS Institute, Track 2 – Firewalls, Perimeter Protection and VPNs, "2.1 TCP/IP for Firewall", 2002, p 8-20

[11] Cisco, Using PIX Firewall Commands, URL: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/cmdref/intro.htm

[12] Veritas, Netbackup BusinessServer, URL: http://www.veritas.com/products/category/ProductDetail.jhtml?productId=nbbs&_requestid=65723

[13] Veritas Support, URL: http://seer.support.veritas.com/docs/237796.htm

[14] Time Synchronization Server, URL: http://www.eecis.udel.edu/~ntp

[15] RFC 1350, URL: http://www.faqs.org/rfcs/rfc1350.html

[16] Cisco, "How NAT Works?", URL: http://www.cisco.com/warp/public/556/nat-cisco.shtml

[17] RFC 1918 Address Allocation for Private Internets (1996), URL: http://www.faqs.org/rfcs/rfc1918.html

[18] CERT, Installing, Configuring and Using TCP Wrapper, URL: http://www.cert.org/security-improvement/implementations/i041.07.html

[19] Oracle Advanced Security, URL: http://otn.oracle.com/docs/deploy/security/pdf/a85430_01.pdf

[20] RSA SecurID Token, URL: http://www.rsasecurity.com/products/securid/tokens.html

[21] National Security Agency, Security Recommendation Guides, "Defense in Depth", URL: http://nsa2.www.conxion.com/support/guides/sd-1.pdf

[22] SANS Institute, Track 2 – Firewall, Perimeter Protection and VPNs, "Firewall 101: Perimeter Protection with Firewalls", 2002, p.26

[23] Gerhard Cronje, "Choosing The Best Firewall" April 10, 2001,
URL: http://rr.sans.org/toppapers/best.php

[24] Curtin, Matt and Ranum, Marcus J. "Internet Firewalls: Frequently Asked Questions" December 1, 2000, URL: http://www.interhack.net/pubs/fwfaq/

[25] GIAC, Certified Students and Posted Practicals, URL: http://www.giac.org/GCFW.php

[26] Cisco, "Overview, Cisco PIX Firewall, Cisco IOS Firewall Feature Set",
URL: http://www.cisco.com/warp/public/cc/pd/rt/2600/prodlit/flrrr_ov.htm

[27] SNORT, The Open source Network Intrusion Detection System, URL: http://www.snort.org/

[28] Cisco IOS Software, "Release Designations Defined",
URL: http://www.cisco.com/kobayashi/library/iosplanner/reldesignation.html#GD

[29] SANS Institute, Track 2 – Firewall, Perimeter Protection and VPNs, "Firewall 102: Perimeter Protection and Defense In-Depth" 2002, p6

[30] Cisco Tech Notes, "Improving Security on Cisco Routers",
URL: http://www.cisco.com/warp/public/707/21.html

[31] SAFE: A Security Blueprint for Enterprise Networks, Cisco Perimeter Security Solution, URL: http://www.cisco.com/en/US/netsol/ns110/ns129/ns131/ns118/networking_solutions_implementation_white_paper09186a008009c8b6.shtml

[32] National Security Agency, "Router Security Configuration Guide", July 9, 2002
URL: http://nsa2.www.conxion.com/cisco/guides/cis-2.pdf

[33] SANS Institute, Track 2 – Firewall, Perimeter Protection and VPNs, "Firewall 102: Perimeter Protection and Defense In-Depth" 2002, p51-58

[34] Using PIX Firewall Commands,
URL: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/cmd_ref/intro.htm

[35] Cisco, Handling ICMP Pings with the PIX Firewall, URL:
http://www.cisco.com/warp/public/110/31.html

[36] Cisco Security Advisory: Cisco VPN 3000 Concentrator Multiple Vulnerabilities, Sept. 3, 2003, URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_security_advisory09186a00800c8154.shtml

[37] RFC 2401, URL: http://www.ietf.org/rfc/rfc2401.txt

[38] B. Schneier and Mudge, "Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP)", Nov. 1998, URL: http://www.counterpane.com/pptp-paper.html

[39] Bruce Schneier, "Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2), 1999, URL: http://www.counterpane.com/pptpv2-paper.html

[40] RFC 2409, URL: http://www.ietf.org/rfc/rfc2409.txt

[41] RFC 2402, URL: http://www.ietf.org/rfc/rfc2402.txt

[42] RFC 2406, URL: http://www.ietf.org/rfc/rfc2406.txt

[43] Configuring Access Control Lists, URL:
http://www.cisco.com/univercd/cc/td/doc/product/l3sw/4908g_l3/ios_12/10w518e/config/acl_cnfg.htm

[44] Lock-and-Key: Dynamic Access List, URL: http://www.cisco.com/warp/public/69/13.html

[45] Port Numbers by IANA, URL: http://www.iana.org/assignments/port-numbers
Protocol Numbers by IANA, URL: http://www.iana.org/assignments/protocol-numbers

[46] SANS/FBI Top 20 List, v3.1, Oct 7, 2002, URL: http://www.sans.org/top20/

[47] Best Current Practice (BCP) Sub-Series, URL: http://www.csrc.nist.gov/fasp/

[48] insecure.org, URL: http://www.insecure.org/nmap/

[49] Sniffer Technologies CyberCop Product End-of-Line Customer FAQ,
URL: http://www.sniffer.com/other/jump/cybercop-eol.asp

[50] Nmap network security scanner man page,
URL: http://www.insecure.org/nmap/data/nmap_manpage.html

[51] Whois at InterNic.org, URL: http://www.internic.org/whois.html

[52] Whois at Network Solutions Inc, URL: http://www.netsol.com/cgi-bin/whois/whois

[53] ARIN Whois, URL: http://ws.arin.net/cgi-bin/whois.pl

[54] Bugtraq Information Database, SecurityFocusOnline, URL: http://online.securityfocus.com/bid

[55] Common Vulnerabilities and Exposure, URL: http://www.cve.mitre.org/

[56] CVE, URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-1024

[57] Security Advisory: Scanning for SSH Can Cause a Crash,
URL: http://www.cisco.com/warp/public/707/SSH-scanning.shtml

[58] SFOnline, Vulnerabilities by Vendor, Security Focus, URL: http://online.securityfocus.com/bid/5114

[59] Security Advisory: Scanning for SSH Can Cause a Crash,
URL: http://www.cisco.com/warp/public/707/SSH-scanning.shtml

[60] Common Vulnerabilities and Exposure,
URL: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0954

[61] SFOnline, Vulnerabilities by Vendor, SecurityFocus, URL: http://online.securityfocus.com/bid/3365

[62] SFOnline, Vulnerabilities by Vendor, Security Focus, URL: http://online.securityfocus.com/bid/1877

[63] Cain & Abel version 2.5, URL: http://www.oxid.it/
[64] ERNW, URL: http://www.ernw.de/download/tomas.zip
[65] SSH1 Remote Root Exploit, Korpinen Pekka and Lyytikäinen Kalle, March 26, 2002,
URL: http://www.hut.fi/~kalyytik/hacker/ssh-crc32-exploit_Korpinen_Lyytikainen.html

[66] Packetstorm exploit archive, Shack exploit [online] [referenced March 20, 2002] <http://packetstorm.widexs.nl/0201-exploits/cm-ssh.tgz>

[67] Microsoft IIS Malformed HTTP Host Header Field Denial of Service Vulnerability, URL: http://online.securityfocus.com/bid/5907